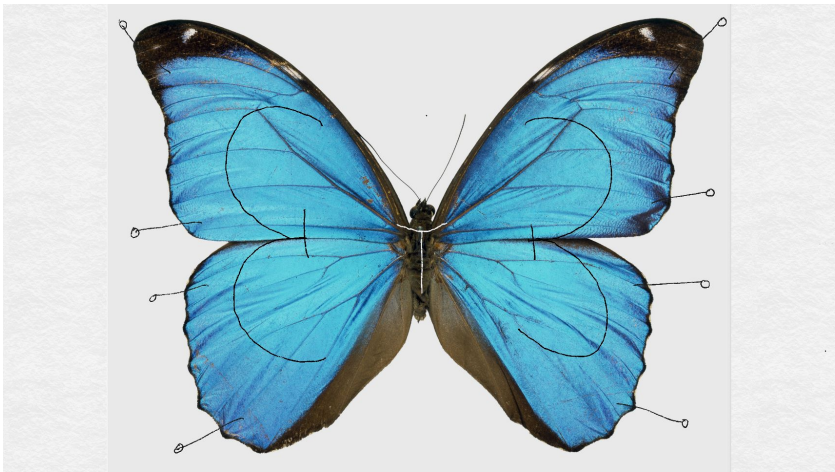# Algebraic Groups

The theory of group schemes of finite type over a field.

J.S. Milne

The book is a comprehensive introduction to the theory of algebraic group schemes over fields, based on modern algebraic geometry, but with minimal prerequisites.

Algebraic groups play much the same role for algebraists that Lie groups play for analysts. This book is the first comprehensive introduction to the theory of algebraic group schemes over fields, including the structure theory of semisimple algebraic groups, written in the language of modern algebraic geometry. When Borel, Chevalley, and others introduced algebraic geometry into the theory of algebraic groups, they used the algebraic geometry of the day, whose terminology conflicts with that of modern (post 1960) algebraic geometry. As Tits wrote in 1960, "the scheme viewpoint ... is not only more general but also, in many respects, more satisfactory." Indeed, allowing nilpotents gives a much richer and more natural theory.

The first eight chapters of the book study general algebraic group schemes over a field. They culminate in a proof of the Barsotti–Chevalley theorem realizing every algebraic group as an extension of an abelian variety by an affine group. The remaining chapters treat only affine algebraic groups. After a review of the Tannakian philosophy, there are short accounts of Lie algebras and finite group schemes. Solvable algebraic groups are studied in detail in Chapters 12-16. The final nine chapters treat reductive algebraic groups over arbitrary fields including the Borel–Chevalley structure theory. Three appendices review the algebraic geometry needed, the existence of quotients of algebraic groups, and root data.

The exposition incorporates simplifications to the theory by Springer, Steinberg, and others. Although the theory of algebraic groups can be considered a branch of algebraic geometry, most of those using it are not algebraic geometers. In the present work, prerequisites have been kept to a minimum. The only requirement is a first course in algebraic geometry including basic commutative algebra.

The cover picture illustrates Grothendieck's vision of a pinned reductive group: the body is a maximal torus T, the wings are the opposite Borel subgroups B, and the pins rigidify it (SGA 3, XXIII, p. 177). The background image is a Blue Morpho butterfly.

Contents

Preface

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

This book represents my attempt to write a modern successor to the three standard works, all titled *Linear Algebraic Groups*, by Borel, Humphreys, and Springer. More specifically, it is an exposition of the theory of group schemes of finite type over a field, based on modern algebraic geometry, but with minimal prerequisites.

It has been clear for fifty years that such a work has been needed.[1] When Borel, Chevalley, and others introduced algebraic geometry into the theory of algebraic groups, the foundations they used were those of the period (e.g., Weil 1946), and most subsequent writers on algebraic groups have followed them. Specifically, nilpotents are not allowed, and the terminology used conflicts with that of modern algebraic geometry. For example, algebraic groups are usually identified with their points in some large algebraically closed field K, and an algebraic group over a subfield k of K is an algebraic group over K equipped with a k-structure. The kernel of a k-homomorphism of algebraic k-groups is an object over K (not k) *which need not be defined over k*.

In the modern approach, nilpotents are allowed,[2] an algebraic k-group is intrinsically defined over k, and the kernel of a homomorphism of algebraic groups over k is (of course) defined over k. Instead of identifying an algebraic group with its points in some "universal" field, it is more convenient to identify it with the functor of k-algebras it defines.

The advantages of the modern approach are manifold. For example, the infinitesimal theory is built into it from the start instead of entering only in an ad hoc fashion through the Lie algebra. The Noether isomorphism theorems hold for

---

[1]"Another remorse concerns the language adopted for the algebrogeometrical foundation of the theory ... two such languages are briefly introduced ... the language of algebraic sets ... and the Grothendieck language of schemes. Later on, the preference is given to the language of algebraic sets ... If things were to be done again, I would probably rather choose the scheme viewpoint ... which is not only more general but also, in many respects, more satisfactory." Tits 1968, p. 2.

[2]To anyone who asked why we need to allow nilpotents, Grothendieck would say that they are already there in nature; neglecting them obscures our vision.

algebraic group schemes, and so the intuition from abstract group theory applies. The kernels of infinitesimal homomorphisms become visible as algebraic group schemes.

The first systematic exposition of the theory of group schemes was in SGA 3. As was natural for its authors (Demazure, Grothendieck, . . .), they worked over an arbitrary base scheme and they used the full theory of schemes (EGA and SGA). Most subsequent authors on group schemes have followed them. The only books I know of that give an elementary treatment of group schemes are Waterhouse 1979 and Demazure and Gabriel 1970. In writing this book, I have relied heavily on both, but neither goes very far. For example, neither treats the structure theory of reductive groups, which is a central part of the theory.

As noted, the modern theory is more general than the old theory. The extra generality gives a richer and more attractive theory, but it does not come for free: some proofs are more difficult (because they prove stronger statements). In this work, I have avoided any appeal to advanced scheme theory. Unpleasantly technical arguments that I have not been able to avoid have been placed in separate sections where they can be ignored by all but the most serious students. By considering only schemes algebraic over a field, we avoid many of the technicalities that plague the general theory. Also, the theory over a field has many special features that do not generalize to arbitrary bases.

Introduction

The book can be divided roughly into five parts.

A. Basic theory of general algebraic groups (Chapters 1–8)

The first eight chapters cover the general theory of algebraic group schemes (not necessarily affine) over a field. After defining them and giving some examples, we show that most of the basic theory of abstract groups (subgroups, normal subgroups, normalizers, centralizers, Noether isomorphism theorems, subnormal series, etc.) carries over with little change to algebraic group schemes. We relate affine algebraic group schemes to Hopf algebras, and we prove that all algebraic group schemes in characteristic zero are smooth. We study the linear representations of algebraic group schemes and their actions on algebraic schemes. We show that every algebraic group scheme is an extension of an étale group scheme by a connected algebraic group scheme, and that every smooth connected group scheme over a perfect field is an extension of an abelian variety by an affine group scheme (Barsotti–Chevalley theorem).

Beginning with Chapter 9, all group schemes are affine.

B. Preliminaries on affine algebraic groups (Chapters 9–11)

The next three chapters are preliminary to the more detailed study of affine algebraic group schemes in the later chapters. They cover basic Tannakian theory, in which the category of representations of an algebraic group scheme plays the role of the topological dual of a locally compact abelian group, Jordan decompositions, the Lie algebra of an algebraic group, and the structure of finite group schemes. Throughout this work we emphasize the Tannakian point of view in which the group and its category of representations are placed on an equal footing.

C. Solvable affine algebraic groups (Chapters 12–16)

The next five chapters study solvable algebraic group schemes. Among these are the diagonalizable groups, the unipotent groups, and the trigonalizable groups.

An algebraic group G is diagonalizable if every linear representation of G is a direct sum of one-dimensional representations; in other words if, relative to some basis, the image of G lies in the algebraic subgroup of diagonal matrices in GL_n. An algebraic group that becomes diagonalizable over an extension of the base field is said to be of multiplicative type.

An algebraic group G is unipotent if every nonzero representation of G contains a nonzero fixed vector. This implies that every representation has a basis for which the image of G lies in the algebraic subgroup of strictly upper triangular matrices in GL_n.

An algebraic group G is trigonalizable if every simple representation has dimension one. This implies that every representation has a basis for which the image of G lies in the algebraic subgroup of upper triangular matrices in GL_n. The trigonalizable groups are exactly the extensions of diagonalizable groups by unipotent groups. Trigonalizable groups are solvable, and the Lie–Kolchin theorem says that all smooth connected solvable algebraic groups become trigonalizable over a finite extension of the base field.

D. Reductive algebraic groups (Chapters 17–25)

This is the heart of the book, The first seven chapters develop in detail the structure theory of split reductive groups and their representations in terms of their root data. Chapter 24 exhibits all the almost-simple algebraic groups, and Chapter 25 explains how the theory of split groups extends to the nonsplit case.

E. Appendices

The first appendix reviews the definitions and statements from algebraic geometry needed in the book. Experts need only note that, as we always work with schemes of finite type over a base field k, it is natural to ignore the nonclosed points (which we do).

The second appendix proves the existence of a quotient of an algebraic group by an algebraic subgroup. This is an important result, but the existence of nilpotents makes the proof difficult, and so most readers should simply accept the statement.

The third appendix reviews the combinatorial objects, root systems and root data, on which the theory of split reductive groups is based.

History

Apart from occasional brief remarks, we ignore the history of the subject, which is quite complex. Many major results were discovered in one situation, and then extended to other more general situations, sometimes easily and sometimes only with difficulty. Without too much exaggeration, one can say that all the theory of algebraic group schemes does is show that the theory of Killing and Cartan for

"local" objects over $\mathbb{C}$ extends in a natural way to "global" objects over arbitrary fields.

Conventions and notation

Throughout, k is a field and R is a finitely generated k-algebra.[1] All k-algebras and R-algebras are required to be commutative and finitely generated unless it is specified otherwise. Noncommutative algebras are referred to as "algebras over k" rather than "k-algebras". Unadorned tensor products are over k. An extension of k is a field containing k, and a separable extension is a separable algebraic extension. When V is a vector space over k, we often write V_R for $V \otimes R$; for $v \in V$, we let $v_R = v \otimes 1 \in V_R$. The symbol k^{a} denotes an algebraic closure of k and k^{s} (resp. k^i) denotes the separable (resp. perfect) closure of k in k^{a}. The characteristic exponent of k is p or 1 according as its characteristic is p or 0. The group of invertible elements of a ring R is denoted by $R^{\times}$. The symbol Alg_R denotes the category of finitely generated R-algebras.

An algebraic scheme over k (or algebraic k-scheme) is a scheme of finite type over k. An algebraic scheme is an algebraic variety if it is geometrically reduced and separated. By a "point" of an algebraic scheme or variety over k we always mean a closed point. For an algebraic scheme $(X, \mathcal{O}_X)$ over k, we often let X denote the scheme and $|X|$ the underlying topological space of closed points. For a locally closed subset Z of $|X|$ (resp. subscheme Z of X), the reduced subscheme of X with underlying space Z (resp. $|Z|$) is denoted by Z_{red}. The residue field at a point x of X is denoted by $\kappa(x)$. When the base field k is understood, we omit it, and write "algebraic scheme" for "algebraic scheme over k". Unadorned products of algebraic k-schemes are over k. See Appendix A for more details.

We let $\mathbb{Z}$ denote the ring of integers, $\mathbb{R}$ the field of real numbers, $\mathbb{C}$ the field of complex numbers, and $\mathbb{F}_p$ the field of p elements (p prime).

A functor is said to be an equivalence of categories if it is fully faithful and essentially surjective. A sufficiently strong version of the axiom of global choice then implies that there exists a quasi-inverse to the functor. We sometimes loosely refer to a natural transformation of functors as a map of functors.

All categories are locally small (i.e., the morphisms from one object to a second are required to form a set). When the objects form a set, the category is said to be small. A category is essentially small if it is equivalent to a small subcategory.

Let P be a partially ordered set. A greatest element of P is a $g \in P$ such that $a \leq g$ for all $a \in P$. An element m in P is maximal if $m \leq a$ implies $a = m$. A greatest element is a unique maximal element. Least and minimal elements are defined similarly. When the partial order is inclusion, we replace least and greatest with smallest and largest. We sometimes use $[x]$ to denote the class of x under an equivalence relation.

---

[1]Except in Appendix C, where R is a set of roots.

Following Bourbaki, we let $\mathbb{N} = \{0, 1, 2, \ldots\}$. An integer is positive if it lies in $\mathbb{N}$. A set with an associative binary operation is a semigroup. A monoid is a semigroup with a neutral element.

By $A \simeq B$ we mean that A and B are canonically isomorphic (or that there is a given or unique isomorphism), and by $A \approx B$ we mean simply that A and B are isomorphic (there exists an isomorphism). The notation $A \subset B$ means that A is a subset of B (not necessarily proper). A diagram $A \to B \rightrightarrows C$ is exact if the first arrow is the equalizer of the pair of arrows.

Suppose that p and q are statements depending on a field k and we wish to prove that $p(k)$ implies $q(k)$. If $p(k)$ implies $p(k^a)$ and $q(k^a)$ implies $q(k)$, then it suffices to prove that $p(k^a)$ implies $q(k^a)$. In such a situation, we simply say that "we may suppose that k is algebraically closed".

We often omit "algebraic" from such expressions as "algebraic subgroup", "unipotent algebraic group", and "semisimple algebraic group". After p. 162, all algebraic groups are affine.

We use the terminology of modern (post 1960) algebraic geometry; for example, for algebraic groups over a field k, a homomorphism is automatically defined over k, not over some large algebraically closed field.[2]

Throughout, "algebraic group scheme" is shortened to "algebraic group". A statement here may be stronger than a statement in Borel 1991 or Springer 1998 even when the two are word for word the same.[3]

All constructions are to be understood as being in the sense of schemes. For example, fibres of maps of algebraic varieties need not be reduced, and the kernel of a homomorphism of smooth algebraic groups need not be smooth.

Numbering

A reference "17.56" is to item 56 of Chapter 17. A reference "(112)" is to the 112th numbered equation in the book (we include the page number where necessary). Section 17c is Section c of Chapter 17 and Section Ac is Section c of Appendix A. The exercises in Chapter 17 are numbered 17-1, 17-2, . . .

Foundations

We use the von Neumann–Bernays–Gödel (NBG) set theory with the axiom of choice, which is a conservative extension of Zermelo–Fraenkel set theory with the axiom of choice (ZFC). This means that a sentence that does not quantify over a proper class is a theorem of NBG if and only if it is a theorem of ZFC. The advantage of NBG is that it allows us to speak of classes.

It is not possible to define an "unlimited category theory" that includes the category of *all* sets, the category of *all* groups, etc., and also the categories of

---

[2] As much as possible, our statements make sense in a world without choice, where algebraic closures need not exist.

[3] An example is Chevalley's theorem on representations; see 4.30.

functors from one of these categories to another. Instead, one must consider only categories of functors from categories that are small in some sense. To this end, we fix a family of symbols $(T_i)_{i \in \mathbb{N}}$ indexed by $\mathbb{N}$,[4] and let Alg_k^0 denote the category of k-algebras of the form $k[T_0, \ldots, T_n]/\mathfrak{a}$ for some $n \in \mathbb{N}$ and ideal $\mathfrak{a}$ in $k[T_0, \ldots, T_n]$. Thus the objects of Alg_k^0 are indexed by the ideals in some subring $k[T_0, \ldots, T_n]$ of $k[T_0, \ldots]$ – in particular, they form a set, and so Alg_k^0 is small. We call the objects of Alg_k^0 *small* k-algebras. If R is a small k-algebra, then the category Alg_R^0 of small R-algebras has as objects pairs consisting of a small k-algebra A and a homomorphism $R \to A$ of k-algebras. Note that tensor products exist in Alg_k^0 – in fact, if we fix a bijection $\mathbb{N} \leftrightarrow \mathbb{N} \times \mathbb{N}$, then $\otimes$ becomes a well-defined bi-functor.

The inclusion functor $\mathsf{Alg}_k^0 \hookrightarrow \mathsf{Alg}_k$ is an equivalence of categories. Choosing a quasi-inverse amounts to choosing an ordered set of generators for each finitely generated k-algebra. Once a quasi-inverse has been chosen, every functor on Alg_k^0 has a well-defined extension to Alg_k.

Alternatively, readers willing to assume additional axioms in set theory may use Mac Lane's "one-universe" solution to defining functor categories (Mac Lane 1969) or Grothendieck's "multi-universe" solution, and define a small k-algebra to be one that is small relative to the chosen universe.

Prerequisites

A first course in algebraic geometry (including basic commutative algebra). Since these vary greatly, we review the definitions and statements that we need from algebraic geometry in Appendix A. In a few proofs, which can be skipped, we assume somewhat more.

References

The citations are author–year, except for the following abbreviations:

CA = Milne 2017 (A Primer of Commutative Algebra).

DG = Demazure and Gabriel 1970 (*Groupes algébriques*).

EGA = Grothendieck 1967 (*Eléments de géometrie algébrique*).

SGA 3 = Demazure and Grothendieck 2011 (*Schémas en groupes, SGA 3*).

SHS = Demazure and Gabriel 1966 (*Séminaire Heidelberg–Strasbourg 1965–66*).

---

[4]Better, use $\mathbb{N}$ itself as the set of symbols.

Definitions and Basic Properties

Recall that k is a field, and that an algebraic k-scheme is a scheme of finite type over k. We let $* = \mathrm{Spm}(k)$.

a. Definition

An algebraic group over k is a group object in the category of algebraic schemes over k. In detail, this means the following.

DEFINITION 1.1. Let G be an algebraic scheme over k and let $m \colon G \times G \to G$ be a regular map. The pair (G, m) is an ***algebraic group*** over k if there exist regular maps

$$e \colon * \to G, \quad \mathrm{inv} \colon G \to G,$$

such that the following diagrams commute:

$$
\begin{array}{ccc}
G \times G \times G & \xrightarrow{\ \mathrm{id} \times m\ } & G \times G \\
\Big\downarrow{\scriptstyle m \times \mathrm{id}} & & \Big\downarrow{\scriptstyle m} \\
G \times G & \xrightarrow{\quad m \quad} & G
\end{array}
\qquad
\begin{array}{ccccc}
* \times G & \xrightarrow{\ e \times \mathrm{id}\ } & G \times G & \xleftarrow{\ \mathrm{id} \times e\ } & G \times * \\
& {\scriptstyle \simeq} \searrow & \Big\downarrow{\scriptstyle m} & \swarrow {\scriptstyle \simeq} & \\
& & G & &
\end{array}
\tag{1}
$$

$$
\begin{array}{ccccc}
G & \xrightarrow{\ (\mathrm{inv},\mathrm{id})\ } & G \times G & \xleftarrow{\ (\mathrm{id},\mathrm{inv})\ } & G \\
\Big\downarrow & & \Big\downarrow{\scriptstyle m} & & \Big\downarrow \\
* & \xrightarrow{\quad e \quad} & G & \xleftarrow{\quad e \quad} & *
\end{array}
\tag{2}
$$

When G is a variety, we call (G, m) a ***group variety***, and when G is an affine scheme, we call (G, m) an ***affine algebraic group***.

For example,

$$\mathrm{SL}_n \overset{\mathrm{def}}{=} \mathrm{Spm}\, k[T_{11}, T_{12}, \dots, T_{nn}]/(\det(T_{ij}) - 1)$$

becomes an affine group variety with the usual matrix multiplication on points. For many more examples, see Chapter 2.

Similarly, an **algebraic monoid** over k is an algebraic scheme M over k together with regular maps $m: M \times M \to M$ and $e: * \to M$ such that the diagrams (1) commute.

DEFINITION 1.2. A **homomorphism** $\varphi: (G, m) \to (G', m')$ of algebraic groups is a regular map $\varphi: G \to G'$ such that $\varphi \circ m = m' \circ (\varphi \times \varphi)$.

An algebraic group G is **trivial** if $e: * \to G$ is an isomorphism, and a homomorphism $G \to G'$ is **trivial** if it factors through $e': * \to G'$. We often write e for the trivial algebraic group.

DEFINITION 1.3. An **algebraic subgroup** of an algebraic group (G, m_G) over k is an algebraic group (H, m_H) over k such that H is a k-subscheme of G and the inclusion map is a homomorphism of algebraic groups. An algebraic subgroup is called a **subgroup variety** if its underlying scheme is a variety.

Let (G, m_G) be an algebraic group and H a nonempty subscheme of G. If $m_G | H \times H$ and $\mathrm{inv}_G | H$ factor through H, then $(H, m_G | H \times H)$ is an algebraic subgroup of G.

Let (G, m) be an algebraic group over k. For any field k' containing k, the pair $(G_{k'}, m_{k'})$ is an algebraic group over k', said to have been obtained from (G, m) by **extension of scalars** or **extension of the base field**.

Algebraic groups as functors

The K-points of an algebraic scheme X with K a field do not see the nilpotents in the structure sheaf. Thus, we are led to consider the R-points with R a k-algebra. Once we do that, the points capture *all* information about X.

1.4. An algebraic scheme X over k defines a functor

$$\tilde{X}: \mathsf{Alg}_k^0 \to \mathsf{Set}, \quad R \rightsquigarrow X(R).$$

For example, if X is affine, say, $X = \mathrm{Spm}(A)$, then

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

The functor $X \rightsquigarrow \tilde{X}$ is fully faithful (Yoneda lemma, A.33); in particular, $\tilde{X}$ determines X uniquely up to a unique isomorphism. We say that a functor from small k-algebras to sets is representable if it is of the form $\tilde{X}$ for an algebraic scheme X over k.

If (G, m) is an algebraic group over k, then $R \rightsquigarrow (G(R), m(R))$ is a functor from small k-algebras to groups.

Let X be an algebraic scheme over k, and suppose that we are given a factorization of $\tilde{X}$ through the category of groups. Then the maps

$$x, y \mapsto xy: X(R) \times X(R) \to X(R), \quad * \mapsto e: * \to X(R), \quad x \mapsto x^{-1}: X(R) \to X(R)$$

given by the group structures on the sets $X(R)$ define, by the Yoneda lemma, morphisms

$$m: X \times X \to X, \quad * \to X, \quad \text{inv}: X \to X$$

making the diagrams (1) and (2) commute. Therefore, (X, m) is an algebraic group over k.

Combining these two statements, we see that to give an algebraic group over k amounts to giving a functor $\mathsf{Alg}_k^0 \to \mathsf{Grp}$ whose underlying functor to sets is representable by an algebraic scheme. We write $\tilde{G}$ for G regarded as a functor to groups.

From this perspective, SL_n can be described as the algebraic group over k sending R to the group $\mathrm{SL}_n(R)$ of $n \times n$ matrices with entries in R and determinant 1.

The functor $R \rightsquigarrow (R, +)$ is represented by $\mathrm{Spm}(k[T])$, and hence is an algebraic group $\mathbb{G}_a$. Similarly, the functor $R \rightsquigarrow (R^\times, \times)$ is represented by $\mathrm{Spm}(k[T, T^{-1}])$, and hence is an algebraic group $\mathbb{G}_m$. See 2.1 and 2.2 below.

We often describe a homomorphism of algebraic groups by giving its action on R-points. For example, when we say that $\mathrm{inv}: G \to G$ is the map $x \mapsto x^{-1}$, we mean that, for all small k-algebras R and all $x \in G(R)$, $\mathrm{inv}(x) = x^{-1}$.

1.5. If (H, m_H) is an algebraic subgroup of (G, m_G), then $H(R)$ is a subgroup of $G(R)$ for all k-algebras R. Conversely, if H is an algebraic subscheme of G such that $H(R)$ is a subgroup of $G(R)$ for all small k-algebras R, then the Yoneda lemma (A.33) shows that the maps

$$(h, h') \mapsto hh': H(R) \times H(R) \to H(R)$$

arise from a morphism $m_H: H \times H \to H$ and that (H, m_H) is an algebraic subgroup of (G, m_G).

1.6. Consider the functor of k-algebras $\mu_3: R \rightsquigarrow \{a \in R \mid a^3 = 1\}$. This is represented by $\mathrm{Spm}(k[T]/(T^3 - 1))$, and so it is an algebraic group. We consider three cases.

(a) The field k is algebraically closed of characteristic $\neq 3$. Then

$$k[T]/(T^3 - 1) \simeq k[T]/(T - 1) \times k[T]/(T - \zeta) \times k[T]/(T - \zeta^2)$$

where $1, \zeta, \zeta^2$ are the cube roots of 1 in k. Thus, μ_3 is a disjoint union of three copies of $\mathrm{Spm}(k)$ indexed by the cube roots of 1 in k.

(b) The field k is of characteristic $\neq 3$ but does not contain a primitive cube root of 1. Then

$$k[T]/(T^3 - 1) \simeq k[T]/(T - 1) \times k[T]/(T^2 + T + 1),$$

and so μ_3 is a disjoint union of $\mathrm{Spm}(k)$ and $\mathrm{Spm}(k[\zeta])$ where ζ is a primitive cube root of 1 in k^s.

(c) The field k is of characteristic 3. Then $T^3 - 1 = (T - 1)^3$, and so μ_3 is not reduced. Although $\mu_3(K) = 1$ for all fields K containing k, the algebraic group μ_3 is not trivial. Certainly, $\mu_3(R)$ may be nonzero if R has nilpotents.

Homogeneity

Recall that, for an algebraic scheme X over k, we write $|X|$ for the underlying topological space of X, and $\kappa(x)$ for the residue field at a point x of $|X|$ (it is a finite extension of k). We can identify $X(k)$ with the set of points x of $|X|$ such that $\kappa(x) = k$ (CA 13.4). An algebraic scheme X over k is said to be **homogeneous** if the group of automorphisms of X (as a k-scheme) acts transitively on $|X|$. We shall see that an algebraic group is homogeneous when k is algebraically closed

1.7. Let (G, m) be an algebraic group over k. The map $m(k): G(k) \times G(k) \to G(k)$ makes $G(k)$ into a group with neutral element $e(*)$ and inverse map $\mathrm{inv}(k)$.

When k is algebraically closed, $G(k) = |G|$, and so $m: G \times G \to G$ makes $|G|$ into a group. The maps $x \mapsto x^{-1}$ and $x \mapsto ax$ ($a \in G(k)$) are automorphisms of $|G|$ as a topological space.

In general, when k is not algebraically closed, m does not make $|G|$ into a group, and even when k is algebraically closed, it does not make $|G|$ into a *topological* group.

1.8. Let (G, m) be an algebraic group over k. For each $a \in G(k)$, there is a translation map

$$l_a: G \simeq \{a\} \times G \xrightarrow{\ m\ } G, \quad x \mapsto ax.$$

For $a, b \in G(k)$,

$$l_a \circ l_b = l_{ab}$$

and $l_e = \mathrm{id}$. Therefore $l_a \circ l_{a^{-1}} = \mathrm{id} = l_{a^{-1}} \circ l_a$, and so l_a is an isomorphism sending e to a. Hence G is homogeneous when k is algebraically closed (but not in general otherwise; see 1.6(b)).

Density of points

Because we allow nilpotents in the structure sheaf, a morphism $X \to Y$ of algebraic schemes is not in general determined by its effect on $X(k)$, even when k is algebraically closed. We introduce some terminology to handle this.

DEFINITION 1.9. Let X be an algebraic scheme over k and S a subset of $X(k)$. We say that S is **schematically dense** (or just **dense**) in X if the only closed subscheme Z of X such that $S \subset Z(k)$ is X itself.

Let $X = \mathrm{Spm}(A)$, and let S be a subset of $X(k)$. Let $Z = \mathrm{Spm}(A/\mathfrak{a})$ be a closed subscheme of X. Then $S \subset Z(k)$ if and only if $\mathfrak{a} \subset \mathfrak{m}$ for all $\mathfrak{m} \in S$. Therefore, S is schematically dense in X if and only if $\bigcap\{\mathfrak{m} \mid \mathfrak{m} \in S\} = 0$.

PROPOSITION 1.10. *Let X be an algebraic scheme over k and S a subset of $X(k) \subset |X|$. The following conditions are equivalent:*
  (a) *S is schematically dense in X;*

(b) *X is reduced and S is dense in* $|X|$;

(c) *the family of homomorphisms*

$$f \mapsto f(s): \mathcal{O}_X \to \kappa(s) = k, \quad s \in S,$$

   is injective.

PROOF. (a)$\Rightarrow$(b). Let $\bar{S}$ denote the closure of S in $|X|$. There is a unique reduced subscheme Z of X with underlying space $\bar{S}$. As $S \subset |Z|$, the scheme $Z = X$, and so X is reduced with underlying space $\bar{S}$.

   (b)$\Rightarrow$(c). Let U be an open affine subscheme of X, and let $A = \mathcal{O}_X(U)$. Let $f \in A$ be such that $f(s) = 0$ for all $s \in S \cap |U|$. Then $f(u) = 0$ for all $u \in |U|$ because $S \cap |U|$ is dense in $|U|$. This means that f lies in all maximal ideals of A, and therefore lies in the radical of A, which is zero because X is reduced (CA 13.11).

   (c)$\Rightarrow$(a). Let Z be a closed subscheme of X such that $S \subset Z(k)$. Because Z is closed in X, the homomorphism $\mathcal{O}_X \to \mathcal{O}_Z$ is surjective. Because $S \subset Z(k)$, the maps $f \mapsto f(s): \mathcal{O}_X \to \kappa(s)$, $s \in S$, factor through $\mathcal{O}_Z$, and so the map $\mathcal{O}_X \to \mathcal{O}_Z$ is injective. Hence the map $\mathcal{O}_X \to \mathcal{O}_Z$ is an isomorphism, which implies that $Z = X$.   □

PROPOSITION 1.11. *A schematically dense subset remains schematically dense under extension of the base field.*

PROOF. Let k' be a field containing k, and let $S \subset X(k)$ be schematically dense. We may suppose that X is affine, say, $X = \mathrm{Spm}(A)$. Let $s': A_{k'} \to k'$ be the map obtained from $s: A \to \kappa(s) = k$ by extension of scalars. The family s', $s \in S$, is injective because the family s, $s \in S$, is injective and k' is flat over k.   □

COROLLARY 1.12. *If X admits a schematically dense subset $S \subset X(k)$, then it is geometrically reduced.*

PROOF. The set S remains schematically dense in $X(k^{\mathrm{a}})$, and so $X_{k^{\mathrm{a}}}$ is reduced.   □

PROPOSITION 1.13. *If S is schematically dense in X and $u, v: X \rightrightarrows Y$ are regular maps from X to a separated algebraic scheme Y such that $u(s) = v(s)$ for all $s \in S$, then $u = v$.*

PROOF. Because Y is separated, the equalizer of the pair of maps is closed in X. As its underlying space contains S, it equals X.   □

REMARK 1.14. Some of the above discussion extends to base rings. For example, let X be an algebraic scheme over a field k and let S be a schematically dense subset of $X(k)$. Let R be a k-algebra and, for $s \in S$, let

$$s' = s \times_{\mathrm{Spm}(k)} \mathrm{Spm}(R) \subset X' = X \times_{\mathrm{Spm}(k)} (R).$$

As in the proof of (1.11), the family of maps $\mathcal{O}_{X'} \to \mathcal{O}_{s'}(s') = R$ is injective. It follows, as in the proof of (1.10), that the only closed R-subscheme of X' containing all s' is X' itself.

DEFINITION 1.15. Let X be an algebraic scheme over a field k, and let k' be a field containing k. We say that $X(k')$ is **dense** in X if the only closed subscheme Z of X such that $Z(k') = X(k')$ is X itself.

PROPOSITION 1.16. *If $X(k')$ is dense in X, then X is reduced. Conversely, if $X(k')$ is dense in the topological space $|X_{k'}|$ and X is geometrically reduced, then $X(k')$ is dense in X.*

PROOF. Recall that X_{red} is the (unique) reduced subscheme of X with underlying space $|X|$. Moreover $X_{\text{red}}(k') = X(k')$ because k' is reduced, and so $X_{\text{red}} = X$ if $X(k')$ is dense in X.

Conversely, suppose that X is geometrically reduced and $X(k')$ is dense in $|X_{k'}|$. Let Z be a closed subscheme of X such that $Z(k') = X(k')$. Then $|Z_{k'}| = |X_{k'}|$ by the density condition. This implies that $Z_{k'} = X_{k'}$ because $X_{k'}$ is reduced, which in turn implies that $Z = X$ (see A.65). □

COROLLARY 1.17. *If X is geometrically reduced, then $X(k')$ is dense in X for every separably closed field k' containing k.*

PROOF. By a standard result (A.48), $X(k')$ is dense in $|X_{k'}|$. □

COROLLARY 1.18. *Let Z and Z' be closed subvarieties of an algebraic scheme X over k. If $Z(k') = Z'(k')$ for some separably closed field k' containing k, then $Z = Z'$.*

PROOF. The closed subscheme $Z \cap Z'$ of Z has the property that $(Z \cap Z')(k') = Z(k')$, and so $Z \cap Z' = Z$. Similarly, $Z \cap Z' = Z'$. □

Thus, a closed subvariety Z of X is determined by the subset $Z(k^s)$ of $X(k^s)$. More explicitly, if $X = \text{Spm}(A)$ and $Z = \text{Spm}(A/\mathfrak{a})$, then $\mathfrak{a}$ is the set of $f \in A$ such that $f(P) = 0$ for all $P \in Z(k^s)$.

Algebraic groups over rings

Although we are only interested in algebraic groups over fields, occasionally we shall need to consider them over more general base rings.

1.19. Let R be a (finitely generated) k-algebra. An algebraic scheme over R is a scheme X equipped with a morphism $X \to \text{Spm}(R)$ of finite type. Equivalently, X is an algebraic scheme over k such that $\mathcal{O}_X$ is equipped with an R-algebra structure compatible with its k-algebra structure. For example, affine algebraic schemes over R are the max-spectra of finitely generated R-algebras. A morphism of algebraic R-schemes $\varphi \colon X \to Y$ is a morphism of k-schemes compatible with the R-algebra structures, i.e., such that $\mathcal{O}_Y \to \varphi_* \mathcal{O}_X$ is a homomorphism of sheaves of R-algebras. Let G be an algebraic scheme over R and let $m \colon G \times G \to G$ be a morphism of R-schemes. The pair (G, m) is an **algebraic group over R** if there exist R-morphisms $e \colon \text{Spm}(R) \to G$ and $\text{inv} \colon G \to G$ such that the diagrams (1) and (2) commute. For example, an algebraic group (G, m) over k gives rise to an algebraic group (G_R, m_R) over R by extension of scalars.

ASIDE 1.20. By definition an algebraic group and its multiplication map are described by polynomials, but we rarely need to know what the polynomials are. Nevertheless, it is of some interest that it is often possible to realize the coordinate ring of an affine algebraic group as a quotient of a polynomial ring in a concrete natural way (Popov 2015).

NOTES. As noted elsewhere, in most of the literature, an algebraic group over a field k is defined to be a group variety over some algebraically closed field K containing k together with a k-structure (see, for example, Springer 1998 1.6.14, 2.1.1). In particular, nilpotents are not allowed. An algebraic group over a field k in our sense is a group scheme of finite type over k in the language of SGA 3. Our notion of an algebraic group over k is essentially the same as that in DG.

b. Basic properties of algebraic groups

PROPOSITION 1.21. If $\varphi\colon (G, m_G) \to (H, m_H)$ is a homomorphism of algebraic groups, then $\varphi \circ e_G = e_H$ and $\varphi \circ \mathrm{inv}_G = \mathrm{inv}_H \circ \varphi$. In particular, the maps e and inv in (1.1) are uniquely determined by (G, m).

PROOF. For every k-algebra R, the map $\varphi(R)$ is a homomorphism of abstract groups $(G(R), m_G(R)) \to (H(R), m_H(R))$, and so it maps the neutral element of $G(R)$ to that of $H(R)$ and the inversion map on $G(R)$ to that on $H(R)$. The Yoneda lemma (A.33) now shows that the same is true for φ. □

We often write e for the image of $e\colon * \to G$ in $G(k)$ or $|G|$. Recall (A.41) that an algebraic scheme X is separated if its diagonal Δ_X is closed in $X \times X$.

PROPOSITION 1.22. Algebraic groups are separated (as algebraic schemes).

PROOF. Let (G, m) be an algebraic group. The diagonal in $G \times G$ is the inverse image of the closed point $e \in G(k)$ under the map $m \circ (\mathrm{id} \times \mathrm{inv})\colon G \times G \to G$ sending (g_1, g_2) to $g_1 g_2^{-1}$, and so it is closed. □

Therefore "group variety" = "geometrically reduced algebraic group".

COROLLARY 1.23. Let G be an algebraic group over k and let k' be an extension of k. If $G(k')$ is dense in G, then a homomorphism $G \to H$ of algebraic groups is determined by its action on $G(k')$.

PROOF. Let φ_1 and φ_2 be homomorphisms $G \to H$ such that $\varphi_1(a) = \varphi_2(a)$ for all $a \in G(k')$. Because H is separated, the equalizer Z of φ_1 and φ_2 is a closed subscheme of G. As $Z(k') = G(k')$, we have $Z = G$. □

DEFINITION 1.24. An algebraic group (G, m) is **commutative** if $m \circ t = m$, where t is the transposition map $(x, y) \mapsto (y, x)\colon G \times G \to G \times G$.

PROPOSITION 1.25. An algebraic group G is commutative if and only if $G(R)$ is commutative for all k-algebras R. A group variety G is commutative if $G(k^s)$ is commutative.

PROOF. According to the Yoneda lemma (A.33), $m \circ t = m$ if and only if $m(R) \circ t(R) = m(R)$ for all k-algebras R, i.e., if and only if $G(R)$ is commutative for all R. This proves the first statement. Let G be a group variety. If $G(k^s)$ is commutative, then $m \circ t$ and m agree on $(G \times G)(k^s)$, which is dense in $G \times G$ (see 1.17). □

Smoothness

Let X be an algebraic scheme over k. For $x \in |X|$, we have

$$\dim(\mathcal{O}_{X,x}) \leq \dim(\mathfrak{m}_x/\mathfrak{m}_x^2).$$

Here $\mathfrak{m}_x$ is the maximal ideal in the local ring $\mathcal{O}_{X,x}$, the "dim" at left is the Krull dimension, and the "dim" at right is the dimension as a $\kappa(x)$-vector space (see CA, §22). When equality holds, the point x is said to be regular. A scheme X is said to be regular if x is regular for all $x \in |X|$. It is possible for X to be regular without X_{k^a} being regular. To remedy this, we need another notion.

Let $k[\varepsilon]$ be the k-algebra generated by an element ε with $\varepsilon^2 = 0$. From the homomorphism $\varepsilon \mapsto 0$, we get a map $X(k[\varepsilon]) \to X(k)$, and we define the **tangent space** $\mathrm{Tgt}_x(X)$ at a point $x \in X(k)$ to be the fibre over x. Thus

$$\mathrm{Tgt}_x(X) \simeq \mathrm{Hom}_{k\text{-linear}}(\mathfrak{m}_x/\mathfrak{m}_x^2, k),$$

and so $\dim \mathrm{Tgt}_x(X) \leq \dim(\mathcal{O}_{X,x})$. When equality holds, the point is said to be smooth. The formation of the tangent space commutes with extension of the base field, and so a point $x \in X(k)$ is smooth on X if and only if it is smooth on X_{k^a}. An algebraic scheme X over an algebraically closed field k is said to be smooth if all $x \in |X|$ are smooth, and an algebraic scheme X over an arbitrary field k is said to be smooth if X_{k^a} is smooth. Smooth schemes are regular, and the converse is true when k is algebraically closed. See Section Ah.

PROPOSITION 1.26. *Let G be an algebraic group over k.*

(a) *If G is reduced and k is perfect, then G is geometrically reduced.*

(b) *If G is geometrically reduced, then it is smooth (and conversely).*

PROOF. (a) This is true for all algebraic schemes (A.43).

(b) We have to show that G_{k^a} is smooth. But G_{k^a} is an algebraic variety, and so some point on it is smooth (A.55), which implies that every point is smooth by homogeneity (1.8). □

Therefore

$$\text{"group variety"} = \text{"smooth algebraic group"}.$$

In characteristic zero, all algebraic groups are smooth (3.23, 8.39 below).

EXAMPLE 1.27. Let k be a nonperfect field of characteristic p, and let $t \in k \smallsetminus k^p$. Let G be the algebraic subgroup of $\mathbb{A}^2$ defined by the equation

$$Y^p - tX^p = 0.$$

The ring $A = k[X, Y]/(Y^p - tX^p)$ is reduced because $Y^p - tX^p$ is irreducible in $k[X, Y]$, but A acquires a nilpotent $y - t^{\frac{1}{p}} x$ when tensored with k^a, and so G is not geometrically reduced. (Over k^a, G becomes the line $Y = t^{\frac{1}{p}} X$ with multiplicity p.)

PROPOSITION 1.28. *The following conditions on an algebraic group G are equivalent:*

(a) *G is smooth;*

(b) *the point e is smooth on G;*

(c) *the local ring $\mathcal{O}_{G,e}$ is regular;*

(d) *G is geometrically reduced.*

PROOF. (a)$\Rightarrow$(b). This implication is obvious from the definitions.

(b)$\Rightarrow$(a). As e is smooth on G, it is smooth on G_{k^a} (see the above discussion). By homogeneity (1.8), all points on G_{k^a} are smooth, which means that G is smooth.

(b)$\Leftrightarrow$(c). Obvious from the definitions (see the above discussion).

(a)$\Leftrightarrow$(d). This was proved in Proposition 1.26.   □

The identity (neutral) component of an algebraic group

For an algebraic group G, the connected component of G containing e is called the ***identity*** (or ***neutral***) ***component*** of G and is denoted by G°. Before continuing, we need to review a little algebraic geometry.

An étale k-algebra is a finite product of finite separable field extensions of k. A finite product of étale k-algebras is again étale, and any quotient of an étale k-algebra is an étale k-algebra. If $A_1, \ldots, A_m$ are étale subalgebras of a k-algebra A (not necessarily finitely generated), then their composite $A_1 \cdots A_m$ is an étale subalgebra of A (because it is a quotient of $A_1 \times \cdots \times A_m$). An étale k-scheme X is the spectrum of an étale k-algebra; equivalently, $|X|$ is discrete and the local rings $\mathcal{O}_{X,x}$, $x \in |X|$, are finite separable field extensions of k. See Section Ai.

Let f be a nontrivial idempotent in a ring A, i.e., $f^2 = f$ and $f \neq 0, 1$. Every idempotent in an integral domain is trivial, and so each prime ideal in A contains exactly one of f or $1 - f$. Therefore $\mathrm{spm}(A)$ is a disjoint union of the closed–open subsets $D(f)$ and $D(1 - f)$. More generally, let X be an algebraic scheme over k. Then $\mathcal{O}(X)$ is a k-algebra (not necessarily finitely generated), and a nontrivial idempotent in $\mathcal{O}(X)$ decomposes X into a disjoint union of two nonempty closed-open subsets.

PROPOSITION 1.29. *Let X be an algebraic scheme over k. There exists a largest étale k-subalgebra $\pi(X)$ in $\mathcal{O}(X)$.*

PROOF. Let A be an étale subalgebra of $\mathcal{O}(X)$. Then $A \otimes k^s \simeq (k^s)^n$ for some n, and so

$$1 = f_1 + \cdots + f_n$$

with the f_i orthogonal idempotents in $\mathcal{O}(G_{k^s})$. The f_i decompose $|G_{k^s}|$ into a disjoint union of n open-closed subsets, and so n is at most the number of connected components of $|G_{k^s}|$. Thus the number $[A:k] = [A \otimes k^s : k]$ is bounded. It follows that the composite of all étale k-subalgebras of $\mathcal{O}(X)$ is an étale k-subalgebra which contains all others. □

Define

$$\pi_0(X) = \mathrm{Spm}(\pi(X)).$$

Under the isomorphism (A.13)

$$\mathrm{Hom}_{k\text{-algebra}}(R, \mathcal{O}(X)) \simeq \mathrm{Hom}_{k\text{-scheme}}(X, \mathrm{Spm}(R)), \quad R \text{ a } k\text{-algebra},$$

the inclusion $\pi(X) \hookrightarrow \mathcal{O}(X)$ corresponds to a morphism $\varphi \colon X \to \pi_0(X)$ that is universal among morphisms from X to an étale k-scheme.

PROPOSITION 1.30. *Let X be an algebraic scheme over k.*

(a) *For all fields k' containing k,*

$$\pi_0(X_{k'}) \simeq \pi_0(X)_{k'}.$$

(b) *Let Y be a second algebraic scheme over k. Then*

$$\pi_0(X \times Y) \simeq \pi_0(X) \times \pi_0(Y).$$

PROOF. (a) Let $\pi = \pi(\mathcal{O}(X))$ and $\pi' = \pi(\mathcal{O}(X_{k'}))$. Then $\pi \otimes k' \subset \pi'$, and we have to prove equality.

Suppose first that $k' = k^s$, and let $\Gamma = \mathrm{Gal}(k^s/k)$. Then π' is stable under Γ. By Galois theory (A.62), π'^Γ is étale over k and $\pi'^\Gamma \otimes k' \simeq \pi'$. On the other hand $\pi \subset \pi'^\Gamma$, and so $\pi = \pi'^\Gamma$. Hence $\pi \otimes k' \simeq \pi'$.

Now suppose that $k = k^s$ and $k' = k^a$. If $k^a \neq k$, then k has characteristic $p \neq 0$. Let $e_1, \ldots, e_m$ be a basis of idempotents for π' as a k^a-vector space. Write $e_j = \sum a_i \otimes c_i$ with $a_i \in \mathcal{O}(X)$ and $c_i \in k^a$. For some r, all the elements $c_i^{p^r}$ lie in k, and so $e_j = e_j^{p^r} = \sum a_i^{p^r} \otimes c_i^{p^r} \in \mathcal{O}(X)$. Hence $\pi \otimes k^a \simeq \pi'$.

Next suppose that k and k' are algebraically closed. We have to show that X is connected if and only if $X_{k'}$ is connected. If $\pi' = k'$, then $\pi = k$ because $\pi \otimes k' \subset \pi'$. Conversely, if X is connected, then $X_{k'}$ is connected because $|X|$ is dense in $|X_{k'}|$.

In the general case, let $k^a \subset k'^a$ be algebraic closures of k and k'. If $\pi \otimes k' \neq \pi'$ then $\pi \otimes k' \otimes_{k'} k'^a \neq \pi' \otimes_{k'} k'^a$, and so $(\pi \otimes k^a) \otimes_{k^a} k'^a \neq \pi' \otimes_{k'} k'^a$. But this contradicts the previous statements.

(b) After (a), we may suppose that $k = k^{\mathrm{a}}$, and then we have to show that $X \times Y$ is connected if X and Y are. But $X \times Y$ is a union of the connected subvarieties $x \times Y$ and $X \times y$ with $x \in |X|$ and $y \in |Y|$, and so this is obvious.□

The argument shows, more precisely, that the formation of the map $X \to \pi_0(X)$ commutes with extension of the base field.

If $\pi(X)$ is a field, then $\mathcal{O}(X)$ has no nontrivial idempotents, and so X is connected. If k is algebraically closed in[1] $\mathcal{O}(X)$, then it is algebraically closed in $\pi(X)$, and so $\pi(X) = k$; in this case, $\pi(X_{k^{\mathrm{a}}}) = k^{\mathrm{a}}$ and $X_{k^{\mathrm{a}}}$ is connected.

PROPOSITION 1.31. *Let X be an algebraic scheme over k.*

(a) *The fibres of the map $\varphi \colon X \to \pi_0(X)$ are the connected components of X.*

(b) *For all $x \in |\pi_0(X)|$, the fibre $\varphi^{-1}(x)$ is a geometrically connected scheme over $\kappa(x)$.*

PROOF. Let $x \in |\pi_0(X)|$. For the fibre $X_x = \varphi^{-1}(x)$, we have $\pi(X_x) = \kappa(x)$. Therefore the statements follow from the above discussion.   □

COROLLARY 1.32. *Let X be a connected algebraic scheme over k such that $X(k) \neq \emptyset$. Then X is geometrically connected, and $X \times Y$ is connected for any connected algebraic scheme Y over k.*

PROOF. By definition, $A = \pi(X)$ is a finite product of separable field extensions of k. If A had more than one factor, $\mathcal{O}(X)$ would contain a nontrivial idempotent, and X would not be connected. Therefore, A is a field containing k. Because $X(k)$ is nonempty, there is a k-homomorphism $A \to k$, and so $A = k$. Now $X_{k^{\mathrm{a}}}$ is connected by the above discussion. Moreover,

$$\pi_0(X \times Y) \simeq \pi_0(X) \times \pi_0(Y) \simeq \pi_0(Y),$$

and so $X \times Y$ is connected.   □

REMARK 1.33. Let X be an algebraic scheme over k.

(a) The connected components of $X_{k^{\mathrm{s}}}$ form a finite set on which $\mathrm{Gal}(k^{\mathrm{s}}/k)$ acts continuously, and $\pi_0(X)$ is the étale scheme over k corresponding to this set under the equivalence $Z \rightsquigarrow Z(k^{\mathrm{s}})$ in (A.62).

(b) The morphism $\varphi^{-1}(x) \to \mathrm{Spm}(\kappa(x))$ is flat because $\kappa(x)$ is a field. Therefore, $\varphi \colon X \to \pi_0(X)$ is faithfully flat.

PROPOSITION 1.34. *Let G be an algebraic group. The identity component G° of G is an algebraic subgroup of G. Its formation commutes with extension of the base field: $(G^\circ)_{k'} \simeq (G_{k'})^\circ$. In particular, the algebraic group G° is geometrically connected.*

---

[1]This means that an a in $\mathcal{O}(X)$ belongs to k if $f(a) = 0$ for some nonzero $f(T) \in k[T]$.

PROOF. The identity component $G°$ of G has a k-point, namely, e, and so $G° \times G°$ is a connected component of $G \times G$ (1.32). As m maps (e, e) to e, it maps $G° \times G°$ into $G°$. Similarly, inv maps $G°$ into $G°$. It follows that $G°$ is an algebraic subgroup of G. Because the formation of the map $G \to \pi_0(G)$ commutes with extension of the base field, so does its fibre over e. In particular, $(G°)_{k^a} \simeq (G_{k^a})°$, and so $G°$ is geometrically connected. □

COROLLARY 1.35. *Every connected component of an algebraic group is irreducible.*

PROOF. Let G be an algebraic group over k, and suppose that some connected component of it is reducible. Then some point of G lies on more than one irreducible component, and the same is true for G_{k^a}. By definition, no irreducible component of G_{k^a} is contained in the union of the remainder. Therefore, there exists a point of G_{k^a} that lies on exactly one irreducible component. By homogeneity (1.8), all points have this property, which is a contradiction. □

Note that G is smooth if $G°$ is smooth (1.28b). A connected component of G, other than $G°$, need not be geometrically connected (see 1.6b).

SUMMARY 1.36. The following conditions on an algebraic group G over k are equivalent:

(a) G is irreducible;

(b) G is connected;

(c) G is geometrically connected.

When G is affine, the conditions are equivalent to:

(d) the quotient of $\mathcal{O}(G)$ by its nilradical is an integral domain.

Algebraic groups are unusual: for an algebraic scheme over k, (b) implies neither (a) nor (c), and neither (a) nor (c) implies the other.

The dimension of an algebraic group

The dimension $\dim(X)$ of an irreducible algebraic scheme X is the common Krull dimension of its local rings $\mathcal{O}_{X,x}$, $x \in |X|$. When X is reduced, this equals the transcendence degree of its function field $k(X)$ over k. An irreducible algebraic scheme X over k becomes over k^a a finite union of irreducible algebraic schemes all of dimension $\dim(X)$. See Section Ag.

The irreducible components of an algebraic group G over k are its connected components (1.35). They all have the same dimension, because this is true over k^a by homogeneity. The **dimension** $\dim(G)$ of G is the common dimension of its connected components, which equals the common Krull dimension of each of its local rings $\mathcal{O}_{G,x}$, $x \in |G|$.

PROPOSITION 1.37. *For an algebraic group G,*

$$\dim \mathrm{Tgt}_e(G) \geq \dim G,$$

with equality if and only if G is smooth.

PROOF. In general, for a point e on an algebraic k-scheme G with $\kappa(e) = k$, $\dim \mathrm{Tgt}_e(G) \geq \dim G$ with equality if and only if the point e is smooth on G (see A.52). An algebraic group is smooth if and only if e is smooth on G (see 1.28). $\square$

c. Algebraic subgroups

Let X and Y be algebraic schemes over k with Y reduced, and let Z be a closed subscheme of X. A morphism $\varphi\colon Y \to X$ factors through Z_{red} if and only if $|\varphi|$ factors through $|Z|$. See A.30.

PROPOSITION 1.38. *Let (G, m) be an algebraic group over k. If G_{red} is geometrically reduced, then it is an algebraic subgroup of G.*

PROOF. If G_{red} is geometrically reduced, then $G_{\mathrm{red}} \times G_{\mathrm{red}}$ is reduced (A.43), and so the restriction of m to $G_{\mathrm{red}} \times G_{\mathrm{red}}$ factors through $G_{\mathrm{red}} \hookrightarrow G$:

$$G_{\mathrm{red}} \times G_{\mathrm{red}} \xrightarrow{m_{\mathrm{red}}} G_{\mathrm{red}} \hookrightarrow G.$$

Similarly, e and inv induce maps $* \to G_{\mathrm{red}}$ and $G_{\mathrm{red}} \to G_{\mathrm{red}}$, and it follows that $(G_{\mathrm{red}}, m_{\mathrm{red}})$ is an algebraic subgroup of (G, m). $\square$

COROLLARY 1.39. *Let G be an algebraic group over k. If k is perfect, then G_{red} is an algebraic subgroup of G.*

PROOF. As k is perfect, G_{red} is geometrically reduced (1.26). $\square$

In general, G_{red} need not be an algebraic group (1.57, 1.58), and when it is an algebraic group, it need not be a normal algebraic subgroup, even when k is perfect (2.35).

LEMMA 1.40. *Let G be an algebraic group over k and S an abstract subgroup of $G(k)$. The Zariski closure $\bar{S}$ of S of $G(k)$ is also a subgroup of $G(k)$.*

PROOF. Let $a, b \in \bar{S}$, and let U be a neighbourhood of ab. As multiplication is continuous, there exist neighbourhoods A and B of a and b such that $AB \subset U$. Both A and B meet S, and so U meets S. As this is true for all neighbourhoods of ab, we see that $ab \in \bar{S}$. Let $a \in \bar{S}$. As inversion is a homeomorphism, a^{-1} lies in the closure of $S^{-1} = S$. $\square$

PROPOSITION 1.41. *Algebraic subgroups of algebraic groups are closed (in the Zariski topology).*

PROOF. Let H be an algebraic subgroup of an algebraic group G over k. The canonical map $|G_{k^a}| \to |G|$ realizes the topological space $|G|$ as a quotient of $|G_{k^a}|$ (see A.20). Thus, $|H|$ is closed in $|G|$ if and only if its inverse image $|H_{k^a}|$ is closed in $|G_{k^a}|$. This allows us to suppose that k is algebraically closed.

We may also suppose that H and G are reduced because passing to the reduced algebraic subgroup does not change the underlying topological space. By definition, $|H|$ is locally closed, i.e., open in its closure $\overline{|H|}$. According to the lemma, $\overline{|H|}$ is a subgroup of $|G|$. Therefore, it is a disjoint union of cosets of $|H|$, which are finite in number. As each coset is open, it is also closed. Therefore $|H|$ is closed in $\overline{|H|}$, and so equals it. □

COROLLARY 1.42. *The algebraic subgroups of an algebraic group satisfy the descending chain condition.*

PROOF. This is true for the closed subschemes of an algebraic scheme (A.24). □

COROLLARY 1.43. *Algebraic subgroups of affine algebraic groups are affine.*

PROOF. Closed subschemes of affine algebraic schemes are affine. □

COROLLARY 1.44. *Let H_1 and H_2 be subgroup varieties of an algebraic group G. If $H_1(k^s) = H_2(k^s)$, then $H_1 = H_2$.*

PROOF. As H_1 and H_2 are closed, we can apply (1.18). □

Recall (p. 9) that we identify $G(k)$ with the set of points x in $|G|$ such that $\kappa(x) = k$. Let S be a subgroup of $G(k)$. If $S = H(k)$ for some algebraic subgroup H of G, then $S = |H| \cap G(k)$, and so it is closed in $G(k)$ for the induced topology (1.41). We prove a converse.

THEOREM 1.45. *Let G be an algebraic group over k and S a closed subgroup of $G(k)$. There is a unique reduced algebraic subgroup H of G such that $S = H(k)$, and H is geometrically reduced. The algebraic subgroups H of G that arise in this way are exactly those for which $H(k)$ is schematically dense in H.*

PROOF. Let H be the reduced closed subscheme of G such that $|H| = S$. Then $S = G(k) \cap |H| = H(k)$. As $H(k)$ is dense in $|H|$ and H is reduced, $H(k)$ is schematically dense in H (see 1.10) and H is geometrically reduced (1.12). Therefore $H \times H$ is reduced, and so the map $m_G \colon H \times H \to G$ factors through H. Similarly, inv_G restricts to a regular map $H \to H$ and $* \to G$ factors through H. Therefore H is an algebraic subgroup of G such that $H(k)$ is schematically dense in H.

Conversely, let H be an algebraic subgroup of G. Then $H(k) = G(k) \cap |H|$ and so $H(k)$ is closed in $G(k)$. If $H(k)$ is schematically dense in H, then the above construction starting with $S = H(k)$ gives back H. □

COROLLARY 1.46. *Let G be an algebraic group over k. Every closed subgroup S of $G(k)$ is the group of k-points of a unique subgroup variety H of G. The subgroup varieties H of G that arise in this way are exactly those for which $H(k)$ is dense in $|H|$.*

PROOF. This is a restatement of the theorem using Proposition 1.10.   □

COROLLARY 1.47. *Let G be an algebraic group over a separably closed field k. The map $H \mapsto H(k)$ is a bijection from the set of subgroup varieties of G onto the set of closed subgroups of $G(k)$.*

PROOF. As k is separably closed, $H(k)$ is dense in $|H|$ for every group subvariety of G (see 1.17).   □

DEFINITION 1.48. Let G be an algebraic group over k and S a subgroup of $G(k)$. The unique subgroup variety H of G such that $H(k)$ is the Zariski closure of S is called the ***Zariski closure*** of S in G.

PROPOSITION 1.49. *The intersection $H = \bigcap_{j \in J} H_j$ of a family $(H_j)_{j \in J}$ of algebraic subgroups of G is an algebraic subgroup of G. If G is affine, then H is affine, and its coordinate ring is $\mathcal{O}(G)/I$ where I is the ideal in $\mathcal{O}(G)$ generated by the ideals $I(H_j)$ of the H_j.*

PROOF. Certainly, H is a closed subscheme. Moreover, for all k-algebras R,

$$H(R) = \bigcap_{j \in J} H_j(R) \quad \text{(intersection inside } G(R)\text{)},$$

which is a subgroup of $G(R)$, and so H is an algebraic subgroup of G (see 1.5). Assume that G is affine. For any k-algebra R,

$$H_j(R) = \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in I(H_j)\}.$$

Therefore,

$$H(R) = \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in \bigcup I(H_j)\}$$
$$= \mathrm{Hom}(\mathcal{O}(G)/I, R).$$ □

In fact, because of Corollary 1.42, every infinite intersection of algebraic subgroups is equal to a finite intersection.

REMARK 1.50. Over a field k of nonzero characteristic p, an intersection of smooth algebraic subgroups of a smooth algebraic group need not be smooth. For example, both SL_p and the group H of scalar matrices in GL_p are smooth algebraic subgroups of GL_p, but $\mathrm{SL}_p \cap H = \mu_p$, which is not reduced (hence not smooth). As another example, let $G = \mathbb{G}_a^2$, and let $t \in k \smallsetminus k^p$. Then $H_1 = \mathbb{G}_a \times \{0\}$ and $H_1 : X^{p^2} - tX^p = Y$ are smooth algebraic subgroups of G, but their intersection is not reduced (it is the group in 1.57 below).

Normal and characteristic subgroups

DEFINITION 1.51. Let G be an algebraic group.

(a) An algebraic subgroup H of G is **normal** if $H(R)$ is normal in $G(R)$ for all small k-algebras R.

(b) An algebraic subgroup H of G is **characteristic** if $\alpha(H_R) = H_R$ for all small k-algebras R and all automorphisms α of G_R.

The conditions hold for all k-algebras R if they hold for all small k-algebras. In (b), G_R and H_R can be interpreted as functors from the category of (small) finitely generated R-algebras to the category of groups, or as algebraic R-schemes (1.19). Because of the Yoneda lemma (A.33), the two interpretations give the same condition.

PROPOSITION 1.52. *The identity component $G°$ of an algebraic group G is a characteristic subgroup of G (hence a normal subgroup).*

PROOF. As $G°$ is the unique connected open subgroup of G containing e, every automorphism of G fixing e maps $G°$ into itself. Let k' be a field containing k. As $(G°)_{k'} = (G_{k'})°$, every automorphism of $G_{k'}$ fixing e maps $(G°)_{k'}$ into itself.

Let R be a k-algebra and let α be an automorphism of G_R. We regard $G_R°$ and G_R as algebraic R-schemes. It suffices to show that $\alpha(G_R°) \subset G_R°$, and, because $G_R°$ is an open subscheme of G_R, for this it suffices to show that $\alpha(|G_R°|) \subset |G_R°|$. Let $x \in |G_R°|$, and let s be the image of x in $\mathrm{Spm}(R)$. Then x lies in the fibre $G_{\kappa(s)}$ of G_R over s:

$$
\begin{array}{ccc}
G_R & \longleftarrow & G_{\kappa(s)} \\
\downarrow & & \downarrow \\
\mathrm{Spm}(R) & \longleftarrow & \mathrm{Spm}(\kappa(s)).
\end{array}
$$

In fact, $x \in |G_R° \cap G_{\kappa(s)}| = |G_{\kappa(s)}°|$. From the first paragraph of the proof, $\alpha_{\kappa(s)}(x) \in |G_{\kappa(s)}°|$, and so $\alpha(x) \in |G_R°|$, as required. □

REMARK 1.53. Let H be an algebraic subgroup of G. If $\alpha(H_R) \subset H_R$ for all k-algebras R and endomorphisms α of G_R, then H is characteristic. To see this, let α be an automorphism of G_R. Then $\alpha^{-1}(H_R) \subset H_R$, and so $H_R \subset \alpha(H_R)$.

Descent of subgroups

1.54. Let G be an algebraic scheme over a field k, let k' be a field containing k, and let H' be an algebraic subgroup of $G' = G_{k'}$.

(a) There exists at most one algebraic subgroup H of G such that $H_{k'} = H'$ (as an algebraic subgroup of $G_{k'}$). When such an H exists, we say that H' is **defined over** k (as an algebraic subgroup of G').

(b) Let k' be a Galois extension of k (possibly infinite) and let $\Gamma = \mathrm{Gal}(k'/k)$. Then H' is defined over k if and only if it is stable under the action of Γ on G', i.e., the sheaf of ideals defining it is stable under the action of Γ on $\mathcal{O}_{G'}$. When $H'(k')$ is schematically dense in H' (see 1.9), H' is stable under the action of Γ on G if and only if $H'(k')$ is stable under the action of Γ on $G(k')$.

Apply A.65 and A.66.

ASIDE 1.55. A submonoid H of a finite abstract group G is a subgroup because the map $x \mapsto hx \colon H \to H$ is injective, hence bijective, for all $h \in H$. A similar statement is true with a similar proof for algebraic groups as a consequence of the Ax–Grothendieck theorem:

> Let X be a scheme of finite presentation over a scheme S. An S-endomorphism of X is an automorphism if it is a monomorphism (EGA IV, 17.9.6).

Let H be an algebraic submonoid of an algebraic group G, and let $h \in H(R)$ for some k-algebra R. Then $x \mapsto hx \colon H(R') \to H(R')$ is injective for all R-algebras R'. This means that left translation $H_R \to H_R$ by h is a monomorphism and hence an isomorphism. Therefore, $x \mapsto hx \colon H(R) \to H(R)$ is bijective for all h and $H(R)$ is a subgroup of $G(R)$. As this is true for all R, we see that H is an algebraic subgroup of G (see 1.5).

d. Examples

We give some examples to illustrate what can go wrong in nonzero characteristic. Recall that $\mathbb{G}_a$ is the algebraic group with points $\mathbb{G}_a(R) = (R, +)$ and underlying scheme $\mathrm{Spm}(k[T]) = \mathbb{A}^1$.

1.56. Let k be nonperfect of characteristic $p > 2$, and let $t \in k \smallsetminus k^p$. Let G be the algebraic subgroup of $\mathbb{G}_a^2$ defined by

$$Y^p - Y = tX^p.$$

This is a connected group variety over k that becomes isomorphic to $\mathbb{G}_a$ over k^{a}, but $G(k)$ is finite if, for example, k is the field $k_0((t))$ of Laurent series over a field k_0 (Exercise 2-5; Rosenlicht 1957, p. 46).

1.57. Let k be nonperfect of characteristic p, and let $t \in k \smallsetminus k^p$. Let G be the finite algebraic subgroup of $\mathbb{G}_a$ defined by the equation

$$X^{p^2} - tX^p = 0.$$

Then G_{red} is defined by the equation $X(X^{p(p-1)} - t) = 0$. It is smooth at 0, but it is not geometrically reduced because $(X^{p(p-1)} - t) = (X^{p-1} - t^{1/p})^p$, and so it is not an algebraic group for any map $m \colon G_{\mathrm{red}} \times G_{\mathrm{red}} \to G_{\mathrm{red}}$ (Exercise 2-4; SGA 3, VI$_A$, 1.3.2a).

1.58. Let k be nonperfect of characteristic $p \geq 3$, and let $t \in k \smallsetminus k^p$. Let G be the algebraic subgroup of $\mathbb{G}_a^4$ defined by the equations

$$U^p - tV^p = 0 = X^p - tY^p.$$

Then G is a *connected* algebraic group of dimension 2, but G_{red} is singular at the origin, and hence not an algebraic group for any map m (SGA 3, VI$_A$, 1.3.2b). Similarly, the algebraic subgroup of $\mathbb{G}_a^3$ defined by

$$X^p - tY^p = 0 = Y^p - tZ^p$$

is a connected one-dimensional algebraic group such that G_{red} is not an algebraic group.

1.59. The formation of G_{red} does not commute with change of the base field. For example, G may be reduced without G_{k^a} being reduced (1.27). The best one can say is that the algebraic subgroup $(G_{k^a})_{\text{red}}$ of G_{k^a} is defined over a finite purely inseparable extension of k.

To see this, let G be an algebraic group over a field k of characteristic $p \neq 0$, and let

$$k^i = k^{p^{-\infty}} \overset{\text{def}}{=} \{x \in k^a \mid \exists m \geq 1 \text{ such that } x^{p^m} \in k\}$$

be the perfect closure of k in k^a – it is the smallest perfect subfield of k^a containing k. Now $(G_{k^i})_{\text{red}}$ is a smooth algebraic subgroup of G_{k^i} (see 1.39), which is defined over a finite subextension of k^i.

e. Kernels and exact sequences

The ***kernel*** of a homomorphism $\varphi\colon G \to H$ of algebraic groups is defined to be the following fibred product:

$$
\begin{array}{ccc}
\operatorname{Ker}(\varphi) = G \times_H * & \longrightarrow & * \\
\downarrow & & \downarrow{\scriptstyle e} \\
G & \overset{\varphi}{\longrightarrow} & H
\end{array}
$$

Thus $\operatorname{Ker}(\varphi)$ is the closed subscheme of G such that $\operatorname{Ker}(\varphi)(R) = \operatorname{Ker}(\varphi(R))$ for all k-algebras R. As $\operatorname{Ker}(\varphi(R))$ is a normal subgroup of $G(R)$ for all R, we see that $\operatorname{Ker}(\varphi)$ is a normal algebraic subgroup of G (1.5). When G and H are affine, so also is $N = \operatorname{Ker}(\varphi)$, and

$$\mathcal{O}(N) = \mathcal{O}(G) \otimes_{\mathcal{O}(H)} k \simeq \mathcal{O}(G)/I_H\mathcal{O}(G)$$

where $I_H = \operatorname{Ker}(\mathcal{O}(H) \xrightarrow{f \mapsto f(e)} k)$ is the ***augmentation ideal*** of H.

EXAMPLE 1.60. Let $\mathbb{G}_a$ be the algebraic group $(\mathbb{A}^1, +)$. The algebraic group G in 1.27 is the kernel of the homomorphism

$$\varphi: \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a, \quad (x, y) \mapsto y^p - tx^p.$$

It is not geometrically reduced, which shows that the kernel of a homomorphism of smooth algebraic groups need not be smooth. As another example, μ_3 is the kernel of $t \mapsto t^3: \mathbb{G}_m \to \mathbb{G}_m$, and it is not smooth in characteristic 3 (see 1.6).

DEFINITION 1.61. A sequence of algebraic groups

$$e \to N \xrightarrow{i} G \xrightarrow{q} Q \tag{3}$$

is exact if i is an isomorphism of N onto the kernel of q. A sequence

$$e \to N \xrightarrow{i} G \xrightarrow{q} Q \to e \tag{4}$$

is **exact** if in addition q is faithfully flat. When (4) is exact, we say that G is an **extension** of Q by N.

Obviously (3) is exact if and only if

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

is exact for all (small) k-algebras R. An exact sequence remains exact under extension of the base field. We shall see (1.71) that, for group varieties (but not algebraic groups in general), a homomorphism $q: G \to Q$ is faithfully flat if it is surjective as a map of schemes, i.e., if $|q|: |G| \to |Q|$ is surjective.

PROPOSITION 1.62. *Let*

$$e \to N \xrightarrow{i} G \xrightarrow{q} Q \to e$$

be an exact sequence of algebraic groups.

   (a) *If N and Q are smooth, then G is smooth.*

   (b) *If G is smooth, then Q is smooth.*

PROOF. (a) By definition, q is flat, and its geometric fibres are translates of N, which are smooth if N is smooth. Thus the map q is smooth if N is smooth. If, in addition, Q is smooth, this implies that G is smooth (A.71).

   (b) If q is faithfully flat, then the map $\mathcal{O}_Q \to q_* \mathcal{O}_G$ is injective (CA 11.12), and remains injective after extension of the base field. Therefore $\mathcal{O}_Q$ is geometrically reduced, hence smooth (1.28), if G is.   □

   In particular, extensions and quotients of group varieties are group varieties. In (1.62), N need not be smooth when G is smooth. For example, $\mathbb{G}_m$ is smooth, but the kernel μ_p of the faithfully flat map $x \mapsto x^p: \mathbb{G}_m \to \mathbb{G}_m$ is not smooth when $p = \text{char}(k) \neq 0$.

PROPOSITION 1.63. *Let $\varphi\colon G \to H$ be a surjective homomorphism of group varieties. The following conditions are equivalent:*

(a) *the map $(d\varphi)_e\colon \mathrm{Tgt}_e(G) \to \mathrm{Tgt}_e(H)$ is surjective;*

(b) *the kernel of φ is smooth;*

(c) *the map φ is smooth.*

PROOF. We may suppose that k is algebraically closed. Let $N = \mathrm{Ker}(\varphi)$. The fibres of φ are the translates N in G, which all have the same dimension, and so (see A.72)

$$\dim G = \dim N + \dim H. \tag{5}$$

We interpret the tangent spaces in terms of dual numbers. The exact commutative diagram

$$
\begin{array}{ccccccc}
0 & \longrightarrow & N(k[\varepsilon]) & \longrightarrow & G(k[\varepsilon]) & \longrightarrow & H(k[\varepsilon]) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & N(k) & \longrightarrow & G(k) & \longrightarrow & H(k)
\end{array}
$$

gives an exact sequence of kernels

$$0 \to \mathrm{Tgt}_e(N) \to \mathrm{Tgt}_e(G) \to \mathrm{Tgt}_e(H),$$

and so

$$\dim \mathrm{Tgt}_e(G) \le \dim \mathrm{Tgt}_e(N) + \dim \mathrm{Tgt}_e(H)$$

with equality if and only if $\mathrm{Tgt}_e(G) \to \mathrm{Tgt}_e(H)$ is surjective. On the other hand, by (1.37),

$$\dim G = \dim \mathrm{Tgt}_e(G)$$
$$\dim H = \dim \mathrm{Tgt}_e(H)$$
$$\dim \mathrm{Tgt}_e(N) \ge \dim N, \text{ with equality if and only if } N \text{ is smooth.}$$

The equivalence of (a) and (b) follows from this and (5).

If φ is smooth, then, by definition (A.71), so are its fibres. In particular N is smooth. Conversely, if $(d\varphi)_e$ is surjective, then, by homogeneity (1.8), $(d\varphi)_g$ is surjective for all $g \in G(k)$. As G and H are smooth, this implies that φ is smooth (A.71). $\qquad\square$

NOTES. As we saw in 1.60, the kernel of a homomorphism $\varphi\colon G \to H$ of smooth algebraic groups over k need not be smooth. This creates problems for those working in a world without nilpotents. In the old literature, an algebraically closed field K containing k is fixed, and the kernel of φ is defined to be $\mathrm{Ker}(\varphi_K)_{\mathrm{red}}$. If there exists a smooth algebraic subgroup N of G such that $N_K = \mathrm{Ker}(\varphi_K)_{\mathrm{red}}$, then the kernel is said to be defined over k.

f.   Group actions

By a functor (resp. group functor) in this section, we mean a functor from small
k-algebras to sets (resp. groups). An **action** of a group functor G on a functor X
is a natural transformation $\mu\colon G \times X \to X$ such that $\mu(R)$ is an action of $G(R)$
on $X(R)$ for all k-algebras R.

An **action** of an algebraic group G on an algebraic scheme X is a regular map

$$\mu\colon G \times X \to X$$

such that the following diagrams commute:

$$
\begin{array}{ccc}
G \times G \times X & \xrightarrow{\;\mathrm{id}\times\mu\;} & G \times X \\
{\scriptstyle m\times\mathrm{id}}\downarrow & & \downarrow{\scriptstyle \mu} \\
G \times X & \xrightarrow{\;\;\mu\;\;} & X
\end{array}
\qquad
\begin{array}{ccc}
* \times X & \xrightarrow{\;e\times\mathrm{id}\;} & G \times X \\
& {\scriptstyle \simeq}\searrow & \downarrow{\scriptstyle \mu} \\
& & X.
\end{array}
$$

Because of the Yoneda lemma (A.33), to give an action of G on X is the same as
giving an action of $\tilde{G}$ on $\tilde{X}$. We often write gx or $g \cdot x$ for $\mu(g,x)$. We say that
a subscheme Y of X is stable under G if the restriction of μ to $G \times Y$ factors
through $Y \hookrightarrow X$.

Let μ be an action of a group functor G on a functor X. The following
diagram obviously commutes:

$$
\begin{array}{ccc}
G \times X & \xrightarrow{(g,x)\mapsto(g,gx)} & G \times X \\
{\scriptstyle \mu}\downarrow{\scriptstyle (g,x)\mapsto gx} & & {\scriptstyle p_2}\downarrow{\scriptstyle (g,x)\mapsto x} \\
X & \xrightarrow{\;\;x\mapsto x\;\;} & X.
\end{array}
$$

Moreover, both horizontal maps are isomorphisms; for example, the inverse of
the top map is $(g,x) \mapsto (g, g^{-1}x)$.

LEMMA 1.64. *Let $\mu\colon G \times X \to X$ be an action of an algebraic group G on an
algebraic scheme X. Then μ is faithfully flat, and it is smooth (resp. finite) if G
is smooth (resp. finite).*

PROOF. The above diagram shows that the $\mu\colon G \times X \to X$ is isomorphic to the
projection map p_2, which is faithfully flat and is smooth or finite if G is.   □

Let μ and μ' be actions of G on X and X'. A morphism $\alpha\colon X \to X'$ is **equi-**
variant or a G-**morphism** if $\alpha(\mu(g,x)) = \mu'(g,\alpha(x))$ for all small k-algebras R,
all $g \in G(R)$, and all $x \in X(R)$.

PROPOSITION 1.65. *Let G be a group functor. Let X and Y be nonempty
algebraic schemes on which G acts, and let $f\colon X \to Y$ be an equivariant map.*

(a) *If Y is reduced and $G(k^{\mathrm{a}})$ acts transitively on $Y(k^{\mathrm{a}})$, then f is faithfully
    flat.*

(b) *If $G(k^a)$ acts transitively on $X(k^a)$, then the set $f(|X|)$ is locally closed in $|Y|$; let $f(X)_{\text{red}}$ denote $f(|X|)$ with its reduced subscheme structure.*

(c) *If X is reduced and $G(k^a)$ acts transitively on $X(k^a)$, then f factors into*

$$X \xrightarrow[\text{flat}]{\text{faithfully}} f(X)_{\text{red}} \xrightarrow{\text{immersion}} Y.$$

Moreover, $f(X)_{\text{red}}$ is stable under the action of G.

PROOF. (a) As $G(k^a)$ acts transitively on $Y(k^a)$ and X is nonempty, the map $f(k^a)$ is surjective, which implies that f is surjective. In proving that f is flat, we may replace k with its algebraic closure. By generic flatness (A.70), there exists a nonempty open subset U of Y such that f defines a flat map from $f^{-1}U$ onto U. As $G(k)$ acts transitively on $Y(k)$, the translates gU of U by elements g of $G(k)$ cover Y, which shows that f is flat. It is faithfully flat because it is surjective.

(b) In order to prove that $f(|X|)$ is locally closed in $|Y|$, it suffices to prove that its inverse image $f_{k^a}(|X_{k^a}|)$ in $|Y_{k^a}|$ is locally closed (because $|Y_{k^a}| \to |Y|$ is a quotient map of topological spaces (A.20)). Thus, we may suppose that k is algebraically closed.

Because $f(|X|)$ is the image of a regular map, it contains a dense open subset U of its closure $\overline{f(|X|)}$ (see A.15). We shall show that $f(|X|)$ is open in $\overline{f(|X|)}$ (hence locally closed in $|Y|$). The translates of $f^{-1}(U)$ by elements of $G(k)$ cover X, and so $y = gu$ for some $(g,u) \in G(k) \times U(k)$. Therefore $y \in gU \subset f(|X|)$, which shows that it is an interior point of $f(|X|)$ in $\overline{f(|X|)}$.

(c) Because X is reduced, f factors through $f(X)_{\text{red}}$, and so the first statement follows from (a) and (b). The proof of the second statement uses similar ideas (DG, II, §5, 3.1). □

Orbits

Let $\mu: G \times X \to X$ be an action of an algebraic group G on an algebraic scheme X. For an $x \in X(k)$, the **orbit map**

$$\mu_x: G \to X, \quad g \mapsto gx,$$

is defined to be the restriction of μ to $G \times \{x\} \simeq G$. If $G(k^a)$ acts transitively on $X(k^a)$, then the orbit map μ_x is surjective because it is on k^a-points. The **orbit** of x is the image of $|\mu_x|$. According to (1.65b), it is a locally closed subset of X.

PROPOSITION 1.66 (ORBIT LEMMA). *Let G be a group variety acting on a variety X over an algebraically closed field. Every orbit of minimum dimension is closed.*

PROOF. The orbit O of $x \in X(k)$ is the image of the regular map μ_x, and so it contains a dense open subset U of its closure $\bar{O}$ (see A.15). But O is a union of the sets gU, $g \in G(k)$, and so is itself open in $\bar{O}$. Therefore $\bar{O} \smallsetminus O$ is closed

of dimension $< \dim \bar{O}$, and so (if nonempty) is a union of orbits of dimension $< \dim O$. Therefore O is closed if it has minimum dimension. □

In particular, there exists a closed orbit.

EXAMPLE 1.67. Let k be algebraically closed. In the action,

$$\mathrm{SL}_2 \times \mathbb{A}^2 \to \mathbb{A}^2, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix},$$

there are two orbits, namely, $\{(0,0)\}$ and its complement. The smaller of these is closed, but the larger is not closed and not even affine.

NOTES. The orbit lemma was first proved in Borel 1956. Today, it is an elementary fact, but in the 1950s it was considered surprising because the statement is false for a complex Lie group acting on complex variety. Proposition 1.65 is DG, II, §5, 3.1.

g.   The homomorphism theorem for smooth groups

In this section, $\varphi : G \to H$ is a homomorphism of algebraic groups over k.

PROPOSITION 1.68. *The image $\varphi(|G|)$ of $|G|$ in $|H|$ is closed.*

PROOF. As in the proof of Proposition 1.65(b), we may suppose that k is algebraically closed. Now $|\varphi(G)| = \varphi(G(k))$, which is a subgroup of $H(k) = |H|$. According to 1.65(b), $|\varphi(G)|$ is open in its closure $\overline{|\varphi(G)|}$, which is also a subgroup of $|H|$ (see 1.40). Therefore, $\overline{|\varphi(G)|}$ is a disjoint union of cosets of $|\varphi(G)|$, which are finite in number. As each coset is open, it is also closed. Therefore $|\varphi(G)|$ is closed in $\overline{|\varphi(G)|}$, and so equals it. □

COROLLARY 1.69. *If φ is dominant, then it is surjective.*

PROOF. The image of $|\varphi|$ is both dense and closed in $|H|$, and so equals $|H|$. □

PROPOSITION 1.70. *If H is reduced and φ is surjective, then φ is faithfully flat.*

PROOF. When we let G act on H through φ, then φ is equivariant. As φ is surjective, $G(k^a)$ acts transitively on $H(k^a)$, and so the statement follows from Proposition 1.65(a). □

SUMMARY 1.71. The following are equivalent (H reduced):
   (a) φ is dominant;
   (b) φ is surjective (i.e., $|\varphi|$ is surjective);
   (c) φ is faithfully flat.

THEOREM 1.72 (HOMOMORPHISM THEOREM). *Let* $\varphi\colon G \to H$ *be a homomorphism of algebraic groups over* k. *If* G *is smooth, then* φ *factors as a composite of homomorphisms*

$$G \xrightarrow{q} I \xrightarrow{i} H$$

with q *faithfully flat and* i *a closed immersion.*

PROOF. Let $I = \varphi(G)_{\mathrm{red}}$. When we let G act on H through φ, the map $\varphi\colon G \to H$ is equivariant, and so $\varphi = i \circ q$ with $q\colon G \to I$ faithfully flat and $i\colon I \to H$ an immersion (1.65c). From Proposition 1.68, we see that i is a closed immersion. As q is faithfully flat, the map $\mathcal{O}_I \to q_*\mathcal{O}_G$ is injective. It remains injective after extension of the base field, and so I is geometrically reduced. As m_H maps $I(k^{\mathrm{a}}) \times I(k^{\mathrm{a}})$ into $I(k^{\mathrm{a}})$, it maps $I \times I$ into I. It follows that I is an algebraic subgroup of H and that q and i are homomorphisms. $\quad\square$

DEFINITION 1.73. When $\varphi\colon G \to H$ factors into $G \xrightarrow{q} I \subset H$ with I an algebraic subgroup of H and q a faithfully flat homomorphism, we call I the ***image*** of φ.

Thus, the image of a homomorphism exists whenever the homomorphism theorem holds. Later we shall see that the homomorphism theorem always holds (3.34, 5.39).

h. Closed subfunctors: definitions and statements

Before defining normalizers and centralizers, we discuss some more general constructions. By a functor in this section, we mean a functor $\mathsf{Alg}_k^0 \to \mathsf{Set}$.

1.74. Let A be a k-algebra, and let h^A denote the functor $R \rightsquigarrow \mathrm{Hom}(A, R)$. Let $\mathfrak{a}$ be an ideal in A. The ***set of zeros*** of $\mathfrak{a}$ in $h^A(R)$ is

$$Z(R) = \{\varphi\colon A \to R \mid \varphi(a) = 0 \text{ for all } a \in \mathfrak{a}\}.$$

A homomorphism of k-algebras $R \to R'$ defines a map $Z(R) \to Z(R')$, and these maps make $R \rightsquigarrow Z(R)$ into a subfunctor of h^A, called the ***functor of zeros*** of $\mathfrak{a}$. For example, if $A = k[T_1, \ldots, T_n]$, then $h^A = \mathbb{A}^n$, and the set of zeros of $\mathfrak{a} = (f_1, \ldots, f_m)$ in $h^A(R)$ is the set of zeros in R^n of the polynomials f_i.

1.75. Let Z be a subfunctor of a functor X. From a map of functors $f\colon h^A \to X$, we obtain a subfunctor $f^{-1}(Z) \stackrel{\mathrm{def}}{=} Z \times_X h^A$ of h^A, namely,

$$R \rightsquigarrow \{a \in h^A(R) \mid f(R)(a) \in Z(R)\}.$$

We say that Z is a ***closed subfunctor*** of X if, for every map $f\colon h^A \to X$, the subfunctor $f^{-1}(Z)$ of h^A is the functor of zeros of some ideal $\mathfrak{a}$ in A.

We defer the proofs of the next three statements to the last section of this chapter.

1.76. Let X be an algebraic scheme over k. The closed subfunctors of $\tilde{X}$ are exactly those of the form $\tilde{Z}$ with Z a closed subscheme of X (see *1.100*).

1.77. Let $Y \to X$ be a map of functors. If Z is a closed subfunctor of X, then $Z \times_X Y$ is a closed subfunctor of Y (see *1.101*).

Let R be a small k-algebra. For a functor X, we let X_R denote the functor of small R-algebras defined by composing X with the forgetful functor $\mathsf{Alg}_R^0 \to \mathsf{Alg}_k^0$. For functors Y and X, we let $\underline{\mathrm{Mor}}(Y, X)$ denote the functor

$$R \rightsquigarrow \mathrm{Mor}(Y_R, X_R).$$

If Z is a subfunctor of X, then $\underline{\mathrm{Mor}}(Y, Z)$ is a subfunctor of $\underline{\mathrm{Mor}}(Y, X)$.

1.78. Let X be a functor and Y an algebraic scheme. If Z is a closed subfunctor of X, then $\underline{\mathrm{Mor}}(\tilde{Y}, Z)$ is a closed subfunctor of $\underline{\mathrm{Mor}}(\tilde{Y}, X)$ (see *1.105*).

i. Transporters

Let $G \times X \to X$ be an action of an algebraic group G on an algebraic scheme X over k, and let Y and Z be subschemes of X. The ***transporter*** $T_G(Y, Z)$ of Y into Z is the functor

$$R \rightsquigarrow \{g \in G(R) \mid gY_R \subset Z_R\}.$$

According to the Yoneda lemma, $gY_R \subset Z_R$ (as schemes) $\iff gY(R') \subset Z(R')$ for all (small) R-algebras R'.

PROPOSITION 1.79. *If Z is closed in X and Y is an algebraic scheme, then $T_G(Y, Z)$ is represented by a closed subscheme of G.*

PROOF. Consider the diagram

$$
\begin{array}{ccc}
T_G(Y,Z) \simeq \underline{\mathrm{Mor}}(Y,Z) \times_{\underline{\mathrm{Mor}}(Y,X)} G & \longrightarrow & G \\
\downarrow & & \downarrow b \\
\underline{\mathrm{Mor}}(Y,Z) & \xrightarrow{\;\;c\;\;} & \underline{\mathrm{Mor}}(Y,X)
\end{array}
$$

in which b is defined by the action of G on X and c is defined by the inclusion of Z into X. Then $\underline{\mathrm{Mor}}(Y, Z)$ is a closed subfunctor of $\underline{\mathrm{Mor}}(Y, X)$ (see *1.78*), and so $T_G(Y, Z)$ is a closed subfunctor of X (see *1.77*). Therefore it is represented by a closed subscheme of G (see *1.76*). □

COROLLARY 1.80. *If Y and Z are closed in X, then the functor*

$$R \rightsquigarrow \{g \in G(R) \mid gY_R = Z_R\}$$

is represented by a closed subscheme of G.

PROOF. The hypothesis implies that $T_G(Y,Z)$ and $T_G(Z,Y)$ are represented by closed subschemes of G. But the functor in question is equal to

$$T_G(Y,Z) \cap \operatorname{inv}(T_G(Z,Y)),$$

and so it also is represented by a closed subscheme of G. □

COROLLARY 1.81. *If Y is closed in G, then the functor*

$$R \rightsquigarrow \{g \in G(R) \mid gY_R = Y_R\}$$

*is represented by a subgroup scheme of G (called the **stabilizer** $\operatorname{Stab}_G(Y)$ of Y in G).*

PROOF. It is clearly a subgroup functor of G, and it is represented by a closed subscheme. □

ASIDE 1.82. Let Y be a subscheme of X. It follows from the Ax–Grothendieck theorem (1.55) that $T_G(Y,Y)$ acts on Y by automorphisms, i.e.,

$$T_G(Y,Y)(R) = \{g \in G(R) \mid gY_R = Y_R\}$$

for all k-algebras R. Thus $T_G(Y,Y) = \operatorname{Stab}_G(Y)$.

j. Normalizers

Let G be an algebraic group over k. We wish to define the normalizer $N = N_G(H)$ of an algebraic subgroup H of G. In characteristic zero, this is the unique algebraic subgroup N of G such that $N(k^a)$ is the normalizer of $H(k^a)$ in $G(k^a)$. In the general case, we need to consider the points in all small k-algebras.

PROPOSITION 1.83. *Let H be an algebraic subgroup of G. There is a unique algebraic subgroup $N = N_G(H)$ of G such that, for all k-algebras R,*

$$N(R) = \left\{ g \in G(R) \mid gH_R g^{-1} = H_R \right\}.$$

In other words, $N_G(H)$ represents the functor

$$R \rightsquigarrow N(R) \overset{\text{def}}{=} \{g \in G(R) \mid gH(R')g^{-1} = H(R') \text{ for all } R\text{-algebras } R'\}.$$

PROOF. The uniqueness follows from the Yoneda lemma (A.33). Clearly $N(R)$ is a subgroup of $G(R)$, and so it remains to show that N is represented by a closed subscheme of G (see 1.5). But, when we let G act on itself by inner automorphisms,

$$N = T_G(H,H) \cap \operatorname{inv}(T_G(H,H)),$$

and so this follows from Proposition 1.79. □

The algebraic subgroup $N_G(H)$ is called the **normalizer** of H in G. Directly from its definition, one sees that the formation of $N_G(H)$ commutes with extension of the base field. Clearly H is normal in G if and only if $N_G(H) = G$.

PROPOSITION 1.84. *Let H be a smooth algebraic subgroup of G and let k' be an extension of k such that $H(k')$ is dense in H. Then $N_G(H)(k)$ consists of the elements of $G(k)$ normalizing $H(k')$ in $G(k')$.*

PROOF. Let $g \in G(k)$ normalize $H(k')$, and let ${}^g H$ denote the image of H under the isomorphism $x \mapsto gxg^{-1} \colon G \to G$. Then ${}^g H \cap H$ is an algebraic subgroup of H such that $({}^g H \cap H)(k') = H(k')$, and so ${}^g H = H$. Therefore $gH(R)g^{-1} = H(R)$ for all k-algebras R, and so $g \in N_G(H)(k)$. The converse is obvious. □

We let $\mathrm{inn}(g)$ denote the inner automorphism $x \mapsto gxg^{-1} \colon G \to G$ of G defined by $g \in G(k)$.

COROLLARY 1.85. *Let H be an algebraic subgroup of a smooth algebraic group G, and let k' be a separably closed field containing k. If $H_{k'}$ is stable under $\mathrm{inn}(g)$ for all $g \in G(k')$, then H is normal in G.*

PROOF. Let $N = N_G(H)$. Then N is an algebraic subgroup of G, and the hypothesis implies that $N(k') = G(k')$. As G is smooth, this implies that $N = G$ (see 1.15b). □

COROLLARY 1.86. *Let H be a subgroup variety of a group variety G, and k' be a separably closed field containing k. If $H(k')$ is normal in $G(k')$, then H is normal in G.*

PROOF. Because H is a variety, $H(k')$ is dense in H, and so Proposition 1.84 shows that $N_G(H)(k') = G(k')$. Because G is a variety, this implies that $N_G(H) = G$. □

COROLLARY 1.87. *Let H be a normal algebraic subgroup of a smooth algebraic group G. If H_{red} is an algebraic subgroup of G, then it is normal in G.*

PROOF. As H is normal in G, $H(k^s)$ is normal in $G(k^s)$, but $H(k^s) = H_{\mathrm{red}}(k^s)$ and so we can apply Corollary 1.86. □

Corollaries 1.86 and 1.87 may fail if G is not smooth. For example, if k is perfect, then G_{red} is a subgroup variety of G such that $G_{\mathrm{red}}(k) = G(k)$, but it need not be normal in G (see 2.35 below for examples).

REMARK 1.88. Let H be a smooth algebraic subgroup of an algebraic group G over k.

(a) If k is perfect, then $N = N_G(H)_{\mathrm{red}}$ is the unique subgroup variety of G such that $N(k^a)$ is the normalizer of $H(k^a)$ in $G(k^a)$.

(b) If $N = N_G(H)$ is smooth, then it is the unique subgroup variety of G such that $N(k^a)$ is the normalizer of $H(k^a)$ in $G(k^a)$.

For (a), note that Proposition 1.84 implies that N has the specified property, which characterizes it by 1.44. Statement (b) follows from (a). Note that (b) always applies in characteristic zero because then all algebraic groups are smooth (3.23, 8.39 below).

DEFINITION 1.89. An algebraic subgroup H of an algebraic group G is **weakly characteristic** if, for all fields k' containing k, $H_{k'}$ is stable under all automorphisms of $G_{k'}$.

PROPOSITION 1.90. *Let $H \subset N$ be algebraic subgroups of a smooth algebraic group G. If H is weakly characteristic in N and N is normal in G, then H is normal in G.*

PROOF. By hypothesis, H_{k^s} is stable under $\mathrm{inn}(g)|N_{k^s}$ for all $g \in G(k^s)$, and so this follows from (1.86). □

REMARK 1.91. A weakly characteristic algebraic subgroup need not be characteristic. For example, the largest unipotent subgroup of a commutative algebraic group over a perfect field is weakly characteristic but not in general characteristic (see 16.19 below).

k. Centralizers

Let G be an algebraic group over k. We wish to define the centralizer $C = C_G(H)$ of an algebraic subgroup H of G. In characteristic zero, this is the unique algebraic subgroup of G such that $C(k^a)$ is the centralizer of $H(k^a)$ in $G(k^a)$. In the general case, we need to consider the points in all small k-algebras.

PROPOSITION 1.92. *Let H be an algebraic subgroup of G. There is a unique algebraic subgroup $C = C_G(H)$ of G such that, for all k-algebras R,*

$$C(R) = \{g \in N(R) \mid g \text{ centralizes } H(R') \text{ in } G(R') \text{ for all } R\text{-algebras } R'\}.$$

PROOF. Let G act on $G \times G$ by

$$g(g_1, g_2) = (g_1, g g_2 g^{-1}), \quad g, g_1, g_2 \in G(R).$$

Embed H diagonally in $G \times G$, and let Δ_H denote the diagonal in $H \times H$. Then Δ_H is closed in $H \times H$ (see 1.22), and hence in $G \times G$. Now $C = T_G(H, \Delta_H)$, and so Proposition 1.79 shows that it is represented by a closed subscheme G. □

The algebraic subgroup $C_G(H)$ is called the **centralizer** of H in G. It is the largest algebraic subgroup of $N_G(H)$ acting trivially on H. Directly from its

definition, one sees that the formation of $C_G(H)$ commutes with extension of
the base field. The **centre** $Z(G)$ of G is defined to be $C_G(G)$. An extension

$$e \to N \xrightarrow{i} G \xrightarrow{\pi} Q \to e$$

is **central** if N is contained in $Z(G)$.

PROPOSITION 1.93. *Let H be a smooth algebraic subgroup of G, and let k' be
an extension of k such that $H(k')$ is dense in H. Then $C_G(H)(k)$ consists of the
elements of $G(k)$ centralizing $H(k')$ in $G(k')$.*

PROOF. Let g be an element of $G(k)$ centralizing $H(k')$. Then $g \in N_G(H)(k)$
(see 1.84), and the homomorphism $x \mapsto gxg^{-1} \colon H \to H$ coincides with the
identity map on an algebraic subgroup H' of H such that $H'(k') = H(k')$. This
implies that $H' = H$, and so g centralizes H. □

COROLLARY 1.94. *Let H be a subgroup variety of a group variety G. If $H(k^s)$
is contained in the centre of $G(k^s)$, then H is contained in the centre of G.*

PROOF. We may suppose that k is separably closed (1.54a). Because H is a
variety, $H(k)$ is dense in H, and so the proposition shows that $C_G(H)(k) =
G(k)$. As G is a group variety, this implies that $C_G(H) = G$ (1.17). □

REMARK 1.95. Let H be a smooth algebraic subgroup of an algebraic group G
over k.
  (a) If k is perfect, then $C = C_G(H)_{\text{red}}$ is the unique subgroup variety of G
      such that $C(k^a)$ is the centralizer of $H(k^a)$ in $G(k^a)$.
  (b) If $C = C_G(H)$ is smooth, then it is the unique subgroup variety of G such
      that $C(k^a)$ is the centralizer of $H(k^a)$ in $G(k^a)$.

The proof is similar to that of the statements in Remark 1.88. Again, (b) always
applies in characteristic zero.

REMARK 1.96. The centralizer of an algebraic subgroup H of an algebraic
group G need not be smooth, even when G and H are smooth. For example, let
k be a field of characteristic $2 \neq 0$, and let $a \in k \smallsetminus k^2$. Let $G = \mathrm{SL}_4$, and let H
be the algebraic subgroup of G generated by

$$h = \begin{pmatrix} 0 & 0 & 0 & a \\ 0 & 0 & a^{-1} & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in G(k).$$

It is smooth (see 2.51 below), and $C_G(H)$ is the algebraic subgroup of G of
matrices

$$\begin{pmatrix} x & 0 & 0 & ay \\ 0 & z & t & 0 \\ 0 & at & z & 0 \\ y & 0 & 0 & x \end{pmatrix} \in G(R)$$

with $(xz + ayt)^2 - a(xt + yz)^2 = 1$. This is not reduced.

REMARK 1.97. The centre $Z(G)$ of a smooth algebraic group need not be smooth – for example, in characteristic p, the centre of SL_p is the nonreduced algebraic group μ_p. For another example, let G, φ, and N be as in 6.48 below, and let $H = \mathbb{G}_a \rtimes_\varphi G$; then $Z(H) = N$, which is not reduced.

For some situations (other than characteristic zero) where centralizers and normalizers are smooth, see (13.16) and (15.20) below.

NOTES. The normalizer N of a subgroup variety H of a group variety G need not be smooth. In the old literature, the normalizer of H in G is defined to be the subgroup variety $(N_{k^a})_{\mathrm{red}}$ of G_{k^a}, which "need not be defined over k" (Borel 1991, p. 52). The centralizer is similarly defined to be a subgroup variety of G_{k^a} (not of G).

l.   Closed subfunctors: proofs

In this section, all functors are from the category of small k-algebras to sets.

Closed subfunctors

LEMMA 1.98. *Let Z be a subfunctor of a functor X. Then Z is closed in X if and only if it satisfies the following condition: for every k-algebra A and map of functors $f : h^A \to Y$, the subfunctor $f^{-1}(Z)$ of h^A is represented by a quotient of A.*

PROOF. This is a restatement of the definition.   □

A map of functors $f : h^A \to X$ corresponds to an element $\alpha \in X(A)$. Explicitly, $f(R) : h^A(R) \to X(R)$ is the map sending $\varphi \in h^A(R) = \mathrm{Hom}(A, R)$ to $X(\varphi)(\alpha) \in X(R)$, and so

$$f^{-1}(Z)(R) = \{\varphi : A \to R \mid X(\varphi)(\alpha) \in Z(R)\}.$$

Therefore, Z is closed in X if and only if, for every A and $\alpha \in X(A)$, the functor

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

is represented by a quotient of A. In down-to-earth terms, this means that there exists an ideal $\mathfrak{a} \subset A$ such that

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

EXAMPLE 1.99. Let B be a k-algebra and Z a subfunctor of $X = h^B$. For the identity map $f : h^B \to X$, $f^{-1}(Z) = Z$. It follows that, if Z is closed in h^B, then it is represented by a quotient of B. Conversely, suppose that Z is represented by a quotient $B/\mathfrak{b}$ of B, so that

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

Let $\alpha \in X(A) = \text{Hom}(B, A)$, and let f be the corresponding map $f : h^A \to X$. Then

$$f^{-1}(Z)(R) = \{\varphi : A \to R \mid \varphi \circ \alpha \in Z(R)\} = \{\varphi : A \to R \mid \varphi(\alpha(\mathfrak{b})) = 0\},$$

and so $f^{-1}(Z)$ is represented by the quotient $A/\alpha(\mathfrak{b})$ of A.

We conclude that the closed subfunctors of h^B are exactly those defined by closed subschemes of $\text{Spm}(B)$.

EXAMPLE 1.100. Consider the functor $h_X : R \rightsquigarrow X(R)$ defined by an algebraic scheme X over k. If Z is a closed subscheme of X, then certainly h_Z is a closed subfunctor of h_X. Conversely, let Z be a closed subfunctor of X. For each open affine subscheme U of X, there is a unique ideal $\mathcal{I}(U)$ in $\mathcal{O}(U)$ such that $Z \cap h_U = h^{\mathcal{O}(U)/\mathcal{I}(U)}$ (apply 1.99). Because of the uniqueness, the sheaves on U and U' defined by $\mathcal{I}(U)$ and $\mathcal{I}(U')$ coincide on $U \cap U'$. Therefore, there exists a (unique) coherent sheaf $\mathcal{I}$ on X such that $\Gamma(U, \mathcal{I}) = \mathcal{I}(U)$ for all open affine subschemes U in X. Now $Z = h_{Z'}$, where Z' is the closed subscheme of X defined by $\mathcal{I}$.

We conclude that the closed subfunctors of h_X are exactly those defined by closed subschemes of X.

PROPOSITION 1.101. *Let Z be a closed subfunctor of a functor X. For every map $Y \to X$ of functors, $Z \times_X Y$ is a closed subfunctor of Y.*

PROOF. Let $f : h^A \to Y$ be a map of functors. Then

$$f^{-1}(Z \times_X Y) \overset{\text{def}}{=} (Z \times_X Y) \times_Y h^A = Z \times_X h^A,$$

which is the functor of zeros of some $\mathfrak{a} \subset A$ because Z is closed in X. □

Restriction of scalars

LEMMA 1.102. *Let A and B be k-algebras and let $\mathfrak{b}$ be an ideal in $B \otimes A$. Among the ideals $\mathfrak{a}$ in A such that $B \otimes \mathfrak{a} \supset \mathfrak{b}$, there exists a smallest one.*

PROOF. Choose a basis $(e_i)_{i \in I}$ for B as k-vector space. Each element b of $B \otimes A$ can be expressed uniquely as a finite sum $b = \sum e_i \otimes a_i$, $a_i \in A$, and we let $\mathfrak{a}_0$ denote the ideal in A generated by the coordinates a_i of the elements $b \in \mathfrak{b}$. Clearly $B \otimes \mathfrak{a}_0 \supset \mathfrak{b}$. Let $\mathfrak{a}$ be a second ideal such that $B \otimes \mathfrak{a} \supset \mathfrak{b}$. Then the coordinates of all elements of $\mathfrak{b}$ lie in $\mathfrak{a}$, and so $\mathfrak{a} \supset \mathfrak{a}_0$. □

Let B be a small k-algebra and X a functor $\mathsf{Alg}_k^0 \to \mathsf{Set}$. We define X_* to be the functor

$$R \rightsquigarrow X(B \otimes R) : \mathsf{Alg}_k^0 \to \mathsf{Set}.$$

PROPOSITION 1.103. *Let B be a small k-algebra, and let Z be a subfunctor of a functor X. If Z is closed in X, then Z_* is closed in X_*.*

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

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

i.e.,

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

We regard α as an element of $X(B \otimes A)$. Because Z is closed in X, there exists an ideal $\mathfrak{b}$ in $B \otimes A$ such that, for all homomorphisms $\varphi': B \otimes A \to R'$,

$$X(\varphi')(\alpha) \in Z(R') \iff \varphi'(\mathfrak{b}) = 0.$$

In particular (taking $\varphi' = B \otimes \varphi$), we have

$$X(B \otimes \varphi)(\alpha) \in Z(B \otimes R) \iff (B \otimes \varphi)(\mathfrak{b}) = 0. \tag{6}$$

According to Lemma 1.102, there exists a well-defined ideal $\mathfrak{a}$ in A such that an ideal $\mathfrak{a}'$ of A contains $\mathfrak{a}$ if and only if $B \otimes \mathfrak{a}' \supset \mathfrak{b}$. On applying this to the ideal $\mathfrak{a}' = \mathrm{Ker}(\varphi)$, we find that

$$\mathfrak{a} \subset \mathrm{Ker}(\varphi) \iff \mathfrak{b} \subset B \otimes \mathrm{Ker}(\varphi) = \mathrm{Ker}(B \otimes \varphi). \tag{7}$$

Now

$$\varphi(\mathfrak{a}) = 0 \overset{(7)}{\iff} (B \otimes \varphi)(\mathfrak{b}) = 0 \overset{(6)}{\iff} X(B \otimes \varphi)(\alpha) \in Z(B \otimes R),$$

as required. $\qquad\square$

Application to Mor

LEMMA 1.104. *An intersection of closed subfunctors of a functor is closed.*

PROOF. Let Z_i, $i \in I$, be closed subfunctors of X and $f: h^A \to X$ a map of functors. For each $i \in I$, there is an ideal $\mathfrak{a}_i$ of A such that $f^{-1}(Z_i) \subset h^A(R)$ is the functor of zeros of $\mathfrak{a}_i$. Now $f^{-1}(\bigcap_{i \in I} Z_i) = \bigcap_{i \in I} f^{-1}(Z_i)$ is the functor of zeros of $\mathfrak{a} = \sum_{i \in I} \mathfrak{a}_i$. $\qquad\square$

THEOREM 1.105. *Let Z be a subfunctor of a functor X, and let Y be an algebraic scheme. If Z is closed in X, then $\underline{\mathrm{Mor}}(Y, Z)$ is closed in $\underline{\mathrm{Mor}}(Y, X)$.*

PROOF. Suppose first that $Y = h^B$ for some k-algebra B (which we may assume to be small). Then, for every k-algebra R,

$$\underline{\mathrm{Mor}}(Y, X)(R) = X(B \otimes R),$$

and so $\underline{\mathrm{Mor}}(Y, X) = X_*$. In this case, the theorem is proved in Proposition 1.103.

Let $Y = \bigcup_i Y_i$ be a finite covering of Y by open affine subschemes, and consider the diagram

$$
\begin{array}{ccc}
\underline{\mathrm{Mor}}(Y,X) & \overset{\rho_i}{\longrightarrow} & \underline{\mathrm{Mor}}(Y_i,X) \\
\cup & & \cup \\
\underline{\mathrm{Mor}}(Y,Z) & \longrightarrow & \underline{\mathrm{Mor}}(Y_i,Z)
\end{array}
$$

in which ρ_i is the restriction map. We know that $\underline{\mathrm{Mor}}(Y_i,Z)$ is closed in the functor $\underline{\mathrm{Mor}}(Y_i,X)$, hence $\rho_i^{-1}\left(\underline{\mathrm{Mor}}(Y_i,Z)\right)$ is closed in $\underline{\mathrm{Mor}}(Y,X)$ (see 1.101), and so (see 1.104) it remains to show that

$$
\underline{\mathrm{Mor}}(Y,Z) = \bigcap_i \rho_i^{-1}\left(\underline{\mathrm{Mor}}(Y_i,Z)\right).
$$

Let $H_i = \rho_i^{-1}\left(\underline{\mathrm{Mor}}(Y_i,Z)\right)$. Certainly, $\underline{\mathrm{Mor}}(Y,Z) \subset \bigcap_i H_i$, and for the reverse inclusion it suffices to show that the map of functors

$$
\left(\bigcap_i H_i\right) \times Y \to X
$$

defined by the evaluation map $\mu:\underline{\mathrm{Mor}}(Y,X) \times Y \to X$ factors through Z. For each i, we know that $H_i \times Y_i \to X$ factors through Z. By definition, Z will become a closed subscheme of an (affine) scheme X after we have pulled back by a map of functors $h^A \to X$. Then $\mu^{-1}(Z)$ is a closed subscheme of $\underline{\mathrm{Mor}}(Y,X) \times Y$ containing $\left(\bigcap_i H_i\right) \times Y_i$ for all i, and hence containing $\left(\bigcap_i H_i\right) \times Y$. Since this holds for all maps $h^A \to X$, it follows that $\mu^{-1}(Z) \supset \left(\bigcap_i H_i\right) \times Y$. □

ASIDE 1.106. In this section, we used that k is a field only to deduce in the proof of Lemma 1.102 that B is free as a k-module. The same arguments suffice to prove the following more general statement: let k be a commutative ring; let X be a functor of k-algebras and Z a closed subfunctor of X; let Y be a scheme locally free over k, i.e., Y admits a covering by open affine subschemes Y_i such that each $\mathcal{O}(Y_i)$ is free as a k-module; then $\underline{\mathrm{Mor}}(Y,Z)$ is a closed subfunctor of $\underline{\mathrm{Mor}}(Y,X)$. See DG, I, §2, 7.5; also Jantzen 2003, 1.15.

Exercises

EXERCISE 1-1. Let k be a field of characteristic zero.

(a) Let R be a k-algebra, and let a be a nilpotent element of R. For an element x of an R-algebra S, let $e^{ax} = 1 + ax + (ax)^2/2! + \cdots$ (finite sum). Show that the maps $x \mapsto e^{ax}:S \to S^\times$ define a homomorphism $\mathbb{G}_{aR} \to \mathbb{G}_{mR}$, and that every homomorphism from $\mathbb{G}_a$ to $\mathbb{G}_m$ over R is of this form for a unique a.

(b) Deduce that the functor $R \rightsquigarrow \mathrm{Hom}(\mathbb{G}_{aR},\mathbb{G}_{mR})$ is not representable (consider the ring $k[[t]] = \varprojlim k[[t]]/(t^n)$).

See https://mathoverflow.net/, question 4062.

Examples and Basic Constructions

Let G be an algebraic group over k. Then $\mathcal{O}(G)$ is a k-algebra. If G is affine, then $G \simeq \mathrm{Spm}(\mathcal{O}(G))$. At the opposite extreme, an algebraic group G is ***anti-affine*** if $\mathcal{O}(G) = k$. For example, an algebraic group is anti-affine if it is complete as an algebraic scheme. Later (8.36), we shall show that every algebraic group is an extension of an affine algebraic group by an anti-affine algebraic group in a unique way. In this chapter, we give examples of affine and anti-affine algebraic groups, and we explain some constructions involving algebraic groups.

When G is affine, we call $\mathcal{O}(G)$ the ***coordinate ring*** of G. If G is embedded as a closed subvariety of some affine space $\mathbb{A}^n$, then $\mathcal{O}(G)$ is the ring of functions on G generated by the coordinate functions on $\mathbb{A}^n$, whence the name. For an affine algebraic group (G, m), the homomorphism of k-algebras $\Delta_G \colon \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$ corresponding to $m \colon G \times G \to G$ is called the ***comultiplication map***.

Recall (1.4) that to give an algebraic group over k amounts to giving a functor from k-algebras to groups whose underlying functor F to sets is representable by an algebraic scheme over k. In the affine case, this means that there is a k-algebra A and a "universal" element $a \in F(A)$ such that, for every k-algebra R and $x \in F(R)$, there exists a unique homomorphism $A \to R$ with the property that $F(A) \to F(R)$ sends a to x.

a. Affine algebraic groups

2.1. The ***additive group*** $\mathbb{G}_a$ is the functor $R \rightsquigarrow (R, +)$. It is represented by $\mathcal{O}(\mathbb{G}_a) = k[T]$, and the universal element in $\mathbb{G}_a(k[T])$ is T: for every k-algebra R and $x \in \mathbb{G}_a(R)$, there is a unique homomorphism $k[T] \to R$ with the property that $\mathbb{G}_a(k[T]) \to \mathbb{G}_a(R)$ sends T to r. The comultiplication map is the k-algebra homomorphism $\Delta \colon k[T] \to k[T] \otimes k[T]$ such that

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

2.2. The **multiplicative group** $\mathbb{G}_m$ is the functor $R \rightsquigarrow (R^\times, \cdot)$. It is represented by $\mathcal{O}(\mathbb{G}_m) = k[T, T^{-1}] \subset k(T)$, and the comultiplication map is the k-algebra homomorphism Δ such that

$$\Delta(T) = T \otimes T.$$

2.3. Let F be a finite group. The **constant algebraic group** F_k has underlying scheme a disjoint union of copies of $\mathrm{Spm}(k)$ indexed by the elements of F, i.e.,

$$F_k = \bigsqcup\nolimits_{a \in F} S_a, \quad S_a = \mathrm{Spm}(k).$$

Then

$$F_k \times F_k = \bigsqcup\nolimits_{(a,b) \in F \times F} S_{(a,b)}, \quad S_{(a,b)} = S_a \times S_b = \mathrm{Spm}(k),$$

and the multiplication map m sends $S_{(a,b)}$ to S_{ab}. For a k-algebra R,

$$F_k(R) = \mathrm{Hom}(\pi_0, F) \quad \text{(maps of sets)}$$

where π_0 is the set of connected components of $\mathrm{spm}(R)$. In particular, $F_k(R) = F$ if R has no nontrivial idempotents. The coordinate ring of F_k is a product of copies of k indexed by the elements of F,

$$\mathcal{O}(F_k) = \prod\nolimits_{a \in F} k_a, \quad k_a = k,$$

and Δ maps the factor k_c diagonally into $\prod_{a,b \in F,\, ab=c} k_a \otimes k_b$.

If F is the trivial group e, then F_k is the trivial algebraic group $*$, which has coordinate ring $\mathcal{O}(*) = k$ and comultiplication map the unique k-algebra homomorphism $k \to k \otimes k$.

2.4. For an integer $n \geq 1$, μ_n is the functor $R \rightsquigarrow \{r \in R \mid r^n = 1\}$. It is represented by $\mathcal{O}(\mu_n) = k[T]/(T^n - 1)$, and the comultiplication map is induced by that of $\mathbb{G}_m$.

2.5. Let k have characteristic $p \neq 0$, and let α_{p^m} be the functor $R \rightsquigarrow \{r \in R \mid r^{p^m} = 0\}$. Then $\alpha_{p^m}(R)$ is a subgroup of $(R, +)$ because $(x + y)^{p^m} = x^{p^m} + y^{p^m}$ in characteristic p. The functor is represented by $\mathcal{O}(\alpha_{p^m}) = k[T]/(T^{p^m})$, and the comultiplication map is induced by that of $\mathbb{G}_a$. Note that

$$k[T]/(T^{p^m}) = k[T]/((T+1)^{p^m} - 1) = k[U]/(U^{p^m} - 1), \quad U = T + 1,$$

and so α_{p^m} and μ_{p^m} are isomorphic as schemes (but not as algebraic groups).

2.6. For a k-vector space V, we let $V_{\mathfrak{a}}$ denote the functor $R \rightsquigarrow V \otimes R$.[1] Recall that for a k-vector space W, the symmetric algebra $\mathrm{Sym}(W)$ on W has the

---

[1]Our notation $V_{\mathfrak{a}}$ is that of DG, II, §1, 2.1. Many other notations are used, for example, $\mathbf{W}(V)$ (SGA 3, I, 4.6.1) or V_a (Jantzen 2003, 2.2).

following universal property: every k-linear map $W \to A$ from W to a k-algebra A extends uniquely to a k-algebra homomorphism $\mathrm{Sym}(W) \to A$. Assume that V is finite-dimensional, and let $V^\vee$ be its dual. Then, for a k-algebra R,

$$V \otimes R \simeq \mathrm{Hom}_k(V^\vee, R) \quad \text{(homomorphisms of k-vector spaces)}$$
$$\simeq \mathrm{Hom}_k(\mathrm{Sym}(V^\vee), R) \quad \text{(homomorphisms of k-algebras)}.$$

Therefore, $V_\mathfrak{a}$ is an algebraic group with $\mathcal{O}(V_\mathfrak{a}) = \mathrm{Sym}(V^\vee)$.

Let $\{e_1, \ldots, e_n\}$ be a basis for V and $\{f_1, \ldots, f_n\}$ the dual basis for $V^\vee$. Then

$$\mathrm{Sym}(V^\vee) \simeq k[f_1, \ldots, f_n] \quad \text{(polynomial ring)}.$$

For this reason, $\mathrm{Sym}(V^\vee)$ is often called the ring of polynomial functions on V. The choice of a basis for V determines an isomorphism $\mathbb{G}_a^n \to V_\mathfrak{a}$.

2.7. For integers $m, n \geq 1$, let $M_{m,n}$ denote the functor sending R to the additive group $M_{m,n}(R)$ of $m \times n$ matrices with entries in R. It is represented by $k[T_{11}, T_{12}, \ldots, T_{mn}]$. For a vector space V over k, we define End_V to be the functor

$$R \rightsquigarrow \mathrm{End}(V_R) \quad \text{(R-linear endomorphisms)}.$$

When V has finite dimension n, the choice of a basis for V determines an isomorphism $\mathrm{End}_V \to M_{n,n}$, and so End_V is an algebraic group.

2.8. The **general linear group** GL_n is the functor $R \rightsquigarrow \mathrm{GL}_n(R)$ (multiplicative group of invertible $n \times n$ matrices with entries in R). It is represented by

$$\mathcal{O}(\mathrm{GL}_n) = \frac{k[T_{11}, T_{12}, \ldots, T_{nn}, T]}{(\det(T_{ij})T - 1)} = k[T_{11}, T_{12}, \ldots, T_{nn}, 1/\det],$$

and the universal element in $\mathrm{GL}_n(k[T_{11}, \ldots])$ is the matrix $(T_{ij})_{1 \leq i,j \leq n}$: for every $(a_{ij}) \in \mathrm{GL}_n(R)$, there is a unique homomorphism $k[T_{11}, \ldots] \to R$ with the property that $\mathrm{GL}_n(k[T_{11}, \ldots]) \to \mathrm{GL}_n(R)$ sends (T_{ij}) to (a_{ij}). The comultiplication map is the k-algebra homomorphism

$$\Delta : k[T_{11}, \ldots] \to k[T_{11}, \ldots] \otimes k[T_{11}, \ldots]$$

such that

$$\Delta T_{ij} = \sum_{1 \leq l \leq n} T_{il} \otimes T_{lj}. \tag{8}$$

Symbolically, the matrix $(\Delta T_{ij}) = (T_{il}) \otimes (T_{lj})$.

More generally, for any vector space V over k, we define GL_V to be the functor

$$R \rightsquigarrow \mathrm{Aut}(V_R) \quad \text{(R-linear automorphisms)}.$$

If V has finite dimension n, then the choice of a basis for V determines an isomorphism $\mathrm{GL}_V \to \mathrm{GL}_n$, and GL_V is an algebraic group.

The algebraic group SL_n is a subgroup of GL_n, and SL_V is defined to be the similar subgroup of GL_V.

2.9. The following are algebraic subgroups of GL_n:

$\mathbb{T}_n: R \rightsquigarrow \{(a_{ij}) \mid a_{ij} = 0 \text{ for } i > j\}$ (upper triangular matrices)

$\mathbb{U}_n: R \rightsquigarrow \{(a_{ij}) \mid a_{ij} = 0 \text{ for } i > j, \, a_{ij} = 1 \text{ for } i = j\}$

$\mathbb{D}_n: R \rightsquigarrow \{(a_{ij}) \mid a_{ij} = 0 \text{ for } i \neq j\}$ (diagonal matrices).

$$
\begin{pmatrix}
* & * & * & \cdots & * \\
  & * & * &   & * \\
  &   & \ddots & \ddots & \\
\mathbf{0} &   &   & * & * \\
  &   &   &   & *
\end{pmatrix}
\qquad
\begin{pmatrix}
1 & * & * & \cdots & * \\
  & 1 & * &   & * \\
  &   & \ddots & \ddots & \\
\mathbf{0} &   &   & 1 & * \\
  &   &   &   & 1
\end{pmatrix}
\qquad
\begin{pmatrix}
* & & & & \\
  & * & & \mathbf{0} & \\
  &   & \ddots & & \\
\mathbf{0} &   &   & * & \\
  &   &   &   & *
\end{pmatrix}
$$
$$\quad\; \mathbb{T}_n \qquad\qquad\qquad\qquad \mathbb{U}_n \qquad\qquad\qquad\qquad \mathbb{D}_n$$

For example, $\mathbb{U}_n$ is represented by the quotient of $k[T_{11}, T_{12}, \ldots, T_{nn}]$ by the ideal generated by the polynomials

$$T_{ij} \; (i > j), \quad T_{ii} - 1 \text{ (all } i).$$

2.10. Let $C \in \mathrm{GL}_n(k)$, and consider the group-valued functor

$$G: R \rightsquigarrow \{A \in \mathrm{GL}_n(R) \mid A^t C A = C\}$$

(A^t is the transpose of A). The condition $A^t C A = C$ is polynomial on the entries of A, and so G is represented by a quotient of $\mathcal{O}(\mathrm{GL}_n)$. Therefore it is an algebraic group. If $C = (c_{ij})$, then an element of $\mathrm{GL}_n(R)$ lies in $G(R)$ if and only if it preserves the form $\phi(\vec{x}, \vec{y}) = \sum c_{ij} x_i y_j$ on R^n. The following examples are especially important (they are the split almost-simple classical groups).

(a) The subgroup SL_n of GL_n does not fit this pattern, but we include it here for reference.

(b) When $\mathrm{char}(k) \neq 2$, the orthogonal group O_{2n+1} is the algebraic group attached to the matrix $C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I_n \\ 0 & I_n & 0 \end{pmatrix}$. Then, $\mathrm{O}_{2n+1}(R)$ consists of the elements of $\mathrm{GL}_{2n+1}(R)$ preserving the symmetric bilinear form

$$\phi(\vec{x}, \vec{y}) = x_0 y_0 + (x_1 y_{n+1} + x_{n+1} y_1) + \cdots + (x_n y_{2n} + x_n y_{2n})$$

on R^{2n+1}. The special orthogonal group SO_{2n+1} is $\mathrm{O}_{2n+1} \cap \mathrm{SL}_{2n+1}$.

(c) The symplectic group Sp_{2n} is the algebraic group attached to the matrix $C = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. Then $\mathrm{Sp}_{2n}(R)$ consists of the elements of $\mathrm{GL}_n(R)$ preserving the skew-symmetric bilinear form

$$\phi(\vec{x}, \vec{y}) = (x_1 y_{n+1} - x_{n+1} y_1) + \cdots + (x_n y_{2n} - x_{2n} y_n) = \vec{x}^t C \vec{y}$$

on R^{2n}. More generally, let V be a vector space of dimension $2n$ over k and ϕ a nondegenerate alternating form on V. Let $\mathrm{Sp}(V, \phi)$ be the

algebraic subgroup of GL_V whose elements preserve ϕ. Choose a basis $e_1, \ldots, e_{2n}$ for V such that $\phi(e_i, e_j) = \pm 1$ if $j = i \pm n$ and $= 0$ otherwise. This identifies V with k^{2n} and $\phi(\vec{x}, \vec{y})$ with $\vec{x}^t C \vec{y}$, and so it defines an isomorphism $\mathrm{Sp}(V, \phi) \to \mathrm{Sp}_{2n}$,

(d) When $\mathrm{char}(k) \neq 2$, the orthogonal group O_{2n} is the algebraic group attached to the matrix $C = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$. Thus, $\mathrm{O}_{2n}(R)$ consists of the elements of $GL_{2n}(R)$ preserving the symmetric bilinear form

$$\phi(\vec{x}, \vec{y}) = (x_1 y_{n+1} + x_{n+1} y_1) + \cdots + (x_n y_{2n} + x_n y_{2n})$$

on R^{2n}. The special orthogonal group SO_{2n} is $\mathrm{O}_{2n} \cap \mathrm{SL}_{2n}$.

More generally, we write $\mathrm{SO}(V, \phi)$ and $\mathrm{O}(V, \phi)$ for the groups attached to a bilinear form ϕ on a vector space V. When $\mathrm{char}(k) = 2$, the orthogonal groups can be defined using quadratic forms instead of bilinear forms (see Section 21j below).

2.11. An algebraic group G over k is a **torus** if it becomes isomorphic to a product of copies of $\mathbb{G}_m$ over a finite separable extension of k.

2.12. An algebraic group U over k is a **vector group** if it is isomorphic to a product of copies of $\mathbb{G}_a$. For example, the algebraic group V_a attached to a finite-dimensional vector space V over k is a vector group. This vector group has a natural action of $\mathbb{G}_m$. An action of $\mathbb{G}_m$ on a vector group U is said to be **linear** if it is defined by an isomorphism $U \to V_a$ and the natural action on V_a. In characteristic zero, there is exactly one linear action of $\mathbb{G}_m$ on a vector group U, namely that defined by the canonical isomorphism $U \simeq \mathrm{Lie}(U)_a$ (see 10.9). In characteristic p, a vector group may have more than one linear action, and it has actions that are not linear, for example, the composite of a linear action with the pth power map on $\mathbb{G}_m$.

2.13. Let V be a finite-dimensional vector space over k. Then GL_V acts on the vector space $T_s^r \overset{\mathrm{def}}{=} V^{\otimes r} \otimes (V^\vee)^{\otimes s}$, and so $t \in T_s^r$ defines a natural map

$$g \mapsto g \cdot t : G(R) \to T_s^r(R), \quad R \text{ a } k\text{-algebra},$$

and hence a morphism of schemes $G \to (T_s^r)_a$. The fibre of this map over t is an algebraic subgroup over GL_V, called the **algebraic group fixing the tensor** t. The **algebraic group fixing tensors** $t_1, \ldots, t_n$ is defined to be the intersection of the algebraic groups fixing the t_i individually.

For example, a $t \in T_s^0$ can be regarded as a multilinear map

$$t : V \times \cdots \times V \to k \quad (s \text{ copies of } V).$$

Let G be the algebraic group fixing t. For a k-algebra R, $G(R)$ consists of the $g \in GL_V(R)$ such that

$$t(g v_1, \ldots, g v_s) = (v_1, \ldots, v_s), \quad \text{all } (v_i) \in V^s.$$

2.14. An algebraic group G over k is ***finite*** if it is finite as a scheme over k. This means that G is affine and $\mathcal{O}(G)$ is a finite k-algebra (see 11.2). The ***order*** $o(G)$ of G is the dimension of $\mathcal{O}(G)$ as a k-vector space.

A finite algebraic group G is ***infinitesimal*** if $|G| = e$. For example, α_{p^r} and μ_{p^r} are infinitesimal when $p = \mathrm{char}(k)$. A finite algebraic group is infinitesimal if and only if its augmentation ideal is nilpotent.

An algebraic group G over k is finite if and only if $G(K)$ is finite for all fields K containing k, and it is infinitesimal if and only if $G(K) = \{e\}$ for all fields containing k.

Recall that "algebraic group" is short for "algebraic group scheme". Thus "finite algebraic group" is short for "finite algebraic group scheme"; but finite implies algebraic, and so we usually abbreviate this to "finite group scheme".

b. Étale group schemes

2.15. An algebraic group over k is said to be ***étale*** if it is étale as a scheme over k (see A.60). Thus, the étale group schemes over k are the group varieties over k of dimension zero. A finite group scheme is étale if and only if it is smooth or, equivalently, its tangent space $\mathrm{Tgt}_e(G)$ at e is zero. The order of an étale group scheme G over k is the order of the abstract group $G(k^s)$.

2.16. Let $\Gamma = \mathrm{Gal}(k^s/k)$. A group in the category of finite discrete Γ-sets is a finite group together with a continuous action of Γ by group homomorphisms (i.e., for each $\gamma \in \Gamma$, the map $x \mapsto \gamma x$ is a group homomorphism). Now (A.62) implies the following statement.

> The functor $G \rightsquigarrow G(k^s)$ is an equivalence from the category of étale group schemes over k to the category of discrete finite groups endowed with a continuous action of Γ by group homomorphisms.

Let K be a subfield of k^s containing k. Then $G(K) = G(k^s)^{\mathrm{Gal}(k^s/K)}$ for any étale group scheme G over k.

2.17. A connected étale group scheme G is trivial (because the point e is both open and closed in G). A finite algebraic group that is both étale and infinitesimal is trivial. Thus a finite algebraic group G over k is trivial if and only if both $\mathrm{Tgt}_e(G)$ and $G(k^s)$ are trivial.

Examples

2.18. The finite constant algebraic groups over k are the étale algebraic groups G such that Γ acts trivially on $G(k^s)$.

2.19. Let X be a group of order 1 or 2. Then $\mathrm{Aut}(X) = 1$, and so there is exactly one étale group scheme of order 1 and one of order 2 over any field k (up to isomorphism).

2.20. Let A be a group of order 3. Such a group is cyclic and $\mathrm{Aut}(A) = \mathbb{Z}/2\mathbb{Z}$. Therefore the étale group schemes of order 3 over k correspond to homomorphisms $\Gamma \to \mathbb{Z}/2\mathbb{Z}$ factoring through $\mathrm{Gal}(K/k)$ for some finite Galois extension K of k. A separable quadratic extension K of k defines such a homomorphism, namely,

$$\sigma \mapsto \sigma|K : \Gamma \to \mathrm{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$$

and all nontrivial such homomorphisms $\Gamma \to \mathbb{Z}/2\mathbb{Z}$ arise in this way. Thus, up to isomorphism, there is exactly one nonconstant étale group scheme G^K of order 3 over k for each separable quadratic extension K of k. If G_0 is the constant étale group of order 3, then $G_0(k)$ has order 3. On the other hand, $G^K(k)$ has order 1 but $G^K(K)$ has order 3. There are infinitely many distinct quadratic extensions of $\mathbb{Q}$, for example, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, ... and hence infinitely many distinct étale group schemes of order 3. When $\mathrm{char}(k) \neq 3$, the finite group scheme μ_3 is the étale group scheme over $\mathbb{Q}$ attached to $\mathbb{Q}[\sqrt[3]{1}]$.

c. Anti-affine algebraic groups

Recall that an algebraic group G over k is anti-affine if $\mathcal{O}(G) = k$. Later we shall show that every anti-affine algebraic group is smooth (8.37).

The simplest anti-affine algebraic groups are the smooth cubic curves in $\mathbb{P}_k^2$. Such a curve is defined C by a homogeneous equation

$$\sum_{i+j+k=3} a_{ijk} X^i Y^j Z^k = 0$$

satisfying a smoothness condition. Fix a point $O \in C(k)$, assumed to exist. For $P, Q \in C(k)$, the line PQ through P and Q meets C in a third point $R \in C(k)$. Let $P + Q$ denote the third point of intersection of the line OR with C. There is regular map $m : C \times C \to C$ such that $m(P, Q) = P + Q$ for all $P, Q \in C(k)$. This makes C into an algebraic group, called an ***elliptic curve***.

Clearly, a complete connected group variety G is anti-affine. Such a group variety is called an ***abelian variety***. Abelian varieties are commutative and projective (8.45). The abelian varieties of dimension 1 are exactly the elliptic curves. When equipped with a polarization of fixed degree (roughly, a distinguished class of projective embeddings), the abelian varieties of dimension d form a family of dimension $d(d+1)/2$. Their study is an important part of mathematics, which we shall ignore here. See, for example, Milne 1986 or Mumford 1970.

Abelian varieties are not the only anti-affine algebraic groups. In nonzero characteristic, certain extensions of abelian varieties by tori are anti-affine, and in characteristic zero, certain extensions of abelian varieties by products of tori with vector groups are anti-affine. See Section 8i.

d.   Homomorphisms of algebraic groups

2.21. For an algebraic scheme X over k,

$$\operatorname{Hom}(X, \mathbb{G}_a) \simeq \operatorname{Hom}(k[T], \mathcal{O}_X(X)) \simeq \mathcal{O}_X(X)$$

(see A.13). Under the second isomorphism a homomorphism φ corresponds to $f = \varphi(T)$. Let G be an affine algebraic group. The morphism of schemes $G \to \mathbb{G}_a$ corresponding to an element f of $\mathcal{O}(G)$ is a homomorphism if and only if

$$\Delta_G(f) = f \otimes 1 + 1 \otimes f.$$

Using this, we can compute the endomorphisms of $\mathbb{G}_a$. In characteristic zero, they are the maps $t \mapsto ct$ for $c \in k$. In characteristic p, they are the maps

$$t \mapsto c_0 t + c_1 t^p + c_2 t^{p^2} + \cdots + c_n t^{p^n}, \quad n \in \mathbb{N}, \quad c_0, \ldots, c_n \in k.$$

See Example 14.40.

2.22. For an algebraic scheme X over k,

$$\operatorname{Hom}(X, \mathbb{G}_m) \simeq \operatorname{Hom}(k[T, T^{-1}], \mathcal{O}_X(X)) \simeq \mathcal{O}_X(X)^{\times}$$

(see A.13). Let G be an affine algebraic group. The morphism $G \to \mathbb{G}_m$ corresponding to $f \in \mathcal{O}(X)^{\times}$ is a homomorphism if and only if

$$\Delta_G(f) = f \otimes f.$$

The only such elements in $k[T, T^{-1}]$ are the powers T^n, $n \in \mathbb{Z}$, of T, and so the endomorphisms of $\mathbb{G}_m$ are the maps $t \mapsto t^n$. Thus $\operatorname{End}(\mathbb{G}_m) \simeq \mathbb{Z}$.

2.23. A homomorphism $\varphi \colon G \to H$ of connected group varieties is an ***isogeny*** if it is surjective (i.e., $|\varphi|$ is surjective) and its kernel is finite. The order of the kernel is called the ***degree*** of the isogeny. An isogeny is ***étale*** if its kernel is étale. This is equivalent to the map $(d\varphi)_e \colon \operatorname{Tgt}_e G \to \operatorname{Tgt}_e H$ on tangent spaces being an isomorphism (see 1.63).

The Frobenius homomorphism

2.24. Let k be a field of characteristic $p \neq 0$, and let f be the map $a \mapsto a^p$. For $g \in k[T_1, \ldots, T_n]$, we let $g^{(p)}$ denote the polynomial obtained by applying f to the coefficients of g. For a closed subscheme X of $\mathbb{A}^n$ defined by polynomials $g_1, g_2, \ldots$, we let $X^{(p)}$ denote the closed subscheme defined by the polynomials $g_1^{(p)}, g_2^{(p)}, \ldots$. Then

$$(a_1, \ldots, a_n) \mapsto (a_1^p, \ldots, a_n^p) \colon \mathbb{A}^n(k) \to \mathbb{A}^n(k)$$

maps $X(k)$ into $X^{(p)}(k)$. We want to realize this map of sets as a morphism of k-schemes $F_X \colon X \to X^{(p)}$.

Let $A = \mathcal{O}(X) = k[T_1, \ldots, T_n]/(g_1, g_2, \ldots)$. Then

$$A^{(p)} \stackrel{\text{def}}{=} \mathcal{O}(X^{(p)}) = \frac{k[T_1, \ldots, T_n]}{(g_1^{(p)}, g_2^{(p)}, \ldots)} = A \otimes_{k,f} k.$$

We define $F_X \colon X \to X^{(p)}$ to be Spm of the homomorphism of k-algebras

$$a \otimes c \mapsto ca^p \colon A \otimes_{k,f} k \to A.$$

It is the dotted arrow in the diagram at left.
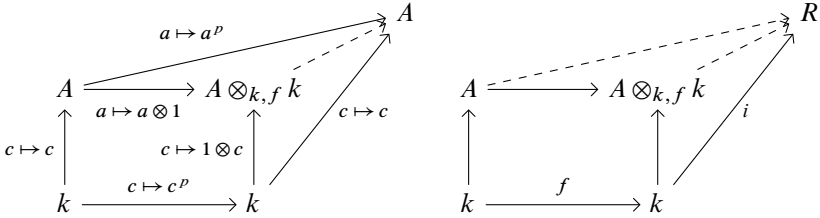
For a k-algebra $k \xrightarrow{i} R$, let $_f R$ denote the k-algebra $k \xrightarrow{f} k \xrightarrow{i} R$. There is a natural one-to-one correspondence

$$\operatorname{Hom}_{k\text{-algebra}}(A, {}_f R) \xleftrightarrow{\text{1:1}} \operatorname{Hom}_{k\text{-algebra}}(A^{(p)}, R)$$

(see the diagram at right), and so $X^{(p)}$ represents the functor $R \rightsquigarrow X(_f R)$. With this identification, $F_X \colon X(R) \to X(_f R)$ is induced by the k-algebra homomorphism $a \mapsto a^p \colon R \to {}_f R$.

We now define F_X more abstractly for any algebraic scheme X over k.

2.25. Let X be a scheme over a field k of characteristic p. The **absolute Frobenius morphism** $\sigma_X \colon X \to X$ acts as the identity map on $|X|$ and as the map

$$f \mapsto f^p \colon \mathcal{O}_X(U) \to \mathcal{O}_X(U)$$

on the sections of $\mathcal{O}_X$ over an open subset U of X. For all morphisms $\varphi \colon X \to Y$ of schemes over $\mathbb{F}_p$,

$$\sigma_Y \circ \varphi = \varphi \circ \sigma_X,$$

i.e., σ is an endomorphism of the identity functor.

2.26. For an algebraic scheme X over k, let $X \rightsquigarrow X^{(p)}$, $\varphi \rightsquigarrow \varphi^{(p)}$ denote base change with respect to $c \mapsto c^p \colon k \to k$. The **relative Frobenius morphism** $F_X \colon X \to X^{(p)}$ is defined by the diagram
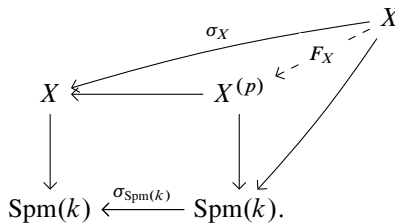
As in the affine case, $X^{(p)}$ represents the functor $R \rightsquigarrow X(_fR)$ and $F_X: X(R) \to X(_fR)$ is induced by the homomorphism $a \mapsto a^p: R \to {}_fR$. Similarly, we can define $F^n: X \to X^{(p^n)}$ by replacing p with p^n in the above discussion. It is the composite of the maps

$$X \xrightarrow{F} X^{(p)} \xrightarrow{F} \cdots \xrightarrow{F} X^{(p^n)}.$$

2.27. The assignment $X \mapsto F_X$ has the following properties.

(a) Functoriality: for all morphisms $\varphi: X \to Y$ of schemes over k, the following diagram commutes:

$$
\begin{array}{ccc}
X & \xrightarrow{\ \varphi\ } & Y \\
\downarrow{\scriptstyle F_X} & & \downarrow{\scriptstyle F_Y} \\
X^{(p)} & \xrightarrow{\ \varphi^{(p)}\ } & Y^{(p)}.
\end{array}
$$

(b) Compatibility with products: $F_{X \times Y}$ is the composite of $F_X \times F_Y$ with the canonical isomorphism $X^{(p)} \times Y^{(p)} \simeq (X \times Y)^{(p)}$.

(c) Base change: the formation of F_X commutes with extension of the base field.

2.28. Now let G be an algebraic group over k. Then $R \rightsquigarrow G(_fR)$ is a functor to groups, and so $G^{(p)}$ is an algebraic group; moreover, $F_G(R): G(R) \to G^{(p)}(R)$ is a homomorphism of groups for all R, and so F_G is a homomorphism of algebraic groups. This can also be deduced directly from the properties (a) and (b), which give a commutative diagram:

$$
\begin{array}{ccc}
G \times G & \xrightarrow{\ m\ } & G \\
\downarrow{\scriptstyle F_{G \times G}} & & \downarrow{\scriptstyle F_G} \\
G^{(p)} \times G^{(p)} & \xrightarrow{\ m^{(p)}\ } & G^{(p)}.
\end{array}
$$

The kernel of F_G^n is a characteristic subgroup of G: if R is a k-algebra and α is an automorphism of G_R, then (by functoriality) there is a commutative diagram

$$
\begin{array}{ccccc}
\mathrm{Ker}(F^n) & \longrightarrow & G_R & \xrightarrow{\ F^n\ } & (G^{(p^n)})_R \\
\vdots\downarrow & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^{(p^n)}} \\
\mathrm{Ker}(F^n) & \longrightarrow & G_R & \xrightarrow{\ F^n\ } & (G^{(p^n)})_R.
\end{array}
$$

If $F_G^n = 0$, then the algebraic group G is said to have **height** $\leq n$.

PROPOSITION 2.29. *If G is smooth and connected, then $G^{(p)}$ is smooth and connected, and the Frobenius map $F_G: G \to G^{(p)}$ is an isogeny of degree $p^{\dim(G)}$ (in particular, it is faithfully flat).*

PROOF. Because of 2.27(c), we may suppose that k is algebraically closed. Then $f: k \to k$ is an isomorphism, and so $G^{(p)}$ is isomorphic to G as a scheme. Therefore it is smooth (resp. connected) if G is smooth (resp. connected). Assume now that G is smooth and connected. The map F_G is obviously dominant, and so it is surjective and faithfully flat (1.71). □

e. Products

2.30. Let $G_1, \ldots, G_n$ be algebraic groups over k. Then $G_1 \times \cdots \times G_n$ is an algebraic group, called the ***product*** of the G_i. It represents the functor

$$R \rightsquigarrow G_1(R) \times \cdots \times G_n(R).$$

When the G_i are affine, $G_1 \times \cdots \times G_n$ is affine, and

$$\mathcal{O}(G_1 \times \cdots \times G_n) \simeq \mathcal{O}(G_1) \otimes \cdots \otimes \mathcal{O}(G_n).$$

2.31. An algebraic group G is the ***almost-direct product*** of its algebraic subgroups $G_1, \ldots, G_n$ if the multiplication map $G_1 \times \cdots \times G_n \to G$ is a faithfully flat homomorphism with finite kernel. This means that the subgroups G_i commute in pairs, that $G_1 \cdots \cdots G_n = G$, and that $G_1 \cap \cdots \cap G_n$ is finite. If G is an almost-direct product of its subgroups G_i, then there is an exact sequence

$$e \to G_1 \cap \cdots \cap G_n \to G_1 \times \cdots \times G_n \to G \to e.$$

An almost-direct product need not be a direct product. For example, the cokernel of $x \mapsto (x, x^{-1}): \mu_2 \to \mathrm{SL}_2 \times \mathrm{SL}_2$ is not a direct product.

2.32. Suppose we have homomorphisms $G_1 \to H \leftarrow G_2$ of algebraic groups. Then $G_1 \times_H G_2$ is an algebraic group, called the ***fibred product*** of G_1 and G_2 over H. It represents the functor

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

When G_1, G_2, and H are affine, $G_1 \times_H G_2$ is affine, and

$$\mathcal{O}(G_1 \times_H G_2) \simeq \mathcal{O}(G_1) \otimes_{\mathcal{O}(H)} \mathcal{O}(G_2).$$

Directly from the definition, one sees that the formation of fibred products of algebraic groups commutes with extension of the base field:

$$(G_1 \times_H G_2)_{k'} \simeq G_{1k'} \times_{H_{k'}} G_{2k'}.$$

If G_1 and G_2 are algebraic subgroups of an algebraic group H, then $G_1 \times_H G_2$ equals their intersection $G_1 \cap G_2$ in H. Note that $G_1 \times_H G_2$ need not be smooth even when all three groups are smooth (1.50).

f.   Semidirect products

DEFINITION 2.33. An algebraic group G is said to be a ***semidirect product*** of its algebraic subgroups N and Q, denoted $G = N \rtimes Q$, if N is normal in G and the map $(n,q) \mapsto nq \colon N(R) \times Q(R) \to G(R)$ is a bijection of sets for all k-algebras R.

In other words, G is a semidirect product of N and Q if $G(R)$ is a semidirect product of its subgroups $N(R)$ and $Q(R)$ for all k-algebras R. For example, the algebraic group of upper triangular $n \times n$ matrices $\mathbb{T}_n$ is the semidirect product, $\mathbb{T}_n = \mathbb{U}_n \rtimes \mathbb{D}_n$, of its subgroups $\mathbb{U}_n$ and $\mathbb{D}_n$.

PROPOSITION 2.34. *An algebraic group G is the semidirect product of subgroups N and Q if and only if there exists a homomorphism $G \to Q'$ whose restriction to Q is an isomorphism and whose kernel is N.*

PROOF. $\Rightarrow$: By assumption, the multiplication map is a bijection of functors $N \times Q \to G$. The composite of the inverse of this map with the projection $N \times Q \to Q$ has the required properties.

$\Leftarrow$: Let $\varphi \colon G \to Q'$ be the given homomorphism. Then N is certainly normal, and for every k-algebra R, $\varphi(R)$ realizes $G(R)$ as a semidirect product $G(R) = N(R) \rtimes Q(R)$ of its subgroups $N(R)$ and $Q(R)$. □

Let N and Q be algebraic groups, and suppose that there is given an action of Q on N

$$(q,n) \mapsto \theta_R(q,n) \colon Q(R) \times N(R) \to N(R)$$

such that, for every q, the map $n \mapsto \theta_R(q,n)$ is a group homomorphism. Then the functor

$$R \rightsquigarrow N(R) \rtimes_{\theta_R} Q(R) \colon \mathsf{Alg}_k^0 \to \mathsf{Grp}$$

is an algebraic group because its underlying functor to sets is $N \times Q$. We denote this algebraic group by $N \rtimes_\theta Q$, and call it the ***semidirect product of N and Q defined by*** θ. For $n,n' \in N(R)$ and $q,q' \in Q(R)$, we have

$$(n,q) \cdot (n',q') = (n \cdot \theta(q)n', qq').$$

The identity element is (e_N, e_Q) and $(n,q)^{-1} = (\theta(q^{-1})n^{-1}, q^{-1})$. Note that

$$(n,e) \cdot (e,q) \cdot (n,e)^{-1} = (n \cdot \theta(q)n^{-1}, q),$$

and so Q is normal in G if and only if the action of Q on N is trivial.

EXAMPLE 2.35. We give examples of an algebraic group G over a field k of characteristic p such that G_{red} is a nonnormal algebraic subgroup of G.

(a) The action $(u,a) \mapsto ua \colon \mathbb{G}_m \times \mathbb{G}_a \to \mathbb{G}_a$ of $\mathbb{G}_m$ on $\mathbb{G}_a$ stabilizes α_{p^n}, and so we can form the semidirect product $G = \alpha_{p^n} \rtimes \mathbb{G}_m$. Then $G_{\mathrm{red}} = \mathbb{G}_m$, which is not normal because the action of $\mathbb{G}_m$ on α_{p^n} is not trivial.

(b) Let $F = \mathbb{Z}/(p-1)\mathbb{Z}$, and let $G = \mu_p \rtimes F_k$ with F_k acting on μ_p by $(n,\zeta) \mapsto \zeta^n$. Then $G_{\mathrm{red}} = F_k$, which is not normal in G because its action on μ_p is not trivial.

EXAMPLE 2.36. Let char$(k) = p$. In contrast to abstract groups, a finite algebraic group of order p may act nontrivially on another group of order p, and so there are noncommutative finite algebraic groups of order p^2. For example, there is an action of μ_p on α_p,

$$(u,t) \mapsto ut : \mu_p(R) \times \alpha_p(R) \to \alpha_p(R),$$

and the corresponding semidirect product $G = \alpha_p \rtimes \mu_p$ is a noncommutative finite connected algebraic group of order p^2. We have $\mathcal{O}(G) = k[t,s]$ with

$$t^p = 1, \quad s^p = 0, \quad \Delta(t) = t \otimes t, \quad \Delta(s) = t \otimes s + s \otimes 1;$$

the normal subgroup scheme α_p corresponds to the quotient of $\mathcal{O}(G)$ obtained by putting $t = 1$, and the subgroup scheme μ_p corresponds to the quotient with $s = 0$ (Tate and Oort 1970, p. 6).

g. The group of connected components

Let G be an algebraic group over k. Because G° is a normal subgroup of G, the set $\pi_0(G_{k^s})$ of connected components of G_{k^s} has a (unique) group structure for which the map $G(k^s) \to \pi_0(G_{k^s})$ is a homomorphism. This group structure is respected by the action of $\mathrm{Gal}(k^s/k)$, and so it arises from an étale group $\pi_0(X)$ over k (see A.62). In this way, we get a homomorphism $\varphi : G \to \pi_0(G)$ of algebraic groups over k which, on k^s-points, becomes $G(k^s) \to \pi_0(G_{k^s})$. This is the homomorphism corresponding to the inclusion $\pi(X) \hookrightarrow \mathcal{O}(X)$ (see 1.29).

PROPOSITION 2.37. *Let G be an algebraic group over k.*

(a) *The homomorphism $G \to \pi_0(G)$ is universal among homomorphisms from G to an étale algebraic group.*

(b) *The kernel of the homomorphism in (a) is G°; there is an exact sequence*

$$e \to G^\circ \to G \xrightarrow{\varphi} \pi_0(G) \to e.$$

(c) *The formation of the exact sequence in (b) commutes with extension of the base field. In particular, for a field k' containing k,*

$$\pi_0(G_{k'}) \simeq \pi_0(G)_{k'}$$
$$(G_{k'})^\circ \simeq (G^\circ)_{k'}.$$

(d) *The fibres of $|G| \to |\pi_0(G)|$ are the connected components of $|G|$. The order of the finite algebraic group $\pi_0(G)$ is the number of connected components of G_{k^s} (and also of G_{k^a}).*

(e) *For algebraic groups G and G',*

$$\pi_0(G \times G') \simeq \pi_0(G) \times \pi_0(G')$$
$$(G \times G')^\circ \simeq G^\circ \times G'^\circ.$$

PROOF. (a) For an algebraic scheme X over k, the map $X \to \pi_0(X)$ is universal among regular maps from X to an étale scheme (p. 15).

(b) Certainly G° is the fibre of φ over e, and we noted in 1.33 that φ is faithfully flat.

(c) Already noted in Propositions 1.30 and 1.34.

(d) Obvious from the definitions.

(e) Apply (b) of Proposition 1.30.   □

DEFINITION 2.38. Let G be an algebraic group over a field k. The quotient $G \to \pi_0(G)$ of G is the ***component group*** or ***group of connected components*** of G.

REMARK 2.39. (a) An algebraic group G is connected if and only if $\pi_0(G) = e$, i.e., G has no nontrivial étale quotient.

(b) Every homomorphism from a connected algebraic group to G factors through $G^\circ \to G$ (because its composite with $G \to \pi_0(G)$ is trivial).

(c) The set $|\pi_0(G)|$ can be identified with the set of $\mathrm{Gal}(k^s/k)$-orbits in the group $\pi_0(G)(k^s)$.

Examples

2.40. The groups $\mathbb{G}_a$, $\mathbb{G}_m$, GL_n, $\mathbb{T}_n$, $\mathbb{U}_n$, $\mathbb{D}_n$ (see 2.1, 2.2, 2.8, 2.9) are connected. For this it suffices to prove that $\mathcal{O}(G)$ is an integral domain (1.36), but this is obvious in each case. For example, $\mathcal{O}(\mathbb{T}_n)$ is the quotient of $\mathcal{O}(\mathrm{GL}_n)$ by the ideal generated by the symbols T_{ij}, $i > j$, which is isomorphic to the polynomial ring in the symbols T_{ij}, $1 \le i \le j \le n$, with the product $T_{11}T_{22}\cdots T_{nn}$ inverted.

2.41. A ***monomial matrix*** over R is an element of $\mathrm{GL}_n(R)$ with exactly one nonzero element in each row and each column. Let G denote the functor sending R to the group of monomial matrices over R. Let $I(\sigma)$ denote the permutation matrix obtained by applying a permutation $\sigma \in S_n$ to the rows of the identity $n \times n$ matrix. The matrices $I(\sigma)$ form a constant algebraic subgroup $(S_n)_k$ of GL_n, and $G = \mathbb{D}_n \cdot (S_n)_k$. For a diagonal matrix $\mathrm{diag}(a_1,\ldots,a_n)$,

$$I(\sigma) \cdot \mathrm{diag}(a_1,\ldots,a_n) \cdot I(\sigma)^{-1} = \mathrm{diag}(a_{\sigma(1)},\ldots,a_{\sigma(n)}), \qquad (9)$$

and so $\mathbb{D}_n$ is normal in G. Clearly $\mathbb{D} \cap (S_n)_k = e$, and so G is the semidirect product

$$G = \mathbb{D}_n \rtimes_\theta (S_n)_k$$

where $\theta\colon S_n \to \mathrm{Aut}(\mathbb{D}_n)$ sends σ to the automorphism in (9). In particular, G is an algebraic subgroup of GL_n. We have $\pi_0(G) = (S_n)_k$ and $G^\circ = \mathbb{D}_n$. An element of $G(R)$ permutes the set of lines Re_i in R^n, and the map $G \to \pi_0(G)$ sends the element to this permutation.

2.42. The group SL_n is connected. The natural isomorphism of set-valued functors

$$(A, r) \mapsto A \cdot \mathrm{diag}(r, 1, \ldots, 1): SL_n(R) \times \mathbb{G}_m(R) \to GL_n(R)$$

defines an isomorphism of k-algebras

$$\mathcal{O}(GL_n) \simeq \mathcal{O}(SL_n) \otimes \mathcal{O}(\mathbb{G}_m),$$

and the algebra on the right contains $\mathcal{O}(SL_n)$. In particular, $\mathcal{O}(SL_n)$ is a subring of $\mathcal{O}(GL_n)$, and so it is an integral domain.

2.43. A **quadratic space** over k is a pair (V, q) consisting of a finite-dimensional vector space over k and a quadratic form on V. Assume that $\mathrm{char}(k) \neq 2$. We define $SO(q)$ to be $SO(\phi_q)$, where ϕ_q is the associated bilinear form: $\phi_q(x, y) = q(x + y) - q(x) - q(y)$. For every nondegenerate quadratic space (V, q), the algebraic group $SO(q)$ is connected. It suffices to prove this after replacing k with k^a, and so we may suppose that q is the diagonal form $X_1^2 + \cdots + X_n^2$, in which case the group is shown to be connected in Exercise 2-9 below.

The determinant defines a quotient map $O(q) \to \{\pm 1\}$ with kernel $SO(q)$. Therefore $O(q)^\circ = SO(q)$ and $\pi_0(O(q)) = \{\pm 1\}$ (constant algebraic group).

2.44. The symplectic group Sp_{2n} is connected (for some hints on how to prove this, see Springer 1998, 2.2.9).

ASIDE 2.45. (a) An algebraic group G over $\mathbb{C}$ is connected for the Zariski topology if and only if $G(\mathbb{C})$ is connected for the complex topology – this is true of any algebraic variety. We could deduce that GL_n over $\mathbb{C}$ is a connected algebraic group from knowing that $GL_n(\mathbb{C})$ is connected for the complex topology. However, it is easier to deduce that $GL_n(\mathbb{C})$ is connected from knowing that GL_n is connected.

(b) An algebraic group G over $\mathbb{R}$ may be connected without $G(\mathbb{R})$ being connected for the real topology, and conversely. For example, GL_2 is connected as an algebraic group, but $GL_2(\mathbb{R})$ is not connected, whereas μ_3 is not connected as an algebraic group, but $\mu_3(\mathbb{R}) = \{1\}$ is connected. Worse, the identity component of $GL_2(\mathbb{R})$ is a Lie group that is not of the form $G(\mathbb{R})$ for any algebraic group over $\mathbb{R}$ (a similar statement applies to the semisimple group PGL_2).

h. The algebraic subgroup generated by a map

Let $\varphi: X \to G$ be a regular map from an algebraic scheme X to an algebraic group G. Under some hypotheses on φ we prove that, among the algebraic subgroups of G through which φ factors, there is a smallest one. Such an algebraic subgroup is said to be **generated by** φ (or X) and is denoted by $\langle X, \varphi \rangle$.

Affine case

Let $\varphi: X \to G$ be a regular map over k from an affine algebraic scheme X to an affine algebraic group G, and assume that there exists an $o \in X(k)$ such that $\varphi(o) = e$. Let I_n denote the kernel of the homomorphism $\mathcal{O}(G) \to \mathcal{O}(X^n)$ of k-algebras defined by the regular map

$$(x_1, \ldots, x_n) \mapsto \varphi(x_1) \cdots \varphi(x_n): X^n \to G.$$

The regular maps

$$X \to X^2 \to \cdots \to X^n \to \cdots \to G,$$
$$(x) \mapsto (x, o) \mapsto \cdots$$

give inclusions

$$I_1 \supset I_2 \supset \cdots \supset I_n \supset \cdots,$$

and we let $I = \bigcap I_n$.

PROPOSITION 2.46. *There exists a smallest algebraic subgroup H of G such that $\varphi: X \to G$ factors through H. If $\varphi(X(R))$ is closed under $g \mapsto g^{-1}$ for all small k-algebras R, then H is the subscheme of G defined by I.*

PROOF. From the diagram of algebraic schemes

$$
\begin{array}{ccc}
X^n \ \times \ X^n & \longrightarrow & X^{2n} \\
\downarrow \quad\quad \downarrow & & \downarrow \\
G \ \times \ G & \xrightarrow{\ \text{mult}\ } & G,
\end{array}
$$

we get a diagram of k-algebras

$$
\begin{array}{ccc}
\mathcal{O}(X^n) \ \otimes \ \mathcal{O}(X^n) & \longleftarrow & \mathcal{O}(X^{2n}) \\
\uparrow \quad\quad \uparrow & & \uparrow \\
\mathcal{O}(G) \ \otimes \ \mathcal{O}(G) & \xleftarrow{\ \Delta\ } & \mathcal{O}(G).
\end{array}
$$

The homomorphism $\mathcal{O}(G) \to \mathcal{O}(X^n)$ factors through $\mathcal{O}(G)/I_n$, and so the diagram shows that

$$\Delta: \mathcal{O}(G) \to \mathcal{O}(G)/I_n \otimes \mathcal{O}(G)/I_n$$

factors through $\mathcal{O}(G) \to \mathcal{O}(G)/I_{2n}$. It follows that

$$\Delta: \mathcal{O}(G) \to \mathcal{O}(G)/I \otimes \mathcal{O}(G)/I$$

factors through $\mathcal{O}(G) \to \mathcal{O}(G)/I$ and defines a multiplication map $m_H: H \times H \to H$. The triple (H, m_H, e) is the smallest algebraic submonoid of G such

that $H(R)$ contains $\varphi(X(R))$ for all k-algebras R, i.e., it is the smallest algebraic submonoid through which φ factors.

If $\varphi(X(R))$ is closed under $g \mapsto g^{-1}$ for all small R, then φ factors through $\mathrm{inv}(H)$, which then has the same property as H. Therefore $H = \mathrm{inv}(H)$, and H is an algebraic subgroup of G.

When $\varphi(X)$ is not closed under inversion, we define H to be the smallest algebraic submonoid through which $\varphi \sqcup \mathrm{inv} \circ \varphi \colon X \sqcup X \to G$ factors. $\qquad \square$

PROPOSITION 2.47. *Let k' be a field containing k. Then $\langle X, \varphi \rangle_{k'} = \langle X_{k'}, \varphi_{k'} \rangle$.*

PROOF. The formation of I commutes with extension of the base field. $\qquad \square$

PROPOSITION 2.48. *If X is geometrically connected (resp. geometrically reduced), then $\langle X, \varphi \rangle$ is geometrically connected (resp. geometrically reduced).*

PROOF. We may suppose that k is algebraically closed. Recall (CA 14.2) that an an affine scheme X is connected if and only if $\mathcal{O}(X)$ has no nontrivial idempotent. Assume that X is connected. If $\mathcal{O}(G)/I$ had a nontrivial idempotent, then so would $\mathcal{O}(G)/I_n$ for some n, but (by definition) the homomorphism of k-algebras $\mathcal{O}(G)/I_n \to \mathcal{O}(X^n)$ is injective. As X is connected and k is algebraically closed, X^n is connected, and so this is a contradiction. The proof for "reduced" is similar. $\qquad \square$

Geometrically reduced case

We begin by reviewing some algebraic geometry.

DEFINITION 2.49. A morphism $\varphi \colon Y \to X$ of algebraic schemes over the field k is **schematically dominant** if the map $\mathcal{O}_X \to \varphi_* \mathcal{O}_Y$ is injective. Similarly, a family $\varphi_i \colon Y_i \to S$, $i \in I$, is **schematically dominant** if the family of maps $\mathcal{O}_X \to \varphi_* \mathcal{O}_{Y_i}$ is injective.

For example, a subset S of $X(k)$ is schematically dense in X if and only if the family of maps $s \to X$, $s \in S$, is schematically dominant (1.10).

The proofs of 1.10–1.13 extend without difficulty to give the following statements. If the family of maps $\varphi_i \colon Y_i \to X$, $i \in I$, is schematically dominant, then $\bigcup_i \varphi_i(|Y_i|)$ is dense in $|X|$; conversely if this union is dense in $|X|$ and X is reduced, then the family $(\varphi_i)_{i \in I}$ is schematically dominant. A schematically dominant family of regular maps remains schematically dominant under extension of the base field. If the family $\varphi_i \colon Y_i \to X$ is schematically dominant, and the Y_i are geometrically reduced, then so also is X.

PROPOSITION 2.50. *Let $\varphi \colon X \to G$ be a regular map over k from an algebraic scheme to an algebraic group, and let φ^n denote the map*

$$(x_1, \ldots, x_n) \mapsto \varphi(x_1) \cdots \varphi(x_n) \colon X^n \to G.$$

If X is geometrically reduced, then there exists a smallest algebraic subgroup H such that φ factors through H, and H is smooth. If, in addition, $\mathrm{inv}(\varphi(X)) \subset \varphi(X)$, then H is the reduced algebraic subscheme of G with underlying set the closure of $\bigcup_n \mathrm{Im}(\varphi^n)$.

PROOF. As for Proposition 2.46, it suffices to prove the second statement. Because X is geometrically reduced, so also is X^n (see A.43). The map $\varphi^n : X^n \to H$ is schematically dominant for n large because it is dominant and H is reduced. It follows that H is geometrically reduced and that its formation commutes with extension of the base field. Therefore, in proving that H is an algebraic subgroup of G, we may suppose that k is algebraically closed. Let Z be the closure of $m(H \times H)$ in G. The intersection of $m^{-1}(Z \smallsetminus H)$ with $H \times H$ is an open subset of $H \times H$, which is nonempty if $m(H \times H)$ is not contained in H. In that case, there exist $x_1, \ldots, x_n, y_1, \ldots, y_n \in X(k)$ such that

$$(\varphi(x_1)\cdots\varphi(x_n), \varphi(y_1)\cdots\varphi(y_n)) \in m^{-1}(Z \smallsetminus H)$$

because $\mathrm{Im}(\varphi^n) \times \mathrm{Im}(\varphi^n)$ is constructible and therefore contains an open subset of its closure (A.15). But this is absurd, because

$$m(\varphi(x_1)\cdots\varphi(x_n), \varphi(y_1)\cdots\varphi(y_n)) = \varphi(x_1)\cdots\varphi(x_n)\varphi(y_1)\cdots\varphi(y_n) \in H(k).$$

The condition $\mathrm{inv}(\varphi(X)) \subset \varphi(X)$ implies that inv maps H into H, and so H is an algebraic subgroup of G. It is smooth because it is geometrically reduced. □

PROPOSITION 2.51. *Let $(\varphi_i : X_i \to G)_{i \in I}$ be a family of regular maps from geometrically reduced algebraic schemes X_i over k to an algebraic group G. There exists a smallest algebraic group H of G such that all φ_i factor through H. Moreover, H is smooth.*

PROOF. When I is finite, we take H to be the algebraic subgroup generated by the map $\bigsqcup_{i \in I} X_i \to G$. When I is infinite, $\bigsqcup X_i$ may not be algebraic k, but Proposition 2.50 holds without that assumption (SGA 3, VI$_B$, §7). Alternatively, rewrite the previous proof for families. □

As before, the formation of the algebraic subgroup generated by a map (or family of maps) commutes with extension of the base field.

EXAMPLE 2.52. Let G be an algebraic group over k, and let S be a closed subgroup of $G(k)$. The algebraic subgroup H of G generated by the family of maps $s \to G$, $s \in S$, is the unique reduced algebraic subgroup of G such that $S = H(k)$ (see 1.45).

PROPOSITION 2.53. *Let $\varphi : X \to G$ be a regular map from a geometrically reduced scheme X over k to an algebraic group G. If X is geometrically connected and $\varphi(X)$ contains e, then the algebraic subgroup of G generated by φ is connected.*

PROOF. We may suppose that k is algebraically closed. Let φ' be the map $\varphi \sqcup \mathrm{inv} \circ \varphi : X \sqcup X \to G$. The hypothesis implies that $\bigcup \mathrm{Im}(\varphi'^n)$ is connected, and so its closure H is connected. □

i. Restriction of scalars

In this section, A is a finite k-algebra and all algebraic groups are assumed to be quasi-projective (in fact, this is automatically true; B.38).

2.54. Let X be a quasi-projective scheme over A. The Weil restriction of X to k is an algebraic scheme $X_{A/k}$ over k such that

$$X_{A/k}(R) = X(A \otimes R)$$

for all k-algebras R. In other words, $X_{A/k}$ represents the functor

$$R \rightsquigarrow X(A \otimes R) : \mathsf{Alg}_k \to \mathsf{Set}.$$

It is easy to prove that $\mathbb{A}^n_{A/k}$ and $\mathbb{P}^n_{A/k}$ exist, and then the existence of $X_{A/k}$ for X a closed subscheme X of $\mathbb{A}^n$ or $\mathbb{P}^n$ follows from Proposition 1.103.

2.55. Let G be an algebraic group over A. The functor $(G)_{A/k}$,

$$R \rightsquigarrow G(A \otimes R) : \mathsf{Alg}^0_k \to \mathsf{Set},$$

takes values in the category of groups, and so it is an algebraic group. Thus $(G)_{A/k}$ is the algebraic group over k such that

$$(G)_{A/k}(R) = G(A \otimes R) \quad \text{for all } k\text{-algebras } R.$$

We say that $(G)_{A/k}$ has been obtained from G by **(Weil) restriction of scalars** (or by **restriction of the base ring**), and call it the **Weil restriction** of G. The functor $G \rightsquigarrow (G)_{A/k}$ is denoted by $\Pi_{A/k}$.[2]

2.56. Let G be an algebraic group over k. For a k-algebra R, the k-algebra homomorphism $r \mapsto 1 \otimes r : R \to A \otimes R$ defines a homomorphism of groups

$$G(R) \to G(A \otimes R) \overset{\text{def}}{=} (\Pi_{A/k} G_A)(R).$$

This homomorphism is natural in R, and so it arises from a homomorphism

$$i_G : G \to \Pi_{A/k} G_A$$

of algebraic k-groups. The homomorphism i_G has the following universal property:

for every group H over A and homomorphism $\alpha : G \to (H)_{A/k}$, there exists a unique homomorphism $\beta : G_A \to H$ such that $(\beta)_{A/k} \circ i_G = \alpha$.

$$
\begin{array}{ccc}
G \xrightarrow{\ i_G\ } (G_A)_{A/k} & \quad & G_A \\
{\scriptstyle \alpha}\searrow \quad \Big\downarrow {\scriptstyle (\beta)_{A/k}} & & \exists !\Big\downarrow {\scriptstyle \beta} \\
(H)_{A/k} & & H
\end{array}
$$

---

[2] Other common notations: $R_{A/k}$ and $\mathrm{Res}_{A/k}$.

Indeed, for an A-algebra R, $\beta(R)$ must be the composite of the maps

$$G_A(R) \stackrel{\text{def}}{=} G(R_0) \xrightarrow{\alpha(R_0)} H(k' \otimes_k R_0) \xrightarrow{\gamma} H(R)$$

where R_0 denotes R regarded as a k-algebra, and γ is induced by the homomorphism of A-algebras $c \otimes r \mapsto cr \colon A \otimes_k R_0 \to R$.

2.57. According to 2.56, for every algebraic group G over k and algebraic group H over A,

$$\operatorname{Hom}(G, \Pi_{A/k} H) \simeq \operatorname{Hom}(G_A, H).$$

In other words, $\Pi_{A/k}$ is right adjoint to the functor "change of base ring $k \to A$". Being a right adjoint, $\Pi_{A/k}$ preserves inverse limits (Mac Lane 1971, V, §5). In particular, it takes products to products, fibred products to fibred products, equalizers to equalizers, and kernels to kernels. This can also be deduced directly from the definition of $\Pi_{A/k}$.

2.58. For any sequence of finite homomorphisms $k \to k' \to A$ with k' a field,

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

Indeed, for an algebraic group G over A and k-algebra R,

$$(\Pi_{k'/k}(\Pi_{A/k'}(G)))(R) = (\Pi_{A/k'}G)(k' \otimes_k R) = G(A \otimes_{k'} k' \otimes_k R)$$
$$\simeq G(A \otimes_k R) = \left(\Pi_{A/k}G\right)(R)$$

because $A \otimes_{k'} k' \otimes_k R \simeq A \otimes_k R$. Alternatively, observe that $\Pi_{k'/k} \circ \Pi_{A/k'}$ is right adjoint to $H \rightsquigarrow H_A$.

2.59. For any field K containing k and algebraic group G over A,

$$\left(\Pi_{A/k}G\right)_K \simeq \Pi_{A \otimes_k K/K}(G_K); \tag{10}$$

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

$$\left(\Pi_{A/k}G\right)_K(R) = \left(\Pi_{A/k}G\right)(R) = G(A \otimes_k R)$$
$$\simeq G(A \otimes_k K \otimes_K R) = \Pi_{A \otimes_k K/K}(G_K)(R)$$

because $A \otimes_k R \simeq A \otimes_k K \otimes_K R$.

2.60. Let A be a product of finite k-algebras, $A = k_1 \times \cdots \times k_n$. To give an algebraic group G over A is the same as giving an algebraic group G_i over each k_i. In this case,

$$(G)_{A/k} \simeq (G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k}. \tag{11}$$

Indeed, for a k-algebra R,

$$(G)_{A/k}(R) = G(A \otimes R) = G_1(k_1 \otimes R) \times \cdots \times G_n(k_n \otimes R)$$
$$= (G_1)_{k_1/k}(R) \times \cdots \times (G_n)_{k_n/k}(R)$$
$$= \left((G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k}\right)(R).$$

2.61. Let A be an étale k-algebra and K a subfield of k^s containing all k-conjugates of A. Then

$$\left(\Pi_{A/k}G\right)_K \simeq \prod_{\sigma:A\to K}\sigma G$$

where σG is obtained from G by extension of scalars by the k-homomorphism $\sigma:A\to K$. Indeed

$$\left(\Pi_{A/k}G\right)_K \overset{(10)}{\simeq} \Pi_{A\otimes K/K}G_K \overset{(11)}{\simeq} \prod_{\sigma:A\to K}G_\sigma$$

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

2.62. Let A and K be as in 2.61, and assume that K is Galois over k with Galois group Γ. There is a functor

$$G\rightsquigarrow G\times_k K=\prod_{\sigma:A\to K}G_\sigma$$

sending an algebraic group over A to an algebraic group over K equipped with an action of Γ. Statement 2.61 says that this factors into
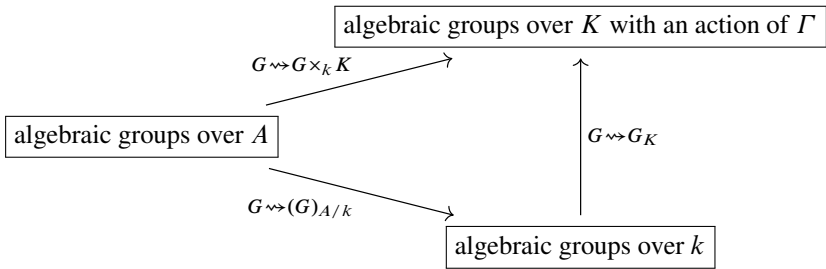
2.63. Let $A=k[\varepsilon]$, where $\varepsilon^2=0$, and let G be an algebraic group over k. For each $P\in G(k)$, the fibre of $G(k[\varepsilon])\to G(k)$ over P is (by definition) the tangent space to G at P. There is an exact sequence

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

where V is the tangent space to G at e.

2.64. We saw in 2.61 that, if k' is separable over k, then $(G)_{k'/k}$ becomes isomorphic to a product of conjugates of G over some field containing k'. This is far from being true when k'/k is a purely inseparable field extension. For example, let k be a nonperfect field of characteristic 2 and let $k'=k[\sqrt{a}]$, where $a\in k\smallsetminus k^2$. Then

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

For an algebraic group G over k,

$$\left(\Pi_{k'/k}G_{k'}\right)_{k'} \overset{2.59}{\simeq} \Pi_{k'\otimes k'/k'}G_{k'\otimes k'}\simeq \Pi_{k'[\varepsilon]/k'}G_{k'[\varepsilon]},$$

which is an extension of $G_{k'}$ by a vector group (2.63).

2.65. If G is smooth, then so is $(G)_{A/k}$ (apply the criterion A.56).

NOTES. The original reference for this section is the notes of Weil's 1959–1960 lectures, published as Weil 1982. For a modern treatment, see Bosch et al. 1990, 7.6.

j. Torsors

Let R_0 be a k-algebra and G an algebraic group over R_0. Let $S_0 = \mathrm{Spm}(R_0)$.

DEFINITION 2.66. A right G-*torsor* over S_0 is a scheme S faithfully flat over S_0 together with an action $S \times_{S_0} G \to S$ of G on S such that the map

$$(s, g) \mapsto (s, sg) \colon S \times_{S_0} G \to S \times_{S_0} S$$

is an isomorphism of S_0-schemes. We also refer to a G-torsor over S_0 as a *torsor under G over S_0*.

If S is a torsor under G over S_0 and R is an R_0-algebra, then either $S(R)$ is empty or it is a principal homogeneous space for $G(R)$. If $S(R_0)$ is nonempty, then S is said to be *trivial*; the choice of an $s \in S(R_0)$ determines an isomorphism $g \mapsto sg \colon S \to G$.

EXAMPLE 2.67. Let G be an algebraic group over k. To give a torsor under G_{S_0} over S_0 amounts to giving a scheme S faithfully flat over S_0 together with an action $S \times G \to S$ of G on S such that $(s, g) \mapsto (s, sg) \colon S \times G \to S \times_{S_0} S$ is an isomorphism (because $S \times_{S_0} (S_0 \times G) \simeq S \times G$).

EXAMPLE 2.68. Let $G \to Q$ be a faithfully flat homomorphism of algebraic groups with kernel N. The action $G \times_Q N \to G$ of N on G induces an isomorphism $G \times_Q G \simeq G \times N$ (Exercise 2-1), and so G is a torsor under N over Q.

PROPOSITION 2.69. *Let $S \to S_0$ be a G-torsor over S_0. If G is affine (resp. smooth, resp. ...) over S_0, then the morphism $S \to S_0$ is affine (resp. smooth, resp. ...).*

PROOF. Consider the diagram

$$
\begin{array}{ccccc}
S & \longleftarrow & S \times_{S_0} S & \xleftarrow{\;\simeq\;} & S \times_{S_0} G \\
\downarrow & & \downarrow & & \downarrow \\
S_0 & \longleftarrow & S & =\!=\!=\!= & S
\end{array}
$$

If the map $G \to S_0$ is affine, then $S \times_{S_0} G \to S$ is affine, which implies that $S \times_{S_0} S \to S$ is affine. This last map comes by a faithfully flat base change from the map $S \to S_0$, and so it also is affine (by descent A.80).   □

COROLLARY 2.70. *Let*

$$e \to N \to G \to Q \to e,$$

be an exact sequence of algebraic groups over k. If N and Q are affine, then so also is G.

PROOF. From 2.68 we see that G is a torsor under N over Q. As N is affine, the map $G \to Q$ is affine, and as Q is affine, this implies that G is affine. □

PROPOSITION 2.71. *Let S and S' be G-torsors over S_0. Every equivariant S_0-morphism $S \to S'$ is an isomorphism.*

PROOF. For every R_0-algebra R, the map $S(R) \to S'(R)$ is a bijection. □

EXAMPLE 2.72. For an algebraic group G over k, we define $H^1_{\text{flat}}(S_0, G)$ to be the set of isomorphism classes of torsors under G over S_0. Let R be a faithfully flat R_0-algebra. The torsors under G_{R_0} over R_0 having an R-point are classified by the cohomology set $H^1(R/R_0, G)$ of the complex

$$G(R) \to G(R \otimes_{R_0} R) \to G(R \otimes_{R_0} R \otimes_{R_0} R)$$

(DG, III, §4). For example, the $\mathbb{G}_{aR_0}$-torsors over R_0 are all trivial because the sequence

$$R \to R \otimes_{R_0} R \to R \otimes_{R_0} R \otimes_{R_0} R$$

is exact (CA 11.11). Thus $H^1_{\text{flat}}(S_0, \mathbb{G}_a) = 0$ (DG, III, §4, 6.6). Similarly, $H^1_{\text{flat}}(S_0, \mathbb{G}_m) = H^1(S_0, \mathcal{O}^\times_{S_0}) = \text{Pic}(S_0)$ (DG, III, §4, 6.10).

Exercises

EXERCISE 2-1. For a homomorphism $G \to H$ of abstract groups with kernel N, show that the map

$$(g,n) \mapsto (g,gn) : G \times N \to G \times_H G \tag{12}$$

is a bijection. Deduce that, for every homomorphism $G \to H$ of algebraic k-groups with kernel N, there is an isomorphism of algebraic k-schemes

$$G \times N \to G \times_H G \tag{13}$$

that becomes (12) when we take points with coordinates in a k-algebra R.

EXERCISE 2-2. Show that for every diagram of abstract groups

$$
\begin{array}{c}
G \\
\downarrow{\scriptstyle \varphi} \\
N \longrightarrow H \longrightarrow H'
\end{array}
\tag{14}
$$

with N the kernel of $H \to H'$ and the map $G \to H'$ surjective, the map

$$(n, g) \mapsto (n \cdot \varphi(g), g): N \times G \to H \times_{H'} G \qquad (15)$$

is a bijection. Deduce that, for every diagram (14) of algebraic groups, there is an isomorphism of algebraic k-schemes

$$N \times G \to H \times_{H'} G$$

that becomes (15) when we take points with coordinates in a k-algebra R.

EXERCISE 2-3. Let $X = \mathrm{Spm}(k \times k')$ with k'/k a separable field extension of degree 5. Show that there does not exist a multiplication map on X making it into an étale group scheme.

EXERCISE 2-4. Let k be a nonperfect field of characteristic p, and let $a \in k \smallsetminus k^p$. Show that the functor

$$R \rightsquigarrow G(R) \overset{\mathrm{def}}{=} \{x \in R \mid x^{p^2} = ax^p\}$$

becomes a finite commutative algebraic group under addition. Show that $G(k)$ has only one element but $\pi_0(G)$ has p. Deduce that G is not isomorphic to the semidirect product of G° and $\pi_0(G)$. (Hence Exercise 11-2 below shows that $\mathcal{O}(G)$ modulo its nilradical is not a Hopf algebra.)

EXERCISE 2-5. Let $G : Y^P = X - tX^p$ be the algebraic group over the field $k = k_0(t)$ in (1.56) (so $p > 2$). Show that $G(k)$ is finite.

EXERCISE 2-6. Let k be a field of characteristic p. Show that the isomorphism classes of extensions

$$0 \to \mu_p \to G \to \mathbb{Z}/p\mathbb{Z} \to 0$$

with G a finite commutative algebraic group are classified by the elements of $k^\times/k^{\times p}$. Show that G_{red} is not a subgroup of G unless the extension splits.

EXERCISE 2-7. What is the map $\mathcal{O}(\mathrm{SL}_n) \to \mathcal{O}(\mathrm{GL}_n)$ defined in Example 2.42?

EXERCISE 2-8. Let q be the quadratic form $x_1^2 + \cdots + x_n^2$ over a field k of characteristic $\neq 2$. Prove directly that $\pi(\mathcal{O}(\mathrm{O}(q))) = k \times k$.

EXERCISE 2-9. Let O_n be the orthogonal group of the diagonal form $x_1^2 + \cdots + x_n^2$ over a field k of characteristic $\neq 2$. For each k-algebra R, let $V(R)$ denote the set of skew-symmetric matrices, i.e., the matrices A such that $A^t = -A$.

(a) Show that the functor $R \mapsto V(R)$ is represented by a finitely generated k-algebra C, and that C is an integral domain.

(b) Show that $A \mapsto (I_n - A)(I_n + A)^{-1}$ defines a bijection from a nonempty open subset of $\mathrm{SO}_n(k^a)$ onto an open subset of $V(k^a)$, with partial inverse $B \mapsto (I_n - B)(I_n + B)^{-1}$.

(c) Deduce that SO_n is connected.

(d) Deduce that SO_n is rational (in the sense of 12.59).

EXERCISE 2-10. Let G be an algebraic group over a field k, and let A be a local artinian ring with residue field k. Show that $(G)_{A/k}$ has a filtration whose quotients are either vector groups or G itself.

EXERCISE 2-11. Let k' be a finite extension of k, and let $\varphi: G \to H$ be a homomorphism of connected affine group varieties over k'. Prove the following (Pink 2004, 1.6):

(a) if k'/k is separable, then $(\varphi)_{k'/k}: (G)_{k'/k} \to (H)_{k'/k}$ is an isogeny if and only if φ is an isogeny;

(b) if k'/k is not separable, then $(\varphi)_{k'/k}: (G)_{k'/k} \to (H)_{k'/k}$ is an isogeny if and only if φ is an étale isogeny.

Affine Algebraic Groups and Hopf Algebras

In this chapter, we concentrate on affine algebraic groups. In particular, we investigate their relation to Hopf algebras.

a. The comultiplication map

Let A be a k-algebra and $\Delta\colon A \to A \otimes A$ a homomorphism of k-algebras. A pair of k-algebra homomorphisms $f_1, f_2\colon A \to R$ defines a homomorphism

$$(f_1, f_2)\colon A \otimes A \to R, \quad (a_1, a_2) \mapsto f_1(a_1) f_2(a_2),$$

and we set

$$f_1 \cdot f_2 = (f_1, f_2) \circ \Delta.$$

Thus $(f_1, f_2) \mapsto f_1 \cdot f_2$ is a binary operation on $\operatorname{Hom}(A, R)$. Because

$$\operatorname{Spm}(A \otimes A) \simeq \operatorname{Spm}(A) \times \operatorname{Spm}(A),$$

we can regard $\operatorname{Spm}(\Delta)$ as a map $\operatorname{Spm}(A) \times \operatorname{Spm}(A) \to \operatorname{Spm}(A)$.

PROPOSITION 3.1. *The pair* $(\operatorname{Spm}(A), \operatorname{Spm}(\Delta))$ *is an algebraic group over* k *if and only if* $(f_1, f_2) \mapsto f_1 \cdot f_2$ *is a group structure on* $\operatorname{Hom}(A, R)$ *for all* k-*algebras* R.

PROOF. Let $(G, m) = (\operatorname{Spm} A, \operatorname{Spm} \Delta)$. The operation on $h^A(R)$ defined by Δ equals that on $G(R)$ defined by m, and so it is a group structure if (G, m) is an algebraic group. Conversely, if Δ defines a group structure on $\operatorname{Hom}(A, R)$ for all R, then h^A is functor to groups whose underlying functor to sets is representable by $\operatorname{Spm}(A)$. This implies that (G, m) is an algebraic group (see 1.4). □

NOTATION 3.2. Let G be an affine algebraic group. For a k-algebra R,

$$G(R) \simeq \mathrm{Hom}_{k\text{-algebra}}(\mathcal{O}(G), R) \simeq \mathrm{Hom}_{R\text{-algebra}}(\mathcal{O}(G)_R, R).$$

An $f \in \mathcal{O}(G)$ defines an evaluation map

$$f_R \colon G(R) \to R, \quad g \mapsto g(f) \overset{\mathrm{def}}{=} f_R(g),$$

which is natural in R. In this way, we get an isomorphism

$$\mathcal{O}(G) \simeq \mathrm{Nat}(G, \mathbb{A}^1) \quad \text{(natural transformations)}$$

where $\mathbb{A}^1$ is the functor sending a k-algebra R to its underlying set. Similarly,

$$\mathcal{O}(G \times G) \simeq \mathrm{Nat}(G \times G, \mathbb{A}^1).$$

With this interpretation

$$(\Delta f)_R(g_1, g_2) = f_R(g_1 \cdot g_2), \quad \text{for } f \in \mathcal{O}(G), \, g_1, g_2 \in G(R). \tag{16}$$

b. Hopf algebras

Let (G, m) be an affine algebraic group over k, and let $A = \mathcal{O}(G)$. We saw in the preceding section that m corresponds to a homomorphism $\Delta \colon A \to A \otimes A$. The maps e and inv correspond to homomorphisms of k-algebras $\epsilon \colon A \to k$ and $S \colon A \to A$, and the diagrams (1) and (2), p. 6, correspond to diagrams

$$
\begin{array}{ccc}
A \otimes A \otimes A & \xleftarrow{\;\mathrm{id}\otimes\Delta\;} & A \otimes A \\
{\scriptstyle \Delta\otimes\mathrm{id}}\uparrow & & \uparrow{\scriptstyle \Delta} \\
A \otimes A & \xleftarrow{\quad\Delta\quad} & A
\end{array}
\qquad
\begin{array}{ccccc}
k \otimes A & \xleftarrow{\;\epsilon\otimes\mathrm{id}\;} & A \otimes A & \xrightarrow{\;\mathrm{id}\otimes\epsilon\;} & A \otimes k \\
& \nwarrow{\scriptstyle \simeq} & \uparrow{\scriptstyle \Delta} & \nearrow{\scriptstyle \simeq} & \\
& & A & &
\end{array}
\tag{17}
$$

$$
\begin{array}{ccccc}
A & \xleftarrow{\;(S,\mathrm{id})\;} & A \otimes A & \xrightarrow{\;(\mathrm{id},S)\;} & A \\
\uparrow & & \uparrow{\scriptstyle \Delta} & & \uparrow \\
k & \xleftarrow{\;\epsilon\;} & A & \xrightarrow{\;\epsilon\;} & k
\end{array}
\tag{18}
$$

DEFINITION 3.3. Let R_0 be a commutative ring. A pair (A, Δ) consisting of a commutative R_0-algebra A and an R_0-algebra homomorphism $\Delta \colon A \to A \otimes A$ is a ***Hopf algebra***[1] over R_0 if there exist R_0-algebra homomorphisms

$$\epsilon \colon A \to R_0, \quad S \colon A \to A$$

---

[1] The general definition of a Hopf algebra does not require A to be commutative. Thus, we are considering only a special class of Hopf algebras, and not all of our statements hold for general Hopf algebras.

such that the diagrams (17, 18) commute:

$$(\text{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \text{id}) \circ \Delta$$
$$(\text{id}, \epsilon) \circ \Delta = \text{id} = (\epsilon, \text{id}) \circ \Delta$$
$$(\text{id}, S) \circ \Delta = \epsilon = (S, \text{id}) \circ \Delta.$$

The maps Δ, ϵ, S are called the ***comultiplication*** map, the ***co-identity*** map, and the ***antipode*** or ***inversion*** respectively. A ***homomorphism*** of Hopf algebras $f : (A, \Delta_A) \to (B, \Delta_B)$ is a homomorphism $f : A \to B$ of R_0-algebras such that $(f \otimes f) \circ \Delta_A = \Delta_B \circ f$. A Hopf algebra (A, Δ) is said to be ***finitely generated*** if A is finitely generated as an R_0-algebra.

3.4. The pair (ϵ, S) in the definition of a Hopf algebra is uniquely determined by (A, Δ). Moreover, for every homomorphism $f : (A, \Delta_A) \to (B, \Delta_B)$ of Hopf algebras,

$$\begin{cases} \epsilon_B \circ f = \epsilon_A \\ f \circ S_A = S_B \circ f. \end{cases} \tag{19}$$

This can be proved in the same way as the similar statement for algebraic groups by using the Yoneda lemma (see 1.21). We sometimes regard a Hopf algebra as a quadruple (A, Δ, S, ϵ).

3.5. Let $f \in \mathcal{O}(G)$, and regard it as a natural transformation $G \to \mathbb{A}^1$ (as in 3.2). Then

$$(\Delta f)_R(g_1, g_2) = f_R(g_1 \cdot g_2),$$
$$(\epsilon f)_R(g) = f(e)$$
$$(Sf)_R(g) = f(g^{-1})$$

for $g, g_1, g_2 \in G(R)$.

Readers new to Hopf algebras should now do Exercise 3-1.

c. Hopf algebras and algebraic groups

The next proposition shows that to give a structure Δ of a Hopf algebra on a k-algebra A is the same as giving a structure m of an algebraic group on $\text{Spm}(A)$.

PROPOSITION 3.6. *Let A be a (finitely generated) k-algebra and $\Delta : A \to A \otimes A$ a homomorphism. The pair (A, Δ) is a Hopf algebra if and only if $\text{Spm}(A, \Delta)$ is an algebraic group.*

PROOF. The diagrams (17, 18) are the same as the diagrams (1, 2) except that the arrows have been reversed. As Spm is a contravariant equivalence from the category of finitely generated k-algebras to that of affine algebraic schemes over k, it is clear that one pair of diagrams commutes if and only if the other does. Alternatively, check that (A, Δ) is a Hopf algebra if and only if Δ makes $\text{Hom}(A, R)$ into a group for all R, and apply (3.1). $\square$

COROLLARY 3.7. *The functor* Spm *is an equivalence from the category of finitely generated Hopf algebras over k to the category of affine algebraic groups, with quasi-inverse* $(G, m) \rightsquigarrow (\mathcal{O}(G), \mathcal{O}(m))$.

d. Hopf subalgebras

DEFINITION 3.8. A k-subalgebra B of a Hopf algebra (A, Δ, S, ϵ) is a ***Hopf subalgebra*** if $\Delta(B) \subset B \otimes B$ and $S(B) \subset B$.

Then $(B, \Delta_A|B)$ is itself a Hopf algebra with $\epsilon_B = \epsilon_A|B$ and $S_B = S_A|B$.

PROPOSITION 3.9. *The image of a homomorphism* $f: A \to B$ *of Hopf algebras is a Hopf subalgebra of B.*

PROOF. Immediate from consequence of 3.4. □

DEFINITION 3.10. A ***Hopf ideal*** in a Hopf k-algebra (A, Δ, S, ϵ) is an ideal $\mathfrak{a}$ in A such that

$$\Delta(\mathfrak{a}) \subset A \otimes \mathfrak{a} + \mathfrak{a} \otimes A, \quad \epsilon(\mathfrak{a}) = 0, \quad S(\mathfrak{a}) \subset \mathfrak{a}.$$

PROPOSITION 3.11. *The kernel of a homomorphism of Hopf k-algebras is a Hopf ideal.*

PROOF. The proof uses the following elementary fact: for a linear map $f: V \to V'$ of k-vector spaces, the kernel of $f \otimes f$ is $V \otimes \text{Ker}(f) + \text{Ker}(f) \otimes V$. To see this, write $V = \text{Ker}(f) \oplus W$, and note that the restriction of $f \otimes f$ to $W \otimes W$ is injective.

Let $\mathfrak{a}$ be the kernel of a homomorphism $f: A \to B$ of Hopf algebras. Then

$$\begin{cases} \Delta_A(\mathfrak{a}) \subset \text{Ker}(f \otimes f) = A \otimes \mathfrak{a} + \mathfrak{a} \otimes A \\ \epsilon_A(\mathfrak{a}) = 0 \quad \text{by (19)} \\ S_A(\mathfrak{a}) \subset \mathfrak{a} \quad \text{by (19)} \end{cases}$$

and so $\mathfrak{a}$ is a Hopf ideal. □

The next result shows that the Hopf ideals are exactly the kernels of homomorphisms of Hopf algebras.

PROPOSITION 3.12. *Let $\mathfrak{a}$ be a Hopf ideal in a Hopf k-algebra A. The vector space $A/\mathfrak{a}$ has a unique Hopf k-algebra structure for which $A \to A/\mathfrak{a}$ is a homomorphism of Hopf k-algebras. Every homomorphism of Hopf k-algebras $A \to B$ whose kernel contains $\mathfrak{a}$ factors uniquely through $A \to A/\mathfrak{a}$.*

PROOF. Routine verification. □

PROPOSITION 3.13. *A homomorphism $f: A \to B$ of Hopf k-algebras induces an isomorphism of Hopf k-algebras*

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

PROOF. Routine verification.   □

PROPOSITION 3.14. *Every homomorphism $A \to B$ of Hopf algebras factors as*

$$A \xrightarrow{q} C \xrightarrow{i} B$$

with q (resp. i) a surjective (resp. injective) homomorphism of Hopf algebras. The factorization is unique up to a unique isomorphism.

PROOF. Immediate consequence of Proposition 3.13.   □

e.   Hopf subalgebras of $\mathcal{O}(G)$ versus subgroups of G

PROPOSITION 3.15. *Let G be an affine algebraic group. In the one-to-one correspondence between closed subschemes of G and ideals in $\mathcal{O}(G)$, algebraic subgroups correspond to Hopf ideals.*

PROOF. Let H be the closed subscheme of G defined by an ideal $\mathfrak{a} \subset \mathcal{O}(G)$. If H is an algebraic subgroup of G, then $\mathfrak{a}$ is the kernel of a homomorphism of Hopf algebras $\mathcal{O}(G) \to \mathcal{O}(H)$, and so is a Hopf ideal (3.11). Conversely, if $\mathfrak{a}$ is a Hopf ideal, then $\mathcal{O}(G)/\mathfrak{a}$ has a unique Hopf algebra structure for which $\mathcal{O}(G) \to \mathcal{O}(G)/\mathfrak{a}$ is a homomorphism of Hopf algebras (3.12). But $\mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a}$, and so this means that H has a unique algebraic group structure for which the inclusion $H \hookrightarrow G$ is a homomorphism of algebraic groups (3.7).   □

f.   Subgroups of $G(k)$ versus algebraic subgroups of G

In this section, we give a direct proof of Theorem 1.45 for affine algebraic groups.

PROPOSITION 3.16. *Let G be an affine algebraic group over k and S a closed subgroup of $G(k)$. There is a unique reduced algebraic subgroup H of G such that $S = H(k)$, and H is geometrically reduced. The algebraic subgroups H of G that arise in this way are exactly those for which $H(k)$ is schematically dense in H.*

PROOF. Each $f \in \mathcal{O}(G)$ defines a function $h(f): S \to k$, and, for $x, y \in S$, $(\Delta_G f)(x, y) = f(x \cdot y)$ (see (16), p. 65). Therefore, when we let $R(S)$ denote the k-algebra of maps $S \to k$ and define $\Delta_S: R(S) \to R(S \times S)$ as in Exercise 3-1, we obtain a commutative diagram

$$
\begin{array}{ccc}
\mathcal{O}(G) & \xrightarrow{\Delta_G} & \mathcal{O}(G \times G) \\
\downarrow{\scriptstyle h} & & \downarrow \\
R(S) & \xrightarrow{\Delta_S} & R(S \times S).
\end{array}
$$

The vertical map at right factors into

$$\mathcal{O}(G \times G) \simeq \mathcal{O}(G) \otimes \mathcal{O}(G) \xrightarrow{h \otimes h} R(S) \otimes R(S) \to R(S \times S).$$

Therefore the kernel $\mathfrak{a}$ of h satisfies

$$\Delta_G(\mathfrak{a}) \subset \mathrm{Ker}(h \otimes h) = \mathcal{O}(G) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathcal{O}(G)$$

(cf. the proof of 3.11). Similarly $\epsilon_G(\mathfrak{a}) = 0$ and $S_G(\mathfrak{a}) \subset \mathfrak{a}$, and so $\mathfrak{a}$ is a Hopf ideal. Because S is closed in $G(k)$, the algebraic subgroup H of G with $\mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a}$ has $H(k) = S$. Clearly, H is the unique reduced algebraic subgroup of G with this property.

Obviously, the algebraic subgroups H arising in this way have the property that $H(k)$ is dense in H. Conversely, if $H(k)$ is dense in H, then the group attached to $S = H(k)$ is H itself. □

ASIDE 3.17. What are the algebraic groups H such that $H(k)$ is schematically dense in H? Recall (1.10, 1.12) that $H(k)$ is schematically dense in H if and only if H is geometrically reduced and $H(k)$ is dense in $|H|$. When k is finite, $H(k)$ cannot be dense in $|H|$ unless H is finite.

We now assume that H is smooth and k is infinite, and ask whether $H(k)$ is dense in $|H|$. When H is finite (hence étale), $H(k)$ is dense in $|H|$ if and only if H is constant. For a general H, $H(k)$ is dense in $|H|$ if and only if this is true for H° and $\pi_0(H)$. If H is connected and affine and k is perfect, then $H(k)$ is dense in $|H|$ (see 17.93). On the other hand, the example of Rosenlicht (1.56) shows that there exist forms H of $\mathbb{G}_a$ over infinite nonperfect fields such that $H(k)$ is finite and hence not dense in $|H|$. When H is nonaffine, there does not seem to be much that one can say. For example, when E is an elliptic curve over $\mathbb{Q}$, the group $E(\mathbb{Q})$ may be finite (hence not dense in E) or infinite (hence dense).

ASIDE 3.18. When k is finite, only the finite subgroup varieties of G arise as the Zariski closure of a subgroup of $G(k)$. Nori (1987) has found a more useful way of defining the "closure" of a subgroup S of $\mathrm{GL}_n(\mathbb{F}_p)$. Let $X = \{x \in S \mid x^p = 1\}$, and let S^+ be the subgroup of S generated by X (it is normal). For each $x \in X$, we get a one-parameter subgroup variety

$$t \mapsto x^t = \exp(t \log x) \colon \mathbb{A}^1 \to \mathrm{GL}_n, \quad \text{where} \quad \begin{cases} \exp(z) = \sum_{i=0}^{p-1} \frac{z^i}{i!} \text{ and} \\ \log(z) = -\sum_{i=1}^{p-1} \frac{(1-z)^i}{i}. \end{cases}$$

Let G be the algebraic subgroup of GL_n generated by these maps. Nori shows that if p is greater than some constant depending only on n, then $S^+ = G(\mathbb{F}_p)^+$. If G is semisimple and simply connected, then $G(\mathbb{F}_p)^+ = G(\mathbb{F}_p)$, and so S^+ is realized as the group of $\mathbb{F}_p$-points of the connected algebraic group G. The map $S \mapsto G$ sets up a one-to-one correspondence between the subgroups S of $\mathrm{GL}_n(\mathbb{F}_p)$ such that $S = S^+$ and the subgroup varieties of $\mathrm{GL}_{n\mathbb{F}_p}$ generated by one-parameter subgroups $t \mapsto \exp(ty)$ defined by elements $y \in M_n(\mathbb{F}_p)$ with $y^p = 0$.

g. Affine algebraic groups in characteristic zero are smooth

In this section, we prove a theorem of Cartier stating that all affine algebraic groups over a field of characteristic zero are smooth.

LEMMA 3.19. *An algebraic group G over an algebraically closed field k is smooth if $\dim \mathrm{Tgt}_e(G) = \dim \mathrm{Tgt}_e(G_{\mathrm{red}})$.*

PROOF. Recall (1.37) that $\dim G \leq \dim \mathrm{Tgt}_e(G)$ with equality if and only if G is smooth, and that a geometrically reduced group is smooth (1.28). Hence

$$\dim G \leq \dim \mathrm{Tgt}_e(G) = \dim \mathrm{Tgt}_e(G_{\mathrm{red}}) = \dim G_{\mathrm{red}}.$$

As $\dim G = \dim G_{\mathrm{red}}$, this shows that $\dim G = \dim \mathrm{Tgt}_e(G)$.   □

LEMMA 3.20. *An algebraic group G over an algebraically closed field k is smooth if every nilpotent element of $\mathcal{O}(G)$ is contained in $\mathfrak{m}_e^2$, where $\mathfrak{m}_e$ is the maximal ideal in $\mathcal{O}(G)$ at e.*

PROOF. As $\mathrm{Tgt}_e(G) \simeq \mathrm{Hom}(\mathfrak{m}_e/\mathfrak{m}_e^2, k)$, (A.51), the hypothesis implies that $\mathrm{Tgt}_e(G) \simeq \mathrm{Tgt}_e(G_{\mathrm{red}})$.   □

LEMMA 3.21. *Let V and V' be vector spaces over a field. Let W be a subspace of V and y a nonzero element of V'. An element x of V lies in W if and only if $x \otimes y$ lies in $W \otimes V'$.*

PROOF. Write $V = W \oplus W'$, and note that $V \otimes V' \simeq (W \otimes V') \oplus (W' \otimes V')$.□

LEMMA 3.22. *Let (A, Δ) be a Hopf algebra over k, and let I denote the augmentation ideal (kernel of the co-identity map ϵ).*

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

(b) *For all $a \in I$,*

$$\Delta(a) = a \otimes 1 + 1 \otimes a \quad \mathrm{mod}\ I \otimes I.$$

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

(b) Let $a \in I$. Using the second diagram in (17), p. 65, we find that

$$(\mathrm{id} \otimes \epsilon)(\Delta(a) - a \otimes 1 - 1 \otimes a) = a \otimes 1 - a \otimes 1 - 1 \otimes 0 = 0$$
$$(\epsilon \otimes \mathrm{id})(\Delta(a) - a \otimes 1 - 1 \otimes a) = 1 \otimes a - 0 \otimes 1 - 1 \otimes a = 0.$$

Hence

$$\Delta(a) - a \otimes 1 - 1 \otimes a \in \mathrm{Ker}(\mathrm{id} \otimes \epsilon) \cap \mathrm{Ker}(\epsilon \otimes \mathrm{id})$$
$$= (A \otimes I) \cap (I \otimes A).$$

That

$$(A \otimes I) \cap (I \otimes A) = I \otimes I$$

follows from comparing

$$A \otimes A = (k \otimes k) \oplus (k \otimes I) \oplus (I \otimes k) \oplus (I \otimes I)$$
$$A \otimes I = (k \otimes I) \oplus (I \otimes I)$$
$$I \otimes A = (I \otimes k) \oplus (I \otimes I).$$

$\square$

THEOREM 3.23 (CARTIER). *Every affine algebraic group over a field of characteristic zero is smooth.*

PROOF. We may suppose that k is algebraically closed. Thus, let G be an algebraic group over an algebraically closed field k of characteristic zero, and let $A = \mathcal{O}(G)$. Let $\mathfrak{m} = \mathfrak{m}_e = \operatorname{Ker}(\epsilon)$. According to Lemma 3.20, it suffices to show that every nilpotent element a of A lies in $\mathfrak{m}^2$.

If a maps to zero in $A_\mathfrak{m}$, then it maps to zero in $A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$, and therefore in $A/\mathfrak{m}^2$ by (CA 5.8), and so $a \in \mathfrak{m}^2$. Thus, we may suppose that there exists an $n \geq 2$ such that $a^n = 0$ in $A_\mathfrak{m}$ but $a^{n-1} \neq 0$ in $A_\mathfrak{m}$. Now $sa^n = 0$ in A for some $s \notin \mathfrak{m}$. On replacing a with sa, we find that $a^n = 0$ in A but $a^{n-1} \neq 0$ in $A_\mathfrak{m}$.

Now $a \in \mathfrak{m}$ (because $A/\mathfrak{m} = k$ has no nilpotents), and so (see 3.22)

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

Because Δ is a homomorphism of k-algebras,

$$0 = \Delta(a^n) = (\Delta a)^n = (a \otimes 1 + 1 \otimes a + y)^n. \tag{20}$$

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

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

As $a^n = 0$ and the terms with $i + j \geq 2$ lie in $A \otimes \mathfrak{m}^2$, equation (20) shows that

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

and so

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

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

$$na^{n-1} \otimes \bar{a} \in a^{n-1}\mathfrak{m} \otimes A/\mathfrak{m}^2 \quad \text{(inside } A \otimes (A/\mathfrak{m}^2)\text{)}. \tag{21}$$

Note that $a^{n-1} \notin a^{n-1}\mathfrak{m}$, because if $a^{n-1} = a^{n-1}m$ with $m \in \mathfrak{m}$, then $(1 - m)a^{n-1} = 0$ and, as $1 - m$ is a unit in $A_\mathfrak{m}$, this would imply $a^{n-1} = 0$ in $A_\mathfrak{m}$, which is a contradiction. Moreover n is a unit in A because it is a nonzero element of k (here we use that k has characteristic 0). We conclude that $na^{n-1} \notin a^{n-1}\mathfrak{m}$, and so (21) implies that $\bar{a} = 0$. In other words, $a \in \mathfrak{m}^2$, as required. $\square$

COROLLARY 3.24. *In characteristic zero, all finite algebraic groups are étale.*

PROOF. Smooth finite schemes are étale (A.60). □

COROLLARY 3.25. *All surjective homomorphisms of affine algebraic groups in characteristic zero are smooth.*

PROOF. Apply Proposition 1.63. □

COROLLARY 3.26. *Let H and H' be affine algebraic subgroups of an algebraic group G over a field k of characteristic zero. If $H(k^a) = H'(k^a)$, then $H = H'$.*

PROOF. Apply Corollary 1.44. □

COROLLARY 3.27. *Let G be an affine algebraic group over a field k of characteristic zero and H an algebraic subgroup of G.*

  (a) *The normalizer N of H in G is the unique algebraic subgroup of G such that $N(k^a)$ is the normalizer of $H(k^a)$ in $G(k^a)$.*
  (b) *The centralizer C of H in G is the unique algebraic subgroup of G such that $C(k^a)$ is the centralizer of $H(k^a)$ in $G(k^a)$.*

PROOF. Apply 1.88 and 1.95. □

REMARK 3.28. Theorem 3.23 fails for algebraic monoids. For example, the nonreduced algebraic scheme $M = \text{Spm}(k[T]/(T^n))$, $n > 1$, admits a monoid structure – take e to be the unique map $* \to M$ and m to be the composite $M \times M \to * \to M$.

NOTES. Cartier (1962, Section 15) sketched a proof of Theorem 3.23 in which he embedded $\mathcal{O}(G)$ in the coordinate ring of a formal group $\hat{G}$ (the "completion" of G), and showed that the latter has no nilpotents. Our proof follows Oort 1966. The theorem is true for all algebraic groups (8.39 below).

h. Smoothness in characteristic $p \neq 0$

PROPOSITION 3.29. *Let G be an affine algebraic group over a perfect field k of characteristic $p \neq 0$, and let r be a positive integer. The image $\mathcal{O}(G)^{p^r}$ of the ring homomorphism*
$$a \mapsto a^{p^r} : \mathcal{O}(G) \to \mathcal{O}(G)$$
is a Hopf subalgebra of $\mathcal{O}(G)$, which is geometrically reduced when r is sufficiently large.

PROOF. Recall (2.24) that the Frobenius map $F^r : G \to G^{(p^r)}$ corresponds to the homomorphism of Hopf k-algebras
$$a \otimes c \mapsto ca^{p^r} : \mathcal{O}(G) \otimes_{k, f^r} k \to \mathcal{O}(G).$$

When k is perfect, this has image $\mathcal{O}(G)^{p^r}$, which is therefore a Hopf subalgebra of $\mathcal{O}(G)$ (see 3.9).

In proving the second part, we may suppose that k is algebraically closed. As the nilradical $\mathfrak{N}$ of $\mathcal{O}(G)$ is finitely generated, there exists an exponent n such that $a^n = 0$ for all $a \in \mathfrak{N}$. Now $\mathcal{O}(G)^{p^r}$ is reduced for all r such that $p^r \geq n$. $\square$

REMARK 3.30. Let G be an affine algebraic group over a field k of characteristic $p \neq 0$. According to the homomorphism theorem (3.34 below), $F^r : G \to G^{(p^r)}$ factors into

$$G \xrightarrow{q} I \xrightarrow{i} G^{(p^r)}$$

with q faithfully flat and i a closed immersion. Here $\mathcal{O}(I)$ is the image of $\mathcal{O}(G^{(p^r)})$ in $\mathcal{O}(G)$. The formation of the factorization commutes with extension of the base field, and so the proposition shows that I is smooth for r sufficiently large.

i. Faithful flatness for Hopf algebras

In this section, we prove an important technical result. For the properties of flatness used, see CA 11.2, 11.3, 11.9.

THEOREM 3.31. *Let $A \subset B$ be finitely generated Hopf algebras over a field k. Then B is faithfully flat over A.*

PROOF. The inclusion $A \hookrightarrow B$ corresponds to a homomorphism of algebraic groups $G \to H$ (so $A = \mathcal{O}(H)$ and $B = \mathcal{O}(G)$), which is dominant, and hence surjective (1.69). If H is reduced, then $G \to H$ is faithfully flat by Proposition 1.70. It remains to prove the theorem when H is nonreduced. After Theorem 3.23, we may suppose that k has characteristic $p \neq 0$. We may also suppose that it is algebraically closed.

We begin with a general remark. Let A be a ring, I a nilpotent ideal in A, and M an A-module. If $M = IM$, then $M = IM = I^2 M = \cdots = 0$. Similarly, a submodule N of M such that $M = N + IM$ equals M.

We now prove the theorem in the case that the augmentation ideal I_A of A is nilpotent. Let $(e_j)_{j \in J}$ be a family of elements in B whose image in $B/I_A B$ is a k-vector space basis. We show that the map

$$(a_j)_{j \in J} \mapsto \sum_j a_j e_j : A^{(J)} \to B$$

is an isomorphism. Here $A^{(J)}$ is a direct sum of copies of A indexed by J. The map is surjective by the general remark. Let N denote its kernel. To show that $N = 0$, it suffices to show that $N = I_A N$ (by the remark again). For this we use the commutative diagram

$$
\begin{array}{ccccccccc}
& I_A \otimes_A N & \longrightarrow & I_A \otimes_A A^{(J)} & \longrightarrow & I_A \otimes_A B & \longrightarrow & 0 & & a \otimes x \\
& \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & & & \downarrow \\
0 & \longrightarrow N & \longrightarrow & A^{(J)} & \longrightarrow & B & \longrightarrow & 0 & & a
\end{array}
$$

Its rows are exact, and the map c is injective because $A \otimes_A B \to B$ is injective and I_A is a direct summand of A. The snake lemma gives an exact sequence of cokernels

$$0 \to \operatorname{Coker}(a) \to \operatorname{Coker}(b) \to \operatorname{Coker}(c) \to 0,$$

but $\operatorname{Coker}(a) = N/I_A N$ and the map $\operatorname{Coker}(b) \to \operatorname{Coker}(c)$ is the isomorphism

$$(a_j) \mapsto \sum a_j \bar{e}_j : (A/I_A)^{(J)} \to B/I_A M,$$

and so $N = I_A N$ as required.

We now prove the general case of the theorem. According to Proposition 3.29, there exists an n such that $\mathcal{O}(H)^{p^n}$ is a reduced Hopf subalgebra of $\mathcal{O}(H)$. Let H' denote the algebraic group such that $\mathcal{O}(H') = \mathcal{O}(H)^{p^n}$, and let M and N denote the kernels of $H \to H'$ and its composite with $G \to H$:

$$
\begin{array}{ccccccc}
e & \longrightarrow & N & \longrightarrow & G & \longrightarrow & H' \\
 & & \downarrow & & \downarrow & & \| \\
e & \longrightarrow & M & \longrightarrow & H & \longrightarrow & H'
\end{array}
$$

Consider the diagrams

$$
\begin{array}{ccc}
H \times_{H'} G & \longleftarrow & G \times_{H'} G \\
\uparrow \simeq & & \uparrow \simeq \\
M \times G & \longleftarrow & N \times G
\end{array}
\qquad
\begin{array}{ccc}
\mathcal{O}(H) \otimes_{\mathcal{O}(H')} \mathcal{O}(G) & \xrightarrow{\ a\ } & \mathcal{O}(G) \otimes_{\mathcal{O}(H')} \mathcal{O}(G) \\
\downarrow \simeq & & \downarrow \simeq \\
\mathcal{O}(M) \otimes \mathcal{O}(G) & \xrightarrow{\ b\ } & \mathcal{O}(N) \otimes \mathcal{O}(G)
\end{array}
$$

The horizontal maps in the diagram at left are obvious from the previous diagram, and the vertical isomorphisms are those in Exercises 2-1 and 2-2. The diagram at right is the corresponding diagram of k-algebras. The map $\mathcal{O}(H') \to \mathcal{O}(G)$ is faithfully flat because we have proved the theorem when H' is reduced. The map a is obtained from $\mathcal{O}(H) \hookrightarrow \mathcal{O}(G)$ by applying $- \otimes_{\mathcal{O}(H')} \mathcal{O}(G)$, and so it is injective. Hence b is also injective, which implies that $\mathcal{O}(M) \to \mathcal{O}(N)$ is injective (as $k \to \mathcal{O}(G)$ is faithfully flat). Now $\mathcal{O}(M) \to \mathcal{O}(N)$ is faithfully flat because we have proved the theorem when the augmentation ideal of $\mathcal{O}(M)$ is nilpotent. It follows that b is faithfully flat, and then that a is faithfully flat. This implies that $\mathcal{O}(H) \to \mathcal{O}(G)$ is faithfully flat. $\qquad\square$

j.   The homomorphism theorem for affine algebraic groups

PROPOSITION 3.32. *Let $A \subset B$ be Hopf algebras with B an integral domain, and let $K \subset L$ be the fields of fractions of A and B. Then $B \cap K = A$; in particular, $A = B$ if $K = L$.*

PROOF. Because B is faithfully flat over A (see 3.31), $cB \cap A = cA$ for all $c \in A$. If a, c are elements of A such that $a/c \in B$, then $a \in cB \cap A = cA$, and so $a/c \in A$. $\qquad\square$

PROPOSITION 3.33. *Every birational homomorphism of connected affine group varieties is an isomorphism.*

PROOF. From such a homomorphism, we get a homomorphism $\alpha \colon A \to B$ of Hopf algebras, both integral domains, which induces an isomorphism on the fields of fractions. Obviously α is injective, and (3.32) shows that it has image B. □

THEOREM 3.34 (HOMOMORPHISM THEOREM FOR AFFINE GROUPS). *Every homomorphism $\varphi \colon G \to H$ of affine algebraic groups factors as a composite of homomorphisms*

$$G \xrightarrow{q} I \xrightarrow{i} H$$

with q faithfully flat and i a closed immersion.

PROOF. According to Proposition 3.14, the homomorphism $\mathcal{O}(\varphi) \colon \mathcal{O}(H) \to \mathcal{O}(G)$ of Hopf k-algebras factors into

$$\mathcal{O}(H) \xrightarrow{a} C \xrightarrow{b} \mathcal{O}(G)$$

with C a finitely generated Hopf k-algebra and a (resp. b) a surjective (resp. injective) homomorphism. On applying Spm, we obtain the required factorization (because of Theorem 3.31). □

COROLLARY 3.35. *Consider a homomorphism $\varphi \colon G \to H$ of affine algebraic groups. If $\mathrm{Ker}(\varphi) = e$, then φ is a closed immersion.*

PROOF. Factor φ as in the theorem. After replacing φ with q, we may suppose that it is faithfully flat. Thus, let $\varphi \colon G \to H$ be a faithfully flat homomorphism such that $\mathrm{Ker}(\varphi) = e$. Then $\varphi(R) \colon G(R) \to H(R)$ is injective for all k-algebras R, and it remains to show that it is surjective. Let $a \in H(R)$. Then a is a homomorphism of k-algebras $\mathcal{O}(H) \to R$. The diagram

$$
\begin{array}{ccc}
\mathcal{O}(G) & \xrightarrow{\;\;b\;\;} & \mathcal{O}(G) \otimes_{\mathcal{O}(H)} R \overset{\text{def}}{=} R' \\
\big\uparrow {\scriptstyle\text{faithfully flat}} & & \big\uparrow {\scriptstyle\text{faithfully flat}} \\
\mathcal{O}(H) & \xrightarrow{\;\;a\;\;} & R
\end{array}
$$

shows that the image of a in $H(R')$ lifts to an element b of $G(R')$. As R' is faithfully flat over R, the rows in the following diagram are exact (CA 11.12):

$$
\begin{array}{ccc}
G(R) \longrightarrow & G(R') \rightrightarrows & G(R' \otimes_R R') \\
\downarrow {\scriptstyle\varphi(R)} & \downarrow {\scriptstyle\varphi(R')} & \downarrow {\scriptstyle\varphi(R' \otimes_R R')} \\
H(R) \longrightarrow & H(R') \rightrightarrows & H(R' \otimes_R R')
\end{array}
$$

A small diagram chase, using that the vertical arrows are injective, now shows that b lies in $G(R)$ and maps to a. □

k. Forms of algebraic groups

Let G be an algebraic group over k, and let K be a field containing k. A K/k-**form** of G is an algebraic group G' over k that becomes isomorphic to G over K. We define K/k-forms of modules, algebras, ... similarly. When G is affine, we show that the isomorphism classes of K/k-forms of G are classified[2] by a certain cohomology set.

In this section, all vector spaces are finite-dimensional.

Nonabelian cohomology

Let Γ be a group, and let A be a group with an action of Γ. A mapping $\sigma \mapsto a_\sigma \colon \Gamma \to A$ is a ***crossed homomorphism*** (or 1-***cocycle***) if $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ for all $\sigma, \tau \in \Gamma$. Two crossed homomorphisms (a_σ) and (b_σ) are ***equivalent*** if there exists a $c \in A$ such that $b_\sigma = c^{-1} \cdot a_\sigma \cdot \sigma c$ for all $\sigma \in \Gamma$. The cohomology set $H^1(\Gamma, A)$ is defined to be the set of equivalence classes of crossed homomorphisms; its elements are called ***cohomology classes***. It is a set with a distinguished element, namely, the equivalence class of principal crossed homomorphisms $\sigma \mapsto c^{-1} \cdot \sigma c$. An exact sequence

$$1 \to A \xrightarrow{\ a\ } B \xrightarrow{\ b\ } C \to 1$$

of Γ-modules give rise to an exact sequence of pointed sets

$$1 \to A^\Gamma \xrightarrow{\ a^0\ } B^\Gamma \xrightarrow{\ b^0\ } C^\Gamma \to H^1(\Gamma, A) \xrightarrow{\ a^1\ } H^1(\Gamma, B) \xrightarrow{\ b^1\ } H^1(\Gamma, C).$$

In particular, this means that the preimage by a^1 of the distinguished element in $H^1(\Gamma, B)$ is the quotient of C^Γ by the action of B^Γ, and the preimage by b^1 of the distinguished element in $H^1(\Gamma, C)$ is the image of a^1. We refer the reader to Serre 1997, I, §5 for a detailed treatment of nonabelian cohomology.

Finite Galois extensions

Let K be a finite Galois extension of k with Galois group Γ. A ***semilinear action*** of Γ on a K-vector space V is a k-linear action such that

$$\sigma(cv) = \sigma c \cdot \sigma v \quad \text{all } \sigma \in \Gamma,\, c \in K,\, v \in V.$$

If $V = K \otimes_k V_0$, then there is a semilinear action of Γ on V for which $V^\Gamma = 1 \otimes V_0 \simeq V_0$, namely, $\sigma(c \otimes v) = \sigma c \otimes v$. In A.64 we prove the following statement:

---

[2]Let A be a set with an equivalence relation $\equiv$. We say that a second set B ***classifies*** the $\equiv$-equivalence classes of elements of A if there is a canonical surjection $A \to B$ whose fibres are the equivalence classes.

3.36. *The functor $V \rightsquigarrow K \otimes_k V$ from k-vector spaces to K-vector spaces endowed with a semilinear action of Γ is an equivalence of categories (with quasi-inverse $V \mapsto V^\Gamma$).*

Let V_0 be a k-vector space equipped with a bilinear form $\phi_0 \colon V \times V \to k$. Let $(V_0, \phi_0)_K$ denote the pair over K obtained from (V_0, ϕ_0) by extension of scalars, and let $\mathcal{A}(K)$ denote the group of automorphisms of $(V_0, \phi_0)_K$.

THEOREM 3.37. *The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the K/k-forms of (V_0, ϕ_0).*

PROOF. Let (V, ϕ) be a K/k form of (V_0, ϕ_0), and choose an isomorphism $f \colon (V_0, \phi_0)_K \to (V, \phi)_K$. Let $a_\sigma(f) = f^{-1} \circ \sigma f$. Then

$$a_\sigma \cdot \sigma a_\tau = (f^{-1} \circ \sigma f) \circ (\sigma f^{-1} \circ \sigma \tau f) = a_{\sigma\tau},$$

and so $a_\sigma(f)$ is a 1-cocycle. Any other isomorphism $f' \colon (V_0, \phi_0)_K \to (V, \phi)_K$ differs from f by an element g of $\mathcal{A}(K)$, and

$$a_\sigma(f \circ g) = g^{-1} \cdot a_\sigma(f) \cdot \sigma g.$$

Therefore, the cohomology class of $a_\sigma(f)$ depends only on (V, ϕ). One sees easily that it depends only on the isomorphism class of (V, ϕ) over k, and that two pairs (V, ϕ) and (V', ϕ') giving rise to the same cohomology class are isomorphic. It remains to show that every cohomology class arises from a pair (V_1, ϕ_1). Let $(a_\sigma)_{\sigma \in \Gamma}$ be a 1-cocycle, and use it to define a new action of Γ on $V_K \overset{\text{def}}{=} K \otimes_k V_0$:

$$\sigma x = a_\sigma \cdot \sigma x, \quad \sigma \in \Gamma, \quad x \in V_K.$$

This action is semilinear, and so $V_1 \overset{\text{def}}{=} \{x \in V_K \mid \sigma x = x\}$ is a k-subspace of V_K such that $K \otimes_k V_1 \simeq V_K$ (by 3.36). Because ϕ_{0K} arises from a pairing over k and a_σ is an automorphism of $(V_0, \phi_0)_K$,

$$\sigma(\phi_{0K}(x, y)) = \phi_{0K}(\sigma x, \sigma y) = \phi_{0K}(\sigma x, \sigma y) \tag{22}$$

for $x, y \in V_K$ and $\sigma \in \Gamma$. If $x, y \in V_1$, then (22) shows that $\phi_{0K}(x, y)$ lies in $K^\Gamma = k$. Thus ϕ_{0K} induces a k-bilinear pairing ϕ_1 on V_1. Now $(a_\sigma)_\sigma$ is the 1-cocycle attached to (V_1, ϕ_1) and the given isomorphism $K \otimes_k V_1 \to V_K$. □

EXAMPLE 3.38. Let V_0 be a vector space over k equipped with a tensor $t_0 \in T_s^r(V_0)$, and let G be the algebraic subgroup of GL_{V_0} fixing t (see 2.13). The cohomology set $H^1(\Gamma, G(K))$ classifies the K/k forms of (V_0, t_0). The proof is the same as that of the theorem.

PROPOSITION 3.39. *For all n, $H^1(\Gamma, \mathrm{GL}_n(K)) = 1$.*

PROOF. Theorem 3.37 applied to $(V_0, \phi_0) = (k^n, 0)$ shows that $H^1(\Gamma, \mathrm{GL}_n(K))$ classifies the isomorphism classes of vector spaces V over k such that $K \otimes_k V \approx K^n$. But these are exactly the k-vector spaces of dimension n, and they fall into a single isomorphism class. □

PROPOSITION 3.40. *For all n, $H^1(\Gamma, \mathrm{SL}_n(K)) = 1$.*

PROOF. Because the determinant map $\det: \mathrm{GL}_n(K) \to K^\times$ is surjective,

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^\times \to 1$$

is an exact sequence of Γ-groups. It gives rise to an exact sequence

$$\mathrm{GL}_n(k) \xrightarrow{\det} k^\times \to H^1(\Gamma, \mathrm{SL}_n) \to H^1(\Gamma, \mathrm{GL}_n),$$

from which the statement follows.   □

PROPOSITION 3.41. *Let ϕ_0 be a nondegenerate alternating bilinear form on V_0, and let Sp be the associated symplectic group. Then $H^1(\Gamma, \mathrm{Sp}(K)) = 1$.*

PROOF. A pair (V, ϕ) over k becoming isomorphic to (V_0, ϕ_0) over K is a vector space over k of dimension $\dim(V_0)$ equipped with a nondegenerate alternating form. All such pairs are isomorphic.   □

EXAMPLE 3.42. (a) Let A be a finite-dimensional algebra over k (not necessarily commutative), and let V denote A regarded as a right A-module. Then $H^1(\Gamma, A_K^\times)$ classifies the K/k-forms of V. If W is such a form, then $W_K \approx V_K$ as right A_K-modules. As an A-module, W_K is a direct sum of $[K:k]$-copies of W, and similarly for V_K. The Krull–Schmidt theorem now shows that $W \approx V$ as A-modules. We deduce that $H^1(\Gamma, A_K^\times) = 1$.

(b) Let ϕ_0 be a nondegenerate bilinear symmetric form on V_0, and let O be the associated orthogonal group. Then $H^1(\Gamma, \mathrm{O}(K))$ classifies the isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K. This can be a very large set (Serre 1970, IV, §3).

(c) In particular, Proposition 3.39 says that $H^1(\Gamma, \mathbb{G}_m) = 1$. When Γ is cyclic with generator σ, this says that the only elements of $K^\times$ with norm 1 are those of the form $\sigma c/c$.

Let G_0 be an affine algebraic group over k, and let $\mathcal{A}(K)$ be the group of automorphisms of $(G_0)_K$. Then Γ acts on $\mathcal{A}(K)$ in a natural way:

$$\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}, \quad \sigma \in \Gamma, \quad \alpha \in \mathcal{A}(K).$$

Let G be a K/k-form of G_0. Choose an isomorphism $f: G_{0K} \to G_K$, and write $a_\sigma = f^{-1} \circ \sigma f$. As before $(a_\sigma)_{\sigma \in \Gamma}$ is a 1-cocycle whose cohomology class depends only on the isomorphism class of G.

THEOREM 3.43. *The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of K/k-forms of G_0.*

PROOF. Let $A_0 = \mathcal{O}(G_0)$. Then $\mathcal{A}(K)$ is the group of automorphisms of $A_0 \otimes K$ as a Hopf algebra, and we have to show that $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of K/k-forms of A_0. But a Hopf algebra is a k-vector space equipped with certain linear maps satisfying certain conditions. The same argument as in the proof of Theorem 3.37 proves the statement.   □

Infinite Galois extensions

The above discussion applies also to infinite Galois extensions K/k provided we endow Γ with its Krull topology. When we give $G(K)$ its discrete topology, then the action of Γ on $G(K)$ is continuous, because

$$G(K) = \bigcup_{k'/k} G(k') = \bigcup_{k'/k} G(K)^{\mathrm{Gal}(K/k')}$$

where k' runs over the finite Galois extensions of k contained in K. When Γ is infinite, we define $H^1(\Gamma, G(K))$ using continuous crossed homomorphisms. Then

$$H^1(\Gamma, G(K)) = \varprojlim H^1(\Gamma_{k'/k}, G(k')), \quad \Gamma_{k'/k} = \mathrm{Gal}(k'/k). \tag{23}$$

When $K = k^{\mathrm{s}}$, we write $H^1(k, G)$ for $H^1(\Gamma, G(K))$. As before, a short exact sequence of Γ-modules gives rise to a six-term exact cohomology sequence.

LEMMA 3.44 (SHAPIRO'S LEMMA). *Let K be a finite extension of k, and let G be a smooth algebraic group over k. Then*

$$H^1(k, (G)_{K/k}) \simeq H^1(K, G).$$

PROOF. This can be proved by a direct calculation (Kneser 1969, 1.3). □

PROPOSITION 3.45. *Let*

$$e \to N \to G \to Q \to e$$

be an exact sequence of algebraic groups. If N is smooth, then there is an exact sequence

$$1 \to N(k) \to G(k) \to Q(k) \to H^1(k, N) \to H^1(k, G) \to H^1(k, Q).$$

PROOF. We have to show that

$$1 \to N(k^{\mathrm{s}}) \to G(k^{\mathrm{s}}) \to Q(k^{\mathrm{s}}) \to 1$$

is exact. Let $q \in Q(k^{\mathrm{s}})$, and regard it as an element of $|Q|$. The preimage P of q in G is a subscheme of G that becomes isomorphic to N over k^{a}. Therefore it is smooth, in particular, an algebraic variety, and so $P(k^{\mathrm{s}})$ is nonempty (A.48). □

PROPOSITION 3.46. *For all n, $H^1(k, \mathrm{GL}_n) = H^1(k, \mathrm{SL}_n) = H^1(k, \mathrm{Sp}_n) = 1$.*

PROOF. These follow from the corresponding statements for finite extensions using (23). □

COROLLARY 3.47. *For all n, $H^1(k, (\mathbb{G}_m)^n) = 1$.*

PROOF. As cohomology commutes with finite products and $\mathrm{GL}_1 = \mathbb{G}_m$, this follows from the proposition. □

REMARK 3.48. Let (V, q) be a nondegenerate quadratic space over a field k of characteristic $\neq 2$. Then $H^1(k, O(q))$ classifies the isomorphism classes of nondegenerate quadratic spaces over k with the same dimension $\dim(V)$. Indeed, all nondegenerate quadratic spaces over k of dimension $\dim(V)$ become isomorphic over k^s.

REMARK 3.49. (a) Theorem 3.43 holds also for infinite Galois extensions K/k. This can be proved by passing to the limit in 3.43 over the finite Galois extensions k' of k contained in K. Specifically, let G be a K/k-form of G_0. This means that there exists an isomorphism $f: G_K \to G'_K$. When we choose f to be defined over a finite extension of k inside K, then the cocycle $a_\sigma = f^{-1} \circ \sigma f$ is continuous, and so it defines an element of $H^1(\Gamma, \mathcal{A}(K))$.

(b) Theorem 3.43 also holds for nonaffine algebraic groups. The proof of this uses that all algebraic groups are quasi-projective (B.38).

PROPOSITION 3.50. *If G is smooth, then $H^1(k, G)$ classifies the isomorphism classes of G-torsors over k.*

PROOF. Let S be a G-torsor. As G is smooth and nonempty, S is smooth and nonempty, and so $S(k^s)$ is nonempty. Let $s \in S(k^s)$. For $\sigma \in \Gamma$, we can write $\sigma s = s \cdot a_\sigma$ with $a_\sigma \in G(k^s)$. Then $\sigma \mapsto a_\sigma$ is a continuous crossed homomorphism $\Gamma \to G(k^s)$, and the map sending S to the class of (a_σ) in $H^1(k, G)$ gives the required bijection. □

Thus, $H^1(k, G) \simeq H^1_{\mathrm{flat}}(k, G)$ when G is smooth.

Inner and outer forms

3.51. Let G be an algebraic group over k. An automorphism of G is **inner** if it becomes of the form $\mathrm{inn}(g)$ over k^a. Later (17.63), we shall see that the group $\mathcal{I}(k)$ of inner automorphisms of G is equal to $\bar{G}(k)$, where $\bar{G}$ is the quotient of G by its centre. For example, for $t \in k^\times$, the automorphism $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & tb \\ t^{-1}c & d \end{smallmatrix}\right)$ of SL_2 is inner because it becomes the inner automorphism defined by $\mathrm{diag}(\sqrt{t}, \sqrt{t^{-1}})$ over k^a. It is also the inner automorphism defined by the element $\mathrm{diag}(t, 1)$ of $\mathrm{PGL}_2(k)$.

3.52. Let K/k be a Galois extension with Galois group Γ, and let $\mathcal{I}(K) \subset \mathcal{A}(K)$ be the group of inner automorphisms of G_{0K}. An **inner K/k-form** of G_0 is a pair (G, f), where G is an algebraic group over k and f is an isomorphism $f: G_{0K} \to G_K$ such that the automorphism $a_\sigma \stackrel{\text{def}}{=} f^{-1} \circ \sigma f$ of G_0 is inner for all $\sigma \in \Gamma$. Two inner forms (G, f) and (G', f') are said to be **equivalent** if there exists an isomorphism $\varphi: G \to G'$ (over k) such that $f' = \varphi_K \circ f$. The equivalence classes of inner forms are classified by $H^1(\Gamma, \mathcal{I}(K))$.

More loosely, we say that a K/k-form G over G_0 is **inner** if it is possible to choose the isomorphism $f: G_{0K} \to G_K$ to satisfy the condition in

the preceding paragraph. Otherwise, we say that the form is ***outer***. A K/k-form is inner or outer according as its cohomology class lies in the image of $H^1(\Gamma, \mathcal{I}(K)) \to H^1(\Gamma, \mathcal{A}(K))$ or not. We caution the reader that, with this definition, the isomorphism classes of inner K/k-forms of G_0 are classified, not by $H^1(\Gamma, \mathcal{I}(K))$, but by the image of this set in $H^1(\Gamma, \mathcal{A}(K))$.

Exercises

EXERCISE 3-1. For a set X, let $R(X)$ denote the k-algebra of maps $X \to k$. For a second set Y, let $R(X) \otimes R(Y)$ act on $X \times Y$ according to the rule $(f \otimes g)(x, y) = f(x)g(y)$.

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

(b) Let Γ be a group and define maps

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

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

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

EXERCISE 3-2. We use the notation of Exercise 3-1. Let Γ be an arbitrary group. From a homomorphism $\rho: \Gamma \to \mathrm{GL}_n(k)$, we obtain a family of functions $g \mapsto \rho(g)_{i,j}$, $1 \le i, j \le n$, on G. Let $R'(\Gamma)$ be the k-subspace of $R(\Gamma)$ spanned by the functions arising in this way for varying n. (The elements of $R'(\Gamma)$ are called the ***representative functions*** on Γ.)

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

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

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

EXERCISE 3-3. Let (A, Δ, S, ϵ) be a Hopf algebra. Prove the following statements by interpreting them as statements about algebraic groups.

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

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

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

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

EXERCISE 3-4. Let A be a product of copies of k indexed by the elements of a finite set S. Show that the k-bialgebra structures on A are in natural one-to-one correspondence with the group structures on S.

EXERCISE 3-5. Let G be an affine algebraic group over a nonperfect field k. Show that G_{red} is an algebraic subgroup of G if $G(k)$ is dense in G (as a scheme).

EXERCISE 3-6. Let $A \to B$ be faithfully flat and M an A-module. If $B \otimes_A M$ is finitely generated over B, show that M is finitely generated. [Choose generators $1 \otimes m_1, \dots, 1 \otimes m_n$ for $B \otimes_A M$, and let N be the A-submodule of M generated by the m_i. Now $B \otimes_A N = B \otimes_A M$ and so $N = M$.]

EXERCISE 3-7. Show that a Hopf algebra B is finitely generated as a k-algebra if its augmentation ideal is finitely generated.

EXERCISE 3-8. Show that every Hopf subalgebra A of a finitely generated Hopf algebra B is finitely generated. [The ideal $I_A B$ in B is finitely generated, and it equals $I_A \otimes_A B$ by flatness. Apply Exercise 3-6.]

EXERCISE 3-9. Let G be an affine group scheme over k (not necessarily of finite type). If there exists a faithfully flat homomorphism $H \to G$ with H an affine algebraic group over k, then G is algebraic.

Linear Representations of Algebraic Groups

Throughout this chapter, G is an affine algebraic group over a field k. We shall see later (8.36) that every algebraic group G over k has a largest affine algebraic quotient G^{aff}. As every linear representation of G factors through G^{aff}, no extra generality would result from allowing G to be nonaffine.

a. Representations and comodules

For a vector space V over k, we let GL_V denote the functor of k-algebras,

$$R \rightsquigarrow \mathrm{Aut}(V_R) \quad (R\text{-linear automorphisms}).$$

When V is finite-dimensional, GL_V is an algebraic group.

A **linear representation** of G is a homomorphism $r\colon G \to \mathrm{GL}_V$ of group-valued functors. When V is finite-dimensional, r is a homomorphism of algebraic groups. A linear representation r is **faithful** if $r(R)\colon G(R) \to \mathrm{Aut}_{R\text{-linear}}(V_R)$ is injective for all k-algebras R. For finite-dimensional linear representations, this is equivalent to ρ being a closed immersion (3.35). A representation is **trivial** if $r(G) = e$. From now on we write "representation" for "linear representation".[1]

To give a representation (V, r) of G on V is the same as giving an action

$$G \times V_{\mathfrak{a}} \to V_{\mathfrak{a}}$$

of G on the functor $V_{\mathfrak{a}}$ such that, for all k-algebras R, the group $G(R)$ acts on $V_{\mathfrak{a}}(R) = R \otimes V$ through R-linear maps. When viewed in this way, we call (V, r) a G-**module.**

---

[1] A nonlinear representation would be a homomorphism $G \to \mathrm{Aut}(V_{\mathfrak{a}})$ (automorphisms of the k-scheme $V_{\mathfrak{a}}$ ignoring its linear structure). In the old literature a group variety is identified with its k^{a}-points, and the representations in our sense are called rational representations to distinguish them from the representations of the abstract group $G(k^{\mathrm{a}})$.

A (right) $\mathcal{O}(G)$-**comodule** is a k-linear map $\rho\colon V \to V \otimes \mathcal{O}(G)$ such that

$$\begin{cases} (\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_{\mathcal{O}(G)}) \circ \rho \\ (\mathrm{id}_V \otimes \epsilon) \circ \rho = \mathrm{id}_V. \end{cases} \tag{24}$$

The map ρ is called the **co-action**. Let (V, ρ) be an $\mathcal{O}(G)$-comodule. An $\mathcal{O}(G)$-**subcomodule** of V is a k-subspace W such that $\rho(W) \subset W \otimes \mathcal{O}(G)$. Then $(W, \rho|W)$ is again an $\mathcal{O}(G)$-comodule.

REMARK 4.1. Let $A = \mathcal{O}(G)$. A representation $r\colon G \to \mathrm{GL}_V \subset \mathrm{End}_V$ of G maps the universal element a in $G(A)$ to an A-linear endomorphism $r(a)$ of $\mathrm{End}(V \otimes A)$, which is uniquely determined by its restriction to a k-linear homomorphism $\rho\colon V \to V \otimes A$. The map ρ is an A-comodule structure on V, and in this way we get a one-to-one correspondence $r \leftrightarrow \rho$ between the representations of G on V and the A-comodule structures on V.

To see this, let $(e_i)_{i \in I}$ be a basis for V and let $(a_{ij})_{i,j \in I}$ be a family of elements of A. When I is infinite, we require that, for each j, only finitely many a_{ij} are nonzero. The map

$$\rho\colon V \to V \otimes A, \quad e_j \mapsto \sum_{i \in I} e_i \otimes a_{ij} \quad \text{(finite sum)},$$

is a comodule structure on V if and only if

$$\left. \begin{array}{l} \Delta(a_{ij}) = \sum_{l \in I} a_{il} \otimes a_{lj} \\ \epsilon(a_{ij}) = \delta_{ij} \end{array} \right\} \quad \text{all } i, j \in I. \tag{25}$$

On the other hand, the maps sending $g \in G(R)$ to the automorphism of V_R with matrix $(a_{ij}(g))_{i,j \in I}$ for all k-algebras R constitute a representation r of G on V if and only if the equalities (25) hold. For example, if the first equality holds, then

$$a_{ij}(g_1 g_2) \overset{3.5}{=} (\Delta a_{ij})(g_1, g_2) = \left(\sum_l a_{il} \otimes a_{lj} \right)(g_1, g_2) = \sum_l a_{il}(g_1) \cdot a_{lj}(g_2),$$

and so $r(g_1 g_2) = r(g_1) \cdot r(g_2)$.

Suppose that I is finite, and let T_{ij} denote the regular function on End_V sending an endomorphism of V to its (i, j)th coordinate. Then $\mathcal{O}(\mathrm{End}_V)$ is a polynomial ring in the symbols T_{ij}, and the homomorphism $\mathcal{O}(\mathrm{End}_V) \to A$ defined by r sends T_{ij} to a_{ij}.

EXAMPLE 4.2. Let $G = \mathrm{GL}_n$ and let r be the standard representation of G on $V = k^n$. Then $\mathcal{O}(G) = k[T_{11}, T_{12}, \ldots, T_{nn}, 1/\det]$ and, relative to the standard basis $(e_i)_{1 \le i \le n}$ for V, the map $r\colon G(R) \to \mathrm{GL}_n(R)$ is (tautologically) $g \mapsto (T_{ij}(g))_{1 \le i, j \le n}$. The corresponding co-action is

$$\rho\colon V \to V \otimes \mathcal{O}(G), \quad e_j \mapsto \sum_{1 \le i \le n} e_i \otimes T_{ij}.$$

As $\Delta(T_{ij}) = \sum_{1 \le l \le n} T_{il} \otimes T_{lj}$ and $\epsilon(T_{ij}) = \delta_{ij}$, this does define a comodule structure on V.

b.   Stabilizers

PROPOSITION 4.3.   *Let $r: G \to \mathrm{GL}_V$ be a finite-dimensional representation of G and W a subspace of V. The functor*

$$R \rightsquigarrow G_W(R) = \{g \in G(R) \mid g(W_R) = W_R\}$$

is represented by an algebraic subgroup G_W of G.

PROOF.   Let $A = \mathcal{O}(G)$ and let $\rho: A \to V \otimes A$ be the co-action corresponding to r. 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

$$\rho(e_j) = \sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in A.$$

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

$$ge_j = \sum_{i \in J \sqcup I} e_i \otimes g(a_{ij}).$$

Thus, $g(W \otimes R) \subset W \otimes R$ if and only if $g(a_{ij}) = 0$ for $j \in J$, $i \in I$. As $g(a_{ij}) = (a_{ij})_R(g)$, this shows that the functor is represented by the quotient of A by the ideal generated by $\{a_{ij} \mid j \in J, i \in I\}$. $\qquad \square$

The subgroup G_W of G is called the ***stabilizer*** of W in V. It is also denoted $\mathrm{Stab}_G(W)$. We say that an algebraic subgroup H of G ***stabilizes*** a subspace W of V if it is contained in the stabilizer of W.

COROLLARY 4.4.   *Let (V, r) be a finite-dimensional representation of G, and let S be a subset of $G(k)$ that is dense in G (as a scheme). A subspace W of V is stable under G if and only if it is stable under S.*

PROOF.   The space W is stable under S if and only if $S \subset G_W(k)$. But, because S is schematically dense in G, this is so if and only if $G_W = G$, i.e., W is stable under G. $\qquad \square$

COROLLARY 4.5.   *Let H be an algebraic subgroup of G such that $H(k)$ is dense in H (as a scheme). If $hW = W$ for all $h \in H(k)$, then W is stable under H.*

PROOF.   Apply the last corollary with $(G, S) = (H, H(k))$. $\qquad \square$

PROPOSITION 4.6.   *Let G act on V and V', and let W and W' be nonzero subspaces of V and V'. Then the stabilizer of $W \otimes W'$ in $V \otimes V'$ is $G_W \cap G_{W'}$.*

PROOF.   Choose a basis for W (resp. W') and extend it to a basis for V (resp. V'). From these bases, we get a basis for $W \otimes W'$ and an extension of it to $V \otimes V'$. The proof of Proposition 4.3 now gives explicit generators for the ideals $\mathfrak{a}(W)$, $\mathfrak{a}(W')$, and $\mathfrak{a}(W \otimes W')$ defining $\mathcal{O}(G_W)$, $\mathcal{O}(G_{W'})$, and $\mathcal{O}(G_{W \oplus W'})$ as quotients of $\mathcal{O}(G)$, from which one can deduce that

$$\mathfrak{a}(W \otimes W') = \mathfrak{a}(W) + \mathfrak{a}(W'). \qquad \square$$

c.   Representations are unions of finite-dimensional representations

PROPOSITION 4.7.   *Every $\mathcal{O}(G)$-comodule (V,ρ) is a filtered union of its finite-dimensional subcomodules.*

PROOF.   A finite sum of finite-dimensional subcomodules is a finite-dimensional subcomodule, and so it suffices to show that each element v of V is contained in a finite-dimensional subcomodule. Let $(e_i)_{i \in I}$ be a basis for $\mathcal{O}(G)$ as a k-vector space, and let

$$\rho(v) = \sum_i v_i \otimes e_i, \quad v_i \in V, \quad \text{(finite sum)}.$$

Write

$$\Delta(e_i) = \sum_{j,k} r_{ijk}(e_j \otimes e_k), \quad r_{ijk} \in k.$$

We shall show that

$$\rho(v_k) = \sum_{i,j} r_{ijk}\left(v_i \otimes e_j\right) \tag{26}$$

from which it follows that the k-subspace of V spanned by v and the v_i is a subcomodule containing v. Recall from (24), p. 84, that

$$(\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_{\mathcal{O}(G)}) \circ \rho.$$

On applying each side of this equation to v, we find that

$$\sum_{i,j,k} r_{ijk}(v_i \otimes e_j \otimes e_k) = \sum_k \rho(v_k) \otimes e_k \quad \text{(inside } V \otimes \mathcal{O}(G) \otimes \mathcal{O}(G)\text{)}.$$

On comparing the coefficients of $1 \otimes 1 \otimes e_k$ in these two expressions, we obtain the equality (26). □

COROLLARY 4.8.   *Every representation of G is a filtered union of its finite-dimensional subrepresentations.*

PROOF.   Let $r\colon G \to \mathrm{GL}_V$ be a representation of G and $\rho\colon V \to V \otimes \mathcal{O}(G)$ the corresponding co-action. A subspace W of V is stable under G if and only if it is an $\mathcal{O}(G)$-subcomodule of V, and so this follows from the proposition. □

d.   Affine algebraic groups are linear

A right action of an algebraic group G on an algebraic scheme X is a regular map $X \times G \to X$ such that, for all k-algebras R, the map $X(R) \times G(R) \to X(R)$ is a right action of the group $G(R)$ on the set $X(R)$. Such an action defines a map

$$\rho\colon \mathcal{O}(X) \to \mathcal{O}(X) \otimes \mathcal{O}(G),$$

which makes $\mathcal{O}(X)$ into an $\mathcal{O}(G)$-comodule. This is the comodule corresponding to the representation of G on $\mathcal{O}(X)$,

$$(gf)(x) = f(xg), \quad g \in G(k), f \in \mathcal{O}(X), x \in X(k).$$

The representation of G on $\mathcal{O}(G)$ arising from $m: G \times G \to G$ is called the **regular representation**.[2] It corresponds to the co-action $\Delta: \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$.

THEOREM 4.9. *The regular representation has a faithful finite-dimensional subrepresentation. In particular, the regular representation itself is faithful.*

PROOF. Let $A = \mathcal{O}(G)$, and let V be a finite-dimensional subcomodule of A containing a set of generators for A as a k-algebra. Let $(e_i)_{1 \le i \le n}$ be a basis for V, and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. According to (4.1), the image of $\mathcal{O}(\mathrm{GL}_V) \to A$ contains the a_{ij}. But, because $\epsilon: A \to k$ is a co-identity (18),

$$e_j = (\epsilon \otimes \mathrm{id}_A) \Delta(e_j) = \sum_i \epsilon(e_i) a_{ij},$$

and so the image contains V; it therefore equals A. We have shown that the map $\mathcal{O}(\mathrm{GL}_V) \to A$ is surjective, which means that $G \to \mathrm{GL}_V$ is a closed immersion. $\square$

COROLLARY 4.10. *Every affine algebraic group is isomorphic to an algebraic subgroup of GL_n for some n.*

PROOF. A faithful representation $G \to \mathrm{GL}_V$ of G on a finite-dimensional vector space V realizes G as an algebraic subgroup of GL_V (3.35). Now choose a basis for V. $\square$

Thus every affine algebraic group can be realized as a group of matrices, and every multiplication map is just matrix multiplication in disguise.

REMARK 4.11. An algebraic group G is said to be **linear** if it admits a faithful finite-dimensional representation. Such a representation is an isomorphism of G onto a (closed) algebraic subgroup of GL_V (see 3.35), and so an algebraic group is linear if and only if it can be realized as an algebraic subgroup of GL_V for some finite-dimensional vector space V. Every linear algebraic group is affine (1.43), and the theorem shows that the converse is true. Therefore, the linear algebraic groups are exactly the affine algebraic groups.

---

[2]For an algebraic monoid G this is the *only* possible definition of a regular representation (in which G acts on the left). It is called the right regular representation. The left regular representation is $(gf)(x) = f(g^{-1}x)$.

e. Constructing all finite-dimensional representations

Let G be an algebraic group over k and V a finite-dimensional k-vector space. The k-vector space $V \otimes \mathcal{O}(G)$ equipped with the k-linear map

$$\mathrm{id}_V \otimes \Delta \colon V \otimes \mathcal{O}(G) \to V \otimes \mathcal{O}(G) \otimes \mathcal{O}(G)$$

is an $\mathcal{O}(G)$-comodule, called the ***free comodule on*** V. The choice of a basis for V realizes $(V \otimes \mathcal{O}(G), \mathrm{id}_V \otimes \Delta)$ as a direct sum of copies of $(\mathcal{O}(G), \Delta)$:

$$
\begin{array}{ccc}
V \otimes \mathcal{O}(G) & \xrightarrow{\;V \otimes \Delta\;} & V \otimes \mathcal{O}(G) \otimes \mathcal{O}(G) \\
\Big\downarrow{\simeq} & & \Big\downarrow{\simeq} \\
\mathcal{O}(G)^n & \xrightarrow{\;\Delta^n\;} & (\mathcal{O}(G) \otimes \mathcal{O}(G))^n.
\end{array}
$$

PROPOSITION 4.12. *Let (V, ρ) be an $\mathcal{O}(G)$-comodule. Let V_0 denote V regarded as a k-vector space and $(V_0 \otimes \mathcal{O}(G), \mathrm{id}_{V_0} \otimes \Delta)$ the free comodule on V_0. Then*

$$\rho \colon V \to V_0 \otimes \mathcal{O}(G)$$

is an injective homomorphism of $\mathcal{O}(G)$-comodules.

PROOF. The commutative diagram (see (24), p. 84)

$$
\begin{array}{ccc}
V & \xrightarrow{\;\rho\;} & V_0 \otimes \mathcal{O}(G) \\
\Big\downarrow{\rho} & & \Big\downarrow{\mathrm{id}_{V_0} \otimes \Delta} \\
V \otimes \mathcal{O}(G) & \xrightarrow{\;\rho \otimes \mathrm{id}_{\mathcal{O}(G)}\;} & V_0 \otimes \mathcal{O}(G) \otimes \mathcal{O}(G)
\end{array}
$$

says exactly that the map $\rho \colon V \to V_0 \otimes \mathcal{O}(G)$ is a homomorphism of $\mathcal{O}(G)$-comodules. It is injective because its composite with $\mathrm{id}_V \otimes \epsilon$ is id_V ((24), p. 84). $\square$

COROLLARY 4.13. *A finite-dimensional $\mathcal{O}(G)$-comodule (V, ρ) arises as a subcomodule of $(\mathcal{O}(G), \Delta)^n$ for $n = \dim V$.*

PROOF. Immediate consequence of the proposition and preceding remarks. $\square$

In other words, every finite-dimensional representation of G arises as a subrepresentation of a direct sum of copies of the regular representation.

THEOREM 4.14. *Let (V, r) be a faithful finite-dimensional representation of G. Then every finite-dimensional representation W of G can be constructed from V by forming tensor products, direct sums, duals, and subquotients.*

PROOF. After Proposition 4.12, we may assume that $W \subset \mathcal{O}(G)^n$ for some n. Let W_i be the image of W under the ith projection $\mathcal{O}(G)^n \to \mathcal{O}(G)$; then $W \hookrightarrow \bigoplus_i W_i$, and so we may even assume that $W \subset \mathcal{O}(G)$.

We choose a basis $(e_i)_{1 \le i \le n}$ for V, and use it to identify G with a subgroup of GL_n. Then there is a surjective homomorphism

$$\mathcal{O}(\mathrm{GL}_n) = k[T_{11}, T_{12}, \ldots, T_{nn}, 1/\det] \twoheadrightarrow \mathcal{O}(G) = k[t_{11}, t_{12}, \ldots, t_{nn}, 1/\det].$$

As W is finite-dimensional, it is contained in a subspace

$$\{f(t_{ij}) \mid \deg f \le s\} \cdot \det^{-s'}$$

of $\mathcal{O}(G)$ for some $s, s' \in \mathbb{N}$. This subspace is stable under GL_n, hence G, and it suffices to show that it can be constructed from V.

The natural representation of GL_n on V has co-action $\rho(e_j) = \sum e_i \otimes T_{ij}$ (see 4.2), and so the representation r of G on V has co-action $\rho(e_j) = \sum e_i \otimes t_{ij}$. For each i, the map

$$e_j \mapsto T_{ij} : (V, \rho) \to (\mathcal{O}(\mathrm{GL}_n), \Delta)$$

is a homomorphism of $\mathcal{O}(\mathrm{GL}_n)$-comodules (by (8), p. 41), and so the homogeneous polynomials of degree 1 in the T_{ij} form an $\mathcal{O}(\mathrm{GL}_n)$-comodule isomorphic to the direct sum of n copies of V. The $\mathcal{O}(\mathrm{GL}_n)$-comodule

$$\{f \in k[T_{11}, T_{12}, \ldots] \mid f \text{ homogeneous of degree } s\}$$

is a quotient of the s-fold tensor product of

$$\{f \in k[T_{11}, T_{12}, \ldots] \mid f \text{ homogeneous of degree } 1\}.$$

For $s = n$, this space contains the one-dimensional representation $g \mapsto \det(g)$, and its dual contains the dual one-dimensional representation $g \mapsto 1/\det(g)$. By summing various of these spaces, we get the space $\{f \mid \deg f \le s\}$, and by tensoring this s-times with $1/\det$ we get $\{f(T_{ij}) \mid \deg f \le s\} \cdot \det^{-s}$.   □

More precisely, the theorem says that W is a subquotient of a direct sum of representations $\bigotimes^m (V \oplus V^\vee)$, $m \in \mathbb{N}$. The dual was used only to construct the representation $1/\det$, and so it is not needed if $r(G) \subset \mathrm{SL}_V$.

Here is a more abstract statement of the proof of Theorem 4.14. Let (V, r) be a faithful representation of G of dimension n and W a second representation. We may realize W as a submodule of $\mathcal{O}(G)^m$ for some m. From r we get a surjective homomorphism $\mathcal{O}(\mathrm{GL}_V) \to \mathcal{O}(G)$. But

$$\mathcal{O}(\mathrm{GL}_V) = \mathrm{Sym}(\mathrm{End}_V)[1/\det],$$

and $\mathrm{End}_V \simeq V^\vee \otimes V$. The choice of a basis for $V^\vee$ determines an isomorphism $\mathrm{End}_V \simeq nV$ of GL_V-modules (cf. the above proof). Hence

$$\mathrm{Sym}(nV)^m \subset \mathcal{O}(\mathrm{GL}_V)^m \twoheadrightarrow \mathcal{O}(G)^m.$$

For some s, $W \cdot \det^s$ is contained in the image of $\mathrm{Sym}(nV)^m$ in $\mathcal{O}(G)^m$. This means that $W \cdot \det^s$ is contained in a quotient of some finite direct sum of tensor powers of V. We can now use that $(V^\vee)^{\otimes n}$ contains the representation $g \mapsto \det(g)^{-1}$ to complete the proof.

f.   Semisimple representations

DEFINITION 4.15. A representation of an algebraic group is *simple* if it is $\neq 0$ and its only subrepresentations are 0 and itself. It is *semisimple* if it is a sum of simple subrepresentations.[3]

PROPOSITION 4.16. *Every simple representation of an algebraic group is finite-dimensional.*

PROOF. Every simple representation contains a nonzero finite-dimensional sub-representation (4.8), and must equal it.   □

PROPOSITION 4.17. *Let (V,r) be a representation of an algebraic group G over k. If V is a sum of simple subrepresentations, say $V = \sum_{i \in I} S_i$ (the sum need not be direct), then for every subrepresentation W of V, there is a subset J of I such that*

$$V = W \oplus \bigoplus_{i \in J} S_i.$$

In particular, V is a direct sum of simple subrepresentations, and W is a direct summand of V.

PROOF. Let J be maximal among the subsets of I such that the sum $S_J = \sum_{j \in J} S_j$ is direct and $W \cap S_J = 0$. We claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). For this, it suffices to show that each S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals S_i or 0. In the first case, $S_i \subset W + S_J$, and in the second $S_J \cap S_i = 0$ and $W \cap (S_J + S_i) = 0$, contradicting the definition of I.   □

We have seen that if V is semisimple, then every subrepresentation W is a direct summand. The converse is also true. This can be proved by the same argument as for modules over a ring (Jacobson 1989, Theorem 3.10, p. 121).

REMARK 4.18. Let (V,r) be a finite-dimensional representation of an algebraic group G over k. By an endomorphism of (V,r) we mean a k-linear map $\alpha \colon V \to V$ such that $\alpha_R \colon V_R \to V_R$ commutes with the action of $G(R)$ on V_R for all small k-algebras R. Equivalently, it is an endomorphism of the corresponding comodule. If (V,r) is simple, then $\mathrm{End}(V,r)$ is a finite-dimensional division algebra D over k. If (V,r) is semisimple and $(V,r) = \bigoplus_i (V_i, r_i)^{s_i}$ is the decomposition of V into its isotypic components, then $\mathrm{End}(V,r) = \prod_i M_{s_i}(D_i)$ with $D_i = \mathrm{End}(V_i, r_i)$, which is semisimple.

PROPOSITION 4.19. *Let (V,r) be a finite-dimensional representation of an algebraic group G over k. Let k' be an extension of k, and let (V',r') be the representation $(V,r) \otimes k'$ of $G_{k'}$.*

---

[3]Traditionally, simple (resp. semisimple) representations of G are said to be irreducible (resp. completely reducible) when regarded as representations of G, and simple (resp. semisimple) when regarded as G-modules. I find this terminology clumsy and confusing, and so I follow DG, in using "simple" and "semisimple" for both.

(a) *If (V',r') is simple (resp. semisimple), then so also is (V,r).*

(b) *If (V,r) is simple and $\mathrm{End}(V,r) = k$, then (V',r') is simple.*

(c) *If (V,r) is semisimple and k' is a separable extension of k or $\mathrm{End}(V,r)$ is a separable algebra over k (i.e., semisimple with étale centre), then (V',r') is semisimple.*

PROOF. The proof is similar to that for representations of algebras (Bourbaki 1958, Chap. 8, §13, no. 4). Alternatively, when k is perfect, it can be deduced from the similar statement for algebras by using the correspondence between representations of G and its algebra of distributions (Section l of Chapter 10). $\square$

LEMMA 4.20 (SCHUR'S). *Let (V,r) be a representation of an algebraic group G. If (V,r) is simple and k is algebraically closed, then $\mathrm{End}(V,r) = k$.*

PROOF. Let $\alpha\colon V \to V$ be an endomorphism of (V,r). Because k is algebraically closed, α has an eigenvector, say, $\alpha(v) = av$, $a \in k$. Now $\alpha - a\colon V \to V$ is a G-homomorphism with nonzero kernel. Because V is simple, the kernel must equal V. Hence $\alpha = a$. $\square$

PROPOSITION 4.21. *Let G_1 and G_2 be algebraic groups over a field k. If (V_1,r_1) and (V_2,r_2) are simple representations of G_1 and G_2 and $\mathrm{End}(V_2,r_2) = k$, then $V_1 \otimes V_2$ is a simple representation of $G_1 \times G_2$. Moreover, every simple representation of $G_1 \times G_2$ is of this form if $\mathrm{End}(V,r) = k$ for all simple representations (V,r) of G_2.*

PROOF. Suppose that V_1 and V_2 are simple, and let W be a nonzero $G_1 \times G_2$-submodule of $V_1 \otimes V_2$. The choice of a basis for V_1 determines an isomorphism $V_1 \otimes V_2 \simeq V_2^d$ of G_2-modules. As $W \hookrightarrow V_2^d$ and V_2 is simple, W is also isomorphic to a direct sum of copies of V_2 as a G_2-module (4.17). Because $\mathrm{End}(V_2) = k$, the inclusion $W \hookrightarrow V_1 \otimes V_2$ is described by a matrix with coefficients in k, and linear algebra[4] now shows that we can choose the basis for V_1 so that the isomorphism $V_1 \otimes V_2 \simeq V_2^d$ maps W onto $V_2^e \subset V_2^d$ for some $e \le d$. This means that $W = V \otimes V_2$ for some nonzero vector subspace V of V_1. In fact, V is necessarily a G_1-submodule of V_1: any nonzero linear form f on V_2 induces a morphism of G_1-modules $\mathrm{id} \otimes f\colon V_1 \otimes V_2 \to V_1$, and the composite

$$W = V \otimes V_2 \to V_1 \otimes V_2 \to V_1$$

is then a morphism of G_1-modules with image V. As V_1 is simple, this implies that $V = V_1$, and so $W = V_1 \otimes V_2$.

For the proof of the converse statement (which we do not need), see Steinberg 1967, §12, when k is algebraically closed, and Zibrowius 2015, 4.1, in general. $\square$

---

[4]The choice of an isomorphism $W \to V_2^e$ and a basis for V_1 identifies $\mathrm{Hom}(W, V_1 \otimes V_2)$ with $M_{d,e}(k)$. The given inclusion $W \hookrightarrow V_1 \otimes V_2$ defines an element of $M_{d,e}(k)$, which can be put in row echelon form by changing the basis for V_1.

g.   Characters and eigenspaces

A **character**[5] of an algebraic group G over k is a homomorphism $G \to \mathbb{G}_m$. As $\mathcal{O}(\mathbb{G}_m) = k[T, T^{-1}]$ and $\Delta(T) = T \otimes T$, to give a character χ of G is the same as giving an invertible element $a = a(\chi)$ of $\mathcal{O}(G)$ such that $\Delta(a) = a \otimes a$; such an element is said to be **group-like**.

A character χ of G defines a representation r of G on a vector space V by the rule

$$r(g)v = \chi(g)v, \quad g \in G(R), v \in V_R.$$

In this case, we say that G acts on V **through the character** χ. In other words, G acts on V through the character χ if r factors through the centre $\mathbb{G}_m$ of GL_V as

$$G \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V. \tag{27}$$

For example, in

$$g \mapsto \begin{pmatrix} \chi(g) & & 0 \\ & \ddots & \\ 0 & & \chi(g) \end{pmatrix}, \quad g \in G(R),$$

G acts on k^n through the character χ. When V is one-dimensional, $\mathrm{GL}_V = \mathbb{G}_m$, and so G always acts on V through some character.

Let $r \colon G \to \mathrm{GL}_V$ be a representation of G and $\rho \colon V \to V \otimes \mathcal{O}(G)$ the corresponding co-action. Let χ be a character of G and $a(\chi)$ the corresponding group-like element of $\mathcal{O}(G)$. Then G acts on V through χ if and only if

$$\rho(v) = v \otimes a(\chi), \quad \text{all } v \in V. \tag{28}$$

More generally, we say that G acts on a subspace W of V **through a character** χ if W is stable under G and G acts on W through χ. Note that this means, in particular, that the elements of W are common eigenvectors for the $g \in G(k)$. If G acts on subspaces W and W' through a character χ, then it acts on $W + W'$ through χ. Therefore, there is a largest subspace V_χ of V on which G acts through χ, called the **eigenspace for G with character** χ.

PROPOSITION 4.22. *Let (V, r) be a representation of G and $\rho \colon V \to V \otimes \mathcal{O}(G)$ the corresponding co-action. For a character χ of G,*

$$V_\chi = \{v \in V \mid \rho(v) = v \otimes a(\chi)\}.$$

PROOF. The set $\{v \in V \mid \rho(v) = v \otimes a(\chi)\}$ is a subspace of V on which G acts through χ (by (28)), and it clearly contains every such subspace.   □

---

[5]In the old literature, a character in our sense is called a rational character to distinguish it from a character of the abstract group $G(k^a)$.

Let A be a Hopf algebra and a a group-like element of A. Then, from the second diagram in (17), p. 65, we see that

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

and so $\epsilon(a) = 1$.

PROPOSITION 4.23. *The group-like elements in A are linearly independent.*

PROOF. If not, it will be possible to express one group-like element e as a linear combination of group-like elements $e_i \neq e$:

$$e = \sum_i c_i e_i, \quad c_i \in k.$$

We may even suppose that the e_i occurring in the sum are linearly independent. Now

$$\Delta(e) = e \otimes e = \sum_{i,j} c_i c_j e_i \otimes e_j$$
$$\Delta(e) = \sum_i c_i \Delta(e_i) = \sum_i c_i e_i \otimes e_i.$$

The $e_i \otimes e_j$ are also linearly independent, and so this implies that

$$\begin{cases} c_i c_i = c_i & \text{all } i \\ c_i c_j = 0 & \text{if } i \neq j. \end{cases}$$

We also know that

$$1 = \epsilon(e) = \sum c_i \epsilon(e_i) = \sum c_i.$$

On combining these statements, we see that the c_i form a complete set of orthogonal idempotents in the field k, and so one of them equals 1 and the remainder are zero, which contradicts our assumption that e is not equal to any of the e_i. $\square$

COROLLARY 4.24. *Let G be an algebraic group. Distinct characters $\chi_1, \ldots, \chi_n$ of G are linearly independent.*

PROOF. Suppose that the sum $\sum c_i \chi_i$, $c_i \in k$, is the zero map $G \to \mathbb{A}^1$. Then $\sum c_i \cdot a(\chi_i) = 0$, and so each $c_i = 0$. $\square$

THEOREM 4.25. *Let $r : G \to \mathrm{GL}(V)$ be a representation of an algebraic group on a vector space V. If V is a sum of eigenspaces, say $V = \sum_{\chi \in \Xi} V_\chi$ with Ξ a set of characters of G, then it is a direct sum of the eigenspaces*

$$V = \bigoplus_{\chi \in \Xi} V_\chi.$$

PROOF. If the sum is not direct, then there exists a finite set $\{\chi_1, \ldots, \chi_m\}$, $m \geq 2$, and a relation
$$v_1 + \cdots + v_m = 0, \quad v_i \in V_{\chi_i}, \quad v_i \neq 0.$$

On applying ρ to this relation, we find that

$$0 = \rho(v_1) + \cdots + \rho(v_m) = v_1 \otimes a(\chi_1) + \cdots + v_m \otimes a(\chi_m).$$

For every linear map $f : V \to k$,

$$0 = f(v_1) \cdot a(\chi_1) + \cdots + f(v_m) \cdot a(\chi_m),$$

which contradicts the linear independence of the $a(\chi_i)$. □

Later (12.12) we shall show that if G is a product of copies of $\mathbb{G}_m$, then every representation is a sum of the eigenspaces.

Let H be an algebraic subgroup of an algebraic group G and χ a character of H. We say that χ *occurs in a representation* (V, r) of G if H acts on some nonzero subspace of V through χ.

PROPOSITION 4.26. *Let H, G, and χ be as above. If χ occurs in some representation of G, then it occurs in the regular representation.*

PROOF. After 4.13, χ occurs in $\mathcal{O}(G)^n$ for some n. Under some projection $\mathcal{O}(G)^n \to \mathcal{O}(G)$, this space maps to a nonzero subspace of $\mathcal{O}(G)$, on which H acts through χ. □

h. Chevalley's theorem

THEOREM 4.27 (CHEVALLEY). *Let G be an algebraic group. Every algebraic subgroup H of G arises as the stabilizer of a one-dimensional subspace L in a finite-dimensional representation (V, r) of G.*

PROOF. Let $\mathfrak{a}$ be the kernel of $\mathcal{O}(G) \to \mathcal{O}(H)$. According to Proposition 4.7, there exists a finite-dimensional k-subspace V of $\mathcal{O}(G)$ containing a generating set of $\mathfrak{a}$ as an ideal and such that

$$\Delta(V) \subset V \otimes \mathcal{O}(G).$$

Let $W = \mathfrak{a} \cap V$ in V. Let $(e_i)_{i \in J}$ be a basis for W, and extend it to a basis $(e_i)_{J \sqcup I}$ for V. Let

$$\Delta e_j = \sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

As in the proof of 4.3, $\mathcal{O}(G_W) = \mathcal{O}(G)/\mathfrak{a}'$, where $\mathfrak{a}'$ is the ideal generated by $\{a_{ij} \mid j \in J, i \in I\}$. Because $\mathcal{O}(G) \to \mathcal{O}(H)$ is a homomorphism of Hopf algebras

$$\Delta(\mathfrak{a}) \subset \mathcal{O}(G) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathcal{O}(G),$$
$$\epsilon(\mathfrak{a}) = 0$$

(see 3.11). The first of these applied to e_j, $j \in J$, shows that $\mathfrak{a}' \subset \mathfrak{a}$, and the second shows that

$$e_j = (\epsilon, \mathrm{id})\Delta(e_j) = \sum_{i \in I} \epsilon(e_i) a_{ij}.$$

As the e_j, $j \in J$, generate $\mathfrak{a}$ (as an ideal), so do the a_{ij}, $j \in J$, and so $\mathfrak{a}' = \mathfrak{a}$. Thus $H = G_W$. The next (elementary) lemma allows us to replace W with the one-dimensional subspace $\bigwedge^d W$ of $\bigwedge^d V$. □

LEMMA 4.28. *Let W be a subspace of dimension d in a vector space V and α an automorphism of V_R for some k-algebra R. Then $D \overset{\text{def}}{=} \bigwedge^d W$ is a one-dimensional subspace of $\bigwedge^d V$ and $\alpha W_R = W_R$ if and only if $(\bigwedge^d \alpha) D_R = D_R$.*

PROOF. Let $(e_j)_{1 \le j \le d}$ be a basis for W, and extend it to a basis $(e_i)_{1 \le i \le n}$ of V. Let $w = e_1 \wedge \ldots \wedge e_d$. For all k-algebras R,

$$W_R = \{v \in V_R \mid w \wedge v = 0 \ (\text{in } \textstyle\bigwedge^{d+1} V_R)\}.$$

To see this, let $v \in V_R$ and write $v = \sum_{i=1}^n a_i e_i$, $a_i \in R$. Then

$$w \wedge w = \sum_{d+1 \le i \le n} a_i e_1 \wedge \cdots \wedge e_d \wedge e_i.$$

As the elements $e_1 \wedge \cdots \wedge e_d \wedge e_i$, $d + 1 \le i \le n$, are linearly independent in $\bigwedge^{d+1} V$, we see that

$$w \wedge v = 0 \iff a_i = 0 \text{ for all } d + 1 \le i \le n.$$

Let $\alpha \in \mathrm{GL}(V_R)$. If $\alpha W_R = W_R$, then obviously $(\bigwedge^d \alpha)(D_R) = D_R$. Conversely, suppose that $(\bigwedge^d \alpha)(D_R) = D_R$, so that $(\bigwedge^d \alpha)w = cw$ for some $c \in R^\times$. If $v \in W_R$, then $w \wedge v = 0$, and so

$$0 = (\textstyle\bigwedge^{d+1} \alpha)(w \wedge v) = (\bigwedge^d \alpha)w \wedge \alpha v = c\,(w \wedge (\alpha v)),$$

which implies that $\alpha v \in W_R$. □

COROLLARY 4.29. *Let G be an algebraic group over k, and let H be an algebraic subgroup of G with the following property: whenever a character χ of H occurs in some representation of G, so also does $-m\chi$ for some $m > 0$. Then it is possible to choose the pair (V, L) in 4.27 so that H acts on L through the trivial character.*

PROOF. Let (V, L) be as in 4.27 and let χ be the character of H acting on L. Then H is the stabilizer of $L^{\otimes m}$ in $V^{\otimes m}$ (see 4.6). By assumption, there exists a representation (V', r') of G and a subspace W of V' such that H stabilizes W and acts on it through $-m\chi$. Now H is the stabilizer of $L^{\otimes m} \otimes W$ in $V^{\otimes m} \otimes W$ (see 4.6), and it acts on it through the character $m\chi - m\chi = 0$. Lemma 4.28 allows us to replace $L^{\otimes m} \otimes W$ with a one-dimensional subspace of a suitable exterior power of $V^{\otimes m} \otimes W$. □

REMARK 4.30. Theorem 4.27 is stronger than the usual form of the theorem (Borel 1991, 5.1; Springer 1998, 5.5.3) even when G and H are both group varieties because it implies that V and L can be chosen so that H is the stabilizer of L *in the sense of schemes*. This means that $H(R)$ is the stabilizer of L_R in V_R for *all* k-algebras R (see the definition p. 85). On applying this with $R = k[\varepsilon]$, $\varepsilon^2 = 0$, we find that $\mathrm{Lie}(H)$ is the stabilizer of L in $\mathrm{Lie}(G)$ – see 10.32 below.

i.   The subspace fixed by a group

Let G be an algebraic group and (V, r) a representation of G. We let V^G denote the subspace of V fixed by G:

$$V^G \overset{\text{def}}{=} \{v \in V \mid g \cdot v_R = v_R \ (\text{in } V_R) \text{ for all } k\text{-algebras } R \text{ and all } g \in G(R)\}.$$

PROPOSITION 4.31. *Let R be a k-algebra. The R-module $V^G \otimes R$ consists of the elements of $V \otimes R$ fixed by all elements of $G(R')$ with R' an R-algebra.*

PROOF. Let $v \in V \otimes R$ be fixed (in $V \otimes R'$) by all elements of $G(R')$ with R' an R-algebra. Let (e_i) be a basis for R as a k-vector space, and write $v = \sum_i v_i \otimes e_i$. It suffices to show that each $v_i \in V^G$. Let $g \in G(S)$ for some k-algebra S, and let g' be the image of g in $G(S \otimes R)$ under the map defined by $s \mapsto s \otimes 1_R \colon S \to S \otimes R$. By hypothesis, $\sum v_i \otimes 1_S \otimes e_i$ is fixed by g':

$$g' \cdot \left(\sum v_i \otimes 1_S \otimes e_i \right) = \sum v_i \otimes 1_S \otimes e_i.$$

But,

$$g' \cdot \left(\sum v_i \otimes 1_S \otimes e_i \right) = \sum g(v_i \otimes 1_S) \otimes e_i$$

and so $g(v_i \otimes 1_S) = v_i \otimes 1_S$ for all i. We have shown that the v_i satisfy the condition to lie in V^G.   □

PROPOSITION 4.32. *Let k' be an extension of k such that $G(k')$ is dense in G. Then*
$$V^G = V \cap V(k')^{G(k')}.$$

PROOF. Certainly, $V^G \subset W \overset{\text{def}}{=} V \cap V(k')^{G(k')}$. Conversely, the stabilizer G_W of W has the property that $G_W(k') = G(k')$, and so equals G.   □

For example, if G is a connected group variety over an infinite perfect field (3.17), or a group variety over a separably closed field (1.17), then
$$V^G = V(k)^{G(k)}.$$

PROPOSITION 4.33. *Let ρ be the co-action of (V, r). Then*
$$V^G = \{v \in V \mid \rho(v) = v \otimes 1 \text{ in } V \otimes \mathcal{O}(G)\}.$$

PROOF. This is the subspace fixed by the universal element $\mathrm{id} \in G(\mathcal{O}(G))$.   □

COROLLARY 4.34. *The formation of V^G commutes with extension of the base field:*

$$(V \otimes k')^{G_{k'}} \simeq V^G \otimes k',$$

for every field k' containing k.

PROOF. The condition in the proposition is linear. □

REMARK 4.35. We can regard the action of G on the vector space V as an action of G on the algebraic scheme $V_{\mathfrak{a}}$ (notation as in 2.6). Then 4.31 shows that

$$(V^G)_{\mathfrak{a}} = (V_{\mathfrak{a}})^G.$$

Exercises

EXERCISE 4-1. Let G be a connected algebraic group over a field k of characteristic zero, and let H be an algebraic subgroup of G. Show that H is normal in G if and only if, for every representation (V, r) of G and character $\chi \in X(H)$, the eigenspace V_χ is stable under G. [Use 4.27.]

EXERCISE 4-2. Let G be an algebraic group over k and H a normal algebraic subgroup of G. From a representation (V, r) of H and a $g \in G(k)$, we get a conjugate representation $h \mapsto r(ghg^{-1})$ of H. Assume that $G(k)$ is schematically dense in G, and let (V, r) be a simple representation of G. Show that $r|H$ is semisimple and that all of its simple constituents are conjugate and have the same multiplicity (Clifford's theorem; see Jacobson 1989, Section 5.2).

EXERCISE 4-3. Let (V, r) be a representation of an algebraic group G over k, and suppose that $\pi_0(G)$ has order prime to char(k). Show that r is semisimple if its restriction to G° is semisimple (extension of Maschke's theorem; see 22.43 below).

Group Theory; the Isomorphism Theorems

In this chapter, we develop some basic group theory. In particular, we show that the Noether isomorphism theorems hold for algebraic groups over a field.

a.   The isomorphism theorems for abstract groups

For reference, we state the isomorphism theorems for abstract groups.

5.1. (Existence of quotients). The kernel of a homomorphism $G \to H$ of groups is a normal subgroup, and every normal subgroup N of G arises as the kernel of a surjective homomorphism $G \to G/N$.

5.2. (Homomorphism theorem). Every homomorphism $\varphi: G \to H$ of groups factors as a composite of homomorphisms

$$G \xrightarrow{q} I \xrightarrow{i} H$$

with q surjective and i injective.

5.3. (Isomorphism theorem). Let H and N be subgroups of G such that H normalizes N. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and the map

$$x(H \cap N) \mapsto xN: H/(H \cap N) \to (HN)/N$$

is an isomorphism.

5.4. (Correspondence theorem). Let N be a normal subgroup of a group G. The map $H \mapsto H/N$ is a bijection from the set of subgroups of G containing N

to the set of subgroups of G/N. A subgroup H containing N is normal in G if and only if H/N is normal in G/N, in which case the natural map

$$G/H \to (G/N)/(H/N)$$

is an isomorphism.

In fact, $H \mapsto H/N$ is an isomorphism from the lattice of subgroups of G containing N to the lattice of subgroups of G/N. With this addendum, 5.4 is often called the lattice theorem.

b. Quotient maps

DEFINITION 5.5. A homomorphism of algebraic groups is a ***quotient map*** if it is faithfully flat.

Thus a homomorphism is a quotient map if it is both flat and surjective. Not every surjective homomorphism is flat. For example, the homomorphism $e \to \alpha_p$ is surjective but not flat. More generally, if G is a nonreduced algebraic group such that G_{red} is an algebraic subgroup, then the homomorphism $G_{\mathrm{red}} \to G$ is surjective but not flat. In these examples, the target group is not reduced – when H is reduced, every surjective homomorphism $G \to H$ is flat (1.70) and hence a quotient map.

For example, for $n \neq 0$, the homomorphism $t \mapsto t^n \colon \mathbb{G}_m \to \mathbb{G}_m$ is a quotient map because it is surjective and $\mathbb{G}_m$ is reduced (it is surjective because it is surjective on k^{a}-points). Note that $\mathbb{G}_m(R) \to \mathbb{G}_m(R)$ need not be surjective because the elements of $R^\times$ need not be nth powers.

DEFINITION 5.6. Let F be a functor from small k-algebras to sets. A subfunctor D of F is **fat** if, for every R and $x \in F(R)$, there exists a faithfully flat R-algebra R' such that the image x' of x in $F(R')$ lies in $D(R')$.

For example, the functor $R \rightsquigarrow R^{\times n}$ is fat in $R \rightsquigarrow R^\times$ because an $a \in R^\times$ becomes an nth power in $R[T]/(T^n - a)$, which is faithfully flat over R.

PROPOSITION 5.7. *Let* $\varphi \colon X \to Y$ *be a faithfully flat morphism of algebraic schemes over* k. *The subfunctor* $R \rightsquigarrow \varphi(X(R))$ *of* $\tilde{Y}$ *is fat.*

PROOF. Let R be a k-algebra, and let $y \in Y(R)$. Write $X \times_Y \mathrm{Spm}(R)$ as a finite union of open affine subschemes U_i. Let $R_i = \mathcal{O}(U_i)$, and let $R' = \prod_i R_i$. We have a diagram

$$
\begin{array}{ccccc}
X & \longleftarrow & X \times_Y \mathrm{Spm}(R) & \longleftarrow & \bigsqcup_i U_i = \mathrm{Spm}(R') \\
\downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \text{faithfully flat}} & & \\
Y & \xleftarrow{\;\;y\;\;} & \mathrm{Spm}(R) & &
\end{array}
$$

in which $\mathrm{Spm}(R') \to \mathrm{Spm}(R)$ is faithfully flat. The diagram provides a lifting of the image of y in $Y(R')$ to $X(R')$. □

PROPOSITION 5.8. *Let $\varphi\colon X \to Y$ be a morphism of algebraic schemes over k such that the subfunctor $R \rightsquigarrow \varphi(X(R))$ of $\tilde{Y}$ is fat. If the first projection $X \times_Y X \to X$ is faithfully flat, then so also is φ.*

PROOF. Let U be an open affine subscheme of Y, and let $X_U = X \times_Y U$. By hypothesis, there exists a faithfully flat map $U' \to U$ such that the composite $U' \to U \to Y$ lifts to a map $U' \to X$ (and hence $U' \to U$ lifts to a map $U' \to X_U$). Consider the diagram with cartesian squares:

$$
\begin{array}{ccccc}
X_U & \longleftarrow & X_U \times_U X_U & \longleftarrow & U' \times_U X_U \\
\downarrow{\scriptstyle \varphi_U} & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi''} \\
U & \longleftarrow & X_U & \longleftarrow & U'.
\end{array}
$$

The map φ' is faithfully flat because it is the pull-back of $X \times_Y X \to X$ by $U \hookrightarrow Y$. Hence φ'' is faithfully flat, and this implies that φ_U is faithfully flat (because $U' \to U$ is faithfully flat; apply A.80). As this is true for all U, it follows that φ is faithfully flat.   □

LEMMA 5.9. *Let $R \to R'$ be a faithfully flat homomorphism of k-algebras, and let X be an algebraic k-scheme. Then the sequence*

$$
X(R) \longrightarrow X(R') \rightrightarrows X(R' \otimes_R R')
$$

is exact. (The maps in the pair are induced by the maps $r \mapsto 1 \otimes r$ and $r \mapsto r \otimes 1$.)

PROOF. The sequence

$$
R \longrightarrow R' \rightrightarrows R' \otimes_R R'
$$

is exact (CA 11.12). Hence, for any k-algebra A, the sequence

$$
\mathrm{Hom}(A, R) \longrightarrow \mathrm{Hom}(A, R') \rightrightarrows \mathrm{Hom}(A, R' \otimes_R R')
$$

is exact. This implies the lemma when X is affine, and the general case is proved by covering X with open affine subschemes.   □

PROPOSITION 5.10. *Let X and Y be algebraic schemes over k, and let D be a fat subfunctor of $\tilde{X}$. Every map of functors $\varphi\colon D \to \tilde{Y}$ extends uniquely to a map of functors $\tilde{X} \to \tilde{Y}$ (hence to a map of schemes $X \to Y$ by the Yoneda lemma).*

PROOF. Let $x \in X(R)$, and let $R \to R'$ be a faithfully flat map such that the image x' of x in $X(R')$ lies in $D(R')$. There is a commutative diagram

$$
\begin{array}{ccccc}
X(R) & \longrightarrow & X(R') & \rightrightarrows & X(R' \otimes_R R') \\
\vdots\,\downarrow{\scriptstyle \varphi} & & \vdots\,\downarrow{\scriptstyle \varphi} & & \vdots\,\downarrow{\scriptstyle \varphi} \\
Y(R) & \longrightarrow & Y(R') & \rightrightarrows & Y(R' \otimes_R R')
\end{array}
$$

with exact rows (the dashed arrows are defined only on the subset $D(-)$ of $X(-)$).
From the diagram, we see that $\varphi(x')$ is the image of a unique element of $Y(R)$,
which we denote $\tilde{\varphi}(x)$. One checks easily that $\tilde{\varphi}(x)$ is independent of the choice
of R'. Thus we have a map $x \mapsto \tilde{\varphi}(x)$ extending $\varphi(R)$ to $X(R)$. These maps for
varying R form a morphism of functors $\tilde{X} \to \tilde{Y}$ extending φ.　　□

COROLLARY 5.11. *Let X and X' be algebraic schemes over k and D and D'
fat subfunctors of $\tilde{X}$ and $\tilde{X}'$ respectively. Every isomorphism $D \to D'$ extends
uniquely to an isomorphism $X \to X'$.*

PROOF. Immediate consequence of the proposition.　　□

PROPOSITION 5.12. *Let X be an algebraic scheme over k and D a fat subfunc-
tor of $\tilde{X}$. Every group structure on D extends uniquely to a group structure on
X.*

PROOF. Let $m: D \times D \to D$ be a group structure on D. The subfunctor $D \times D$
of $\tilde{X} \times \tilde{X}$ is fat, and so m extends uniquely to a map of functors $\tilde{m}: \tilde{X} \times \tilde{X} \to \tilde{X}$.
By assumption, there exist maps $e: * \to D$ and $\mathrm{inv}: D \to D$ making the diagrams
in 1.1 commute for D. These maps extend uniquely to $\tilde{X}$ and make the similar
diagrams commute. Now $\tilde{X}$ is a functor to groups, and so (X, m) is an algebraic
group.　　□

THEOREM 5.13. *Let $q: G \to Q$ be a quotient map of algebraic groups over k,
and let N be the kernel. Every homomorphism $\varphi: G \to H$ whose kernel contains
N factors uniquely through q:*

$$
\begin{array}{ccc}
G & \xrightarrow{\ q\ } & Q \\
 & {\scriptstyle\varphi}\searrow & \big\downarrow{\scriptstyle\exists!} \\
 & & H.
\end{array}
$$

PROOF. Let D denote the functor $R \rightsquigarrow G(R)/N(R)$. By assumption, the functor
$\tilde{\varphi}: \tilde{G} \to \tilde{H}$ factors through D,

$$
\tilde{\varphi} = \left(\tilde{G} \to D \xrightarrow{\ \varphi_0\ } \tilde{H} \right).
$$

As D is a fat subfunctor of Q, the map φ_0 arises from a unique morphism
$\varphi': Q \to H$. This makes the diagram commute, and it is a homomorphism
because φ_0 is a homomorphism of group functors.　　□

　　It follows that a quotient map $q: G \to Q$ is uniquely determined by its kernel
N up to a unique isomorphism. We denote any such map by $q: G \to G/N$ and
call G/N the ***quotient*** of G by N.

NOTES. In DG, III, §1, 1.4, a subfunctor D of a functor F is said to be dodu[1] if, for every small R and $x \in F(R)$, there exists a finite faithfully flat family of R-algebras $(R_i)_{i \in I}$ such that the image x_i of x in $F(R_i)$ lies in $D(R_i)$ for all i. Clearly a fat subfunctor is dodu, and a dodu subfunctor of $\tilde{X}$ is fat if $D(\prod R_i) \to \prod D(R_i)$ is surjective for all finite families (R_i) of k-algebras.

c.   Existence of quotients

The kernel of a homomorphism of algebraic groups is obviously normal. Less obvious is that every normal algebraic subgroup is the kernel of a quotient map.

THEOREM 5.14. *Every normal algebraic subgroup N of an algebraic group G arises as the kernel of a quotient map $G \to Q$.*

Affine case

LEMMA 5.15. *Let N be an algebraic subgroup of an algebraic group G, and let (V, r) be a representation of G. If N is normal in G, then V^N is stable under G.*

PROOF. Let $v \in V^N \otimes R$, let $g \in G(R)$ for some R, and let $n \in N(R')$ for some R-algebra R'. Then

$$n(g \cdot v)_{R'} = (ng) \cdot v_{R'} = (gn') \cdot v_{R'} = g(n' \cdot v_{R'}) = g \cdot v$$

because $n' \stackrel{\text{def}}{=} g^{-1}ng \in N(R')$. According to Proposition 4.31, this implies that $g \cdot v \in V^N \otimes R$, as required.   □

LEMMA 5.16. *Let H be a normal algebraic subgroup of an affine algebraic group G over an algebraically closed field k. If a character χ of H occurs in a representation of G, then so also does $-m\chi$ for some $m > 0$.*

PROOF. Let χ be a character of H occurring in a representation (V, r) of G. It suffices to show that there exists a representation (W, r_W) of G and a one-dimensional subspace L_1 in W such that (a) H acts on L_1 through $m\chi$ and (b) L_1 is a direct summand of W as an H-module, because then $L_1^\vee$ is a direct summand of $W^\vee$ as an H-module and H acts on it through $-m\chi$.

Suppose first that $G(k)$ is dense in G (as a scheme). By assumption, there is a line L in V on which H acts through χ. Let W be the sum of all one-dimensional subspaces in V stable under H. If D is such a subspace D, then gD is stable under $gHg^{-1} = H$ for all $g \in G(k)$. Therefore W is stable under $G(k)$, and hence under G (see 4.5). As W is a sum of simple representations of H, Proposition 4.17 shows that L is a direct summand of W as an H-module.

We now prove the general case. We may suppose that G has characteristic $p \neq 0$. There exists an $r > 0$ such that the image I of $F^r : G \to G^{(p^r)}$ is smooth (see 3.30). The group H acts on the line $L^{\otimes p^r}$ in $V^{\otimes p^r}$ through $p^r \chi$, and

---

[1]Larousse: dodu adj. Se dit d'un animal gras, bien en chair.

the functoriality of the Frobenius map implies that $p^r \chi$ factors through the quotient $H^{(p^r)}$ of H. Let N denote the kernel of $F^n : G \to G^{(p^r)}$. Then $L^{\otimes p^r} \subset (V^{\otimes p^r})^N$ and G acts on $(V^{\otimes p^r})^N$ through its quotient I. The sum of the one-dimensional subspaces in $(V^{\otimes p^r})^N$ stable under H is stable under $I(k)$, hence under I and G, and contains $L^{\otimes p^r}$ as a direct summand. □

LEMMA 5.17. *Let G be an affine algebraic group over an algebraically closed field k. Every normal algebraic subgroup N of G is the kernel of a representation of G.*

PROOF. According to 4.29 and 5.16, it is possible to choose the pair (V, L) in Chevalley's theorem (4.27) so that N acts on L through the trivial character. Because N is normal, G stabilizes V^N (see 5.15). The kernel of the representation of G on V^N obviously contains N, but as it stabilizes L, it must also be contained in N. □

PROPOSITION 5.18. *Every normal algebraic subgroup N of an affine algebraic group G is the kernel of a quotient map $G \to Q$ with Q affine.*

PROOF. Lemma 5.17 shows that $N_{k'}$ is the kernel of a homomorphism $\alpha : G_{k'} \to H_{k'}$ for some extension k' of k, which we may choose to be finite. Let β be the composite of the homomorphisms

$$G \xrightarrow{i_G} (G)_{k'/k} \xrightarrow{(\alpha)_{k'/k}} (H)_{k'/k}$$

(notation as in 2.56). On a k-algebra R, these homomorphisms become

$$G(R) \xrightarrow{i_G(R)} G(R') \xrightarrow{\alpha(R')} H(R'), \quad R' = k' \otimes R,$$

where $i_G(R)$ is induced by the natural inclusion $R \to R'$. The map $i_G(R)$ is injective because $R \to R'$ is faithfully flat, and so

$$\mathrm{Ker}(\beta(R)) = G(R) \cap N(R') = N(R).$$

Hence N is the kernel of the homomorphism $\beta : G \to (H)_{k'/k}$. Factor β as in 3.34: $\beta = (G \xrightarrow{q} I \xrightarrow{i} H)$ with q faithfully flat and i a closed immersion. Then q is a quotient map with kernel N. □

This proves Theorem 5.14 for an affine G.

COROLLARY 5.19. *Every normal algebraic subgroup N of an affine algebraic group G is the kernel of a representation of G.*

PROOF. Let N be the kernel of a quotient map $G \to Q$ with Q affine. Now choose a faithful representation of Q (which exists by 4.9). □

General case

First we need the notion of a quotient with respect to a nonnormal subgroup.

DEFINITION 5.20. Let H be an algebraic subgroup of an algebraic group G over k. A ***quotient*** of G by H is an algebraic scheme X equipped with an action $\mu: G \times X \to X$ of G and a point $o \in X(k)$ such that, for all small k-algebras R,

(a) the nonempty fibres of the map $g \mapsto go: G(R) \to X(R)$ are the cosets of $H(R)$ in $G(R)$;

(b) each element of $X(R)$ lifts to an element of $G(R')$ for some faithfully flat R-algebra R'.

In other words, (X, μ, o) is a quotient of G by H if the orbit map $\mu_o: G \to X$, $g \mapsto go$, realizes $\tilde{G}/\tilde{H}$ as a fat subfunctor of $\tilde{X}$.

PROPOSITION 5.21. *Let (X, μ, o) be a quotient of G by H, and let $\varphi: G \to X'$ be a morphism of schemes over k. If $\varphi(R)$ is constant on the cosets of $H(R)$ in $G(R)$ for all small k-algebras R, then φ factors uniquely through $\mu_o: G \to X$.*

$$\begin{array}{ccc} G & \xrightarrow{\mu_o} & X \\ & \searrow{\varphi} & \big\downarrow \\ & & X'. \end{array}$$
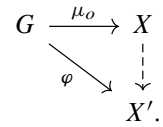
PROOF. By assumption $\tilde{\varphi}: \tilde{G} \to \tilde{X}'$ factors uniquely through $\tilde{G}/\tilde{H}$. Because $\tilde{G}/\tilde{H}$ is fat in $\tilde{X}$, the resulting map $\tilde{G}/\tilde{H} \to \tilde{X}'$ extends uniquely to a map of schemes $X \to X'$ (see 5.10). □

PROPOSITION 5.22. *Let (X, μ, o) be a quotient of G by H. Let X' be a scheme on which G acts, and let o' be a point of $X'(k)$ fixed by H. There is a unique G-equivariant map $X \to X'$ making the diagram at right commute:*

$$\begin{array}{ccc} G & \xrightarrow{g \mapsto go} & X \\ & \searrow{g \mapsto go'} & \big\downarrow \\ & & X'. \end{array}$$
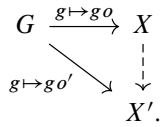
PROOF. The orbit map $g \mapsto go': G \to X'$ is constant on the cosets of H in G, and so this follows from Proposition 5.21. □

Thus, when it exists, the quotient (X, μ, o) of G by H is uniquely determined up to a unique isomorphism. We denote X by G/H and (loosely) call it the quotient of G by H.

PROPOSITION 5.23. *Let G/H be the quotient of G by H. Then*

$$\dim G = \dim H + \dim G/H.$$

PROOF. We may suppose that k is algebraically closed. Then we may pass to the associated reduced schemes, and apply A.72. □

PROPOSITION 5.24. *Let G/H be the quotient of G by H. The map*

$$(g, h) \mapsto (g, gh): G \times H \to G \times_{G/H} G$$

is an isomorphism.

PROOF. For all k-algebras R, the map

$$(g,h) \mapsto (g, gh) \colon G(R) \times H(R) \to G(R) \times_{G(R)/H(R)} G(R)$$

is a bijective. As $G(R)/H(R)$ injects into $(G/H)(R)$, the map remains bijective when $G(R)/H(R)$ is replaced with $(G/H)(R)$. □

PROPOSITION 5.25. *Let G/H be the quotient of G by H. The canonical map $q \colon G \to G/H$ is faithfully flat.*

PROOF. According to the lemma, the first projection map $G \times_{G/H} G \to G$ differs by an isomorphism from the projection map $G \times H \to G$, and so it is faithfully flat. This implies that the map $G \to G/H$ is faithfully flat (5.8). □

COROLLARY 5.26. *If G is smooth, so also is G/H.*

PROOF. Because q is faithfully flat, the map $\mathcal{O}_{G/H} \to q_*\mathcal{O}_G$ is injective, and remains so after extension of the base field. Therefore, if G is smooth, then G/H is geometrically reduced, which implies that it is smooth because it becomes homogeneous over k^{a}. □

COROLLARY 5.27. *The scheme G is an H-torsor over G/H.*

PROOF. Combine Lemma 5.24 and Proposition 5.25. □

THEOREM 5.28. *Let $i \colon H \to G$ be a homomorphism of algebraic groups with trivial kernel. There exists an algebraic scheme X equipped with an action $\mu \colon G \times X \to X$ of G and a point $o \in X(k)$ such that the map $g \mapsto go \colon G \to X$ realizes $\tilde{G}/\tilde{H}$ as a fat subfunctor of $\tilde{X}$.*

PROOF. This is proved in Appendix B (Theorem B.37). For the case that G is affine, see Section 7e. □

In particular, a quotient G/H exists for every algebraic subgroup H of an algebraic group G.

We now prove Theorem 5.14 for a general algebraic group G. Let N be a normal algebraic subgroup of G, and let $q \colon G \to X$ be the faithfully flat map given by Theorem 5.28. Then $D \colon R \rightsquigarrow G(R)/N(R)$ is a fat subfunctor of X equipped with a group structure. It follows that X admits a unique group structure for which q is a homomorphism (5.12). Now q is a quotient map with kernel N.

PROPOSITION 5.29. *The quotient G/H (in the sense of 5.20) is affine if G is affine and H is normal.*

PROOF. We just showed that, when H is normal, G/H is an algebraic group and $q \colon G \to G/H$ is a quotient map. As its kernel is H, Theorem 5.13 shows that this is isomorphic to the quotient map $G \to Q$ in 5.18. As Q is affine, so also is G/H. □

ASIDE 5.30. Let G be an affine algebraic group. We saw in (5.29) that G/H is affine if H is normal, but G/H may be affine without H being normal. When G and H are smooth and G is reductive, Matsushima's criterion says that G/H is affine if and only if H° is reductive. For example, the quotient GL_n/H of GL_n by a connected subgroup variety H is affine if and only if H is reductive. See Borel 1985 (whose proof using étale cohomology works for connected H) or Richardson 1977 (whose proof works in characteristic p using the conjecture of Mumford (12.58) proved by Haboush).

d.   Monomorphisms of algebraic groups

PROPOSITION 5.31. *The following conditions on a homomorphism $\varphi\colon G \to H$ of algebraic groups over k are equivalent:*

(a) *$\varphi(R)\colon G(R) \to H(R)$ is injective for all (small) k-algebras R;*

(b) *$\mathrm{Ker}(\varphi) = e$;*

(c) *φ is a monomorphism in the category of algebraic groups over k;*

(d) *φ is a monomorphism in the category of algebraic schemes over k.*

PROOF. (a)⇔(b): The sequence

$$e \to \mathrm{Ker}(\varphi)(R) \to G(R) \to H(R)$$

is exact for all R.

(c)⇒(b): There are two homomorphisms $\mathrm{Ker}(\varphi) \to G$ whose composite with φ is the trivial homomorphism, namely, the given inclusion and the trivial homomorphism. The two must be equal, and so $\mathrm{Ker}(\varphi)$ is trivial.

(d)⇒(c): This is obvious.

(a)⇒(d): Let $\varphi_1, \varphi_2\colon X \to G$ be morphisms such that $\varphi \circ \varphi_1 = \varphi \circ \varphi_2$. Then $\varphi(R) \circ \varphi_1(R) = \varphi(R) \circ \varphi_2(R)$ for all R, and so $\varphi_1(R) = \varphi_2(R)$ for all R. This implies that $\varphi_1 = \varphi_2$ (Yoneda lemma A.33).   □

DEFINITION 5.32. A homomorphism of algebraic groups satisfying the equivalent conditions of the proposition is called a ***monomorphism***.

PROPOSITION 5.33. *If a homomorphism of algebraic groups is both a monomorphism and a quotient map, then it is an isomorphism.*

PROOF. Let $\varphi\colon G \to H$ be such a homomorphism. We have to show that $\varphi(R)$ is surjective for all k-algebras R. Let $h \in H(R)$. Because φ is faithfully flat, there exists a faithfully flat R-algebra R' and a $g \in G(R')$ mapping to h in $H(R')$ (see 5.7). In the commutative diagram below, the rows are exact (5.9) and the vertical maps are injective:

$$
\begin{array}{ccc}
G(R) \longrightarrow & G(R') \rightrightarrows & G(R' \otimes_R R') \\
\downarrow{\scriptstyle \varphi(R)} & \downarrow{\scriptstyle \varphi(R')} & \downarrow{\scriptstyle \varphi(R' \otimes_R R')} \\
H(R) \longrightarrow & H(R') \rightrightarrows & H(R' \otimes_R R')
\end{array}
$$

A diagram chase shows that $g \in G(R)$, and maps to h in $H(R)$. □

THEOREM 5.34. *A homomorphism of algebraic groups is a monomorphism if and only if it is a closed immersion.*

PROOF. Certainly, a closed immersion has trivial kernel. For the converse, let $i : H \to G$ be a monomorphism, and let $G \to X$ be the quotient map in 5.28. Then H is the fibre over the distinguished point $e \in X(k)$, i.e., it is the pull-back of the map $e \to X$. As e is a closed point of X, this is a closed immersion. □

We sketch a direct proof of Theorem 5.34, not using the results of Appendix B.

DEFINITION 5.35. Let A be a ring (not necessarily a k-algebra). A finitely generated A-algebra B is said to be ***quasi-finite*** over A if the ring $B \otimes_A \kappa(\mathfrak{p})$ is finite over $\kappa(\mathfrak{p})$ for all prime ideals $\mathfrak{p}$ of A. (Here $\kappa(\mathfrak{p})$ is the field of fractions of $A/\mathfrak{p}$.)

THEOREM 5.36 (ZARISKI'S MAIN THEOREM). *Let B be a finitely generated A-algebra, quasi-finite over A, and let A' be the integral closure of A in B. Then*
  (a) *the map $\mathrm{Spec}\, B \to \mathrm{Spec}\, A'$ is a closed immersion, and*
  (b) *there exists an A-subalgebra A'' of A', finite over A, such that $\mathrm{Spec}\, B \to \mathrm{Spec}\, A''$ is an open immersion.*

PROOF. See CA 17.12. □

PROPOSITION 5.37. *Let $\varphi : X \to Y$ be a morphism of algebraic schemes over k. If $\varphi(R)$ is injective for all small k-algebras R, then there exists a dense open subset U of Y such that $\varphi^{-1}(U)$ is nonempty and $\varphi|\varphi^{-1}(U)$ is an immersion.*

PROOF. It suffices to prove this with X and Y affine. Certainly $X \to Y$ is quasi-finite, and so Theorem 5.36 provides a factorization $\varphi = (X \overset{i}{\hookrightarrow} Y' \overset{\pi}{\longrightarrow} Y)$ with i an open immersion and π finite. The subset $\pi(Y' \smallsetminus i(X))$ of Y is proper and closed, and its complement U has the required properties. □

We now prove Theorem 5.34. Let $\varphi : G \to H$ be a monomorphism of algebraic groups. Then $|\varphi|$ is injective with closed image. In proving that it is a closed immersion, we may suppose that k is algebraically closed. According to Proposition 5.37, there is a dense open subset U of H such that $\varphi^{-1}(U)$ is nonempty and $\varphi|\varphi^{-1}(U)$ is an immersion. Using homogeneity, we deduce that φ is an immersion. As $|\varphi(G)|$ is closed (1.68), φ is a closed immersion.

REMARK 5.38. (a) For a proof of Proposition 5.37 that avoids using Zariski's main theorem, see DG, I, §3, no. 4, where one also finds an example of a mono-morphism of algebraic schemes that is not a local immersion.[2]

---

[2]A morphism $\varphi : X \to Y$ of algebraic schemes over k is a ***local immersion*** if X admits a covering by open subsets U such that $\varphi|U$ is an immersion. If X is irreducible, then every injective local immersion $X \to Y$ is an immersion. A monomorphism $X \to Y$ becomes a local immersion on an open subset of X.

(b) As in the affine case (see 3.35), it is possible to deduce Theorem 5.34 easily from the homomorphism theorem. However, we use Theorem 5.34 to prove the general case of the homomorphism theorem (5.39).

(c) Theorem 5.34 may fail for more general group schemes than those we consider (SGA 3, VIII, 7).

e. The homomorphism theorem

THEOREM 5.39 (HOMOMORPHISM THEOREM). *Every homomorphism of algebraic groups $\varphi\colon G \to H$ factors into a composite of homomorphisms*

$$G \xrightarrow{q} I \xrightarrow{i} H$$

with q faithfully flat and i a closed immersion.

PROOF. Let $N = \mathrm{Ker}(\varphi)$. Then $q\colon G \to G/N$ is faithfully flat, and φ factors through q (see 5.13):
$$\varphi = i \circ q.$$
The homomorphism $i\colon G/N \to H$ is a monomorphism, and hence is a closed immersion (5.34). □

REMARK 5.40. The factorization in 5.39 is essentially unique: if $i \circ q = i' \circ q$ with q and q' faithfully flat and i and i' embeddings, then there exists a unique isomorphism j such that $j \circ q = q'$ and $i = i' \circ j$:

DEFINITION 5.41. A homomorphism of algebraic groups is an ***embedding*** if it is a closed immersion.

Thus, every homomorphism of algebraic groups is the composite of a quotient map and an embedding. An embedding φ is injective as a map of schemes (i.e., $|\varphi|$ is injective), but an injective homomorphism need not be an embedding. For example, the trivial homomorphism $\alpha_p \to e$ is injective but not an embedding.

REMARK 5.42. Recall (1.73) that the image of a homomorphism $\varphi\colon G \to H$ is the algebraic group I in 5.39 regarded as a subgroup of H. We denote it by $\varphi(G)$ or $\mathrm{Im}(\varphi)$. Note that $\varphi(G)$ is the smallest algebraic subgroup of H through which φ factors. The morphism $\varphi\colon G \to \varphi(G)$ is surjective, and its fibres are cosets of $\mathrm{Ker}(\varphi)$ in G, and so

$$\dim(G) = \dim(\varphi(G)) + \dim(\mathrm{Ker}(\varphi)).$$

Note that the factorization in 5.39 can be written

$$
\begin{array}{ccc}
G & \xrightarrow{\ \varphi\ } & H \\
\downarrow{\scriptstyle q} & & \uparrow{\scriptstyle i} \\
G/N & \xrightarrow{\ \simeq\ } & \mathrm{Im}(\varphi)
\end{array}
$$

with $N = \mathrm{Ker}(\varphi)$.

PROPOSITION 5.43. *The following conditions on a homomorphism $\varphi\colon G \to Q$ of algebraic groups are equivalent:*

(a) *φ is a quotient map;*

(b) *the subfunctor $R \rightsquigarrow \varphi(G(R))$ of $\tilde{Q}$ is fat;*

(c) *the homomorphism $\mathcal{O}_Q \to \varphi_* \mathcal{O}_G$ is injective.*

PROOF. (a)$\Rightarrow$(b). Special case of Proposition 5.7.

(b)$\Rightarrow$(c). Let U be an open affine subset of Q, and let $R = \mathcal{O}_Q(U)$. On applying (b) to the element $\mathrm{Spm}(R) \hookrightarrow Q$ of $Q(R)$, we see that there exists a faithfully flat map $R \to R'$ and a commutative diagram

$$
\begin{array}{ccc}
G & \longleftarrow & \mathrm{Spm}(R') \\
\downarrow{\scriptstyle \varphi} & & \downarrow \\
Q & \longleftarrow & \mathrm{Spm}(R).
\end{array}
$$

From this, we get a commutative diagram

$$
\begin{array}{ccc}
\mathcal{O}_G(\varphi^{-1}U) & \longrightarrow & R' \\
\uparrow & & \uparrow \\
\mathcal{O}_Q(U) & =\!=\!= & R.
\end{array}
$$

As $R \to R'$ is injective, so also is $\mathcal{O}_Q(U) \to \mathcal{O}_G(\varphi^{-1}U)$.

(c)$\Rightarrow$(a). Let $\varphi = i \circ q$ be the factorization in 5.39. By assumption, the composite of the maps

$$
\mathcal{O}_Q \to i_* \mathcal{O}_I \to \varphi_* G
$$

is injective, and so $\mathcal{O}_Q \to i_* \mathcal{O}_I$ is injective, but it is also surjective because i is a closed immersion. Therefore, i is an isomorphism, and φ is faithfully flat. □

ASIDE 5.44. Recall that a morphism φ in a category is an epimorphism if $\alpha \circ \varphi = \beta \circ \varphi$ implies $\alpha = \beta$. An epimorphism in the category of affine algebraic groups need not be faithfully flat. Consider, for example,

$$
\mathbb{T}_2 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \hookrightarrow \mathrm{SL}_2 .
$$

The quotient $SL_2 / \mathbb{T}_2 \simeq \mathbb{P}^1$, and so a morphism from SL_2 to an affine scheme is constant if it is constant on the orbits of $\mathbb{T}_2$. However, a homomorphism $\varphi \colon H \to G$ of algebraic groups *is* faithfully flat if it is an epimorphism in the category of algebraic *schemes*. To see this, factor φ as in Theorem 5.39, and use that the quotient G/I exists (5.28). For a recent study of epimorphisms in the category of algebraic groups, see Brion 2016.

PROPOSITION 5.45. *Let $\varphi \colon G \to Q$ be a homomorphism of algebraic groups with kernel N. Then Q is the quotient of G by N if and only if the functor*

$$R \rightsquigarrow G(R)/N(R)$$

is a fat subfunctor of Q.

PROOF. Because N is the kernel of $G \to Q$, the sequence

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

is exact for all R, and so $G(R)/N(R) \subset Q(R)$. Hence $G(R)/N(R) \simeq \varphi(G(R))$, and so the statement follows from Proposition 5.43.   □

PROPOSITION 5.46. *Let I be the image of a homomorphism $\varphi \colon G \to H$ of algebraic groups. Then $G \to I$ is a quotient map, and, for all k-algebras R, $I(R)$ consists of the elements of $H(R)$ that lift to $G(R')$ for some faithfully flat R-algebra R'.*

PROOF. The homomorphism $G \to I$ is faithfully flat by definition, and this implies the second part of the statement (5.43).   □

PROPOSITION 5.47. *Let $\varphi \colon G \to H$ be a homomorphism of algebraic groups over k. If φ is faithfully flat, then $G(k') \to H(k')$ is surjective for every algebraically closed field k' containing k. Conversely, if $G(k') \to H(k')$ is surjective for some separably closed field k' containing k and H is smooth, then φ is a quotient map.*

PROOF. If φ is faithfully flat, then so also is $\varphi_{k'}$. Let $h \in H(k')$. For some finitely generated k'-algebra R, the image h' of h in $H(R)$ lifts to an element g of $G(R)$. Zariski's lemma (CA 13.1) shows that there exists a k'-algebra homomorphism $R \to k'$. Under the map $H(R) \to H(k')$, h' maps to h, and under the map $G(R) \to G(k')$, g maps to an element lifting h.

For the converse statement, let I be the image of φ. Then $I(k') = H(k')$, and so $I = H$ (see 1.17).   □

COROLLARY 5.48. *If*

$$e \to N \to G \to Q \to e \tag{29}$$

is exact, then

$$e \to N(k^{\mathrm{a}}) \to G(k^{\mathrm{a}}) \to Q(k^{\mathrm{a}}) \to e \tag{30}$$

is exact. Conversely, if Q is reduced, (30) is exact, and $e \to N \to G \to Q$ is exact, then (29) is exact.

PROOF. The necessity follows from the proposition. Conversely, if Q is reduced and $G(k^{\mathrm{a}}) \to Q(k^{\mathrm{a}})$ is surjective, then $G \to Q$ is surjective, and so it is faithfully flat (1.71). $\qquad\square$

EXAMPLE 5.49. The algebraic group PGL_n is defined as the quotient $\mathrm{GL}_n / \mathbb{G}_m$ of GL_n (with $\mathbb{G}_m$ embedded diagonally). The map $\mathrm{GL}_n(k) \to \mathrm{PGL}_n(k)$ is surjective because $H^1(k, \mathbb{G}_m) = 1$ (see 3.46), and so $\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/k^\times$. The determinant map on $\mathrm{GL}_n(k)$ defines a surjective homomorphism $\mathrm{PGL}_n(k) \to k^\times / k^{\times n}$. The quotient map $\mathrm{GL}_n \to \mathrm{PGL}_n$ induces a quotient map $\mathrm{SL}_n \to \mathrm{PGL}_n$ with kernel μ_n. Let $A \in \mathrm{GL}_n(k)$. The element of $\mathrm{PGL}_n(k)$ represented by A is in the image of $\mathrm{SL}_n(k)$ if and only if its $\det(A)$ is an nth power in k.

f. The isomorphism theorem

Let H and N be algebraic subgroups of an algebraic group G. We say that H **normalizes** N if $H(R)$ normalizes $N(R)$ in $G(R)$ for all k-algebras R. The actions of $H(R)$ on $N(R)$ define an action θ of H on N by group homomorphisms, and multiplication on G defines a homomorphism $N \rtimes_\theta H \to G$. We define $NH = HN$ to be the image of this homomorphism. Then

$$N \rtimes_\theta H \to NH$$

is a quotient map and an element of $G(R)$ lies in $(HN)(R)$ if and only if it lies in $H(R')N(R')$ for some faithfully flat R-algebra R' (see 5.46). This means that HN is the unique algebraic subgroup of G containing $R \rightsquigarrow H(R)N(R)$ as a fat subfunctor. If H and N are smooth, then HN is smooth (see 1.62); if $H \cap N$ is also smooth, then

$$(HN)(k^{\mathrm{s}}) = H(k^{\mathrm{s}}) \cdot N(k^{\mathrm{s}})$$

and HN is the unique smooth algebraic subgroup of G with this property.

EXAMPLE 5.50. Consider the algebraic subgroups SL_n and $\mathbb{G}_m$ (nonzero scalar matrices) of GL_n. Then $\mathbb{G}_m \cdot \mathrm{SL}_n = \mathrm{GL}_n$, but $\mathbb{G}_m(k) \cdot \mathrm{SL}_n(k) \neq \mathrm{GL}_n(k)$ in general (an invertible matrix is the product of a scalar matrix with a matrix of determinant 1 if and only if its determinant is an nth power in k). The functor $R \rightsquigarrow \mathbb{G}_m(R) \cdot \mathrm{SL}_n(R)$ is fat in GL_n.

PROPOSITION 5.51. *Let H and N be algebraic subgroups of an algebraic group G with N normal. The canonical map*

$$N \rtimes_\theta H \to G \tag{31}$$

is an isomorphism if and only if $N \cap H = \{e\}$ and $NH = G$.

PROOF. There is an exact sequence

$$e \to N \cap H \to N \rtimes_\theta H \to NH \to e.$$

Therefore (31) is an embedding if and only if $N \cap H = \{e\}$, and it is a quotient map if and only if $NH = G$. $\qquad\square$

THEOREM 5.52 (ISOMORPHISM THEOREM). *Let H and N be algebraic subgroups of an algebraic group G such that H normalizes N. Then $H \cap N$ is a normal algebraic subgroup of H, and the natural map*

$$H/H \cap N \to HN/N$$

is an isomorphism.

PROOF. For each k-algebra R, $H(R)$ and $N(R)$ are subgroups of $G(R)$, and $H(R)$ normalizes $N(R)$. Moreover $H(R) \cap N(R) = (H \cap N)(R)$, and so the isomorphism theorem in abstract group theory gives us an isomorphism

$$H(R)/(H \cap N)(R) \simeq H(R) \cdot N(R)/N(R), \qquad (32)$$

natural in R. Now $R \rightsquigarrow H(R)/(H \cap N)(R)$ is a fat subfunctor of $H/H \cap N$ and $R \rightsquigarrow H(R) \cdot N(R)/N(R)$ is a fat subfunctor of HN/N, and so (32), regarded as an isomorphism of functors, extends uniquely to an isomorphism $H/H \cap N \to HN/N$ (see 5.11). □

COROLLARY 5.53. *In the situation of the theorem, there is a diagram*

$$
\begin{array}{ccccccc}
e & \longrightarrow & N & \longrightarrow & HN & \longrightarrow & HN/N & \longrightarrow & e \\
& & & & & & \uparrow{\scriptstyle\simeq} & & \\
& & & & & & H/H \cap N & &
\end{array}
$$

in which the row is exact.

PROOF. Restatement of the theorem. □

g. The correspondence theorem

PROPOSITION 5.54. *Let H and N be algebraic subgroups of an algebraic group G, with N normal. The image of H in G/N is an algebraic subgroup of G/N whose inverse image in G is HN.*

PROOF. Let $\bar{H}$ be the image of H in G/N. It is the unique algebraic subgroup of G/N containing $R \rightsquigarrow H(R)N(R)/N(R)$ as a fat subfunctor. The inverse image H' of $\bar{H}$ in G is the fibred product $G \times_{G/N} \bar{H}$ regarded as an algebraic subgroup of G. Recall that

$$\left(G \times_{G/N} \bar{H}\right)(R) = G(R) \times_{(G/N)(R)} \bar{H}(R).$$

Now $R \rightsquigarrow G(R) \times_{(G/N)(R)} \bar{H}(R)$ contains $R \rightsquigarrow H(R)N(R)$ as a fat subfunctor, and so H' is the (unique) algebraic subgroup of G containing $R \rightsquigarrow H(R)N(R)$ as a fat subfunctor. In other words, $H' = HN$ (see 5.46). □

THEOREM 5.55 (CORRESPONDENCE THEOREM). *Let N be a normal algebraic subgroup of an algebraic group G. The map $H \mapsto H/N$ is a bijection from the set of algebraic subgroups of G containing N to the set of algebraic subgroups of G/N. An algebraic subgroup H of G containing N is normal in G if and only if H/N is normal in G/N, in which case the natural map*

$$G/H \to (G/N)/(H/N)$$

is an isomorphism.

PROOF. The first statement follows from Proposition 5.54. For the second statement, note that the map

$$G(R)/H(R) \to (G(R)/N(R))/(H(R)/N(R))$$

defined by the quotient map $G(R) \to G(R)/N(R)$ is an isomorphism, natural in R. The algebraic group G/H (resp. $(G/N)/(H/N)$) contains the left (resp. right) functor as a fat subfunctor, and so we can apply 5.11. □

COROLLARY 5.56. *Let H and N be algebraic subgroups of G such that N is normal. If G/N is smooth and $H(k^{\mathrm{a}})N(k^{\mathrm{a}}) = G(k^{\mathrm{a}})$, then $HN = G$.*

PROOF. The restriction of the quotient map $G \to G/N$ to H has kernel $H \cap N$, and hence factors into $H \to H/H \cap N \xrightarrow{i} G/N$ with i a closed immersion (5.39). The hypothesis implies that i is surjective on k^{a}-points. As $(G/N)_{k^{\mathrm{a}}}$ is reduced, this implies that i is an isomorphism. Thus $HN/N \simeq G/N$ (by 5.52), which implies that $HN = G$ (by 5.55). □

COROLLARY 5.57. *For an algebraic group G over a perfect field k,*

$$G = G_{\mathrm{red}} \cdot G^{\circ}.$$

PROOF. Because k is perfect, G_{red} is an algebraic subgroup of G (see 1.39). The homomorphism $G_{\mathrm{red}}(k^{\mathrm{a}}) = G(k^{\mathrm{a}}) \to \pi_0(G)(k^{\mathrm{a}})$ is surjective, and so $G(k^{\mathrm{a}}) = G_{\mathrm{red}}(k^{\mathrm{a}}) \cdot G^{\circ}(k^{\mathrm{a}})$. As $\pi_0(G)$ is smooth, we can apply the last corollary. □

NOTES. The Noether isomorphism theorems fail in the category of group varieties. Consider, for example, the algebraic group GL_n and its normal subgroups SL_n and $\mathbb{G}_m$ (scalar matrices). If $n = p = \mathrm{char}(k)$, then $\mathrm{SL}_p \cap \mathbb{G}_m = e$ in the category of group varieties, but

$$\mathrm{SL}_p / \mathrm{SL}_p \cap \mathbb{G}_m \to \mathrm{SL}_p \cdot \mathbb{G}_m / \mathbb{G}_m \tag{33}$$

is the homomorphism $\mathrm{SL}_p \to \mathrm{PGL}_p$, which is not an isomorphism of group varieties (it is purely inseparable of degree p). In the category of algebraic group schemes, $\mathrm{SL}_p \cap \mathbb{G}_m = \mu_p$, and (33) is the isomorphism

$$\mathrm{SL}_p / \mu_p \to \mathrm{PGL}_p.$$

This failure, of course, causes endless problems, but when Borel, Chevalley, and others introduced algebraic geometry into the study of algebraic groups they based it on the algebraic geometry of the day, which did not allow nilpotents.

The isomorphism theorems for algebraic group schemes over a field are widely used but rarely stated.

h.   The connected-étale exact sequence

PROPOSITION 5.58. *Let G be an algebraic group. Then $G°$ is the unique connected normal algebraic subgroup of G such that $G/G°$ is étale.*

PROOF. Let N be a connected normal algebraic subgroup of G such that G/N is étale. According to Proposition 2.37(a), the homomorphism $G \to G/N$ factors through $G \to \pi_0(G)$, and so there is a commutative diagram

$$
\begin{array}{ccccccccc}
e & \longrightarrow & G° & \longrightarrow & G & \longrightarrow & \pi_0 G & \longrightarrow & e \\
& & \downarrow & & \| & & \downarrow & & \\
e & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & e
\end{array}
$$

with exact rows. On applying the snake lemma (Exercise 5-7) to the diagram, we obtain an exact sequence of algebraic groups:

$$e \to G° \to N \to \pi_0 G.$$

As N is connected, the homomorphism $N \to \pi_0 G$ is trivial, and so $G° \simeq N$. $\square$

Let G be an algebraic group. Proposition 5.58 says that

$$e \to G° \to G \to \pi_0(G) \to e$$

is the unique exact sequence with $G°$ connected and $\pi_0(G)$ étale. It is called the *connected-étale exact sequence*.

PROPOSITION 5.59. *Let*

$$e \to N \to G \to Q \to e$$

be an exact sequence of algebraic groups.
  (a) *If N and Q are connected, then G is connected.*
  (b) *If G is connected, then Q is connected.*

PROOF. If N is connected, then it maps to e in $\pi_0(G)$, and so $G \to \pi_0(G)$ factors through Q, and hence through $\pi_0(Q)$, which is trivial if Q is connected. The surjective homomorphism $G \to Q \to \pi_0(Q)$ factors through $\pi_0(G)$, and so $\pi_0(Q)$ is trivial if $\pi_0(G)$ is. $\square$

More generally, the sequence $\pi_0(N) \to \pi_0(G) \to \pi_0(Q) \to e$ is exact (Exercise 5-9). In Proposition 5.59, N need not be connected when G is connected. For example, $\mathbb{G}_m$ is connected, but the kernel μ_n of the quotient map $x \mapsto x^n : \mathbb{G}_m \to \mathbb{G}_m$ is not connected unless n is a power of the characteristic exponent of k.

EXAMPLE 5.60. Let G be finite. When k has characteristic zero, G is étale, and so $G = \pi_0(G)$ and $G^\circ = 1$. Otherwise, there is an exact sequence

$$e \to G^\circ \to G \to \pi_0(G) \to e.$$

When k is perfect, the homomorphism $G \to \pi_0(G)$ has a section, and G is a semidirect product $G = G^\circ \rtimes \pi_0(G)$ (see 11.3 below).

ASIDE 5.61. In general, the connected-étale sequence does not split, even when k is perfect. However, there is the following result: let $e \to N \to G \to Q \to e$ be an exact sequence of algebraic groups with Q finite; then there exists a finite algebraic subgroup F of G mapping onto Q (so $G = N \cdot F$); if Q is étale and k is perfect, then F may be chosen to be étale (Brion 2015a, 1.1).

i.   The category of commutative algebraic groups

THEOREM 5.62. *The commutative algebraic groups over k form an abelian category.*

PROOF. The Hom sets are commutative groups, and composition of morphisms is bilinear. Moreover, the product $G_1 \times G_2$ of two commutative algebraic groups is both a product and a sum of G_1 and G_2. Thus the category of commutative algebraic groups over a field is additive. Every morphism in the category has both a kernel and cokernel, and the canonical morphism from the coimage of the morphism to its image is an isomorphism (homomorphism theorem, 5.39, 5.42). Therefore the category is abelian. □

COROLLARY 5.63. *The affine commutative algebraic groups over k form an abelian subcategory of the category of all commutative algebraic groups over k.*

PROOF. In fact, they form a thick subcategory: they form a full subcategory by definition; subgroups of affine groups are affine (1.43); quotients of affine groups are affine (5.29); extensions of affine groups are affine (2.70). □

COROLLARY 5.64. *The finitely generated commutative cocommutative Hopf algebras over a field form an abelian category.*

PROOF. This category is contravariantly equivalent to that in Theorem 5.62. □

NOTES. Theorem 5.62 is proved in SGA 3, VI$_A$, 5.4.3, p. 327 and DG, III §3, 7.4. Corollary 5.64 is proved purely in the context of Hopf algebras in Sweedler 1969, Chapter XVI, for finite-dimensional commutative cocommutative Hopf algebras, and in Takeuchi 1972, 4.16, for finitely generated commutative cocommutative Hopf algebras.

j. Sheaves

In the remainder of this chapter, we explain how to use sheaves to treat some of
the earlier material more efficiently. All functors are from the category of small
k-algebras to sets or groups.

DEFINITION 5.65. A *flat sheaf* (better, *sheaf for the flat topology*) is a functor
F such that
   (a) (local) for all small k-algebras $R_1, \dots, R_m$

$$F(R_1 \times \cdots \times R_n) \simeq F(R_1) \times \cdots \times F(R_m);$$

   (b) (descent) for all faithfully flat homomorphisms $R \to R'$ of small k-algebras,
       the sequence
$$F(R) \to F(R') \rightrightarrows F(R' \otimes_R R')$$

   is exact. The maps $F(R') \to F(R' \otimes_R R')$ are defined by the homomorph-
   isms $R' \to R' \otimes_R R'$ sending r to $r \otimes 1$ or $1 \otimes r$.
A *morphism* of flat sheaves is a natural transformation.

EXAMPLE 5.66. Let $F = h^A \overset{\text{def}}{=} \operatorname{Hom}(A, -)$ for some k-algebra A. Then F is a
sheaf. Condition (a) is obvious, and condition (b) follows from the exactness of

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

for any faithfully flat homomorphism $R \to R'$ (CA 11.12). Similarly, for an
algebraic scheme X over k, the functor h_X is a flat sheaf (cf. 5.9).

LEMMA 5.67. *Let D be a fat subfunctor of a sheaf S. Every morphism $D \to S'$
from D to a sheaf S' extends uniquely to S.*

PROOF. The proof of (5.10) shows this.   □

PROPOSITION 5.68. *Let F be a functor. Among the morphisms from F to a flat
sheaf there exists a universal one $\alpha \colon F \to aF$.*

The universality means that every homomorphism β
from F to a sheaf S factors uniquely through α:

$$\begin{array}{ccc} F & \xrightarrow{\ \alpha\ } & aF \\ & \beta\searrow & \big\downarrow{\scriptstyle\exists !} \\ & & S. \end{array}$$

The pair (aF, α) is called the *sheaf associated with F* (or the sheafification of
F). It is unique up to a unique isomorphism.
     We prove the proposition in two steps. A family $(R_i)_{i \in I}$ of R-algebras is
faithfully flat if the homomorphism $R \to \prod_{i \in I} R_i$ is faithfully flat. A functor is
separated if $F(R) \to \prod F(R_i)$ is injective whenever $(R_i)_{i \in I}$ is a finite faithfully
flat family of small R-algebras.

LEMMA 5.69. *Let F be a functor. Among the morphisms from F to a separated functor, there exists a universal one $\alpha\colon F \to F'$.*

PROOF. For $a, b \in F(R)$, write $a \sim b$ if a and b have the same image in $\prod F(R_i)$ for some finite faithfully flat family $(R_i)_{i \in I}$ of small R-algebras. Define

$$F'(R) = F(R)/\sim.$$

One checks easily that this is a separated functor, and that the morphism $F \to F'$ is universal.   □

LEMMA 5.70. *Let F be a separated functor. Among the morphisms from F to a flat sheaf there exists a universal one $\alpha\colon F \to aF$.*

PROOF. Let

$$(aF)(R) = \varinjlim \mathrm{Eq}\left(\prod_{i \in I} F(R_i) \rightrightarrows \prod_{(i,j) \in I \times I} F(R_i \otimes_R R_j)\right)$$

where the limit is over finite faithfully flat families $(R_i)_{i \in I}$ of small R-algebras. One checks easily that this is a sheaf, and that the morphism $F \to aF$ is universal.   □

Now, for a functor F, the composite of the morphisms $F \to F' \to aF'$ is the required universal morphism from F to a sheaf. This completes the proof of Proposition 5.68.

EXAMPLE 5.71. Let D be a subfunctor of a sheaf S. The pair $(S, D \hookrightarrow S)$ is the sheaf associated with D if and only if, for every small R and $x \in S(R)$, there exists a finite faithfully flat family of R-algebras $(R_i)_{i \in I}$ such that the image x_i of x in $S(R_i)$ lies in $D(R_i)$ for all i. For example, if D is fat in S, then S is the sheaf associated with D.

If F is local (i.e., satisfies (a) of 5.65) and separated, then

$$(aF)(R) = \varinjlim \mathrm{Eq}\left(F(R') \rightrightarrows F(R' \otimes_R R')\right)$$

where the limit is over the small faithfully flat R-algebras R'.

5.72. Let F be a flat sheaf. We say that F is ***representable*** if there exists an algebraic k-scheme X such that $\tilde{X} \approx F$. To show that F is representable, it suffices (by descent theory) to show that it becomes representable over a nonzero k-algebra R, i.e., that there exists an algebraic R-scheme X and bijections $X(R') \to F(R')$, natural in R', for every R-algebra R'.

k.   The isomorphism theorems for functors to groups

By a group functor we mean a functor from small k-algebras to groups. A homomorphism of group functors is a natural transformation. A subgroup functor of a group functor G is a subfunctor H such that $H(R)$ is a subgroup of $G(R)$ for all R; it is normal if $H(R)$ is normal in $G(R)$ for all R. When N is a normal subgroup functor of G, we define G/N to be the group functor $R \rightsquigarrow G(R)/N(R)$. For subgroup functors H and N of G with N normal, we define HN to be the subgroup functor $R \rightsquigarrow H(R)N(R)$ of G.

   Let $\varphi: G \to H$ be a homomorphism of group functors. The kernel of φ is the group functor $R \rightsquigarrow \mathrm{Ker}(\varphi(R))$, and the image φG of φ is the subfunctor $R \rightsquigarrow \varphi(G(R))$ of H. A homomorphism $\varphi: G \to H$ is surjective or injective if $\varphi(R)$ is surjective or injective for all small k-algebras R.

   With these definitions, the isomorphism theorems (5.1–5.4) hold with "group" replaced by "group functor". Each statement can be checked for one k-algebra R at a time, when it becomes the statement for abstract groups.

l.   The isomorphism theorems for sheaves of groups

Let P denote the category of functors and S the category of sheaves. Then S is a full subcategory of P, and Proposition 5.68 says that the functor $a: \mathsf{P} \to \mathsf{S}$ is left adjoint to the inclusion functor $i: \mathsf{S} \to \mathsf{P}$:

$$\mathrm{Hom}_{\mathsf{P}}(F, iS) \simeq \mathrm{Hom}_{\mathsf{S}}(aF, S).$$

As a has a right adjoint, it preserves finite direct limits; similarly, i preserves finite inverse limits (Mac Lane 1971, V, §5). Using this, we can deduce the isomorphism theorems for sheaves of groups from the previous case, as we now explain.

5.73. (Existence of quotients). Let $\varphi: G \to H$ be a homomorphism of sheaves of groups. The kernel of φ is automatically a sheaf, and hence a sheaf of normal subgroups of G. We say that φ is a **quotient map** if H is the sheaf associated with the functor $R \rightsquigarrow \varphi(G(R))$, for example, if the image φG of G is fat in H. Let N be a sheaf of normal subgroups of G. We define $G\tilde{/}N$ to be the sheaf associated with the group functor G/N. The canonical map $q: G \to G\tilde{/}N$ is a quotient map of sheaves of groups with kernel N. Let φ be a homomorphism from G to a sheaf of groups H whose kernel contains N; then φ factors uniquely through $G \to G/N$ (previous case), and then $G/N \to H$ factors uniquely through $G/N \to G\tilde{/}N$ because H is a sheaf:

$$G \longrightarrow G/N \longrightarrow G\tilde{/}N$$

$$\varphi \qquad \exists! \qquad \exists!$$

$$H.$$

5.74. (Homomorphism theorem). Consider a homomorphism $\varphi\colon G \to H$ of sheaves of groups. We define the image $\mathrm{Im}(\varphi)$ of φ to be the sheaf associated with the group functor φG. It is the smallest sheaf of subgroups of H through which φ factors, and φG is a fat subfunctor of $\mathrm{Im}(\varphi)$. The map φ defines an isomorphism of group functors

$$G/N \to \varphi G$$

with $N = \mathrm{Ker}(\varphi)$. On passing to the associated sheaves, we obtain an isomorphism of sheaves

$$G\tilde{/}\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi),$$

and hence a factorization of φ:

$$
\begin{array}{ccc}
G & \xrightarrow{\;\varphi\;} & H \\
\downarrow{\scriptstyle q} & & \uparrow{\scriptstyle i} \\
G\tilde{/}N & \xrightarrow{\;\simeq\;} & \mathrm{Im}(\varphi).
\end{array}
$$

Let G be a sheaf of groups.

5.75. (Isomorphism theorem). Let H and N be subgroup sheaves of G such that H normalizes N. We define HN to be the sheaf associated with the group functor $R \rightsquigarrow H(R)N(R)$. Then HN is a sheaf of subgroups of G, $H \cap N$ is a normal subgroup of H, and the map

$$xH \cap N \mapsto xN\colon H\tilde{/}(H \cap N) \to (HN)\tilde{/}N$$

is an isomorphism because it is obtained from an isomorphism of group functors by passing to the associated sheaves.

5.76. (Correspondence theorem). Let N be a sheaf of normal subgroups of G. The map $H \mapsto H\tilde{/}N$ is a bijection from the set of sheaves of subgroups of G containing N to the set of sheaves of subgroups of $G\tilde{/}N$. A sheaf of subgroups H containing N is normal if and only if $H\tilde{/}N$ is normal in $G\tilde{/}N$, in which case the natural map

$$G\tilde{/}H \to (G\tilde{/}N)/(H\tilde{/}N)$$

is an isomorphism. Again, all these statements can be derived easily from the corresponding statements for group functors.

m. The isomorphism theorems for algebraic groups

Recall that $\tilde{G}$ is the flat sheaf defined by an algebraic group G; moreover, the functor $G \rightsquigarrow \tilde{G}$ is fully faithful, and so identifies the category of algebraic groups over k with the category of group functors whose underlying functor is representable by an algebraic k-scheme. In order to prove (5.1–5.4) for algebraic

groups, it suffices to show that each of the constructions in the preceding section takes algebraic groups to algebraic groups.

We shall need to use the following three statements relating algebraic groups to the functors they define.

5.77. *A homomorphism φ of algebraic groups is a closed immersion if $\varphi(R)$ is injective for all small k-algebras R (see 5.34).*

5.78. *A homomorphism $\varphi\colon G \to H$ of algebraic groups is faithfully flat if the functor $R \rightsquigarrow \varphi(G(R))$ is fat in $\tilde{H}$ (see 5.43).*

5.79. *For an algebraic group G and a normal algebraic subgroup N, the sheaf $G\tilde{/}N$ is represented by an algebraic group (5.14).*

THEOREM 5.80 (EXISTENCE OF QUOTIENTS). *The kernel of a homomorphism $G \to H$ of algebraic groups is a normal algebraic subgroup, and every normal algebraic subgroup N of G arises as the kernel of a quotient map $G \to G/N$.*

PROOF. Let G/N represent $G\tilde{/}N$ (see 5.79). As $\tilde{G} \to G\tilde{/}N$ has kernel $\tilde{N}$, the homomorphism $q\colon G \to G/N$ has kernel N. The homomorphism $G \to G/N$ is a quotient map because the functor $R \rightsquigarrow \varphi(G(R))$ is fat in $G\tilde{/}N$ (see 5.78).   □

THEOREM 5.81 (HOMOMORPHISM THEOREM). *Every homomorphism of algebraic groups is the composite of a quotient map with an embedding.*

PROOF. Let $\varphi\colon G \to H$ be a homomorphism of algebraic groups, and let $N = \mathrm{Ker}(\varphi)$. Then $\tilde{\varphi}$ factors into

$$\tilde{G} \xrightarrow{\tilde{q}} \tilde{G}\tilde{/}\tilde{N} \xrightarrow{\tilde{i}} \tilde{H} \tag{34}$$

with q a quotient map and i an embedding. Now $G\tilde{/}N$ is represented by an algebraic group G/N (see 5.79), and so (34) arises from a diagram

$$G \xrightarrow{q} G/N \xrightarrow{i} H$$

in which q is a quotient map (5.78) and i is an embedding (5.77).   □

THEOREM 5.82 (ISOMORPHISM THEOREM). *Let H and N be algebraic subgroups of G with N normal in G. Then HN is an algebraic subgroup of G, $H \cap N$ is a normal algebraic subgroup of H, and the map*

$$xH \cap N \mapsto xN\colon H/H \cap N \to HN/N \tag{35}$$

is an isomorphism.

PROOF. As before, we define HN to be the image of the homomorphism $H \rtimes_\theta N \to G$ of algebraic groups. It is the sheaf associated with the subfunctor $R \rightsquigarrow H(R)N(R)$ of $\tilde{G}$. Now (35) is the map of algebraic groups corresponding by the Yoneda lemma to the isomorphism

$$\tilde{H} \tilde{/} \widetilde{H \cap N} \to \tilde{H} \tilde{N} \tilde{/} \tilde{N}. \qquad \qquad \square$$

We leave the statement and proof of the correspondence theorem as an exercise to the reader.

n. Some category theory

We interpret some of the statements in this chapter in the language of category theory.

Let A be a category. A morphism $\alpha: A \to B$ in A is a monomorphism if $\alpha \circ f = \alpha \circ g$ implies $f = g$, and an epimorphism if $f \circ \alpha = g \circ \alpha$ implies $f = g$. If $\alpha: A \to B$ is a monomorphism (resp. epimorphism) then we call A a subobject of B (resp. we call B a quotient object of A).

Let $\alpha: A \to B$ a morphism. The subobjects of B through which α factors form a partially ordered set. A least object in this set (if it exists) is called the image of α. The coimage of α is defined similarly.

A null object of A is an object e such that, for every object A of A, each of the sets $\mathrm{Hom}(A, e)$ and $\mathrm{Hom}(e, A)$ has exactly one element. A morphism is trivial if it factors through e.

Assume that A has a null object. Let $\alpha: A \to B$ be a morphism. We call a morphism $u: K \to A$ a kernel of α if $\alpha \circ u$ is trivial and every other morphism with this property factors uniquely through u. Similarly, we define the notion of a cokernel.

A subobject $u: A' \to A$ is normal if it is the kernel of some morphism $A \to B$. The notion of a conormal quotient object is defined similarly. A category is normal (resp. conormal) if every subobject is normal (resp. every quotient object is conormal). A normal and conormal category with kernels and cokernels is exact if every morphism $\alpha: A \to B$ can be written as a composite $A \xrightarrow{q} I \xrightarrow{v} B$ with q an epimorphism and v a monomorphism.

Now let A denote the category of algebraic groups over a field k. A morphism in A is a monomorphism if and only if it is a closed immersion (5.34). Thus, the subobjects of G are essentially the algebraic subgroups of G. A quotient map is an epimorphism, but not every epimorphism is a quotient map (5.44). The image of a homomorphism $\alpha: G \to H$ as we defined it is an image in the sense of categories.

The trivial group e is a null object in A. The kernel of a homomorphism as we defined it is a kernel in the sense of categories, but not every subobject is normal. Every homomorphism $\alpha: A \to B$ can be written as a composite of an epimorphism and a monomorphism.

Clearly, A is not an exact category, but some of the results for exact categories hold for A. However, when we replace A with the category of commutative algebraic groups, then we do get an exact category (even an abelian category).

Exercises

EXERCISE 5-1. Let A and B be algebraic subgroups of an affine algebraic group G. If B is normal, show that AB is the algebraic subgroup of G with $\mathcal{O}(AB) = \mathcal{O}(G)/\mathfrak{a}$, where $\mathfrak{a}$ is the kernel of homomorphism $\mathcal{O}(G) \to \mathcal{O}(A) \otimes \mathcal{O}(B)$ defined by the map $a, b \mapsto ab \colon A \times B \to G$ (of set-valued functors).

EXERCISE 5-2. Let A, B, C be algebraic subgroups of an algebraic group G such that A is a normal subgroup of B and B normalizes C. Show:

(a) $C \cap A$ is a normal subgroup of $C \cap B$;

(b) CA is a normal subgroup of CB (note that CB is defined because B normalizes C and CA is defined because C is normal in CB).

EXERCISE 5-3 (DEDEKIND'S MODULAR LAWS). Let $A \supset C$ and B be subgroups of a group G. Show:

(a) $A \cap (BC) = (A \cap B)C$;

(b) if $G = BC$, then $A = (A \cap B)C$.

Deduce that the same statement is true with "algebraic group" for "group" if B is normal in G.

EXERCISE 5-4. Let N and Q be algebraic subgroups of G with N normal. Show that G is the semidirect product of N and Q if and only if (a) $G = NQ$, (b) $N \cap Q = e$, and (c) the restriction to Q of the canonical map $G \to G/N$ is an isomorphism.

EXERCISE 5-5. Let H be an algebraic subgroup of an algebraic group G over a perfect field k.

(a) Show that $(G/H)(k^{\mathrm{a}}) \simeq (G/H_{\mathrm{red}})(k^{\mathrm{a}})$, and deduce that G/H_{red} is finite if and only if G/H is finite.

(b) Show that $(G^{\circ})_{\mathrm{red}} = G_{\mathrm{red}} \cap G^{\circ} = (G_{\mathrm{red}})^{\circ}$; denote this algebraic group by G°_{red}.

(c) Show that $G/G^{\circ}_{\mathrm{red}}$ is finite, and that G°_{red} is the smallest algebraic subgroup of G with this property.

EXERCISE 5-6. Let N be an algebraic subgroup of a smooth algebraic group G over an algebraically closed field k. Show that N_{red} is a normal algebraic subgroup of G.

EXERCISE 5-7 (EXTENDED SNAKE LEMMA). A homomorphism $u\colon G \to G'$ of algebraic groups is said to be **normal** if its image is a normal subgroup of G'. For a normal homomorphism $u\colon G \to G'$, the quotient map $G' \to G'/u(G)$ is the cokernel of u in the category of algebraic groups over k. Show that the extended snake lemma holds for algebraic groups: if in the commutative diagram

$$e \to \operatorname{Ker} f \longrightarrow \operatorname{Ker} a \longrightarrow \operatorname{Ker} b \longrightarrow \operatorname{Ker} c$$
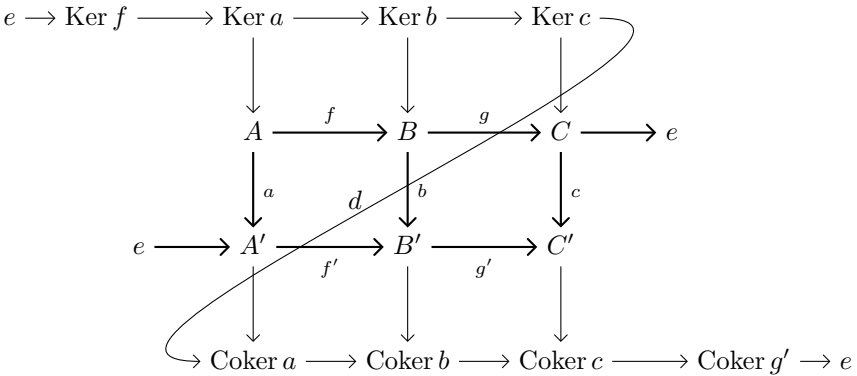
the homomorphisms a, b, c are normal and the sequences (f, g) and (f', g') are exact, then the sequence

$$e \to \operatorname{Ker} f \to \cdots \to \operatorname{Ker} c \xrightarrow{\ d\ } \operatorname{Coker} a \to \cdots \to \operatorname{Coker} g' \to e$$

exists and is exact.

EXERCISE 5-8. Show that a pair of normal homomorphisms

$$G \xrightarrow{\ f\ } G' \xrightarrow{\ g\ } G''$$

of algebraic groups whose composite is normal gives rise to an exact (kernel–cokernel) sequence

$$0 \to \operatorname{Ker} f \to \operatorname{Ker} g \circ f \xrightarrow{\ f\ } \operatorname{Ker} g \longrightarrow \operatorname{Coker} f \xrightarrow{\ g\ } \operatorname{Coker} g \circ f \to \operatorname{Coker} g \to 0.$$

[Use the extended snake lemma.]

EXERCISE 5-9. Let $e \to N \to G \to Q \to e$ be an exact sequence. Show that

$$\pi_0(N) \to \pi_0(G) \to \pi_0(Q) \to e$$

is exact. Give an example to show that $\pi_0(N) \to \pi_0(G)$ need not be a closed immersion.

EXERCISE 5-10. Let

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of sheaves. Show that G is algebraic group if N and Q are.

Subnormal Series; Solvable and Nilpotent Algebraic Groups

Once the isomorphism theorems have been proved, much of the basic theory of abstract groups carries over to algebraic groups.

a. Subnormal series

Let G be an algebraic group over k.

DEFINITION 6.1. A **subnormal series**[1] of G is a finite sequence $(G_i)_{i=0,\ldots,s}$ of algebraic subgroups of G such that $G_0 = G$, $G_s = e$, and G_i is a normal subgroup of G_{i-1} for $i = 1,\ldots,s$:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = e.$$

A subnormal series $(G_i)_i$ is a **normal series** (resp. **characteristic series**) if each G_i is normal (resp. characteristic) in G.

PROPOSITION 6.2. *Let H be an algebraic subgroup of an algebraic group G. If*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

is a subnormal series for G, then

$$H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_s = e$$

is a subnormal series for H, and

$$H \cap G_i / H \cap G_{i+1} \hookrightarrow G_i / G_{i+1}.$$

---

[1] In French, a subnormal series is called a "suite de composition". In both English and German, a composition series (*Kompositionsreihe*) is a *maximal* subnormal series. Some of the literature on algebraic groups in English follows the French convention.

PROOF. As G_{i+1} is normal in G_i and $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}$, the isomorphism theorem (5.52) gives an isomorphism

$$H \cap G_i / H \cap G_{i+1} \simeq (H \cap G_i) \cdot G_{i+1} / G_{i+1}.$$

The second group is an algebraic subgroup of G_i / G_{i+1}. □

Two subnormal series

$$\begin{cases} G = G_0 \supset G_1 \supset \cdots \supset G_s = e \\ G = H_0 \supset H_1 \supset \cdots \supset H_t = e \end{cases} \tag{36}$$

are said to be *equivalent* if $s = t$ and there is a permutation π of $\{1, 2, \ldots, s\}$ such that $G_i / G_{i+1} \approx H_{\pi(i)} / H_{\pi(i)+1}$.

THEOREM 6.3. *Any two subnormal series (36) in an algebraic group G have equivalent refinements.*

PROOF. Let $G_{i,j} = G_{i+1}(G_i \cap H_j)$ and $H_{j,i} = H_{j+1}(H_j \cap G_i)$, and consider the refinements

$$\cdots \supset G_i = G_{i,0} \supset G_{i,1} \supset \cdots \supset G_{i,t} = G_{i+1} \supset \cdots$$
$$\cdots \supset H_j = H_{j,0} \supset H_{j,1} \supset \cdots \supset H_{j,s} = H_{j+1} \supset \cdots$$

of the original series. According to the next lemma,

$$G_{i,j} / G_{i,j+1} \simeq H_{j,i} / H_{j,i+1},$$

and so the refinement $(G_{i,j})$ of (G_i) is equivalent to the refinement $(H_{j,i})$ of (H_i). □

LEMMA 6.4 (BUTTERFLY LEMMA). *Let $H_1 \supset N_1$ and $H_2 \supset N_2$ be algebraic subgroups of an algebraic group G with N_1 and N_2 normal in H_1 and H_2. Then $N_1(H_1 \cap N_2)$ and $N_2(N_1 \cap H_2)$ are normal algebraic subgroups of $N_1(H_1 \cap H_2)$ and $N_2(H_2 \cap H_1)$ respectively, and there is a canonical isomorphism of algebraic groups*

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)}.$$

PROOF. The algebraic group $H_1 \cap N_2$ is normal in $H_1 \cap H_2$, and so $N_1(H_1 \cap N_2)$ is normal in $N_1(H_1 \cap H_2)$ (see Exercise 5-2).

Dedekind's modular law (Exercise 5-3) with $G = H_1$, $A = H_1 \cap H_2$, $B = N_1$, and $C = H_1 \cap N_2$ shows that

$$(H_1 \cap H_2) \cap N_1(H_1 \cap N_2) = (H_1 \cap H_2 \cap N_1)(H_1 \cap N_2)$$
$$= (H_2 \cap N_1)(H_1 \cap N_2).$$

As $H_1 \cap H_2$ normalizes $N_1(H_1 \cap H_2)$, the isomorphism theorem (5.52) shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)} \simeq \frac{N_1(H_1 \cap N_2) \cdot (H_1 \cap H_2)}{N_1(H_1 \cap N_2)},$$

which simplifies to

$$\frac{H_1 \cap H_2}{(H_2 \cap N_1)(H_1 \cap N_2)} \simeq \frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)}.$$

A symmetric argument shows that

$$\frac{H_1 \cap H_2}{(H_2 \cap N_1)(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)},$$

and so

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)}. \qquad \square$$
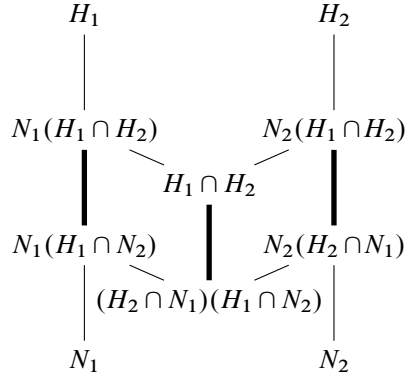
Similar statements in the category of group varieties hold only up to purely inseparable isogenies (Rosenlicht 1956).

b. Isogenies

DEFINITION 6.5. An algebraic subgroup H (not necessarily normal) of an algebraic group G has *finite index* if the quotient scheme G/H is finite.

A subgroup H in G has finite index if and only if $\dim H = \dim G$ (see 5.23). If G is smooth, then G/H is smooth, and hence étale if finite. Thus, an algebraic subgroup of a smooth group G has finite index if and only if it contains G°.

DEFINITION 6.6. A homomorphism of algebraic groups $G \to H$ is an *isogeny* if its kernel is finite and its image has finite index in H.

Thus, a homomorphism of smooth algebraic groups $G \to H$ is an isogeny if and only if its kernel is finite and its image contains H°. This agrees with Definition 2.23. A composite of isogenies is an isogeny (cf. Exercise 5-8).

DEFINITION 6.7. Two algebraic groups G and H are *isogenous*, denoted $G \sim H$, if there exist algebraic groups $G_1, \ldots, G_n$ such that $G = G_1$, $H = G_n$, and, for each $i = 1, \ldots, n-1$, there exists either an isogeny $G_i \to G_{i+1}$ or an isogeny $G_{i+1} \to G_i$.

In other words, "isogeny" is the equivalence relation generated by the binary relation "there exists an isogeny from G to H".

DEFINITION 6.8. An algebraic group is *strongly connected* if it has no proper algebraic subgroup of finite index.

An algebraic group is connected if it is strongly connected. The converse is true for smooth groups.

DEFINITION 6.9. The ***strong identity component*** G^{so} of an algebraic group G is the intersection of the algebraic subgroups of finite index.

If G is smooth, then $G^{\mathrm{so}} = G^\circ$.

PROPOSITION 6.10. *The quotient G/G^{so} is finite (hence G^{so} is the smallest algebraic subgroup having the same dimension as G).*

PROOF. Because the algebraic subgroups of G satisfy the descending chain condition (1.42), $G^{\mathrm{so}} = H_1 \cap \cdots \cap H_r$ for certain algebraic subgroups $H_1, \cdots, H_r$ such that G/H_i is finite. The map $G \to G/H_1 \times \cdots \times G/H_r$ realizes G/H as a subscheme of a finite scheme. □

6.11. Let G be an algebraic group over a perfect field k. Then

$$(G^\circ)_{\mathrm{red}} = G_{\mathrm{red}} \cap G^\circ = (G_{\mathrm{red}})^\circ.$$

We denote this subgroup by G°_{red}. The quotient scheme G/G°_{red} is finite, and G°_{red} is the smallest algebraic subgroup of G for which this is true (Exercise 5-5). Thus $G^\circ_{\mathrm{red}} = G^{\mathrm{so}}$. In general G°_{red} is not normal in G. However, if G_{red} is normal in G, then G°_{red} is normal in G because $(G_{\mathrm{red}})^\circ$ is a characteristic subgroup of G_{red}; in this case, G^{so} is the smallest normal algebraic subgroup having the same dimension as G.

c. Composition series for algebraic groups

Let G be an algebraic group over k. A subnormal series

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

is a ***composition series*** if

$$\dim G_0 > \dim G_1 > \cdots > \dim G_s$$

and the series cannot be refined, i.e., for no i does there exist a normal algebraic subgroup N of G_i containing G_{i+1} and such that

$$\dim G_i > \dim N > \dim G_{i+1}.$$

In other words, a composition series is a subnormal series whose terms have strictly decreasing dimensions and which is maximal among subnormal series with this property. This disagrees with the usual definition that a composition series is a maximal subnormal series, but it appears to be the correct definition for algebraic groups as few algebraic groups have maximal subnormal series – for example, the infinite chain

$$\mu_l \subset \mu_{l^2} \subset \mu_{l^3} \subset \cdots \subset \mathbb{G}_m$$

shows that $\mathbb{G}_m$ does not.

LEMMA 6.12. *Consider a subnormal series*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

for G. If $\dim G = \dim G_i/G_{i+1}$ for some i, then $G \sim G_i/G_{i+1}$.

PROOF. The maps

$$G_i/G_{i+1} \leftarrow G_i \rightarrow G_{i-1} \rightarrow \cdots \rightarrow G_0 = G$$

are isogenies. □

THEOREM 6.13. *Let G be an algebraic group over a field k. Then G admits a composition series. If*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

and

$$G = H_0 \supset H_1 \supset \cdots \supset H_t = e$$

are both composition series, then $s = t$ and there exists a permutation π of $\{1, 2, \ldots, s\}$ such that G_i/G_{i+1} is isogenous to $H_{\pi(i)}/H_{\pi(i)+1}$ for all i.

PROOF. The existence of a composition series is obvious. For the proof of the second statement, we use the notation of the proof of Theorem 6.3:

$$G_{i,j} \overset{\text{def}}{=} G_{i+1}(H_j \cap G_i)$$

$$H_{j,i} \overset{\text{def}}{=} H_{j+1}(G_i \cap H_j).$$

Note that, for a fixed i, only one of the quotients $G_{i,j}/G_{i,j+1}$ has dimension > 0, say, that with $j = \pi(i)$. Now

$$
\begin{aligned}
G_i/G_{i+1} &\sim G_{i,\pi(i)}/G_{i,\pi(i)+1} & \text{(6.12)} \\
&\approx H_{\pi(i),i}/H_{\pi(i),i+1} & \text{(butterfly lemma)} \\
&\sim H_{\pi(i)}/H_{\pi(i)+1} & \text{(6.12)}.
\end{aligned}
$$

As $i \mapsto \pi(i)$ is a bijection, this completes the proof. □

EXAMPLE 6.14. The algebraic group GL_n has composition series

$$\text{GL}_n \supset \text{SL}_n \supset e$$

$$\text{GL}_n \supset \mathbb{G}_m \supset e$$

with quotients $\{\mathbb{G}_m, \text{SL}_n\}$ and $\{\text{PGL}_n, \mathbb{G}_m\}$ respectively. They have equivalent refinements

$$\text{GL}_n \supset \text{SL}_n \supset \mu_n \supset e$$

$$\text{GL}_n \supset \mathbb{G}_m \supset \mu_n \supset e.$$

REMARK 6.15. If G is connected, then it admits a composition series in which all the G_i are connected. Indeed, given a composition series $(G_i)_i$, we may replace each G_i with G_i°. Then $G_i^\circ \subset G_{i-1}^\circ$, and G_i° is normal in G_{i-1} because it is characteristic in G_i (see 1.52). Therefore $(G_i^\circ)_i$ is still a composition series.

d. The derived groups and commutator groups

Let G be an algebraic group over k.

DEFINITION 6.16. The **derived group** of G is the intersection of the normal algebraic subgroups N of G such that G/N is commutative. It is denoted $\mathcal{D}G$ (or G^{der} or $[G,G]$).

PROPOSITION 6.17. *The quotient $G/\mathcal{D}G$ is commutative (hence $\mathcal{D}G$ is the smallest normal algebraic subgroup with this property).*

PROOF. As in the proof of Proposition 6.10, $\mathcal{D}G$ is an intersection of normal subgroups $N_1, \ldots, N_r$ such that each quotient G/N_i is commutative. Now $G/\mathcal{D}G$ is a subgroup of the commutative group $G/N_1 \times \cdots \times G/N_r$. □

We shall need another description of $\mathcal{D}G$, which is analogous to the description of the derived group as the subgroup generated by commutators.

PROPOSITION 6.18. *If G is affine or smooth, $\mathcal{D}G$ is the algebraic subgroup of G generated by the commutator map*

$$G \times G \to G, \quad (g_1, g_2) \mapsto [g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}.$$

PROOF. Let H be the algebraic subgroup of G generated by G^2 and the map $(g_1, g_2) \mapsto [g_1, g_2]$ (see 2.46, 2.50). By definition, H is the smallest algebraic subgroup containing the commutator subgroup of $G(R)$ for all R. It follows that H is normal in G and that $G(R)/H(R)$ is commutative for all R. As the functor $R \rightsquigarrow G(R)/H(R)$ is fat in G/H, we see that G/H is commutative. If N is another normal subgroup of G such that G/N is commutative, then N contains the image of the commutator map and so $N \supset H$. We conclude that $H = \mathcal{D}G$. □

COROLLARY 6.19. *Assume that G is affine or smooth.*

(a) *For every field $k' \supset k$, $\mathcal{D}G_{k'} = (\mathcal{D}G)_{k'}$.*

(b) *If G is connected (resp. smooth), then $\mathcal{D}G$ is connected (resp. smooth).*

(c) *For every k-algebra R, the group $(\mathcal{D}G)(R)$ consists of the elements of $G(R)$ that lie in the derived group of $G(R')$ for some faithfully flat R-algebra R'.*

(d) *Let H be a commutative algebraic group over k and R a k-algebra. Every homomorphism $G_R \to H_R$ is trivial on $(\mathcal{D}G)_R$.*

(e) *$\mathcal{D}G$ is a characteristic subgroup of G.*

PROOF. (a) The algebraic subgroup generated by a map has this property (Section 2h).

(b) Apply Propositions 2.48, 2.50, and 2.53.

(c) Immediate consequence of the proposition.

(d) Immediate consequence of (c).

(e) Let R be a k-algebra and R' an R-algebra. Clearly the derived group of $G(R')$ is preserved by all automorphisms of G_R, and it follows from (c) that $(\mathcal{D}G)_R$ is preserved by all automorphisms of G_R. □

When G is affine, there is an explicit description of the coordinate ring of $\mathcal{D}G$. Let I_n denote the kernel of the homomorphism $\mathcal{O}(G) \to \mathcal{O}(G^{2n})$ of k-algebras defined by the regular map

$$(g_1, g_2, \ldots, g_{2n}) \mapsto [g_1, g_2] \cdot [g_3, g_4] \cdots : G^{2n} \to G. \tag{37}$$

From the regular maps

$$G^2 \to G^4 \to \cdots \to G^{2n} \to \cdots,$$
$$(g_1, g_2) \mapsto (g_1, g_2, e, e) \mapsto \cdots$$

we get inclusions

$$I_1 \supset I_2 \supset \cdots \supset I_n \supset \cdots,$$

and we let $I = \bigcap I_n$. The coordinate ring of $\mathcal{D}G$ is $\mathcal{O}(G)/I$ (see 2.46).

PROPOSITION 6.20. *Let G be an affine group variety over k.*
  (a) *The coordinate ring of $\mathcal{D}G$ equals $\mathcal{O}(G)/I_n$ for some n.*
  (b) *If k is algebraically closed, then $(\mathcal{D}G)(k) = \mathcal{D}(G(k))$.*

PROOF. (a) We may suppose that G is connected. As G is smooth and connected, so also is G^{2n} (see 3.11). Therefore, each ideal I_n is prime, and a descending sequence of prime ideals in a noetherian ring terminates (CA 21.6).

(b) Let V_n be the image of $G^{2n}(k)$ in $G(k)$. Its closure in $G(k)$ is the zero set of I_n. Being the image of a regular map, V_n contains a dense open subset U of its closure (A.15). Choose n as in the first part, so that the zero set of I_n is $\mathcal{D}G(k)$. Then

$$U \cdot U^{-1} \subset V_n \cdot V_n \subset V_{2n} \subset \mathcal{D}(G(k)) = \bigcup_m V_m \subset \mathcal{D}G(k).$$

It remains to show that $U \cdot U^{-1} = \mathcal{D}G(k)$. Let $g \in \mathcal{D}G(k)$. Because U is open and dense in $\mathcal{D}G(k)$, so is gU^{-1}, which must therefore meet U, forcing g to lie in $U \cdot U^{-1}$. □

PROPOSITION 6.21. *The derived group $\mathcal{D}G$ of a connected group variety G is the unique connected subgroup variety of G such that $(\mathcal{D}G)(k^a) = \mathcal{D}(G(k^a))$.*

PROOF. The derived group has these properties by Corollary 6.19 and Proposition 6.20, and it is the only algebraic subgroup with these properties because $(\mathcal{D}G)(k^a)$ is dense in $\mathcal{D}G$. □

EXAMPLE 6.22. Let $G = \mathrm{GL}_n$. Then $\mathcal{D}G = \mathrm{SL}_n$. Certainly, $\mathcal{D}G \subset \mathrm{SL}_n$. Conversely, every element of $\mathrm{SL}_n(k)$ is a commutator, because $\mathrm{SL}_n(k)$ is generated by elementary matrices, and every elementary matrix is a commutator if k has at least three elements (see 20.24 below for this argument in the case $n = 2$). It follows that $\mathcal{D}(\mathrm{PGL}_n) = \mathrm{PGL}_n$.

REMARK 6.23. The (abstract) group $G(k)$ may have commutative quotients without G having commutative quotients, i.e., we may have $G = \mathcal{D}G$ but $G(k) \neq \mathcal{D}(G(k))$. This is the case for $G = \mathrm{PGL}_n$ if $k^\times \neq k^{\times n}$ because there is a surjection $\det: \mathrm{PGL}_n(k) \to k^\times / k^{\times n}$ (see 5.49) and commutators have determinant 1.

Commutator groups

We need a modest generalization of the derived group. For subgroups H_1 and H_2 of an abstract group G, we let $[H_1, H_2]$ denote the subgroup of G generated by the commutators $[h_1, h_2] = h_1 h_2 h_1^{-1} h_2^{-1}$ with $h_1 \in H_1$ and $h_2 \in H_2$.

DEFINITION 6.24. Let H_1 and H_2 be algebraic subgroups of an algebraic group G. If H_1 and H_2 are smooth or G is affine, we define the ***commutator subgroup*** $[H_1, H_2]$ of G to be the algebraic subgroup generated by the commutator map

$$(h_1, h_2) \mapsto [h_1, h_2]: H_1 \times H_2 \to G.$$

REMARK 6.25. (a) For any k-algebra R, the group $[H_1, H_2](R)$ consists of the elements of $G(R)$ that lie in $[H_1(R'), H_2(R')]$ for some faithfully flat R-algebra R'.

   (b) Let H_1 and H_2 be connected group subvarieties of a connected group variety G. Then $[H_1, H_2]$ is the unique connected subgroup variety of G such that $[H_1, H_2](k^a) = [H_1(k^a), H_2(k^a)]$.

e.   Solvable algebraic groups

DEFINITION 6.26. An algebraic group G is ***solvable*** if there is a subnormal series
$$G = G_0 \supset G_1 \supset \cdots \supset G_t = e$$
such that each quotient G_i / G_{i+1} is commutative (such a series is called a ***solvable series*** for G).

   In other words, G is solvable if it can be constructed from commutative algebraic groups by successive extensions.

PROPOSITION 6.27. *Algebraic subgroups, quotients, and extensions of solvable algebraic groups are solvable.*

PROOF. Let G be a solvable algebraic group. The intersection of a solvable series for G with a subgroup H of G is a solvable series for H (see 6.2), and its image in a quotient Q of G is a solvable series for Q (correspondence theorem 5.55).

   Let G be an algebraic group containing a solvable normal algebraic subgroup N such that G/N is solvable. The inverse image of a solvable series for G/N can be combined with a solvable series for N to give a solvable series for G.   □

EXAMPLE 6.28. The group $\mathbb{T}_n$ of upper triangular matrices is solvable (see 6.49 below). For example,

$$\mathbb{T}_2 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \supset \mathbb{U}_2 = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \supset e$$

is a subnormal series for $\mathbb{T}_2$ with commutative quotients $\mathbb{G}_m \times \mathbb{G}_m$, $\mathbb{G}_a$.

EXAMPLE 6.29. A finite abstract group is solvable if and only if it is solvable when regarded as a constant algebraic group. Thus, the theory of solvable algebraic groups includes the theory of solvable finite groups, which is already rather extensive. A constant algebraic group G is solvable if $G(k)$ does not contain an element of order 2 (Feit–Thompson theorem).

Let G be an algebraic group. Write $\mathcal{D}^2 G$ for the second derived group $\mathcal{D}(\mathcal{D}G)$ of G, $\mathcal{D}^3 G$ for the third derived group $\mathcal{D}(\mathcal{D}^2 G)$ and so on. The **derived series** for G is the normal series

$$G \supset \mathcal{D}G \supset \mathcal{D}^2 G \supset \cdots.$$

If G is smooth, then $\mathcal{D}^n G$ is a smooth characteristic subgroup of G, and each quotient $\mathcal{D}^n G/\mathcal{D}^{n+1} G$ is commutative; if G is also connected, then $\mathcal{D}^n G$ is connected.

PROPOSITION 6.30. *An algebraic group G is solvable if and only if its derived series terminates with e.*

PROOF. If the derived series terminates with e, then it is a solvable series for G. Conversely, if $G \supset G_1 \supset \cdots$ is a solvable series for G, then $G_1 \supset \mathcal{D}G$, $G_2 \supset \mathcal{D}^2 G$, and so on. □

COROLLARY 6.31. *Assume that G is affine or smooth, and let k' be a field containing k. Then G is solvable if and only if $G_{k'}$ is solvable.*

PROOF. The derived series of $G_{k'}$ is obtained from that of G by extension of scalars (6.19a). Hence one series terminates with e if and only if the other does. □

COROLLARY 6.32. *Let G be a solvable algebraic group, and assume that G is affine or smooth. If G is connected (resp. smooth, resp. smooth and connected), then it admits a solvable series whose terms are connected (resp. smooth, resp. smooth and connected).*

PROOF. The derived series has the required property (6.19). □

In particular, a group variety is solvable if and only if it admits a solvable series of group subvarieties.

DEFINITION 6.33. A solvable algebraic group G over k is **split** if it admits a subnormal series $G = G_0 \supset G_1 \supset \cdots \supset G_n = e$ such that each quotient G_i/G_{i+1} is isomorphic to $\mathbb{G}_a$ or to $\mathbb{G}_m$.

Each term G_i in such a subnormal series is smooth, connected, and affine (1.62, 5.59, 2.70); in particular, G itself is smooth, connected, and affine.

NOTES. In the literature, a split solvable algebraic group over k is said to be k-solvable (k-résoluble) or k-split. We adopt the second term, but can omit the "k" because of our convention that statements concerning an algebraic group G over k are always intrinsic to G over k. With this caveat, our definition agrees with those in the literature (Rosenlicht 1963; Borel 1991, 15.1; Springer 1998, 12.3.5; Conrad et al. 2015, A.1, p. 466).

f. Nilpotent algebraic groups

DEFINITION 6.34. An algebraic group G is **nilpotent** if it admits a **central** subnormal series, i.e., a normal series

$$G = G_0 \supset G_1 \supset \cdots \supset G_t = e$$

such that each quotient G_i/G_{i+1} is contained in the centre of G/G_{i+1} (such a series is called a **nilpotent series** for G).

In other words, G is nilpotent if it can be constructed from commutative algebraic groups by successive *central* extensions.

REMARK 6.35. A normal series $G = G_0 \supset G_1 \supset \cdots$ is central if and only if $[G, G_i] \subset G_{i+1}$ for all i.

EXAMPLE 6.36. The group $\mathbb{U}_n$ is nilpotent (see 6.49 below), but not $\mathbb{T}_n$ – the subnormal series in Example 6.28 is not central because

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \frac{a}{b}c \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}.$$

PROPOSITION 6.37. *Algebraic subgroups and quotients (but not necessarily extensions) of nilpotent algebraic groups are nilpotent.*

PROOF. The proof for subgroups and quotients is the same as for solvable groups (6.27). The algebraic group $\mathbb{T}_2$ is an extension of nilpotent (even commutative) groups, but is not itself nilpotent (6.36). □

Let G be a connected group variety. The **descending central series** for G is the subnormal series

$$G^0 = G \supset G^1 = [G, G] \supset \cdots \supset G^i = [G, G^{i-1}] \supset \cdots.$$

PROPOSITION 6.38. *A connected group variety G is nilpotent if and only if its descending central series terminates with e.*

PROOF. If the descending central series terminates with e, then it is a nilpotent series for G. Conversely, if $G \supset G_1 \supset \cdots$ is a nilpotent series for G, then $G_1 \supset G^1$, $G_2 \supset G^2$, and so on. □

COROLLARY 6.39. *A connected group variety G is nilpotent if and only if it admits a nilpotent series whose terms are connected group varieties.*

PROOF. The descending central series has this property (6.19).   □

In particular, a group variety is nilpotent if and only if it admits a nilpotent series of subgroup varieties.

COROLLARY 6.40. *Let G be a nilpotent connected group variety. If $G \neq e$, then it contains a nontrivial connected group variety in its centre.*

PROOF. As $G \neq e$, its descending central series has length at least one, and the last nontrivial term has the required properties.   □

g. Existence of a largest algebraic subgroup with a given property

Let P be a property of algebraic groups. We assume the following:
  (a) every extension of groups with property P has property P;
  (b) every quotient of a group with property P has property P.
For example, "smooth" and "connected" are properties satisfying (a) and (b) (1.62, 5.59).

LEMMA 6.41. *Let H and N be algebraic subgroups of an algebraic group G with N normal. If H and N have property P, then so also does HN.*

PROOF. Consider the diagram in Corollary 5.53. Because H has property P, so also does its quotient $H/H \cap N$. Hence HN/N has property P, and it follows that the same is true of HN.   □

We now assume that the trivial group e has property P. An algebraic group G need not contain a maximal normal algebraic subgroup with property P. For example, quotients and extensions of finite algebraic groups are finite, but $\mathbb{G}_m$ has no largest finite algebraic subgroup – if N is a finite algebraic subgroup, then $N \cdot \mu_\ell^n$ will be larger for some n.

PROPOSITION 6.42. *Every algebraic group G contains a largest smooth connected normal subgroup H with property P. The quotient G/H contains no nontrivial such subgroup.*

PROOF. The group G certainly contains a smooth connected normal subgroup H with property P (e.g., the trivial group) and hence a maximal one (e.g., any of greatest dimension). Let H and N be any two such maximal subgroups. According to Lemma 6.41, HN has the same properties and so $H = HN = N$. This proves the first statement. If G/H contained a nontrivial smooth connected normal algebraic subgroup with property P, then its inverse image in G would properly contain H and would violate the maximality of H.   □

Recall (6.8) that an algebraic group G is strongly connected if it has no algebraic subgroup of finite index. Clearly quotients and extensions of strongly connected algebraic groups are strongly connected.

PROPOSITION 6.43. *Every algebraic group G contains a largest strongly connected normal subgroup H with property P. The quotient G/H contains no nontrivial such subgroup.*

PROOF. The proof is essentially the same as that of Proposition 6.42. □

For example, every algebraic group contains a largest strongly connected finite algebraic subgroup, namely e.

h. Semisimple and reductive groups

It is convenient at this point to introduce the groups that will be the main topic of study for the last third of the book. Throughout this section, all algebraic groups are affine.

6.44. Let G be a connected group variety over k. Extensions and quotients of solvable algebraic groups are solvable (6.27), and so G contains a largest connected solvable normal subgroup variety (6.42). This is called the **radical** $R(G)$ of G. A connected group variety G over an algebraically closed field is said to be **semisimple** if $R(G) = e$. A connected group variety over a field k is **semisimple** if G_{k^a} is semisimple, i.e., if its **geometric radical** $R(G_{k^a})$ is trivial. If k is algebraically closed, then $G/R(G)$ is semisimple.

6.45. An algebraic group G is said to be **unipotent** if every nonzero representation of G has a nonzero fixed vector.[2] Let Q be a quotient of a unipotent group G. A nonzero representation of Q can be regarded as a representation of G, and so has a nonzero fixed vector; hence Q is unipotent. Let G be an algebraic group containing a normal subgroup N such that both N and G/N are unipotent, and let $G \to \mathrm{GL}_V$ be a nonzero representation of G. The subspace V^N is stable under G (see 5.15), and the representation of G on it factors through G/N. As V is nonzero, V^N is nonzero, and so $V^G = (V^N)^{G/N}$ is nonzero. Hence G is unipotent.

6.46. Let G be a connected group variety over k. It follows from 6.45 that among the connected normal unipotent subgroup varieties of G, there is a largest one. This is called the **unipotent radical** $R_u(G)$ of G. A connected group variety G over an algebraically closed field is said to be **reductive** if $R_u(G) = e$. A connected group variety over a field k is said to be **reductive** if G_{k^a} is reductive, i.e., if its **geometric unipotent radical** $R_u(G_{k^a})$ is trivial. If k is algebraically closed, then $G/R_u(G)$ is reductive.

---

[2]Equivalently, for every finite-dimensional representation $r: G \to \mathrm{GL}_V$ of G, there is a basis such that $r(G) \subset \mathbb{U}_n$. For a comparison with other definitions in the literature, see p. 286.

6.47. A connected group variety G is **pseudo-reductive** if $R_u(G) = e$. Every reductive group is pseudo-reductive, but the following example shows that not all pseudo-reductive groups are reductive. In particular, a connected group variety G over k may be pseudo-reductive without G_{k^a} being pseudo-reductive.

6.48. Let $\mathrm{char}(k) = p$, and let $t \in k \smallsetminus k^p$. Let G be the algebraic group over k

$$R \rightsquigarrow \{(x, y) \in R^2 \mid x^p - t y^p \in R^\times\}$$

with the multiplication

$$(x, y)(x', y') = (xx' + tyy', xy' + x'y).$$

Then $\mathcal{O}(G) = k[X, Y, Z]/((X^p - tY^p)Z - 1)$, and G is a connected group variety (the polynomial $(X^p - tY^p)Z - 1$ is irreducible over k^a). Let $\varphi \colon G \to \mathbb{G}_m$ be the homomorphism $(x, y) \mapsto x^p - t y^p$. The kernel N of φ is the algebraic group defined by $X^p - tY^p = 0$, which is reduced but not geometrically reduced (1.27). We have $R_u(G) = e$, but $R_u(G_{k^a}) = (N_{k^a})_{\mathrm{red}} \simeq \mathbb{G}_a$. Thus G is pseudo-reductive but not reductive. (This example is from Springer 1998, 12.1.6, where it is credited to Tamagawa.)

NOTES. Our definitions in this section agree with those in SGA 3 (see XIX 1.2, 1.6, 2.7). Springer (1998, p. 222) defines the unipotent radical of a group variety G over k to be that of G_{k^a}, and notes that in the example in 6.48, this is "not defined over the ground field". For a group variety G over a field k, he calls $R(G)$ and $R_u(G)$ the "k-radical" and "unipotent k-radical" of G. His notions of "reductive" and "k-reductive" coincide with our notions of "reductive" and "pseudo-reductive" (Springer 1998, p. 251).

i.   A standard example

The next example plays a fundamental role in the theory.

6.49. Fix an $n \in \mathbb{N}$. We number the pairs (i, j), $1 \le i < j \le n$, as follows:

$$
\begin{array}{ccccccc}
(1,2) & (2,3) & \cdots & (n-1,n) & (1,3) & \cdots & (n-2,n) & \cdots & (1,n) \\
C_1 & C_2 & & C_{n-1} & C_n & & C_{2n-3} & & C_{\frac{n(n-1)}{2}}.
\end{array}
$$

For $r = 0, \ldots, m = \frac{n(n-1)}{2}$, let $U_n^{(r)}$ and $P_n^{(r)}$ denote the algebraic subgroups of $\mathbb{U}_n$ such that

$$U_n^{(r)}(R) = \{(a_{ij}) \in \mathbb{U}_n(R) \mid a_{ij} = 0 \text{ for } (i, j) = C_l, l \le r\}$$
$$P_n^{(r)}(R) = \{(a_{ij}) \in \mathbb{U}_n(R) \mid a_{ij} = 0 \text{ for } (i, j) = C_l, l \ne r\}$$

for all k-algebras R. In particular, $U_n^{(0)} = \mathbb{U}_n$. For example, when $n = 3$,

$$C_1 = (1,2),\ U_3^{(1)} = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\},\ P_3^{(1)} = \left\{ \begin{pmatrix} 1 & * & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \simeq U_3^{(0)}/U_3^{(1)}$$

$$C_2 = (2,3),\ U_3^{(2)} = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\},\ P_3^{(2)} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \simeq U_3^{(1)}/U_3^{(2)}$$

$$C_3 = (1,3),\ U_3^{(3)} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\},\ P_3^{(3)} = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \simeq U_3^{(2)}/U_3^{(3)}.$$

Then:

(a) Each $U_n^{(r)}$ is a normal algebraic subgroup of $\mathbb{T}_n$, and

$$\mathbb{U}_n = U_n^{(0)} \supset \cdots \supset U_n^{(r)} \supset U_n^{(r+1)} \supset \cdots \supset U_n^{(m)} = e. \tag{38}$$

(b) For $r > 0$, the maps

$$\begin{array}{ccccc} \mathbb{G}_a & \xrightarrow{\ p_r\ } & P_n^{(r)} & \longrightarrow & U_n^{(r-1)}/U_n^{(r)} \\ c & \mapsto & 1 + c E_{i_0 j_0} & \mapsto & \left(1 + c E_{i_0,j_0}\right) \cdot U_n^{(r)}, \end{array}$$

are isomorphisms of algebraic groups. Here $(i_0, j_0) = C_r$ and $E_{i_0 j_0}$ is the matrix with 1 in the (i_0, j_0)th position and zeros elsewhere.

(c) For $r > 0$,

$$A \cdot (1 + c E_{i_0 j_0}) \cdot A^{-1} \equiv 1 + \left(\frac{a_{ii}}{a_{jj}} c \right) E_{i_0 j_0} \pmod{U_n^r(R)}$$

where $A = (a_{ij}) \in \mathbb{T}_n(R)$, $c \in \mathbb{G}_a(R) = R$, and $(i_0, j_0) = C_r$.

Therefore

$$\mathbb{T}_n \supset U_n^{(0)} \supset \cdots \supset U_n^{(r)} \supset U_n^{(r+1)} \supset \cdots \supset U_n^{(m)} = e \tag{39}$$

is a normal series in $\mathbb{T}_n$, with quotients $\mathbb{T}_n/U_n^{(0)} \simeq \mathbb{G}_m^n$ and $U_n^{(r)}/U_n^{(r+1)} \simeq \mathbb{G}_a$. Moreover, the action of $\mathbb{T}_n$ on each quotient $\mathbb{G}_a$ is linear (i.e., factors through the natural action of $\mathbb{G}_m$ on $\mathbb{G}_a$), and $\mathbb{U}_n$ acts trivially on each quotient $\mathbb{G}_a$. Hence, (39) is a solvable series for $\mathbb{T}_n$ and (38) is a central series for $\mathbb{U}_n$, which is therefore nilpotent.

The proofs of (a), (b), and (c) are straightforward, and are left as an exercise to the reader (see SHS, Exp. 12).

Algebraic Groups Acting on Schemes

All schemes are algebraic over k, and all functors are from the category of small k-algebras to sets or groups.

a. Group actions

Recall (Section 1f) that an action of a group functor G on a functor X is a natural transformation $\mu: G \times X \to X$ such that $\mu(R)$ is an action of $G(R)$ on $X(R)$ for all small k-algebras R, and that an action of an algebraic group G on an algebraic scheme X is a regular map $\mu: G \times X \to X$ such that certain diagrams commute. Because of the Yoneda lemma, to give an action of G on X is the same as giving an action of $\tilde{G}$ on $\tilde{X}$. We often write gx or $g \cdot x$ for $\mu(g,x)$. An action μ is ***trivial*** if it factors through the projection $G \times X \to X$.

b. The fixed subscheme

Let $\mu: G \times X \to X$ be an action of a group functor G on a separated algebraic scheme X over k. The next theorem shows that there exists a largest closed subscheme X^G of X on which G acts trivially.

THEOREM 7.1. *The functor $\tilde{X}^G$,*

$$R \rightsquigarrow \{x \in X(R) \mid \mu(g, x_{R'}) = x_{R'} \text{ for all } g \in G(R') \text{ and all } R\text{-algebras } R'\}$$

is represented by a closed subscheme X^G of X.

PROOF. An $x \in X(R)$ defines maps

$$g \mapsto gx_{R'}: G(R') \to X(R')$$
$$g \mapsto x_{R'}: G(R') \to X(R'),$$

natural in the R-algebra R'. Thus, we get two maps $X(R) \to \underline{\mathrm{Mor}}(G_R, X_R)$, natural in R. These are the components of the map γ in the following diagram of functors:

$$
\begin{array}{ccc}
\tilde{X}^G & \longrightarrow & \underline{\mathrm{Mor}}(G, \Delta_X) \\
\downarrow & & \downarrow {\scriptstyle \mathrm{closed}} \\
\tilde{X} & \xrightarrow{\ \gamma\ } & \underline{\mathrm{Mor}}(G, X \times X)
\end{array}
$$

The diagram is cartesian because it is when each functor is evaluated at a k-algebra R. As X is separated, the diagonal Δ_X is a closed subscheme of $X \times X$, and so $\underline{\mathrm{Mor}}(G, \Delta_X)$ is a closed subfunctor of $\underline{\mathrm{Mor}}(G, X \times X)$ (see 1.78). Hence $\tilde{X}^G$ is a closed subfunctor of $\tilde{X}$ (see 1.77), which implies that it is represented by a closed subscheme of X (see 1.76). □

The subscheme X^G is called the **fixed subscheme** for the action. Directly from its definition, one sees that its formation commutes with extension of the base field.

REMARK 7.2. Let $\mu: G \times X \to X$ be an action of a group variety G on an algebraic variety X over k. Then $X^G(k^{\mathrm{a}}) = X(k^{\mathrm{a}})^{G(k^{\mathrm{a}})}$, and so

$$
X^G(k) = X(k) \cap X(k^{\mathrm{a}})^{G(k^{\mathrm{a}})}.
$$

When k is perfect, $(X^G)_{\mathrm{red}}$ is the unique closed subvariety of X such that

$$
(X^G)_{\mathrm{red}}(k^{\mathrm{a}}) = X(k^{\mathrm{a}})^{G(k^{\mathrm{a}})}.
$$

In general, X^G need not be reduced.

c. Orbits and isotropy groups

Let $\mu: G \times X \to X$ be an action of an algebraic group G on an algebraic scheme X. For $x \in X(k)$, the image of the orbit map $\mu_x: G \to X$, $g \mapsto gx$, is locally closed in X (see 1.65). We now define the **orbit** O_x of x to be $\mu_x(|G|)$ equipped with its structure of a reduced subscheme of X.

EXAMPLE 7.3. Let G be an algebraic group over an algebraically closed field k. The orbits of G° acting on G are the connected components of G.

PROPOSITION 7.4. *Let $\mu: G \times X \to X$ be an action of an algebraic group G on an algebraic scheme X, and let $x \in X(k)$.*

(a) *If X is reduced and $G(k^{\mathrm{a}})$ acts transitively on $X(k^{\mathrm{a}})$, then the orbit map $\mu_x: G \to X$ is faithfully flat and $O_x = X$.*

(b) *If G is reduced, then O_x is stable under G and the map $\mu_x: G \to O_x$ is faithfully flat. If G is smooth, then O_x is smooth.*

PROOF. (a) This is a special case of Proposition 1.65(a).

(b) The first statement follows from Proposition 1.65(c) applied to $f = \mu_x$. As μ_x is faithfully flat, the map $\mathcal{O}_{O_x} \to \mu_{x*}(\mathcal{O}_G)$ is injective, and remains so after extension of the base field. Therefore O_x is geometrically reduced, and its smooth locus is nonempty (A.55). By homogeneity (over k^a), the smooth locus equals O_x.   □

PROPOSITION 7.5. *Let* $\mu: G \times X \to X$ *be an action of a smooth algebraic group* G *on an algebraic scheme* X.

(a) *A reduced closed subscheme* Y *of* X *is stable under* G *if and only if* $Y(k^a)$ *is stable under* $G(k^a)$.

(b) *Let* Y *be a subscheme of* X, *and let* $|\bar{Y}|$ *denote the closure of* $|Y|$. *If* Y *is stable under* G, *then* $\left|\bar{Y}\right|_{\mathrm{red}}$ *and* $(|\bar{Y}| \smallsetminus |Y|)_{\mathrm{red}}$ *are stable under* G.

PROOF. (a) As G is geometrically reduced and Y is reduced, $G \times Y$ is reduced (A.43). It follows that $\mu: G \times Y \to X$ factors through Y if and only if $\mu(k^a)$ factors through $Y(k^a)$.

(b) When we identify $X(k^a)$ with $|X_{k^a}|$, the set $\left|\bar{Y}\right|_{\mathrm{red}}(k^a)$ becomes identified with the closure of $Y(k^a)$ in $X(k^a)$. As $G(k^a)$ acts continuously on $X(k^a)$ and stabilizes $Y(k^a)$, it stabilizes the closure of $Y(k^a)$. Now (a) shows that $\left|\bar{Y}\right|_{\mathrm{red}}$ is stable under the action of G. A similar argument applies to $(|\bar{Y}| \smallsetminus |Y|)_{\mathrm{red}}$.   □

For $x \in X(k)$, the *isotropy group* G_x at x is defined to be the fibre of the orbit map $\mu_x: G \to X$ over x. It is a closed subscheme of G, and, for all k-algebras R,

$$G_x(R) = \{g \in G(R) \mid gx_R = x_R\}.$$

This is a subgroup of $G(R)$, and so G_x is an algebraic subgroup of G.

PROPOSITION 7.6. *Let* $G \times X \to X$ *be an action of a smooth algebraic group on an algebraic scheme* X *over* k, *and let* Y *be a nonempty subscheme of* X. *If* Y *has smallest dimension among those stable under* G, *then it is closed.*

PROOF. Let Y be a nonempty stable subscheme of X. Then $(|\bar{Y}| \smallsetminus |Y|)_{\mathrm{red}}$ is stable under G (see 7.5), and

$$\dim(Y) > \dim(|\bar{Y}| \smallsetminus |Y|)_{\mathrm{red}}.$$

If Y has smallest possible dimension, then $|\bar{Y}| = |Y|$.   □

When k is algebraically closed, any nonempty subscheme of smallest dimension among those stable under G is an orbit, and so the proposition implies the orbit lemma (1.66).

DEFINITION 7.7. A nonempty algebraic scheme X with an action of G is a *homogeneous space* under G if $G(k^a)$ acts transitively on $X(k^a)$ and the orbit map $\mu_x: G_{k^a} \to X_{k^a}$ is faithfully flat for some $x \in X(k^a)$.

The orbit map μ_x is then faithfully flat for all $x \in X(k^{\mathrm{a}})$.

ASIDE 7.8. One can ask whether every algebraic G-scheme X over k is a union of homogeneous subspaces. A necessary condition for this is that the k^{a}-points of X over a single point of X lie in a single orbit of $G_{k^{\mathrm{a}}}$. Under this hypothesis, the answer is yes if G is smooth and connected and the field k is perfect, but not in general otherwise. See Exercise 7-1.

d.   The functor defined by projective space

7.9. Let R be a k-algebra. A submodule M of an R-module N is said to be a direct summand of N if there exists another submodule M' of M (a complement of M) such that $N = M \oplus M'$. If M is a direct summand of a finitely generated projective R-module N, then M is also finitely generated and projective, and so $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module of finite rank for every maximal ideal $\mathfrak{m}$ in R (CA 12.6). If $M_{\mathfrak{m}}$ is of constant rank r, then we say that M has **rank r**.

Note that if M is locally a direct summand of R^{n+1} (for the Zariski topology), then the quotient module R^{n+1}/M is also locally a direct summand of R^{n+1}, hence projective, and so M is (globally) a direct summand of R^{n+1}.

7.10. Let

$$P^n(R) = \{\text{direct summands of rank 1 of } R^{n+1}\}.$$

Then P^n is a functor from k-algebras to sets. One can show that P^n is local in the sense of (A.34). Let H_i be the hyperplane $T_i = 0$ in k^{n+1}, and let

$$P_i^n(R) = \{L \in P^n(R) \mid L \oplus H_{iR} = R^{n+1}\}.$$

The P_i^n form an open affine cover of P^n, and so P^n is an algebraic scheme over k (see A.34). We denote it by $\mathbb{P}^n$. When R is a field, every R-subspace of R^{n+1} is a direct summand, and so $\mathbb{P}^n(R)$ consists of the lines through the origin in R^{n+1}.

e.   Quotients of affine algebraic groups

This section provides a treatment of the quotients of affine algebraic groups independent of Appendix B. In particular, we give an explicit construction of G/H when G is smooth and affine, and we sketch a proof of the existence of G/H for a general affine G.

PROPOSITION 7.11. *Let $G \times X \to X$ be an action of an algebraic group on a separated algebraic scheme X, and let $o \in X(k)$. Then (X, o) is the quotient of G by G_o if and only if the orbit map $\mu_o \colon G \to X$ is faithfully flat.*

PROOF. If (X, o) is the quotient of G by G_o, then μ_o is faithfully flat by Proposition 5.25. Conversely, from the definition of G_o, we see that $G_o(R)$ is the stabilizer in $G(R)$ of $o \in X(R)$, and so the condition (a) of Definition 5.20 is satisfied. If μ_o is faithfully flat, then Proposition 5.7 shows that the condition (b) is also satisfied. $\square$

PROPOSITION 7.12. *Let $G \times X \to X$ be an action of a reduced algebraic group G on a separated algebraic scheme X, and let $o \in X(k)$. Assume that the quotient G/G_o exists. Then the orbit map induces an isomorphism $G/G_o \to O_o$.*

PROOF. Because G is reduced, the orbit map μ_0 is faithfully flat (7.4). Hence we can apply Proposition 7.11. $\square$

COROLLARY 7.13. *Let $G \times X \to X$ be an action of a group variety G on an algebraic variety X, and let $o \in X(k)$. Assume that the quotient G/G_o exists. Then the orbit map induces an isomorphism $G/G_o \to O_o$.*

PROOF. Special case of the proposition. $\square$

REMARK 7.14. In the situation of the corollary, the group G_o need not be smooth – consider, for example, the action in characteristic p of SL_p on PGL_p by left translation. In the old literature, the isotropy group H_o is defined to be the reduced subscheme of $(G_{k^a})_o$, which need not be defined over k. Even when it is defined over k, the map $G/H_o \to O_o$ need not be an isomorphism (it is finite and purely inseparable).

PROPOSITION 7.15. *Let H' be an algebraic subgroup of G containing H:*

$$G \supset H' \supset H.$$

If G/H' and G/H exist, then the canonical map $\bar{q} \colon G/H \to G/H'$ is faithfully flat. If the scheme H'/H is smooth (resp. finite) over k, then the morphism $G/H' \to G/H$ is smooth (resp. finite and flat). In particular, the map $G \to G/H$ is smooth (resp. finite and flat) if H is smooth (resp. finite).

PROOF. We have a cartesian square of functors

$$
\begin{array}{ccc}
\tilde{G} \times (\tilde{H}'/\tilde{H}) & \xrightarrow{\ (g,x) \mapsto gx\ } & \tilde{G}/\tilde{H} \\
\downarrow {\scriptstyle (g,x) \mapsto g} & & \downarrow \\
\tilde{G} & \xrightarrow{\quad q' \quad} & \tilde{G}/\tilde{H}'.
\end{array}
$$

On passing to the associated sheaves and applying the Yoneda lemma, we get a cartesian square of algebraic schemes

$$
\begin{array}{ccc}
G \times (H'/H) & \xrightarrow{\ \mu\ } & G/H \\
\downarrow {\scriptstyle p_1} & & \downarrow {\scriptstyle \bar{q}} \\
G & \xrightarrow{\quad q' \quad} & G/H'.
\end{array}
$$

Because q' is faithfully flat, whatever properties p_1 has, so will $\bar{q}$ (see A.80). □

REMARK 7.16. (a) Let H' be an algebraic subgroup of G containing H. Then H'/H is a closed subscheme of G/H, and is the quotient of H' by H. In fact, it is the fibre over the special point of the morphism $G/H \to G/H'$ (see 7.15).

(b) Let H' be an algebraic subgroup of G containing H and having the same dimension as H. Then $\dim(H'/H) = 0$ (see 5.23), and so H'/H is finite (2.14). Therefore the canonical map $G/H \to G/H'$ is finite and flat (7.15). In particular, it is proper.

(c) Consider an algebraic group G acting on an algebraic variety X. Assume that $G(k^{\mathrm{a}})$ acts transitively on $X(k^{\mathrm{a}})$. By homogeneity, X is smooth, and, for any $o \in X(k)$, the map $g \mapsto go \colon G \to X$ defines an isomorphism $G/G_o \to X$. When k is perfect, $(G_o)_{\mathrm{red}}$ is a smooth algebraic subgroup of G (see 1.39), and $G/(G_o)_{\mathrm{red}} \to X$ is finite and purely inseparable by (b).

Existence of the quotient for smooth affine G

PROPOSITION 7.17. *Let $G \times X \to X$ be the action of a smooth algebraic group on a separated algebraic scheme X. For every $o \in X(k)$, the quotient G/G_o exists and the canonical map $G/G_o \to X$ is an immersion.*

PROOF. As G is smooth, the orbit O_o is stable under G and $\mu_o \colon G \to O_o$ is faithfully flat (7.4), and so the pair (O_o, o) is a quotient of G by G_o by (7.11). That $G/G_o \to X$ is an immersion follows from (1.65c). □

THEOREM 7.18. *If G is smooth and affine, then the quotient G/H exists as a separated algebraic scheme for every algebraic subgroup H of G.*

PROOF. According to Chevalley's theorem (4.27), there exists a representation of G on a vector space k^{n+1} such that H is the stabilizer of a one-dimensional subspace L of k^{n+1}. Recall that $\mathbb{P}^n$ represents the functor

$$R \rightsquigarrow \{\text{direct summands of rank 1 of } R^{n+1}\}.$$

The representation of G on k^{n+1} defines a natural action of $G(R)$ on the set $\mathbb{P}^n(R)$, and hence an action of G on $\mathbb{P}^n$ (Yoneda lemma). For this action of G on $\mathbb{P}^n$, H is the isotropy group at L regarded as an element of $\mathbb{P}^n(k)$. Now Proposition 7.17 completes the proof . □

EXAMPLE 7.19. The proof of Theorem 7.18 shows that, for every representation (V, r) of G and line L, the orbit of L in $\mathbb{P}(V)$ is a quotient of G by the stabilizer of L in G. For example, let $G = \mathrm{GL}_2$ and let $H = \mathbb{T}_2 = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$. Then H is the subgroup fixing the line $L = \{\left(\begin{smallmatrix} * \\ 0 \end{smallmatrix}\right)\}$ in the natural action of G on k^2. Hence G/H is isomorphic to the orbit of L, but G acts transitively on the set of lines, and so $G/H \simeq \mathbb{P}^1$. In particular, the quotient is a complete variety.

Existence of the quotient for nonsmooth affine G

To remove the "smooth" from Theorem 7.18, it suffices to remove the "smooth" from Proposition 7.17.

PROPOSITION 7.20. *Let $G \times X \to X$ be the action of an algebraic group on a separated algebraic scheme X. For every $o \in X(k)$, the quotient G/G_o exists and the canonical map $G/G_o \to X$ is an immersion.*

PROOF. When G is smooth, this becomes Proposition 7.17. Otherwise, there exists a finite purely inseparable extension k' of k and a smooth algebraic subgroup G' of $G_{k'}$ such that $G'_{k^a} = (G_{k^a})_{red}$ (see 1.59). Let $H = G_o$ and let $H' = G'_o = H_{k'} \cap G'$. Then G'/H' exists as an algebraic scheme over k' because G' is smooth. Now $G_{k'}/H_{k'}$ exists because this is true for the algebraic subgroups G' and H', which are defined by nilpotent ideals, and we can apply Lemma 7.24 below. Therefore G/H exists because $(G/H)_{k'} \simeq G_{k'}/H_{k'}$ exists and we can apply Lemma 7.21 below.

In proving that $i: G/G_o \to X$ is an immersion, we may suppose that k is algebraically closed. As i is a monomorphism, there exists an open subset U of X such that $i^{-1}U \neq \emptyset$ and $U \to X$ is an immersion (A.35). Now the open sets $i^{-1}(gU) = g i^{-1}(U)$, $g \in G(k)$, cover G/G_o.   □

LEMMA 7.21. *Let K/k be a finite purely inseparable extension of fields, and let F be a sheaf on Alg_k. If the restriction of F to Alg_K is representable by an algebraic scheme over K, then F is representable by an algebraic scheme over k.*

PROOF. See DG, III, 2, 7.4. In the affine case, which is all we need, this follows from the elementary result Theorem B.18.   □

LEMMA 7.22. *Let S be an algebraic scheme and let $R \rightrightarrows S$ be an equivalence relation on S such that the first projection $R \to S$ is faithfully flat of finite presentation. Let S_0 be a subscheme of S defined by a nilpotent ideal that is saturated for the relation R, and let R_0 be the induced relation on S_0. If S_0/R_0 exists as a scheme, so also does S/R.*

PROOF. See DG, III, 2, 7.1, 7.2.   □

LEMMA 7.23. *Let R_0 and R be equivalence relations on a scheme S. Assume: R and S are algebraic; R_0 is the subscheme of R defined by a nilpotent ideal; and the canonical projections $R_0 \to S$ and $R \to S$ are flat. If S/R_0 is an algebraic scheme over k, then so also is G/R.*

PROOF. See DG, III, §2, 7.3.   □

LEMMA 7.24. *Let G be an algebraic group G_0, H, and H_0 subgroups of G with $H_0 \subset G_0$. Assume that G_0 (resp. H_0) is the subgroup of G (resp. H) defined by a nilpotent ideal. Then G/H exists if G_0/H_0 exists.*

PROOF. If G_0/H_0 exists, then so also does G/H_0 (by 7.22). Hence G/H exists by Lemma 7.23 applied to the equivalence schemes $G \times_{G/H} G \simeq G \times H$ and $G \times_{G/H_0} G \simeq G \times H_0$. In particular, as H_0/H_0 is trivial, we see that H/H_0 is an algebraic scheme such that $|H/H_0|$ has only a single point, and so H/H_0 is affine. □

f. Linear actions on schemes

In this section, G is an affine algebraic group over k.

Affine case

A representation (V, r) of G is, in particular, an action of G on $V_\mathfrak{a}$. The left action of G on V defines right actions of G on $V^\vee$ and its symmetric powers. In particular, it defines an action of G on $\operatorname{Sym}(V^\vee) = \mathcal{O}(V_\mathfrak{a})$. This is the action corresponding to the action of G on $V_\mathfrak{a}$.

PROPOSITION 7.25. *Let $G \times X \to X$ be an action of G on an affine algebraic scheme X over k. There exists a finite-dimensional representation (V, r) of G and an equivariant closed immersion $X \hookrightarrow V_\mathfrak{a}$.*

PROOF. The k-algebra $\mathcal{O}(X)$ is finitely generated, and so some finite-dimensional G-stable subspace V contains a generating set for $\mathcal{O}(X)$ (see 4.8). The G-equivariant map $V \hookrightarrow \mathcal{O}(X)$ of k-vector spaces extends to an equivariant homomorphism $\operatorname{Sym}(V) \to \mathcal{O}(X)$ of k-algebras. This is surjective, and so the equivariant map $X \to (V^\vee)_\mathfrak{a}$ of k-schemes it defines is a closed immersion. □

General case

DEFINITION 7.26. An action of G on an algebraic scheme X over k is said to be ***linear*** if there exists a representation $r: G \to \operatorname{GL}_V$ of G on a finite-dimensional vector space V and an equivariant immersion $X \hookrightarrow \mathbb{P}(V)$.

PROPOSITION 7.27. *Let $G \times X \to X$ be a transitive action of G on an algebraic variety X over k. If $X(k)$ is nonempty then the action is linear.*

PROOF. Let $o \in X$. Then the orbit map $\mu_o: G/G_o \to X$ is an immersion. As X is reduced and the action is transitive, the orbit map is an isomorphism. The proof of Theorem 7.18 shows that the action of G on G/G_o is linear. □

REMARK 7.28. In the situation of the proposition, we can choose the representation (V, r) so that the G-equivariant immersion $X \hookrightarrow \mathbb{P}(V)$ does not factor through $\mathbb{P}(W)$ for any subrepresentation W of V. We then say that the embedding $X \hookrightarrow \mathbb{P}(V)$ is ***nondegenerate***.

g. Flag varieties

A *flag* F in finite-dimensional vector space V is a sequence of distinct subspaces $0 = V_0 \subset V_1 \subset \cdots \subset V_r = V$ of V. If $r = \dim V$, then $\dim V_i = i$ for all i and F is a *maximal flag*.

Let F be a flag in V, and let $\mathcal{B}(F)$ be the functor sending a k-algebra R to the set of sequences of R-modules

$$0 = F_0 \subset F_1 \subset \cdots \subset F_r = R \otimes V$$

with F_i a direct factor of $R \otimes V$ of rank $\dim(V_i)$.

PROPOSITION 7.29. *Let F be a flag in a finite-dimensional vector space V, and let $B(F)$ be the algebraic subgroup of GL_V fixing F. Then $\mathrm{GL}_V / B(F)$ represents the functor $\mathcal{B}(F)$.*

PROOF. The functor $R \rightsquigarrow \mathrm{GL}_V(R)/B(F)(R)$ is a fat subfunctor of both $\mathcal{B}(F)$ and $R \rightsquigarrow (\mathrm{GL}_V / B(F))(R)$. $\square$

A variety of the form $\mathrm{GL}_V / B(F)$ is called a *flag variety*.

PROPOSITION 7.30. *Flag varieties are projective (hence complete).*

PROOF. This is a standard basic result in algebraic geometry. We sketch the proof.

Let V be a vector space of dimension n over a field k, and let $G_d(V)$ be the set of subspaces W of dimension d. Then $\bigwedge^d W$ is a one-dimensional subspace of $\bigwedge^d V$, and the condition that a line in $\bigwedge^d V$ be of this form is a polynomial condition. Therefore the map $W \mapsto \bigwedge^d W$ realizes $G_d(V)$ as a closed subvariety of $\mathbb{P}(\bigwedge^d V)$, called the *Grassmann variety* of d-dimensional subspaces of V.

Now let $0 < d_1 < \cdots < d_r = n$. Then $G_{d_1}(V) \times \cdots \times G_{d_r}(V)$ parameterizes families of subspaces $(V_1, \ldots, V_r)$ of V with $\dim V_i = d_i$. The condition that V_i be contained in V_{i+1} is a polynomial condition. Therefore the variety of flags of dimensions $d_1, \ldots, d_r$ is a closed subvariety of $G_{d_1}(V) \times \cdots \times G_{d_r}(V)$. As closed subvarieties and products of projective varieties are again projective varieties, this shows that flag varieties are projective. $\square$

Exercises

EXERCISE 7-1. Let G be a connected group variety acting on algebraic variety X. A subscheme of X is homogeneous if it is a homogeneous space for the action of G.

(a) Show that a point of x of X lies in a homogeneous subscheme of X if $\kappa(x)$ is separable over k and the k^{a}-points of X over x lie in a single $G_{k^{\mathrm{a}}}$-orbit.

(b) Show that (a) may fail if the k^{a}-points of X over x do not lie in a single orbit (e.g., if G is the trivial group).

(c) Show that (a) may fail if G is not connected. [Consider the natural action of μ_n on $X = \mathbb{G}_m$, and let x be such that $[\kappa(x):k]$ does not divide n.]

(d) Show that (a) may fail without the separability condition. [Let $G = \{(u,v) \mid v^p = u - tu^p\}$, $t \in k \smallsetminus k^p$. Then G is a smooth algebraic group, which acts on $\mathbb{P}^2$ by $(u,v)(a\!:\!b\!:\!c) = (a + uc\!:\!b + vc\!:\!c)$. The Zariski closure X of G in $\mathbb{P}^2$ has a unique point x on the line at infinity, and $\kappa(x) = k(t)$. Then $X \smallsetminus \{x\} = G$ with G acting by translation, and so it is a homogeneous space for G, but the complement $\{x\}$ of $X \smallsetminus \{x\}$ in X is not a homogeneous space – it is not even smooth.]

See <https://mathoverflow.net/>, question 150207.

EXERCISE 7-2. Let G be a group variety acting on irreducible varieties X and Y, and assume that the actions of $G(k^{\mathrm{a}})$ on $X(k^{\mathrm{a}})$ and $Y(k^{\mathrm{a}})$ are transitive. Let $\varphi\colon X \to Y$ be an equivariant quasi-finite dominant morphism. Show that φ is finite (hence proper).

The Structure of General Algebraic Groups

In this chapter, we explain the position that affine algebraic groups occupy within the category of all algebraic groups.

a. Summary

Every smooth connected algebraic group G over a field k contains a largest smooth connected *affine* normal algebraic subgroup N (see 8.2). When k is perfect, the quotient G/N is an abelian variety (Barsotti–Chevalley theorem 8.27); otherwise G/N may be an extension of a unipotent algebraic group by an abelian variety (8.8).

On the other hand, every connected algebraic group G contains a connected affine normal algebraic subgroup N (not necessarily smooth) such that G/N is an abelian variety (8.28). If k is perfect and G is smooth, then N is smooth, and it agrees with the group in the preceding paragraph.

smooth ●
    | unipotent   smooth ●   ●
    ● | abelian variety | abelian variety
    | abelian variety   ●   ●
    ● | smooth affine | affine
    | smooth affine e ● e ●
e ●   base field perfect
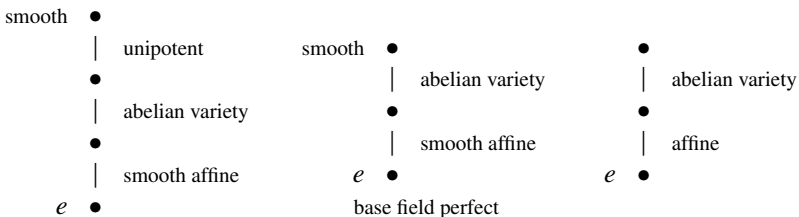
Finally, every algebraic group G has a greatest affine algebraic quotient $G \to G^{\mathrm{aff}}$ (see 8.36). The algebraic groups arising as the kernel N of such a quotient map are the anti-affine groups, i.e., those with $\mathcal{O}(N) = k$. The anti-affine groups are smooth, connected, and commutative (8.14, 8.37). In nonzero characteristic, they are semi-abelian varieties, i.e., extensions of abelian varieties

148

by tori, but in characteristic zero they may also be an extension of a semi-abelian variety by a vector group (Section 8i).

b. Normal affine algebraic subgroups

We include the next statement for reference.

PROPOSITION 8.1. *Let*

$$e \to N \to G \to Q \to e$$

be an exact sequence of algebraic groups.
  (a) *If N and Q are affine (resp. smooth, resp. connected), then G is affine (resp. smooth, resp. connected).*
  (b) *If G is affine (resp. smooth, resp. connected), then Q is affine (resp. smooth, resp. connected).*

PROOF. See 1.62, 2.70, 5.29, and 5.59. □

In particular, extensions and quotients of connected affine group varieties are again connected affine group varieties.

PROPOSITION 8.2. *Every algebraic group G contains a largest smooth connected affine normal subgroup N. The quotient G/N contains no nontrivial such subgroup.*

PROOF. Every smooth connected affine normal subgroup of greatest dimension is such a subgroup N (6.42). □

c. Pseudo-abelian varieties

DEFINITION 8.3. A *pseudo-abelian variety* is a smooth connected algebraic group in which every smooth connected affine normal algebraic subgroup is trivial.

EXAMPLE 8.4. Abelian varieties are pseudo-abelian: every algebraic subgroup is closed (1.41), hence complete (A.75a), hence finite if affine (A.75g), and hence trivial if also smooth and connected (A.75).

PROPOSITION 8.5. *Pseudo-abelian varieties remain pseudo-abelian under separable algebraic field extensions.*

PROOF. Let G be a pseudo-abelian variety over k. If the statement is false, then there exists a finite Galois extension k' of G such that the largest smooth connected affine normal subgroup N of $G_{k'}$ is nontrivial. Because it is unique, N is stable under the action of the Galois group, and hence is defined over k (see 1.54), which is a contradiction. □

PROPOSITION 8.6. *Let G be a smooth connected algebraic group. There exists a unique smooth connected affine normal subgroup N of G such that G/N is a pseudo-abelian variety.*

PROOF. The largest smooth connected affine normal subgroup N of G has the required property (8.2). If N' is a second smooth connected affine normal subgroup of G such that G/N' is pseudo-abelian, then N' is maximal among the smooth connected affine normal subgroups of G, and so equals N.   □

COROLLARY 8.7. *The formation of the subgroup N in 8.2 commutes with separable extensions of the base field.*

PROOF. Proposition 8.5 shows that it retains the properties that determine it uniquely.   □

REMARK 8.8. Later (8.26) we shall show that, over a perfect field, all pseudo-abelian varieties are abelian varieties. Over an arbitrary base field, Totaro (2013) shows that every pseudo-abelian variety G is an extension of a connected unipotent group variety U by an abelian variety A in a unique way.

d.   Local actions

PROPOSITION 8.9. *Let $G \times X \to X$ be an algebraic group acting on an irreducible algebraic scheme X over k. If the action is faithful and there is a fixed point $P \in X(k)$, then G is affine.*

PROOF. Because G fixes P, it acts on the local ring $\mathcal{O}_P$ at P. For $n \in \mathbb{N}$, the formation of $\mathcal{O}_P/\mathfrak{m}_P^{n+1}$ commutes with extension of the base, and so the action of G defines homomorphisms $G(R) \to \mathrm{Aut}(R \otimes_k (\mathcal{O}_P/\mathfrak{m}_P^{n+1}))$ for all small k-algebras R. These are natural in R, and so arise from a homomorphism $\rho_n \colon G \to \mathrm{GL}_{\mathcal{O}_P/\mathfrak{m}_P^{n+1}}$ of algebraic groups. Let $H_n = \mathrm{Ker}(\rho_n)$, and let H denote the intersection of the descending sequence of algebraic subgroups $\cdots \supset H_n \supset H_{n+1} \supset \cdots$. Because G is noetherian, there exists an n_0 such that $H = H_n$ for all $n \geq n_0$.

Let $\mathcal{I}$ be the sheaf of ideals in $\mathcal{O}_X$ corresponding to the closed algebraic subscheme X^H of X. Then $\mathcal{I}\mathcal{O}_P \subset \mathfrak{m}_P^n$ for all $n \geq n_0$, and so $\mathcal{I}\mathcal{O}_P \subset \bigcap_n \mathfrak{m}_P^n$, which is zero by the Krull intersection theorem (CA 3.16). It follows that X^H contains an open neighbourhood of P. As X^H is closed and X is irreducible, X^H equals X. Therefore $H = e$, and the representation of G on $\mathcal{O}_P/\mathfrak{m}_P^{n+1}$ is faithful for all $n \geq n_0$. This means that $\rho_n \colon G \to \mathrm{GL}_{\mathcal{O}_P/\mathfrak{m}_P^{n+1}}$ is a monomorphism, hence a closed immersion (5.34), and so G is affine.   □

COROLLARY 8.10. *Let G be a connected algebraic group and $\mathcal{O}_e$ the local ring at the neutral element e. The action of G on itself by conjugation defines a representation of G on the k-vector space $\mathcal{O}_e/\mathfrak{m}_e^{n+1}$. For all sufficiently large n, the kernel of this representation is the centre of G.*

PROOF. Apply the above proof to the faithful action $G/Z \times G \to G$.   □

COROLLARY 8.11. *The quotient of a connected algebraic group by its centre is affine.*

PROOF. The action of G/Z on G by conjugation is faithful with fixed point e. □

e.   Anti-affine algebraic groups and abelian varieties

Recall that a group variety G over k is anti-affine if $\mathcal{O}(G) = k$. For example, a complete connected group variety is anti-affine. Every homomorphism $\varphi \colon G \to H$ from an anti-affine group variety to an affine algebraic group is trivial (because φ is the morphism corresponding to the trivial homomorphism $\mathcal{O}(H) \to \mathcal{O}(G)$; A.12). In particular, an algebraic group that is both affine and anti-affine is trivial.

PROPOSITION 8.12. *Every homomorphism from an anti-affine algebraic group G to a connected algebraic group H factors through the centre of H.*

PROOF. From the homomorphism $G \to H$ and the action of H on itself by conjugation, we obtain a representation G on the k-vector space $\mathcal{O}_{H,e}/\mathfrak{m}_e^{n+1}$ ($n \in \mathbb{N}$). Because G is anti-affine, this is trivial, which implies that $G \to H$ factors through $Z(H) \hookrightarrow H$ (see 8.10).   □

COROLLARY 8.13. *Let G be a connected algebraic group. Every anti-affine algebraic subgroup H of G is contained in the centre of G.*

PROOF. Apply the proposition to the inclusion map.   □

COROLLARY 8.14. *Every anti-affine algebraic G is commutative and connected.*

PROOF. Corollary 8.13 shows that G is commutative. The map $G \to \pi_0(G)$ is surjective, but $\pi_0(G)$ is affine, and so it is trivial.   □

DEFINITION 8.15. An ***abelian subvariety*** of an algebraic group is a complete connected subgroup variety.

f.   Rosenlicht's decomposition theorem.

Recall that a ***rational map*** $\phi \colon X \dashrightarrow Y$ of algebraic varieties is an equivalence class of pairs (U, ϕ_U) with U a dense open subset of X and ϕ_U a morphism $U \to Y$; in the equivalence class, there is a pair with largest U (and U is called "the open subvariety on which ϕ is defined"). We shall need to use the following results, which are proved, for example, in Milne 1986.

8.16. Every rational map from a normal variety to a complete variety is defined on an open set whose complement has codimension ≥ 2 (*ibid.* 3.2).

8.17. Every rational map from a smooth variety to a connected group variety is defined on an open set whose complement is either empty or has pure codimension 1 (*ibid.* 3.3).

8.18. Every rational map from a smooth variety V to an abelian variety A is defined on the whole of V (combine 8.16 and 8.17).

8.19. Every regular map from a connected group variety to an abelian variety sending e to e is a homomorphism (*ibid.* 3.6).

8.20. Every abelian variety is commutative (8.14, or apply 8.19 to $x \mapsto x^{-1}$).

8.21. Multiplication by a nonzero integer on an abelian variety is faithfully flat with finite kernel (*ibid.* 8.2).

LEMMA 8.22. *Let G be a commutative connected group variety over k, and let*

$$(v,g) \mapsto v + g : V \times G \to V$$

be a G-torsor. There exists a morphism $\phi : V \to G$ and an integer n such that $\phi(v + g) = \phi(v) + ng$ for all $v \in V$, $g \in G$.

PROOF. Suppose first that $V(k)$ contains a point P. Then

$$g \mapsto g + P : G \to V$$

is an isomorphism. Its inverse $\phi : V \to G$ sends a point v of V to the unique point $(v - P)$ of G such that $P + (v - P) = v$. In this case $\phi(v + g) = \phi(v) + ng$ with $n = 1$.

In the general case, because V is an algebraic variety, there exists a $P \in V$ whose residue field $K \overset{\text{def}}{=} \kappa(P)$ is a finite *separable* extension of k (of degree n, say). Let $P_1, \ldots, P_n$ be the k^a-points of V lying over P, and let $\tilde{K}$ denote the Galois closure (over k) of K in k^a. Then the P_i lie in $V(\tilde{K})$. Let $\Gamma = \text{Gal}(\tilde{K}/k)$.

For each i, we have a morphism

$$\phi_i : V_{\tilde{K}} \to G_{\tilde{K}} \quad v \mapsto (v - P_i)$$

defined over $\tilde{K}$. The sum $\sum \phi_i$ is Γ-equivariant, and so arises from a morphism $\phi : V \to G$ over k. For $g \in G$,

$$\phi(v + g) = \sum_{i=1}^{n} \phi_i(v + g) = \sum_{i=1}^{n} (\phi_i(v) + g) = \phi(v) + ng. \qquad \square$$

PROPOSITION 8.23. *Let A be an abelian subvariety of a connected group variety G. There exists a regular map $\phi : G \to A$ and an integer n such that $\phi(g + a) = \phi(g) + na$ for all $g \in G$ and $a \in A$.*

PROOF. Because A is a normal subgroup of G (even central, see 8.13), it is the kernel of a quotient map $\pi: G \to Q$ (5.14), which is smooth because A is smooth (1.63). Let K be the field of rational functions on Q, and let $V \to \mathrm{Spm}(K)$ be the map obtained by pull-back with respect to $\mathrm{Spm}(K) \to Q$. Then V is an A_K-torsor over K (see 5.27). The morphism $\phi: V \to A_K$ over K given by the lemma extends to a rational map $G \dashrightarrow Q \times A$ over k. On projecting to A, we get a rational map $G \dashrightarrow A$. This extends to a morphism $\phi: G \to A$ (see 8.18) satisfying

$$\phi(g + a) = \phi(g) + na$$

on a dense open subset of G, and hence on the whole of G. $\qquad\square$

The next theorem says that every abelian subvariety of an algebraic group has an almost-complement. It is a key ingredient in Rosenlicht's proof of the Barsotti–Chevalley theorem.

THEOREM 8.24 (ROSENLICHT DECOMPOSITION THEOREM). *Let A be an abelian subvariety of a connected group variety G. There exists a normal algebraic subgroup N of G such that the map*

$$(a, n) \mapsto an: A \times N \to G \tag{40}$$

is a faithfully flat homomorphism with finite kernel. When k is perfect, N can be chosen to be smooth.

PROOF. Let $\phi: G \to A$ be the map given by Proposition 8.23. After we apply a translation, this will be a homomorphism (8.19) whose restriction to A is multiplication by n. The kernel of ϕ is a normal algebraic subgroup N of G.

Because A is contained in the centre of G (see 8.13), the map (40) is a homomorphism. It is surjective, hence faithfully flat (1.71), because its image contains N and the homomorphism $A \to G/N \simeq A$ it induces is the surjective map multiplication by n. Its kernel is $A \cap N$, which is the finite group scheme A_n (see 8.21).

When k is perfect, we can replace N with N_{red}, which is a smooth algebraic subgroup of N (1.39). $\qquad\square$

g.   Rosenlicht's dichotomy

The next result is the second key ingredient in Rosenlicht's proof of the Barsotti–Chevalley theorem.

PROPOSITION 8.25. *Let G be a connected group variety over an algebraically closed field k. Either G is complete or it contains an affine algebraic subgroup of dimension > 0.*

Suppose that G is not complete (so $\dim G > 0$), and let X denote G regarded as a left homogeneous space for G. We may hope[1] that X can be embedded as a dense open subvariety of a complete variety $\bar{X}$ in such a way that the action of G on X extends to $\bar{X}$. The action of G on $\bar{X}$ then preserves $E \overset{\text{def}}{=} \bar{X} \smallsetminus X$. Let $P \in E$, and let H be the isotropy group at P. Then H is an algebraic subgroup of G and

$$\dim(G) - \dim(H) \overset{5.23}{=} \dim(G/H) \leq \dim E \leq \dim G - 1,$$

and so $\dim(H) \geq 1$. As H fixes P and acts faithfully on $\bar{X}$, it is affine (8.9).

The above sketch is essentially Rosenlicht's original proof of the proposition, except that, lacking an equivariant completion of X, he works with an "action" of G on $\bar{X}$ given by a rational map $G \times \bar{X} \dashrightarrow \bar{X}$ (Rosenlicht 1956, Lemma 1, p. 437). We refer the reader to Brion et al. 2013, 2.3, or Milne 2013, 4.1, for the details.

h. The Barsotti–Chevalley theorem

THEOREM 8.26. *Every pseudo-abelian variety over a perfect field is complete (hence an abelian variety).*

PROOF. Let G be a pseudo-abelian variety over perfect field k. Because of Proposition 8.5, we may suppose that k is algebraically closed. We use induction on the dimension of G. Let $Z = Z(G)$.

Suppose first that Z has dimension zero, and hence is affine. For large n, the sequence

$$e \to Z \to G \to \mathrm{GL}_{\mathcal{O}_e / \mathfrak{m}_e^{n+1}}$$

is exact (8.10), and it realizes G as an extension of affine algebraic groups. Therefore G is affine (8.1a), and, as $\mathcal{O}(G) = k$, it equals the trivial algebraic group, which is indeed complete.

Now assume that $\dim(Z) > 0$. If Z_{red} is complete, then there exists a smooth almost-complement N to Z_{red} (see 8.24). As $G = Z_{\mathrm{red}} \cdot N$, every connected affine normal subgroup variety of N is normal in G, and hence trivial. Therefore N is pseudo-abelian, and so, by the induction hypothesis, it is complete. As G is a quotient of $Z_{\mathrm{red}} \times N$, it also is complete (A.75d).

If Z_{red} is not complete, then it contains a connected affine subgroup variety N of dimension > 0 (see 8.25). Because N is contained in the centre of G, it is normal in G, which contradicts the hypothesis on G. □

THEOREM 8.27 (BARSOTTI 1955; CHEVALLEY 1960). *Let G be a connected group variety G over a perfect field. Then G contains a unique connected affine normal subgroup variety N such that G/N is an abelian variety.*

---

[1] Indeed, every homogeneous space X for G can be embedded equivariantly as a dense open subset of a complete variety (8.44), but the proof uses Proposition 8.25.

PROOF. According to Proposition 8.6, G contains a unique connected affine normal subgroup variety N such that G/N is a pseudo-abelian variety, but, because the ground field is perfect, "pseudo-abelian variety" is the same as "abelian variety". □

On weakening the hypotheses in the theorem, we obtain a weaker statement.

THEOREM 8.28. *Let G be a connected algebraic group over a field k. Then G contains a connected affine normal algebraic subgroup N such that G/N is an abelian variety.*

PROOF. Suppose first that G is smooth. It follows from Proposition 8.26 that there exists a finite purely inseparable extension k' of k such that $G_{k'}$ acquires a connected affine normal algebraic subgroup N' for which $G_{k'}/N'$ is complete. Let $G' = G_{k'}$. By induction on the degree of k' over k, we may suppose that $k'^p \subset k$. Consider the Frobenius map $F: G' \to G'^{(p)}$. Let N be the pull-back under F of the algebraic subgroup $N'^{(p)}$ of $G'^{(p)}$. If $\mathcal{I}' \subset \mathcal{O}_{G'}$ is the sheaf of ideals defining N', then the sheaf of ideals $\mathcal{I}$ defining N is generated by the pth powers of the local sections of $\mathcal{I}'$. As $k'^p \subset k$, we see that $\mathcal{I}$ is generated by local sections of $\mathcal{O}_G$, and so there is a subgroup N_0 of G such that $N_{0k'} = N$. Now N_0 is connected, normal, and affine because N is, and G/N_0 is complete because G'/N is complete (it is a quotient of G'/N').

For a general G, we use that the kernel of the Frobenius map $F^n: G \to G^{(p^n)}$ is finite (hence affine) and that $G^{(p^n)}$ is smooth for large enough n (see 2.29). Let N' be a connected affine normal algebraic subgroup of $G^{(p^n)}$ such that $G^{(p^n)}/N'$ is complete. Its inverse image in G is the required subgroup. □

COROLLARY 8.29. *Every pseudo-abelian variety is commutative.*

PROOF. Let G be a pseudo-abelian variety. Because G is smooth and connected, so also is its commutator subgroup $\mathcal{D}G$ (see 6.19). Let N be as in Theorem 8.28. As G/N is commutative, $\mathcal{D}G \subset N$. Therefore $\mathcal{D}G$ is affine. As it is a smooth connected normal subgroup of G, it is trivial. □

Notes

8.30. The subgroup variety N in Theorem 8.27 is characterized by each of the following properties: (a) it is the largest connected affine subgroup variety of G; (b) it is connected, affine, and normal, and the quotient G/N is complete; (c) it is the smallest connected affine normal subgroup variety of G such that G/N is complete. From (b) we see that the formation of N commutes with extension of the base field.

8.31. The algebraic subgroup N in Theorem 8.28 need not be smooth even when G is smooth.

8.32. Let G be a connected algebraic group over k. If N_1 and N_2 are affine normal algebraic subgroups of G such that G/N_1 and G/N_2 are complete, then $G/N_1 \cap N_2$ is also complete because there is a closed immersion $G/N_1 \cap N_2 \hookrightarrow G/N_1 \times G/N_2$. If G/N is complete, then so also is G/N°. Therefore, the subgroup N in Theorem 8.28 is the smallest affine normal subgroup of G such that G/N is complete.

8.33. The map $G \to G/N = A$ in Theorem 8.27 is universal among maps from G to an abelian variety sending e to e. Therefore (by definition) A is the Albanese variety of G and $G \to A$ is the Albanese map. In his proof of Theorem 8.27, Chevalley begins with the Albanese map $G \to A$ of G, and proves that its kernel is affine. The above proof Theorem 8.27 is that of Rosenlicht 1956. The first published proof of the theorem is in Barsotti 1955.

i.   Anti-affine groups

Let G be an algebraic group over k. We shall show (8.36) that the k-algebra $\mathcal{O}(G)$ is finitely generated. As in the affine case (Section 3b), the map $\mathcal{O}(m)$ then defines a Hopf algebra structure on $\mathcal{O}(G)$, and so

$$G^{\mathrm{aff}} \stackrel{\mathrm{def}}{=} \mathrm{Spm}(\mathcal{O}(G), \mathcal{O}(m))$$

is an affine algebraic group over k.

Let A be a k-algebra. To give a morphism $G \to \mathrm{Spm}(A)$ of k-schemes is the same as giving a homomorphism of k-algebras $A \to \mathcal{O}(G)$:

$$\mathrm{Hom}(G, \mathrm{Spm}(A)) \simeq \mathrm{Hom}(A, \mathcal{O}(G)) \qquad (41)$$

(see A.13). When A has a Hopf algebra structure, group homomorphisms correspond under (41) to Hopf algebra homomorphisms. Therefore, for an affine algebraic group H,

$$\mathrm{Hom}(G, H) \simeq \mathrm{Hom}(G^{\mathrm{aff}}, H). \qquad (42)$$

Let $\phi: G \to G^{\mathrm{aff}}$ be the homomorphism corresponding in (41) to the identity map on $\mathcal{O}(G)$. Then (42) shows that ϕ is universal among homomorphisms from G to affine algebraic groups.

PROPOSITION 8.34. *Every Hopf algebra over k is a directed union of finitely generated Hopf subalgebras over k.*

PROOF. Let (A, Δ) be a Hopf k-algebra. By Proposition 4.7, every finite subset of A is contained in a finite-dimensional k-subspace V such that $\Delta(V) \subset V \otimes A$. Let (e_i) be a basis for V as a k-vector space, and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. Then $\Delta(a_{ij}) = \sum_k a_{ik} \otimes a_{kj}$ (see (25), p. 84), and the subspace L of A spanned by the e_i and a_{ij} satisfies $\Delta(L) \subset L \otimes L$. The k-subalgebra A' generated by L satisfies $\Delta(A') \subset A' \otimes A'$. It follows that A is a directed union $A = \bigcup A'$ of finitely generated subalgebras A' such that $\Delta(A') \subset A' \otimes A'$.

Let $a \in A$. If $\Delta(a) = \sum b_i \otimes c_i$, then $\Delta(Sa) = \sum Sc_i \otimes Sb_i$ (Exercise 3-3(b)). Therefore, the k-subalgebra A' generated by L and SL satisfies $S(A') \subset A'$, and so it is a finitely generated Hopf subalgebra of A. It follows that A is the directed union of its finitely generated Hopf subalgebras. □

COROLLARY 8.35. *Let B be a Hopf algebra over k. If B is an integral domain, then it is finitely generated as a k-algebra if and only if its field of fractions is finitely generated as a field over k.*

PROOF. The necessity being obvious, we prove the sufficiency. According to the proposition, there is a finitely generated Hopf subalgebra A of B containing a generating set for the field of fractions of B. Then A and B have the same field of fractions, and so are equal (3.32). □

PROPOSITION 8.36. *Let G be an algebraic group over k.*

(a) *The k-algebra $\mathcal{O}(G)$ is finitely generated.*

(b) *The pair $\mathrm{Spm}(\mathcal{O}(G), \mathcal{O}(m))$ is an algebraic group G^{aff} over k.*

(c) *The natural map $\phi: G \to G^{\mathrm{aff}}$ is universal for homomorphisms from G to affine algebraic groups, and it is faithfully flat.*

(d) *The kernel N of ϕ is anti-affine.*

PROOF. (a) According to Proposition 8.34, $\mathcal{O}(G)$ is a filtered union $\mathcal{O}(G) = \bigcup_i \mathcal{O}_i$ of Hopf algebras with each $\mathcal{O}_i$ finitely generated as a k-algebra. Correspondingly, we obtain a family of homomorphisms $f_i: G \to G_i$ of algebraic groups over k with $G_i = \mathrm{Spm}(\mathcal{O}_i)$. Let $N = \bigcap_i \mathrm{Ker}(f_i)$. Then $N = \mathrm{Ker}(f_{i_0})$ for some i_0 (see 1.42), and $G/N \to G_{i_0}$ is a closed immersion (5.34). Therefore G/N is affine. We have morphisms $G \xrightarrow{a} G/N \xrightarrow{b} G_{i_0}$ and corresponding homomorphisms $\mathcal{O}_{i_0} \xrightarrow{b'} \mathcal{O}(G/N) \xrightarrow{a'} \mathcal{O}(G)$. As b' is surjective and $a' \circ b'$ is injective, we have $\mathcal{O}_{i_0} \simeq \mathcal{O}(G/N)$. Similarly, $\mathcal{O}_{i_1} \simeq \mathcal{O}(G/N)$ if $\mathcal{O}_{i_1} \supset \mathcal{O}_{i_0}$, and so $\mathcal{O}_{i_0} = \mathcal{O}_{i_1}$ as a subalgebra of $\mathcal{O}(G)$. Therefore $\mathcal{O}(G) = \bigcup_i \mathcal{O}_i = \mathcal{O}(G_{i_0})$, which is finitely generated.

(b, c) After the above discussion, it remains to show that ϕ is faithfully flat, but this follows from the criterion (c) of (5.43).

(d) This follows from the definition of N. □

Thus every algebraic group is an extension of an affine algebraic group by an anti-affine algebraic group

$$e \to G_{\mathrm{ant}} \to G \to G^{\mathrm{aff}} \to e,$$

in a unique way; in fact, it is a *central* extension (8.13).

PROPOSITION 8.37. *Every anti-affine algebraic group is smooth and connected.*

PROOF. Let G be an anti-affine algebraic group over a field k. Then G_{k^a} is anti-affine, and so we may suppose that k is algebraically closed. Then G_{red}° is an algebraic subgroup of G (see 1.39). As $G \to G/G_{\mathrm{red}}^\circ$ is faithfully flat, the map $\mathcal{O}(G/G_{\mathrm{red}}^\circ) \to \mathcal{O}(G)$ is injective. Therefore $\mathcal{O}(G/G_{\mathrm{red}}^\circ) = k$. As G/G_{red}° is finite, in particular affine, it is trivial, and so $G = G_{\mathrm{red}}^\circ$. □

COROLLARY 8.38. *An algebraic group G is affine if $Z(G^\circ)$ is affine.*

PROOF. Let $N = \mathrm{Ker}(G \to G^{\mathrm{aff}})$. Because N is anti-affine, it is contained in G°, and hence in $Z(G^\circ)$ (see 8.13). In particular, it is affine. The square

$$
\begin{array}{ccc}
G \times N & \longrightarrow & G \\
{\scriptstyle\text{affine}}\Big\downarrow & & \Big\downarrow \\
G & \xrightarrow{\ \text{faithfully flat}\ } & G/N
\end{array}
$$

is cartesian (5.24), and so the morphism $G \to G/N$ is affine (A.80). As $G/N \simeq G^{\mathrm{aff}}$ is affine, this implies that G is affine (8.38). □

COROLLARY 8.39. *Every algebraic group over a field of characteristic zero is smooth.*

PROOF. As extensions of smooth algebraic groups are smooth (8.1), this follows from Propositions 8.36 and 8.37. □

In the remainder of this section, we describe the classification of anti-affine algebraic groups in terms of abelian varieties.

Consider an extension

$$e \to T \to G \to A \to e \tag{43}$$

of an abelian variety A by a torus T. The group of characters $X^*(T)$ of T is defined to be $\mathrm{Hom}(T_{k^s}, \mathbb{G}_m)$. By definition, the torus T becomes isomorphic to $\mathbb{G}_m^r$ ($r = \dim T$) over k^s, and so $X^*(T) \approx \mathrm{End}(\mathbb{G}_m)^r \simeq \mathbb{Z}^r$. From a character χ of T, we obtain, by extension of scalars and pushout from (43), an extension

$$e \to \mathbb{G}_m \to G_\chi \to A_{k^s} \to e$$

over k^s, and hence an element $c(\lambda) \in \mathrm{Ext}^1(A_{k^s}, \mathbb{G}_m)$. Let $A^\vee$ be the dual abelian variety to A. Then

$$\mathrm{Ext}^1(A_{k^s}, \mathbb{G}_m) \simeq A^\vee(k^{\mathrm{sep}})$$

(e.g., Milne 1986, 11.3), and so the extension (43) gives rise to a homomorphism $c: X^*(T) \to A^\vee(k^s)$.

PROPOSITION 8.40. *The algebraic group G is anti-affine if and only if the homomorphism c is injective.*

PROOF. See Brion 2009, 2.1. □

In nonzero characteristic p, all anti-affine algebraic groups are of this form, but in characteristic zero, extensions of an abelian variety by a vector group may also be anti-affine.

Let A be an abelian variety over a field k of characteristic zero. In this case, there is a "universal vector extension" $E(A)$ of A such that every extension G of A by a vector group U fits into a unique diagram

$$
\begin{array}{ccccccccc}
e & \longrightarrow & H^1(A,\mathcal{O}_A)^\vee_\mathfrak{a} & \longrightarrow & E(A) & \longrightarrow & A & \longrightarrow & e \\
& & \downarrow{\scriptstyle\gamma} & & \downarrow & & \| & & \\
e & \longrightarrow & U & \longrightarrow & G & \longrightarrow & A & \longrightarrow & e
\end{array}
$$

with γ a k-linear map. The algebraic group $E(A)$ is anti-affine, and G is anti-affine if and only if γ is surjective. Therefore, the anti-affine extensions of A by vector groups are classified by the quotient spaces of $H^1(A,\mathcal{O}_A)^\vee$, or, equivalently, by the subspaces of $H^1(A,\mathcal{O}_A)$.

More generally, we need to consider extensions

$$e \to U \times T \to G \to A \to e$$

of A by the product of a vector group U with a torus T. Such a G is anti-affine if and only if both G/U and G/T are anti-affine, and every anti-affine group over A arises in this way. Thus we arrive at the following statement.

THEOREM 8.41. *Let A be an abelian variety over a field k.*

(a) *If k has nonzero characteristic, then the isomorphism classes of anti-affine groups over A are in one-to-one correspondence with the free abelian subgroups Λ of $A^\vee(k^s)$ of finite rank stable under the action of $\mathrm{Gal}(k^s/k)$.*

(b) *If k has characteristic zero, then the isomorphism classes of anti-affine groups over A are in one-to-one correspondence with the pairs (Λ, V) where Λ is as in (a) and V is a subspace of the k-vector space $H^1(A,\mathcal{O}_A)$.*

PROOF. See Brion 2009, 2.7; also Sancho de Salas 2001; Sancho de Salas and Sancho de Salas 2009. □

j. Extensions of abelian varieties by affine algebraic groups: a survey

After the Barsotti–Chevalley theorem, the study of smooth algebraic groups over perfect fields comes down to the study of (a) abelian varieties, (b) affine algebraic groups, and (c) the extensions of one by the other. Topic (a) is beyond the scope of this book while topic (b) occupies the rest of it. Here we discuss (c). For simplicity, we take k to be algebraically closed.

Let A and H be algebraic groups over k. An extension of A by H is an exact sequence

$$e \longrightarrow H \xrightarrow{\ i\ } G \xrightarrow{\ p\ } A \longrightarrow e \tag{44}$$

of algebraic groups. Two extensions (G, i, p) and (G', i', p') of A by H are equivalent if there exists an isomorphism $f : G \to G'$ such that the following diagram commutes:

$$
\begin{array}{ccccccccc}
e & \longrightarrow & H & \xrightarrow{\ i\ } & G & \xrightarrow{\ p\ } & A & \longrightarrow & e \\
  &   & \| &   & \downarrow f & & \| & & \\
e & \longrightarrow & H & \xrightarrow{\ i'\ } & G' & \xrightarrow{\ p'\ } & A & \longrightarrow & e.
\end{array}
$$

We let $\mathrm{Ext}(A, H)$ denote the set of equivalence classes of extensions of A by H.

For an exact sequence (44), the sequence

$$
e \longrightarrow Z(H) \xrightarrow{\ Z(i)\ } Z(G) \xrightarrow{\ f\ } A \longrightarrow e \tag{45}
$$

is exact, and the map $(44) \mapsto (45)$ defines a bijection

$$
\mathrm{Ext}(A, H) \to \mathrm{Ext}(A, Z(H))
$$

where $\mathrm{Ext}(A, Z(H))$ denotes the set of equivalence classes of extensions of A by $Z(H)$ in the (abelian) category of commutative algebraic groups. Hence $\mathrm{Ext}(A, H)$ has the structure of a commutative group, and every extension of A by H splits if $Z(H) = e$. See Wu 1986.

It remains to compute $\mathrm{Ext}(A, Z)$, where Z is a commutative affine algebraic group. Every connected commutative group variety G over k is a product of copies of $\mathbb{G}_m$ with a unipotent group variety U; when k has characteristic zero, U is vector group $V_{\mathfrak{a}}$ (product of copies of $\mathbb{G}_a$) (see 16.15 below). There are the following results:

(a) $\mathrm{Ext}(A, \mathbb{G}_m) \simeq H^1(A, \mathcal{O}_A^\times)$, which is canonically isomorphic to the group of divisor classes on A algebraically equivalent to zero (equal to the group of k-points of the dual abelian variety of A) (Weil, Barsotti; Serre 1959, VII.16).

(b) It remains to compute $\mathrm{Ext}(A, U)$, where U is unipotent. In characteristic 0, we have

$$
\mathrm{Ext}^1(A, V_{\mathfrak{a}}) \simeq H^1(A, \mathcal{O}_A \otimes V) \simeq V^{\dim(A)}
$$

(Barsotti; Serre 1959, VII.18). In characteristic p, the computation is more complicated, and involves $\mathrm{Ext}(N, Z^\circ)$, where N is the factor of A_{p^m} which, together with its Cartier dual, is local, and p^m is large enough to kill Z. However, when A is ordinary, it is still true that $\mathrm{Ext}(A, U) \simeq U(k)^{\dim A}$. See Wu 1986.

k. Homogeneous spaces are quasi-projective

All schemes are algebraic over the field k. Recall the following definitions.

DEFINITION 8.42. Let X be a separated algebraic scheme equipped with an action of G. We say that X is a **homogeneous space under G** (resp. a **torsor under G**) if the map

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

is faithfully flat (resp. an isomorphism).

THEOREM 8.43. *Let G be an algebraic group over k and X a homogeneous space under G. Then X is quasi-projective.*

Raynaud (1970, VI, 2.6) derives Theorem 8.43 from more general results on schemes. In the rest of this section, we sketch a more elementary proof.

It suffices to prove Theorem 8.43 after an extension of the base field k. This allows us to assume that there exists an $o \in X$, and hence that $X \simeq G/H$ with H the isotropy group at o. In this case, we prove a stronger result.

THEOREM 8.44. *Let G be an algebraic group and H an algebraic subgroup of G. There exists a projective scheme X equipped with an action of G and an equivariant open immersion $G/H \to X$ with schematically dense image.*

The starting point for the proof is the following theorem.

THEOREM 8.45. *Every abelian variety is projective.*

This was first proved in Barsotti 1953 and Matsusaka 1953. Weil (1957) gave a simpler proof, which can be found in Milne 1986.

We now sketch the proof of Theorem 8.44. Let G and H be as in the statement of the theorem. According to Theorem 8.28, there exists a connected affine normal algebraic subgroup N of G such that G/N is complete. Lemma 5.24 provides us with an isomorphism

$$(g,g') \mapsto (g,gg') \colon G \times HN \xrightarrow{\simeq} G \times_{G/HN} G, \tag{46}$$

from which we deduce an isomorphism

$$G \times (N/H \cap N) \overset{5.62}{\simeq} G \times HN/H \to G \times_{G/HN} G/H.$$

Now the top square in the following diagram is cartesian, and the rest of the diagram obviously commutes:

Choose a representation (V, r) of N containing a line L with stabilizer $H \cap N$. Then N acts on $\mathbb{P}(V)$ and the isotropy group at $[L]$ is $H \cap N$. Therefore the canonical map $N/H \cap N \hookrightarrow \mathbb{P}(V)$ is an immersion (7.20). Let Y denote the closure of $N/H \cap N$ in $\mathbb{P}(V)$.

The top square in the above diagram defines a descent datum on $G \times (N/H \cap N)$ relative to the faithfully flat map $G \to G/HN$ (see A.81). The isomorphism (46) allows us to interpret the descent datum on $G \times (N/H \cap N)$ in terms of group actions (see the above diagram). This and the fact that the embedding $N/H \cap N \to Y$ is equivariant allows us to extend the descent datum on $G \times (N/H \cap N)$ to $G \times Y$, and even to $G \times \mathbb{P}(V)$. Now descent theory tells us that $G \times Y$ arises from a scheme X over G/NH, i.e., that there is a cartesian square

$$
\begin{array}{ccc}
G \times Y & \longrightarrow & X \\
\downarrow & & \downarrow \\
G & \longrightarrow & G/HN
\end{array}
$$

containing the cartesian square in the previous diagram as a subdiagram. As $G \times Y$ is projective over G, descent theory tells us that X is projective over G/HN, but G/HN, being a quotient of G/N, is complete, and hence projective (8.45). Therefore X is a projective scheme over k. The natural inclusion of G/H into X is the required equivariant projective embedding.

See Brion 2015b, 5.2 for a more detailed proof.

Exercises

EXERCISE 8-1. Let G be an algebraic group. Show that $G/Z(G)$ is affine if G is connected or $\mathcal{D}G$ is affine.

EXERCISE 8-2. Show that the definitions of homogeneous space in 7.7 and 8.42 are equivalent. [Use A.67.]

We now concentrate on *affine* algebraic groups. By "algebraic group" we shall mean "affine algebraic group" and by "group variety" we shall mean "affine group variety".

Tannaka Duality; Jordan Decompositions

A character of a topological group is a continuous homomorphism from the group to the circle group $\{z \in \mathbb{C} \mid z\bar{z} = 1\}$. A locally compact commutative topological group G can be recovered from its character group $G^\vee$ because the canonical homomorphism $G \to G^{\vee\vee}$ is an isomorphism of topological groups (Pontryagin duality). As the dual of a compact commutative group is a discrete commutative group, the study of the former is equivalent to that of the latter.

Clearly, "commutative" is required in the above statements, because every character is trivial on the derived group. However, Tannaka showed that it is possible to recover a compact noncommutative group from the category of its unitary representations. In this chapter, we prove an analogue of this for algebraic groups. The Tannakian perspective is that an algebraic group G and its category $\mathsf{Rep}(G)$ of finite-dimensional representations should be considered equal partners. Recall that all algebraic groups are affine over a base field k.

a. Recovering a group from its representations

Let R_0 be a ring and let A be an R_0-algebra (not necessarily finitely generated) equipped with R_0-homomorphisms $\Delta: A \to A \otimes A$ and $\epsilon: A \to R_0$ for which the diagrams (17), p. 65, commute. Then the functor

$$G: R \rightsquigarrow \mathrm{Hom}_{R_0\text{-algebra}}(A, R)$$

is an affine monoid over R_0. There is a ***regular representation*** r_A of G on A in which an element g of $G(R)$ acts on $f \in A$ according to the rule

$$(r_A(g) f_R)(x) = f_R(x \cdot g) \text{ all } x \in G(R). \tag{47}$$

LEMMA 9.1. *With the above notation, let u be an R_0-algebra endomorphism of A. If the diagram*

$$
\begin{array}{ccc}
A & \xrightarrow{\Delta} & A \otimes A \\
\downarrow{\scriptstyle u} & & \downarrow{\scriptstyle 1 \otimes u} \\
A & \xrightarrow{\Delta} & A \otimes A
\end{array}
\tag{48}
$$

commutes, then there exists a $g \in G(R_0)$ such that $u = r_A(g)$.

PROOF. Let $\phi: G \to G$ be the morphism corresponding to u, so that

$$(uf)_R(x) = f_R(\phi_R x) \text{ all } f \in A, \, x \in G(R). \tag{49}$$

We shall prove that the lemma holds with $g = \phi(e)$.

From (48), we obtain a commutative diagram

$$
\begin{array}{ccc}
G & \xleftarrow{m} & G \times G \\
\downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle 1 \times \phi} \\
G & \xleftarrow{m} & G \times G.
\end{array}
$$

Thus

$$\phi_R(x \cdot y) = x \cdot \phi_R(y), \quad \text{all } x, y \in G(R).$$

On setting $y = e$ in the last equation, we find that $\phi_R(x) = x \cdot g_R$ with $g_R = \phi_R(e)$. Therefore, for $f \in A$ and $x \in G(R)$,

$$(uf)_R(x) \overset{(49)}{=} f_R(x \cdot g_R) \overset{(47)}{=} (r_A(g)f)_R(x),$$

and so $u = r_A(g)$.   □

Let G be an algebraic group over a field k. Let R be a k-algebra, and let $g \in G(R)$. For every finite-dimensional representation (V, r_V) of G over k, we have an R-linear map $\lambda_V \overset{\text{def}}{=} r_V(g) \colon V_R \to V_R$. These maps satisfy the following conditions:

(a) for all representations V and W, $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$;

(b) $\lambda_{\mathbb{1}}$ is the identity map (here $\mathbb{1} = k$ with the trivial action);

(c) for all G-equivariant maps $u \colon V \to W$, $\lambda_W \circ u_R = u_R \circ \lambda_V$.

THEOREM 9.2. *Let G be an algebraic group over k and R a k-algebra. Suppose that, for every finite-dimensional representation (V, r_V) of G, we are given an R-linear map $\lambda_V \colon V_R \to V_R$. If the family (λ_V) satisfies the conditions (a, b, c), then there exists a unique $g \in G(R)$ such that $\lambda_V = r_V(g)$ for all V.*

PROOF. Let V be a (possibly infinite-dimensional) representation of G. Recall (4.8) that V is a union of its finite-dimensional subrepresentations, $V = \bigcup_{i \in I} V_i$. It follows from (c) that

$$\lambda_{V_i} | V_i \cap V_j = \lambda_{V_i \cap V_j} = \lambda_{V_j} | V_i \cap V_j$$

for all $i, j \in I$. Therefore, there is a unique R-linear endomorphism λ_V of V_R such that $\lambda_V | W = \lambda_W$ for every finite-dimensional subrepresentation $W \subset V$. The conditions (a, b, c) will continue to hold for the enlarged family.

In particular, we have an R-linear map $\lambda_A : A \to A$, $A = \mathcal{O}(G)_R$, corresponding to the regular representation r_A of G on A. The map $m : A \otimes A \to A$ is equivariant[1] for the representations $r_A \otimes r_A$ and r_A, which means that λ_A is a k-algebra homomorphism. Similarly, the map $\Delta : A \to A \otimes A$ is equivariant for the representations r_A on A and $1 \otimes r_A$ on $A \otimes A$, and so the diagram in (9.1) commutes with u replaced by λ_A. Now Lemma 9.1, applied to the affine monoid G_R over R, shows that there exists a $g \in G(R)$ such $\lambda_A = r(g)$.

Let (V, r_V) be a finitely generated representation of G, and let V_0 denote the underlying k-vector space. There is an injective homomorphism of representations $\rho : V \to V_0 \otimes \mathcal{O}(G)$ (see 4.12). By definition λ and $r(g)$ agree on $\mathcal{O}(G)$, and they agree on V_0 by condition (b). Therefore they agree on $V_0 \otimes \mathcal{O}(G)$ by (a), and so they agree on V by (c).

This proves the existence of g. It is uniquely determined by λ_V for any faithful representation (V, r_V). □

Notes

Let G be an algebraic group over k and let $\mathsf{Rep}(G)$ (or $\mathsf{Rep}_k(G)$) denote the category of representations of G on finite-dimensional k-vector spaces.

9.3. Let (λ_V) be a family satisfying the conditions (a, b, c). As G is an algebraic group, each λ_V is an isomorphism and $\lambda_{V^\vee} = (\lambda_V)^\vee$ because this true of the maps $r_V(g)$.

9.4. Theorem 9.2 identifies $g \in G(R)$ with the collection of families (λ_V) satisfying the conditions (a, b, c). Thus, from the category $\mathsf{Rep}(G)$, its tensor structure, and the forgetful functor, we can recover the functor $R \rightsquigarrow G(R)$, and hence the group G itself. For this reason, Theorem 9.2 is often called the *reconstruction theorem*.

9.5. Suppose that k is an algebraically closed field, and that G is smooth, so that $\mathcal{O}(G)$ can be identified with a ring of k-valued functions on $G(k)$. For each representation (V, r_V) of G over k and $u \in V^\vee$, we have a function ϕ_u on $G(k)$,

$$\phi_u(g) = \langle u, r_V(g) \rangle \in k.$$

Then $\phi_u \in \mathcal{O}(G)$, and every element of $\mathcal{O}(G)$ arises in this way. In this way, we can recover $\mathcal{O}(G)$ directly as the ring of "representative functions" on G (cf. Springer 1998, 2.5.5).

---

[1]Here are the details. For $x \in G(R)$,

$$(r(g) \circ m)(f \otimes f')(x) = (r(g)(ff'))(x) = (ff')(xg) = f(xg) \cdot f'(xg)$$
$$(m \circ r(g) \otimes r(g))(f \otimes f')(x) = ((r(g)f) \cdot (r(g)f'))(x) = f(xg) \cdot f'(xg).$$

9.6. In Theorem 9.2, instead of all representations of G, it suffices to choose a faithful representation V and take all quotients of subrepresentations of a direct sum of representations of the form $\otimes^n (V \oplus V^\vee)$ (see 4.14). Then Theorem 9.2 can be interpreted as saying that G is the subgroup G' of GL_V fixing all tensors in subquotients of representations $\otimes^n (V \oplus V^\vee)$ fixed by G.

9.7. In general, we can't omit "subquotients of" from (9.6). Consider for example, the subgroup $B = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ of GL_2 acting on $V = k \times k$ and suppose that a vector $v \in (V \oplus V^\vee)^{\otimes n}$ is fixed by B. Then $g \mapsto gv$ is a regular map $\mathrm{GL}_2 / B \to (V \oplus V^\vee)^{\otimes n}$ of algebraic varieties. As $\mathrm{GL}_2 / B \simeq \mathbb{P}^1$ and $(V \oplus V^\vee)^{\otimes n}$ is affine, the image of the map is a point (A.75g). Therefore, v is fixed by GL_2, and so $B' = \mathrm{GL}_2$.

9.8. Let ω denote the forgetful functor $\mathsf{Rep}_k(G) \to \mathsf{Vec}_k$, and, for a k-algebra R, let $\omega_R = R \otimes \omega$. Let $\mathrm{End}^\otimes(\omega_R)$ denote the set of natural transformations $\lambda : \omega_R \to \omega_R$ commuting with tensor products, i.e., such that (a) $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ for all representations V and W of G and (b) $\lambda_{\mathbb{1}}$ is the identity map. Theorem 9.2 says that the canonical map $G(R) \to \mathrm{End}^\otimes(\omega_R)$ is an isomorphism. Now let $\underline{\mathrm{End}}^\otimes(\omega)$ denote the functor $R \rightsquigarrow \mathrm{End}^\otimes(\omega_R)$. Then $G \simeq \underline{\mathrm{End}}^\otimes(\omega)$. Because of (9.3), this can be written $G \simeq \underline{\mathrm{Aut}}^\otimes(\omega)$.

NOTES. The short direct proof of Theorem 9.2 follows Springer 1998, 2.5.3.

b.　Jordan decompositions

The Jordan decomposition of a linear map

Recall that an endomorphism α of a vector space V over k is **diagonalizable** if V has a basis of eigenvectors for α, and that it is **semisimple** if it becomes diagonalizable after an extension of k. For example, the linear map $x \mapsto Ax : k^n \to k^n$ defined by an $n \times n$ matrix A is diagonalizable if and only if there exists an invertible matrix P with entries in k such that PAP^{-1} is diagonal, and it is semisimple if and only if there exists such a matrix P with entries in some field containing k.

From linear algebra, we know that α is semisimple if and only if no irreducible factor of its minimum polynomial $m_\alpha(T)$ has a multiple root; in other words, if and only if the subring $k[\alpha]$ of $\mathrm{End}_k(V)$ generated by α is étale.

Recall that an endomorphism α of a vector space V is **nilpotent** if $\alpha^m = 0$ for some $m > 0$, and that it is **unipotent** if $\mathrm{id}_V - \alpha$ is nilpotent. If α is nilpotent, then its minimum polynomial divides T^m for some m, and so the eigenvalues[2] of α are all zero. From linear algebra, we know that the converse is also true, and so α is unipotent if and only if its eigenvalues all equal 1.

---

[2] We define the **eigenvalues** of an endomorphism of a vector space to be the *family* (not the set) of roots of its characteristic polynomial in some algebraically closed field.

Let α be an endomorphism of a finite-dimensional vector space V over k. We say that the eigenvalues of α lie in k if the characteristic polynomial $P_\alpha(T)$ of α splits in $k[X]$:

$$P_\alpha(T) = (T - a_1)^{n_1} \cdots (T - a_r)^{n_r}, \quad a_i \in k.$$

For each eigenvalue a of α in k, the ***primary space***[3] is defined to be

$$V^a = \{v \in V \mid (\alpha - a)^N v = 0 \text{ for some } N > 0\}.$$

PROPOSITION 9.9. *If the eigenvalues of α lie in k, then V is a direct sum of its primary spaces:*

$$V = \bigoplus_i V^{a_i}.$$

PROOF. Let $P(T)$ be a polynomial in $k[T]$ such that $P(\alpha) = 0$, and suppose that $P(T) = Q(T)R(T)$ with Q and R relatively prime. Then there exist polynomials $a(T)$ and $b(T)$ such that

$$a(T)Q(T) + b(T)R(T) = 1.$$

For any $v \in V$,
$$a(\alpha)Q(\alpha)v + b(\alpha)R(\alpha)v = v, \tag{50}$$

and so $\mathrm{Ker}(Q(\alpha)) \cap \mathrm{Ker}(R(\alpha)) = 0$. As

$$Q(\alpha)R(\alpha) = 0 = R(\alpha)Q(\alpha),$$

(50) expresses v as the sum of an element of $\mathrm{Ker}(R(\alpha))$ and an element of $\mathrm{Ker}(Q(\alpha))$. Thus, V is the direct sum of $\mathrm{Ker}(Q(\alpha))$ and $\mathrm{Ker}(P(\alpha))$.

On applying this remark repeatedly to the characteristic polynomial

$$(T - a_1)^{n_1} \cdots (T - a_r)^{n_r}$$

of α and its factors, we find that

$$V = \bigoplus_i \mathrm{Ker}(\alpha - a_i)^{n_i},$$

as claimed. □

COROLLARY 9.10. *The eigenvalues of α lie in k if and only if, for some choice of basis for V, the matrix of α is upper triagonal.*

PROOF. The sufficiency is obvious, and the necessity follows from proposition.□

An endomorphism satisfying the equivalent conditions of the corollary is said to be ***trigonalizable***.[4]

---

[3]This is Bourbaki's terminology; "generalized eigenspace" is also used.

[4]The terms "triangulable" and "triagonalizable" are also used; in French "trigonalisable" is standard.

THEOREM 9.11. *Let V be a finite-dimensional vector space over a perfect field, and let α be an automorphism of V. There exist unique automorphisms α_s and α_u of V such that*

(a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$, *and*

(b) α_s *is semisimple and α_u is unipotent.*

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

PROOF. Assume first that the eigenvalues of α lie in k, so that V is a direct sum of the primary spaces of α, say, $V = \bigoplus_{1 \le i \le m} V^{a_i}$, where the a_i are the distinct roots of P_α. Define α_s to be the automorphism of V that acts as a_i on V^{a_i} for each i. Then α_s is a semisimple automorphism of V, and $\alpha_u \overset{\text{def}}{=} \alpha \circ \alpha_s^{-1}$ commutes with α_s (because it does on each V^{a_i}) and is unipotent (because its eigenvalues are 1). Thus α_s and α_u satisfy (a) and (b).

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

$$Q(T) \equiv a_i \bmod (T - a_i)^{n_i}, \quad i = 1, \dots, m.$$

Then $Q(\alpha)$ acts as a_i on V^{a_i} for each i, and so $\alpha_s = Q(\alpha)$, which is a polynomial in α. Similarly, $\alpha_s^{-1} \in k[\alpha]$, and so $\alpha_u \overset{\text{def}}{=} \alpha \circ \alpha_s^{-1} \in k[\alpha]$.

It remains to prove the uniqueness of α_s and α_u. Let $\alpha = \beta_s \circ \beta_u$ be a second decomposition satisfying (a) and (b). Then β_s and β_u commute with α, and therefore also with α_s and α_u (because they are polynomials in α). It follows that $\beta_s^{-1} \alpha_s$ is semisimple and that $\alpha_u \beta_u^{-1}$ is unipotent. Since they are equal, both must equal 1. This completes the proof when the a_i lie in k.

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 of $k' \otimes_k V$. Let A be the matrix of α. The first part of the proof allows us to write $A = A_s A_u = A_u A_s$ with A_s (resp. A_u) a semisimple (resp. unipotent) matrix with entries in k'; moreover, this decomposition is unique.

Let $\sigma \in \mathrm{Gal}(k'/k)$, and for a matrix $B = (b_{ij})$, define σB to be (σb_{ij}). Because A has entries in k, $\sigma A = A$. Now $A = (\sigma A_s)(\sigma A_u)$ is again a decomposition of A into commuting semisimple and unipotent matrices. By the uniqueness of the decomposition, $\sigma A_s = A_s$ and $\sigma A_u = A_u$. Since this is true for all $\sigma \in \mathrm{Gal}(k'/k)$, the matrices A_s and A_u have entries in k. Let α_s and α_u be the endomorphisms of V with matrices A_s and A_u. Then $\alpha = \alpha_s \circ \alpha_u$ is a decomposition of α satisfying (a) and (b).

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

$$A_s = c_0 + c_1 A + \dots + c_{n-1} A^{n-1} \qquad (n = \dim V).$$

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

$$\alpha_s = c_0 + c_1 \alpha + \dots + c_{n-1} \alpha^{n-1} \in k[\alpha].$$

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

The automorphisms α_s and α_u are called the ***semisimple*** and ***unipotent parts*** of α, and $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$ is the ***(multiplicative) Jordan decomposition*** of α.

EXAMPLE 9.12. The matrix at left has the following Jordan decomposition,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

PROPOSITION 9.13. *Let α and β be automorphisms of vector spaces V and W over a perfect field k, and let $\varphi : V \to W$ be a k-linear map. If $\varphi \circ \alpha = \beta \circ \varphi$, then $\varphi \circ \alpha_s = \beta_s \circ \varphi$ and $\varphi \circ \alpha_u = \beta_u \circ \varphi$.*

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that the eigenvalues of α and β lie in k. Recall that α_s acts on each primary space V^a, $a \in k$, as multiplication by a. As φ obviously maps V^a into W^a, it follows that $\varphi \circ \alpha_s = \beta_s \circ \varphi$. Similarly, $\varphi \circ \alpha_s^{-1} = \beta_s^{-1} \circ \varphi$, and so $\varphi \circ \alpha_u = \beta_u \circ \varphi$. □

PROPOSITION 9.14. *Let V be a vector space over a perfect field. If a subspace W of V is stable under α, then it is stable under α_s and α_u and the Jordan decomposition of $\alpha|W$ is $\alpha_s|W \circ \alpha_u|W$.*

PROOF. The subspace W is stable under α_s and α_u because each is a polynomial in α. Clearly the decomposition $\alpha|W = \alpha_s|W \circ \alpha_u|W$ satisfies (a) and (b) of Theorem 9.11 and so is the Jordan decomposition $\alpha|W$. □

PROPOSITION 9.15. *For any automorphisms α and β of vector spaces V and W over a perfect field,*

$$(\alpha \otimes \beta)_s = \alpha_s \otimes \beta_s$$
$$(\alpha \otimes \beta)_u = \alpha_u \otimes \beta_u.$$

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that the eigenvalues of α and β lie in k. For any $a, b \in k$, $V^a \otimes W^b \subset (V \otimes W)^{ab}$, and so $\alpha_s \otimes \beta_s$ and $(\alpha \otimes \beta)_s$ both act on $V^a \otimes W^b$ as multiplication by ab. This shows that $(\alpha \otimes \beta)_s = \alpha_s \otimes \beta_s$. Similarly, $(\alpha_s^{-1} \otimes \beta_s^{-1}) = (\alpha \otimes \beta)_s^{-1}$, and so $(\alpha \otimes \beta)_u = \alpha_u \otimes \beta_u$. □

EXAMPLE 9.16. Let k be a nonperfect field of characteristic 2, so that there exists an $a \in k \smallsetminus k^2$, and let $M = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$. In the algebraic closure of k, M has the Jordan decomposition

$$M = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{pmatrix}\begin{pmatrix} 0 & 1/\sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix}$$

(the matrix at right is unipotent only because $-1 = 1$). These matrices do not have coefficients in k, and so, if M had a Jordan decomposition in $M_2(k)$, then it would have two distinct Jordan decompositions in $M_2(k^{\mathrm{a}})$, contradicting the theorem. Thus M has no Jordan decomposition over k.

Infinite-dimensional vector spaces

Let V be a vector space, possibly infinite-dimensional, over a perfect field k. An endomorphism α of V is *locally finite* if V is a union of finite-dimensional subspaces stable under α. A locally finite endomorphism is *semisimple* (resp. *locally nilpotent*, *locally unipotent*) if its restriction to every stable finite-dimensional subspace is semisimple (resp. nilpotent, unipotent).

Let α be a locally finite automorphism of V. By assumption, every $v \in V$ is contained in a finite-dimensional subspace W stable under α, and we define $\alpha_s(v) = (\alpha|W)_s(v)$. According to Theorem 9.11, this is independent of the choice of W, and so in this way we get a semisimple automorphism of V. Similarly, we can define α_u. Thus:

THEOREM 9.17. *Let α be a locally finite automorphism of a vector space V. There exist unique automorphisms α_s and α_u such that*

(a) $\alpha = \alpha_s \circ \alpha_u = \alpha_u \circ \alpha_s$, *and*

(b) α_s *is semisimple and α_u is locally unipotent.*

For any finite-dimensional subspace W of V stable under α,

$$\alpha|W = (\alpha_s|W) \circ (\alpha_u|W) = (\alpha_u|W) \circ (\alpha_s|W)$$

is the Jordan decomposition of $\alpha|W$.

Jordan decompositions in algebraic groups

After these preliminaries, we can prove the following important theorem.

THEOREM 9.18. *Let G be an algebraic group over a perfect field k, and let $g \in G(k)$. Then there exist unique elements $g_s, g_u \in G(k)$ such that, for every representation (V, r_V) of G, $r_V(g_s) = r_V(g)_s$ and $r_V(g_u) = r_V(g)_u$. Furthermore,*

$$g = g_s g_u = g_u g_s. \tag{51}$$

PROOF. In view of Propositions 9.13 and 9.15, the first assertion follows immediately from Theorem 9.2 applied to the families $(r_V(g)_s)_V$ and $(r_V(g)_u)_V$. Now choose a faithful representation r_V. Then the equality (51) follows from

$$r_V(g) = \begin{cases} r_V(g)_s r_V(g)_u = r_V(g_s) r_V(g_u) = r_V(g_s g_u) \\ r_V(g)_u r_V(g)_s = r_V(g_u) r_V(g_s) = r_V(g_u g_s). \end{cases}$$

$\square$

The elements g_s and g_u are called the **semisimple** and **unipotent parts** of g, and $g = g_s g_u$ is the **Jordan decomposition** (or **Jordan–Chevalley decomposition**) of g.

9.19. Let G be an algebraic group over a perfect field k. An element g of $G(k)$ is said to be **semisimple** (resp. **unipotent**) if $g = g_s$ (resp. $g = g_u$). Thus, g is semisimple (resp. unipotent) if $r(g)$ is semisimple (resp. unipotent) for one faithful representation (V, r) of G, in which case $r(g)$ is semisimple (resp. unipotent) for all representations r of G.

9.20. To check that a decomposition $g = g_s g_u$ is the Jordan decomposition, it suffices to check that $r(g) = r(g_s)r(g_u)$ is the Jordan decomposition of $r(g)$ for a single faithful representation of G.

9.21. Homomorphisms of algebraic groups preserve Jordan decompositions. To see this, let $u: G \to G'$ be a homomorphism and let $g = g_s g_u$ be a Jordan decomposition in $G(k)$. If $r: G' \to \mathrm{GL}_V$ is a representation of G', then $r \circ u$ is a representation of G, and so

$$(r \circ u)(g) = ((r \circ u)(g_s)) \cdot ((r \circ u)(g_u))$$

is the Jordan decomposition in $\mathrm{GL}(V)$. When we choose r to be faithful, this implies that $u(g) = u(g_s) \cdot u(g_u)$ is the Jordan decomposition of $u(g)$.

9.22. Let G be a group variety over an algebraically closed field. In general, the set $G(k)_s$ of semisimple elements in $G(k)$ is not closed for the Zariski topology. However, the set $G(k)_u$ of unipotent elements is closed. To see this, embed G in GL_n. A matrix A is unipotent if and only if its characteristic polynomial is $(T-1)^n$. But the coefficients of the characteristic polynomial of A are polynomials in the entries of A, and so this is a polynomial condition on A.

9.23. We defined Jordan decompositions for arbitrary algebraic groups G, not necessarily smooth. However, as the base field is perfect, G_{red} is a smooth algebraic subgroup of G and $G_{\mathrm{red}}(k) = G(k)$. Therefore everything comes down to smooth groups.

NOTES. For vector spaces, the Jordan decomposition can be read off from the Jordan normal form. It was defined for group varieties by Kolchin and Borel, and was made a fundamental tool by Chevalley. It is sometimes called the Jordan–Chevalley decomposition. Our proof of the existence of Jordan decompositions is the standard one, except that we made Theorem 9.2 explicit.

c. Characterizing categories of representations

Pontryagin duality identifies the topological groups that arise as the dual of a locally compact commutative group. Similarly, Tannakian theory identifies the tensor categories that arise as the category of representations of an algebraic group.

In this section, k-algebras are not required to be finitely generated, and we largely ignore set-theoretic questions. An additive category C is said to be k-*linear* if the Hom sets are k-vector spaces and composition is k-bilinear. Functors of k-linear categories are required to be k-linear, i.e., the maps $\mathrm{Hom}(a,b) \to \mathrm{Hom}(Fa, Fb)$ defined by F are required to be k-linear.

By an ***affine group*** over k we mean a functor G from Alg_k^0 to groups whose underlying functor to sets is represented by a k-algebra $\mathcal{O}(G)$:

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

When $\mathcal{O}(G)$ is finitely generated, G is an affine algebraic group. By a representation of an affine group over k we mean a representation on a finite-dimensional vector space over k.

Let $\omega: \mathsf{A} \to \mathsf{B}$ be a faithful functor of categories. We say that a morphism $\omega X \to \omega Y$ *lives in* A if it lies in $\mathrm{Hom}(X, Y) \subset \mathrm{Hom}(\omega X, \omega Y)$.

For k-vector spaces U, V, W, there are canonical isomorphisms

$$
\begin{aligned}
&\phi_{U,V,W}: U \otimes (V \otimes W) \to (U \otimes V) \otimes W, \quad u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w \\
&\psi_{U,V}: U \otimes V \to V \otimes U, \qquad\qquad\qquad\quad u \otimes v \mapsto v \otimes u.
\end{aligned}
\tag{52}
$$

We let Vec_k denote the category of finite-dimensional vector spaces over k.

THEOREM 9.24. *Let C be an essentially small k-linear abelian category and let $\otimes: \mathsf{C} \times \mathsf{C} \to \mathsf{C}$ be a k-bilinear functor. The pair $(\mathsf{C}, \otimes)$ is the category of representations of an affine group G over k if and only if there exists a k-linear exact faithful functor $\omega: \mathsf{C} \to \mathsf{Vec}_k$ such that*

(a) $\omega(X \otimes Y) = \omega(X) \otimes \omega(Y)$ *for all X, Y;*

(b) *the isomorphisms $\phi_{\omega X, \omega Y, \omega Z}$ and $\psi_{\omega X, \omega Y}$ live in C for all X, Y, Z;*

(c) *there exists an (identity) object $\mathbf{1}$ in C such that $\omega(\mathbf{1}) = k$ and the canonical isomorphisms*

$$\omega(\mathbf{1}) \otimes \omega(X) \simeq \omega(X) \simeq \omega(X) \otimes \omega(\mathbf{1})$$

live in C for all X;

(d) *for every object X such that $\omega(X)$ has dimension 1, there exists an object X^{-1} in C such that $X \otimes X^{-1} \approx \mathbf{1}$.*

PROOF. If $(\mathsf{C}, \otimes) = (\mathsf{Rep}(G), \otimes)$ for some affine group scheme G over k, then the forgetful functor has the required properties, which proves the necessity of the condition. The sufficiency is proved in Section e below, after some preliminaries in Section d. $\square$

Notes

9.25. The group scheme G depends on the choice of ω. Once ω has been chosen, G has the same description as in 9.2, namely, for a k-algebra R, the group $G(R)$ consists of families $(\lambda_X)_{X \in \mathrm{ob}(\mathsf{C})}$, $\lambda_X \in \mathrm{End}(X) \otimes R$, such that

  (a) for all X, Y in C, $\lambda_{X \otimes Y} = \lambda_X \otimes \lambda_Y$;

  (b) $\lambda_{\mathbb{1}}$ is the identity map;

  (c) for all morphisms $u \colon X \to Y$, $\lambda_Y \circ u_R = u_R \circ \lambda_X$.

With the terminology of 9.8, $G = \underline{\mathrm{Aut}}^{\otimes}(\omega)$. Therefore 9.2 shows that, when we start with $(\mathsf{C}, \otimes) = (\mathsf{Rep}(G), \otimes)$, we get back the group G.

9.26. Let C be a k-linear abelian category equipped with a k-bilinear functor $\otimes \colon \mathsf{C} \times \mathsf{C} \to \mathsf{C}$. The **dual** of an object X of C is an object $X^{\vee}$ equipped with an "evaluation map" $\mathrm{ev} \colon X^{\vee} \otimes X \to \mathbb{1}$ having the property that the map

$$\alpha \mapsto \mathrm{ev} \circ (\alpha \otimes \mathrm{id}_X) \colon \mathrm{Hom}(T, X^{\vee}) \to \mathrm{Hom}(T \otimes X, \mathbb{1})$$

is an isomorphism for all objects T of C. If there exists a functor ω as in Theorem 9.24, then duals always exist.

9.27. The affine group G attached to $(\mathsf{C}, \otimes, \omega)$ is algebraic if and only if there exists an object X such that every object of C is isomorphic to a subquotient of a direct sum of objects $\bigotimes^m (X \oplus X^{\vee})$. The necessity follows from Theorem 4.14.

9.28. Let $(\mathsf{C}, \otimes, \omega)$ and $(\mathsf{C}', \otimes', \omega')$ be two triples satisfying the conditions of Theorem 9.24. Every k-linear exact tensor functor $\mathsf{C} \to \mathsf{C}'$ compatible with the tensor structures and the functors ω arises from a unique homomorphism $G' \to G$ of the corresponding affine groups. Indeed, such a functor obviously defines a homomorphism of group-valued functors $\tilde{G}' \to \tilde{G}$ (see 9.25), to which we can apply the Yoneda lemma.

Examples

9.29. Let M be a commutative group. An M-**gradation** on a finite-dimensional vector space V over k is a family $(V_m)_{m \in M}$ of subspaces of V such that $V = \bigoplus_{m \in M} V_m$. If V is graded by a family of subspaces $(V_m)_m$ and W is graded by $(W_m)_m$, then $V \otimes W$ is graded by the family of subspaces

$$(V \otimes W)_m = \bigoplus_{m_1 + m_2 = m} V_{m_1} \otimes W_{m_2}.$$

For the category of finite-dimensional M-graded vector spaces, the forgetful functor satisfies the conditions of 9.24, and so the category is the category of representations of an affine group. When M is finitely generated, this is the algebraic group $D(M)$ defined in 12.3 below.

9.30. Let K be a topological group. The category $\mathsf{Rep}_{\mathbb{R}}(K)$ of continuous representations of K on finite-dimensional real vector spaces has a natural tensor product. The forgetful functor satisfies the conditions of Theorem 9.24, and so there is an algebraic group $\tilde{K}$ over $\mathbb{R}$, called the **real algebraic envelope** of K, and an equivalence

$$\mathsf{Rep}_{\mathbb{R}}(K) \to \mathsf{Rep}_{\mathbb{R}}(\tilde{K}).$$

This equivalence is induced by a homomorphism $K \to \tilde{K}(\mathbb{R})$, which is an isomorphism when K is compact (Serre 1993, 5.2).

9.31. Let G be a connected complex Lie group or a finitely generated abstract group and let C be the category of representations of G on finite-dimensional complex vector spaces. With the obvious functors $\otimes: \mathsf{C} \times \mathsf{C} \to \mathsf{C}$ and $\omega: \mathsf{C} \to \mathsf{Vec}_{\mathbb{C}}$, this category satisfies the hypotheses of Theorem 9.24, and so it is the category of representations of an affine group $A(G)$. Almost by definition, there exists a homomorphism $P: G \to A(G)(\mathbb{C})$ with the property that, for each representation (V, ρ) of G, there is a unique representation $(V, \hat{\rho})$ of $A(G)$ such that $\hat{\rho} = \rho \circ P$.

The group $A(G)$ was introduced and studied by Hochschild and Mostow in a series of papers published in the *American Journal of Mathematics* between 1957 and 1969 – it is called the **Hochschild–Mostow group**. For a brief exposition of this work, see Magid 2011.

d. Categories of comodules over a coalgebra

A **coalgebra**[5] over k is a k-vector space C equipped with a pair of k-linear maps

$$\Delta: C \to C \otimes C, \quad \epsilon: C \to k$$

such that the diagrams (17), p. 65, commute. The linear dual $C^{\vee}$ of C becomes an associative algebra over k with the multiplication

$$C^{\vee} \otimes C^{\vee} \overset{\text{can.}}{\hookrightarrow} (C \otimes C)^{\vee} \overset{\Delta^{\vee}}{\longrightarrow} C^{\vee},$$

and the structure map

$$k \simeq k^{\vee} \overset{\epsilon^{\vee}}{\longrightarrow} C^{\vee}.$$

We say that C is **cocommutative** (resp. **étale**) if $C^{\vee}$ is commutative (resp. étale).

Let (C, Δ, ϵ) be a coalgebra over k. A C-comodule is a k-linear map $\rho: V \to V \otimes C$ satisfying the conditions (24), p. 84. Let $(e_i)_{i \in I}$ be a basis for V, and let $\rho(e_j) = \sum e_i \otimes c_{ij}$. Then the conditions become

$$\left. \begin{array}{rcl} \Delta(c_{ij}) & = & \sum_{k \in I} c_{ik} \otimes c_{kj} \\ \epsilon(c_{ij}) & = & \delta_{ij} \end{array} \right\} \quad \text{all } i, j \in I.$$

---

[5]Strictly speaking, this is a *co-associative* coalgebra over k *with co-identity*.

These equations show that the k-subspace spanned by the c_{ij} is a subcoalgebra of C, which we denote C_V. Clearly, C_V is the smallest subspace of C such that $\rho(V) \subset V \otimes C_V$, and so it is independent of the choice of the basis. Alternatively, C_V is the image of the map $V^\vee \otimes V \to C$ defined by ρ followed by the evaluation map. When V is finite-dimensional over k, so also is C_V. If (V, ρ) is a subcomodule of the C-comodule (C, Δ), then $V \subset C_V$.

If C is k-coalgebra, then $\mathsf{Comod}(C)$ is a k-linear abelian category, and the forgetful functor $\omega \colon \mathsf{Comod}(C) \to \mathsf{Vec}_k$ is exact, faithful, and k-linear. The next theorem provides a converse statement.

THEOREM 9.32. *Let* C *be an essentially small k-linear abelian category, and let* $\omega \colon \mathsf{C} \to \mathsf{Vec}_k$ *be an exact faithful k-linear functor. Then there exists a coalgebra* C *such that* C *is equivalent to the category of C-comodules of finite dimension.*

The proof will occupy the rest of this section.

Because ω is faithful, $\omega(\mathrm{id}_X) = \omega(0)$ if and only if $\mathrm{id}_X = 0$, and so $\omega(X)$ is the zero object if and only if X is the zero object. It follows that, if $\omega(u)$ is a monomorphism (resp. an epimorphism, resp. an isomorphism), then so also is u. For objects X, Y of C, $\mathrm{Hom}(X, Y)$ is a subspace of $\mathrm{Hom}(\omega X, \omega Y)$, and hence has finite dimension over k.

For monomorphisms $X \xrightarrow{\ x\ } Y$ and $X' \xrightarrow{\ x'\ } Y$ with the same target, we write $x \le x'$ if there exists a morphism $X \to X'$ (necessarily unique) giving a commutative triangle. The lattice of subobjects of Y is obtained from the collection of monomorphisms by identifying two monomorphisms x and x' if $x \le x'$ and $x' \le x$. The functor ω maps the lattice of subobjects of Y injectively[6] to the lattice of subspaces of ωY. Hence X has finite length.

Similarly ω maps the lattice of quotient objects of Y injectively to the lattice of quotient spaces of ωY.

For X in C, we let $\langle X \rangle$ denote the full subcategory of C whose objects are the quotients of subobjects of direct sums of copies of X. For example, if C is the category of finite-dimensional comodules over a coalgebra C, then $\langle X \rangle$ is the category of finite-dimensional comodules over C_X (see above).

Let X be an object of C and S a subset of $\omega(X)$. The intersection of the subobjects Y of X such that $\omega(Y) \supset S$ is the smallest subobject with this property – we call it the subobject of X *generated* by S.

An object Y is *monogenic* if it is generated by a single element, i.e., there exists a $y \in \omega(Y)$ such that

$$Y' \subset Y, \ y \in \omega(Y') \implies Y' = Y.$$

Proof of Theorem 9.32 in the case that C *is generated by a single object*

In the next three lemmas, we assume that $\mathsf{C} = \langle X \rangle$ for some X.

---

[6] If $\omega(X) = \omega(X')$, then the kernel of $\binom{x}{x'} \colon X \times X' \to Y$ projects isomorphically onto each of X and X' (because it does after ω has been applied).

LEMMA 9.33. *For every monogenic object Y of C,*

$$\dim_k \omega(Y) \leq (\dim_k \omega(X))^2.$$

PROOF. By hypothesis, there are maps $Y \xleftarrow{\text{onto}} Y_1 \hookrightarrow X^m$. Let y_1 be an element of $\omega(Y_1)$ whose image y in $\omega(Y)$ generates Y, and let Z be the subobject of Y_1 generated by y_1. The image of Z in Y contains y and so equals Y. Hence it suffices to prove the lemma for Z, i.e., we may suppose that $Y \subset X^m$ for some m. We shall deduce that $Y \hookrightarrow X^{m'}$ for some $m' \leq \dim_k \omega(X)$, from which the lemma follows.

Suppose that $m > \dim_k \omega(X)$. The generator y of Y lies in $\omega(Y) \subset \omega(X^m) = \omega(X)^m$. Let $y = (y_1, \ldots, y_m)$ in $\omega(X)^m$. Since $m > \dim_k \omega(X)$, there exist $a_i \in k$, not all zero, such that $\sum a_i y_i = 0$. The a_i define a surjective morphism $X^m \to X$ whose kernel N is isomorphic to X^{m-1}.[7] As $y \in \omega(N)$, we have $Y \subset N$, and so Y embeds into X^{m-1}. Continue in this fashion until $Y \subset X^{m'}$ with $m' \leq \dim_k \omega(X)$. ◻

As $\dim_k \omega(Y)$ can take only finitely many values when Y is monogenic, there exists a monogenic P for which $\dim_k \omega(P)$ has its largest possible value. Let $p \in \omega(P)$ generate P.

LEMMA 9.34.   (a) *The pair (P, p) represents the functor ω.*

   (b) *The object P is a projective generator for C, i.e., the functor $\operatorname{Hom}(P, -)$ is exact and faithful.*

PROOF. (a) Let X be an object of C, and let $x \in \omega(X)$; we have to prove that there exists a unique morphism $f \colon P \to X$ such that $\omega(f)$ sends p to x. The uniqueness follows from the fact p generates P (the equalizer E of two f is a subobject of P such that $\omega(E)$ contains p). To prove the existence, let Q be the smallest subobject of $P \times X$ such that $\omega(Q)$ contains (p, x). The morphism $Q \to P$ defined by the projection map is surjective because P is generated by p. Therefore,

$$\dim_k \omega(Q) \geq \dim_k \omega(P),$$

but because $\dim_k(\omega(P))$ is maximal, equality must hold, and so $Q \to P$ is an isomorphism. The composite of its inverse with the second projection $Q \to X$ is a morphism $P \to X$ sending p to x.

(b) The object P is projective because ω is exact, and it is a generator because ω is faithful. ◻

Let $A = \operatorname{End}(P)$ – it is a k-algebra of finite dimension as a k-vector space (not necessarily commutative) – and let h^P be the functor $X \rightsquigarrow \operatorname{Hom}(P, X)$.

---

[7]Extend $(a_1, \ldots, a_m)$ to an invertible matrix $\begin{pmatrix} a_1, \ldots, a_m \\ A \end{pmatrix}$; then $A \colon X^m \to X^{m-1}$ defines an isomorphism of N onto X^{m-1} because $\omega(A)$ is an isomorphism $\omega(N) \to \omega(X)^{m-1}$.

LEMMA 9.35. *The functor h^P is an equivalence from C to the category of right A-modules of finite dimension over k. Its composite with the forgetful functor is canonically isomorphic to ω.*

PROOF. Because P is a projective generator, h^P is exact and faithful. It remains to prove that it is essentially surjective and full.

Let M be a right A-module of finite dimension over k, and choose a finite presentation for M,

$$A^m \xrightarrow{u} A^n \to M \to 0$$

where u is an $m \times n$ matrix with coefficients in A. This matrix defines a morphism $P^m \to P^n$ whose cokernel X has the property that $h^P(X) \simeq M$. Therefore h^P is essentially surjective.

We have just shown that every object X in C occurs in an exact sequence

$$P^m \xrightarrow{u} P^n \to X \to 0.$$

Let Y be a second object of C. Then

$$\operatorname{Hom}(P^m, Y) \simeq h^P(Y)^m \simeq \operatorname{Hom}(A^m, h^P(Y)) \simeq \operatorname{Hom}(h^P(P^m), h^P(Y)),$$

and the composite of these maps is that defined by h^P. From the diagram

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Hom}(X,Y) & \longrightarrow & \operatorname{Hom}(P^n,Y) & \longrightarrow & \operatorname{Hom}(P^m,Y) \\
& & \downarrow & & \downarrow{\simeq} & & \downarrow{\simeq} \\
0 & \longrightarrow & \operatorname{Hom}(h^P(X),h^P(Y)) & \longrightarrow & \operatorname{Hom}(A^n,h^P(Y)) & \longrightarrow & \operatorname{Hom}(A^m,h^P(Y))
\end{array}
$$

we see that $\operatorname{Hom}(X,Y) \to \operatorname{Hom}(h^P(X),h^P(Y))$ is an isomorphism, and so h^P is full.

For the second statement, $\omega(X) \simeq \operatorname{Hom}(P,X) \simeq \operatorname{Hom}(h^P(P),h^P(X)) = \operatorname{Hom}(A,h^P(X)) \simeq h^P(X)$. $\qquad\square$

As A is a finite k-algebra, its linear dual $C = A^\vee$ is a k-coalgebra, and to give a right A-module structure on a k-vector space is the same as giving a left C-comodule structure. Together with Lemma 9.35, this completes the proof of Theorem 9.32 in the case that $\mathsf{C} = \langle X \rangle$. Note that

$$A \overset{\text{def}}{=} \operatorname{End}(P) \simeq \operatorname{End}(h^P) \simeq \operatorname{End}(\omega),$$

and so

$$C \simeq \operatorname{End}(\omega)^\vee,$$

i.e., the coalgebra C is the k-linear dual of the algebra $\operatorname{End}(\omega)$.

EXAMPLE 9.36. Let A be a finite k-algebra (not necessarily commutative). Because A is finite, its dual $A^\vee$ is a coalgebra, and the left A-module structures on k-vector space correspond to right $A^\vee$-comodule structures. If we take C to be $\mathsf{Mod}(A)$, ω to be the forgetful functor, and X to be A regarded as a left A-module, then

$$\mathrm{End}(\omega|\langle X\rangle)^\vee \simeq A^\vee,$$

and the equivalence of categories $\mathsf{C} \to \mathsf{Comod}(A^\vee)$ in Theorem 9.37 below simply sends an A-module V to V with its canonical $A^\vee$-comodule structure. This is explained in detail in 9.41 and 9.42.

Proof of Theorem 9.32 in the general case

We now consider the general case. For an object X of C, let $A_X = \mathrm{End}(\omega|\langle X\rangle)$, and let $C_X = A_X^\vee$. For each Y in $\langle X\rangle$, A_X acts on $\omega(Y)$ on the left, and so $\omega(Y)$ is a right C_X-comodule; moreover, $Y \rightsquigarrow \omega(Y)$ is an equivalence of categories

$$\langle X\rangle \to \mathsf{Comod}(C_X).$$

Define a partial ordering on the set of isomorphism classes of objects in C by the rule

$$[X] \le [Y] \text{ if } \langle X\rangle \subset \langle Y\rangle.$$

Note that $[X], [Y] \le [X \oplus Y]$, so that we get a directed set, and that if $[X] \le [Y]$, then restriction defines a homomorphism $A_Y \to A_X$. When we pass to the limit over the isomorphism classes, we obtain the following more precise form of the theorem.

THEOREM 9.37. *Let C be an essentially small k-linear abelian category and let $\omega\colon \mathsf{C} \to \mathsf{Vec}_k$ be a k-linear exact faithful functor. Let $C(\omega)$ be the k-coalgebra $\varinjlim_{[X]} \mathrm{End}(\omega|\langle X\rangle)^\vee$. For each object Y in C, the vector space $\omega(Y)$ has a natural structure of a right $C(\omega)$-comodule, and the functor $Y \rightsquigarrow \omega(Y)$ is an equivalence of categories $\mathsf{C} \to \mathsf{Comod}(C(\omega))$.*

ASIDE 9.38. It is essential in Theorems 9.24 and 9.37 that C be essentially small, because otherwise the underlying "set" of $C(\omega)$ may be a proper class. For example, let S be a proper class and let C be the category of finite-dimensional vector spaces graded by S. In this case $C(\omega)$ contains an idempotent for each element of S, and so cannot be a set.

NOTES. The proof of Theorem 9.37 follows Serre 1993, 2.5.

e. Proof of Theorem 9.24

Bialgebras

When we drop the requirement of an antipode from the definition of a Hopf algebra, we get the notion of a bialgebra, which is self-dual.

DEFINITION 9.39. A **bialgebra** over k is a k-module with compatible structures of an associative algebra with identity and of a co-associative coalgebra with co-identity. Specifically, a bialgebra over k is a quintuple $(A, m, e, \Delta, \epsilon)$, where

(a) (A, m, e) is an associative algebra over k with identity e;

(b) (A, Δ, ϵ) is a co-associative coalgebra over k with co-identity ϵ;

(c) $\Delta : A \to A \otimes A$ is a homomorphism of algebras;

(d) $\epsilon : A \to k$ is a homomorphism of algebras.

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

PROPOSITION 9.40. *For a quintuple $(A, m, e, \Delta, \epsilon)$ satisfying (a) and (b) of 9.39, the following conditions are equivalent:*

(a) Δ *and ϵ are algebra homomorphisms;*

(b) *m and e are coalgebra homomorphisms.*

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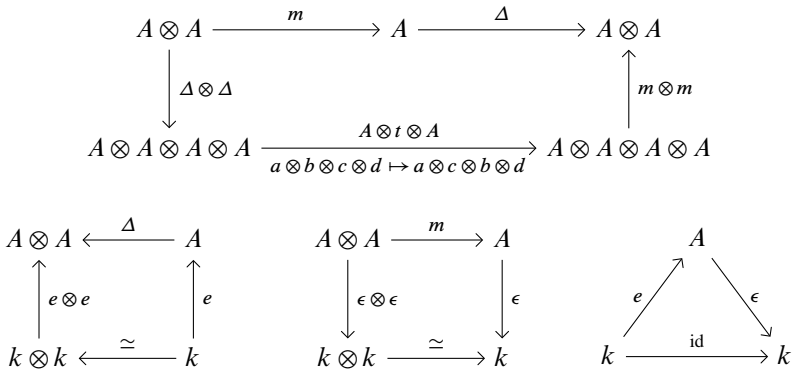
The first and second diagrams commute if and only if Δ is an algebra homomorphism, and the third and fourth diagrams commute if and only if ϵ is an algebra homomorphism. On the other hand, the first and third diagrams commute if and only if m is a coalgebra homomorphism, and the second and fourth commute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

Categories of comodules over a bialgebra

9.41. Let A be a finite k-algebra (not necessarily commutative), and let R be a commutative k-algebra. Consider the functors

$$\mathsf{Mod}(A) \xrightarrow[\text{forget}]{\omega} \mathsf{Vec}(k) \xrightarrow[V \rightsquigarrow R \otimes_k V]{\phi_R} \mathsf{Mod}(R).$$

For $M \in \mathrm{ob}(\mathsf{Mod}(A))$, let $M_0 = \omega(M)$. An element λ of $\mathrm{End}(\phi_R \circ \omega)$ is a family of R-linear maps

$$\lambda_M \colon R \otimes_k M_0 \to R \otimes_k M_0,$$

functorial in M. An element of $R \otimes_k A$ defines such a family, and so we have a map

$$u \colon R \otimes_k A \to \mathrm{End}(\phi_R \circ \omega),$$

which we shall show to be an isomorphism by defining an inverse β. Let $\beta(\lambda) = \lambda_A(1 \otimes 1)$. Clearly $\beta \circ u = \mathrm{id}$, and so we need only show that $u \circ \beta = \mathrm{id}$. The A-module $A \otimes_k M_0$ is a direct sum of copies of A, and the additivity of λ implies that $\lambda_{A \otimes M_0} = \lambda_A \otimes \mathrm{id}_{M_0}$. The map $a \otimes m \mapsto am \colon A \otimes_k M_0 \to M$ is A-linear, and hence

$$
\begin{array}{ccc}
R \otimes_k A \otimes_k M_0 & \longrightarrow & R \otimes_k M \\
\downarrow{\scriptstyle \lambda_A \otimes \mathrm{id}_{M_0}} & & \downarrow{\scriptstyle \lambda_M} \\
R \otimes_k A \otimes_k M_0 & \longrightarrow & R \otimes_k M
\end{array}
$$

commutes. Therefore

$$\lambda_M(1 \otimes m) = \lambda_A(1) \otimes m = (u \circ \beta(\lambda))_M(1 \otimes m) \text{ for } 1 \otimes m \in R \otimes M,$$

i.e., $u \circ \beta = \mathrm{id}$.

9.42. Let C be a k-coalgebra and ω the forgetful functor on $\mathsf{Comod}(C)$. When C is finite over k, to give an object of $\mathsf{Comod}(C)$ is essentially the same as giving a finitely generated module over the k-algebra $A = C^{\vee}$, and so 9.41 shows that

$$C \simeq \mathrm{End}(\omega)^{\vee}.$$

In the general case,

$$C \simeq \varinjlim_{[X]} C_X \simeq \varinjlim_{[X]} \mathrm{End}(\omega_C|\langle X \rangle)^{\vee}.$$

Let $u \colon C \to C'$ be a homomorphism of k-coalgebras. A co-action $V \to V \otimes C$ of C on V defines a co-action $V \to V \otimes C'$ of C' on V by composition with $\mathrm{id}_V \otimes u$. Thus, u defines a functor $F \colon \mathsf{Comod}(C) \to \mathsf{Comod}(C')$ such that

$$\omega_{C'} \circ F = \omega_C. \tag{53}$$

LEMMA 9.43. *Every functor $F \colon \mathsf{Comod}(C) \to \mathsf{Comod}(C')$ satisfying the condition (53) arises, as above, from a unique homomorphism of k-coalgebras $C \to C'$.*

PROOF. The functor F defines a homomorphism

$$\varinjlim_{[X]} \mathrm{End}(\omega_{C'}|\langle FX \rangle) \to \varinjlim_{[X]} \mathrm{End}(\omega_C|\langle X \rangle),$$

and $\varinjlim_{[X]} \text{End}(\omega_{C'}|\langle FX \rangle)$ is a quotient of $\varinjlim_{[Y]} \text{End}(\omega_{C'}|\langle Y \rangle)$. On passing to the duals, we get a homomorphism

$$\varinjlim \text{End}(\omega_C|\langle X \rangle)^\vee \to \varinjlim \text{End}(\omega_{C'}|\langle Y \rangle)^\vee$$

and hence a homomorphism $C \to C'$. This has the required property.   □

Let C be a coalgebra over k. Then $(C \otimes C, \Delta_C \otimes \Delta_C, \epsilon_C \otimes \epsilon_C)$ is again a coalgebra over k, and a coalgebra homomorphism $m: C \otimes C \to C$ defines a functor

$$\phi^m: \text{Comod}(C) \times \text{Comod}(C) \to \text{Comod}(C)$$

sending (V, W) to $V \otimes W$ with the co-action

$$V \otimes W \xrightarrow{\rho_V \otimes \rho_W} V \otimes C \otimes W \otimes C \simeq V \otimes W \otimes C \otimes C \xrightarrow{V \otimes W \otimes m} V \otimes W \otimes C.$$

PROPOSITION 9.44. *The map* $m \mapsto \phi^m$ *defines a one-to-one correspondence between the set of k-coalgebra homomorphisms* $m: C \otimes C \to C$ *and the set of k-bilinear functors*

$$\phi: \text{Comod}(C) \times \text{Comod}(C) \to \text{Comod}(C)$$

such that $\phi(V, W) = V \otimes W$ *as k-vector spaces.*

(a) *The homomorphism m is associative if and only if the canonical isomorphisms of vector spaces*

$$u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w: U \otimes (V \otimes W) \to (U \otimes V) \otimes W$$

are isomorphisms of C-comodules for all C-comodules U, V, W.

(b) *The homomorphism m is commutative (i.e., $m(a, b) = m(b, a)$ for all $a, b \in C$) if and only if the canonical isomorphisms of vector spaces*

$$v \otimes w \mapsto w \otimes v: V \otimes W \to W \otimes V$$

are isomorphisms of C-comodules for all C-comodules W, V.

(c) *There is an identity map $e: k \to C$ if and only if there exists a C-comodule U with underlying vector space k such that the canonical isomorphisms of vector spaces*

$$U \otimes V \simeq V \simeq V \otimes U$$

are isomorphisms of C-comodules for all C-comodules V.

PROOF. The pair $(\text{Comod}(C) \times \text{Comod}(C), \omega \otimes \omega)$, with

$$(\omega \otimes \omega)(X, Y) = \omega(X) \otimes \omega(Y) \qquad (\text{as a } k\text{-vector space}),$$

satisfies the conditions of (9.37), and $\varinjlim \text{End}(\omega \otimes \omega|\langle (X, Y) \rangle)^\vee = C \otimes C$. Thus

$$(\text{Comod}(C) \times \text{Comod}(C), \omega_C \otimes \omega_C) \simeq (\text{Comod}(C \otimes C), \omega_{C \otimes C}),$$

and so the first statement of the proposition follows from Lemma 9.43. The remaining statements involve only routine checking.   □

THEOREM 9.45. *Let* C *be an essentially small k-linear abelian category and* $\otimes: C \times C \to C$ *a k-bilinear functor. Let* $\omega: C \to \mathsf{Vec}_k$ *be a k-linear exact faithful functor satisfying (a), (b), and (c) of 9.24. Let* $C(\omega) = \varinjlim \mathrm{End}(\omega|\langle X \rangle)^{\vee}$, *so that* ω *defines an equivalence of categories* $C \to \mathsf{Comod}(C(\omega))$ *(Theorem 9.37). Then* $C(\omega)$ *has a unique structure* (m, e) *of a commutative k-bialgebra such that* $\otimes = \phi^m$ *and* $\omega(\mathbb{1}) = (k \xrightarrow{e} C(\omega) \simeq k \otimes C(\omega))$.

PROOF. To give a bialgebra structure on a coalgebra (A, Δ, ϵ), one has to give coalgebra homomorphisms (m, e) such that m is commutative and associative and e is an identity map. Thus, the statement is an immediate consequence of Proposition 9.44. $\qquad\square$

Categories of representations of affine groups

We now prove a more precise version of Theorem 9.24.

THEOREM 9.46. *Let* C *be an essentially small k-linear abelian category, let* $\otimes: C \times C \to C$ *be a k-bilinear functor. Let* ω *be an exact faithful k-linear functor* $C \to \mathsf{Vec}_k$ *satisfying the conditions (a), (b), and (c) of 9.24. For each k-algebra R, let $G(R)$ be the set of families*

$$(\lambda_V)_{V \in \mathrm{ob}(C)}, \quad \lambda_V \in \mathrm{End}_{R\text{-linear}}(\omega(V)_R),$$

such that

⋄ $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ *for all* $V, W \in \mathrm{ob}(C)$,

⋄ $\lambda_{\mathbb{1}} = \mathrm{id}_{\omega(\mathbb{1})}$ *for every identity object of $\mathbb{1}$ of* C, *and*

⋄ $\lambda_W \circ \omega(u)_R = \omega(u)_R \circ \lambda_V$ *for all arrows u in* C.

Then G is an affine monoid over k, and ω defines an equivalence of tensor categories,

$$C \to \mathsf{Rep}(G).$$

When ω satisfies the following condition, G is an affine group:

(d) *for every object X such that $\omega(X)$ has dimension 1, there exists an object X^{-1} in C such that $X \otimes X^{-1} \approx \mathbb{1}$.*

PROOF. Theorem 9.45 allows us to assume that $C = \mathsf{Comod}(C)$ for C a k-bialgebra, and that $\otimes$ and ω are the natural tensor product structure and forgetful functor. Let G be the affine monoid corresponding to C. Using 9.41 we find that, for every k-algebra R,

$$\underline{\mathrm{End}}(\omega)(R) \overset{\mathrm{def}}{=} \mathrm{End}(\phi_R \circ \omega) = \varprojlim \mathrm{Hom}_{k\text{-linear}}(C_X, R) = \mathrm{Hom}_{k\text{-linear}}(C, R).$$

An element $\lambda \in \mathrm{Hom}_{k\text{-linear}}(C_X, R)$ corresponds to an element of $\underline{\mathrm{End}}(\omega)(R)$ commuting with the tensor structure if and only if λ is a k-algebra homomorphism; thus

$$\underline{\mathrm{End}}^{\otimes}(\omega)(R) = \mathrm{Hom}_{k\text{-algebra}}(C, R) = G(R).$$

We have shown that $\underline{\operatorname{End}}^{\otimes}(\omega)$ is representable by the affine monoid $G = \operatorname{Spec}(C)$ and that ω defines an equivalence of tensor categories

$$\mathsf{C} \to \mathsf{Comod}(C) \to \mathsf{Rep}_k(G).$$

On applying (d) to the highest exterior power of an object of C, we find that $\underline{\operatorname{End}}^{\otimes}(\omega) = \underline{\operatorname{Aut}}^{\otimes}(\omega)$, which completes the proof. $\qquad\square$

NOTES. The proof of Theorem 9.46 follows Deligne and Milne 1982, §2. There are shorter but less elementary proofs.

f. Tannakian categories

In this section, we sketch a little of the abstract theory of Tannakian categories. For more, see Saavedra Rivano 1972 or Deligne and Milne 1982.

A k-linear ***tensor category*** is a system $(\mathsf{C}, \otimes, \phi, \psi)$ in which C is a k-linear category, $\otimes \colon \mathsf{C} \times \mathsf{C} \to \mathsf{C}$ is a k-bilinear functor, and ϕ and ψ are functorial isomorphisms

$$\phi_{X,Y,Z} \colon X \otimes (Y \otimes Z) \to (X \otimes Y) \otimes Z$$
$$\psi_{X,Y} \colon X \otimes Y \to Y \otimes X$$

satisfying certain natural conditions which ensure that the tensor product of every (unordered) finite family of objects of C is well-defined up to a well-defined isomorphism. In particular, there is an identity object $\mathbb{1}$ (tensor product of the empty family) such that $X \rightsquigarrow \mathbb{1} \otimes X \colon \mathsf{C} \to \mathsf{C}$ is an equivalence of categories.

For example, the category of representations of an affine monoid G over k on finite-dimensional k-vector spaces becomes a k-linear tensor category when equipped with the usual tensor product and the isomorphisms (52), p. 172.

A k-linear tensor category is ***rigid*** if every object has a dual (in the sense of 9.26). For example, the category of representations of G is rigid if G is an affine group. A rigid abelian k-linear tensor category $(\mathsf{C}, \otimes)$ is a ***Tannakian category*** over k if $\operatorname{End}(\mathbb{1}) = k$ and there exists a k-algebra R and an exact faithful k-linear functor $\omega \colon (\mathsf{C}, \otimes) \to (\mathsf{Vec}_R, \otimes)$ preserving the tensor structure. Such a functor is said to be an R-***valued fibre functor*** for C.

A Tannakian category over k is said to be ***neutral*** if there exists a k-valued fibre functor. The first main theorem in the theory of neutral Tannakian categories is the following (Deligne and Milne 1982, Theorem 2.11).

THEOREM 9.47. *Let* $(\mathsf{C}, \otimes)$ *be a neutral Tannakian category over* k *and* ω *a* k-*valued fibre functor. Then,*

(a) *the functor* $\underline{\operatorname{Aut}}^{\otimes}(\omega)$ *(see 9.8) of* k-*algebras is represented by an affine group scheme* G;

(b) *the functor* $\mathsf{C} \to \mathsf{Rep}(G)$ *defined by* ω *is an equivalence of tensor categories.*

PROOF. The functor ω satisfies the conditions of Theorem 9.24. For (a), (b), and (c), this is obvious; for (d) one has to note that if $\omega(X)$ has dimension 1, then the map ev: $X^\vee \otimes X \to \mathbb{1}$ is an isomorphism.   □

For an affine group scheme G over k, the pair $(\mathsf{Rep}(G), \otimes)$ is a neutral Tannakian category over k, and the forgetful functor is a fibre functor; moreover the obvious morphism of functors $G \to \underline{\mathrm{Aut}}^\otimes(\omega_{\mathrm{forget}})$ is an isomorphism. Thus, the theorem gives a dictionary between the neutralized Tannakian categories over k and the affine group schemes over k. To complete the theory in the neutral case, it remains to describe the fibre functors for C with values in a k-algebra R.

THEOREM 9.48. *Let* $\mathsf{C}, \otimes, \omega, G$ *be as in Theorem 9.47 and* R *a* k-*algebra.*

(a) *For every* R-*valued fibre functor* ν *on* C, *the functor*

$$R \rightsquigarrow \mathrm{Isom}^\otimes(\omega \otimes R, \nu)$$

is represented by an affine scheme $\underline{\mathrm{Isom}}^\otimes(\omega_R, \nu)$ *over* R *which, when endowed with the obvious right action of* G_R, *becomes a* G_R-*torsor for the flat (fpqc) topology.*

(b) *The functor* $\nu \rightsquigarrow \underline{\mathrm{Isom}}^\otimes(\omega_R, \nu)$ *establishes an equivalence between the category of* R-*valued fibre functors on* C *and the category of right* G_R-*torsors on* $\mathrm{Spec}(R)$ *for the flat (fpqc) topology.*

PROOF. The proof is an extension of that of Theorems 9.24 and 9.47 – see Deligne and Milne 1982, Theorem 3.2.   □

The theory of nonneutral Tannakian categories is more difficult, and the fundamental classification theorems were proved only in Deligne 1990.

g. Properties of G versus those of $\mathsf{Rep}(G)$

Since the study of G is equivalent to the study of $\mathsf{Rep}(G)$, the properties of one should be reflected in the properties of the other. Here we provide a brief dictionary.

9.49. *An algebraic group* G *is finite if and only if there exists a representation* (V, r) *such that every representation of* G *is a subquotient of* V^n *for some* $n \geq 0$.

If G is finite, then the regular representation X of G is finite-dimensional, and has the required property. Conversely if $\mathsf{Rep}(G) = \langle X \rangle$, then $G = \mathrm{Spec}(B)$, where B is the linear dual of the finite k-algebra $A_X = \mathrm{End}(\omega)$. See Section e.

9.50. *An algebraic group* G *has no finite quotients if and only if, for every representation* V *on which* G *acts nontrivially, the full subcategory of* $\mathsf{Rep}(G)$ *of subquotients of* V^n, $n \geq 0$, *is not stable under* $\otimes$. *In characteristic zero, an algebraic group has no finite quotients if and only if it is connected.*

Consequence of 9.49.

9.51. *By definition, an algebraic group is unipotent if the only simple represent-ations are one-dimensional spaces with the trivial action. These are the groups isomorphic to an algebraic subgroup of* $\mathbb{U}_n$ *for some n (see 14.5).*

9.52. *By definition, an algebraic group is trigonalizable if every simple rep-resentation has dimension* 1. *These are the groups isomorphic to an algebraic subgroup of* $\mathbb{T}_n$ *for some n (see 16.2).*

9.53. *A connected group variety G over an algebraically closed field is solvable if and only if it is trigonalizable (Lie–Kolchin theorem 16.30).*

9.54. *A connected group variety over a perfect field is reductive if it has a faithful semisimple representation (19.17). A connected group variety G over a field of characteristic zero is reductive if and only if* Rep(G) *is semisimple (22.42).*

9.55. *Let* $\varphi\colon G \to G'$ *be a homomorphism of algebraic groups over k, and let* ω^φ *be the corresponding functor* Rep(G') $\to$ Rep(G).

(a) *φ is faithfully flat if and only if ω^φ is fully faithful and every subobject of $\omega^\varphi(X')$, for $X' \in$ ob(Rep(G')), is isomorphic to the image of a subobject of X'.*

(b) *φ is a closed immersion if and only if every object of* Rep(G) *is isomorphic to a subquotient of an object of the form of $\omega^\varphi(X')$, where X' is an object of* Rep(G').

See Deligne and Milne 1982, 2.21.

The Lie Algebra of an Algebraic Group

Recall that all algebraic groups are affine over a base field k. In this chapter, an algebra A over k is (as in Bourbaki) a k-vector space equipped with a bilinear map $A \times A \to A$ (not necessarily associative or commutative).

a. Definition

DEFINITION 10.1. A *Lie algebra* over a field k is a vector space $\mathfrak{g}$ over k together with a k-bilinear map

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

(called the **bracket**) such that
  (a) $[x, x] = 0$ for all $x \in \mathfrak{g}$, and
  (b) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in \mathfrak{g}$.
A **homomorphism of Lie algebras** is a k-linear map $u: \mathfrak{g} \to \mathfrak{g}'$ such that

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

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

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

$$[x, y] = -[y, x], \text{ for all } x, y \in \mathfrak{g}, \tag{54}$$

and that (54) allows us to rewrite the Jacobi identity as

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]] \tag{55}$$

or

$$[[x,y],z] = [x,[y,z]] - [y,[x,z]]$$

We shall be mainly concerned with finite-dimensional Lie algebras.

EXAMPLE 10.2. The Lie algebra $\mathfrak{sl}_2$ is the k-vector space of 2×2 matrices of trace 0 equipped with the bracket $[x,y] = xy - yx$. The elements

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

form a basis for $\mathfrak{sl}_2$ and $[X,Y] = H$, $[H,X] = 2X$, $[H,Y] = -2Y$.

EXAMPLE 10.3. Let A be an associative algebra over k. The bracket $[a,b] = ab - ba$ is k-bilinear, and it makes A into a Lie algebra because $[a,a]$ is obviously 0 and the Jacobi identity can be proved by a direct calculation. In fact, on expanding out the left side of the Jacobi identity for a,b,c one obtains a sum of 12 terms, 6 with plus signs and 6 with minus signs; by symmetry, each permutation of a,b,c must occur exactly once with a plus sign and exactly once with a minus sign. When A is the endomorphism ring $\text{End}_{k\text{-linear}}(V)$ of a k-vector space V, this Lie algebra is denoted $\mathfrak{gl}_V$, and when $A = M_n(k)$, it is denoted $\mathfrak{gl}_n$. Let E_{ij} denote the matrix with 1 in the ijth position and 0 elsewhere. These matrices form a basis for $\mathfrak{gl}_n$, and

$$[E_{ij}, E_{i'j'}] = \delta_{ji'} E_{ij'} - \delta_{j'i} E_{i'j} \quad (\delta_{ij} = \text{ Kronecker delta}).$$

EXAMPLE 10.4. Let A be an algebra over k. A k-linear map $D : A \to A$ is a **derivation** of A if

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

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 $\mathfrak{gl}_A$.

DEFINITION 10.5. Let $\mathfrak{g}$ be a Lie algebra over k. For a fixed x in $\mathfrak{g}$, the k-linear map

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

is called the **adjoint map** of x, and is denoted $\text{ad}_{\mathfrak{g}}(x)$ or $\text{ad}(x)$. The Jacobi identity (specifically (55)) says that $\text{ad}_{\mathfrak{g}}(x)$ is a derivation of $\mathfrak{g}$:

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

Directly from the definitions, one sees that

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

and so

$$\text{ad}_{\mathfrak{g}} : \mathfrak{g} \to \text{Der}_k(\mathfrak{g})$$

is a homomorphism of Lie algebras. It is called the **adjoint representation**.

b.   The Lie algebra of an algebraic group

10.6. Let G be an algebraic group over k. The tangent space of G at the neutral element e is
$$L(G) = \mathrm{Ker}(G(k[\varepsilon]) \to G(k)), \quad \varepsilon^2 = 0.$$

Thus, an element of $L(G)$ is a homomorphism $\varphi \colon \mathcal{O}(G) \to k[\varepsilon]$ whose composite with $\varepsilon \mapsto 0 \colon k[\varepsilon] \to k$ is the co-identity map $\epsilon \colon \mathcal{O}(G) \to k$. In particular, φ maps the augmentation ideal $I_G = \mathrm{Ker}(\epsilon)$ into (ε). As $\varepsilon^2 = 0$, φ factors through $\mathcal{O}(G)/I_G^2$. Now $\mathcal{O}(G)/I_G^2 \simeq k \oplus (I_G/I_G^2)$ (see 3.22), and φ sends $(a,b) \in k \oplus I_G/I_G^2$ to $a + D(b)\varepsilon$ with $D(b) \in k$. The map $\varphi \mapsto D$ is a bijection, and so

$$L(G) \simeq \mathrm{Hom}_{k\text{-linear}}(I_G/I_G^2, k). \tag{56}$$

We define the Lie algebra of G to be

$$\mathrm{Lie}(G) = \mathrm{Hom}_{k\text{-linear}}(I_G/I_G^2, k).$$

Note that $\mathrm{Lie}(G)$ is a k-vector space.

Following a standard convention, we write $\mathfrak{g}$ for $\mathrm{Lie}(G)$, $\mathfrak{h}$ for $\mathrm{Lie}(H)$, and so on.

10.7. Let $G = \mathrm{GL}_n$, and let $I_n = \mathrm{diag}(1, \dots, 1)$. Then

$$L(G) = \{I_n + A\varepsilon \mid A \in M_n(k)\}.$$

On the other hand, $\mathcal{O}(G)$ is the k-algebra of polynomials in the symbols T_{11}, $T_{12}, \dots, T_{nn}$ with $\det(T_{ij})$ inverted. The co-identity map sends T_{ii} to 1 and T_{ij} to 0 if $i \neq j$, and so the ideal I_G is generated by the polynomials $T_{ij} - \delta_{ij}$ with δ_{ij} the Kronecker delta. It follows that the k-vector space I_G/I_G^2 has basis

$$(T_{11} - \delta_{11}) + I_G^2, (T_{12} - \delta_{12}) + I_G^2, \dots, (T_{nn} - \delta_{nn}) + I_G^2,$$

and so

$$\mathrm{Hom}_{k\text{-linear}}(I_G/I_G^2, k) \simeq M_n(k).$$

The isomorphism $\mathrm{Lie}(\mathrm{GL}_n) \to L(\mathrm{GL}_n)$ is $A \mapsto I_n + A\varepsilon$.

We define the bracket on $\mathrm{Lie}(\mathrm{GL}_n)$ to be

$$[A, B] = AB - BA. \tag{57}$$

Thus $\mathrm{Lie}(\mathrm{GL}_n) \simeq \mathfrak{gl}_n$. Regard $I_n + A\varepsilon$ and $I_n + B\varepsilon$ as elements of $G(k[\varepsilon])$ where now $k[\varepsilon] = k[T]/(T^3)$. Then the commutator of $I_n + A\varepsilon$ and $I_n + B\varepsilon$ in $G(k[\varepsilon])$ is

$$(I_n + A\varepsilon)(I_n + B\varepsilon)(I_n + A\varepsilon)^{-1}(I_n + B\varepsilon)^{-1}$$
$$= (I_n + A\varepsilon)(I_n + B\varepsilon)(I_n - A\varepsilon + A^2\varepsilon^2)(I_n - B\varepsilon + B^2\varepsilon^2)$$
$$= I_n + 2(AB - BA)\varepsilon^2$$

and so the bracket measures the failure of commutativity in $\mathrm{GL}_n(k[\varepsilon])$ modulo ε^3.

Shortly, we shall see that there is a unique functorial way of defining a bracket on the Lie algebras of all algebraic groups that gives (57) in the case of GL_n.

10.8. We have

$$
L(\mathbb{U}_n) = \left\{ \begin{pmatrix} 1 & \varepsilon c_{12} & \cdots & \varepsilon c_{1\,n-1} & \varepsilon c_{1n} \\ 0 & 1 & \cdots & \varepsilon c_{2\,n-1} & \varepsilon c_{2\,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \varepsilon c_{n-1\,n} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \right\},
$$

and

$$
\mathrm{Lie}(\mathbb{U}_n) \simeq \mathfrak{n}_n \overset{\text{def}}{=} \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \geq j\}.
$$

10.9. Let V_a be the algebraic group defined by a finite-dimensional k-vector space V (see 2.6). Then $\mathcal{O}(V_a) = \mathrm{Sym}(V^\vee) = \bigoplus_{n \geq 0}(V^\vee)^{\otimes n}$, the augmentation ideal $I = \bigoplus_{n \geq 1}(V^\vee)^{\otimes n}$, and $I/I^2 \simeq (V^\vee)^{\otimes 1} = V^\vee$. Therefore

$$
\mathrm{Lie}(V_a) \simeq \mathrm{Hom}_{k\text{-linear}}(V^\vee, k) \simeq V,
$$

and so $V_a \simeq (\mathrm{Lie}(V_a))_a$. In fact, $U \simeq \mathrm{Lie}(U)_a$ for any vector group U.

10.10. Let $t: V \times \cdots \times V \to k$ be an r tensor, and let G be the algebraic subgroup of GL_V fixing t (see 2.13). Then

$$
\mathrm{Lie}(G) \simeq \{g \in \mathrm{End}(V) \mid \sum_j t(v_1, \ldots, g v_j, \ldots, v_r) = 0 \text{ all } (v_i)\}.
$$

Indeed, $L(G)$ consists of the endomorphisms $1 + g\varepsilon$ of $V(k[\varepsilon])$ such that

$$
t((1+g\varepsilon)v_1, (1+g\varepsilon)v_2, \ldots) = t(v_1, v_2, \ldots).
$$

On expanding this and cancelling, we obtain the assertion.

10.11. We write $e^{\varepsilon X}$ for the element of $L(G) \subset G(k[\varepsilon])$ corresponding to an element X of $\mathrm{Lie}(G)$ under the isomorphism (56): $L(G) \simeq \mathrm{Lie}(G)$. For example, if $G = \mathrm{GL}_n$, so $\mathrm{Lie}(G) = \mathfrak{gl}_n$, then

$$
e^{\varepsilon X} = I + \varepsilon X \qquad (X \in M_n(k), \ e^{\varepsilon X} \in \mathrm{GL}_n(k[\varepsilon])).
$$

We have

$$
e^{\varepsilon(X+X')} = e^{\varepsilon X} \cdot e^{\varepsilon X'}, \quad X, X' \in \mathrm{Lie}(G),
$$
$$
e^{\varepsilon(cX)} = e^{(c\varepsilon)X}, \quad c \in k, \quad X \in \mathrm{Lie}(G).
$$

The first equality expresses that $X \mapsto e^{\varepsilon X} : \mathrm{Lie}(G) \to L(G)$ is a homomorphism of abelian groups, and the second that multiplication by c on $\mathrm{Lie}(G)$ corresponds to the multiplication of c on $L(G)$ induced by the action $a + b\varepsilon \mapsto a + bc\varepsilon$ of c on $k[\varepsilon]$ (Exercise 10-1).

10.12. An action of an algebraic group G on an algebraic group U defines a linear representation of G on the vector space $\mathrm{Lie}(U)$. When U is a vector group, there is a canonical isomorphism $U \to \mathrm{Lie}(U)_{\mathfrak{a}}$ (see 10.9), and we say that the action of G on U is **linear** if this isomorphism is G-equivariant. For a finite-dimensional vector space V, the linear actions of G on $V_{\mathfrak{a}}$ correspond to the linear representation of G on V.

ASIDE 10.13. In characteristic zero, every action of an algebraic group G on a vector group U is linear (because it commutes with the exponential map 14.32). This is no longer true in characteristic $p \neq 0$ (2.12; see also McNinch 2014b).

c.   Basic properties of the Lie algebra

10.14. Let (G_i, φ_{ij}) be an inverse system of algebraic groups indexed by a finite set I. For each i, the sequence $0 \to L(G_i) \to G_i(k[\varepsilon]) \to G_i(k)$ is exact. On passing to the inverse limit, we obtain an exact sequence

$$0 \to \varprojlim(L(G_i)) \to (\varprojlim G_i)(k[\varepsilon]) \to (\varprojlim G_i)(k),$$

and so $\varprojlim(L(G_i) \simeq L(\varprojlim G_i)$. Hence

$$\varprojlim(\mathrm{Lie}(G_i)) \simeq \mathrm{Lie}(\varprojlim G_i).$$

For example, an exact sequence of groups $e \to G' \to G \to G''$ gives an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}(G') \to \mathrm{Lie}(G) \to \mathrm{Lie}(G''),$$

and the functor Lie commutes with fibred products:

$$\mathrm{Lie}(H_1 \times_G H_2) \simeq \mathrm{Lie}(H_1) \times_{\mathrm{Lie}(G)} \mathrm{Lie}(H_2).$$

In particular, if H_1 and H_2 are algebraic subgroups of G, then $\mathrm{Lie}(H_1)$ and $\mathrm{Lie}(H_2)$ are subspaces of $\mathrm{Lie}(G)$ and

$$\mathrm{Lie}(H_1 \cap H_2) = \mathrm{Lie}(H_1) \cap \mathrm{Lie}(H_2).$$

Consider, for example, the subgroups SL_2 and $\mathbb{G}_m$ (scalar matrices) in GL_2 over a field k of characteristic 2. Then $\mathrm{SL}_2 \cap \mathbb{G}_m = \mu_2$, and

$$\mathrm{Lie}(\mathrm{SL}_2) \cap \mathrm{Lie}(\mathbb{G}_m) = \{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix} \right) \mid a \in k \} = \mathrm{Lie}(\mu_2)$$

(because $a + a = 0$ in k). Note that, in a world without nilpotents, $\mathrm{SL}_2 \cap \mathbb{G}_m = e$ and $\mathrm{Lie}(\mathrm{SL}_2 \cap \mathbb{G}_m) \neq \mathrm{Lie}(\mathrm{SL}_2) \cap \mathrm{Lie}(\mathbb{G}_m)$.

PROPOSITION 10.15. *Let $H \subset G$ be algebraic groups such that $\mathrm{Lie}(H) = \mathrm{Lie}(G)$. If H is smooth and G is connected, then $H = G$.*

PROOF. Recall that $\dim(\mathfrak{g}) \geq \dim(G)$, with equality if and only if G is smooth (1.37). From

$$\dim(H) = \dim(\mathfrak{h}) = \dim(\mathfrak{g}) \geq \dim(G) \geq \dim(H),$$

we see that $\dim(\mathfrak{g}) = \dim(G)$, and so G is smooth, and that $\dim(G) = \dim(H)$, and so $G = H$ (because G is smooth and connected). □

COROLLARY 10.16. *Let H_1 and H_2 be smooth connected subgroups of G such that $\mathrm{Lie}(H_1) = \mathrm{Lie}(H_2)$. If $H_1 \cap H_2$ is smooth, then $H_1 = H_2$.*

PROOF. From

$$\mathrm{Lie}(H_1 \cap H_2) = \mathrm{Lie}(H_1) \cap \mathrm{Lie}(H_2) = \mathrm{Lie}(H_1),$$

we see that $H_1 \cap H_2 = H_1$. Similarly it equals H_2. □

COROLLARY 10.17. *Let $H_1, \ldots, H_n$ be smooth algebraic subgroups of a connected algebraic group G. If the Lie algebras of the H_i generate $\mathrm{Lie}(G)$ as a Lie algebra, then the H_i generate G as an algebraic group.*

PROOF. By definition, the algebraic subgroup generated by the H_i is the smallest algebraic subgroup H of G such that all inclusion maps $H_i \hookrightarrow G$ factor through H – it exists, and is smooth (2.51). We have $\mathrm{Lie}(H_i) \subset \mathrm{Lie}(H) \subset \mathrm{Lie}(G)$ for all i, and so $\mathrm{Lie}(H) = \mathrm{Lie}(G)$. Therefore $H = G$. □

The examples $\mathrm{Lie}(\alpha_p) = \mathrm{Lie}(\mathbb{G}_a)$ and $\mathrm{Lie}(G^\circ) = \mathrm{Lie}(G)$ show that we need H to be smooth and G to be connected in Proposition 10.15.

d.   The adjoint representation; definition of the bracket

10.18. Let G be an algebraic group over k with Lie algebra $\mathfrak{g}$. For a k-algebra R (commutative and finitely generated), we define $\mathfrak{g}(R)$ by the exact sequence

$$0 \to \mathfrak{g}(R) \to G(R[\varepsilon]) \overset{\varepsilon \mapsto 0}{\longrightarrow} G(R) \to 0.$$

Thus $\mathfrak{g}(k) = L(G) \simeq \mathfrak{g}$. For example, let V be a k-vector space, and let $G = \mathrm{GL}_V$. Let $V(\varepsilon) = R[\varepsilon] \otimes V$. Then $V(\varepsilon) = V_R \oplus \varepsilon V_R$ as an R-module, and

$$\mathfrak{g}(R) = \{\mathrm{id} + \varepsilon \alpha \mid \alpha \in \mathrm{End}(V_R)\}$$

where $\mathrm{id} + \varepsilon \alpha$ acts on $V(\varepsilon)$ by

$$(\mathrm{id} + \varepsilon \alpha)(x + \varepsilon y) = x + \varepsilon y + \varepsilon \alpha(x). \tag{58}$$

10.19. Recall (3.22) that we have a split-exact sequence of k-vector spaces

$$0 \to I \to \mathcal{O}(G) \xrightarrow{\epsilon} k \to 0$$

where I is the augmentation ideal (maximal ideal at e in $\mathcal{O}(G)$). On tensoring this with R, we get an exact sequence of R-modules

$$0 \to I_R \to \mathcal{O}(G)_R \xrightarrow{\epsilon_R} R \to 0.$$

By definition, an element of $\mathfrak{g}(R)$ is a homomorphism $\varphi \colon \mathcal{O}(G)_R \to R[\varepsilon]$ whose composite with $\varepsilon \mapsto 0 \colon R[\varepsilon] \to R$ is ϵ_R. As in 10.6, φ factors through

$$\mathcal{O}(G)_R / I_R^2 \simeq R \oplus I_R / I_R^2,$$

and corresponds to an R-linear homomorphism $I_R / I_R^2 \to R$. Hence

$$\mathfrak{g}(R) \simeq \operatorname{Hom}_{R\text{-linear}}(I_R / I_R^2, R) \simeq \operatorname{Hom}_{k\text{-linear}}(I / I^2, k) \otimes R = \mathfrak{g} \otimes R.$$

As in (10.11), we write $e^{\varepsilon X}$ for the element of $\mathfrak{g}(R)$ corresponding to an element X of $\mathfrak{g} \otimes R$ under this isomorphism. For a homomorphism $f \colon G \to H$,

$$f(e^{\varepsilon X}) = e^{\varepsilon \operatorname{Lie}(f)(X)}, \quad \text{for } X \in \mathfrak{g} \otimes R. \tag{59}$$

This expresses that the isomorphism $\mathfrak{g} \otimes R \simeq \mathfrak{g}(R)$ is functorial.

10.20. The group $G(R[\varepsilon])$ acts on $\mathfrak{g}(R)$ by inner automorphisms. As $G(R)$ is a subgroup of $G(R[\varepsilon])$, it also acts. In this way, we get a homomorphism

$$G(R) \to \operatorname{Aut}_{k\text{-linear}}(\mathfrak{g}(R)),$$

which is natural in R, and so defines a representation

$$\operatorname{Ad} \colon G \to \operatorname{GL}_{\mathfrak{g}}.$$

This is called the ***adjoint representation*** (or ***action***) of G.

For example, from

$$(A, I + X\varepsilon) \mapsto I + AXA^{-1}\varepsilon \colon \operatorname{GL}_n(R) \times \mathfrak{gl}_n(R) \to \mathfrak{gl}_n(R),$$

we deduce that the adjoint action of GL_n on $\mathfrak{gl}_n$ is conjugation: $\operatorname{Ad}(A)(X) = AXA^{-1}$.

10.21. By definition,

$$x \cdot e^{\varepsilon X} \cdot x^{-1} = e^{\varepsilon \operatorname{Ad}(x)X} \text{ for } x \in G(R), \ X \in \mathfrak{g} \otimes R. \tag{60}$$

For a homomorphism $f \colon G \to H$,

$$
\begin{CD}
G \times \mathfrak{g} @>{(x,X) \mapsto \operatorname{Ad}(x)X}>> \mathfrak{g} \\
@V{f \times \operatorname{Lie}(f)}VV @VV{\operatorname{Lie}(f)}V \\
H \times \mathfrak{h} @>{(y,Y) \mapsto \operatorname{Ad}(y)Y}>> \mathfrak{h}
\end{CD}
\tag{61}
$$

commutes, i.e.,

$$\mathrm{Lie}(f)(\mathrm{Ad}(x)X) = \mathrm{Ad}(f(x))\mathrm{Lie}(f)(X) \text{ for } x \in G(R),\ X \in \mathfrak{g} \otimes R.$$

Indeed,

$$e^{\varepsilon \mathrm{LHS}} \overset{(59)}{=} f(e^{\varepsilon \mathrm{Ad}(x)X}) \overset{(60)}{=} f(x \cdot e^{\varepsilon X} \cdot x^{-1})$$

and

$$e^{\varepsilon \mathrm{RHS}} \overset{(60)}{=} f(x) \cdot e^{\varepsilon \mathrm{Lie}(f)(X)} \cdot f(x)^{-1},$$

which agree because of (59).

10.22. On applying the functor Lie to Ad, we get a homomorphism of k-vector spaces $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$. For $x, y \in \mathfrak{g}$, define

$$[x, y] = \mathrm{ad}(x)(y). \tag{62}$$

This is the promised bracket. From (61), we obtain a commutative diagram

$$
\begin{array}{ccc}
\mathfrak{g} \times \mathfrak{g} & \xrightarrow{\ (x,X) \mapsto \mathrm{ad}(x)X\ } & \mathfrak{g} \\
{\scriptstyle \mathrm{Lie}(f) \times \mathrm{Lie}(f)} \downarrow & & \downarrow {\scriptstyle \mathrm{Lie}(f)} \\
\mathfrak{h} \times \mathfrak{h} & \xrightarrow{\ (y,Y) \mapsto \mathrm{ad}(y)Y\ } & \mathfrak{h}
\end{array}
$$

which shows that $\mathrm{Lie}(f)$ preserves the bracket.

THEOREM 10.23. *There is a unique functor* Lie *from the category of algebraic groups over k to the category of Lie algebras with the following properties:*

(a) $\mathrm{Lie}(G) = \mathrm{Hom}_{k\text{-}linear}(I_G/I_G^2, k)$ *as a k-vector space;*

(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* $\mathrm{ad}_{\mathfrak{g}}\colon \mathfrak{g} \to \mathrm{Der}(\mathfrak{g})$ *of $\mathfrak{g}$.*

PROOF. The uniqueness follows from the fact that every algebraic group admits a faithful representation $G \to \mathrm{GL}_n$ (see 4.9), which induces an injection $\mathfrak{g} \to \mathfrak{gl}_n$ (see 10.14). It remains to show that the bracket (62) has the property (b). An element $I + \varepsilon A \in L(\mathrm{GL}_n)$ acts on $M_n(k[\varepsilon])$ as

$$X + \varepsilon Y \mapsto (I + \varepsilon A)(X + \varepsilon Y)(I - \varepsilon A) = X + \varepsilon Y + \varepsilon(AX - XA). \tag{63}$$

On taking V to be $M_n(k)$ in (10.18), and comparing (63) with (58), we see that $\mathrm{ad}(A)$ acts as $\mathrm{id} + \varepsilon u$ with $u(X) = AX - XA$, as required. This completes the proof of the first statement.

The second statement is immediate from our definition of the bracket. $\quad\square$

REMARK 10.24. We saw in 10.19 and 10.20 that $\mathfrak{gl}_n(R) \simeq M_n(R)$ and that

$$\mathrm{Ad}(A)(X) = AXA^{-1}, \quad A \in \mathrm{GL}_n(R), \quad X \in \mathfrak{gl}_n(R).$$

Let G be an algebraic subgroup of GL_n. Then $\mathfrak{g} \subset \mathfrak{gl}_n$, and the adjoint map on GL_n restricts to the adjoint map on G (see 10.21). This gives an explicit description of the adjoint map on G.

REMARK 10.25. Even in characteristic zero, infinitely many nonisomorphic connected algebraic groups can have the same Lie algebra. For example, for each integer $n > 0$, 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 $\mathbb{G}_a$. No two G_n are isomorphic, but their Lie algebras equal the two-dimensional Lie algebra $\langle x, y \mid [x, y] = y \rangle$.

EXAMPLE 10.26. Let G be the orthogonal group $R \rightsquigarrow \{X \in M_n(R) \mid X^t \cdot X = I_n\}$ over k, and assume that $\mathrm{char}(k) \neq 2$. The Lie algebra of G is

$$\mathfrak{g} = \{I_n + \varepsilon Y \in M_n(k) \mid Y^t + Y = 0\},$$

which can be identified with the set of skew-symmetric matrices. We saw in Exercise 2-9 that the map $X \mapsto (I_n - X)(I_n + X)^{-1}$ defines a birational map $\lambda: G \dashrightarrow \mathfrak{g}$. This map is equivariant for the action of G on G by conjugation and the adjoint action of G on $\mathfrak{g}$, i.e.,

$$\lambda(gXg^{-1}) = \mathrm{Ad}(g)(\lambda(X))$$

for all g and X such that both sides are defined.[1]

e.   Description of the Lie algebra in terms of derivations

DEFINITION 10.27. Let A be an algebra over k and M an A-module. A k-linear map $D: A \to M$ is a *k-derivation* of A into M if

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad \text{(Leibniz rule)}.$$

For example, $D(1) = D(1 \times 1) = D(1) + D(1)$, and so $D(1) = 0$. By linearity, this implies that
$$D(c) = 0 \text{ for all } c \in k.$$

Conversely, every additive map $A \to M$ zero on k and satisfying the Leibniz rule is a k-derivation.

---

[1]Let G be a connected group variety with Lie algebra $\mathfrak{g}$ over a field k of characteristic zero. A rational map $\lambda: G \dashrightarrow \mathfrak{g}$ is called a *Cayley map* if it is birational and G-equivariant. The Cayley map for the orthogonal group (as above) was found by Cayley (1846). It is known that Cayley maps exist for SL_2, SL_3, SO_n, Sp_n, and PGL_n, and that they do not exist for SL_n, $n \geq 4$, or G_2. See Lemire et al. 2006. The Cayley map, when it exists, gives an explicit realization of the group as a rational variety.

Let $u: A \to k[\varepsilon]$ be a k-linear map, and write

$$u(f) = u_0(f) + \varepsilon u_1(f).$$

Then

$$u(fg) = u(f)u(g) \iff \begin{cases} u_0(fg) = u_0(f)u_0(g) \\ u_1(fg) = u_0(f)u_1(g) + u_0(g)u_1(f). \end{cases}$$

The first condition says that u_0 is a homomorphism $A \to k$ and, when we use u_0 to make k into an A-module, the second condition says that u_1 is a k-derivation $A \to k$.

Recall that $\mathcal{O}(G)$ has a coalgebra structure (Δ, ϵ). By definition, the elements of $L(G)$ are the k-algebra homomorphisms $u: \mathcal{O}(G) \to k[\varepsilon]$ whose composite with $\varepsilon \mapsto 0: k[\varepsilon] \to k$ is ϵ, i.e., such that $u_0 = \epsilon$. Thus, we have proved the following statement.

PROPOSITION 10.28. *Let $\mathcal{O}(G)$ act on k through ϵ. There is a natural one-to-one correspondence between the elements of $L(G)$ and the k-derivations $\mathcal{O}(G) \to k$, i.e.,*

$$L(G) \simeq \mathrm{Der}_{k,\epsilon}(\mathcal{O}(G), k).$$

The correspondence is $\epsilon + \varepsilon D \leftrightarrow D$, and the Leibniz condition is

$$D(fg) = \epsilon(f) \cdot D(g) + \epsilon(g) \cdot D(f).$$

Let $A = \mathcal{O}(G)$, and consider the space $\mathrm{Der}_k(A, A)$ of k-derivations of A into A. As noted (10.4), $\mathrm{Der}_k(A, A)$ becomes a Lie algebra with the bracket

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

A derivation $D: A \to A$ is **left invariant** if

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

If D and D' are left invariant, then

$$\begin{aligned} \Delta \circ [D, D'] &= \Delta \circ (D \circ D' - D' \circ D) \\ &= (\mathrm{id} \otimes D) \circ \Delta \circ D' - (\mathrm{id} \otimes D') \circ \Delta \circ D \\ &= (\mathrm{id} \otimes (D \circ D')) \circ \Delta - (\mathrm{id} \otimes (D' \circ D)) \circ \Delta \\ &= (\mathrm{id} \otimes [D, D']) \circ \Delta \end{aligned}$$

and so $[D, D']$ is also left invariant.

PROPOSITION 10.29. *The map*

$$D \mapsto \epsilon \circ D: \mathrm{Der}_k(A, A) \to \mathrm{Der}_{k,\epsilon}(A, k)$$

defines an isomorphism from the subspace of $\mathrm{Der}_k(A, A)$ consisting of left invariant derivations onto $\mathrm{Der}_{k,\epsilon}(A, k)$.

PROOF. If D is a left invariant derivation $A \to A$, then

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

and so D is determined by $\epsilon \circ D$. Conversely, if $d \colon A \to k$ is a derivation, the $D = (\mathrm{id} \otimes d) \circ \Delta$ is a left invariant derivation $A \to A$.   □

Thus $L(G)$ is isomorphic (as a k-vector space) to the space of left invariant derivations $A \to A$, which is a Lie subalgebra of $\mathrm{Der}_k(A, A)$. In this way, $L(G)$ acquires a Lie algebra structure, which is clearly natural in G. We leave it as an exercise to the reader to check that this agrees with the previously defined Lie algebra structure for $G = \mathrm{GL}_n$, and hence for all G.

f.   Stabilizers

Let (V, r) be a representation of an algebraic group G and W a subspace of V. Recall (4.3) that the stabilizer $G_W = \mathrm{Stab}_G(W)$ of W is the algebraic subgroup of G such that

$$G_W(R) = \{\alpha \in G(R) \mid \alpha(W_R) = W_R\}$$

for all k-algebras R.

DEFINITION 10.30. Let $\mathfrak{g} \to \mathfrak{gl}(V)$ be a representation of the Lie algebra $\mathfrak{g}$ and W a subspace of V. The **stabilizer** of W in $\mathfrak{g}$ is

$$\mathrm{Stab}_{\mathfrak{g}}(W) = \{x \in \mathfrak{g} \mid xW \subset W\}.$$

On applying the functor Lie to a representation $r \colon G \to \mathrm{GL}_V$ of G, we obtain a representation $dr \colon \mathfrak{g} \to \mathfrak{gl}_V$ of $\mathfrak{g}$ (see 10.31).

PROPOSITION 10.31. *Let (V, r) be a representation of G and W a subspace of V. Then*

$$\mathrm{Lie}(\mathrm{Stab}_G(W)) = \mathrm{Stab}_{\mathfrak{g}}(W).$$

PROOF. It suffices to prove this with $G = \mathrm{GL}_V$. Let $\alpha \in \mathfrak{gl}_V$. Then

$$\mathrm{id} + \alpha\varepsilon \in L(G_W) \iff \mathrm{id} + \alpha\varepsilon \in G_W(k[\varepsilon]) \iff (\mathrm{id} + \alpha\varepsilon) W[\varepsilon] \subset W[\varepsilon].$$

But

$$(\mathrm{id} + \alpha\varepsilon)(w_0 + w_1\varepsilon) = w_0 + (w_1 + \alpha w_0)\varepsilon,$$

which lies in $W[\varepsilon]$ if and only if $\alpha w_0 \in W$. Thus $e^{\varepsilon\alpha} \in L(G_W)$ if and only if α stabilizes W.   □

Therefore, $\dim \mathrm{Stab}_G(W)) \leq \dim \mathrm{Stab}_{\mathfrak{g}}(W)$, and equality holds if and only if $\mathrm{Stab}_G(W)$ is smooth.

EXAMPLE 10.32. In the situation of Chevalley's theorem (4.27), the group $H = \mathrm{Stab}_G(L)$, and so $\mathfrak{h} = \mathrm{Stab}_{\mathfrak{g}}(L)$.

g. Centres

The *centre* $z(\mathfrak{g})$ of a Lie algebra is the kernel of the adjoint map:

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

PROPOSITION 10.33. *Let G be a smooth connected algebraic group. Then*

$$\dim z(\mathfrak{g}) \geq \dim Z(G).$$

If equality holds, then $Z(G)$ is smooth and $\mathrm{Lie}(Z(G)) = z(\mathfrak{g})$.

PROOF. There are maps

$$\mathrm{Ad}: G \to \mathrm{Aut}(\mathfrak{g}), \quad \mathrm{Ker}(\mathrm{Ad}) \supset Z(G) \tag{64}$$
$$\mathrm{ad}: \mathfrak{g} \to \mathrm{Der}(\mathfrak{g}), \quad \mathrm{Ker}(\mathrm{ad}) = z(\mathfrak{g}). \tag{65}$$

The second map is obtained by applying Lie to the first (see 10.23), and so (see 10.14) $\mathrm{Ker}(\mathrm{ad}) = \mathrm{Lie}(\mathrm{Ker}(\mathrm{Ad})) \supset \mathrm{Lie}(Z(G))$. Therefore

$$\dim z(\mathfrak{g}) = \dim \mathrm{Ker}(\mathrm{ad}) = \dim \mathrm{Lie}(\mathrm{Ker}(\mathrm{Ad})) \overset{(1.37)}{\geq} \dim \mathrm{Ker}(\mathrm{Ad}) \overset{(64)}{\geq} \dim Z(G), \tag{66}$$

which proves the first part of the statement.

If $\dim z(\mathfrak{g}) = \dim Z(G)$, then equality holds throughout, and so

$$\dim \mathrm{Lie}(\mathrm{Ker}(\mathrm{Ad})) = \dim \mathrm{Ker}(\mathrm{Ad}) = \dim Z(G).$$

The first equality implies that $\mathrm{Ker}\,\mathrm{Ad}$ is smooth (1.37), and the second equality then implies that $Z(G)^\circ = (\mathrm{Ker}\,\mathrm{Ad})^\circ$. Hence $Z(G)^\circ$ is smooth, which implies that $Z(G)$ is smooth. Finally, $\mathrm{Lie}(Z(G)) \subset z(\mathfrak{g})$, and so they are equal if they have the same dimension. □

h. Centralizers

PROPOSITION 10.34. *Let G be an algebraic group and H an algebraic subgroup of G. The action of H on G by conjugation defines an action of H on $\mathrm{Lie}(G)$, and*

$$\mathrm{Lie}(C_G(H)) = \mathrm{Lie}(G)^H$$
$$\mathrm{Lie}(N_G(H))/\mathrm{Lie}(H) = (\mathrm{Lie}(G)/\mathrm{Lie}(H))^H.$$

PROOF. We prove the first statement. Let $C = C_G(H)$ and $\mathfrak{c} = \mathrm{Lie}(C)$. Clearly,

$$\mathfrak{c} = \{X \in \mathfrak{g} \mid e^{\varepsilon X} \in C(k[\varepsilon])\}.$$

Let $X \in \mathfrak{g}$. The condition that $X \in \mathfrak{c}$ is that

$$x \cdot (e^{\varepsilon X})_S \cdot x^{-1} = (e^{\varepsilon X})_S \text{ for all } k[\varepsilon]\text{-algebras } S \text{ and } x \in H(S), \tag{67}$$

where $(e^{\varepsilon X})_S$ is the image of $e^{\varepsilon X}$ in $C(S)$. On the other hand, the condition that $X \in \mathfrak{g}^H$ is that

$$y \cdot e^{\varepsilon' X_R} \cdot y^{-1} = e^{\varepsilon' X_R} \text{ for all } k\text{-algebras } R \text{ and } y \in H(R), \qquad (68)$$

where X_R is the image of X in $\mathfrak{g} \otimes R$.

We show that (67) $\implies$ (68). Let $y \in H(R)$ for some k-algebra R. Take $S = R[\varepsilon]$. Then $y \in H(R) \subset H(S)$, and (67) for $y \in H(S)$ implies (68) for $y \in H(R)$.

We show that (68) $\implies$ (67). Let $x \in H(S)$ for some $k[\varepsilon]$-algebra S; there is a $k[\varepsilon]$-homomorphism $\varphi \colon S[\varepsilon'] \to S$ acting as the identity on S and sending ε' to $\varepsilon 1_S$. On taking $R = S$ in (68), and applying φ, we obtain (67).

The proof of the second statement uses similar arguments (SHS, Exposé 4, 3.4).   □

Therefore, $\dim C_G(H) \leq \dim \mathfrak{g}^H$, and equality holds if and only if $C_G(H)$ is smooth.

i. An example of Chevalley

The following example of Chevalley shows that the Lie algebra of a noncommutative algebraic group may be commutative. It also shows that the centre of a smooth algebraic group need not be smooth, and the homomorphism $\mathrm{Ad} \colon G \to \mathrm{GL}_\mathfrak{g}$ need not be smooth.

10.35. Let k be an algebraically closed field of characteristic $p \neq 0$, and let G be the algebraic group over k such that $G(R)$ consists of the matrices

$$A(a,b) = \begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix}, \quad a,b \in R, \quad a \in R^\times.$$

Define regular functions on G by

$$X \colon A(a,b) \mapsto a$$
$$Y \colon A(a,b) \mapsto b.$$

Then $\mathcal{O}(G) = k[X,Y,X^{-1}]$, which is an integral domain, and so G is connected and smooth. Note that

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a' & 0 & 0 \\ 0 & a'^p & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a' & 0 & 0 \\ 0 & a'^p & b - a'^p b + a^p b' \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore G is not commutative, and its centre consists of the elements $A(a,b)$ with $a^p = 1$ and $b = 0$. It follows that

$$\mathcal{O}(Z(G)) = \mathcal{O}(G)/(X^p - 1, Y) \simeq k[X]/(X^p - 1),$$

which is not reduced; in fact, $Z(G) = \mu_p$.

On the other hand,

$$L(G) = \left\{ \begin{pmatrix} 1+a\varepsilon & 0 & 0 \\ 0 & 1 & b\varepsilon \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a,b \in k \right\} \subset L(\mathrm{GL}_3),$$

and so

$$\mathrm{Lie}(G) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \,\middle|\, a,b \in k \right\} \subset \mathfrak{gl}_3 = M_3(k),$$

which is obviously commutative. Moreover,

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1+a'\varepsilon & 0 & 0 \\ 0 & 1 & b'\varepsilon \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1+a'\varepsilon & 0 & 0 \\ 0 & 1 & a^p b'\varepsilon \\ 0 & 0 & 1 \end{pmatrix},$$

and so the kernel of $\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$ consists of the elements $A(a,b)$ with $a^p = 1$. Thus

$$\mathrm{Ker}(\mathrm{Ad}) = \mathrm{Spm}\left(\mathcal{O}(G)/(X^p - 1)\right) = \mathrm{Spm}(k[X,Y]/(X^p - 1)),$$

which is not reduced, and so Ad is not smooth. Note that,

$$\dim \mathfrak{z}(\mathfrak{g}) = 2 > \dim(\mathrm{Ker}(\mathrm{Ad})) = 1 > \dim(Z(G)) = 0,$$

and so all of the inequalities in (66) are strict.

j. The universal enveloping algebra

Recall (10.3) that an associative algebra A over k 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, $(U(\mathfrak{g}), \mathfrak{g} \xrightarrow{\rho} [U(\mathfrak{g})])$, that is universal:

$$\left\{ \begin{array}{c} \mathrm{Hom}(\mathfrak{g}, [A]) \simeq \mathrm{Hom}(U(\mathfrak{g}), A). \\ \alpha \circ \rho \leftrightarrow \alpha \end{array} \right.$$

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

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

$$T(V) = k \oplus V \oplus V^{\otimes 2} \oplus V^{\otimes 3} \oplus \cdots, \quad V^{\otimes n} = V \otimes \cdots \otimes V \quad (n \text{ copies}),$$

with the algebra structure defined by juxtaposition:

$$(x_1 \otimes \cdots \otimes x_m) \cdot (y_1 \otimes \cdots \otimes y_n) = x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n.$$

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

$$x \otimes y - y \otimes x - [x, y], \quad x, y \in \mathfrak{g}. \tag{69}$$

The composite $\mathfrak{g} \to T(\mathfrak{g}) \to U(\mathfrak{g})$ is then a Lie algebra homomorphism $\mathfrak{g} \to [U(\mathfrak{g})]$, and the extension of a k-linear map $\alpha\colon \mathfrak{g} \to A$ to $T(\mathfrak{g}) \to A$ factors through $U(\mathfrak{g})$ if and only if α is a Lie algebra homomorphism $\mathfrak{g} \to [A]$. Therefore $U(\mathfrak{g})$ and the map $\mathfrak{g} \to [U(\mathfrak{g})]$ have the required universal property.

When $\mathfrak{g}$ is commutative, (69) becomes $x \otimes y - y \otimes x$, and so $U(\mathfrak{g})$ is the symmetric algebra on $\mathfrak{g}$; in particular, $U(\mathfrak{g})$ is commutative.

The choice of a basis $e_1, e_2, \ldots$ for the vector space $\mathfrak{g}$ realizes $T(\mathfrak{g})$ as the algebra over k of noncommuting polynomials in the e_i and $U(\mathfrak{g})$ as a quotient of this algebra. In particular, $U(\mathfrak{g})$ is finitely generated as an algebra over k if $\mathfrak{g}$ is finite-dimensional.

THEOREM 10.36 (POINCARÉ, BIRKHOFF, WITT). *Let $(e_i)_{i \in I}$ be an ordered[2] basis for $\mathfrak{g}$ as a k-vector space, and let $\varepsilon_i = \rho(e_i)$. Then the ordered monomials*

$$\varepsilon_{i_1} \varepsilon_{i_2} \cdots \varepsilon_{i_n}, \quad i_1 \leq i_2 \leq \cdots \leq i_n, \tag{70}$$

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

For example, if $\mathfrak{g}$ is finite-dimensional with basis $\{e_1, \ldots, e_r\}$ as a k-vector space, then the monomials

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

form a basis for $U(\mathfrak{g})$ as a k-vector space. If $\mathfrak{g}$ is commutative, then $U(\mathfrak{g})$ is the polynomial algebra in the symbols $\varepsilon_1, \ldots, \varepsilon_r$.

The family $(\varepsilon_i)_{i \in I}$ generates $U(\mathfrak{g})$ as an algebra over k, and so the monomials $\varepsilon_{i_1} \varepsilon_{i_2} \cdots \varepsilon_{i_m}$, $m \in \mathbb{N}$, generate $U(\mathfrak{g})$ as a k-vector space. The relations implied by (69),

$$xy = yx + [x, y],$$

allow us to "reorder" the factors in such a monomial, and deduce that the ordered monomials (70) span $U(\mathfrak{g})$. The import of the theorem is that the set of ordered monomials is linearly independent. The proof of this makes use of the Jacobi identity.

---

[2]By ordered we mean totally ordered.

Proof of the PBW theorem

Choose a basis $\mathcal{B}$ for $\mathfrak{g}$ as a k-vector space and a total ordering of $\mathcal{B}$. The monomials

$$x_1 \otimes x_2 \otimes \cdots \otimes x_m, \quad x_i \in \mathcal{B}, \quad m \in \mathbb{N},$$

form a basis for $T(\mathfrak{g})$ as a k-vector space. We say that such a monomial is **ordered** if $x_1 \leq x_2 \leq \cdots \leq x_m$. We have to show that the images of the ordered monomials in $U(\mathfrak{g})$ form a basis for $U(\mathfrak{g})$ regarded as a k-vector space.

From now on "monomial" means a monomial $S = x_1 \otimes \cdots \otimes x_m$ with the $x_i \in \mathcal{B}$. The **degree** of S is m. An **inversion** in S is a pair (i, j) with $i < j$ but $x_i > x_j$. We say that a monomial "occurs" in a tensor if it occurs with nonzero coefficient.

By definition, $U(\mathfrak{g})$ is the quotient of $T(\mathfrak{g})$ by the two-sided ideal $I(\mathfrak{g})$ generated by the elements (69). As a k-vector space, $I(\mathfrak{g})$ is spanned by elements

$$A \otimes x \otimes y \otimes B - A \otimes y \otimes x \otimes B - A \otimes [x, y] \otimes B$$

with $x, y \in \mathcal{B}$ and A, B monomials. In fact, because $[x, y] = -[y, x]$, the elements of this form with $x < y$ already span $I(\mathfrak{g})$.

Let $T \in T(\mathfrak{g})$. We say that T is **reduced** if all the monomials occurring in it are ordered. We define a partial ordering on the elements of $T(\mathfrak{g})$ by requiring that $T < T'$ if

(a) the greatest degree of an unordered monomial occurring in T is less than the similar number for T', or

(b) both T and T' contain unordered monomials of the same largest degree n, but the total number of inversions in monomials of degree n occurring in T is less than the similar number for T'.

For example, if $x < y < z$, then

$$y \otimes x + z \otimes x + z \otimes y < y \otimes x \otimes z + x \otimes z \otimes y < z \otimes y \otimes x.$$

The ordering measures how nonreduced a tensor is.

For $r, s \geq 0$, we define a k-linear map $\sigma_{r,s} \colon T(\mathfrak{g}) \to T(\mathfrak{g})$ by requiring that $\sigma_{r,s}$ fix all monomials except those of the form

$$A \otimes x \otimes y \otimes B, \quad \deg(A) = r, \quad \deg(B) = s, \quad x > y,$$

and that it maps this monomial to

$$A \otimes y \otimes x \otimes B + A \otimes [x, y] \otimes B.$$

Note that $\sigma_{r,s}$ fixes all reduced tensors.

Let $T, T' \in T(\mathfrak{g})$. We write $T \to T'$ if T' is obtained from T by a single map $\sigma_{r,s}$, and $T \xrightarrow{\;*\;} T'$ if T' is obtained from T by zero or more such maps. In the first case, we call T' a **simple reduction** of T, and in the second case, a **reduction** of T. Note that if $T \xrightarrow{\;*\;} T'$ and T is reduced, then $T = T'$.

After these preliminaries, we are ready to prove the theorem.

STEP 1. *Let $T \in T(\mathfrak{g})$. Then $\sigma_{r,s}(T) - T \in I(\mathfrak{g})$ and $\sigma_{r,s}(T) \leq T$ for all $r, s \in \mathbb{N}$; moreover, $T < \sigma_{r,s}(T)$ for some r, s unless T is reduced.*

PROOF. The first part of the assertion is obvious from the definitions. Let T be nonreduced and S a nonreduced monomial of highest degree occurring in T. Then $\sigma_{r,s}(S) < S$ for some $r, s \in \mathbb{N}$. As $\sigma_{r,s}(S') \leq S'$ for all monomials $S' \neq S$ occurring in T, we have $\sigma_{r,s}(T) < T$.   □

STEP 2. *Let $T \in T(\mathfrak{g})$. Then there exists a reduction $T \xrightarrow{*} T'$ with T' reduced. Therefore the images of the ordered monomials span $U(\mathfrak{g})$.*

PROOF. Let $T \in T(\mathfrak{g})$. According to Step 1, there exists a sequence of simple reductions $T \to T_1 \to T_2 \to \cdots$ with $T > T_1 > T_2 > \cdots$. Clearly, the sequence stops with a reduced tensor T' after a finite number of steps. Moreover, $T \equiv T_1 \equiv T_2 \equiv \cdots \equiv T'$ modulo $I(\mathfrak{g})$, and so T' represents the image of T in $U(\mathfrak{g})$.□

STEP 3. *No nonzero element of $I(\mathfrak{g})$ is reduced.*

PROOF. The elements

$$x \otimes y - y \otimes x - [x, y], \quad x, y \in \mathcal{B}, \quad x > y$$

of $T(\mathfrak{g})$ are linearly independent over k. Let T be a nonzero element of $I(\mathfrak{g})$. Then T is a linear combination of distinct terms

$$A \otimes x \otimes y \otimes B - A \otimes y \otimes x \otimes B - A \otimes [x, y] \otimes B,$$

with $x, y \in \mathcal{B}$, $x > y$, and A, B monomials. By considering the terms with $\deg(A)$ a maximum, one sees that T cannot be reduced.   □

STEP 4. *(PBW confluence) Let $A \xrightarrow{*} B_1$ and $A \xrightarrow{*} B_2$ be reductions of a monomial A. Then there exist reductions $B_1 \xrightarrow{*} C_1$ and $B_2 \xrightarrow{*} C_2$ with $C_1 - C_2 \in I(\mathfrak{g})$.*

PROOF. First suppose that the reductions $A \xrightarrow{*} B_1$ and $A \xrightarrow{*} B_2$ are simple. If the pairs $x \otimes y$ and $x' \otimes y'$ involved in the reductions to B_1 and B_2 don't overlap, the statement is obvious, because

$$\sigma_{r,s} \circ \sigma_{r',s'} = \sigma_{r',s'} \circ \sigma_{r,s}$$

if $r' \neq r - 1, r + 1$. Otherwise, A has the form

$$A = A' \otimes x \otimes y \otimes z \otimes B', \quad x > y > z,$$

and the reductions $A \to B_1$ and $A \to B_2$ have the form

$$x \otimes \underline{y \otimes z} \to y \otimes x \otimes z + [x, y] \otimes z$$
$$x \otimes \underline{y \otimes z} \to x \otimes z \otimes y + x \otimes [y, z].$$

But,

$$y \otimes \underline{x \otimes z} + [x, y] \otimes z \rightarrow \underline{y \otimes z} \otimes x + y \otimes [x, z] + [x, y] \otimes z$$
$$\rightarrow z \otimes y \otimes x + [y, z] \otimes x + y \otimes [x, z] + [x, y] \otimes z$$

and

$$\underline{x \otimes z} \otimes y + x \otimes [y, z] \rightarrow z \otimes \underline{x \otimes y} + [x, z] \otimes y + x \otimes [y, z]$$
$$\rightarrow z \otimes y \otimes x + z \otimes [x, y] + [x, z] \otimes y + x \otimes [y, z].$$

The terms on the right differ by

$$[[y, z], x] + [y, [x, z]] + [[x, y], z],$$

which, because of the Jacobi identity (10.1b), lies in $I(\mathfrak{g})$.

Next suppose only that $A \xrightarrow{*} B_1$ is simple. This case can be proved by repeatedly applying the simple case:
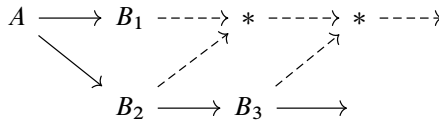
The deduction of the general case is similar. □

Let $T \in T(\mathfrak{g})$. In Step 2 we showed that there exists a reduction $T \xrightarrow{*} T'$ with T' reduced. If T' is unique, then we say that T is **uniquely reducible**, and we set $\mathrm{red}(T) = T'$.

STEP 5. *Every monomial A is uniquely reducible.*

PROOF. Suppose $A \xrightarrow{*} B_1$ and $A \xrightarrow{*} B_2$ with B_1 and B_2 reduced. According to Step 4, $B_1 - B_2 \in I(\mathfrak{g})$, and hence is zero (Step 3). □

STEP 6. *If S and T are uniquely reducible, so also is $S + T$, and $\mathrm{red}(S + T) = \mathrm{red}(S) + \mathrm{red}(T)$.*

PROOF. Let $W = \sigma(S + T)$ be a reduced reduction of $S + T$. It suffices to show that

$$W = \mathrm{red}(S) + \mathrm{red}(T).$$

There exists a reduction σ' such that $\sigma'(\sigma(S)) = \mathrm{red}(S)$. Now

$$\sigma'(\sigma(S + T)) = \sigma'(W) = W$$

because W is reduced, and

$$\sigma'(\sigma(S + T)) = \sigma'(\sigma(S)) + \sigma'(\sigma(T)) = \mathrm{red}(S) + (\sigma'\sigma)(T).$$

Let σ'' be such that $\sigma''(\sigma'\sigma)(T) = \mathrm{red}(T)$. Then

$$W = \sigma''(W) = \sigma''(\mathrm{red}(S)) + \sigma''(\sigma'\sigma(T)) = \mathrm{red}(S) + \mathrm{red}(T). \qquad \square$$

An induction argument now shows that every T in $T(\mathfrak{g})$ is uniquely reducible.

STEP 7. *The map $T \mapsto \mathrm{red}(T): T(\mathfrak{g}) \to T(\mathfrak{g})$ is k-linear and has the following properties:*

(a) $T - \mathrm{red}(T) \in I(\mathfrak{g})$;

(b) $\mathrm{red}(T) = T$ *if T is reduced;*

(c) $\mathrm{red}(T) = 0$ *if $T \in I(\mathfrak{g})$.*

PROOF. The map is additive by definition, and it obviously commutes with multiplication by elements of k; hence it is k-linear. Both (a) and (b) follow from the fact that $\mathrm{red}(T)$ is a reduction of T (see Step 1). For (c), if $T \in I(\mathfrak{g})$ then $\mathrm{red}(T)$ is reduced and lies in $I(\mathfrak{g})$, and so is zero (Step 3).   □

STEP 8. *Completion of the proof.*

PROOF. Let $T(\mathfrak{g})(\mathrm{red})$ denote the k-subspace of $T(\mathfrak{g})$ consisting of reduced tensors. The map red is a k-linear projection onto $T(\mathfrak{g})(\mathrm{red})$ with kernel $I(\mathfrak{g})$:

$$T(\mathfrak{g}) \simeq I(\mathfrak{g}) \oplus T(\mathfrak{g})(\mathrm{red}) \quad \text{(as k-vector spaces)}.$$

Thus, $T(\mathfrak{g})/I(\mathfrak{g}) \simeq T(\mathfrak{g})(\mathrm{red})$ as required.   □

REMARK 10.37. The proof shows that the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$ can be identified with the k-vector subspace $T(\mathfrak{g})_{\mathrm{red}}$ equipped with the multiplication
$$T \cdot T' = \mathrm{red}(T \otimes T').$$

NOTES. The above proof of the PBW theorem follows notes of Casselman (*Introduction to Lie Algebras*) and Bergman 1978. The latter writes

> [This proof] is quite close to Birkhoff's original proof ... Birkhoff 1937. Witt's proof looks rather different. He considers a certain action of the permutation group S_n upon the space spanned by monomials of degree $\leq n$. The Jacobi identity turns out to correspond to the defining relations $((i, i+1)(i+1, i+2))^3 = 1$ in a presentation of S_n in terms of generators $(i, i+1)$. Poincaré's 1899 proof is more or less by "brute force", and appears to have a serious gap, but it is a surprisingly early example of the idea of constructing a ring as the [quotient] algebra of a free associative algebra by (in effect) the ideal generated by a system of relations.

k. The universal enveloping p-algebra

In this section, k has characteristic $p \neq 0$. Let x_0 and x_1 be elements of a Lie algebra $\mathfrak{g}$ over k. For $0 < r < p$, let

$$s_r(x_0, x_1) = -\frac{1}{r} \sum_u \mathrm{ad}x_{u(1)} \mathrm{ad}x_{u(2)} \cdots \mathrm{ad}x_{u(p-1)}(x_1)$$

where u runs over the maps $\{1, 2, \ldots, p-1\} \to \{0, 1\}$ taking r times the value 0. For example, $s_1(a,b)$ equals $[a,b]$ if $p = 2$, and $s_1(a,b) = [[a,b],b]$ and $2s_2(a,b) = [[a,b],a]$ if $p = 3$.

PROPOSITION 10.38. *Let A be an associative algebra over k (not necessarily commutative). For $a, b \in A$, write*

$$\mathrm{ad}(a)b = [a,b] = ab - ba.$$

Then the Jacobson formulas hold for $a, b \in A$:

(a) $\mathrm{ad}(a)^p = \mathrm{ad}(a^p)$

(b) $(a+b)^p = a^p + b^p + \displaystyle\sum_{0 < r < p} s_r(a,b)$.

PROOF. When we put $L_a(b) = ab = R_b(a)$, we find that

$$\mathrm{ad}(a^p)(b) = (L_a^p - R_a^p)(b) = (L_a - R_a)^p(b) = \mathrm{ad}(a)^p(b),$$

which proves (a).

Let S_p denote the symmetric group on p symbols. We claim that, for $a_1, \ldots, a_p \in A$,

$$\sum_{s \in S_p} a_{s(1)} \cdots a_{s(p)} = \sum_{t \in S_{p-1}} \mathrm{ad}(a_{t(1)}) \cdots \mathrm{ad}(a_{t(p-1)})(a_p). \tag{71}$$

The right-hand side equals

$$\sum_{i,j} \sum_{t \in S_{p-1}} (-1)^{p-1-r} a_{t(i_1)} \cdots a_{t(i_r)} a_p a_{t(j_{p-1-r})} \cdots a_{t(j_1)},$$

where $i = (i_1, \ldots, i_r)$ runs over the strictly increasing sequences of integers in $\{1, \ldots, p-1\}$ and where $j = (j_1, \ldots, j_{p-1-r})$ denotes the strictly increasing sequence whose values are the integers in $\{1, \ldots, p-1\}$ distinct from $i_1, \ldots, i_r$. This sum equals

$$\sum_r (-1)^{p-1-r} \binom{p-1}{p-1-r} \sum_{v \in S_{p-1}} a_{v(1)} \cdots a_{v(r)} a_p a_{v(r+1)} \cdots a_{v(p-1)}.$$

But the identity

$$(T-1)^{p-1} = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \cdots + 1$$

in $k[T]$ shows that

$$(-1)^{p-1-r} \binom{p-1}{p-1-r} = 1,$$

which proves (71).

We now prove (b). If $x_0, x_1 \in A$, then

$$(x_0 + x_1)^p = x_0^p + x_1^p + \sum_{0 < r < p} \sum_{w \in F(r)} x_{w(1)} \cdots x_{w(p)},$$

where $F(r)$ is the set of maps from $\{1, \ldots, p\}$ to $\{0, 1\}$ taking r times the value 0. For $s \in S_p$, let $w_s \in F(r)$ denote the map such that

$$w_s^{-1}(0) = \{s^{-1}(1), \ldots, s^{-1}(r)\}.$$

Then $s \mapsto w_s$ is a surjective map such that the inverse image of each $w \in F(r)$ contains $r!(p-r)!$ elements. Putting

$$a_1 = \cdots = a_r = x_0$$
$$a_{r+1} = \cdots = a_p = x_1$$

we therefore have

$$x_{w_s(1)} \cdots x_{w_s(p)} = a_{s(1)} \cdots a_{s(p)}$$

and

$$\sum_{w \in F(r)} x_{w(1)} \cdots x_{w(p)} = \frac{1}{r!(p-r)!} \sum_{s \in S_p} a_{s(1)} \cdots a_{s(p)}.$$

Similarly, we may prove that

$$s_r(x_0, x_1) = \left(-\frac{1}{r}\right) \frac{1}{r!(p-r-1)!} \sum_{t \in S_{p-1}} \mathrm{ad}(a_{t(1)}) \cdots \mathrm{ad}(a_{t(p-1)})(a_p).$$

The required formula now follows from (71). □

DEFINITION 10.39. A *p-Lie algebra* is a Lie algebra $\mathfrak{g}$ equipped with a map

$$x \mapsto x^{[p]} : \mathfrak{g} \to \mathfrak{g}$$

such that
  (a) $(cx)^{[p]} = c^p x^{[p]}$, all $c \in k$, $x \in \mathfrak{g}$;
  (b) $\mathrm{ad}(x^{[p]}) = (\mathrm{ad}(x))^p$, all $x \in \mathfrak{g}$;
  (c) $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{0 < r < p-1} s_r(x, y)$, all $x, y \in \mathfrak{g}$.

Note that Proposition 10.38 says that $[A]$ becomes a p-Lie algebra when we set $a^{[p]} = a^p$.

Let $\mathfrak{g}$ be a p-Lie algebra and $\rho: \mathfrak{g} \to U(\mathfrak{g})$ the universal map. The elements $\rho(x)^{[p]} - \rho(x^{[p]})$ lie in the centre of $U(\mathfrak{g})$, and we define $U^{[p]}(\mathfrak{g})$ to be the quotient of $U(\mathfrak{g})$ by the ideal they generate. Regard $U^{[p]}(\mathfrak{g})$ as a p-Lie algebra, and let j denote the composite $\mathfrak{g} \to U(\mathfrak{g}) \to U^{[p]}(\mathfrak{g})$. Then j is a homomorphism of p-Lie algebras, and the pair $(U^{[p]}(\mathfrak{g}), j)$ is universal: every k-linear map

$\alpha: \mathfrak{g} \to A$ with A associative extends uniquely to a homomorphism $T(\mathfrak{g}) \to A$ of algebras over k, which factors through $U^{[p]}(\mathfrak{g})$ if and only if it is a p-Lie algebra homomorphism,

$$
\begin{cases} \operatorname{Hom}(\mathfrak{g}, [A]) \simeq \operatorname{Hom}(U^{[p]}(\mathfrak{g}), A). \\ \alpha \circ j \leftrightarrow \alpha \end{cases}
$$

The functor $\mathfrak{g} \rightsquigarrow U^{[p]}(\mathfrak{g})$ is left adjoint to the functor sending an associative algebra over k to its associated p-Lie algebra.

THEOREM 10.40. *Let $(e_i)_{i \in I}$ be an ordered basis for $\mathfrak{g}$ as a k-vector space, and let $\varepsilon_i = j(e_i)$. Then the set consisting of 1 and the monomials*

$$
\varepsilon_{i_1}^{n_{i_1}} \cdots \varepsilon_{i_r}^{n_{i_r}}, \quad i_1 < \cdots < i_r, \quad 0 < n_{i_j} < p
$$

forms a basis for $U^{[p]}(\mathfrak{g})$ as a k-vector space.

PROOF. Identify $\mathfrak{g}$ with its image in $U(\mathfrak{g})$, and let $c_i = e_i^p - e_i^{[p]}$. The c_i lie in the centre of $U(\mathfrak{g})$, and generate the kernel of the map $U(\mathfrak{g}) \to U^{[p]}(\mathfrak{g})$. Let U_{p-1} denote the subspace of $U(\mathfrak{g})$ generated by the monomials $\prod e_i^{m_i}$ with $\sum m_i \le p - 1$. As $c_i \equiv e_i^p$ modulo U_{p-1}, the PBW theorem (10.36) implies that the monomials

$$
\prod e_i^{n_i} \prod c_i^{m_i}, \quad 0 \le n_i < p, \quad m_i \ge 0
$$

form a basis for $U(\mathfrak{g})$, from which the statement follows. □

COROLLARY 10.41. *If $\mathfrak{g}$ is finite-dimensional as a k-vector space, so also is $U^{[p]}(\mathfrak{g})$, and the map $j: \mathfrak{g} \to U^{[p]}(\mathfrak{g})$ is injective.*

PROOF. Obvious from the theorem. □

NOTES. This section follows DG, II, §7, no. 3. See also Jacobson 1962, V.7.

l. The algebra of distributions (hyperalgebra) of an algebraic group

In characteristic zero, the Lie algebra of a connected algebraic group G captures much of the information of G. For example, the connected algebraic subgroups of G are in natural one-to-one correspondence with the Lie subalgebras of $\mathfrak{g}$, and, if G is semisimple and simply connected, then $\operatorname{Rep}(G) \simeq \operatorname{Rep}(\mathfrak{g})$ (see 23.70). To obtain similar statements in characteristic $p \ne 0$, it is necessary to replace the Lie algebra of G with its *algebra of distributions* $\operatorname{Dist}(G)$ (also called its *hyperalgebra*).

Let X be an affine scheme over k. Let $x \in X(k)$, and let $I_x \subset \mathcal{O}(X)$ be the ideal of functions zero at x. A ***distribution on X of order $\leq n$ with support on x*** is a k-linear map $\mu: \mathcal{O}(X) \to k$ such that $\mu(I_x^{n+1}) = 0$. These distributions form a k-vector space $\mathrm{Dist}_n(X, x)$. Clearly, $\mathrm{Dist}_0(X, x) \simeq k^\vee \simeq k$, and

$$\mathrm{Dist}_n(X, x) \simeq k \oplus (I_x/I_x^{n+1})^\vee, \quad n > 0.$$

In particular, $\mathrm{Dist}_1(X, x) \simeq k \oplus \mathrm{Tgt}_x(X)$. We let $\mathrm{Dist}(X, x)$ denote the k-vector space of all linear maps $\mu: \mathcal{O}(X) \to k$ such that $\mu(I_x^{n+1}) = 0$ for some $n \geq 0$. Thus $\mathrm{Dist}(X, x) = \bigcup_n \mathrm{Dist}_n(X, x)$.

For an algebraic group G over k, we write $\mathrm{Dist}(G)$ for $\mathrm{Dist}(G, e)$. When $\mu, \mu' \in \mathrm{Dist}(G)$, we define $\mu \cdot \mu'$ to be the composite

$$\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes \mathcal{O}(G) \xrightarrow{(\mu, \mu')} k.$$

In this way, $\mathrm{Dist}(G)$ becomes a filtered associative algebra over k whose associated graded algebra is commutative, and $\mathrm{Dist}_1(G) \simeq k \oplus \mathfrak{g}$. When k has characteristic zero, the natural inclusion $\mathfrak{g} \to \mathrm{Dist}(G)$ extends to an isomorphism $U(\mathfrak{g}) \to \mathrm{Dist}(G)$ of algebras over k (apply 11.27 below), and so $\mathrm{Dist}(G)$ contributes nothing new. When k has characteristic $p \neq 0$, the natural inclusion $\mathfrak{g} \to \mathrm{Dist}(G)$ extends to an injective homomorphism $U^{[p]}(\mathfrak{g}) \to \mathrm{Dist}(G)$, but this is not an isomorphism. The k-algebra $\mathrm{Dist}(G)$ acts on every finite-dimensional representation of G, and the resulting functor from G-modules to $\mathrm{Dist}(G)$-modules is fully faithful when k is perfect and G is connected, but it is not essentially surjective. Under the same hypotheses on G and k, a subspace of a representation of G is stable under G if and only if it is stable under $\mathrm{Dist}(G)$. See DG, II, §4, 5–6, and Jantzen 1997, I, Chapter 7.

Exercises

EXERCISE 10-1. A nonzero element c of k defines an endomorphism of $k[\varepsilon]$ sending ε to $c\varepsilon$, and hence an endomorphism of $L(G)$ for any algebraic group G. Show that this agrees with the action of c on $L(G)$ arising from the isomorphism $L(G) \simeq \mathrm{Hom}(I/I^2, k) = \mathrm{Lie}(G)$.

Finite Group Schemes

In this chapter we study finite group schemes, i.e., finite algebraic groups. They are automatically affine. A finite algebraic group is étale unless the base field has characteristic $p \neq 0$ and p divides the order of the group (11.31), and so this is largely a study of p-phenomena in characteristic p.

a. Generalities

PROPOSITION 11.1. *The following conditions on a finitely generated k-algebra A are equivalent: (a) A is artinian; (b) A has Krull dimension zero; (c) A is a finite k-algebra; (d) $\mathrm{spm}(A)$ is discrete (in which case it is finite).*

PROOF. (a)$\Leftrightarrow$(b). A noetherian ring is artinian if and only if it has dimension zero (CA 16.6).

(b)$\Rightarrow$(c). According to the Noether normalization theorem (CA 8.1), there exist algebraically independent elements $x_1, \ldots, x_r$ in A such that A is finite over $k[x_1, \ldots, x_r]$. As $k[x_1, \ldots, x_r]$ has Krull dimension r (CA 18.16) and $\dim k[x_1, \ldots, x_r] \leq \dim A$ (CA 7.7), we see that (b) implies that $r = 0$ and that A is finite over k.

(c)$\Rightarrow$(a). This is obvious.

(d)$\Rightarrow$(b). Let $\mathfrak{m}$ be a maximal ideal in A. As $\{\mathfrak{m}\}$ is open in $\mathrm{spm}(A)$, there exists an $f \in A$ such that $\mathrm{spm}(A_f) = \{\mathfrak{m}\}$. Now A_f is again a finitely generated k-algebra, and so every prime ideal in A_f is an intersection of maximal ideals (CA 13.11). But A_f has only one maximal ideal $\mathfrak{m}$, and so A_f has no prime ideals except $\mathfrak{m}$. It follows that no prime ideal of A is properly contained in $\mathfrak{m}$. As this is true of all maximal ideals in A, the ring A has dimension zero.

(a)$\Rightarrow$(d). Because A is artinian, it has only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, and some product, say, $\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r}$, equals 0 (CA §16). Now the Chinese remainder theorem (CA 2.13) shows that

$$A \simeq A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_r^{n_r}$$

and so $\mathrm{spm}(A) = \bigsqcup \mathrm{spm}(A/\mathfrak{m}_i^{n_i}) = \bigsqcup \{\mathfrak{m}_i\}$ (disjoint union of open one-point sets). Therefore, $\mathrm{spm}(A)$ is finite and discrete.   □

PROPOSITION 11.2. *The following conditions on an algebraic scheme X over k are equivalent: (a) X is affine and $\mathcal{O}(X)$ is a finite k-algebra; (b) X has dimension zero; (c) the morphism $X \to \mathrm{Spm}\, k$ is finite; (d) $|X|$ is discrete (in which case it is finite).*

PROOF. The implications (a)$\Rightarrow$(b)$\Rightarrow$(c)$\Rightarrow$(d) follow immediately from 11.1. It remains to prove (d)$\Rightarrow$(a). Assume that $|X|$ is discrete, and write X as a finite union of open affine subschemes, $X = \bigcup_i U_i$. Then U_i is discrete, and so $U_i = \mathrm{Spm}(A_i)$ with A_i artinian (11.1). It follows that $|X|$ is a finite union of open-closed one-point subsets u_j, and that $\mathcal{O}_X(u_j)$ is a local artinian ring A_j. Now $X = \bigsqcup_j \mathrm{Spm}(A_j)$, which is affine with coordinate ring the artinian ring $\prod A_j$.   □

An algebraic scheme over k is ***finite*** if it satisfies the equivalent conditions of 11.2, and an algebraic group over k is finite if it is finite as a scheme over k (2.14).

PROPOSITION 11.3. *Let G be a finite group scheme over k. If k is perfect, then the connected-étale exact sequence*

$$e \to G^\circ \to G \to \pi_0(G) \to e$$

splits and realizes G as a semidirect product $G^\circ \rtimes \pi_0(G)$.

PROOF. As $G^\circ(k^a) = e$, the sequence gives an isomorphism $G(k^a) \to \pi_0(G)(k^a)$ (see 5.48). If k is perfect, then G_{red} is an algebraic subgroup of G (1.39), and the map $G \to \pi_0(G)$ induces an isomorphism $G_{\mathrm{red}} \to \pi_0(G)$ because both groups are étale and the homomorphism becomes an isomorphism on k^a-points:

$$G_{\mathrm{red}}(k^a) = G(k^a) \xrightarrow{\simeq} \pi_0(G)(k^a).$$

Now Proposition 2.34 applied to the homomorphism $G \to \pi_0(G)$ shows that $G \simeq G^\circ \rtimes \pi_0(G)$.   □

The automorphism group of α_p is $\mathbb{G}_m$, and so there is a natural action of $\mathbb{Z}/n\mathbb{Z}$ on α_p if k contains a primitive nth root of 1. Therefore the semidirect product in the proposition need not be a direct product.

The following are examples of finite group schemes whose connected-étale exact sequence does not split.

EXAMPLE 11.4. Let k be a nonperfect field of characteristic p, and let $c \in k \smallsetminus k^p$. Let

$$G = \bigsqcup\nolimits_{i=0}^{p-1} G_i, \quad G_i = \mathrm{Spm}(k[T]/(T^p - c^i)).$$

For $a \in G_i(R)$ and $b \in G_j(R)$, define

$$ab = \begin{cases} ab \in G_{i+j}(R) & \text{if } i+j < p \\ ab/c \in G_{i+j-p}(R) & \text{if } i+j \geq p. \end{cases}$$

This makes $G(R)$ into a group, and G into a finite algebraic group. Its identity component is $G_0 = \mu_p$, and there is an exact sequence

$$0 \to \mu_p \to G \to (\mathbb{Z}/p\mathbb{Z})_k \to 0$$

such that the fibre over $i \in (\mathbb{Z}/p\mathbb{Z})_k$ is G_i. This is nonsplit because $G_i \simeq$ $\mathrm{Spm}(k[\sqrt[p]{c^i}])$ and $k[\sqrt[p]{c^i}]$ is a field $\neq k$ if i is not divisible by p.

EXAMPLE 11.5. Let k and c be as in 11.4. Let

$$G = \bigsqcup_{i=0}^{p-1} G_i, \quad G_i = \mathrm{Spm}(k[T]/(T^p - ic)).$$

For $a \in G_i(R)$ and $b \in G_j(R)$, define

$$ab = \begin{cases} a+b \in G_{i+j}(R) & \text{if } i+j < p \\ a+b \in G_{i+j-p}(R) & \text{if } i+j \geq p. \end{cases}$$

This makes $G(R)$ into a group, and G into a finite algebraic group. Its identity component is $G_0 = \alpha_p$, and there is a nonsplit exact sequence

$$0 \to \alpha_p \to G \to (\mathbb{Z}/p\mathbb{Z})_k \to 0.$$

b. Locally free finite group schemes over a base ring

The most important finite group schemes over a ring (or base scheme) are those that are locally free. We now review the definitions.

11.6. Let R_0 be a commutative ring and M an R_0-module. Then M is said to be locally free of finite rank if there exists a finite family $(f_i)_{i \in I}$ of elements of R_0 generating the unit ideal R_0 and such that, for all $i \in I$, the R_{0f_i}-module M_{f_i} is free of finite rank. This is equivalent to M being finitely presented and flat (CA 12.6). Therefore, when R_0 is noetherian, an R_0-module is locally free of finite rank if and only if it is finitely generated and flat.

An R_0-algebra is said to be locally free of finite rank if it is so as an R_0-module. When R_0 is noetherian, an R_0-algebra is locally free of finite rank if and only if it is finite and flat.

11.7. Let $S = \mathrm{Spec}(R_0)$. A morphism of schemes $\varphi: X \to S$ is said to be finite if X is affine and $\mathcal{O}(X)$ is a finite R_0-algebra. Such a morphism is said to be locally free if $\mathcal{O}(X)$ is a locally free R_0-algebra. A group scheme G over S is finite (resp. locally free and finite) if it is so as a scheme over S.

11.8. A finite group scheme G over $S = \mathrm{Spec}(R_0)$ is said to be *locally free* of finite order r over S if $\mathcal{O}(G)$ is locally free of constant rank r as an R_0-algebra. When S is noetherian and connected, G is locally free of finite order over S (for some r) if and only if it is finite and flat.

11.9. Let R_0 be a noetherian ring. To give a locally free finite group scheme over R_0 is the same as giving a flat finite R_0-algebra A together with an R_0-homomorphism $\Delta: A \to A \otimes_{R_0} A$ such that (A, Δ) is a Hopf algebra over R_0, i.e., there exist R_0-algebra homomorphisms $\epsilon: A \to R_0$ and $S: A \to A$ making the diagrams (17) and (18), p. 65, commute.

PROPOSITION 11.10. *Let G be a locally free finite group scheme of rank $o(G)$ over a ring R_0 and H a locally free finite subgroup scheme of G of rank $o(H)$. Then*
$$o(G) = o(H) \cdot \mathrm{rank}(G/H).$$
In particular, the order of H divides the order of G. If H is normal, then
$$o(G) = o(H) \cdot o(G/H).$$

PROOF. The morphism $G \to G/H$ is locally free of rank $o(H)$ (see A.67), and the ranks in $G \to G/H \to \mathrm{Spm}(R_0)$ multiply.   □

c. Cartier duality

We show that the category of *commutative* finite group schemes over a field k is self-dual.

For a k-vector space V, we let V' denote the dual vector space. If V and W are finite-dimensional, then there are canonical isomorphisms $V \to V''$ and $V' \otimes W' \to (V \otimes W)'$. Moreover, $k' = k$.

Let G be a finite group scheme, and let $A = \mathcal{O}(G)$. We have k-linear maps
$$\begin{cases} m: A \otimes A \to A \\ e: k \to A \end{cases} \qquad \begin{cases} \Delta: A \to A \otimes A \\ \epsilon: A \to k \end{cases}$$
defining the algebra and coalgebra structures respectively. On passing to the linear duals, we obtain k-linear maps
$$\begin{cases} m': A' \to A' \otimes A' \\ e': A' \to k \end{cases} \qquad \begin{cases} \Delta': A' \otimes A' \to A' \\ \epsilon': k \to A' \end{cases}$$
The duals of the diagrams (17), p. 65, show that (Δ', ϵ') defines an algebra structure on A' (not necessarily commutative), and dually (m', e') defines a coalgebra structure on A'. The algebra (A', Δ', ϵ') is commutative if and only if G is commutative.

LEMMA 11.11. *If G is commutative, then the system $(A', \Delta', \epsilon', m', e')$ is a Hopf algebra.*

PROOF. The system is obviously a bialgebra (9.39), and we shall show that, if S is an antipode for $\mathcal{O}(G)$, then S' is an antipode for $(A', \Delta', \ldots)$. It suffices to show that S' is an algebra homomorphism, and for this we have to check that $\Delta' \circ (S' \otimes S') = S' \circ \Delta'$, or, equivalently, that $\Delta \circ S = (S \otimes S) \circ \Delta$. In other words, we have to check that the diagram at left below commutes. This corresponds (under a category equivalence) to the diagram at right, which commutes precisely because G is commutative (the inverse of a product of two elements is the product of the inverses of the elements):

$$
\begin{array}{ccc}
\mathcal{O}(G) \xrightarrow{\ \Delta\ } \mathcal{O}(G) \otimes \mathcal{O}(G) & \qquad & G \xleftarrow{\ m\ } G \times G \\
\Big\downarrow{\scriptstyle S} \qquad\qquad \Big\downarrow{\scriptstyle S \otimes S} & & \Big\uparrow{\scriptstyle \mathrm{inv}} \qquad\qquad \Big\uparrow{\scriptstyle \mathrm{inv}\times\mathrm{inv}} \\
\mathcal{O}(G) \xrightarrow{\ \Delta\ } \mathcal{O}(G) \otimes \mathcal{O}(G) & & G \xleftarrow{\ m\ } G \times G.
\end{array}
$$

□

Thus, the category of commutative finite group schemes has an autoduality:

$$\mathcal{O}(G) = (A, m, e, \Delta, \epsilon) \leftrightarrow (A', \Delta', \epsilon', m', e') = \mathcal{O}(G').$$

The group scheme G' is called the **Cartier dual** of G. The functor $G \rightsquigarrow G'$ is a contravariant equivalence from the category of commutative finite group schemes over k to itself, and $(G')' \simeq G$.

We now describe the functor of points $R \rightsquigarrow G'(R)$ of the Cartier dual of G. For a k-algebra R, let G_R denote the functor of R-algebras $R' \rightsquigarrow G(R')$, and let $\underline{\mathrm{Hom}}(G, \mathbb{G}_m)(R)$ denote the set of natural transformations $u \colon G_R \to \mathbb{G}_{mR}$ of group-valued functors. This becomes a group under the multiplication

$$(u_1 \cdot u_2)(g) = u_1(g) \cdot u_2(g), \quad g \in G(R'), \quad R' \text{ an } R\text{-algebra.}$$

In this way, $R \rightsquigarrow \underline{\mathrm{Hom}}(G, \mathbb{G}_m)(R)$ becomes a functor from k-algebras to groups.

THEOREM 11.12. *There is a canonical isomorphism*

$$G' \simeq \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$$

of functors from k-algebras to groups.

PROOF. Let R be a k-algebra. We have

$$G(R) = \mathrm{Hom}_{R\text{-algebra}}(\mathcal{O}(G), R) \hookrightarrow \mathrm{Hom}_{R\text{-linear}}(\mathcal{O}(G), R) = \mathcal{O}(G')_R. \quad (72)$$

The multiplication in $\mathcal{O}(G)$ corresponds to comultiplication in $\mathcal{O}(G')$, from which it follows that the image of the map (72) consists of the group-like elements in $\mathcal{O}(G')_R$. On the other hand, we know that $\mathrm{Hom}(G'_R, \mathbb{G}_m)$ also consists of the group-like elements in $\mathcal{O}(G')_R$ (p. 92). Thus,

$$G(R) \simeq \underline{\mathrm{Hom}}(G', \mathbb{G}_m)(R).$$

This isomorphism is natural in R, and so $G \simeq \underline{\mathrm{Hom}}(G', \mathbb{G}_m)$. Replace G with G' and use that $(G')' \simeq G$ to obtain the required isomorphism.

□

Theorem 11.12 gives a natural bimultiplicative morphism of schemes

$$G \times G' \to \mathbb{G}_m$$

inducing isomorphisms

$$\begin{cases} G \to \underline{\mathrm{Hom}}(G', \mathbb{G}_m) \\ G' \to \underline{\mathrm{Hom}}(G, \mathbb{G}_m). \end{cases}$$

This is called the ***Cartier pairing***.

EXAMPLE 11.13. The action

$$(i, \zeta) \mapsto \zeta^i : (\mathbb{Z}/n\mathbb{Z})_k \times \mu_n \to \mathbb{G}_m$$

defines isomorphisms of algebraic groups

$$\begin{cases} (\mathbb{Z}/n\mathbb{Z})_k \to \underline{\mathrm{Hom}}(\mu_n, \mathbb{G}_m) \\ \mu_n \to \underline{\mathrm{Hom}}((\mathbb{Z}/n\mathbb{Z})_k, \mathbb{G}_m). \end{cases}$$

EXAMPLE 11.14. Let $G = \alpha_p$, so that $\mathcal{O}(G) = k[X]/(X^p) = k[x]$. Let $1, y,$ $y_2, \ldots, y_{p-1}$ be the basis of $\mathcal{O}(G') = \mathcal{O}(G)'$ dual to $1, x, \ldots, x^{p-1}$. Then $y^i = i! y_i$; in particular, $y^p = 0$. In fact, $G' \simeq \alpha_p$, and the pairing $\alpha_p \times \alpha_p \to \mathbb{G}_m$ is

$$a, b \mapsto \exp(ab) : \alpha_p(R) \times \alpha_p(R) \to R^\times$$

where

$$\exp(ab) = 1 + \frac{ab}{1!} + \frac{(ab)^2}{2!} + \cdots + \frac{(ab)^{p-1}}{(p-1)!}.$$

REMARK 11.15. Let G be a commutative finite group scheme of p-power order over a perfect field k of characteristic $p \neq 0$. The examples show that, if G is connected, then G' may be connected or étale (or neither). However, if G is étale, then G' is connected. In proving this, we may suppose that k is algebraically closed, and then that $G = (\mathbb{Z}/p^m\mathbb{Z})_k$, in which case its dual is μ_{p^m}.

THEOREM 11.16. *Let G be a commutative finite group scheme of p-power order over a perfect field k of characteristic $p \neq 0$. Then G has a unique decomposition*

$$G = G_{ec} \times G_{cc} \times G_{ce}$$

where G_{ec} (resp. G_{cc}, resp. G_{ce}) is étale with connected dual (resp. connected with connected dual, resp. connected with étale dual).

PROOF. We know (11.3) that G can be written uniquely as $G = G_c \times G_e$ with G_c connected and G_e étale. Now $(G_c)' = (G_c)'_c \times (G_c)'_e$, and so $G_c = (G_c)'' = G_{cc} \times G_{ce}$. On the other hand, $(G_e)'$ is connected, and so $(G_e)' = G_{ec}$. ☐

ASIDE 11.17. Everything in this section extends to locally free finite group schemes over a ring (or scheme).

d. Finite group schemes of order p

LEMMA 11.18. *Let (A, Δ) be a finite bialgebra algebra over k, and let (A', Δ') be its dual. Let $d: A \to k$ be a derivation regarded as an element of A'. Then*

$$\Delta'(d) = d \otimes 1 + 1 \otimes d.$$

PROOF. By definition, $\Delta'(d) = d \circ m$, and so, for $x, y \in A$,

$$\Delta'(d)(x \otimes y) = d(xy) = xd(y) + yd(x) = (d \otimes 1 + 1 \otimes d)(x \otimes y). \qquad \square$$

PROPOSITION 11.19. *Let G be a finite group scheme of prime order p over an algebraically closed field k. If $\operatorname{char}(k) \neq p$, then G is isomorphic to $(\mathbb{Z}/p\mathbb{Z})_k$, and if $\operatorname{char}(k) = p$, then G is isomorphic to $(\mathbb{Z}/p\mathbb{Z})_k$, μ_p, or α_p. In particular, G is commutative.*

PROOF. From the connected-étale sequence

$$e \to G^\circ \to G \to \pi_0(G) \to e$$

and the equality $o(G) = o(G^\circ) \cdot o(\pi_0(G))$, we find that G is either connected or étale.

If G is étale, then it is constant because k is algebraically closed, and so G is isomorphic to $(\mathbb{Z}/p\mathbb{Z})_k$.

If G is connected, then $A = \mathcal{O}(G)$ is a local artinian ring and its augmentation ideal $I \subset A$ is nilpotent and nonzero. By Nakayama's lemma $I \neq I^2$ and so there exists a non-zero k-derivation $d: A \to k$. Regard d as an element of A'. Then $\Delta_{A'}(d) = d \otimes 1 + 1 \otimes d$ (see 11.18), and $k[d]$ is a sub k-bialgebra of A'. As $k[d]$ is commutative, the dual is a surjective k-bialgebra homomorphism $A'' \simeq A \to (k[d])'$. Because $o(G)$ is a prime p, it follows that the rank of $k[d]$ is p, and so $k[d] = A'$. In particular, (A', Δ', ϵ') is commutative, and so G is commutative.

Now $G' = \operatorname{Spm}(A')$ is either connected or étale. If G' is étale, then $G' \approx (\mathbb{Z}/p\mathbb{Z})_k$ and $G \approx \mu_p$. As G is connected this implies that $\operatorname{char}(k) = p$. If G' is connected, then d is nilpotent; in fact, $d^p = 0$ but $d^{p-1} \neq 0$ because $k[d]$ has rank p. As $\Delta_{A'}(d) = d \otimes 1 + 1 \otimes d$ and $\Delta_{A'}$ is a ring homomorphism, k must have characteristic p and $G' \approx \alpha_p$. Hence $G \approx \alpha_p$, which completes the proof. $\square$

REMARK 11.20. (a) The proof of Proposition 11.19 follows Tate and Oort 1970, p. 6. The proposition can also be proved using the correspondence between algebraic groups of height 1 and p-Lie algebras (11.37).

(b) There exist noncommutative finite group schemes of order p^2 (see 2.36).

e. Derivations of Hopf algebras

In preparation for the next section, we determine the derivations from a Hopf
algebra. Let R_0 be a commutative ring.

11.21. Let A be an R_0-algebra and M an A-module. Recall (10.27) that an
R_0-derivation $D: A \to M$ is an R_0-linear map such that

$$D(ab) = aD(b) + bD(a).$$

We say that an R_0-derivation $d: A \to \Omega$ is **universal** if every R_0-derivation
$D: A \to M$ is of the form $\lambda \circ d$ for a unique A-linear map $\lambda: \Omega \to M$:

$$\lambda \leftrightarrow \lambda \circ d: \operatorname{Hom}_{A\text{-linear}}(\Omega, M) \simeq \operatorname{Der}_{R_0}(A, M).$$

Such a pair (Ω, d) is uniquely determined up to a unique isomorphism.

11.22. Let B be an R_0-algebra and N a B-module. We can make the direct
sum $B \oplus N$ into a commutative B-algebra with $N^2 = 0$ by setting

$$(b, n)(b', n') = (bb', bn' + b'n).$$

Let A be an R_0-algebra. A homomorphism $A \to B \oplus N$ is a pair (φ, D) with φ
a homomorphism $A \to B$ and D an R_0-derivation for the A-module structure on
N defined by φ.

11.23. More generally, consider a diagram

$$
\begin{array}{ccc}
 & & C \\
 & \nearrow^{\gamma} & \downarrow \\
A & \xrightarrow{\varphi} & B = C/J
\end{array}
$$

of R_0-algebras with J an ideal in C such that $J^2 = 0$. The action of C on J
factors through B. Write J_φ for J regarded as an A-module by means of φ.
Suppose that there exists an R_0-algebra homomorphism $\gamma_0: A \to C$ making the
diagram commute. Let γ be another R_0-linear map $A \to C$ lifting φ. Then $\gamma =
\gamma_0 + D$ with D an R_0-linear map $A \to J$, and γ is an R_0-algebra homomorphism
if and only if D is an R_0-derivation $A \to J_\varphi$. Thus, the set of liftings of φ is
either empty or a principal homogeneous space under $\operatorname{Der}_{R_0}(A, J_\varphi)$.

11.24. Let A be an R_0-algebra and let $\epsilon: A \to R_0$ be an R_0-algebra homo-
morphism with kernel I (so that $A \simeq R_0 \oplus I$). Let M be an R_0-module, and
let M_ϵ denote M endowed with the A-module structure defined by ϵ. Every
derivation $D: A \to M_\epsilon$ is zero on R_0 and I^2, and hence defines an R_0-linear map
$I/I^2 \to M$. Every R_0-linear map $I/I^2 \to M$ arises from a unique derivation,
and so

$$\operatorname{Der}_{R_0}(A, M_\epsilon) \simeq \operatorname{Hom}_{R_0\text{-linear}}(I/I^2, M).$$

Let (A, Δ) be a Hopf algebra over R_0. Thus, $A \simeq R_0 \oplus I$, and we let $\pi \colon A \to I/I^2$ denote the map $a = (a_0, b) \mapsto b \bmod I^2$.

THEOREM 11.25. *Let (A, Δ) be a Hopf algebra over R_0. Then*

$$(1 \otimes \pi) \circ \Delta \colon A \to A \otimes_{R_0} I/I^2$$

is the universal R_0-derivation for A.

We shall deduce this from a more explicit statement. Let M be an A-module. For an R_0-linear map $\lambda \colon I/I^2 \to M$, we define $D_\lambda = (\mathrm{id}, \lambda \circ \pi) \circ \Delta$:

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\mathrm{id} \otimes \pi} A \otimes I/I^2 \xrightarrow{\mathrm{id} \otimes \lambda} A \otimes M \xrightarrow{a \otimes m \mapsto am} M.$$

Explicitly, if $\Delta(a) = \sum a_i \otimes a_i'$, then $D_\lambda(a) = \sum a_i \cdot \lambda \pi(a_i')$.

PROPOSITION 11.26. *The map $\lambda \mapsto D_\lambda$ is an R_0-linear isomorphism*

$$\mathrm{Hom}_{R_0\text{-linear}}(I/I^2, M) \to \mathrm{Der}_{R_0}(A, M).$$

PROOF. Let B be an R_0-algebra and N an R_0-module. Make $B \oplus N$ into a B-algebra with $N^2 = 0$ (see 11.22). Then $G(B \oplus N) \overset{\mathrm{def}}{=} \mathrm{Hom}(A, B \oplus N)$ acquires a group structure from the Hopf algebra structure on A. This can be described as follows:

$$(\varphi, D)(\varphi', D') = (\varphi \cdot \varphi', \varphi \cdot D' + \varphi' \cdot D)$$

with

$$\left\{ \begin{array}{l} \varphi \cdot \varphi' = (\varphi, \varphi') \circ \Delta \quad \text{(product in } G(B) = \mathrm{Hom}(A, B)) \\[2mm] \varphi \cdot D' = (\varphi, D') \circ \Delta = \left(A \xrightarrow{\Delta} A \otimes A \xrightarrow{a \otimes a' \mapsto \varphi(a) \cdot D'(a')} N \right) \\[2mm] \varphi' \cdot D = (\varphi', D) \circ \Delta. \end{array} \right.$$

Let $j \colon B \oplus N \to B$ be the projection map. Then $j_* \colon G(B \oplus N) \to G(B)$ projects $G(B \oplus N)$ onto its subgroup $G(B)$, and so

$$G(B \oplus N) = H \rtimes G(B), \quad H = \mathrm{Ker}(j_*).$$

Let $\varphi \colon A \to B$ be an element of $G(B)$, and write N_φ for N regarded as an A-module by means of φ. According to (11.22), the fibre $j_*^{-1}(\varphi)$ over φ consists of the pairs (φ, D) with D an R_0-derivation $A \to N_\varphi$:

$$j_*^{-1}(\varphi) = \{(\varphi, D) \in G(B \oplus N)\} \simeq \mathrm{Der}_{R_0}(A, N_\varphi).$$

Let $\epsilon_B \colon A \xrightarrow{\epsilon} R_0 \to B$ be the neutral element in $G(B)$. Then

$$x \mapsto (\varphi, 0) \cdot x \colon j_*^{-1}(\epsilon_B) \to j_*^{-1}(\varphi)$$

is a bijection. Explicitly, this is the map $(\epsilon_B, D) \mapsto (\varphi, \varphi \cdot D)$, and so we have a bijection

$$D \mapsto (\varphi, D) \circ \Delta : \mathrm{Der}_{R_0}(A, N_{\epsilon_B}) \to \mathrm{Der}_\varphi(A, N_\varphi).$$

On the other hand (11.24), we have a bijection

$$\lambda \mapsto \lambda \circ \pi : \mathrm{Hom}_{R\text{-linear}}(I/I^2, N) \to \mathrm{Der}_{R_0}(A, N_{\epsilon_B}).$$

On composing these maps, and taking $B = A$, $N = M$, and $\varphi = \mathrm{id}_A$, we obtain the required isomorphism.   □

To prove Theorem 11.25, we have to show that the map

$$\mathrm{Hom}_{A\text{-linear}}(A \otimes_{R_0} I/I^2, M) \to \mathrm{Der}_{R_0}(A, M)$$

"composition with $(1 \otimes \pi) \circ \Delta$" is an isomorphism. But its composite with the obvious isomorphism

$$\mathrm{Hom}_{R_0\text{-linear}}(I/I^2, M) \to \mathrm{Hom}_{A\text{-linear}}(A \otimes I/I^2, M)$$

is the isomorphism in Proposition 11.26.

f. Structure of the underlying scheme of a finite group scheme

LEMMA 11.27. *Let (A, Δ) be a finitely generated Hopf algebra over k, and let I be its augmentation ideal. Let $n \geq 0$ be such that $n!$ is nonzero in k. Let $x_1, \ldots, x_r$ be elements of I forming a basis for the k-vector space I/I^2. Then the monomials*

$$x_1^{m_1} \cdots x_r^{m_r}, \quad m_1 + \cdots + m_r = n$$

form a basis for the k-vector space I^n/I^{n+1}.

PROOF. Clearly the monomials generate I^n/I^{n+1}, and so it remains to prove that they are linearly independent modulo I^{n+1}.

Let π be the projection $A = k \oplus I \to I/I^2$ killing k. Let $d_i : I/I^2 \to k$ be the k-linear map such that $d_i(x_j) = \delta_{ij}$ (Kronecker delta). According to (11.25), there exists a (unique) derivation $D_i : A \to k$ such that

$$D_i(a) = \sum_j a_j \cdot d_i(\pi(b_j)) \quad \text{if } \Delta(a) = \sum a_j \otimes b_j.$$

A direct calculation using (3.22b) shows that $D_i(x_j) = \delta_{ij}$. More generally,

$$D_r^{m_r} D_{r-1}^{m_{r-1}} \cdots D_1^{m_1}(x_1^{m_1} \cdots x_r^{m_r}) = m_1! \cdots m_r!,$$

while $D_r^{m_r} D_{r-1}^{m_{r-1}} \cdots D_1^{m_1}$ is zero on any other monomial of total degree $m_1 + \cdots + m_r = n$. Because of our hypothesis on n, the integer on the right is not zero in k. Therefore, on applying the operators $D_r^{m_r} D_{r-1}^{m_{r-1}} \cdots D_1^{m_1}$ to a linear relation among the monomials of total degree n, we find that the relation is trivial.   □

Recall (2.24) that an algebraic group G is said to have height ≤ 1 if the Frobenius map $F_G: G \to G^{(p)}$ is trivial. This means that $a^p = 0$ for all $a \in I$.

PROPOSITION 11.28. *Let G be a connected finite group scheme of height 1 over a field k of characteristic p. Then*

$$\mathcal{O}(G) \approx k[T_1, \ldots, T_r]/(T_1^p, \ldots, T_r^p) \tag{73}$$

for some $r \geq 1$.

PROOF. Let $t_1, \ldots, t_r$ be elements of $I = I_G$ forming a basis for the k-vector space I/I^2. The monomials $t_1^{m_1} \cdots t_r^{m_r}$, $m_1 + \cdots + m_r \leq p - 1$ clearly span $\mathcal{O}(G)$, but the lemma (applied with $n = 0, \ldots, p-1$) implies that they are linearly independent. □

THEOREM 11.29. *Let G be a connected finite group scheme over a perfect field k of characteristic p. Then*

$$\mathcal{O}(G) \approx k[T_1, \ldots, T_r]/(T_1^{p^{e_1}}, \ldots, T_r^{p^{e_r}})$$

for some integers $e_1, \ldots, e_r \geq 1$.

PROOF. Let $A = \mathcal{O}(G)$, and let $I = I_A$ denote its augmentation ideal. Because G is connected, I is nilpotent. If $x^p = 0$ for all $x \in I$, then G has height 1, and the statement was proved in Proposition 11.28. In the general case, we argue by induction on the order of G. Because k is perfect,

$$B \stackrel{\text{def}}{=} A^p = \{a^p \mid a \in A\}$$

is a Hopf subalgebra of A (see 3.29). By the induction hypothesis,

$$B = k[t_1, \ldots, t_r] \simeq k[T_1, \ldots, T_r]/(T_1^{q_1}, \ldots, T_r^{q_r}), \quad q_i = \text{power of } p.$$

For each i, choose a $y_i \in A$ with $y_i^p = t_i$, and choose a set $\{z_j\}$ in A that is maximal with respect to the requirement that $z_j^p = 0$ for all j and that the z_j be linearly independent in I/I^2. We prove the statement by showing that the homomorphism

$$\begin{cases} Y_i \mapsto y_i \\ Z_j \mapsto z_j \end{cases} \quad C \stackrel{\text{def}}{=} \frac{k[\ldots, Y_i, \ldots, Z_j, \ldots]}{(\ldots, Y_i^{pq_i}, \ldots, Z_j^p, \ldots)} \to A$$

is an isomorphism.

Embed B in C by $t_i \mapsto Y_i^p$. Then C is a free B-module. By Theorem 3.31, A is faithfully flat (hence free) over the local ring B. As in the proof of that theorem, it suffices to show that the map $C/I_B C \to A/I_B A$ is an isomorphism. Clearly,

$$C/I_B C \simeq k[\ldots, Y_i, \ldots, Z_j, \ldots]/(\ldots, Y_i^p, \ldots, Z_j^p, \ldots).$$

The kernel of $\mathrm{Spm}(A, \Delta) \to \mathrm{Spm}(B, \Delta)$ has height 1, and so its coordinate ring $A/I_B A$ also has the form (73). A homomorphism between two k-algebras of the form (73) is an isomorphism if it is an isomorphism modulo the squares of the maximal ideals, because it is surjective by Nakayama's lemma and the two algebras have the same dimension as k-vector spaces. As $I_B A \subset I^2$, it remains to show that the elements y_i and z_j form a basis for I/I^2.

Let a be an element of I, and write a^p in I_B as a polynomial in the t_i with coefficients in k. As k is perfect, we can take a pth root of this to get a polynomial u in the y_i such that $u^p = a^p$. Then $(a-u)^p = 0$, and it follows from the definition of the set $\{z_j\}$ that $a-u$ modulo I^2 is a linear combination of the z_j. Hence the elements y_i and z_j span I/I^2. Suppose that $\sum a_i y_i + \sum b_j z_j$ lies in I^2. On raising this to the pth power, we find that the element $\sum a_i^p y_i^p = \sum a_i^p t_i$ is in I_B^2. But the t_i form a basis for I_B/I_B^2, and so this implies that all a_i are zero. Now $\sum b_j z_j$ lies in I^2, which by definition of the set $\{z_j\}$ implies that all b_j are zero. This completes the proof that the elements y_j and z_j form a basis for I/I^2.   □

COROLLARY 11.30. *Every connected finite group scheme has order a power of the characteristic exponent of the base field.*

PROOF. A connected finite group scheme remains connected under extension of the base field, and so this follows from the theorem.   □

The theorem allows us to reprove Cartier's theorem (3.23).

COROLLARY 11.31. *Let G be an algebraic group over a field k.*
  (a) *If k has characteristic zero, then G is smooth.*
  (b) *If k has characteristic $p \neq 0$ and G is finite of order not divisible by p, then G is étale.*

PROOF. (a) We may suppose that k is algebraically closed. Let x be a nilpotent element of $A = \mathcal{O}(G)$. Certainly $x \in I$. Suppose $x \notin I^2$. Then x is part of a basis for the k-vector space I/I^2, and so, for all $n \geq 0$, x^n is nonzero modulo I^{n+1} (see 11.27). Hence x is not nilpotent. Therefore $x \in I^2$. Now Lemma 3.20 shows that G is smooth.

(b) If $p \nmid o(G)$, then $G^\circ = e$, and so $G = \pi_0(G)$.   □

Theorem 11.29 fails when k is not perfect (Exercise 11-3).

g.   Finite group schemes of order n are killed by n

Consider the algebraic group $G = \mathrm{GL}_n$ over a field k of characteristic $p \neq 0$, and let
$$\mathcal{O}(\mathrm{GL}_n) = k[T_{11}, \ldots, T_{nn}, 1/\det].$$

Let $U = (T_{ij})$ ($n \times n$ matrix with coefficients in $\mathcal{O}(G)$). The augmentation ideal I_G of G is generated by the entries of the matrix $U - I_n = (T_{ij} - \delta_{ij})$. Let

$[p]:\mathcal{O}(G) \to \mathcal{O}(G)$ denote the homomorphism corresponding to the pth power map $x \mapsto x^p:G(R) \to G(R)$. Then $[p]U = U^p$, and so

$$[p](U - I_n) = U^p - I_n = (U - I_n)^p$$

– this matrix has (i,j)th entry $(T_{ij} - \delta_{ij})^p$. Therefore

$$[p]I_{\mathrm{GL}_n} \subset I_{\mathrm{GL}_n}^p. \tag{74}$$

PROPOSITION 11.32. *Let G be a finite group scheme over k of order n. Then, for all k-algebras R, the order of every element of $G(R)$ divides n. In other words, the nth power map $n_G:G \to G$ is trivial.*

PROOF. The statement is true for étale group schemes because it is true for abstract groups (apply 2.16). Also, it is true for an extension G of Q by N if it is true for Q and N because $o(G) = o(N) \cdot o(Q)$ and the sequence

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

is exact. Thus, we may suppose that G is connected, and hence that $n = p^m$ for some m (see 11.30).

    The regular representation realizes G as a closed subgroup scheme of GL_n (see 4.9). Therefore we have a surjective homomorphism of Hopf algebras, $\mathcal{O}(\mathrm{GL}_n) \to \mathcal{O}(G)$. This maps the augmentation ideal of GL_n onto that of $\mathcal{O}(G)$, and (74) implies that $[p]I_G \subset I_G^p$, where $[p]$ now denotes the homomorphism $\mathcal{O}(G) \to \mathcal{O}(G)$ corresponding to $p_G:G \to G$. On iterating, we find that $[p^m]I_G \subset I_G^{p^m}$. But in an artinian local ring of length p^m with maximal ideal I, one has $I^{p^m} = 0$. Hence $[p^m]I_G = 0$, and so $[p^m]f = f(1) = [1]f$, all $f \in \mathcal{O}(G)$, as claimed. □

COROLLARY 11.33. *Let G be a locally free finite group scheme of order n over a reduced ring R_0. Then $n_G = 0_G$.*

PROOF. The equalizer of the homomorphisms $n_G, 1_G:G \rightrightarrows G$ is a closed subscheme Z of G. As R_0 is reduced, $R_{0\mathfrak{p}}$ is reduced (hence a field) if $\mathfrak{p}$ is minimal; moreover, the map $R_0 \to \prod_{\mathfrak{p} \text{ minimal}} R_{0\mathfrak{p}}$ is injective (because $R_0 \to \prod_{\mathfrak{p} \text{ minimal}} R_0/\mathfrak{p}$ is injective). Consider the diagram

$$
\begin{array}{ccc}
\mathcal{O}(G) & \xrightarrow{a} & \prod_{\mathfrak{p}} \mathcal{O}(G)_{\mathfrak{p}} \\
\downarrow & & \downarrow b \\
\mathcal{O}(Z) & \longrightarrow & \prod_{\mathfrak{p}} \mathcal{O}(Z)_{\mathfrak{p}}
\end{array}
\qquad \text{(products over the minimal primes of } R_0\text{).}
$$

The map a is injective because $\mathcal{O}(G)$ is flat over R_0, and Proposition 11.32 applied to $G_{R_{0\mathfrak{p}}}$ shows that b is an isomorphism. It follows that $\mathcal{O}(G) \to \mathcal{O}(Z)$ is injective, hence an isomorphism. □

NOTES. The proof of Theorem 11.32 follows Tate 1997, p. 142. The theorem is also true for *commutative* locally free finite group schemes over arbitrary base schemes (Deligne; see Tate and Oort 1970, p. 4).

h. Finite group schemes of height at most one

Let k be a field of characteristic $p \neq 0$ and $\mathfrak{g}$ a p-Lie algebra over k. Recall that the universal enveloping p-Lie algebra $j : \mathfrak{g} \to U^{[p]}(\mathfrak{g})$ has the following property: every p-Lie algebra homomorphism $\mathfrak{g} \to [A]$ with A an associative algebra over k extends uniquely to a homomorphism $U^{[p]}(\mathfrak{g}) \to A$ of associative algebras over k. From this universality we deduce that there is:

(a) a unique homomorphism of associative algebras over k

$$\Delta : U^{[p]}(\mathfrak{g}) \to U^{[p]}(\mathfrak{g}) \times U^{[p]}(\mathfrak{g})$$

such that $\Delta(j(x)) = 1 \otimes j(x) + j(x) \otimes 1$ for $x \in \mathfrak{g}$;

(b) a unique homomorphism $\epsilon : U^{[p]}(\mathfrak{g}) \to k$ such that $\epsilon \circ j = 0$;

(c) a unique anti-homomorphism $S : U^{[p]}(\mathfrak{g}) \to U^{[p]}(\mathfrak{g})$ such that $S(j(x)) = -j(x)$ for $x \in \mathfrak{g}$.

Let $u \in U^{[p]}(\mathfrak{g})$, and write $\Delta u = \sum u_i \otimes v_i$. Then

$$\sum u_i \otimes v_i = \sum v_i \otimes u_i, \quad \sum u_i \otimes \Delta v_i = \sum \Delta u_i \otimes v_i,$$

$$\sum \epsilon(u_i) v_i = u, \quad \sum S(u_i) v_i = \varepsilon(u).$$

It suffices to check these equalities when $u = 1$ or $j(x)$, $x \in \mathfrak{g}$, in which case they are obvious.

PROPOSITION 11.34. *When $\mathfrak{g}$ is commutative, the pair $(U^{[p]}(\mathfrak{g}), \Delta)$ is a Hopf algebra with ϵ and S as co-identity and inversion.*

PROOF. This is exactly what the above identities say.   □

We now consider a general finite-dimensional p-Lie algebra $\mathfrak{g}$ over k. Let $U = U^{[p]}(\mathfrak{g})$. For a k-algebra R, we let Δ_R and ϵ_R denote the maps

$$U \otimes R \xrightarrow{\Delta \otimes R} U \otimes U \otimes R \xrightarrow{\simeq} (U \otimes R) \otimes_R (U \otimes R)$$

$$U \otimes R \xrightarrow{\epsilon \otimes R} k \otimes R \simeq R.$$

PROPOSITION 11.35. *Let $\mathfrak{g}$ be a p-Lie algebra. The functor*

$$R \rightsquigarrow G(\mathfrak{g})(R) \overset{\text{def}}{=} \left\{ x \in \left(U^{[p]}(\mathfrak{g}) \otimes R \right)^{\times} \,\middle|\, \Delta_R x = x \otimes x, \quad \epsilon_R x = 1 \right\}$$

is a finite group scheme of height ≤ 1.

PROOF. By definition, $G(\mathfrak{g})(R)$ is a monoid; it is a group because $x \in G(\mathfrak{g})(R)$ implies that $S(x)x = \epsilon(x) = 1$. Let

$$A = \text{Hom}_{k\text{-linear}}(U^{[p]}(\mathfrak{g}), k).$$

When equipped with the multiplication

$$A \otimes A \simeq (U \otimes U)^\vee \xrightarrow{\Delta^\vee} U^\vee = A,$$

it becomes an associative commutative k-algebra with ϵ as its identity element. Moreover, as $U^{[p]}(\mathfrak{g})$ is finite-dimensional (10.40), there is a canonical isomorphism

$$i: U^{[p]}(\mathfrak{g}) \otimes R \simeq \text{Hom}_{k\text{-linear}}(A, R).$$

For $x \in U^{[p]}(\mathfrak{g}) \otimes R$, one checks that $i(x)$ is a homomorphism of k-algebras if and only if $x \in G(\mathfrak{g})(R)$. Consequently, i induces an isomorphism $G(\mathfrak{g}) \to \text{Spm}(A)$, and so $G(\mathfrak{g})$ is a finite scheme over k. Finally, the coproduct $\Delta_A: A \to A \otimes A$ defined by the group structure on $G(\mathfrak{g})$ is the dual of the multiplication map $U \otimes U \to U$ (apply (16), p. 65). For more details, see DG, II, §7, 3.9. □

For an algebraic group G over k, the pth power operation on the space $\text{Der}_k(\mathcal{O}(G), \mathcal{O}(G))$ preserves the left invariant derivations, and makes $\text{Lie}(G)$ into a p-Lie algebra.

PROPOSITION 11.36. *Let $\mathfrak{g}$ be a p-Lie algebra and G an algebraic group over k. For every homomorphism of p-Lie algebras $\alpha: \mathfrak{g} \to \text{Lie}(G)$, there exists a unique homomorphism $\varphi: G(\mathfrak{g}) \to G$ such that $\alpha = \text{Lie}(\varphi) \circ \text{Lie}(\varphi)$.*

PROOF. Let β be the composite map

$$\mathfrak{g} \xrightarrow{\varphi} \text{Lie}(G) \longrightarrow \text{Der}(\mathcal{O}_G, \mathcal{O}_G).$$

and $\rho: G(\mathfrak{g})^{\text{opp}} \to \text{Aut}(G)$ the corresponding homomorphism. Then $f: a \mapsto \rho(a)(1)$ is the required homomorphism. For more details, see DG, II, §7, 3.11. □

In particular, for p-Lie algebras $\mathfrak{g}$ and $\mathfrak{g}'$, $\text{Hom}(\mathfrak{g}, \mathfrak{g}') \simeq \text{Hom}(G(\mathfrak{g}), G(\mathfrak{g}'))$.

PROPOSITION 11.37. *The functor $\mathfrak{g} \rightsquigarrow G(\mathfrak{g})$ is an equivalence from the category of finite-dimensional p-Lie algebras over k to the category of algebraic groups over k of height ≤ 1.*

PROOF. Proposition 11.36 shows that the functor is fully faithful, and the functor sending G to its p-Lie algebra is a quasi-inverse. For the details, see DG, II, §7, 4.1. □

In particular, every algebraic group G of height ≤ 1 is isomorphic to $G(\mathfrak{g})$ for some p-Lie algebra $\mathfrak{g}$.

COROLLARY 11.38. *Let G be a smooth connected algebraic group and $\mathfrak{h}$ a p-Lie subalgebra of $\text{Lie}(G)$ stable under the adjoint action of G. Then there exists an isogeny $\varphi: G \to G'$ with infinitesimal kernel such that $\text{Ker}(d\varphi) = \mathfrak{h}$; moreover, φ is universal among isogenies ψ such that $\text{Ker}(d\psi) \supset \mathfrak{h}$.*

PROOF. The inclusion $\mathfrak{h} \to \text{Lie}(G)$ arises from an embedding $H \to G$ with H of height 1. Because $\mathfrak{h}$ is stable under G, the image of H is normal in G. Now the isogeny $G \to G/H$ has the required properties. (For a more direct proof, see Springer 1998, 12.2.5.) □

i. The Verschiebung morphism

Let k be a field of characteristic p. Recall (2.28) that, for every algebraic group G over k, we have a Frobenius homomorphism $F_G: G \to G^{(p)}$. When G is a commutative finite group scheme, F_G induces a homomorphism $V_G: (G^{(p)})' \simeq (G')^{(p)} \to G'$ on the Cartier dual. This is the Verschiebung morphism. We shall need another description of V_G, but first we give another description of F_G.

Let V be a vector space over k. The symmetric group S_p acts on $\bigotimes^p V$ by

$$\tau(v_1 \otimes \cdots \otimes v_p) = v_{\tau(1)} \otimes \cdots \otimes v_{\tau(p)},$$

and $\mathrm{Sym}^p V$ is defined to be the greatest quotient of $\bigotimes^p V$ on which S_p acts trivially: $\mathrm{Sym}^p V = (V^{\otimes p})_{S_p}$. Now let G be an algebraic group over k (not necessarily finite), and let $A = \mathcal{O}(G)$. The action of F_G on A is the composite of the k-linear maps on the top row of the following diagram:

$$x \cdot a^p \longleftarrow\!\!\!\mid [x(a \otimes \cdots \otimes a)] \longleftarrow\!\!\!\mid a \otimes x$$

$$A \longleftarrow \mathrm{Sym}^p(A) \longleftarrow A \otimes_{k,f} k \qquad (f(a) = a^p)$$

with *multiplication* and *quotient* maps, and $A^{\otimes p}$.
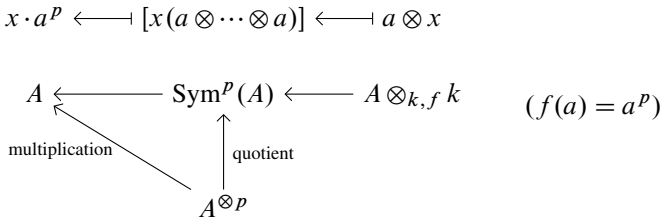
If A is finite, then we can form this diagram for the dual A' of A, and take its dual, to get a diagram

$$A \longrightarrow (A^{\otimes p})^{S_p} \xrightarrow{\ \lambda_A\ } A \otimes_{k,f} k$$

with *comultiplication* and *inclusion* maps, and $A^{\otimes p}$.
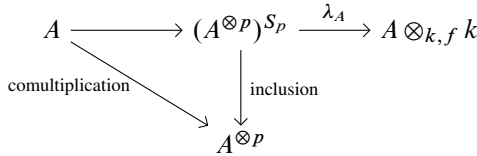
with λ_A the unique k-linear map sending $x \cdot (a \otimes \cdots \otimes a)$ to $a \otimes x$. In fact, this diagram exists for every Hopf algebra A.

DEFINITION 11.39. For an algebraic group G (not necessarily finite) over a field k, the **Verschiebung morphism**[1] is the morphism $V_G: G^{(p)} \to G$ corresponding to the homomorphism $A \otimes_{k,f} k \to A$ in the above diagram.

The assignment $G \mapsto V_G$ has the following properties.
  (a) Functoriality: for all homomorphisms $\varphi: G \to H$ of schemes over k,

$$V_H \circ \varphi^{(p)} = \varphi \circ V_G.$$

---

[1]"Verschiebung" means "shift". Its name is perhaps explained by (75), p. 227. The French term is "décalage". The notation V_G is universal.

(b) Compatibility with products: $V_{G \times H}$ is the composite of $V_G \times V_H$ with the canonical isomorphism $G^{(p)} \times H^{(p)} \simeq (G \times H)^{(p)}$.

(c) Base change: the formation of V_G commutes with extension of the base field.

PROPOSITION 11.40. *Let G be a commutative group scheme over k. Then:*

(a) $V_G \circ F_G = p \cdot \mathrm{id}_G$,

(b) $F_G \circ V_G = p \cdot \mathrm{id}_{G^{(p)}}$.

PROOF. (a) Let $A = \mathcal{O}(G)$. By construction, F_G and V_G correspond to the maps f_A and v_A in the following diagram:

$$
\begin{array}{ccccc}
& & \overset{v_A}{\longrightarrow} & & \\
A & \longrightarrow & (A^{\otimes p})^{S_p} & \overset{}{\longrightarrow} & A \otimes_{k,\sigma} k \\
& & & \lambda_A & \\
\text{comultiplication} & & \downarrow \text{inclusion} & & \downarrow f_A \\
& & A^{\otimes p} & \longrightarrow & A. \\
& & & \text{multiplication} &
\end{array}
$$
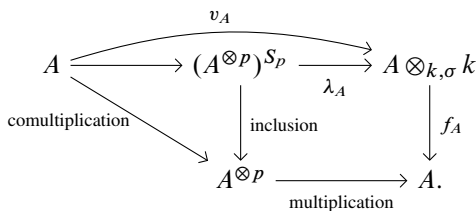
The square at right commutes. In terms of the group schemes, the diagram becomes

$$
\begin{array}{ccc}
& \overset{V_G}{\longleftarrow} & \\
G & & G^{(p)} \\
& & \\
\text{multiplication} & & \uparrow F_G \\
& & \\
G \times \cdots \times G & \longleftarrow & G. \\
& \text{diagonal} &
\end{array}
$$
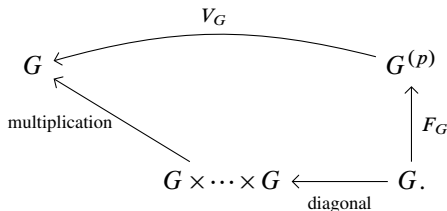
Hence

$$V_G \circ F_G = (\text{multiplication}) \circ (\text{diagonal}) = p \cdot \mathrm{id}_G.$$

(b) Because of the functoriality of F_G,

$$F_G \circ V_G = (V_G)^{(p)} \circ F_{G^{(p)}}.$$

But $(V_G)^{(p)} = V_{G^{(p)}}$ because V_G commutes with base change, and so the right-hand side equals $V_{G^{(p)}} \circ F_{G^{(p)}}$, which (a) shows to equal $p \cdot \mathrm{id}_{G^{(p)}}$. $\quad\square$

COROLLARY 11.41. *A smooth commutative group scheme G has exponent p if and only if $V_G = 0$.*

PROOF. If $V_G = 0$, then $p \cdot \mathrm{id}_G = 0$ because $p \cdot \mathrm{id}_G = V_G \circ F_G$. Conversely, if G is smooth and $p \cdot \mathrm{id}_G = 0$, then $V_G = 0$ because F_G is faithfully flat (2.29). $\square$

j. The Witt schemes W_n

Fix a prime number p. Let $T_0, T_1, \ldots$ be a sequence of symbols, and define (Witt) polynomials

$$
\begin{aligned}
w_0 &= T_0 \\
w_1 &= T_0^p + pT_1 \\
&\quad \cdots \\
w_n &= T_0^{p^n} + pT_1^{p^{n-1}} + \cdots + p^n T_n \\
&\quad \cdots
\end{aligned}
$$

These are polynomials with coefficients in $\mathbb{Z}$. If we invert p, then we can express the T_i as polynomials in the w_i, namely, $T_0 = w_0$, $T_1 = p^{-1}w_1 - w_0^p$, ... Let $U_0, U_1, \ldots$ be a second sequence of symbols.

PROPOSITION 11.42. *There exist unique polynomials*

$$
S_i, P_i \in \mathbb{Z}[T_0, T_1, \ldots, U_0, U_1, \ldots], \quad i = 0, 1, \ldots,
$$

such that, for all $n \geq 0$,

$$
\begin{aligned}
w_n(S_0, \ldots) &= w_n(T_0, \ldots) + w_n(U_0, \ldots) \\
w_n(P_0, \ldots) &= w_n(T_0, \ldots) \cdot w_n(U_0, \ldots).
\end{aligned}
$$

PROOF. It is obvious that there exist unique such polynomials with coefficients in $\mathbb{Z}[1/p]$, and so the point of the proof is to show that p does not occur in the denominators. For this, see Serre 1962, II, §6, Thm 6.   □

For example,

$$
S_0(a,b) = a_0 + b_0 \quad S_1(a,b) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p}
$$

$$
P_0(a,b) = a_0 \cdot b_0 \quad P_1(a,b) = b_0^p a_1 + b_1 a_0^p + pa_1 b_1.
$$

PROPOSITION 11.43. *Let R be a commutative ring. For $n \geq 0$, the rules*

$$
\begin{aligned}
a + b &= (S_0(a,b), \ldots, S_n(a,b)) \\
a \cdot b &= (P_0(a,b), \ldots, P_n(a,b))
\end{aligned}
$$

define the structure of a commutative ring on R^{n+1} (we denote this ring by $W_n(R)$).

PROOF. From the definition of the polynomials S_i and P_i, one sees that the map

$$
a \mapsto (w_0(a), \ldots, w_n(a)) : W_n(R) \to R^{n+1}
$$

is a homomorphism. If p is invertible in R, then the map is a bijection, which proves the proposition for such R.

Because W_n is a functor, it suffices to prove the proposition for the ring $R = \mathbb{Z}[T_0, \ldots]$, and hence for any ring containing $\mathbb{Z}[T_0, \ldots]$. But $\mathbb{Z}[T_0, \ldots]$ can be embedded into $\mathbb{C}$, and we know the proposition for $R = \mathbb{C}$. □

The ring $W_n(R)$ is called the ring of **Witt vectors of length** n with coefficients in R. For example,
$$W_n(\mathbb{F}_p) \simeq \mathbb{Z}/p^{n+1}\mathbb{Z}.$$

Clearly, $R \rightsquigarrow (W_n(R), +)$ is an algebraic group scheme over $\mathbb{Z}$. For example, $W_0 = \mathbb{G}_a$.

We now fix a base field k of characteristic $p \neq 0$, and regard W_n as an algebraic group over k. The map
$$V: W_n(R) \to W_{n+1}(R), \quad (a_0, \ldots, a_n) \mapsto (0, a_0, \ldots, a_n) \tag{75}$$

is additive. This can be proved by the same argument as Proposition 11.43. Thus, we obtain a homomorphism of algebraic groups
$$V: W_n \to W_{n+1}.$$

PROPOSITION 11.44. *For all $n, r \geq 0$, there is an exact sequence*
$$0 \to W_n \xrightarrow{V^r} W_{n+r} \xrightarrow{\text{truncate}} W_r \to 0.$$

PROOF. In fact, for all k-algebras R, the sequence
$$0 \to W_n(R) \xrightarrow{V^r} W_{n+r}(R) \xrightarrow{\text{truncate}} W_r(R) \to 0$$

is obviously exact. □

As W_n is defined over $\mathbb{F}_p \subset k$, we have $W_n^{(p)} \simeq W_n$. The Frobenius morphism $W_n \to W_n^{(p)} \simeq W_n$ acts on $W_n(R)$ as $(a_0, \ldots, a_n) \mapsto (a_0^p, \ldots, a_n^p)$ and the Verschiebung morphism is the composite of the morphisms
$$W_n \xrightarrow{V} W_{n+1} \xrightarrow{\text{truncate}} W_n.$$

In this case, it is easy to verify directly that $VF = p = FV$. In particular, $V_{\mathbb{G}_a} = 0$.

k. Commutative group schemes over a perfect field

In this section, k is a perfect field of characteristic $p \neq 0$.

Finite group schemes over k of order prime to p are étale (11.31), and so are classified in terms of the Galois group of k (see 2.16). In this section, we explain

the classification of commutative finite group schemes over k of order a power of p (which we call finite algebraic p-**groups**).

Let $W = W(k)$ be the ring of Witt vectors with entries in k, i.e., $W(k) = \varprojlim W_n(k)$. Then W is a complete discrete valuation ring with maximal ideal generated by $p = p1_W$ and residue field k. For example, if $k = \mathbb{F}_p$, then $W = \mathbb{Z}_p$. The Frobenius automorphism σ of W is the unique automorphism such that $\sigma a \equiv a^p \pmod{p}$. The ***Dieudonné ring*** $D = W_\sigma[F, V]$ is defined to be the W-algebra of noncommutative polynomials in F and V over W, subject to the following relations ($c \in W$):

$$F \cdot c = \sigma c \cdot F;$$
$$\sigma c \cdot V = V \cdot c;$$
$$FV = p = VF.$$

Thus, to give a left D-module is the same as giving a W-module M together with endomorphisms F and V of M satisfying the following relations ($c \in W$, $m \in M$):

$$F(c \cdot m) = \sigma c \cdot Fm;$$
$$V(\sigma c \cdot m) = c \cdot Vm;$$
$$FV = p \cdot \mathrm{id}_M = VF.$$

Such a module is called a ***Dieudonné module***. We say that M is finitely generated (resp. of finite length) if it is so as a W-module.

For an algebraic group G over k, we define

$$M(G) = \varinjlim_n \mathrm{Hom}(G, W_n) \quad \text{(homomorphisms of algebraic groups).}$$

THEOREM 11.45. *The functor M is a contravariant equivalence from the category of commutative unipotent algebraic groups over k to the category of finitely generated Dieudonné modules killed by a power of V. The group G is finite if and only if $M(G)$ is of finite length, in which case the order of G is the length of $M(G)$ as a W-module.*

PROOF. See DG, V, §1, 4.3.   □

For algebraic groups killed by V, the theorem is a special case of (11.37).

Recall (11.41) that a commutative finite group scheme G of p-power order is a product $G = G_{ec} \times G_{cc} \times G_{ce}$, where G_{ec} is étale with connected dual, G_{cc} is connected with connected dual, and G_{ce} is connected with étale dual. The functor M is defined for $G = G_{ec} \times G_{cc}$, and we define it for $G = G_{ce}$ by setting

$$M(G) = M(G')'$$

where the inner ' denotes the Cartier dual, and the outer ' denotes dual as a Dieudonné module (i.e., $(M, F, V)' = (M', F', V')$ with $M' = \mathrm{Hom}_{W\text{-linear}}(M, W)$ and F' and V' the maps induced by V and F).

THEOREM 11.46. *The function $G \rightsquigarrow M(G)$ is a contravariant equivalence from the category of commutative finite algebraic p-groups to the category of Dieudonné modules of finite length. The order of G is $p^{length(M(G))}$. For every perfect field k' containing k, there is functorial isomorphism*

$$M(G_{k'}) \simeq W(k') \otimes_{W(k)} M(G).$$

PROOF. This can be deduced from Theorem 11.45 (Demazure 1972, III, 6). □

For example:

$$M(\mathbb{Z}/p\mathbb{Z}) = W/pW, \quad F = \sigma, \quad V = 0;$$
$$M(\mu_p) = W/pW, \quad F = 0, \quad V = \sigma^{-1};$$
$$M(\alpha_p) = W/pW, \quad F = 0, \quad V = 0.$$

The theorem reduces the study of commutative algebraic p-groups over perfect fields to semilinear algebra. There are important generalizations of the theorem to Dedekind domains, and other rings.

Exercises

EXERCISE 11-1. Show that an étale algebra over a field k is diagonalizable over k if it becomes diagonalizable over a purely inseparable extension of k.

EXERCISE 11-2. Let G be a finite (hence affine) algebraic group. Show that the following conditions are equivalent:

  (a) the k-algebra $\mathcal{O}(G_{red})$ is étale;
  (b) $\mathcal{O}(G_{red}) \otimes \mathcal{O}(G_{red})$ is reduced;
  (c) G_{red} is an algebraic subgroup of G;
  (d) G is isomorphic to the semidirect product of G° and $\pi_0 G$.

EXERCISE 11-3. (Waterhouse 1979, Chapter 14, Exercise 1). Let k be a nonperfect field of characteristic p, let $c \in k \smallsetminus k^p$, and let G be the subgroup scheme of $\mathbb{G}_a \times \mathbb{G}_a$ such that

$$G(R) = \{(x, y) \mid x^{p^2} = 0, \ y^p = cx^p\} \quad \text{all } k\text{-algebras } R.$$

Show that G is finite and connected, but that its coordinate ring is not a truncated k-algebra $k[T_1, \ldots, T_r]/(T_1^{p^{e_1}}, \ldots, T_r^{p^{e_r}})$. [Compute the dimension of $\{a \in A \mid a^p = 0\}$.]

Groups of Multiplicative Type; Linearly Reductive Groups

Recall that all algebraic groups are affine over a base field k.

a. The characters of an algebraic group

Recall (p. 92) that a character of an algebraic group G is a homomorphism $\chi\colon G \to \mathbb{G}_m$. As $\mathcal{O}(\mathbb{G}_m) = k[T, T^{-1}]$ and $\Delta_{\mathbb{G}_m}(T) = T \otimes T$, to give a character χ of G is the same as giving an invertible element $a = a(\chi)$ of $\mathcal{O}(G)$ such that $\Delta(a) = a \otimes a$. Such elements are said to be group-like, and so there is a one-to-one correspondence $\chi \leftrightarrow a(\chi)$ between the characters of G and the group-like elements of $\mathcal{O}(G)$.

The sum $\chi + \chi'$ of characters χ and χ' of G is defined by

$$(\chi + \chi')(g) = \chi(g) \cdot \chi'(g), \quad g \in G(R), \quad R \text{ a } k\text{-algebra.}$$

Then $\chi + \chi'$ is again a character, and the set of characters is a commutative group, denoted $X(G)$. The correspondence $\chi \leftrightarrow a(\chi)$ has the property that

$$a(\chi + \chi') = a(\chi) \cdot a(\chi').$$

A **cocharacter** of G is a homomorphism $\lambda\colon \mathbb{G}_m \to G$. In the literature, this is often called a one-parameter subgroup of G.

b. The algebraic group $D(M)$

Let M be a finitely generated commutative abstract group (written multiplicatively), and let $k[M]$ be the k-vector space with basis M. Thus, the elements of $k[M]$ are finite sums

$$\sum_i a_i m_i, \quad a_i \in k, \quad m_i \in M.$$

When we endow $k[M]$ with the multiplication extending that on M,

$$\left(\textstyle\sum_i a_i m_i\right)\left(\textstyle\sum_j b_j n_j\right) = \textstyle\sum_{i,j} a_i b_j m_i n_j,$$

then $k[M]$ becomes a k-algebra, called the **group algebra** of M. It becomes a Hopf algebra when we set

$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad S(m) = m^{-1} \qquad (m \in M)$$

because, for m an element of the basis M,

$$(\mathrm{id} \otimes \Delta)(\Delta(m)) = m \otimes (m \otimes m) = (m \otimes m) \otimes m = (\Delta \otimes \mathrm{id})(\Delta(m)),$$
$$(\epsilon \otimes \mathrm{id})(\Delta(m)) = 1 \otimes m, \qquad (\mathrm{id} \otimes \epsilon)(\Delta(m)) = m \otimes 1,$$
$$(S, \mathrm{id})(m \otimes m) = \epsilon(m) = (\mathrm{id}, S)(m \otimes m),$$

as required ((17), (18), p. 65). Note that $k[M]$ is generated as a k-algebra by any set of generators for M as an abelian group, and so it is finitely generated.

EXAMPLE 12.1. Let M be a cyclic group, generated by e.
  (a) Case e of infinite order. The elements of $k[M]$ are finite sums $\sum_{i \in \mathbb{Z}} a_i e^i$ with the obvious addition and multiplication, and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, $S(e) = e^{-1}$. Therefore, $k[M] \simeq \mathcal{O}(\mathbb{G}_m)$ as a Hopf algebra.
  (b) Case e of order n. The elements of $k[M]$ are sums $a_0 + a_1 e + \cdots + a_{n-1} e^{n-1}$ with the obvious addition and multiplication (using $e^n = 1$), and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, and $S(e) = e^{n-1}$. Therefore, $k[M] \simeq \mathcal{O}(\mu_n)$ as a Hopf algebra.

EXAMPLE 12.2. If V and W are vector spaces with bases $(e_i)_{i \in I}$ and $(f_j)_{j \in J}$, then $V \otimes W$ is a vector space with basis $(e_i \otimes f_j)_{(i,j) \in I \times J}$. Therefore, if M_1 and M_2 are commutative groups, then

$$(m_1, m_2) \leftrightarrow m_1 \otimes m_2 : k[M_1 \times M_2] \leftrightarrow k[M_1] \otimes k[M_2]$$

is an isomorphism of k-vector spaces, which respects the Hopf k-algebra structures.

PROPOSITION 12.3. *For every finitely generated commutative group M, the functor $D(M)$*

$$R \rightsquigarrow \mathrm{Hom}(M, R^\times) \quad \textit{(homomorphisms of groups)}$$

is represented by the algebraic group $\mathrm{Spm}(k[M])$. *The choice of a basis for M determines an isomorphism of $D(M)$ with a finite product of copies of $\mathbb{G}_m$ and various μ_n.*

PROOF. To give a k-linear map $k[M] \to R$ is the same as giving a map of sets $M \to R$, and the first is a k-algebra homomorphism if and only if the second is a homomorphism of groups $M \to R^{\times}$. This shows that $D(M)$ is represented by $k[M]$, and is therefore an algebraic group.

The choice of a basis for M as a $\mathbb{Z}$-module determines a decomposition

$$M \simeq \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

and hence a decomposition of k-bialgebras (12.1, 12.2)

$$k[M] \simeq \mathcal{O}(\mathbb{G}_m) \otimes \cdots \otimes \mathcal{O}(\mathbb{G}_m) \otimes \mathcal{O}(\mu_{n_1}) \otimes \cdots \otimes \mathcal{O}(\mu_{n_r}). \qquad \square$$

LEMMA 12.4. *The group-like elements of $k[M]$ are exactly the elements of M.*

PROOF. Let $e \in k[M]$ be group-like. Then $e = \sum c_i e_i$ for some $c_i \in k$ and $e_i \in M$. The argument in the proof of Lemma 4.23 shows that, if the e_i are chosen to be linearly independent, then the c_i form a complete set of orthogonal idempotents in k, and so one equals 1 and the remainder are zero. Therefore $e = e_i$ for some i. $\qquad \square$

Thus $X(D(M)) \simeq M$. The character of $D(M)$ corresponding to $m \in M$ is

$$D(M)(R) = \mathrm{Hom}(M, R^{\times}) \xrightarrow{\; f \mapsto f(m) \;} R^{\times} = \mathbb{G}_m(R).$$

REMARK 12.5. Let p be the characteristic exponent of k. Then:

$D(M)$ is connected	$\iff$	the only torsion in M is p-torsion
$D(M)$ is smooth	$\iff$	M has no p-torsion
$D(M)$ is smooth and connected	$\iff$	M is free.

For example, $D(\mathbb{Z}) = \mathbb{G}_m$, which is connected and smooth, and $D(\mathbb{Z}/n\mathbb{Z}) = \mu_n$, which is connected and nonsmooth if n is a power of p, and is étale and nonconnected if n is relatively prime to p. Moreover,

$$D(M/\{\text{prime-to-}p \text{ torsion}\}) = D(M)^{\circ} \quad \text{(identity component of } D(M)\text{)}$$
$$D(M/\{p\text{-torsion}\}) = D(M)_{\mathrm{red}} \quad \text{(reduced algebraic subgroup)}$$
$$D(M/\{\text{torsion}\}) = D(M)_{\mathrm{red}}^{\circ} \quad \text{(reduced identity component).}$$

REMARK 12.6. When the binary operation on M is denoted by $+$, it is more natural to describe $k[M]$ as the vector space with basis the set of symbols $\{e^m \mid m \in M\}$. The multiplication is then $e^m \cdot e^n = e^{m+n}$ and the comultiplication is $\Delta(e^m) = e^m \otimes e^m$.

c. Diagonalizable groups

DEFINITION 12.7. An algebraic group G is ***diagonalizable*** if the group-like elements in $\mathcal{O}(G)$ span it as a k-vector space.

THEOREM 12.8. *An algebraic group G is diagonalizable if and only if it is isomorphic to $D(M)$ for some commutative group M.*

PROOF. The group-like elements of $k[M]$ span it by definition. Conversely, suppose that the group-like elements M span $\mathcal{O}(G)$. Lemma 4.23 shows that they form a k-linear basis for $\mathcal{O}(G)$, and so the inclusion $M \hookrightarrow \mathcal{O}(G)$ extends to an isomorphism $k[M] \to \mathcal{O}(G)$ of vector spaces. This isomorphism is compatible with the comultiplication maps because it is on the basis elements $m \in M$. □

THEOREM 12.9. *(a) The functor $M \rightsquigarrow D(M)$ is a contravariant equivalence from the category of finitely generated commutative groups to the category of diagonalizable algebraic groups (with quasi-inverse $G \rightsquigarrow X(G)$).*
(b) A sequence

$$0 \to M' \to M \to M'' \to 0$$

of commutative groups is exact if and only if the corresponding sequence of algebraic groups

$$e \to D(M'') \to D(M) \to D(M') \to e$$

is exact (i.e., both of the functors D and X are exact).
(c) Algebraic subgroups and quotient groups of diagonalizable algebraic groups are diagonalizable.

PROOF. (a) Certainly, D is a contravariant functor from the category of finitely generated commutative groups to that of diagonalizable algebraic groups. Theorem 12.8 shows that it is essentially surjective, and so it remains to show that it is fully faithful, i.e., that the map

$$\mathrm{Hom}(M, M') \to \mathrm{Hom}(D(M'), D(M)) \tag{76}$$

is an isomorphism for all M, M'. As D sends finite direct sums to finite products, it suffices to prove that the map (76) is an isomorphism when M and M' are cyclic. If, for example, $M = \mathbb{Z} = M'$, then

$$\mathrm{Hom}(M, M') = \mathrm{End}(\mathbb{Z}) \simeq \mathbb{Z},$$
$$\mathrm{Hom}(D(M'), D(M)) = \mathrm{End}(\mathbb{G}_m, \mathbb{G}_m) = \{T^i \mid i \in \mathbb{Z}\} \simeq \mathbb{Z},$$

and (76) becomes the identity map. The remaining cases are similarly easy.

(b) The map $k[M'] \to k[M]$ is injective, and so $D(M) \to D(M')$ is a quotient map (5.43). Its kernel is represented by $k[M]/I_{k[M']}$, where $I_{k[M']}$ is the augmentation ideal of $k[M']$. But $I_{k[M']}$ is the ideal generated the elements $m-1$ for $m \in M'$, and so $k[M]/I_{k[M']}$ is the quotient ring obtained by setting $m = 1$ for all

$m \in M'$. Therefore $M \to M''$ defines an isomorphism $k[M]/I_{k[M']} \to k[M'']$. This shows that D is exact, and the proof that X is exact is equally easy.

(c) Let H be an algebraic subgroup of a diagonalizable group G. The map $\mathcal{O}(G) \to \mathcal{O}(H)$ is surjective and it sends group-like elements to group-like elements (being a homomorphism of Hopf algebras). As the group-like elements of $\mathcal{O}(G)$ span it, the same is true of $\mathcal{O}(H)$.

Let $D(M) \to Q$ be a quotient map. Its kernel equals $D(M'')$ for some quotient M'' of M. Let M' be the kernel of $M \to M''$. Then $D(M) \to D(M')$ and $D(M) \to Q$ are quotient maps with the same kernel, and so they are isomorphic (5.13).   □

EXAMPLE 12.10. Extensions of diagonalizable groups need not be diagonalizable. For example, the algebraic group G of monomial 2×2 matrices (2.41) is an extension

$$e \to \mathbb{D}_2 \to G \to S_2 \to e$$

of diagonalizable groups without itself being diagonalizable (because it is not commutative). Later (12.22, 15.39) we shall see that an extension of diagonalizable groups is diagonalizable if it is commutative, which is always the case if the quotient is connected.

d.   Diagonalizable representations

DEFINITION 12.11. A representation of an algebraic group is ***diagonalizable*** if it is a sum of one-dimensional representations (according to Theorem 4.25, it is then a *direct* sum of one-dimensional representations).

Recall that $\mathbb{D}_n$ is the group of invertible diagonal $n \times n$ matrices; thus

$$\mathbb{D}_n \simeq \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{n \text{ copies}} \simeq D(\mathbb{Z}^n).$$

A finite-dimensional representation (V, r) of an algebraic group G is diagonalizable if and only if there exists a basis for V such that $r(G) \subset \mathbb{D}_n$. In more down-to-earth terms, the representation defined by an inclusion $G \subset \mathrm{GL}_n$ is diagonalizable if and only if there exists a matrix P in $\mathrm{GL}_n(k)$ such that, for all k-algebras R and $g \in G(R)$,

$$PgP^{-1} \in \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\}.$$

THEOREM 12.12. *The following conditions on an algebraic group G are equivalent:*

(a) *G is diagonalizable;*

(b) *every representation of G is diagonalizable;*

(c) *every finite-dimensional representation of G is diagonalizable;*

(d) *for every representation (V, r) of G, $V = \bigoplus_{\chi \in X(G)} V_\chi$ (here V_χ is the eigenspace with character χ, p. 92).*

PROOF. (a)$\Rightarrow$(b): Let (V, r) be a representation of a diagonalizable group G, and let $\rho \colon V \to V \otimes \mathcal{O}(G)$ be the corresponding comodule. We have to show that V is a sum of one-dimensional representations or, equivalently, that V is spanned by vectors u such that $\rho(u) \in \langle u \rangle \otimes \mathcal{O}(G)$.

Let $v \in V$. As the group-like elements form a basis $(e_i)_{i \in I}$ for $\mathcal{O}(G)$, we can write

$$\rho(v) = \sum_{i \in I} u_i \otimes e_i, \quad u_i \in V.$$

On applying the identities (24), p. 84, to this equality, we find that

$$\sum_i u_i \otimes e_i \otimes e_i = \sum_i \rho(u_i) \otimes e_i$$
$$v = \sum u_i.$$

The first equality shows that

$$\rho(u_i) = u_i \otimes e_i \in \langle u_i \rangle \otimes_k \mathcal{O}(G),$$

and the second shows that the set of u_i arising in this way span V.

(b)$\Rightarrow$(a): In particular, the regular representation of G is diagonalizable, and so $\mathcal{O}(G)$ is spanned by its eigenvectors. Let $f \in \mathcal{O}(G)$ be an eigenvector for the regular representation, and let χ be the corresponding character. Then

$$f(hg) = f(h)\chi(g) \quad \text{for } h, g \in G(R), R \text{ a } k\text{-algebra.}$$

In particular, $f(g) = f(e)\chi(g)$, and so f is a scalar multiple of χ. Hence $\mathcal{O}(G)$ is spanned by its characters.

(b)$\Rightarrow$(c): Trivial.

(c)$\Rightarrow$(b): As every representation is a union of finite-dimensional subrepresentations (4.8), (b) implies that every representation is a sum (not necessarily direct) of one-dimensional subrepresentations.

(b)$\Rightarrow$(d): Certainly, (c) implies that $V = \sum_{\chi \in X(G)} V_\chi$, and Theorem 4.25 implies that the sum is direct.

(d)$\Rightarrow$(b): Clearly each space V_χ is a sum of one-dimensional representations. $\qquad\square$

REMARK 12.13. Let M be a finitely generated commutative group. Recall (9.29) that an M-gradation on a finite-dimensional k-vector space V is a family of subspaces $(V_m)_{m \in M}$ such that $V = \bigoplus_{m \in M} V_m$. To give a representation of $D(M)$ on V is the same as giving an M-gradation of V – the subspace V_m is the eigenspace for the character m of $D(M)$.

e. Tori

DEFINITION 12.14. An algebraic group over k is a **torus** if it becomes iso-morphic to a finite product of copies of $\mathbb{G}_m$ over some field containing k. A torus over k is **split** if it is isomorphic to a product of copies of $\mathbb{G}_m$ over k.

The split tori are the smooth connected diagonalizable algebraic groups. Under the equivalence of categories $M \rightsquigarrow D(M)$, the split tori correspond to free $\mathbb{Z}$-modules M of finite rank. A quotient of a split torus is again a split torus. The algebraic subgroups of split tori are exactly the diagonalizable groups.

It follows that a quotient of a torus is a torus. An algebraic subgroup of a torus is a torus if and only if it is smooth and connected.

EXAMPLE 12.15. Let T be the split torus $\mathbb{G}_m \times \mathbb{G}_m$. Each pair (m_1, m_2) in $\mathbb{Z} \times \mathbb{Z}$ defines a character

$$(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2} : T(R) \to \mathbb{G}_m(R)$$

of T. In this way, we get an isomorphism $X(T) \simeq \mathbb{Z} \times \mathbb{Z}$. Each representation V of T decomposes into a direct sum

$$V = \bigoplus\nolimits_{(m_1, m_2) \in \mathbb{Z} \times \mathbb{Z}} V_{(m_1, m_2)}$$

with $V_{(m_1, m_2)}$ the subspace on which T acts through the character $(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2}$. In this way, the category $\mathsf{Rep}(T)$ acquires a gradation by the group $\mathbb{Z} \times \mathbb{Z}$.

DEFINITION 12.16. Let (V, r) be a representation of a torus T. The characters χ of T such that the eigenspace $V_\chi \neq 0$ are called the **weights** of T on V (and the nonzero eigenspaces are called the **weight spaces**).

f. Groups of multiplicative type

DEFINITION 12.17. An algebraic group over k is of **multiplicative type** if it becomes diagonalizable over some field containing k.

The tori are the smooth connected algebraic groups of multiplicative type. Subgroups and quotient groups (but not necessarily extensions) of groups of multiplicative type are of multiplicative type because this is true of diagonalizable groups (12.9, 12.10).

The terminology "of multiplicative type" is clumsy. Following DG, IV, §1, 2.1, p. 474, we sometimes say that such a group is **multiplicative** (so *the* multiplicative group $\mathbb{G}_m$ is *a* multiplicative group).

Recall (p. 174) that a coalgebra over k is a k-vector space C equipped with a pair of k-linear maps

$$\Delta : C \to C \otimes C, \quad \epsilon : C \to k$$

such that the diagrams (17), p. 65, commute. The linear dual $C^\vee$ of C becomes an associative algebra over k with the multiplication

$$C^\vee \otimes C^\vee \overset{\text{can.}}{\hookrightarrow} (C \otimes C)^\vee \xrightarrow{\Delta^\vee} C^\vee, \tag{77}$$

and the structure map

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

We say that C is **coétale** if it is finite-dimensional and $C^\vee$ is commutative and étale. More generally, we say that a coalgebra is **coétale** if it is a directed union of finite-dimensional coétale subcoalgebras.

Let (C, Δ, ϵ) be a coalgebra over k. A C-comodule is a k-linear map $\rho: V \to V \otimes C$ satisfying the conditions (24), p. 84. Let C_V be the image of the map $V^\vee \otimes V \to C$ defined by ρ. Then C_V is a subcoalgebra of V, and it is finite-dimensional if V is (see p. 175).

THEOREM 12.18. *The following conditions on an algebraic group G over k are equivalent:*

 (a) *G is of multiplicative type;*

 (b) *G is commutative and $\mathrm{Hom}(G, \mathbb{G}_a) = 0$;*

 (c) *G is commutative and $\mathcal{O}(G)$ is coétale;*

 (d) *G becomes diagonalizable over k^s.*

PROOF. First note that

$$\mathrm{Hom}(G, \mathbb{G}_a) \simeq \{f \in \mathcal{O}(G) \mid \Delta(f) = f \otimes 1 + 1 \otimes f\}.$$

The condition on f is linear, and so $\mathrm{Hom}(G, \mathbb{G}_a)$ is a subspace of $\mathcal{O}(G)$ such that

$$\mathrm{Hom}(G_{k'}, \mathbb{G}_{ak'}) \simeq \mathrm{Hom}(G, \mathbb{G}_a) \otimes k'$$

for all fields k' containing k.

(a)$\Rightarrow$(b). We may replace k with an extension field k', and so suppose that G is diagonalizable. If $u: G \to \mathbb{G}_a$ is a nontrivial homomorphism, then $g \mapsto \left(\begin{smallmatrix} 1 & u(g) \\ 0 & 1 \end{smallmatrix}\right)$ is a nonsemisimple representation of G, which contradicts Theorem 12.12.

(b)$\Rightarrow$(c). We may suppose that k is algebraically closed. Let C be a finite-dimensional subcoalgebra of $\mathcal{O}(G)$, i.e., a finite-dimensional k-subspace such that $\Delta(C) \subset C \otimes C$. Let $A = C^\vee$ and let $\langle\,,\,\rangle$ denote the pairing $(f, a) \mapsto f(a): C^\vee \times C \to k$. Then A is a finite product of local artinian rings with residue field k (CA 16.7). If one of these local rings is not a field, then there exists a surjective homomorphism of k-algebras $A \to k[\epsilon]$, where $\epsilon^2 = 0$. This can be written $x \mapsto \langle x, a \rangle + \langle x, b \rangle \epsilon$ with $a, b \in C$ and $b \neq 0$. For $x, y \in A$,

$$\langle xy, a \rangle + \langle xy, b \rangle \epsilon = \langle x \otimes y, \Delta a \rangle + \langle x \otimes y, \Delta b \rangle \epsilon$$

(definition (77) of the product in A) and

$$(\langle x,a\rangle + \langle x,b\rangle\varepsilon)(\langle y,a\rangle + \langle y,b\rangle\varepsilon) = \langle x\otimes y, a\otimes a\rangle + \langle x\otimes y, a\otimes b + b\otimes a\rangle\varepsilon.$$

On equating these expressions, we find that

$$\Delta a = a\otimes a$$
$$\Delta b = a\otimes b + b\otimes a.$$

On the other hand, the structure map $k\to A$ is $(\epsilon|C)^\vee$, and so $\epsilon(a) = 1$. Now

$$1 = (e\circ\epsilon)(a) = ((S,\mathrm{id}_A)\circ\Delta)(a) = S(a)a$$

and so a is a unit in A. Finally,

$$\Delta(ba^{-1}) = \Delta b\cdot\Delta a^{-1} = (a\otimes b + b\otimes a)(a^{-1}\otimes a^{-1})$$
$$= 1\otimes ba^{-1} + ba^{-1}\otimes 1,$$

and so ba^{-1} is a nonzero element of $\mathrm{Hom}(G,\mathbb{G}_a)\neq 0$, which contradicts (b). Therefore A is a product of fields.

(c)$\Rightarrow$(d). We may suppose that k is separably closed. Let C be a finite-dimensional subcoalgebra of $\mathcal{O}(G)$, and let $A = C^\vee$. By assumption, A is a product of copies of k. Let $a_1,\dots,a_n$ be elements of C such that

$$x\mapsto (\langle x,a_1\rangle,\dots,\langle x,a_n\rangle)\colon A\to k^n$$

is an isomorphism. Then the set $\{a_1,\dots,a_n\}$ spans C and, on using that the map is a homomorphism, one finds as in the above step that each a_i is a group-like element of C. This implies that $\mathcal{O}(G)$ is spanned by its group-like elements because $\mathcal{O}(G)$ is a union of finite-dimensional subcoalgebras (specifically, of the coalgebras C_V defined on p. 175).

(d)$\Rightarrow$(a). This is obvious from the definitions. $\square$

COROLLARY 12.19. *If an algebraic group over k becomes diagonalizable over some extension of k, then it becomes diagonalizable over a finite separable extension of k.*

PROOF. It is of multiplicative type. Therefore it splits over k^s, and hence over a finite subextension of k^s. $\square$

COROLLARY 12.20. *If a group of multiplicative type splits over a purely inseparable extension of k, then it is already split over k.*

PROOF. This is a consequence of Exercise 11-1 when the group is finite, and the general case follows. $\square$

COROLLARY 12.21. *A smooth commutative algebraic group G is of multiplicative type if and only if $G(k^\mathrm{a})$ consists of semisimple elements.*

PROOF. We may suppose that k is algebraically closed. Choose a faithful finite-dimensional representation (V, r) of G, and identify G with $r(G)$.

If G is of multiplicative type, then there exists a basis of V for which $G \subset \mathbb{D}_n$, from which it follows that the elements of $G(k)$ are diagonalizable (hence semisimple). Conversely, if the elements of $G(k)$ are semisimple, they form a commuting set of diagonalizable endomorphisms of V, and we know from linear algebra that there exists a basis for V such that $G(k) \subset \mathbb{D}_n(k)$. Because G is smooth, this implies that $G \subset \mathbb{D}_n$. □

Later (17.25), we shall show that every smooth connected algebraic group such that $G(k^a)$ consists of semisimple elements is a torus.

COROLLARY 12.22. *An extension of algebraic groups of multiplicative type is of multiplicative type if and only if it is commutative.*

PROOF. The condition is certainly necessary. On the other hand, an exact sequence

$$e \to G' \to G \to G'' \to e$$

with G commutative gives rise to an exact sequence

$$0 \to \mathrm{Hom}(G'', \mathbb{G}_a) \to \mathrm{Hom}(G, \mathbb{G}_a) \to \mathrm{Hom}(G', \mathbb{G}_a)$$

of abelian groups, and we can apply the criterion (12.18c). □

NOTES. The proof of Theorem 12.18 follows the exercises in Waterhouse 1979.

g. Classification of groups of multiplicative type

Let Γ denote the Galois group of k^s / k endowed with the Krull topology. An action of Γ on a commutative group M is continuous for the discrete topology on M if every element of M is fixed by an open subgroup of Γ, i.e.,

$$M = \bigcup_K M^{\mathrm{Gal}(k^s/K)}$$

where K runs through the finite extensions of k contained in k^s.

For an algebraic group G, we let $X^*(G) = X(G_{k^s})$. In other words, $X^*(G)$ consists of the characters of G defined over k^s. The group Γ acts on $X^*(G)$, and, because every homomorphism $G_{k^s} \to \mathbb{G}_{m k^s}$ is defined over a finite extension of K, the action is continuous. Now $G \rightsquigarrow X^*(G)$ is a contravariant functor from algebraic groups over k to finitely generated $\mathbb{Z}$-modules equipped with a continuous action of Γ. Note that

$$X^*(G_1 \times G_2) \simeq X^*(G_1) \oplus X^*(G_2).$$

Moreover,

$$X^*(G)^\Gamma = X(G) \quad \text{(characters defined over } k, \text{ p. 230).}$$

The tori are the groups G of multiplicative type such that $X^*(G)$ is torsion-free.

Let M be a finitely generated $\mathbb{Z}$-module equipped with a continuous action of Γ. Let $D(M_0)$ be the diagonalizable group over k^s attached to the $\mathbb{Z}$-module M. The coordinate ring of $D(M_0)$ is $k^s[M]$, and the continuous action of Γ on M extends to a semilinear action on $k^s[M]$. We define $D(M)$ to be the algebraic group over k with coordinate ring $k[M]^\Gamma$. It becomes isomorphic to $D(M_0)$ over k^s, and so is of multiplicative type.

THEOREM 12.23. *The functor X^* is a contravariant equivalence from the category of algebraic groups of multiplicative type over k to the category of finitely generated $\mathbb{Z}$-modules equipped with a continuous action of Γ (with quasi-inverse $M \rightsquigarrow D(M)$). Under the equivalence, short exact sequences correspond to short exact sequences.*

PROOF. The statement follows easily from the similar statement over k^s (Theorem 12.9) and Galois descent (A.64, A.66). □

COROLLARY 12.24. *Every algebraic group G of multiplicative type is an extension*

$$e \to G' \to G \to G'' \to e$$

of a finite group G'' of multiplicative type by a torus G'.

PROOF. Let $M = X^*(G)$; then the sequence corresponds to

$$0 \to M_{\mathrm{tors}} \to M \to M/M_{\mathrm{tors}} \to 0.$$ □

COROLLARY 12.25. *Let G and H be groups of multiplicative type over a field k, and let k' be a purely inseparable extension of k. Then*

$$\mathrm{Hom}(G, H) \simeq \mathrm{Hom}(G_{k'}, H_{k'}).$$

PROOF. If G and H are split, this is certainly true, because then

$$\mathrm{Hom}(G, H) \simeq \mathrm{Hom}(X(H), X(G)),$$

which does not change with extension of the base field. In general, there is a finite Galois extension K of k splitting G and H. Then Kk' is a finite Galois extension of k' with the same Galois group Γ. Now $\mathrm{Hom}(G, H) \simeq \mathrm{Hom}(G_K, H_K)^\Gamma \simeq \mathrm{Hom}(G_{Kk'}, H_{Kk'})^\Gamma \simeq \mathrm{Hom}(G_{k'}, H_{k'})$. □

REMARK 12.26. Let G be a group of multiplicative type over k. For every $K \subset k^s$,

$$G(K) = \mathrm{Hom}(X^*(G), (k^s)^\times)^{\Gamma_K}$$

where Γ_K is the subgroup of Γ of elements fixing K, and the notation means that $G(K)$ equals the group of homomorphisms $X^*(G) \to (k^s)^\times$ commuting with the actions of Γ_K.

EXAMPLE 12.27. Let $k = \mathbb{R}$, so that Γ is cyclic of order 2, and let $M = \mathbb{Z}$. Then $\text{Aut}(\mathbb{Z}) = \mathbb{Z}^{\times} = \{\pm 1\}$, and so there are two possible actions of Γ on $X^*(G)$.

(a) Trivial action. Then $D(M)(\mathbb{R}) = \mathbb{R}^{\times}$, and $D(M) \simeq \mathbb{G}_m$.

(b) The element $\iota \neq 1$ of Γ acts on $\mathbb{Z}$ as $m \mapsto -m$. Then $D(M)(\mathbb{R}) = \text{Hom}(\mathbb{Z}, \mathbb{C}^{\times})^{\Gamma}$, which consists of the elements of $\mathbb{C}^{\times}$ fixed under the following action of ι:

$$\iota z = \bar{z}^{-1}.$$

Thus $G(\mathbb{R}) = \{z \in \mathbb{C}^{\times} \mid z\bar{z} = 1\}$, which is compact.

EXAMPLE 12.28. The algebraic group μ_n is of multiplicative type for all n. The constant algebraic group $(\mathbb{Z}/n\mathbb{Z})_k$ is of multiplicative type if k has characteristic 0 or it has characteristic p not dividing n. When k has characteristic $p \neq 0$, the group $(\mathbb{Z}/p\mathbb{Z})_k$ is unipotent and not of multiplicative type. More generally, an étale group scheme over k is of multiplicative type if and only if its order is prime to the characteristic exponent of k.

NOTATION 12.29. Let H be an algebraic group of multiplicative type over k. Then $H = D(M)$ with $M = X^*(H)$. We define

$$H_t \stackrel{\text{def}}{=} D(M/M_{\text{tors}}).$$

It is the largest subtorus of H. It is also the unique subtorus T of H such that H/T is finite, which shows that its formation commutes with extension of the base field. Note that $H_t = (H)^{\circ}_{\text{red}}$. If H is a normal algebraic subgroup of a smooth algebraic group G, then H_t is normal in G (by 1.52 and 1.87).

h. Representations of a group of multiplicative type

An abelian category is **semisimple** if every object is a finite sum of simple objects (then every object is a finite direct sum of simple objects; cf. 4.17). When G is a diagonalizable algebraic group, $\text{Rep}(G)$ is a semisimple abelian category and the isomorphism classes of simple objects in $\text{Rep}(G)$ are classified by the characters of G (see 12.12). When G is of multiplicative type, the description of $\text{Rep}(G)$ is only a little more complicated.

Let k^s be a separable closure of k and $\Gamma = \text{Gal}(k^s/k)$.

THEOREM 12.30. *Let G be an algebraic group of multiplicative type over k. Then $\text{Rep}(G)$ is a semisimple abelian category, and the isomorphism classes of simple objects in $\text{Rep}(G)$ are classified by the orbits of Γ acting on $X^*(G)$. Let (V, r) be the representation corresponding to an orbit Ξ, and let $\chi \in \Xi$; then $\text{End}(V, r) \simeq k_{\chi}$ where k_{χ} is the subfield of k^s fixed by the subgroup of $\text{Gal}(k^s/k)$ fixing χ.*

PROOF. The group G is split by a finite Galois extension K of k – let $\bar{\Gamma} =$ Gal(K/k). Then $\bar{\Gamma}$ acts on $\mathcal{O}(G_K) \simeq K \otimes \mathcal{O}(G)$ through its action on K. Let (V, r) be a representation of G_K, and let ρ be the corresponding co-action. By a semilinear action of $\bar{\Gamma}$ on (V, r), we mean a semilinear action of $\bar{\Gamma}$ on V fixing ρ. It follows from descent theory (A.64, A.65, A.66) that the functor $V \rightsquigarrow V_K$ from $\mathsf{Rep}_k(G)$ to the category of objects of $\mathsf{Rep}_K(G_K)$ equipped with a semilinear action of $\bar{\Gamma}$ is an equivalence of categories.

Let V be a representation of G over k. Then $K \otimes V$ is a representation of G_K equipped with a semilinear action of $\bar{\Gamma}$. As a representation of G_K it decomposes into a direct sum

$$K \otimes V = \bigoplus_{\chi \in X(G_K)} V_\chi.$$

An element γ of $\bar{\Gamma}$ acts on $K \otimes V$ by mapping V_χ isomorphically onto $V_{\gamma\chi}$. Thus, we see that the set of χ occurring in the sum is stable under the action of $\bar{\Gamma}$. Conversely, if Ξ is an orbit of $\bar{\Gamma}$ in $X(G_K)$, then $\bigoplus_{\chi \in \Xi} V_\chi$ has a natural semilinear action of G_K, and so arises from a (simple) representation of G over k. From this the statement follows easily.   □

ASIDE 12.31. Let A be a semisimple abelian category such that the Hom sets are finite-dimensional k-vector spaces and composition is k-bilinear. To describe such a semisimple abelian category up to equivalence, it suffices to list the isomorphism classes of simple objects in A and, for each class, describe the isomorphism class of the endomorphism algebra of an object in the class (these are finite-dimensional division algebras over k).

i.   Density and rigidity

For a commutative algebraic group G and integer $n \geq 1$, we let G_n denote the kernel of multiplication by n on G.

Density theorem

The density theorems say that the family of subschemes G_n is schematically dense in an algebraic group G of multiplicative type. When G is smooth, it suffices to take the G_n with n prime to the characteristic.

THEOREM 12.32 (SMOOTH CASE). *Let G be a smooth algebraic group of multiplicative type. The only closed subscheme of G containing every G_n with n prime to the characteristic of k is G itself.*

PROOF. We may suppose that k is algebraically closed. Let X be a closed subscheme of G containing the G_n. Then X contains every étale subgroup of H. Moreover, $X(k)$ contains an infinite subset of $H(k)$ for every copy H of $\mathbb{G}_m$ contained in G, and therefore contains $H(k)$. As G is a product of an étale group with some copies of $\mathbb{G}_m$ (12.3), this implies that $X(k^a) = G(k^a)$. As G is reduced, $X = G$.   □

THEOREM 12.33. *Let G be an algebraic group of multiplicative type over k. The only closed subscheme of G containing every G_n is G itself.*

PROOF. We may suppose that k is algebraically closed. We have to show that an element of $\mathcal{O}(G)$ is zero if its image in $\mathcal{O}(G_n)$ is zero for all $n \geq 1$. Write $G = \mathbb{G}_m^r \times N$, where N is finite of order d (see 12.3). Then

$$\mathcal{O}(G) = k[t_1,\ldots,t_r,t_1^{-1},\ldots,t_r^{-1}] \otimes \mathcal{O}(N),$$

and, if $d \mid n$,

$$\mathcal{O}(G_n) = \big(k[t_1,\ldots,t_r]/(t_1^n-1,\ldots,t_r^n-1)\big) \otimes \mathcal{O}(N).$$

The family of maps $k[t_1,\ldots,t_r] \to k[t_1,\ldots,t_r]/(t_1^n-1,\ldots,t_r^n-1)$ is obviously injective, and it remains injective when tensored over $k[t_1,\ldots,t_r]$ with the ring $k[t_1,\ldots,t_r^{-1}]$. It follows that the family of maps $\mathcal{O}(G) \to \mathcal{O}(G_n)$ is injective. $\quad\square$

COROLLARY 12.34. *Let G be an algebraic group of multiplicative type. If two homomorphisms from G to an algebraic group H coincide on G_n for all $n \geq 1$, then they are equal.*

PROOF. The difference kernel is a closed subscheme of G (as H is separated 1.22). $\quad\square$

Rigidity theorem

LEMMA 12.35. *Let G and H be algebraic groups of multiplicative type over k with G finite. Then $\underline{\mathrm{Hom}}(G,H)$ is a finite étale group scheme over k.*

PROOF. We may suppose that k is algebraically closed. Then H is an algebraic subgroup of a split torus, and so we may suppose that $H = \mathbb{G}_m$. Now $\underline{\mathrm{Hom}}(G,H)$ is the Cartier dual of G, which is an étale group scheme (see Section 11c). $\quad\square$

The next theorem says that diagonalizable groups are rigid in the sense that a family of homomorphisms from one to a second parameterized by a connected algebraic scheme is constant.

THEOREM 12.36. *Let G and H be diagonalizable groups over k, and let X be a connected algebraic scheme over k. Let $\phi: X \times G \to H$ be a morphism such that, for all k-algebras R and $x \in X(R)$, the map $g \mapsto \phi(x,g): G(R) \to H(R)$ is a homomorphism. For any $x_0 \in X(k)$, we have $\phi(x,g) = \phi(x_0,g)$ for all k-algebras R and $(x,g) \in X(R) \times G(R)$.*

PROOF. The map ϕ defines a morphism $X \to \underline{\mathrm{Hom}}(G,H)$. If G is finite, then $\underline{\mathrm{Hom}}(G,H)$ is étale over k, and so the morphism is constant, as required.

In proving the general case, we may suppose that k is algebraically closed and X is affine. Let Z be the closed subscheme of $X \times G$ on which the two maps $(x,g) \mapsto \phi(x,g)$ and $(x,g) \mapsto \phi(x_0,g)$ coincide. Then $Z \supset X \times G_n$

for all n by the first case, and so it remains to show that the family of maps $\mathcal{O}(X \times G) \to \mathcal{O}(X \times G_n)$ is injective. But $\mathcal{O}(X \times G) \to \mathcal{O}(X \times G_n)$ is obtained from $\mathcal{O}(G) \to \mathcal{O}(G_n)$ by tensoring with $\mathcal{O}(X)$ over k, and we saw in the proof of Theorem 12.33 that the family of maps $\mathcal{O}(G) \to \mathcal{O}(G_n)$ is injective. □

COROLLARY 12.37. *Every action* $\mu: G \times H \to H$ *by group homomorphisms of a connected algebraic group G on a group H of multiplicative type is trivial.*

PROOF. The hypothesis says that, for a fixed $g \in G(R)$, the map $h \mapsto \mu(g,h)$ is a homomorphism $H(R) \to H(R)$. Therefore Theorem 12.36 shows that $\mu(g,h) = \mu(e,h) = h$ for all g,h. □

COROLLARY 12.38. *Every normal multiplicative subgroup N of a connected algebraic group G is contained in the centre of G.*

PROOF. The action G on N by inner automorphisms is trivial. □

REMARK 12.39. (a) Similarly, every normal étale subgroup of a connected algebraic group is central (the automorphism group scheme of an étale group is étale; for example, $\underline{\mathrm{Aut}}(N_k) = (\mathrm{Aut}(N))_k$).

(b) It is essential in 12.37 that G act by group homomorphisms. For example, the multiplication map of $\mathbb{G}_m$ is a nontrivial action of $\mathbb{G}_m$ on $\mathbb{G}_m$ as a scheme.

COROLLARY 12.40. *Let H be a subgroup of multiplicative type of an algebraic group G. Then $N_G(H)^\circ = C_G(H)^\circ$, i.e., $C_G(H)$ is an open subgroup of $N_G(H)$.*

PROOF. Theorem 12.36 applied to

$$\phi: N_G(H)^\circ \times H \to H, \quad (g,h) \mapsto ghg^{-1}$$

shows that $ghg^{-1} = ehe^{-1} = h$ for all g,h, and so $N_G(H)^\circ \subset C_G(H)$. □

COROLLARY 12.41. *Let N be a normal subgroup of an algebraic group H such that N and H/N are of multiplicative type. Every action of a connected algebraic group G on H by group homomorphisms preserving N is trivial.*

PROOF. Corollary 12.37 shows that the action of G on H factors through an action $G \times H/N \to H$, and then through an action $G \times H/N \to N$. Theorem 12.36 now shows that this action is trivial. □

COROLLARY 12.42. *An extension of algebraic groups of multiplicative type is of multiplicative type if it is connected.*

PROOF. Let G be an algebraic group with a normal subgroup N such that N and G/N are of multiplicative type. Then the action of G on itself by inner automorphisms is trivial (12.41). Therefore G is commutative, and so it is of multiplicative type (12.22). □

REMARK 12.43. For a set M, define M_k to be the scheme over k (not necessarily of finite type) equal to the disjoint union of copies of $\mathrm{Spm}(k)$ indexed by the elements of M. For an algebraic scheme X over k,

$$M_k(X) = \mathrm{Hom}(\pi_0(X), M).$$

When M is a group, M_k becomes a group scheme over k.

Let R be a k-algebra R with no idempotents except 0 and 1. Then

$$\mathrm{Hom}(\mathbb{G}_{mR}, \mathbb{G}_{mR})(R) \simeq \mathbb{Z}.$$

To prove this, let $e_i = T^i$, and argue as in the proof of Proposition 4.23. It follows that the obvious map

$$\mathbb{Z}_k \to \underline{\mathrm{Hom}}(\mathbb{G}_m, \mathbb{G}_m)$$

is an isomorphism. More generally, for finitely generated $\mathbb{Z}$-modules M, M',

$$\mathrm{Hom}(M', M)_k \simeq \underline{\mathrm{Hom}}(D(M), D(M')).$$

Hence,

$$\mathrm{Hom}(X, \underline{\mathrm{Hom}}(D(M), D(M')) \simeq \mathrm{Hom}(\pi_0(X), \mathrm{Hom}(M', M))$$

for an algebraic k-scheme X. This provides a more geometric proof of Theorem 12.36.

j. Central tori as almost-factors

DEFINITION 12.44. An algebraic subgroup of an algebraic group G is ***central*** if it is contained in the centre of G.

For example, every normal torus in a connected algebraic group is central (12.38).

DEFINITION 12.45. An algebraic group G is ***perfect*** if it equals its derived group.

In other words, G is perfect if it has no nontrivial commutative quotient. A smooth connected algebraic group is perfect if it has no commutative quotient of nonzero dimension. Quotients of perfect algebraic groups are obviously perfect. We shall see later (21.50) that semisimple algebraic groups are perfect.

PROPOSITION 12.46. *Let T be a central torus in a connected group variety G over k.*

  (a) *The algebraic subgroup $T \cap \mathcal{D}G$ is finite.*
  (b) *If G/T is perfect, then the sequence*

$$e \to T \cap \mathcal{D}(G) \to T \times \mathcal{D}(G) \to G \to e \qquad (78)$$

  is exact. In particular, $G/\mathcal{D}(G)$ is a torus.

PROOF. We may suppose that k is algebraically closed.

(a) An algebraic group N is finite if $N(k)$ is finite (because $k = k^{\mathrm{a}}$). Note that

$$(T \cap \mathcal{D}G)(k) = T(k) \cap (\mathcal{D}G)(k).$$

Choose a faithful representation $G \to \mathrm{GL}_V$ of G (which exists by 4.9), and identify G with its image. Because T is diagonalizable, V is a direct sum

$$V = V_{\chi_1} \oplus \cdots \oplus V_{\chi_r}, \quad \chi_i \neq \chi_j, \quad \chi_i \in X^*(T),$$

of eigenspaces for the action of T (see 12.12). When we choose bases for the V_{χ_i}, the group $T(k)$ consists of the matrices

$$\begin{pmatrix} A_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_r \end{pmatrix}$$

with A_i of the form $\mathrm{diag}(\chi_i(t), \ldots, \chi_i(t))$, $t \in k$. As $\chi_i \neq \chi_j$ for $i \neq j$, we see that the centralizer of $T(k)$ in $\mathrm{GL}(V)$ consists of the matrices of this shape but with the A_i arbitrary. Because $(\mathcal{D}G)(k)$ is generated by commutators, its elements have determinant 1 on each summand V_{χ_i}. But $\mathrm{SL}(V_{\chi_i})$ contains only finitely many scalar matrices $\mathrm{diag}(a_i, \ldots, a_i)$, and so $T(k) \cap (\mathcal{D}G)(k)$ is finite.

(b) The subgroup $T \cdot \mathcal{D}(G)$ of G is normal (because it contains the derived group). The algebraic group $G/(T \cdot \mathcal{D}(G))$ is a quotient both of $G/\mathcal{D}(G)$ and of G/T, and so it is both commutative and perfect, hence trivial. Therefore,

$$G = T \cdot \mathcal{D}(G).$$

As T is central, the multiplication map $T \times \mathcal{D}(G) \to G$ is a homomorphism. Its kernel is $T \cap \mathcal{D}(G)$ and its image is G.   □

EXAMPLE 12.47. The centre of GL_n is $\mathbb{G}_m$ (nonzero scalar matrices), its derived group is SL_n, and the quotient $\mathrm{GL}_n / \mathbb{G}_m = \mathrm{PGL}_n$ is perfect (because simple and noncommutative). The sequence (78) is

$$1 \to \mu_n \to \mathbb{G}_m \times \mathrm{SL}_n \to \mathrm{GL}_n \to 1.$$

k. Maps to tori

For the notion of a (Weil) divisor on a normal algebraic variety, we refer the reader to A.78.

PROPOSITION 12.48. *Let X and Y be irreducible algebraic varieties over an algebraically closed field k. Every regular map $u: X \times Y \to \mathbb{G}_m$ is of the form $u = u_1 \cdot u_2$ with u_1 (resp. u_2) a regular map $X \to \mathbb{G}_m$ (resp. $Y \to \mathbb{G}_m$).*

PROOF. Let x_0 and y_0 be normal points on X and Y, and let v be the regular function on $X \times Y$ such that

$$v(x,y) = u(x,y_0) \cdot u(x_0,y) \cdot u(x_0,y_0)^{-1}. \tag{79}$$

We shall show that $u = v$. It suffices to prove this on an open neighbourhood of (x_0,y_0), and so we may suppose that X and Y are both affine and normal.

Let $\bar{X}$ and $\bar{Y}$ be normal projective varieties containing X and Y as dense open subsets. We regard u and v as rational functions on $\bar{X} \times \bar{Y}$. As the functions u and v take values in $k^\times$ on $X \times Y$, the divisor (u/v) of u/v on $\bar{X} \times \bar{Y}$ has support in

$$\big((\bar{X} \smallsetminus X) \cup \bar{Y}\big) \cup (\bar{X} \times (\bar{Y} \smallsetminus Y)).$$

Therefore it is a sum of divisors of the form $D \times \bar{Y}$ and $\bar{X} \times E$, where D and E are irreducible components of $\bar{X} \smallsetminus X$ and $\bar{Y} \smallsetminus Y$ of codimension one. If u/v is zero on $D \times \bar{Y}$, then u/v is regular on U and zero on $U \cap (D \times \{y_0\})$ for some open subset U of $X \times Y$ meeting $D \times \{y_0\}$. But $u(x,y_0) = v(x,y_0)$ for $x \in X$, which gives a contradiction. Similarly, v/u does not have a zero on $D \times \bar{Y}$, and so no divisor of the form $D \times \bar{Y}$ occurs in (u/v). Similarly, no divisor of the form $\bar{X} \times E$ occurs in (u/v), and so u/v is a constant. On taking $(x,y) = (x_0,y_0)$, we see that the constant is 1. □

PROPOSITION 12.49. *Let G be a connected group variety, and let T be a group of multiplicative type. Every regular map $\varphi : G \to T$ such that $\varphi(e) = e$ is a homomorphism of algebraic groups.*

PROOF. We may suppose that k is algebraically closed, and then that $T = \mathbb{G}_m$. According to Proposition 12.48, there exist regular maps $\varphi_1, \varphi_2 : G \to \mathbb{G}_m$ such that $\varphi \circ m = \varphi_1 \cdot \varphi_2$, i.e., such that

$$\varphi(g_1 g_2) = \varphi_1(g_1)\varphi_2(g_2) \text{ for } g_1, g_2 \in G. \tag{80}$$

In particular, $\varphi_1(e)\varphi_2(e) = e$, and so we can scale φ_1 and φ_2 so that $\varphi_1(e) = e = \varphi_2(e)$. On taking g_1 (resp. g_2) to be e in (80), we find that $\varphi = \varphi_2$ (resp. $\varphi = \varphi_1$), and so $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. □

REMARK 12.50. For a variety X over a field k, let $U(X) = \Gamma(X, \mathcal{O}_X^\times)/k^\times$. Proposition 12.48 shows that

$$U(X) \oplus U(Y) \simeq U(X \times Y)$$

when k is algebraically closed. In fact, this is true over more general fields (cf. Grothendieck 1972, VIII, 4.1): it suffices to prove that the identity

$$u(x,y) = u(x,y_0) \cdot u(x_0,y) \cdot u(x_0,y_0)^{-1}$$

holds for some $x_0 \in X(k)$ and $y_0 \in Y(k)$, and for this we may extend the base field and then normalize.

ASIDE 12.51. Note the similarity of the statements 8.19 and 12.49. Rosenlicht (1961) defines a connected group variety G (not necessarily affine) over an algebraically closed field k to be *toroidal* if it satisfies the following equivalent conditions:

(a) every maximal connected affine subgroup variety of G is a torus;

(b) G contains no algebraic subgroup isomorphic to $\mathbb{G}_a$;

(c) for every connected subgroup variety H of G, the points of $H(k)$ of finite order prime to $\mathrm{char}(k)$ are dense in H.

Tori and abelian varieties are toroidal; connected subgroup varieties, quotients, and extensions of toroidal groups are toroidal; all toroidal groups are commutative (and hence of multiplicative type if affine). In the same article, Rosenlicht proves Proposition 12.48 for all toroidal algebraic groups, and deduces Proposition 12.49 for such groups.

l. Linearly reductive groups

DEFINITION 12.52. An algebraic group is *linearly reductive* if every finite-dimensional representation is semisimple.

REMARK 12.53. (a) If G is linearly reductive, then every representation is a sum of simple representations (because it is a union of finite-dimensional subrepresentations). This implies that it is a direct sum of simple representations (4.17).

(b) An algebraic group G over k is linearly reductive if and only if the endomorphism algebra of every finite-dimensional representation of G is semisimple. The necessity is obvious (4.18), and we prove the sufficiency. If $\alpha\colon V \to W$ is a nonzero homomorphism of finite-dimensional representations of G, then there exists a $\beta\colon W \to V$ such that $\alpha \circ \beta \neq 0$ because otherwise $\left(\begin{smallmatrix} 0 & 0 \\ \alpha & 0 \end{smallmatrix}\right)\mathrm{End}(V \oplus W)$ would be a nonzero nilpotent right ideal in $\mathrm{End}(V \oplus W)$. Now let V be a finite-dimensional representation of G, and let W be a maximal subrepresentation. The quotient map $\alpha\colon V \to V/W$ is nonzero, and so there exists a map $\beta\colon V/W \to V$ such that $\alpha \circ \beta \neq 0$. As V/W is simple, $\alpha \circ \beta$ is an isomorphism, and we may suppose that it equals $\mathrm{id}_{V/W}$. Now $V = \mathrm{Im}(\beta) \oplus W$. Repeating the argument for W, we eventually obtain V as a sum of simple representations.

(c) Let G be an algebraic group over k, and let k' be a field containing k. If $G_{k'}$ is linearly reductive, then so is G (apply 4.19a). Conversely, if G is linearly reductive and k' is separable over k, then $G_{k'}$ is linearly reductive. Indeed, the representations of the form $(V,r) \otimes k'$ are semisimple (4.19c), and every representation of $G_{k'}$ is a subquotient of such a representation (this follows from 4.14).[1]

PROPOSITION 12.54. *A commutative algebraic group is linearly reductive if and only if it is of multiplicative type.*

---

[1]In fact, it follows from the classification (12.56) that G is linearly reductive if and only if $G_{k'}$ is linearly reductive (no condition on k'/k).

PROOF. We saw in (12.30) that $\mathsf{Rep}(G)$ is semisimple if G is of multiplicative type. Conversely, if $\mathsf{Rep}(G)$ is semisimple, then $\mathrm{Hom}(G, \mathbb{U}_2) = 0$. But $\mathbb{U}_2 \simeq \mathbb{G}_a$, and so G is of multiplicative type by (12.18). □

EXAMPLE 12.55. Over a field of characteristic 2, the representation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & ac & bd \\ 0 & a^2 & b^2 \\ 0 & c^2 & d^2 \end{pmatrix} : \mathrm{SL}_2 \to \mathrm{GL}_3$$

is not semisimple because ac and bd are not linear polynomials in a^2, b^2, c^2, d^2 (Exercise 12-9).

REMARK 12.56. Later (22.43) we shall prove that an algebraic group G over a field of characteristic zero is linearly reductive if and only if G° is reductive. An algebraic group G over a field of characteristic $p \neq 0$ is linearly reductive if and only if G° is a torus and p does not divide the index $(G : G^\circ)$. This was proved by Nagata (1961/1962) for group varieties, and is often referred to as Nagata's theorem. See DG, IV, §3, 3.6, or Kohls 2011.

Let G be a linearly reductive group and (V, r) a representation of G. Then V has a unique decomposition $V = V^G \oplus V'$ with V' equal to the sum of all simple subrepresentations on which G acts nontrivially. The ***Reynolds operator*** is the unique linear map $\rho : V \to V^G$ with $\rho | V^G = \mathrm{id}$ and $\rho(V') = 0$.

The group $\mathrm{GL}_n(k)$ acts linearly on $k[T_1, \ldots, T_n]$ as follows: let $g = (a_{ij}) \in \mathrm{GL}_n(k)$ and let $f \in k[T_1, \ldots, T_n]$; then $(gf)(T_1, \ldots, T_n) = f(T_1', \ldots, T_n')$ with $T_j' = \sum_i a_{ij} T_j$.

THEOREM 12.57 (HILBERT). *Let G be a linearly reductive subgroup of GL_n, and let $A = k[T_1, \ldots, T_n]$. Then A^G is finitely generated as a k-algebra.*

PROOF. Let $\mathfrak{a}$ be the ideal of A^G generated by the invariant polynomials of degree > 0. According to the Hilbert basis theorem (CA 3.7), the ideal $\mathfrak{a}A$ is finitely generated, say,

$$\mathfrak{a}A = (g_1, \ldots, g_m),$$

where we have chosen the g_i to be homogeneous elements of $\mathfrak{a}$. Let $f \in A^G$ be homogeneous of degree $d > 0$. We shall prove by induction on d that $f \in k[g_1, \ldots, g_m]$. Let

$$f = r_1 g_1 + \cdots + r_m g_m, \quad a_i \in A, \quad \deg(r_i) < \deg(f).$$

On applying ρ, we find that

$$f = \rho(f) = \rho(r_1)g_1 + \cdots + \rho(r_m)g_m.$$

By the induction hypothesis, the $\rho(r_i)$ lie in $k[g_1, \ldots, g_m]$, and so f lies in $k[g_1, \ldots, g_m]$. □

ASIDE 12.58. A similar argument shows, more generally, that for any linear representation (V, r) of a linearly reductive group G, the ring $\mathrm{Sym}(V)^G$ of invariant polynomials is finitely generated as a k-algebra. As noted above, reductive groups are not necessarily linearly reductive in characteristic p. This was a problem for geometric invariant theory in characteristic p, which was resolved by the proof of the next statement.

> The following conditions on a group variety G are equivalent: (a) G is reductive; (b) for every representation (V, r) of G and nonzero vector v fixed by G, there is a nonzero G-invariant polynomial f without constant term such that $f(v) \neq 0$; (c) for every finitely generated k-algebra A on which G acts linearly, the ring of invariants A^G is finitely generated as a k-algebra.

The key implication (a)⇒(b) was conjectured by Mumford and proved by Haboush (see Mumford et al. 1994).

In the fourteenth of his famous problems, Hilbert asked whether $\mathrm{Sym}(V)^G$ is finitely generated for all group varieties G. Nagata (1960) gave the first counterexample to this, with G a product of thirteen copies of $\mathbb{G}_a$. Since then, many more counterexamples have been found. For a recent paper on the topic, see Totaro 2008.

m. Unirationality

DEFINITION 12.59. An irreducible variety X is said to be **rational** (resp. **unirational**) if its field of rational functions $k(X)$ is a purely transcendental extension of k (resp. contained in a purely transcendental extension of k).

Equivalently, X is rational (resp. unirational) if there exists an isomorphism (resp. a surjective regular map) from an open subset of some affine space $\mathbb{A}^n$ to an open subset of X. If X is unirational and k is infinite, then $X(k)$ is dense in X because this is true of an open subset of $\mathbb{A}^n$.

PROPOSITION 12.60. *Let k' be a finite extension of k. The Weil restriction $(\mathbb{G}_m)_{k'/k}$ of $\mathbb{G}_m$ is rational.*

PROOF. Let $(\mathbb{A}^1)_*$ denote the Weil restriction of $\mathbb{A}^1$, so $(\mathbb{A}^1)_*(R) = k' \otimes R'$ for all k-algebras R. Let $(e_i)_{1 \leq i \leq n}$ be a basis for k' as a k-vector space. For a k-algebra R,
$$k' \otimes R = Re_1 \oplus \cdots \oplus Re_n,$$
and the map sending $\alpha = a_1 e_1 + \cdots + a_n e_n \in k' \otimes R$ to $(a_1, \ldots, a_n) \in R^n$,
$$(\mathbb{A}^1)_*(R) \to \mathbb{A}^n(R),$$
is a bijection natural in R. From this we get an isomorphism of algebraic varieties $(\mathbb{A}^1)_* \to \mathbb{A}^n$. An element α of $(\mathbb{A}^1)_*(R)$ lies in $(\mathbb{G}_m)_{k'/k}(R)$ if and only if its norm $\mathrm{Nm}_{k' \otimes R/R}(\alpha)$ is nonzero. There exists a polynomial $P \in k[X_1, \ldots, X_n]$ such that $\mathrm{Nm}_{k' \otimes R/R}(\alpha) = P(a_1, \ldots, a_n)$, and the isomorphism $(\mathbb{A}^1)_* \to \mathbb{A}^n$ maps $(\mathbb{G}_m)_{k'/k}$ isomorphically onto the complement of the zero set of P in $\mathbb{A}^n$. □

LEMMA 12.61. *Let k' be a finite separable extension of k. Then*

$$X^*((\mathbb{G}_m)_{k'/k}) \simeq \mathbb{Z}^{\text{Hom}_k(k',k^s)} \quad \text{(isomorphism of } \text{Gal}(k^s/k)\text{-modules)}.$$

PROOF. Here $\mathbb{Z}^{\text{Hom}_k(k',k^s)}$ is the free abelian group on the set of k-homomorphisms $k' \to k^s$. An element $\sum n_\sigma \sigma$ of this group corresponds to the character of $(\mathbb{G}_m)_{k'/k}$ that acts on k^s-points as

$$c \otimes a \mapsto (\textstyle\prod_\sigma \sigma(c)^{n_\sigma})a \colon (k' \otimes k^s)^\times \to (k^s)^\times. \qquad \square$$

DEFINITION 12.62. A torus is said to be ***induced*** (or ***quasi-split*** or ***quasi-trivial***) if it is of the form $(\mathbb{G}_m)_{A/k}$ for an étale k-algebra A.

In other words, T is induced if it is a finite product of tori of the form $(\mathbb{G}_m)_{k'/k}$ with k' a finite separable extension of k.

PROPOSITION 12.63. *Every torus T is a quotient of an induced torus.*

PROOF. Let $\Gamma = \text{Gal}(k^s/k)$, and let M be a continuous Γ-module that is finitely generated (as a $\mathbb{Z}$-module). The stabilizer Δ of an element e of M is an open subgroup of Γ, and there is a homomorphism $\mathbb{Z}[\Gamma/\Delta] \to M$ sending 1 to e. On applying this remark to the elements of a finite generating set for M, we get a surjective homomorphism $\prod_i \mathbb{Z}[\Gamma/\Delta_i] \to M$ of continuous Γ-modules (finite product; each Δ_i open). On applying this remark to the dual of $X^*(T)$, and using that the dual of $\mathbb{Z}[\Gamma/\Delta]$ has the same form, we obtain an injective homomorphism

$$X^*(T) \to \bigoplus_i \mathbb{Z}[\Gamma/\Delta_i] \tag{81}$$

of Γ-modules. Let $k_i = (k^s)^{\Delta_i}$. Then $\mathbb{Z}[\Gamma/\Delta_i] \simeq X^*((\mathbb{G}_m)_{k_i/k})$ (see 12.61), and so the map (81) arises from a surjective homomorphism

$$\prod_i (\mathbb{G}_m)_{k_i/k} \to T$$

of tori. $\qquad \square$

PROPOSITION 12.64. *Every torus is unirational, and every induced torus is rational.*

PROOF. Combine 12.60 with 12.63. $\qquad \square$

COROLLARY 12.65. *If T is a torus over an infinite field k, then $T(k)$ is dense in $|T|$.*

PROOF. Combine 12.64 with the remark following 12.59. $\qquad \square$

There exist tori, even over fields of characteristic zero, that are not rational. Later (17.93) we shall use 12.64 to show that every connected group variety over a perfect field is unirational.

Exercises

EXERCISE 12-1. Let D be a diagonalizable group over a field k with characteristic exponent p, and let $X = X(D)$. For an algebraic subgroup D_1 of D, let

$$D_1^{\perp} = \{\chi \in X \mid \chi | D = 1\}.$$

Similarly, for a submodule of X_1 of X, let

$$X_1^{\perp} = \bigcap \{\text{Ker}(\chi) \mid \chi \in X_1\}.$$

(a) Show that the maps $D_1 \mapsto D_1^{\perp}$ and $X_1 \mapsto X_1^{\perp}$ are reciprocal bijections between the set of algebraic subgroups of D and the set of $\mathbb{Z}$-submodules of X.

(b) Show that $X(D_1) = X/D_1^{\perp}$; hence D_1 is connected (resp. smooth) if and only if $X/D_1^{\perp}$ has no prime-to-p torsion (resp. $X/D_1^{\perp}$ has no p torsion).

(c) Show that $X(D/D_1) = D_1^{\perp}$.

EXERCISE 12-2. Let T be a torus, and let S be a subtorus of T. Show that there exists a subtorus S' of T such that $S \cap S'$ is finite and $S \cdot S' = T$. When T is split show that S' can be chosen so that $S \cap S' = e$.

EXERCISE 12-3. Show that every algebraic group of multiplicative type is a subgroup of a torus.

EXERCISE 12-4. Let k'/k be a cyclic Galois extension of degree n with Galois group Γ generated by σ, and let $G = (\mathbb{G}_m)_{k'/k}$.

(a) Show that $X^*(G) \simeq \mathbb{Z}[\Gamma]$ (group algebra $\mathbb{Z} + \mathbb{Z}\sigma + \cdots + \mathbb{Z}\sigma^{n-1}$ of Γ).

(b) Show that

$$\text{End}_{\Gamma}(X^*(G)) = \left\{ \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} \middle| a_i \in \mathbb{Z} \right\}.$$

EXERCISE 12-5. A torus T is said to be ***anistropic*** if $X(T) = 0$; otherwise it is said to be ***isotropic***.

(a) Show that T is anistropic if and only if every morphism $\mathbb{A}^1 \smallsetminus \{0\} \to T$ is constant (i.e., has image a point).

(b) Show that $T^a \overset{\text{def}}{=} \bigcap_{\chi \in X(T)} \text{Ker}(\chi)$ is the largest anisotropic subtorus of a torus T.

EXERCISE 12-6. Let T be a torus over k. Show that there are unique subtori T^a and T^s of T such that T^a is anisotropic, T^s is split, and T is the almost-direct product of T^a and T^s (i.e., $T^a \cap T^s$ is finite and $T^a \cdot T^s = T$).

EXERCISE 12-7. Let T be a torus over $\mathbb{R}$. Show that $T(\mathbb{R})$ is compact if and only if T is anisotropic.

EXERCISE 12-8. Show that an extension of linearly reductive algebraic groups is linearly reductive.

EXERCISE 12-9. Verify that the map in Example 12.55 is a representation of SL_2, and that the representation is not semisimple.

EXERCISE 12-10. Let k' be a finite extension of an infinite field k, and let $G = (\mathbb{G}_m)_{k'/k}$. Show that $G(k)$ is dense in $|G|$. (In fact, this is true whenever G is the Weil restriction of a reductive group; Pink 2004, 1.7.)

Tori Acting on Schemes

Schemes with an action of a torus arise frequently in the theory of algebraic groups. In this chapter, we prove the basic theorems concerning such actions. In particular, we prove the Białynicki-Birula decomposition (13.47), which will allow us to show that the Bruhat decomposition exists on the level of schemes.

Throughout, all schemes are algebraic over the field k. Recall that all algebraic groups are affine.

a. The smoothness of the fixed subscheme

Recall that tori are linearly reductive.

THEOREM 13.1. *Let G be a linearly reductive group variety acting on a smooth variety X over k. Then the fixed-point scheme X^G is smooth.*

We shall need to use some basic results on regular local rings.

13.2. Let A be a local ring with maximal ideal $\mathfrak{m}$ and residue field $\kappa = A/\mathfrak{m}$. Let d denote the Krull dimension of A. Every set of generators for $\mathfrak{m}$ has at least d elements. If there exists a set with d elements, then A is said to be ***regular***, and a set of generators with d elements is called a ***regular system of parameters*** for A (Matsumura 1986, p. 105).

(a) A local ring A is regular if and only if the canonical map

$$\operatorname{Sym}_\kappa(\mathfrak{m}/\mathfrak{m}^2) \to \operatorname{gr}(A) \overset{\text{def}}{=} \bigoplus_{n \geq 0} \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

is an isomorphism (Matsumura 1986, 14.4).

(b) Assume that A is regular. Let $t_1, \ldots, t_d$ be a regular system of parameters for A, and let $\mathfrak{a} = (t_1, \ldots, t_s)$ for some $s \leq d$. Then $A/\mathfrak{a}$ is local of dimension $d - s$; its maximal ideal $\mathfrak{m}/\mathfrak{a}$ is generated by $\{t_{s+1} + \mathfrak{a}, \ldots, t_d + \mathfrak{a}\}$, and so $A/\mathfrak{a}$ is regular. Every regular quotient of A is of this form (Matsumura 1986, 14.2).

We require several lemmas.

LEMMA 13.3. *Let A be a regular local ring of dimension d and $\mathfrak{m}$ the maximal ideal in A. Let $\mathfrak{a}$ be an ideal in A, and let $s \in \mathbb{N}$. If, for every $n \in \mathbb{N}$, there exists a regular system of parameters $t_1, \ldots, t_d$ for A such that*

$$\mathfrak{a} \equiv (t_1, \ldots, t_s) \mod \mathfrak{m}^{n+1}, \tag{82}$$

then $A/\mathfrak{a}$ is regular (of dimension $d - s$).

PROOF. Let $B = A/\mathfrak{a}$, and let $\mathfrak{n}$ denote the maximal ideal $\mathfrak{m}/\mathfrak{a}$ of B. We shall prove that B is regular by showing that, for every $n \geq 1$, the canonical map

$$\mathrm{Sym}^n_{B/\mathfrak{n}}(\mathfrak{n}/\mathfrak{n}^2) \to \mathfrak{n}^n/\mathfrak{n}^{n+1} \tag{83}$$

is an isomorphism. Fix an n, and let $t_1, \ldots, t_d$ be a regular system of parameters for A such that (82) holds. Let $\mathfrak{b} = (t_1, \ldots, t_s)$. By assumption,

$$\mathfrak{a} + \mathfrak{m}^{i+1} = \mathfrak{b} + \mathfrak{m}^{i+1}$$

holds for $i = n$, and therefore also for $i = 1$. Hence,

$$(\mathfrak{b} + \mathfrak{m}) / (\mathfrak{b} + \mathfrak{m}^2) \simeq (\mathfrak{a} + \mathfrak{m}) / (\mathfrak{a} + \mathfrak{m}^2) \simeq \mathfrak{n}/\mathfrak{n}^2,$$
$$(\mathfrak{b} + \mathfrak{m}^n) / (\mathfrak{b} + \mathfrak{m}^{n+1}) \simeq (\mathfrak{a} + \mathfrak{m}^n) / (\mathfrak{a} + \mathfrak{m}^{n+1}) \simeq \mathfrak{n}^n/\mathfrak{n}^{n+1}.$$

The quotient ring $A/\mathfrak{b}$ is regular (13.2b), and so the canonical map

$$\mathrm{Sym}^n_{B/\mathfrak{n}}((\mathfrak{b} + \mathfrak{m}) / (\mathfrak{b} + \mathfrak{m}^2)) \to (\mathfrak{b} + \mathfrak{m}^n) / (\mathfrak{b} + \mathfrak{m}^{n+1})$$

is an isomorphism (13.2a). It follows that the map (83) is an isomorphism. As n was arbitrary, this completes the proof. □

Let S be a set of automorphisms of a separated algebraic k-scheme X. The functor

$$R \rightsquigarrow \{x \in X(R) \mid sx = x \text{ for all } s \in S\}$$

is represented by a closed subscheme X^S of X, namely, by the intersection of the equalizers of the pairs of maps $s, \mathrm{id} \colon X \rightrightarrows X$ for $s \in S$. When S is a subgroup of $\mathrm{Aut}(X)$, this is the fixed subscheme of the constant group functor $R \rightsquigarrow S$.

LEMMA 13.4. *Let S be a set of automorphisms of a smooth variety X and $x \in X(k)$ a fixed point of S. Then $\mathcal{O}_{X^S, x} = \mathcal{O}_{X, x}/\mathfrak{a}$, where*

$$\mathfrak{a} = \{f - f \circ s \mid f \in \mathfrak{m}, s \in S\}.$$

PROOF. Let R be a local k-algebra. Obviously, a local homomorphism $\mathcal{O}_{X, x} \to R$ is fixed by the automorphisms in S if and only if it factors through $\mathcal{O}_{X, x}/\mathfrak{a}$. Thus

$$\mathrm{Hom}(\mathcal{O}_{X, x}/\mathfrak{a}, R) \simeq \mathrm{Hom}(\mathcal{O}_{X, x}, R)^S =_{\mathbb{C}} \mathrm{Hom}(\mathcal{O}_{X^S, x}, R).$$

From this the statement follows. □

LEMMA 13.5. *Let G be a group variety acting on an algebraic variety X, and let S be a subset of $G(k)$ that is dense in $|G|$. If X^S is smooth, then X^G is smooth and equals X^S.*

PROOF. Assume that X^S is smooth. Clearly, $X^G \subset X^S$, and it remains to show that $X^S \supset X^G$. By assumption S is schematically dense in G, hence also in G_{k^a} (see 1.11), and so S is Zariski-dense in $G(k^a)$. Therefore the isotropy group at an $x \in X^S(k^a)$ equals G_{k^a}, and so $X^S(k^a) = X(k^a)^{G(k^a)} = X^G(k^a)$. As X^S is reduced and X^G is closed, this implies that $X^S = X^G$. □

LEMMA 13.6. *Let G be a linearly reductive group variety acting on a smooth variety X, and let S be a subset of $G(k)$ that is dense in $|G|$. Then X^S is smooth.*

PROOF. As S is Zariski-dense in $G(k^a)$ (see the preceding proof), we may suppose that k is algebraically closed. Let $x \in X(k)^S$, and let $\mathfrak{m}$ be the maximal ideal in $\mathcal{O}_{X,x}$. As in the preceding proof, $G(k)$ fixes x, and so it acts on $\mathcal{O}_{X,x}$ by k-algebra automorphisms leaving $\mathfrak{m}$ invariant. For all $n \geq 0$, the action of $G(k)$ on $\mathcal{O}_{X,x}/\mathfrak{m}^n$ arises from a representation of G on the k-vector space $\mathcal{O}_{X,x}/\mathfrak{m}^n$ (cf. the proof of 8.9).

Decompose $V \stackrel{\text{def}}{=} \mathfrak{m}/\mathfrak{m}^2$ into a direct sum $V = V_0 \oplus V_1 \oplus \cdots \oplus V_r$ with V_0 a trivial representation of G and the remaining V_i nontrivial simple representations of G (here we use that G is linearly reductive). Choose any basis $(v_{0j})_j$ for V_0, and choose a basis $(v_{ij})_j$ for V_i ($i \neq 0$) from the set $\{f - f \circ s \mid f \in V_i, s \in S\}$ – this set spans V_i because the representation of S on V_i is nontrivial and simple (by 4.4). We shall apply Lemma 13.3 to the ideal

$$\mathfrak{a} = \{f - f \circ s \mid f \in \mathfrak{m}, \quad s \in G(k)\}$$

in $\mathcal{O}_{X,x}$.

Fix an $n \in \mathbb{N}$. For $i = 0, 1, \ldots, r$, choose a G-stable subspace W_i of $\mathfrak{m}/\mathfrak{m}^{n+1}$ mapping isomorphically onto V_i. Lift each v_{ij} to a $w_{ij} \in W_i$, and then lift w_{ij} to an element $u_{ij} \in \mathfrak{m}$. Thus

$$u_{ij} \mapsto w_{ij} \to v_{ij} \text{ under } \mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^{n+1} \to \mathfrak{m}/\mathfrak{m}^2.$$

Now $\{u_{ij} \mid i \geq 0, \ j \text{ arbitrary}\}$ is a regular system of parameters for $\mathcal{O}_{X,x}$, and its subset $\{u_{ij} \mid i > 0, \ j \text{ arbitrary}\}$ generates $\mathfrak{a}$ modulo $\mathfrak{m}^{n+1}$. As n was arbitrary, this shows that $\mathcal{O}_{X,x}/\mathfrak{a}$ is regular (13.3), and we know (13.4) that $\mathcal{O}_{X^S,x} = \mathcal{O}_{X,x}/\mathfrak{a}$. □

On combining the last two lemmas, we obtain the following theorem.

THEOREM 13.7. *Let G be a linearly reductive group variety acting on a smooth variety X, and let $S \subset G(k)$ be dense in $|G|$. Then X^S is smooth and equals X^G.*

This implies Theorem 13.1 because we may suppose k to be separably closed and take S to be $G(k)$.

COROLLARY 13.8. *Let G be an algebraic group acting on a smooth variety X. Let $s \in G(k)$ be semisimple, and let G' be the closure of the subgroup of $G(k)$ generated by s. Then X^s is smooth, and $X^{G'} = X^s$.*

PROOF. Let (V, r) be a representation of G'. A subspace of V is stable under G' if and only if it is stable under s. It follows that (V, r) is semisimple, and that G' is linearly reductive. Now the theorem applies. □

THEOREM 13.9 (SMOOTHNESS OF CENTRALIZERS). *Let H be a linearly reductive group variety acting on a smooth algebraic group G. Then G^H is smooth.*

PROOF. Special case of Theorem 13.1. □

COROLLARY 13.10. *Let H be a subgroup variety of a group variety G. If H is a multiplicative type, then $C_G(H)$ and $N_G(H)$ are smooth.*

PROOF. Recall (12.30) that multiplicative groups are linearly reductive. Let H act on G by inner automorphisms. Then $G^H = C_G(H)$, and so $C_G(H)$ is smooth. As $C_G(H)^\circ = N_G(H)^\circ$ (see 12.40), $N_G(H)$ is also smooth. □

COROLLARY 13.11. *Let H be a subgroup variety of multiplicative type of a group variety G.*

 (a) *$N_G(H)$ is the unique subgroup variety of G such that $N_G(H)(k^a)$ is the normalizer of $H(k^a)$ in $G(k^a)$.*

 (b) *$C_G(H)$ is the unique subgroup variety of G such that $C_G(H)(k^a)$ is the centralizer of $H(k^a)$ in $G(k^a)$.*

PROOF. Combine 13.10 with 1.88 and 1.95. □

Notes

13.12. The proof of (13.1) follows Iversen 1972. Similar arguments can be used to prove more general statements. For example, let $\mathcal{C}_x(X)$ denote the tangent cone at a point x on an algebraic scheme X over k. If x is fixed by an action of a smooth linearly reductive group G on X, then $\mathcal{C}_x(X^G) = \mathcal{C}_x(X)^G$ (Fogarty 1973, 5.2).

13.13. In each of the following examples (from Fogarty 1973, §6) the fixed scheme for the action is not reduced (hence not smooth):

 (a) $\mathbb{G}_a$ acts on $\mathbb{P}^1$ by $t(x : y) = (x + ty : y)$.

 (b) SL_p acts on SL_p by conjugation ($p = \mathrm{char}(k)$); indeed, $\mathrm{SL}_p^{\mathrm{SL}_p} = \mu_p$.

 (c) $\mathbb{G}_m$ acts suitably on the factorial scheme $X_0^2 + X_1 X_2 \cdots + X_{2n-1} X_{2n} = 0$, $n \geq 2$.

Note that (b) shows that SL_p is not linearly reductive in characteristic p.

13.14. Theorem 13.1 characterizes linearly reductive group varieties: a group variety G is linearly reductive if X^G is smooth whenever X is smooth (Fogarty and Norman 1977).

13.15. Theorem 13.9 holds also for nonsmooth linearly reductive groups H. See Theorem 15.20 below.

13.16. Let G be a reductive group over a field k of characteristic $p \neq 0$. It is known that the centralizers of *all* algebraic subgroups of G are smooth provided p is not in a specific small set of primes depending only on the root datum of G (Bate et al. 2010, Herpel 2013). For example, this is true for GL_V and all p, and it is true for SL_V and all p not dividing the dimension of V.

b.　Limits in schemes

> Let $\mathbb{R}^\times$ act continuously on $\mathbb{R}^n$, and let $a \in \mathbb{R}^n$. If $\lim_{t \to 0} ta$ exists, then it is a fixed point of the action because $t'(\lim_{t \to 0} ta) = \lim_{t \to 0} t'ta = \lim_{t \to 0} ta$. Similarly, if $\lim_{t \to \infty} ta$ exists, then it is fixed by the action. We prove similar statements in an algebraic setting.

Let X be a separated algebraic scheme over k and $\varphi \colon \mathbb{A}^1 \smallsetminus 0 \to X$ a regular map. If φ extends to a regular map $\tilde{\varphi} \colon \mathbb{A}^1 \to X$, then the extension is unique, and we say that $\lim_{t \to 0} \varphi(t)$ exists and set it equal to $\tilde{\varphi}(0)$. Similarly, if φ extends to $\tilde{\varphi} \colon \mathbb{P}^1 \smallsetminus 0 \to X$, then we let $\lim_{t \to \infty} \varphi(g) = \tilde{\varphi}(\infty)$.

When X is affine, φ corresponds to a homomorphism of k-algebras

$$f \mapsto f \circ \varphi \colon \mathcal{O}(X) \to k[T, T^{-1}],$$

and $\lim_{t \to 0} \varphi$ exists if and only if $f \circ \varphi \in k[T]$ for all $f \in \mathcal{O}(X)$. Similarly, $\lim_{t \to \infty} \varphi$ exists if and only if $f \circ \varphi \in k[T^{-1}]$ for all $f \in \mathcal{O}(X)$.

More generally, let R be a k-algebra and $\varphi \colon (\mathbb{A}^1 \smallsetminus 0)_R \to X_R$ a morphism of R-schemes. If φ extends to a morphism $\tilde{\varphi} \colon \mathbb{A}^1_R \to X_R$, then we say that $\lim_{t \to 0} \varphi(t)$ exists and we set it equal to the restriction of $\tilde{\varphi}$ to

$$0_R = \mathrm{Spm}(R[T]/(T)) \subset \mathbb{A}^1_R.$$

Thus, when it exists, $\lim_{t \to 0} \varphi(t)$ is an R-point of X.

In the following, 0 is the closed subscheme $\mathrm{Spm}(k[T]/(T))$ of the affine line $\mathbb{A}^1 = \mathrm{Spm}(k[T])$, and we identify the underlying scheme of $\mathbb{G}_m$ with $\mathbb{A}^1 \smallsetminus 0$.

EXAMPLE 13.17. Let $\mathbb{G}_m$ act on $\mathbb{A}^n$ according to the rule

$$t(x_1, \ldots, x_n) = (t^{m_1} x_1, \ldots, t^{m_n} x_n), \quad t \in \mathbb{G}_m(k), \quad x_i \in k, \quad m_i \in \mathbb{Z}.$$

Assume that the m_i are not all 0. Let $v = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$, and let

$$b_i = \begin{cases} a_i & \text{if } m_i = 0 \\ 0 & \text{otherwise.} \end{cases}$$

The orbit map

$$\mu_v \colon \mathbb{G}_m \to \mathbb{A}^n, \quad t \mapsto (t^{m_1} a_1, \ldots, t^{m_n} a_n)$$

corresponds to the homomorphism of k-algebras

$$k[T_1, \ldots, T_n] \to k[T, T^{-1}], \quad T_i \mapsto a_i T^{m_i}. \tag{84}$$

Suppose first that $m_i \geq 0$ for all i. Then the homomorphism (84) takes values in $k[T]$, and so μ_v extends uniquely to a regular map $\tilde{\mu}_v \colon \mathbb{A}^1 \to \mathbb{A}^n$, namely, to

$$t \mapsto (t^{m_1} a_1, \ldots, t^{m_n} a_n) \colon \mathbb{A}^1 \to \mathbb{A}^n,$$

where we have set $0^0 = \lim_{t \to 0} t^0 = 1$. Note that

$$\lim_{t \to 0} \mu_v(t) \overset{\mathrm{def}}{=} \tilde{\mu}_v(0) = (b_1, \ldots, b_n),$$

which is certainly fixed by the action of $\mathbb{G}_m$ on $\mathbb{A}^n$.

On the other hand, if $m_i \leq 0$ for all i, then the homomorphism (84) maps into $k[T^{-1}]$, and so $\tilde{\mu}_v$ extends uniquely to a regular map $\tilde{\mu}_v \colon \mathbb{P}^1 \smallsetminus \{0\} \to \mathbb{A}^n$ with

$$\lim_{t \to \infty} \mu_v(t) \overset{\mathrm{def}}{=} \tilde{\mu}_v(\infty) = (b_1, \ldots, b_n).$$

Let (V, r) be a finite-dimensional representation of $\mathbb{G}_m$. Then r defines an action of $\mathbb{G}_m$ on the scheme V_a. Let $V = \bigoplus_{i \in \mathbb{Z}} V_i$ denote the decomposition of V into its eigenspaces (so $t \in \mathbb{G}_m(k)$ acts on V_i as t^i). Note that $V_0 = V^{\mathbb{G}_m}$, and that the vector $(b_1, \ldots, b_n)$ in the above example is the component of $(a_1, \ldots, a_n)$ in V_0. The i for which $V_i \neq 0$ are the weights of $\mathbb{G}_m$ on V.

PROPOSITION 13.18. *Let $v \in V$, and let $v = \sum_i v_i$ with $v_i \in V_i$.*
   (a) *If the weights of $\mathbb{G}_m$ on V are ≥ 0, then $\lim_{t \to 0} tv$ exists and equals v_0.*
   (b) *If the weights of $\mathbb{G}_m$ on V are ≤ 0, then $\lim_{t \to \infty} tv$ exists and equals v_0.*
   (c) *The subscheme of V_a on which $\lim_{t \to 0} tv$ exists is $(\bigoplus_{i \geq 0} V_i)_a$, the fixed subscheme is $(V_0)_a$, and the map $v \mapsto \lim_{t \to 0} tv \colon (\bigoplus_{i \geq 0} V_i)_a \to (V_0)_a$ is the natural projection.*

PROOF. Choose a basis of eigenvectors for V, and apply Example 13.17.   □

EXAMPLE 13.19. If the weights of $\mathbb{G}_m$ on V are > 0, then 0 is the unique fixed point for the action, and $\lim_{t \to 0} tv = 0$ for all $v \in V$. If the weights are all < 0, then 0 is again the unique fixed point, but $\lim_{t \to 0} tv$ exists only if $v = 0$.

Similarly, a finite-dimensional representation (V, r) of $\mathbb{G}_m$ defines an action of $\mathbb{G}_m$ on the scheme $\mathbb{P}(V)$:

$$t, [v] \mapsto [tv] \colon \mathbb{G}_m \times \mathbb{P}(V) \to \mathbb{P}(V).$$

Here $[v]$ denotes the image in $\mathbb{P}(V)$ of a nonzero $v \in V$. Obviously, a point $[v]$ of $\mathbb{P}(V)$ is fixed by $\mathbb{G}_m$ if and only if v is an eigenvector.

PROPOSITION 13.20. *Let $v \in V$. The orbit map*

$$\mu_{[v]}: \mathbb{G}_m \to \mathbb{P}(V), \quad t \mapsto t[v],$$

extends uniquely to a regular map $\tilde{\mu}_{[v]}: \mathbb{P}^1 \to \mathbb{P}(V)$. Either $[v]$ is a fixed point or the closure of its orbit in $\mathbb{P}(V)$ has exactly two fixed points, namely, $\lim_{t \to 0} t \cdot [v] = \tilde{\mu}_{[v]}(0)$ and $\lim_{t \to \infty} t \cdot [v] = \tilde{\mu}_{[v]}(\infty)$.

PROOF. Write V as a sum of eigenspaces, $V = \bigoplus_{i \in \mathbb{Z}} V_i$, and let

$$v = v_r + v_{r+1} + \cdots + v_s, \quad v_i \in V_i.$$

If $[v]$ is fixed, then there is nothing to prove, and so we assume that it is moved.

Then $r < s$ and $e = v_r$ is a nonzero vector in V_r. Extend e to a basis $\{e, \ldots\}$ of eigenvectors of V, and let $\{e^\vee, \ldots\}$ be the dual basis (of $V^\vee$). Then $\mathbb{G}_m$ acts on the affine space

$$D(e^\vee) \overset{\text{def}}{=} \{[v] \in \mathbb{P}(V) \mid e^\vee(v) \neq 0\} \approx \mathbb{A}^n$$

with nonnegative weights $0, \ldots, s - r$. According to Proposition 13.18, the orbit map $\mu_{[v]}$ extends to a regular map $\tilde{\mu}: \mathbb{A}^1 \to D(e^\vee)$ with $\tilde{\mu}(0) = [v_r]$ and $[v_r]$ is a fixed point. Similarly, $\mu_{[v]}$ extends to a regular map $\tilde{\mu}: \mathbb{P}^1 \smallsetminus 0 \to \mathbb{P}(V)$ with $\tilde{\mu}(\infty) = [v_s]$ and $[v_s]$ is a fixed point.

It is now obvious that the closure of the orbit of $[v]$ has exactly two boundary points, namely, $[v_r]$ and $[v_s]$, and that these are exactly the fixed points in the closure of the orbit. $\square$

c.   The concentrator scheme in the affine case

Let $\mu: \mathbb{G}_m \times X \to X$ be an action of $\mathbb{G}_m$ on an affine scheme X over k. Such an action defines a $\mathbb{Z}$-gradation

$$\mathcal{O}(X) = \bigoplus_{n \in \mathbb{Z}} \mathcal{O}(X)_n$$

on the coordinate ring $\mathcal{O}(X)$, with $\mathcal{O}(X)_n$ the subspace of $\mathcal{O}(X)$ on which $\mathbb{G}_m$ acts through the character $t \mapsto t^n$.[1] Note that $\mathcal{O}(X)_m \cdot \mathcal{O}(X)_n \subset \mathcal{O}(X)_{m+n}$ for all $m, n \in \mathbb{Z}$, and so this is a gradation of $\mathcal{O}(X)$ as a k-algebra. For $x \in X(k)$, the orbit map $\mu_x: \mathbb{G}_m \to X$ corresponds to the homomorphism of coordinate rings

$$\sum_n f_n \mapsto \sum_n f_n(x) T^n: \mathcal{O}(X) \to k[T, T^{-1}].$$

It follows that $\lim_{t \to 0} tx$ exists if and only if $f_n(x) = 0$ for all $n < 0$. If $\lim_{t \to 0} tx$ exists, then

$$f(\lim_{t \to 0} tx) = f_0(x), \quad \text{all } f \in \mathcal{O}(X). \tag{85}$$

---

[1] We are letting $\mathbb{G}_m$ act on $\mathcal{O}(X)$ on the right: $f^t(x) = f(tx)$. When an algebraic monoid G acts on a scheme X on the *left*, there is only a *right* action of G on $\mathcal{O}(X)$.

Now let Z be a closed subscheme of X stable under the action of $\mathbb{G}_m$. The restriction map $\mathcal{O}(X) \to \mathcal{O}(Z)$ is a homomorphism of graded k-algebras, and so its kernel is a graded ideal $\mathfrak{a} = \bigoplus_{n \in \mathbb{Z}} \mathfrak{a}_n$. From (85) we see that $\lim_{t \to 0} tx \in Z(k)$ if and only if $f_0(x) = 0$ for all $f \in \mathfrak{a}$.

DEFINITION 13.21. Let X be an affine scheme over k with an action of $\mathbb{G}_m$, and let Z be a closed subscheme of X stable under $\mathbb{G}_m$. The ***concentrator scheme*** of Z in X, denoted $X(Z)$, is the closed subscheme of X defined by the ideal generated by $L = \mathfrak{a}_0 + \sum_{n < 0} \mathcal{O}(X)_n$.

It follows from the above discussion that $X(Z)(k)$ consists of the x in $X(k)$ such that $\lim_{t \to 0} tx$ exists and lies in $Z(k)$. Let $A = \mathcal{O}(X(Z))$. Then A is a graded k-algebra, $A = \bigoplus_{n \in \mathbb{N}} A_n$. From the homomorphisms $A_0 \to A \to A/\bigoplus_{n > 0} A_n \simeq A_0$, we obtain morphisms $Z^{\mathbb{G}_m} \to X(Z) \to Z^{\mathbb{G}_m}$. The first is the natural inclusion and the second sends x to $\lim_{t \to 0} tx$.

PROPOSITION 13.22. *Let $x \in X(Z)(k)$. If x is a regular point on X and $\lim_{t \to 0} tx$ is a regular point on Z, then x is a regular point on $X(Z)$.*

The proof is an exercise in commutative algebra which we defer until later in this section.

PROPOSITION 13.23. *When X and Z are smooth, $X(Z)$ is the unique smooth closed subscheme of X such that*

$$X(Z)(k^a) = \{x \in X(k^a) \mid \lim_{t \to 0} tx \text{ exists and lies in } Z(k^a)\}.$$

PROOF. The definition of $X(Z)$ commutes with extension of the base field, which shows that $X(Z)(k^a)$ has the given description. Now Proposition 13.22 applied to X_{k^a} shows that all $x \in X(Z)(k^a)$ are regular, which implies that $X(Z)$ is smooth (A.54). The uniqueness is a consequence of the smoothness. □

We shall need a description of $X(Z)(R)$ for all k-algebras R.

Let X be a scheme over k with an action μ of an algebraic group G. Let R be a k-algebra and let $x \in X(R)$. The ***orbit map*** $\mu_x : G_R \to X$ is defined to be the composite of the maps

$$G \times \mathrm{Spm}(R) \xrightarrow{\mathrm{id} \times x} G \times X \xrightarrow{\mu} X.$$

It is a morphism of k-schemes $G_R \to X$, but we sometimes regard it as a morphism of R-schemes $G_R \to X_R$:

For an R-algebra R', the map $\mu_x(R')$ is

$$g \mapsto g x_{R'} : G(R') \to X(R').$$

When X is affine, the orbit map corresponds to a k-algebra homomorphism $\mathcal{O}(X) \to \mathcal{O}(G) \otimes R$, and hence to an R-algebra homomorphism $\mathcal{O}(X) \otimes R \to \mathcal{O}(G) \otimes R$.

Now let X be an affine scheme over k with an action μ of $\mathbb{G}_m$, and let $x \in X(R)$. Then μ_x is a morphism $\mathbb{G}_{mR} \to X_R$ of R-schemes. Write tx for $\mu_x(t)$. When it exists, $\lim_{t \to 0} tx$ is an R-point of X (see p.).

PROPOSITION 13.24. *In the situation of Definition 13.21, an element x of $X(R)$ lies in $X(Z)(R)$ if and only if $\lim_{t \to 0} tx$ exists and lies in $Z(R)$.*

PROOF. Let $\mathcal{O}(X) = \bigoplus_n \mathcal{O}(X)_n$ be the gradation defined by the action of $\mathbb{G}_m$ on X, and regard $x \in X(R)$ as a homomorphism of k-algebras $\mathcal{O}(X) \to R$. Then μ_x corresponds to the homomorphism of k-algebras

$$\sum_n f_n \mapsto \sum_n x(f_n) T^n : \mathcal{O}(X) \to R[T, T^{-1}].$$

Now the same argument as in the case $R = k$ applies.   □

More formally, we can say that the diagram

$$
\begin{array}{ccc}
X(Z)(R) & \longrightarrow & X(R) \\
\downarrow & & \downarrow b \\
X(R[T]) & \xrightarrow{\ a\ } & X(R[T, T^{-1}])
\end{array}
\tag{86}
$$

is cartesian. Here a is defined by the inclusion $R[T] \hookrightarrow R[T, T^{-1}]$ and b sends an element of $X(R)$ to its orbit map.

Proof of Proposition 13.22

In the following lemmas, A is a noetherian commutative ring with a $\mathbb{Z}$-gradation $A = \bigoplus_{n \in \mathbb{Z}} A_n$, the subring A_0 is a local ring with maximal ideal $\mathfrak{m}_0$, and $\mathfrak{m}$ is the maximal ideal $\mathfrak{m}_0 + \bigoplus_{n \neq 0} A_n$ in A. We let $\kappa = A_0/\mathfrak{m}_0 \simeq A/\mathfrak{m}$.

LEMMA 13.25. *Let M be a finitely generated $\mathbb{Z}$-graded A-module. The following are equivalent: (a) $M = \mathfrak{m}M$; (b) $M_\mathfrak{m} = 0$; (c) $M = 0$.*

PROOF. If $M = \mathfrak{m}M$, then $M_\mathfrak{m} = \mathfrak{m}M_\mathfrak{m}$, and so $M_\mathfrak{m} = 0$ by Nakayama's lemma. Suppose that $M_\mathfrak{m} = 0$, and let x be a homogeneous element of M. By assumption, there exists an $a \in A \smallsetminus \mathfrak{m}$ such that $ax = 0$. Write $a = \sum a_n$ with $a_n \in A_n$. Then $a_n x = 0$ for all n, but a_0 is invertible, and so $x = 0$. Thus $M = 0$. Finally, if $M = 0$, then certainly $M = \mathfrak{m}M$.   □

LEMMA 13.26. *Let $M \supset N$ be finitely generated $\mathbb{Z}$-graded A-modules. The following are equivalent: (a) $M = N + \mathfrak{m}M$; (b) $M_\mathfrak{m} = N_\mathfrak{m}$; (c) $M = N$.*

PROOF. Apply Lemma 13.25 to M/N. □

LEMMA 13.27 (HESSELINK 1981, 5.6). *Let* $\mathfrak{a} \neq A$ *be a graded ideal in* A, *and let* $\mathfrak{b}$ *be the ideal in* A *generated by* $L = \mathfrak{a}_0 + \sum_{n<0} A_n$. *If the local rings* $A_\mathfrak{m}$ *and* $(A/\mathfrak{a})_\mathfrak{m}$ *are regular, then so also is* $(A/\mathfrak{b})_\mathfrak{m}$.

PROOF. Since $\mathfrak{a}$ is graded, it is contained in $\mathfrak{m}$. Let $\mathfrak{n}$ denote the maximal ideal $(\mathfrak{a}+\mathfrak{m})/\mathfrak{a}$ of $A/\mathfrak{a}$, and let d and $d-r$ denote the Krull dimensions of $A_\mathfrak{m}$ and $(A/\mathfrak{a})_\mathfrak{n}$ respectively. From the exact sequence

$$0 \to (\mathfrak{a}+\mathfrak{m}^2)/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2 \to 0$$

we see that $(\mathfrak{a}+\mathfrak{m}^2)/\mathfrak{m}^2$ has dimension r as a κ-vector space. Both $(\mathfrak{a}+\mathfrak{m}^2)/\mathfrak{m}^2$ and $\mathfrak{m}/\mathfrak{m}^2$ are spanned by homogeneous elements. Therefore there are homogeneous elements $x_1, \ldots, x_d$ in $\mathfrak{m}$ such that the images of $x_1, \ldots, x_r$ in $(\mathfrak{a}+\mathfrak{m}^2)/\mathfrak{m}$ form a κ-basis, and the images of $x_1, \ldots, x_d$ in $\mathfrak{m}/\mathfrak{m}^2$ form a κ-basis.

Let $\mathfrak{a}'$ denote the ideal $(x_1, \ldots, x_r)$ in A. The local ring $(A/\mathfrak{a}')_\mathfrak{m}$ is regular of dimension $d-r$ (see 13.2b). It is a quotient of $(A/\mathfrak{a})_\mathfrak{m}$, which is also regular of dimension $d-r$, and so it equals $(A/\mathfrak{a})_\mathfrak{m}$. Hence $\mathfrak{a}A_\mathfrak{m} = \mathfrak{a}'A_\mathfrak{m}$, which implies that $\mathfrak{a} = \mathfrak{a}'$ (see 13.26). Similarly, $\mathfrak{m} = (x_1, \ldots, x_d)$ because $\mathfrak{m}A_\mathfrak{m} = (x_1, \ldots, x_d)A_\mathfrak{m}$.

Let $\mathfrak{b}'$ be the ideal in A generated by those x_i that lie in L, i.e., by the set

$$\{x_i \mid \deg(x_i) < 0 \text{ or } i \leq r \text{ and } \deg(x_i) \leq 0\}.$$

Because $\mathfrak{b}'_\mathfrak{m}$ is generated by a subset of a regular system of parameters, the local ring $(A/\mathfrak{b}')_\mathfrak{m}$ is regular (13.2b). It remains to prove that $\mathfrak{b}' = \mathfrak{b}$. From Lemma 13.26 we see that it suffices to show that $\mathfrak{b} \subset \mathfrak{b}' + \mathfrak{m}\mathfrak{b}$. For this it suffices to show that every element b of L lies in $\mathfrak{b}' + \mathfrak{m}\mathfrak{b}$.

Let $b \in A_n$ with $n < 0$. Then $b \in \mathfrak{m}$, and so $b = \sum_{i=1}^{d} a_i x_i$ with $\deg(a_i) + \deg(x_i) = n$. For every i, we have $\deg(x_i) < 0$ or $\deg(b_i) < 0$, so that $x_i b_i \in \mathfrak{b}' \cup \mathfrak{m}\mathfrak{b}$. This proves that $b \in \mathfrak{b}' + \mathfrak{m}\mathfrak{b}$.

Let $b \in \mathfrak{a}_n$ with $n \leq 0$. We may write $b = \sum_{i=1}^{r} x_i b_i$ with $\deg(x_i) + \deg(b_i) = n$. For every $i \leq r$, we have $\deg(x_i) \leq 0$ or $\deg(b_i) < 0$, so that $x_i b_i \in \mathfrak{b}' \cup \mathfrak{m}\mathfrak{b}$. This proves that $b \in \mathfrak{b}' + \mathfrak{m}\mathfrak{b}$. □

To deduce Proposition 13.22, apply Lemma 13.27 with $A = \mathcal{O}(X)$ and $\mathfrak{a}$ the ideal of Z in $\mathcal{O}(X)$, both localized with respect to the set $A_0 \smallsetminus \mathfrak{m}_0$, where $\mathfrak{m}_0$ is the ideal of the point $\lim_{t\to 0} tx$ in A_0.

d. Limits in algebraic groups

Let G be an algebraic group and $\lambda: \mathbb{G}_m \to G$ a cocharacter of G. Then λ defines an action of $\mathbb{G}_m$ on G:

$$(t, g) \mapsto \lambda(t) g \lambda(t)^{-1}: \mathbb{G}_m \times G \to G.$$

We write $t \cdot g$ for $\text{inn}(\lambda(t))(g) = \lambda(t) g \lambda(t)^{-1}$.

We define $P_G(\lambda)$ to be the concentrator subscheme of G in G. Thus $P_G(\lambda)$ is the closed subscheme of G such that

$$P_G(\lambda)(R) = \{g \in G(R) \mid \lim_{t \to 0} t \cdot g \text{ exists}\}$$

for all k-algebras R. We let $Z_G(\lambda) = C_G(\lambda \mathbb{G}_m)$.

PROPOSITION 13.28. *The subscheme $P_G(\lambda)$ is an algebraic subgroup of G, and*

$$P_G(\lambda) \cap P_G(-\lambda) = Z_G(\lambda).$$

PROOF. For the first assertion it remains to show that $P_G(\lambda)(R)$ is a subgroup of $G(R)$ for all small R, but the maps a and b in diagram (86), p. 262, are group homomorphisms, and so this is obvious. It follows from the definitions of $P_G(\lambda)$ and $P_G(-\lambda)$ that $P_G(\lambda) \cap P_G(-\lambda)$ is the zero set of $\bigoplus_{n \neq 0} \mathcal{O}(X)_n$, but this equals $G^{\mathbb{G}_m} \stackrel{\text{def}}{=} Z_G(\lambda)$.   □

PROPOSITION 13.29. *The subfunctor*

$$R \rightsquigarrow \{g \in G(R) \mid \lim_{t \to 0} t \cdot g \text{ exists and equals } e\}$$

of G is represented by a normal algebraic subgroup $U_G(\lambda)$ of $P_G(\lambda)$.

PROOF. For each R, we have maps $P_G(\lambda)(R) \to G(R[T]) \xrightarrow{T \mapsto 0} G(R)$ and hence a morphism of schemes $P_G(\lambda) \to G$ sending g to $\lim_{t \to 0} t \cdot g$. The scheme U_G is the fibre of this morphism over e. Obviously $U_G(R)$ is a normal algebraic subgroup of $P_G(\lambda)(R)$ for all R.   □

Note that $U_G(\lambda)$ is the concentrator scheme of e in G.

PROPOSITION 13.30. *Let G be a smooth algebraic group over k and λ a cocharacter of G.*

(a) *$P_G(\lambda)$ is the unique smooth algebraic subgroup of G such that*

$$P_G(\lambda)(k^{\mathrm{a}}) = \{g \in G(k^{\mathrm{a}}) \mid \lim_{t \to 0} t \cdot g \text{ exists (in } G(k^{\mathrm{a}}))\}.$$

(b) *$U_G(\lambda)$ is the unique smooth algebraic subgroup of $P(\lambda)$ such that*

$$U_G(\lambda)(k^{\mathrm{a}}) = \{g \in P_G(\lambda)(k^{\mathrm{a}}) \mid \lim_{t \to 0} t \cdot g \text{ exists and equals } e\}.$$

PROOF. Apply Theorem 13.23.   □

EXAMPLE 13.31. Let $G = \mathrm{SL}_2$, and let λ be the homomorphism sending t to $\mathrm{diag}(t, t^{-1})$. Then

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} a & bt^2 \\ \frac{c}{t^2} & d \end{pmatrix},$$

and so $\lim\limits_{t \to 0} \begin{pmatrix} a & bt^2 \\ \frac{c}{t^2} & d \end{pmatrix}$ exists, and equals $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, if and only if $c = 0$. Therefore,

$$P(\lambda) = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right\}, \quad U(\lambda) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}, \quad Z(\lambda) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}$$

$$P(-\lambda) = \left\{ \begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix} \right\}, \quad U(-\lambda) = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \right\}, \quad Z(-\lambda) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}.$$

EXAMPLE 13.32. Let $G = \mathrm{GL}_3$, and let λ be the homomorphism sending t to $\mathrm{diag}(t^{m_1}, t^{m_2}, t^{m_3})$ with $m_1 \geq m_2 \geq m_3$. Then

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \xrightarrow[\mathrm{diag}(t^{m_1}, t^{m_2}, t^{m_3})]{\text{conjugate by}} \begin{pmatrix} a & t^{m_1 - m_2} b & t^{m_1 - m_3} c \\ t^{m_2 - m_1} d & e & t^{m_2 - m_3} f \\ t^{m_3 - m_1} g & t^{m_3 - m_2} h & i \end{pmatrix}.$$

If $m_1 > m_2 > m_3$, then

$$P(\lambda) = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\}, \quad U(\lambda) = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad Z(\lambda) = \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\}.$$

If $m_1 = m_2 > m_3$, then

$$P(\lambda) = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix} \right\}, \quad U(\lambda) = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad Z(\lambda) = \left\{ \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\}.$$

Let G be an algebraic group over k and $\lambda \colon \mathbb{G}_m \to G$ a cocharacter of G. Then $\mathbb{G}_m$ acts on the Lie algebra $\mathfrak{g}$ of G through $\mathrm{Ad} \circ \lambda$. We let $\mathfrak{g}_n(\lambda)$ denote the subspace of $\mathfrak{g}$ on which $\mathbb{G}_m$ acts through the character $t \mapsto t^n$, and we let

$$\mathfrak{g}_-(\lambda) = \bigoplus_{n < 0} \mathfrak{g}_n, \quad \mathfrak{g}_+(\lambda) = \bigoplus_{n > 0} \mathfrak{g}_n.$$

Thus

$$\mathfrak{g} = \mathfrak{g}_-(\lambda) \oplus \mathfrak{g}_0(\lambda) \oplus \mathfrak{g}_+(\lambda).$$

THEOREM 13.33. *Let G be a smooth algebraic group over k, and let $\lambda \colon \mathbb{G}_m \to G$ be a cocharacter of G.*

(a) *The groups $P(\lambda)$, $Z(\lambda)$, and $U(\lambda)$ are smooth algebraic subgroups of G, and $U(\lambda)$ is a normal subgroup of $P(\lambda)$.*

(b) *The multiplication map $U(\lambda) \rtimes Z(\lambda) \to P(\lambda)$ is an isomorphism of algebraic groups.*

(c) $\mathrm{Lie}(Z(\lambda)) = \mathfrak{g}_0(\lambda)$, $\mathrm{Lie}(U(\pm\lambda)) = \mathfrak{g}_\pm(\lambda)$, $\mathrm{Lie}(P(\lambda)) = \mathfrak{g}_0(\lambda) \oplus \mathfrak{g}_+(\lambda)$.

(d) *The multiplication map $U(-\lambda) \times P(\lambda) \to G$ is an open immersion of algebraic varieties.*

(e) *If G is connected, then so are $P(\lambda)$, $Z(\lambda)$, and $U(\lambda)$.*

PROOF. Theorem 13.1 shows that $Z(\lambda)$ is smooth, and Theorem 13.23 shows that $P(\lambda)$ and $U(\lambda)$ are smooth. We already know that $U(\lambda)$ is normal in $P(\lambda)$.

We first consider the case $G = \mathrm{GL}_V$. According to Theorem 12.12, there exists a basis for V such that $\lambda(\mathbb{G}_m) \subset \mathbb{D}_n$, say,

$$\lambda(t) = \mathrm{diag}(t^{m_1}, \ldots, t^{m_n}), \quad m_1 \geq \cdots \geq m_n.$$

Then $P(\lambda)$ is defined as a subscheme of GL_n by the vanishing of the coordinate functions T_{ij} for which $m_i - m_j < 0$. Obviously, it is smooth and connected. Similarly, $U(\lambda)$ is smooth and connected because it is defined by the equations $T_{ii} = 0$ (all i) and $T_{ij} = 0$ ($m_i - m_j \leq 0$, $i \neq j$). The map $P(\lambda) \to Z(\lambda)$ sending g to $\lim_{t \to 0} tg$ is a homomorphism that is the identity on $Z(\lambda)$ and has kernel $U(\lambda)$. This proves (b). Statement (c) can be proved by a direct calculation using the description of the Lie algebra in terms of dual numbers. From (c) we deduce that the multiplication map $U(-\lambda) \times P(\lambda) \to G$ induces an isomorphism on the tangent spaces at the identity elements; in particular it is dominant. It is also injective because $U(-\lambda) \cap P(\lambda) = e$ (intersection as functors, and hence also as schemes). Finally, $U(-\lambda) \times P(\lambda) \to U(-\lambda) \cdot P(\lambda)$ is an orbit map for an action of $U(-\lambda) \times P(\lambda)$ on G, and hence it is an isomorphism from $U(-\lambda) \times P(\lambda)$ onto an open subset of the closure G of its image (1.65).

We now consider the general case. Embed G in $H = \mathrm{GL}_V$ for some V. Then λ is also a cocharacter of H, and, with the obvious notation,

$$P_G(\lambda) = P_H(\lambda) \cap G, \quad U_G(\lambda) = U_H(\lambda) \cap G, \quad Z_G(\lambda) = Z_H(\lambda) \cap G,$$

because this is true for the functors they define. Therefore (see 10.14)

$$\mathrm{Lie}(P_G(\lambda)) = \mathrm{Lie}(P_H(\lambda)) \cap \mathfrak{g} = \mathfrak{g}_0(\lambda) + \mathfrak{g}_+(\lambda), \tag{87}$$

$$\mathrm{Lie}(U_G(\pm\lambda)) = \mathrm{Lie}(U_H(\pm\lambda)) \cap \mathfrak{g} = \mathfrak{g}_\pm, \tag{88}$$

$$\mathrm{Lie}(Z_G(\lambda)) = \mathrm{Lie}(Z_H(\lambda)) \cap \mathfrak{g} = \mathfrak{g}_0 \tag{89}$$

because we know (c) for H. This proves (c) for G. The map

$$g \mapsto \lim_{t \to 0} tg : G \to Z_G(\lambda)$$

is the restriction to G of the similar map for H, and therefore is the identity on $Z_G(\lambda) = Z_H(\lambda) \cap G$ and has kernel $U_H(\lambda) \cap G = U_G(\lambda)$. This proves (b) for G. Statement (c) for G implies (d) as in the case of GL_n, and statement (d) obviously implies (e). $\square$

PROPOSITION 13.34. *Let $\varphi : G \to G'$ be a surjective homomorphism of connected group varieties. Let λ be a cocharacter of G, and let $\lambda' = \varphi \circ \lambda$. Then*

$$\varphi(P_G(\lambda)) = P_{G'}(\lambda'), \quad \varphi(U_G(\lambda)) = U_{G'}(\lambda').$$

PROOF. From the definitions of the groups, we see that φ maps $P_G(\lambda)$ into $P_{G'}(\lambda')$ and $U_G(-\lambda)$ into $U_{G'}(-\lambda')$. It follows from Theorem 13.33(d) that the product of the homomorphisms $P_G(\lambda) \to P_{G'}(\lambda')$ and $U_G(-\lambda) \to U_{G'}(-\lambda')$ is dominant, and hence surjective (1.71). Therefore each map is surjective. □

NOTES. Modulo nilpotents, Theorem 13.33 was announced in Borel and Tits 1978. Our proof is adapted from that in Springer 1998, 13.4.2. For an extension to nonsmooth algebraic groups G, see Conrad et al. 2015, 2.1.8.

e. Luna maps

Luna maps

The Zariski topology is too coarse for many purposes. For example, the implicit function theorem fails, and smooth varieties of the same dimension need not be locally isomorphic. However, these statements become true when the Zariski topology is replaced by the étale topology.

Let Y and X be varieties over k, and let $P \in Y(k)$. When Y and X are smooth, a regular map $\varphi \colon Y \to X$ is said to be **étale** at $P \in Y(k)$ if the map $(d\varphi)_P \colon \mathrm{Tgt}_P(Y) \to \mathrm{Tgt}_{\varphi(P)}(X)$ on tangent spaces is an isomorphism. In general, we say φ is **étale** at P if the map $\hat{\mathcal{O}}_{X,\varphi(P)} \to \hat{\mathcal{O}}_{Y,P}$ on the completions of the local rings is an isomorphism.

LEMMA 13.35. *Let $x \in X(k)$ be a smooth point on a connected affine algebraic variety X of dimension d over k. Then there exists a regular map $\varphi \colon X \to \mathbb{A}^d$ étale at x.*

PROOF. Let $\mathfrak{m} \subset \mathcal{O}(X)$ be the maximal ideal at x. Recall that $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathrm{Tgt}_x(X)^\vee$. Because x is smooth, there exist regular functions $f_1, \ldots, f_d \in \mathfrak{m}$ whose images in $\mathfrak{m}/\mathfrak{m}^2$ span it as a k-vector space. This means that $(df_1)_x, \ldots, (df_d)_x$ form a basis for $\mathrm{Tgt}_x(V)^\vee$. The map $(f_1, \ldots, f_d) \colon U \to \mathbb{A}^d$ is étale at x because $\mathrm{Tgt}_x(U) \to \mathrm{Tgt}_{(0,\ldots,0)}(\mathbb{A}^d)$ is dual to the map $(dT_i)_{(0,\ldots,0)} \mapsto (df_i)_x$. □

The proof of the lemma can be stated more abstractly as follows: let W be a finite-dimensional k-subspace of $\mathfrak{m}$ mapping isomorphically onto $\mathfrak{m}/\mathfrak{m}^2 = \mathrm{Tgt}_x(X)^\vee$, and let $\alpha \colon (\mathrm{Tgt}_x X)^\vee \to W$ be the inverse isomorphism; the inclusion of W into $\mathcal{O}(X)$ extends uniquely to a homomorphism of k-algebras $\mathrm{Sym}(W) \to \mathcal{O}(X)$, and the composite of this with $\mathrm{Sym}(\alpha)$ is a homomorphism of k-algebras

$$\mathrm{Sym}((\mathrm{Tgt}_x X)^\vee) \to \mathcal{O}(X),$$

which defines a regular map $\varphi \colon X \to (\mathrm{Tgt}_x X)_{\mathfrak{a}}$. This map sends x to 0 and is étale at x.

LEMMA 13.36. *Let $G \times X \to X$ be an action of an algebraic group G on an affine algebraic scheme X over k. Let $x \in X(k)$ be a smooth point of X such that the isotropy group G_x is linearly reductive. Then there exists a regular map $\varphi \colon X \to (\mathrm{Tgt}_x X)_{\mathfrak{a}}$ such that*

(a) φ commutes with the actions of G_x,

(b) φ is étale at x, and

(c) $\varphi(x) = 0$.

PROOF. Let $\mathfrak{m}$ be the maximal ideal at x in $\mathcal{O}(X)$. The quotient map $\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2$ commutes with the actions of G_x. As G_x is linearly reductive, it has a section. This means that there exists a k-subspace W of $\mathfrak{m}$, stable under G_x, mapping isomorphically onto $\mathfrak{m}/\mathfrak{m}^2$. The map $\varphi: X \to (\mathrm{Tgt}_x X)_\mathfrak{a}$ defined by W (as above) has the required properties.   □

The map φ in the lemma depends on the choice of a G_x-stable complement W to $\mathfrak{m}^2$ in $\mathfrak{m}$. A map $\varphi: X \to (\mathrm{Tgt}_x X)_\mathfrak{a}$ arising in this way is called a ***Luna map***. Note that G_x is of multiplicative type, hence linearly reductive, if G is of multiplicative type.

EXAMPLE 13.37. Let $\mathbb{G}_m$ act on $X = \mathbb{A}^n$ according to the rule

$$t(x_1, \ldots, x_n) = (t^{m_1} x_1, \ldots, t^{m_n} x_n), \quad m_i > 0.$$

The only fixed point is $o = (0, \ldots, 0)$. The maximal ideal at o in $\mathcal{O}(X) = k[T_1, \ldots, T_n]$ is $\mathfrak{m} = (T_1, \ldots, T_n)$, and the weights of $\mathbb{G}_m$ acting on $\mathfrak{m}/\mathfrak{m}^2$ are $m_1, \ldots, m_n$. The k-vector space W spanned by the symbols T_i is a $\mathbb{G}_m$-stable complement to $\mathfrak{m}^2$ in $\mathfrak{m}$, and the corresponding Luna map $X \to \mathrm{Sym}(W)$ is the identity map $\mathbb{A}^n \to \mathbb{A}^n$. Note that the weights of $\mathbb{G}_m$ on $\mathrm{Tgt}_o(X)$ are $m_1, \ldots, m_n$.

Monoids and gradations by monoids

LEMMA 13.38. *The following conditions on a finitely generated submonoid S of a free $\mathbb{Z}$-module M of finite rank are equivalent:*

(a) *the set $S \smallsetminus \{0\}$ is a semigroup;*

(b) *a sum $m_1 s_1 + \cdots + m_n s_n$, $s_i \in S \smallsetminus \{0\}$, $m_i \in \mathbb{N}$, is zero only if all m_i are zero;*

(c) *there exists a basis $e_1, \ldots, e_n$ for M such that $S \subset \left\{ \sum_i m_i e_i \mid m_i \in \mathbb{N} \right\}$.*

PROOF. The implications (c)⇒(b)⇒(a) are obvious. An elementary proof of the implication (a)⇒(c) can be found in Kambayashi and Russell 1982, 1.6.   □

LEMMA 13.39 (NAKAYAMA'S LEMMA, GRADED CASE). *Let $A = \bigoplus_{s \in S} A_s$ be a k-algebra graded by S, where S is a monoid satisfying the equivalent conditions of 13.38. Let $I = \bigoplus_{s \neq 0} A_s$. For any graded A_0-submodule E of A such that $I = E \oplus I^2$, the canonical map $\mathrm{Sym}_{A_0}(E) \to A$ is surjective.*

PROOF. Because $S \smallsetminus \{0\}$ is a semigroup, I is an ideal. We identify S with a submonoid of $\sum \mathbb{N} e_i \subset \mathbb{Z}^r$. For an element $s = \sum m_i e_i$ of S, let $t(s) = \sum_i m_i \in \mathbb{N}$. The image of $\mathrm{Sym}_{A_0}(E) \to A$ is the A_0-subalgebra $A_0[E]$ generated by E. Let $a \in A_s$. We shall prove by induction on $t(s)$ that $a \in k[E]$. Certainly this

is true if $s = 0$, and so we may suppose that $a \in I$. There exists an $e \in E$ such that $a - e \in I^2$, and so we may suppose that $a \in I^2$. Write $a = \sum_i b_i c_i$ with b_i and c_i homogeneous elements of I. The equality still holds when we omit any terms $b_i c_i$ with $\deg(b_i) + \deg(c_i) \neq s$. For the remaining terms, $t(b_i) < t(s)$ and $t(c_i) < t(s)$, and so $b_i, c_i \in k[E]$. $\qquad\square$

Varieties with a strictly definite torus action

DEFINITION 13.40. Let T be a torus over k. An action of T on a vector space V (possibly infinite-dimensional) is ***definite*** if there exists a basis $e_1, \ldots, e_n$ for $X^*(T)$ such that the set S of weights of T_{k^s} on V_{k^s} is contained in $\sum \mathbb{N} e_i$; it is ***strictly definite*** if in addition $0 \notin S$. An action of T on an affine algebraic scheme X is ***definite*** if the action of T on $\mathcal{O}(X)$ is definite.

THEOREM 13.41. *Let X be a geometrically connected affine algebraic variety over k equipped with an action of a torus T, and let $x \in X(k)$ be a smooth point fixed by T. If the action of T on $\mathrm{Tgt}_x X$ is strictly definite, then $X^T = \{x\}$ and every Luna map $\varphi: X \to (\mathrm{Tgt}_x X)_{\mathfrak{a}}$ is an isomorphism.*

PROOF. We may suppose that k is algebraically closed. We assume first that X is irreducible. Let $A = \mathcal{O}(X)$ and let $\mathfrak{m} \subset A$ be the maximal ideal at x. Then $A = \bigoplus_{s \in X(T)} A_s$ and $\mathfrak{m} = \bigoplus_{s \in X(T)} \mathfrak{m}_s$ where $t \in T(k)$ acts on A_s and $\mathfrak{m}_s$ as multiplication by $s(t)$. As $A/\mathfrak{m} = k$, we have $A_s = \mathfrak{m}_s$ for all $s \neq 0$. Let φ be the Luna map defined by a $\mathbb{G}_m$-stable complement W to $\mathfrak{m}^2$ in $\mathfrak{m}$. We have $W = \bigoplus_{s > S} W_s$. The canonical map

$$\mathrm{Sym}^j(W) \to \mathfrak{m}^j / \mathfrak{m}^{j+1}$$

is surjective, and so $(\mathfrak{m}^j / \mathfrak{m}^{j+1})_s = 0$ for $s \notin S$.

Because X is irreducible, A is an integral domain; hence it embeds into $A_{\mathfrak{m}}$, and the Krull intersection theorem for $A_{\mathfrak{m}}$ (CA 3.16) implies that $\bigcap_{j \geq 0} \mathfrak{m}^j = 0$. Therefore a nonzero element of $\mathfrak{m}$ of weight s gives a nonzero element of weight s in $\mathfrak{m}^j / \mathfrak{m}^{j+1}$ for some j. It follows that $\mathfrak{m}_s = 0$ for $s \notin S$. Now

$$A_0 = k, \quad A_s = 0 \quad \text{for } s \notin S, \quad \mathfrak{m} = \bigoplus_{s \in S} A_s,$$

and so the graded Nakayama lemma (13.39) shows that the canonical map

$$\mathrm{Sym}_k(W) \to A$$

is surjective, which means that the Luna map

$$\varphi: X \to \mathrm{Spm}(\mathrm{Sym}_k(W)) \simeq (\mathrm{Tgt}_x X)_{\mathfrak{a}}$$

is a closed immersion. As $\dim(X) = \dim \mathrm{Tgt}_x(X)$, it is an isomorphism.

Let $\lambda: \mathbb{G}_m \to T$ be a homomorphism such that $\langle s, \lambda \rangle > 0$ for all $s \in S$. Then the weights of $\mathbb{G}_m$ on $\mathrm{Tgt}_x X$ are strictly positive and so $\lim_{t \to 0} tz = 0$ for all

$z \in \mathrm{Tgt}_x X$ (see 13.37). It follows that $\lim_{t \to 0} tz = x$ for all $z \in X$, and so x is the unique fixed point in X. This completes the proof when X is irreducible.

We now assume only that X is connected. Because T is connected, every irreducible component of X is stable under T. Let X_1 be an irreducible component of X containing x. Then $x = \lim_{t \to 0} tz$ for all $z \in X_1$ (see above). Let X' be a second irreducible component of X. Then $X_1 \cap X'$ is a nonempty closed subset of X_1 stable under T. Let $z \in X_1 \cap X'$; then $x = \lim_{t \to 0} tz \in X_1 \cap X'$. Therefore x lies in X', and in every other irreducible component of X. Let $X_1, \dots, X_n$ be the irreducible components of X. Then X_i corresponds to a (minimal) prime ideal $\mathfrak{p}_i \subset \mathfrak{m}_x$ in A, and $\bigcap_i \mathfrak{p}_i = 0$ (because X is reduced). From the Krull intersection theorem applied to the rings $A/\mathfrak{p}_i$, we find that $\bigcap_{j \geq 0} \mathfrak{m}^j \subset \mathfrak{p}_i$ for all i, and so $\bigcap_{j \geq 0} \mathfrak{m}^j = 0$. Now the same argument as in the irreducible case applies. $\qquad \square$

COROLLARY 13.42. *Let* $\varphi \colon X \to Y$ *be a morphism of connected affine varieties over* k, *equivariant with respect to actions of a torus* T. *If there is a smooth fixed point* $x \in X(k)$ *such that* φ *is étale at* x *and the action of* T *on* $\mathrm{Tgt}_x(X)$ *is strictly definite, then* φ *is an isomorphism.*

PROOF. Because φ is étale at x, the image $\varphi(x)$ of x in Y is smooth and the map on tangent spaces $d\varphi \colon \mathrm{Tgt}_x(X) \to \mathrm{Tgt}_{\varphi(x)}(Y)$ is an equivariant isomorphism. It follows that there is a commutative diagram

$$
\begin{array}{ccc}
X & \xrightarrow{\ \varphi\ } & Y \\
\downarrow & & \downarrow \\
\mathrm{Tgt}_x(X) & \xrightarrow{\ d\varphi\ } & \mathrm{Tgt}_{\varphi(x)}(Y)
\end{array}
$$

in which the vertical arrows are Luna maps, and hence isomorphisms. $\qquad \square$

Varieties with a definite torus action

Before proving the next theorem, we need a result from algebraic geometry.

LEMMA 13.43. *Let* Z *be the closed subscheme of an affine scheme* X *defined by an ideal* $I \subset \mathcal{O}(X)$. *If* X *and* Z *are both smooth, then* I/I^2 *is a finitely generated projective* $\mathcal{O}(Z)$-*module.*

PROOF. As $\mathcal{O}(X)$ is noetherian, I is finitely generated as an $\mathcal{O}(X)$-module, and so its quotient I/I^2 is finitely generated as an $\mathcal{O}(X)/I$-module. Let $z \in Z$. Let $\mathfrak{m}_z$ be the ideal at z in $\mathcal{O}(X)$ and $\mathfrak{n}_z$ the ideal at z in $\mathcal{O}(Z)$. There is an exact sequence

$$0 \to (I/I^2) \otimes_{\mathcal{O}(Z)} \kappa(z) \to \mathfrak{m}_z/\mathfrak{m}_z^2 \to \mathfrak{n}_z/\mathfrak{n}_z^2 \to 0,$$

and so $\dim_{\kappa(z)}((I/I^2) \otimes_{\mathcal{O}(Z)} \kappa(z)) = \dim X - \dim Z$. In particular, the dimension of $(I/I^2) \otimes_{\mathcal{O}(Z)} \kappa(z)$ as a $\kappa(z)$-vector space is independent of z. This implies that I/I^2 is projective (CA 12.6). See also Hartshorne 1977, II, 8.17. $\qquad \square$

Let X be a geometrically integral affine algebraic scheme over k with an action of a split torus T. Then $\mathcal{O}(X) = \bigoplus_{s \in S} \mathcal{O}(X)_s$ with S a submonoid of $X(T)$. If the action of T on X is definite, then $I \overset{\text{def}}{=} \bigoplus_{s \neq 0} \mathcal{O}(X)_s$ is an ideal in $\mathcal{O}(X)$ and $\mathrm{Spm}(\mathcal{O}(X)/I)$ is the closed subscheme X^T of X. Moreover, the composite of the maps

$$\mathcal{O}(X)_0 \to \mathcal{O}(X) \to \mathcal{O}(X)/I$$

is an isomorphism. In particular, we have a "retraction" map $X \to X^T$. When T is nonsplit, we still have a decomposition $\mathcal{O}(X) = \mathcal{O}(X)_0 \oplus I$, and hence a retraction map.

THEOREM 13.44. *Let X be a smooth geometrically connected affine scheme over k with an action of a split torus T. If the action of T on X is definite, then the retraction map $\gamma \colon X \to X^T$ realizes X as a vector bundle over X^T. More precisely, every point $x_0 \in X^T$ has an open neighbourhood U such that the restriction of γ to $\gamma^{-1}(U)$ is isomorphic to the projection map $U \times (\mathrm{Tgt}_{x_0} X)_{\mathfrak{a}} \to U$:*

PROOF. Let $A = \mathcal{O}(X)$, so that $I = \bigoplus_{s \neq 0} A_s$. According to Theorem 13.1, the fixed scheme $X^T = \mathrm{Spm}(A/I)$ is smooth. Therefore, the A_0-module I/I^2 is finitely generated and projective, and its rank is $\dim X - \dim X^T$. The quotient map $I \to I/I^2$ is a homomorphism of graded A-modules. Hence, A_s maps onto $(I/I^2)_s$ for every nonzero $s \in S$. The A_0-module $(I/I^2)_s$ is projective because it is a direct summand of I/I^2, and so the surjection $A_s \to (I/I^2)_s$ admits a section $\gamma_s \colon (I/I^2)_s \to A_s$. Let E_s denote the image of γ_s, and let $E = \bigoplus_{s \neq 0} E_s$. Then E is a graded A_0-submodule of I such that $I = E \oplus I^2$. Now the graded Nakayama lemma (13.39) shows that the map $\mathrm{Sym}_{A_0}(E) \to A$ defined by the inclusion $i \colon E \hookrightarrow A$ is surjective. On the other hand, $\mathrm{Sym}_{A_0}(E)$ is an integral domain over k of transcendence degree equal to

$$\mathrm{tr.deg.}(A_0) + \mathrm{rank}_{A_0}(I/I^2) = \dim X^T + (\dim X - \dim X^T) = \dim X.$$

Therefore the map $\mathrm{Sym}_{A_0}(E) \to A$ is an isomorphism. We now have A_0-isomorphisms

$$\mathrm{Sym}_{A_0}(I/I^2) \simeq \mathrm{Sym}_{A_0}(E) \simeq A \tag{90}$$

realizing $X = \mathrm{Spm}(A)$ as a vector bundle over $X^T = \mathrm{Spm}(A_0)$. As T acts as a group of A_0-linear automorphisms on the projective module I/I^2 and since $I/I^2 \to A$ is T-equivariant (because it preserves weights), the isomorphisms (90) are T-equivariant, which proves the last assertion of the theorem.

When we replace A_0 with a suitable ring of fractions, then I/I^2 becomes free, and in fact $I/I^2 \simeq A_0 \otimes \mathrm{Tgt}_{x_0}(X)^\vee$. From this we obtain an isomorphism $\mathrm{Sym}_{A_0}(I/I^2) \simeq A_0 \otimes_{\kappa(x_0)} \mathrm{Sym}_{\kappa(x_0)}(\mathrm{Tgt}_0(X)^\vee)$. □

NOTES. The terminology in 13.40 was suggested by Białynicki-Birula 1973, p. 482. Theorem 13.44 is from Kambayashi and Russell 1982.

f. The Białynicki-Birula decomposition

DEFINITION 13.45. An action of a torus T on a scheme X over k is ***locally affine*** if X admits a covering by T-invariant open affine subschemes.

Recall (7.26) that an action of a torus T on a scheme X is linear if there exists a representation (V, r) of G and a G-equivariant immersion $X \to \mathbb{P}(V)$. The next lemma shows that linear actions of split tori are locally affine.

LEMMA 13.46. *Let (V, r) be a finite-dimensional representation of a split torus T. Then $\mathbb{P}(V)$ admits a covering by T-stable open affine subsets.*

PROOF. Let $\{e_1, \ldots, e_n\}$ be a basis of eigenvectors for the action of T on V and $\{e_1^\vee, \ldots, e_n^\vee\}$ the dual basis (of $V^\vee$). Then the sets $D(e_i^\vee) \overset{\text{def}}{=} \{[v] \in \mathbb{P}(V) \mid e_i^\vee(v) \neq 0\}$ form a covering with the required properties. □

Let X be a scheme equipped with an action of $\mathbb{G}_m$, and let $x \in X(k)$. If x is fixed by $\mathbb{G}_m$, then $\mathbb{G}_m$ acts on the tangent space $\mathrm{Tgt}_x X$, which therefore decomposes into a direct sum

$$\mathrm{Tgt}_x X = \bigoplus_{i \in \mathbb{Z}} \mathrm{Tgt}_x(X)_i$$

of eigenspaces (so $t \in T(k)$ acts on $\mathrm{Tgt}_x(X)_i$ as multiplication by t^i). Let

$$\mathrm{Tgt}_x^+ X = \bigoplus_{i>0}(\mathrm{Tgt}_x X)_i \quad \text{(contracting subspace)}$$

$$\mathrm{Tgt}_x^- X = \bigoplus_{i<0}(\mathrm{Tgt}_x X)_i.$$

THEOREM 13.47 (BIAŁYNICKI-BIRULA DECOMPOSITION). *Let X be a smooth algebraic variety over k equipped with a locally affine action of $\mathbb{G}_m$.*

(a) *Let Z be a connected component of $X^{\mathbb{G}_m}$. There exist a unique smooth subvariety $X(Z)$ of X such that*

$$X(Z)(k^a) = \{y \in X(k^a) \mid \lim_{t \to 0} ty \text{ exists and lies in } Z(k^a)\}$$

and a unique regular map $\gamma_Z \colon X(Z) \to Z$ sending $y \in X(Z)(k^a)$ to the limit $\lim_{t \to 0} ty \in Z(k^a)$.

(b) *The map γ_Z realizes $X(Z)$ as a fibre bundle over Z. More precisely, every point $z \in Z(k)$ has an open neighbourhood U such that the restriction of γ_Z to $\gamma_Z^{-1}(U)$ is isomorphic over U to the projection $U \times (\mathrm{Tgt}_z^+(X))_{\mathfrak{a}} \to U$.*

(c) *The topological space $|X|$ is a disjoint union of the locally closed subsets $|X(Z)|$ as Z runs over the connected components of $X^{\mathbb{G}_m}$.*

PROOF. We prove this in the next section.   □

COROLLARY 13.48. *Let X be a smooth algebraic variety over k with an action of $\mathbb{G}_m$, and let $z \in X(k)$ be a fixed point for the action. There exists a unique smooth closed subscheme $X(z)$ of X such that*

$$X(z)(k^{\mathrm{a}}) = \{x \in X(k^{\mathrm{a}}) \mid \lim_{t \to 0} tx = z\}.$$

Moreover, $\mathrm{Tgt}_z(X(z)) = \mathrm{Tgt}_z^+(X)$, the fixed subscheme $X(z)^{\mathbb{G}_m} = \{z\}$, and every Luna map $X(z) \to \mathrm{Tgt}_z^+(X)_{\mathfrak{a}}$ is an isomorphism.

PROOF. Let Z be a connected component of $X^{\mathbb{G}_m}$ containing z. Then the fibre $X(z)$ of $X(Z) \to Z$ over z has the required properties.   □

The following diagram illustrates the theorem and corollary:

$$X(Z) \longleftrightarrow X(Z)_U \xrightarrow{\approx} U \times (\mathrm{Tgt}_z^+ X)_{\mathfrak{a}} \qquad X(Z)_z \xrightarrow{\ \mathrm{Luna}\ } (\mathrm{Tgt}_z^+ X)_{\mathfrak{a}}$$

with vertical maps to $Z \longleftarrow U$ and projection, and a second diagram with vertical map to z.

We say that $X^{\mathbb{G}_m}$ is finite and constant if $X^{\mathbb{G}_m}$ is finite as a scheme over k and $X^{\mathbb{G}_m}(k) = X^{\mathbb{G}_m}(k^{\mathrm{a}})$. When X is smooth, this means that $X^{\mathbb{G}_m}$ is a constant étale scheme.

COROLLARY 13.49. *Let X be a smooth connected scheme over k with a locally affine action of $\mathbb{G}_m$ such that $X^{\mathbb{G}_m}$ is finite and constant.*

(a) *For each $x \in X^{\mathbb{G}_m}(k)$, there is a unique smooth subscheme $X(x)$ of X such that*

$$X(x)(k^{\mathrm{a}}) = \{y \in X(k^{\mathrm{a}}) \mid \lim_{t \to 0} ty \text{ exists and equals } x\}.$$

The tangent space to $X(x)$ at x is the subspace $\mathrm{Tgt}_x^+(X)$ of $\mathrm{Tgt}_x(X)$, and every Luna map $X(x) \to \mathrm{Tgt}_x^+(X)$ is an isomorphism.

(b) *The topological space $|X|$ is a disjoint union of locally closed subsets $|X(x)|$ for $x \in X^G(k)$.*

(c) *There is a unique $x_- \in X^{\mathbb{G}_m}(k)$ (called the attracting point) such that $X(x_-)$ is open and dense in X, and a unique $x_+ \in X^{\mathbb{G}_m}(k)$ (called the repelling point) such that $X(x_+) = \{x_+\}$.*

PROOF. Statement (a) is a special case of the theorem. The union in (b) is finite, and each set $X(x)$ is open in its closure, and so there is a unique point x_- such that $X(x_-)$ is dense in X. Note that, for $x \in X^{\mathbb{G}_m}$,

$$X(x) \text{ is dense in } X \iff X(x) \text{ is open in } X$$
$$\iff \operatorname{Tgt}_x(X) = \operatorname{Tgt}_x^+(X)$$
$$\iff \dim(X(x)) = \dim(X).$$

By considering the reciprocal action (i.e., composing with $t \mapsto t^{-1}$), we see that there is a unique point x_+ such that $\operatorname{Tgt}_{x_+}(X) = \operatorname{Tgt}_x^-(X)$. Note that, for $x \in X$,

$$\operatorname{Tgt}_x(X) = \operatorname{Tgt}_x^-(X) \iff \dim(X(x_+)) = 0 \iff X(x_+) = \{x^+\}. \qquad \square$$

EXAMPLE 13.50. Let $\mathbb{G}_m$ act on $X = \mathbb{P}^n$ according to the rule

$$t(x_0:\cdots:x_i:\cdots:x_n) = (t^{r_0}x_0:\cdots:t^{r_i}x_i:\cdots:t^{r_n}x_n).$$

If $r_0 > r_1 > \cdots > r_n$, then the fixed points are $P_0, \ldots, P_n$ with

$$P_i = (0:\cdots:0:\overset{i}{1}:0:\cdots:0).$$

We can write the action as

$$t(x_0:\cdots:1:\cdots:x_n) = (t^{r_0-r_i}x_0:\cdots:1:\cdots:t^{r_n-r_i}x_n),$$

on an affine open neighbourhood of P_i, and so

$$X(P_i) = \{(x_0:\cdots:x_{i-1}:1:0:\cdots:0)\} \simeq \mathbb{A}^i.$$

The Białynicki-Birula decomposition is

$$X = X(P_n) \sqcup \cdots \sqcup X(P_0) \simeq \mathbb{A}^n \sqcup \cdots \sqcup \mathbb{A}^0.$$

Here P_n is the attracting point and P_0 is the repelling point.

LEMMA 13.51. *Let T be a split torus and (V, r) a finite-dimensional representation of T. There exists a cocharacter $\lambda \colon \mathbb{G}_m \to T$ such that $\mathbb{P}(V)^{\lambda(\mathbb{G}_m)} = \mathbb{P}(V)^T$.*

PROOF. Write V as a sum of eigenspaces, $V = \bigoplus_{i=1}^m V_{\chi_i}$, with the χ_i distinct. Let λ be an element of $X_*(T)$ not lying on any of the finitely many hyperplanes $\langle \chi_i - \chi_j \rangle^\perp$, $i \neq j$, in $X_*(T)_{\mathbb{Q}}$. Then the integers $\langle \lambda, \chi_i \rangle$, $1 \leq i \leq m$, are distinct, and so $\lambda(\mathbb{G}_m)$ and T have the same eigenvectors in V, and hence the same fixed points in $\mathbb{P}(V)$. $\qquad \square$

Let (V, r) be a finite-dimensional representation of a split torus T. Let X be a smooth connected closed subscheme of $\mathbb{P}(V)$ stable under T. Let λ be as in the lemma. On applying Theorem 13.47 to the action of $\lambda(\mathbb{G}_m)$ on X, we obtain for each $x \in X^T(k)$ a smooth subscheme $X(x, \lambda)$ of X such that

$$X(x, \lambda)(k') = \{y \in X(k') \mid \lim_{t \to 0} \lambda(t)y \text{ exists and equals } x\}$$

for all fields k' containing k; moreover, $X(x, \lambda)$ is an affine space, isomorphic to the contracting subspace of $\mathrm{Tgt}_x X$ for the action of $\lambda(\mathbb{G}_m)$. If X^T is finite and $X^T(k) = X^T(k^s)$, then there exists a unique attracting fixed point x_- and a unique repelling point x_+.

PROPOSITION 13.52. *If X^T is finite and constant, then, for every λ as in 13.51, there exists an $x \in X^T(k)$ and a smooth open affine subscheme $U(x)$ of X such that*

$$U(x)(k^{\mathrm{a}}) = \{y \in X(k^{\mathrm{a}}) \mid x \in \overline{T \cdot y}\}.$$

Moreover, $U(x) \approx \mathbb{A}^{\dim(X)}$.

PROOF. Let λ be as in 13.51, so $\mathbb{P}(V)^{\lambda(\mathbb{G}_m)} = \mathbb{P}(V)^T$. On applying 13.49, we see that there exists a unique point $x_- \in X^T$ such that $X(x_-, \lambda)$ is open in X; moreover, $\mathrm{Tgt}_{x_-}(X) = \mathrm{Tgt}_{x_-}^+(X)$. We shall show that $X(x_-, \lambda)$ has the required properties. We may suppose that k is algebraically closed.

Let $y \in X(k)$. If $\lim_{t \to 0} \lambda(t)y = x_-$, then $x_- \in \overline{T \cdot y}$, and so $X(x_-, \lambda) \subset \{y \in X(k) \mid x \in \overline{T \cdot y}\}$. Conversely, let $y \in X(k)$ be such that $x \in \overline{T \cdot y}$. The intersection $X(x_-, \lambda) \cap \overline{T \cdot y}$ is then a nonempty open subset of $\overline{T \cdot y}$. We deduce that $X(x_-, \lambda) \cap Ty \neq \emptyset$. As $\lambda(\mathbb{G}_m)$ commutes with T, the action of T leaves $X(x_-, \lambda)$ stable, and so $Ty \subset X(x_-, \lambda)$. Therefore $y \in X(x_-, \lambda)$. □

Recall (7.28) that a closed immersion $X \hookrightarrow \mathbb{P}(V)$ is nondegenerate if X is not contained in $\mathbb{P}(W)$ for any subrepresentation W of V.

PROPOSITION 13.53. *Let (V, r) be a finite-dimensional representation of a split torus T, and let X be a smooth connected closed subscheme of $\mathbb{P}(V)$ stable under T. Assume that the embedding $X \to \mathbb{P}(V)$ is nondegenerate and X^T is finite and constant. Let Ψ be the set of characters of T occurring in V. Let λ be a cocharacter of T such that the integers $\langle \chi, \lambda \rangle$, $\chi \in \Psi$, are distinct.*

(a) *Let $\chi_- \in \Psi$ be such that $\langle \chi_-, \lambda \rangle$ is minimum. Then V_{χ_-} has dimension 1, and the line V_{χ_-} belongs to X. It is the unique attracting point of $\lambda(\mathbb{G}_m)$ in X.*

(b) *Let $\chi_+ \in \Psi$ be such that $\langle \chi_+, \lambda \rangle$ is maximum. Then V_{χ_+} has dimension 1, and the line V_{χ_+} belongs to X. It is the unique repelling point of $\lambda(\mathbb{G}_m)$ in X.*

PROOF. (a) Since the projective embedding $X \to \mathbb{P}(V)$ is nondegenerate, there exists a line $[v] \in X$ with $v = \sum_{\chi \in \Psi} v_\chi$, $v_\chi \in V_\chi$, $v_{\chi_-} \neq 0$. Then

$$\lim_{t \to 0} [\lambda(t)v] = [v_{\chi_-}];$$

in particular, $x_- = [v_{\chi_-}]$ is a fixed point of X. The action of $\lambda(\mathbb{G}_m)$ on the tangent space $\mathrm{Tgt}_{x_-}(\mathbb{P}(V))$ has no dilating vectors. We deduce that x_- is an attracting fixed point of X because we know that X has only isolated fixed points. Moreover, as X is irreducible, it is the unique attracting fixed point in X. We deduce that, if $[v']$, $v = \sum v'_\chi$, lies in X, then $v'_\chi \in [v_\chi]$. Again, because $X \to \mathbb{P}(V)$ is nondegenerate, $\dim(V_{\chi_-}) = 2$. We have also shown that the line V_{χ_-} belongs to X, and that it is the unique attracting fixed point of $\lambda(\mathbb{G}_m)$ in X.

(b) Apply (a) to $-\lambda$. $\square$

PROPOSITION 13.54. *Let $T \times X \to X$ be an action of a split torus on a scheme X, and let $\lambda : \mathbb{G}_m \to T$ be a nontrivial homomorphism. Then $X(x, \lambda) = X(x, \lambda \circ n)$ for all $n > 0$.*

PROOF. Clearly, $\lim_{t \to 0} \lambda(t)y$ exists and equals x if and only if $\lim_{t \to 0} \lambda(t^n)y$ exists and equals x. $\square$

ASIDE 13.55. On combining the above results with Białynicki-Birula 1976, one obtains the following variant of the decomposition theorem (Brosnan 2005, 3.2). Let X be a smooth projective variety over k equipped with an action of $\mathbb{G}_m$. Then there is a numbering $X^{\mathbb{G}_m} = \bigsqcup_{i=1}^n Z_i$ of the set of connected components of the (smooth closed) fixed point scheme, a filtration

$$X = X_n \supset X_{n-1} \supset \cdots \supset X_0 \supset X_{-1} = \emptyset,$$

and affine fibrations $\varphi_i : X_i \smallsetminus X_{i-1} \to Z_i$. The relative dimension a_i of the affine fibration φ_i is the dimension of $\mathrm{Tgt}_z^+(X)$ for any z in Z_i, and the dimension of Z_i is the dimension of $\mathrm{Tgt}_z X^{\mathbb{G}_m}$.

NOTES. Theorem 13.47 was proved in the context of varieties over algebraically closed fields in Białynicki-Birula 1973 and extended to schemes in Hesselink 1981.

g. Proof of the Białynicki-Birula decomposition

Let X be a separated algebraic scheme over k equipped with an action μ of $\mathbb{G}_m$, and let Z be a $\mathbb{G}_m$-stable closed subscheme Z of X. The **concentrator functor** Φ sends an affine k-scheme U to the set $\Phi(U)$ of morphisms $\varphi : \mathbb{A}^1 \times U \to X$ of k-schemes such that

(a) the restriction of φ to $\mathbb{G}_m \times U$ is $\mathbb{G}_m$-equivariant, i.e.,

$$\varphi(a, u) = a \cdot \varphi(1, u), \text{ all } a \in \mathbb{G}_m(R), u \in U(R);$$

(b) the restriction of φ to $0 \times U$ factors through Z.

We say that Φ is representable if there exists a universal pair (Y, φ) satisfying (a) and (b). This means that Y is a scheme over k (not necessarily affine) and φ is a

morphism $\mathbb{A}^1 \times Y \to X$ satisfying (a) and (b) and such that, for every $h \in \Phi(U)$, there is a unique morphism $\alpha: U \to Y$ such that $h = (\mathrm{id} \times \alpha) \circ \varphi$:

$$
\begin{array}{ccc}
U & & \mathbb{A}^1 \times U \\
\Big\downarrow{\scriptstyle \exists!\,\alpha} & & \Big\downarrow{\scriptstyle \mathrm{id}\times\alpha} \searrow^{h} \\
Y & & \mathbb{A}^1 \times Y \xrightarrow{\ f\ } X
\end{array}
$$

Then Y is called the ***concentrator scheme***, and the maps

$$
\begin{aligned}
i: Y \to X \quad &\text{equal to} \quad Y \simeq 1 \times Y \xrightarrow{\varphi} X \\
p: Y \to Z \quad &\text{equal to} \quad Y \simeq 0 \times Y \xrightarrow{\varphi} Z
\end{aligned}
$$

are called the ***realization morphisms***. For $y \in Y(k)$, $p(y) = \lim_{t \to 0} t \cdot i(y)$.

EXAMPLE 13.56. Let $X = \mathbb{P}^1$ with $\mathbb{G}_m$ acting by $t(x_0{:}x_1) = (x_0{:}tx_1)$, and let Z be the subscheme $\mathbb{P}^1$. The fixed points are $0 = (1{:}0)$ and $\infty = (0{:}1)$. The concentrator scheme is $\mathbb{A}^1 \sqcup \{\infty\}$ with i the obvious morphism to $\mathbb{P}^1$ and p the morphism sending $\mathbb{A}^1$ to 0 and ∞ to ∞. Note that $i \sqcup p: \mathbb{A}^1 \sqcup \infty \to \mathbb{P}^1$ is not an immersion, and i is not a closed immersion.

REMARK 13.57. A $\varphi \in \Phi(U)$ is determined by its restriction $\varphi|$ to $\mathbb{G}_m \times U$ because $\mathbb{G}_m$ is schematically dense in $\mathbb{A}^1$, and $\varphi|$ is determined by the element $\varphi|1 \times U$ of $X(U)$. Using this, one sees that Φ is isomorphic to the functor Φ' sending a k-algebra R to the set of points $x \in X(R)$ such that $\mu_x: \mathbb{G}_{mR} \to X_R$ extends to an R-morphism $\mathbb{A}^1_R \to X_R$ mapping 0_R into Z_R. In other words, $x \in X(R)$ if $\lim_{t \to 0} t \cdot x$ exists and lies in $Z(R)$. In particular, if X is affine, then Φ is represented by concentrator scheme $X(Z)$ in the sense of Definition 13.21.

PROPOSITION 13.58. *Let X be a separated scheme over k equipped with an action of $\mathbb{G}_m$, and let Z be a $\mathbb{G}_m$-stable closed subscheme Z of X. If (X, μ) is locally affine, then the concentrator functor Φ is representable by a scheme $X(Z)$ with an action of $\mathbb{A}^1$; moreover, the morphism $i: X(Z) \to X$ is a local immersion and the morphism $p: X(Z) \to Z$ is affine.*

PROOF. To prove that a functor is representable, we must show (a) that it is local and (b) that it admits a finite covering by open subfunctors each of which is representable by an affine scheme (A.34). That Φ is local follows easily from its definition. Let $X = \bigcup X_i$ be an open covering of X by G-invariant open affine subschemes, and let $Z_i = Z \cap X_i$. The concentrator functor Φ_i of (X_i, Z_i) is an open subfunctor of Φ_i, and is representable by an affine scheme $X(Z)_i = X_i(Z_i)$ (see 13.57). Therefore Φ is represented by a scheme $X(Z)$. The $X(Z)_i$ form an open affine covering of $X(Z)$, and the restriction of i to $X(Z)_i$ is a closed immersion into X_i. Therefore i is locally an immersion. The schemes Z_i form an open affine covering of Z, and $p^{-1}(Z_i)$ is the affine scheme Y_i. Therefore p is affine. $\qquad\square$

We now prove Theorem 13.47. Let (X, μ) be as in the statement of the theorem and let Z be a connected component of $X^{\mathbb{G}_m}$. As in the proof of Proposition 13.58, we let $X = \bigcup X_i$ be an open covering of X by G-invariant open affine subschemes, and we let $Z_i = Z \cap X_i$. Part (a) of the theorem was proved in Proposition 13.58. Moreover, it is clear from its proof that, for (b), we may suppose that X is affine. Now $X(Z)$ is the concentrator scheme in the sense of Definition 13.21, but we also know from Remark 13.57 that it represents the functor Φ. In particular, it has an action of $\mathbb{A}^1$ extending the action of $\mathbb{G}_m$ that it acquires as a subscheme of X. This implies that the action of $\mathbb{G}_m$ on $X(Z)$ is definite, i.e., $\mathcal{O}(X(Z)) = \bigoplus_{n \in \mathbb{N}} \mathcal{O}(X(Z))_n$. Thus (b) of the theorem follows from Theorem 13.44. Finally, (c) of the theorem is obvious.

Exercises

EXERCISE 13-1. Consider the action

$$t(x_0 : x_1 : x_2 : x_3) = (t^{r_0} x_0 : t^{r_1} x_1 : t^{r_2} x_2 : t^{r_3} x_3)$$

of $\mathbb{G}_m$ on $\mathbb{P}^2$. Compute the Białynicki-Birula decomposition of $\mathbb{P}^2$ in each of the following cases:

(a) $r_0 = r_1 > r_2 > r_3$;   (b) $r_0 > r_1 = r_2 > r_3$;   (c) $r_0 > r_1 > r_2 = r_3$.

Unipotent Algebraic Groups

Recall that all algebraic groups are affine over a base field k.

a. Preliminaries from linear algebra

Recall that an element r of a ring is unipotent if $r - 1$ is nilpotent. An endomorphism of a finite-dimensional vector space V is unipotent if and only if its characteristic polynomial is $(T - 1)^{\dim V}$. These are exactly the endomorphisms of V whose matrix relative to some basis of V lies in

$$\mathbb{U}_n(k) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 1 & * & * & \ldots & * \\ 0 & 1 & * & \ldots & * \\ 0 & 0 & 1 & \ldots & * \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}.$$

PROPOSITION 14.1. *Whenever an abstract group G acts on a nonzero finite-dimensional vector space V by unipotent endomorphisms, there is a nonzero vector fixed by G.*

PROOF. We use the double centralizer theorem (Lang 2002, XVII, 3.5):

> Let M be a faithful left module over a ring A (not necessarily commutative), and let $C = \text{End}_A(M)$. If M is simple as an A-module and finitely generated as a C-module, then $\text{End}_C(M) = A$.

Being fixed by G is a linear condition, and so we may replace k with its algebraic closure.[1] We may also replace V with a simple submodule. We now have to show that $V = V^G$. Let A be the k-subalgebra of $\text{End}_k(V)$ generated by G.

---

[1] For any representation (V, r) of an abstract group G, the subspace V^G of V is the intersection of the kernels of the linear maps $v \mapsto gv - v \colon V \to V$ ($g \in G$). It follows that $(V \otimes k^{\mathrm{a}})^{G_{k^{\mathrm{a}}}} \simeq V^G \otimes k^{\mathrm{a}}$, and so $(V \otimes k^{\mathrm{a}})^{G_{k^{\mathrm{a}}}} \neq 0 \Rightarrow V^G \neq 0$.

As V is simple as an A-module and k is algebraically closed, $\mathrm{End}_A(V) = k$ (cf. 4.20). Therefore, $A = \mathrm{End}_k(V)$. The k-subspace J of A spanned by the elements $g - \mathrm{id}_V$, $g \in G$, is a two-sided ideal in A. Because A is a simple algebra over k (it is isomorphic to $M_n(k)$), either $J = 0$, and the proposition is proved, or $J = A$. But every element of J has trace zero because G acts by unipotent endomorphisms, and so $J \neq A$. □

COROLLARY 14.2. *In the situation of the proposition, there exists a basis of V for which G acts through $\mathbb{U}_n(k)$.*

PROOF. Let e_1 be a nonzero element of V fixed by G. Then G acts on $V/\langle e_1 \rangle$ by unipotent endomorphisms, and so there is an element e_2 of V whose image in $V/\langle e_1 \rangle$ is nonzero and fixed by G. Continuing in this fashion, we obtain a basis $\{e_1, e_2, \ldots, e_n\}$ for V with the required property. □

b. Unipotent algebraic groups

Recall (6.45) that an algebraic group G is unipotent if every nonzero representation of G has a nonzero fixed vector. Equivalently, G is unipotent if its only simple representations are one-dimensional spaces with the trivial action. In terms of the associated comodule (V, ρ), the condition $V^G \neq 0$ means that there exists a nonzero vector $v \in V$ such that $\rho(v) = v \otimes 1$ (see 4.33).

As every representation is a union of finite-dimensional representations (4.8), it suffices to check the conditions for finite-dimensional representations.

A finite-dimensional representation (V, r) of an algebraic group G is said to be **unipotent** if there exists a basis of V for which $r(G) \subset \mathbb{U}_n$. Equivalently, (V, r) is unipotent if there exists a flag $V = V_m \supset \cdots \supset V_1 \supset 0$ stable under G and such that G acts trivially on each quotient V_{i+1}/V_i.

PROPOSITION 14.3. *An algebraic group G is unipotent if and only if every finite-dimensional representation (V, r) of G is unipotent.*

PROOF. Let (V, r) be a finite-dimensional representation of G with $V \neq 0$.

Suppose that G is unipotent, and let $V = V_m \supset \cdots \supset V_1 \supset 0$ be a composition series for V, i.e., a maximal subnormal series for V as a G-module. Each quotient V_{i+1}/V_i is simple, and so G acts trivially on it. Therefore (V, r) is unipotent.

Suppose that (V, r) is unipotent, and let $V = V_m \supset \cdots \supset V_1 \supset 0$ be as in the definition. In particular, G acts trivially on V_1, which we may suppose to be nonzero. Now $V^G \supset V_1 \neq 0$. Therefore G is unipotent. □

We next prove that every algebraic subgroup of $\mathbb{U}_n$ is unipotent. In particular, $\mathbb{G}_a$ is unipotent and, in characteristic p, its subgroups α_p and $\mathbb{Z}/p\mathbb{Z}$ are unipotent.

DEFINITION 14.4. A Hopf algebra (A, Δ) over k is **coconnected** if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \cdots$ of A by subspaces C_i such that[2]

$$\begin{cases} C_0 = k, \\ \bigcup_{r \geq 0} C_r = A, \\ \Delta(C_r) \subset \sum_{i=0}^{r} C_i \otimes C_{r-i}. \end{cases} \tag{91}$$

THEOREM 14.5. *The following conditions on an algebraic group G are equivalent:*

(a) *G is unipotent;*

(b) *G is isomorphic to an algebraic subgroup of $\mathbb{U}_n$ for some n;*

(c) *the Hopf algebra $\mathcal{O}(G)$ is coconnected.*

PROOF. (a)$\Rightarrow$(b). Apply Proposition 14.3 to a faithful finite-dimensional representation of G (which exists by 4.9).

(b)$\Rightarrow$(c): Every quotient of a coconnected Hopf algebra is coconnected because the image of a filtration satisfying (91) will still satisfy (91), and so it suffices to show that $\mathcal{O}(\mathbb{U}_n)$ is coconnected. Recall that $\mathcal{O}(\mathbb{U}_n) \simeq k[X_{ij} \mid i < j]$, and that

$$\Delta(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \sum_{i < l < j} X_{il} \otimes X_{lj}. \tag{92}$$

Assign a weight of $j - i$ to X_{ij}, so that a monomial $\prod X_{ij}^{n_{ij}}$ has weight $\sum n_{ij}(j - i)$, and let C_r be the subspace spanned by the monomials of weight $\leq r$. Clearly, $C_0 = k$, $\bigcup_{r \geq 0} C_r = A$, and $C_i C_j \subset C_{i+j}$. It remains to check the third condition in (91), and it suffices to do this for the monomials in C_r. For the X_{ij} the condition can be read off from (92). We proceed by induction on the weight of a monomial. If the condition holds for monomials P, Q of weights r, s, then $\Delta(PQ) = \Delta(P)\Delta(Q)$ lies in

$$\left(\sum_i C_i \otimes C_{r-i} \right) \left(\sum_j C_j \otimes C_{s-j} \right) \subset \sum_{i,j} \left(C_i C_j \otimes C_{r-i} C_{s-j} \right)$$
$$\subset \sum_{i,j} C_{i+j} \otimes C_{r+s-i-j},$$

as required.

(c)$\Rightarrow$(a). Assume that $A = \mathcal{O}(G)$ is coconnected, say, $A = \bigcup_{r \geq 0} C_r$, and let $\rho: V \to V \otimes A$ be an A-comodule. Then V is a union of the subspaces

$$V_r \stackrel{\text{def}}{=} \{v \in V \mid \rho(v) \in V \otimes C_r\}.$$

---

[2]This definition is probably as mysterious to the reader as it is to the author. Basically, it is the condition that you arrive at when looking at Hopf algebras with only one group-like element (so the corresponding affine group has only the trivial character). See Sweedler 1967.

If V_0 contains a nonzero vector v, then $\rho(v) = v' \otimes 1$ for some vector v'; on applying ϵ, we find that $v = v'$, and so v is a fixed vector. To complete the proof, it suffices to show that

$$V_r = 0 \implies V_{r+1} = 0,$$

because then $V_0 = 0 \implies V = 0$. By definition, $\rho(V_{r+1}) \subset V \otimes C_{r+1}$, and so

$$((\mathrm{id} \otimes \Delta) \circ \rho)(V_{r+1}) \subset V \otimes \sum_i C_i \otimes C_{r+1-i}.$$

Hence $(\mathrm{id} \otimes \Delta) \circ \rho$ maps V_{r+1} to zero in $V \otimes A/C_r \otimes A/C_r$. We now use that $(\mathrm{id} \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}) \circ \rho$. If $V_r = 0$, then the map $V \to V \otimes A/C_r$ defined by ρ is injective, and also the map $V \to (V \otimes A/C_r) \otimes A/C_r$ defined by $(\rho \otimes \mathrm{id}) \circ \rho$ is injective; hence $V_{r+1} = 0$. □

COROLLARY 14.6. *An algebraic group is unipotent if and only if it admits a faithful unipotent representation.*

PROOF. Restatement of the equivalence of (a) and (b). □

COROLLARY 14.7. *Subgroups, quotients, and extensions of unipotent algebraic groups are unipotent.*

PROOF. For quotients and extensions, this was proved in 6.45. As a unipotent group admits a faithful unipotent representation, so does every algebraic subgroup. □

COROLLARY 14.8. *Every algebraic group contains a largest smooth connected normal unipotent subgroup.*

PROOF. Apply Proposition 6.42. □

The unipotent subgroup in the corollary may not stay "largest" with extension of the base field (6.48).

COROLLARY 14.9. *Let G be an algebraic group over k, and let k' be an extension of k. Then G is unipotent over k if and only if $G_{k'}$ is unipotent over k'.*

PROOF. If G is unipotent, then $\mathcal{O}(G)$ is coconnected (14.9). But then $\mathcal{O}(G) \otimes k'$ is obviously coconnected, and so $G_{k'}$ is unipotent. Conversely, suppose that $G_{k'}$ is unipotent, and let (V, r) be a representation of G. Then $(V \otimes k')^{G_{k'}} \simeq V^G \otimes k'$ (see 4.34), and so V^G is nonzero if $(V \otimes k')^{G_{k'}}$ is nonzero. □

COROLLARY 14.10. *Let G be an algebraic group over a perfect field k. If G is unipotent, then all elements of $G(k)$ are unipotent, and the converse is true when $G(k)$ is dense in G (as a scheme).*

PROOF. Let (V, r) be a faithful finite-dimensional representation G (which exists by 4.9). If G is unipotent, then $r(G) \subset \mathbb{U}_n$ for some basis of V (see 14.3), and so $r(g)$ is unipotent for every $g \in G(k)$; this implies that g is unipotent (9.19). Conversely, if the elements of $G(k)$ are unipotent, then they act unipotently on V, and so there exists a basis of V for which $r(G(k)) \subset \mathbb{U}_n(k)$ (see 14.2). Because $G(k)$ is dense in G, this implies that $r(G) \subset \mathbb{U}_n$. □

COROLLARY 14.11. *An algebraic subgroup G of GL_V is unipotent if there exists a subgroup of $G(k)$ that is dense in G (as a scheme) and consists of unipotent endomorphisms.*

PROOF. Let S be such a subgroup. There exists a basis of V for which $S \subset \mathbb{U}_n(k)$ (see 14.2). Then $S \subset (\mathbb{U}_n \cap G)(k)$, and so $\mathbb{U}_n \cap G = G$. Therefore $G \subset \mathbb{U}_n$. □

COROLLARY 14.12. *A smooth algebraic group G is unipotent if and only if the elements of $G(k^a)$ are unipotent.*

PROOF. As G is smooth, $G(k^a)$ is dense in G. If its elements are unipotent, then G_{k^a} is unipotent (14.10), and so G is unipotent (14.9). Conversely, if G is unipotent, then G_{k^a} is unipotent (14.9), and so the elements of $G(k^a)$ are unipotent (14.10). □

The last corollary fails for nonsmooth G. For example, μ_p is not unipotent even though $\mu_p(k^a)$ consists of unipotent elements if $\mathrm{char}(k) = p$.

EXAMPLE 14.13. Let G be a smooth algebraic group and λ a cocharacter of G. The subgroup $U(\lambda)$ of G (see 13.29) is unipotent because, as we saw in the proof of Theorem 13.33, it can be realized as an algebraic subgroup of $\mathbb{U}_n$.

The proof of Theorem 14.5 follows Waterhouse 1979, 8.3.

PROPOSITION 14.14. *A finite étale algebraic group G is unipotent if and only if its order is a power of the characteristic exponent of k.*

PROOF. We may suppose that k is algebraically closed (14.9), and hence that G is constant. Let p be the characteristic exponent of k. If G is not a p-group, then it contains a nontrivial subgroup H of order prime to p. According to Maschke's theorem, every nonzero finite-dimensional representation of H is semisimple, and so there exist nontrivial simple representations. Hence H is not unipotent, and it follows that G is not unipotent (14.7). Conversely, a finite p-group over a field of characteristic p has no nontrivial simple representations (Lang 2002, XVIII, Exercise 13), and so such a group is unipotent. □

COROLLARY 14.15. *Let G be an algebraic group over k. If G is unipotent, then $\pi_0(G)$ has order a power of the characteristic exponent of k; in particular, G is connected if k has characteristic zero.*

PROOF. As $\pi_0(G)$ is a quotient of G, it is unipotent, and so we can apply the proposition. □

PROPOSITION 14.16. *An algebraic group that is both multiplicative and unipotent is trivial.*

PROOF. Let G be an algebraic group, and let (V, r) be a faithful finite-dimensional representation of G. If G is multiplicative, then V is a direct sum of simple representations (12.30); if G is also unipotent, then the action of G on each of the simple representations is trivial; and so G is trivial.   □

COROLLARY 14.17. *The intersection of a unipotent algebraic subgroup of an algebraic group with an algebraic subgroup of multiplicative type is trivial.*

PROOF. Both properties are inherited by subgroups (12.9, 14.7).   □

COROLLARY 14.18. *There are no nontrivial homomorphisms over k*

  (a) *from a unipotent algebraic group to an algebraic group of multiplicative type, or*

  (b) *from an algebraic group of multiplicative type to a unipotent algebraic group.*

PROOF. In both cases, the image is both unipotent and multiplicative (12.9, 14.7).   □

   We saw in Exercise 1-1 that (a) fails over rings with nilpotents. In Proposition 15.18 below, we shall show that (b) remains true over all k-algebras R.

EXAMPLE 14.19. The map $a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ realizes $\mathbb{G}_a$ as an algebraic subgroup of $\mathbb{U}_2$, and so $\mathbb{G}_a$ is unipotent. Therefore all algebraic subgroups of $\mathbb{G}_a$ are unipotent; for example, in characteristic $p \neq 0$, the groups α_p and $(\mathbb{Z}/p\mathbb{Z})_k$ are unipotent. These examples show that a unipotent algebraic group need not be smooth or connected in nonzero characteristic.

EXAMPLE 14.20. Let k be a nonperfect field of characteristic $p \neq 0$, and let $t \in k \smallsetminus k^p$. The algebraic subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^p = X - tX^p$$

becomes isomorphic to $\mathbb{G}_a$ over $k[t^{\frac{1}{p}}]$, but it is not isomorphic to $\mathbb{G}_a$ over k. To see this, we use that G is canonically an open subscheme of the complete regular curve C with function field the field of fractions of $\mathcal{O}(G)$ (see 20.2 below). The complement of G in C consists of a single point with residue field $k[t^{\frac{1}{p}}]$. For $G = \mathbb{G}_a$, the same construction realizes G as an open subset of $\mathbb{P}^1$ whose complement consists of a single point with residue field k (see 14.57).

PROPOSITION 14.21. *Every unipotent algebraic group admits a central normal series whose quotients are isomorphic to algebraic subgroups of $\mathbb{G}_a$. In particular, every unipotent algebraic group is nilpotent (a fortiori solvable).*

PROOF. Embed the unipotent algebraic group G in $\mathbb{U}_n$. Recall (6.49) that $\mathbb{U}_n$ has a central series

$$\mathbb{U}_n = U_n^{(0)} \supset \cdots \supset U_n^{(r)} \supset U_n^{(r+1)} \supset \cdots \supset U_n^{(m)} = e, \quad m = \frac{n(n-1)}{2},$$

whose quotients are canonically isomorphic to $\mathbb{G}_a$. The intersection of such a series with G has the required properties (see 6.2). □

For example, every form of $\mathbb{G}_a$ is an extension of $\mathbb{G}_a$ by a finite subgroup of $\mathbb{G}_a$ (see 14.57).

PROPOSITION 14.22. *An algebraic group G is unipotent if and only if every nontrivial algebraic subgroup of it admits a nontrivial homomorphism to $\mathbb{G}_a$.*

PROOF. Let G be a unipotent algebraic group. Every algebraic subgroup of G is unipotent (14.7), and Proposition 14.21 shows that every nontrivial unipotent algebraic group admits a nontrivial homomorphism to $\mathbb{G}_a$.

Conversely, suppose that all algebraic subgroups of G admit homomorphisms to $\mathbb{G}_a$. In particular, G admits a nontrivial homomorphism to $\mathbb{G}_a$, whose kernel we denote by G_1. If $G_1 \neq 1$, then (by hypothesis) it admits a nontrivial homomorphism to $\mathbb{G}_a$, whose kernel we denote by G_2. Continuing in this fashion, we obtain a subnormal series whose quotients are algebraic subgroups of $\mathbb{G}_a$. The series terminates in e because the algebraic subgroups of G satisfy the descending chain condition (1.42). Now Corollary 14.7 shows that G is unipotent. □

PROPOSITION 14.23. *Let G be a connected algebraic group, and let N be the kernel of the adjoint representation $\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$ (see 10.23). Then $N/Z(G)$ is unipotent.*

PROOF. We may suppose that k is algebraically closed (14.9). Let $\mathcal{O}_e = \mathcal{O}(G)_e$ (the local ring at the identity element), and let $\mathfrak{m}_e$ be its maximal ideal. The action of G on itself by conjugation defines a representation of G on the k-vector space $\mathcal{O}_e/\mathfrak{m}_e^{n+1}$ for all n (see 8.10). The representation on $\mathfrak{m}_e/\mathfrak{m}_e^2$ is the contragredient of the adjoint representation (10.20), and so N acts trivially on $\mathfrak{m}_e/\mathfrak{m}_e^2$. It follows that N acts trivially on each of the quotients $\mathfrak{m}_e^i/\mathfrak{m}_e^{i+1}$. For n sufficiently large, the representation r_n of $N/Z(G)$ on $\mathcal{O}_e/\mathfrak{m}^{n+1}$ is faithful (8.10). As $N/Z(G)$ acts trivially on the quotients $\mathfrak{m}_e^i/\mathfrak{m}_e^{i+1}$ of the flag

$$\mathcal{O}_e/\mathfrak{m}^{n+1} \supset \mathfrak{m}_e/\mathfrak{m}^{n+1} \supset \mathfrak{m}_e^2/\mathfrak{m}^{n+1} \supset \cdots,$$

it is unipotent (14.6). □

REMARK 14.24. (a) In characteristic zero, the only algebraic subgroups of $\mathbb{G}_a$ are e and $\mathbb{G}_a$ itself. To see this, note that a proper algebraic subgroup of $\mathbb{G}_a$ must have dimension 0; hence it is étale (3.24), and hence is trivial (14.14).

(b) We saw in Proposition 14.21 that every unipotent algebraic group is nilpotent. Conversely, every connected nilpotent algebraic group G contains a largest subgroup G_s of multiplicative type; the group G_s is characteristic and central, and the quotient G/G_s is unipotent (16.47 below).

PROPOSITION 14.25. *Every connected group variety of dimension one is commutative.*

PROOF. We may suppose that k is algebraically closed. Let G be a connected group variety of dimension one. If $G(k) \subset Z(G)(k)$, then $G \subset Z(G)$, as claimed. Otherwise, there exists a noncentral element g in $G(k)$, and we consider the morphism $x \mapsto xgx^{-1} \colon G \to G$. The image I of this map is connected and $\neq e$, and so $I(k)$ is infinite and dense. Therefore I contains an open subset of G (see A.15), and so $G(k) \smallsetminus I(k)$ is finite. Embed G into GL_V, and consider the map $G(k) \to k^{\dim V}$ sending an element of $G(k)$ to the coefficients of its characteristic polynomial. This map is constant on $I(k)$, and so it takes only finitely many values as x runs over $G(k)$. As $G(k)$ is connected and the map is continuous, the characteristic polynomials are constant, and equal $\det(T - e) = (T - 1)^{\dim V}$. Hence G is unipotent (14.12) and solvable (14.21). In particular the derived group $\mathcal{D}G$ of G is a proper subgroup of G. As $\mathcal{D}G$ is a connected group variety (6.19), this implies that $\mathcal{D}G = e$, which contradicts the existence of a noncentral g. □

PROPOSITION 14.26. *Let U be a unipotent subgroup (not necessarily normal) of an algebraic group G. Then G/U is isomorphic to a subscheme of an affine space (i.e., it is quasi-affine).*

PROOF. According to Chevalley's theorem (4.27), there exists a representation (V, r) of G such that U is the stabilizer of a one-dimensional subspace L of V. As U is unipotent, it acts trivially on L, and so $V^U = L$. When we regard r as an action of G on $V_{\mathfrak{a}}$, the isotropy group at any nonzero element of L is U, and so the map $g \mapsto gx$ is an immersion $G/U \to V_{\mathfrak{a}}$ (see 7.17). □

NOTES. Traditionally, a group variety G is said to be unipotent if its elements in some (large) algebraically closed field are unipotent (Springer 1998, p. 36). This agrees with our definition (by 14.12).

Demazure and Gabriel (1970, IV, §2, 2.1) define a group scheme G over k to be unipotent if it is affine and if, for all closed subgroups $H \neq e$ of G, there exists a nontrivial homomorphism $H \to \mathbb{G}_a$. For algebraic group schemes, this agrees with our definition (by 14.22).

SGA 3 (XVII, 1.1, 1.4) defines an algebraic group over k to be unipotent if it admits a subnormal series over k^{a} whose quotients are isomorphic to algebraic subgroups of $\mathbb{G}_a$. This is agrees with our definition (by 14.7, 14.9, 14.21).

c.   Unipotent elements in algebraic groups

All representations (and vector spaces) in this section are finite-dimensional.

DEFINITION 14.27. Let G be an algebraic group over k. An element u of $G(k)$ is **_unipotent_** if $r(u)$ is unipotent for all finite-dimensional representations r of G.

When k is perfect, this agrees with the definition in 9.19. If G is unipotent, then all elements of $G(k)$ are unipotent because all representations of G are unipotent (14.3). Conversely, if G is smooth and all elements of $G(k^a)$ are unipotent, then G is unipotent (14.12).

14.28. Let V be a vector space over a field k of characteristic zero, and let R be a k-algebra. For a nilpotent endomorphism N of the R-module V_R, we define

$$\exp(N) = I + N + N^2/2! + N^3/3! + \cdots.$$

It is an automorphism of V_R with inverse $\exp(-N)$. For a unipotent endomorphism u of V_R, we define

$$\log(u-1) = (u-1) - (u-1)^2/2 + (u-1)^3/3 - \cdots.$$

It is a nilpotent endomorphism of V_R, and exp and log are inverse maps.

14.29. Let V be a vector space over a field k of characteristic zero. If r is a representation of $\mathbb{G}_a$ on V, then $u = r(1)$ is a unipotent endomorphism of V and $N = \log(u)$ is a nilpotent endomorphism. The representation r can be recovered from N because

$$r(t) = \exp(tN).$$

In this way, we obtain one-to-one correspondences between (a) representations r of $\mathbb{G}_a$ on V, (b) unipotent endomorphisms u of V, and (c) nilpotent endomorphisms N of V.

14.30. Let G be an algebraic group over a field k of characteristic zero, and let $\varphi \colon \mathbb{G}_a \to G$ be a homomorphism. Then $u = \varphi(1)$ is a unipotent element of $G(k)$. Conversely, let u be a unipotent element of $G(k)$. Let R be a k-algebra, and let $t \in R$. For a representation (V, r_V) of G, define

$$\lambda_V(t) = \exp(t \log(r_V(u) - 1)).$$

The family $(\lambda_V(t))_V$ satisfies the conditions of Theorem 9.2, and so there exists a unique $g \in G(R)$ such that $\lambda_V(t) = r_V(g)$ for all representations V. The map $t \mapsto g \colon R \to G(R)$ is a homomorphism natural in R, and so it arises from a homomorphism of algebraic groups $\varphi \colon \mathbb{G}_a \to G$. In this way, we get a one-to-one correspondence between homomorphisms $\varphi \colon \mathbb{G}_a \to G$ and unipotent elements u of $G(k)$: to φ, we attach the unipotent element $u = \varphi(1)$; to u, we attach the homomorphism φ such that

$$r_V(\varphi(t)) = \exp(t \log(r_V(u) - 1))$$

for all $t \in \mathbb{G}_a(R)$ and representations (V, r_V) of G.

d.   Unipotent algebraic groups in characteristic zero

In this section, k is a field of characteristic zero.

Recall (2.6) that, for a finite-dimensional vector space V, $V_{\mathfrak{a}}$ is the algebraic group representing the functor $R \rightsquigarrow R \otimes V$. Recall also that $\mathrm{Lie}(\mathrm{GL}_V) = \mathfrak{gl}_V$, that $\mathrm{Lie}(\mathrm{GL}_n) = \mathfrak{gl}_n$, and that $\mathrm{Lie}(\mathbb{U}_n)$ is the Lie subalgebra

$$\mathfrak{n}_n \stackrel{\mathrm{def}}{=} \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \geq j\}$$

of $\mathfrak{gl}_n$ (see 10.8).

14.31. Let G be a unipotent algebraic group over k. A finite-dimensional representation (V, r_V) of G defines a representation $dr_V : \mathfrak{g} \to \mathfrak{gl}_V$ of $\mathfrak{g}$. For a suitable choice of a basis for V, the image of r_V is contained in $\mathbb{U}_n$ (see 14.3); then the image of dr_V is contained in $\mathrm{Lie}(\mathbb{U}_n) = \mathfrak{n}_n$, and so consists of nilpotent endomorphisms. Let $X \in R \otimes \mathfrak{g}$ for some k-algebra R. Then $dr_V(X)$ is a nilpotent endomorphism of $R \otimes V$, and so there is a well-defined endomorphism $\exp(dr_V(X))$ of $R \otimes V$. For a fixed $X \in R \otimes \mathfrak{g}$, these maps have the following properties:

(a) for all representations (V, r_V) and (W, r_W) of G,

$$\exp(dr_{V \otimes W}(X)) = \exp(dr_V(X)) \otimes \exp(dr_W(X));$$

(b) if G acts trivially on V, then $\exp(dr_k(X))$ is the identity map;

(c) for all G-equivariant maps $u : (V, r_V) \to (W, r_W)$,

$$\exp(dr_W(X)) \circ u_R = u_R \circ \exp(dr_V(X)).$$

According to Theorem 9.2, there is a (unique) element $\exp(X) \in G(R)$ such that

$$r_V(\exp(X)) = \exp((dr_V)(X))$$

for all (V, r_V). On varying X, we obtain a map $\exp : R \otimes \mathfrak{g} \to G(R)$ for each R. These maps are natural in R, and hence (by the Yoneda lemma) they define a morphism of *schemes*

$$\exp : \mathfrak{g}_{\mathfrak{a}} \to G.$$

One checks directly that, for $X \in R \otimes \mathfrak{g}$ and $g \in G(R)$,

$$g \cdot \exp(X) \cdot g^{-1} = \exp(\mathrm{Ad}(g)(X))$$
$$\mathrm{Ad}(\exp(X)) = 1 + \mathrm{ad}(X) + \mathrm{ad}(X)^2/2! + \mathrm{ad}(X)^3/3! + \cdots.$$

Moreover, if $X, Y \in \mathfrak{g}_R$ are such that $[X, Y] = 0$, then

$$\exp(X + Y) = \exp(X) \cdot \exp(Y). \tag{93}$$

For $X \in R \otimes \mathfrak{g}$,

$$\exp(\varepsilon X) = e^{\varepsilon X} \in G(R[\varepsilon]).$$

For a homomorphism $\varphi\colon G \to H$ of algebraic groups, the diagram

$$
\begin{array}{ccc}
\mathfrak{g}_{\mathfrak{a}} & \xrightarrow{\ \exp\ } & G \\
\ \downarrow{\scriptstyle d\varphi} & & \ \downarrow{\scriptstyle \varphi} \\
\mathfrak{h}_{\mathfrak{a}} & \xrightarrow{\ \exp\ } & H
\end{array}
$$

commutes.

PROPOSITION 14.32. *For all unipotent algebraic groups G, the exponential map*

$$\exp\colon \operatorname{Lie}(G)_{\mathfrak{a}} \to G$$

is an isomorphism of schemes. When G is commutative, it is an isomorphism of algebraic groups.

PROOF. For $G = \mathbb{G}_a$, both statements can be checked directly from the definitions.

In general, G admits a central normal series whose quotients are subgroups of $\mathbb{G}_a$ (see 14.21), and hence equal $\mathbb{G}_a$ (14.24). In particular G contains a copy of $\mathbb{G}_a$ in its centre if $\dim G > 0$. We assume (inductively) that the first statement of the proposition holds for $G/\mathbb{G}_a$, and deduce it for G.

Consider the diagram

$$
\begin{array}{ccc}
\operatorname{Lie}(G)_{\mathfrak{a}} & \xrightarrow{\ \ \exp\ \ } & G \\
\downarrow & & \downarrow \\
(\operatorname{Lie}(G)/\operatorname{Lie}(\mathbb{G}_a))_{\mathfrak{a}} & \xrightarrow{\ \exp\ } & G/\mathbb{G}_a.
\end{array}
$$

The vertical maps are faithfully flat. Moreover, $\operatorname{Lie}(G)_{\mathfrak{a}}$ is a $\operatorname{Lie}(\mathbb{G}_a)_{\mathfrak{a}}$-torsor over the base, and G is a $\mathbb{G}_a$-torsor over $G/\mathbb{G}_a$. As the bottom horizontal arrow is an isomorphism (induction) and the top arrow is equivariant for the isomorphism $\exp\colon \operatorname{Lie}(\mathbb{G}_a)_{\mathfrak{a}} \to \mathbb{G}_a$, this shows that the top arrow is an isomorphism (2.71).

For the second statement, if G is commutative, then so also is $\mathfrak{g}$, and (93) shows that exp is an isomorphism. $\qquad\square$

COROLLARY 14.33. *The functor $G \rightsquigarrow \operatorname{Lie}(G)$ is an equivalence from the category of commutative unipotent algebraic groups to that of finite-dimensional k-vector spaces, with quasi-inverse $V \rightsquigarrow V_{\mathfrak{a}}$.*

PROOF. The two functors are quasi-inverse because, for each commutative unipotent algebraic group G, $\operatorname{Lie}(G)_{\mathfrak{a}} \simeq G$ (see 14.32), and for each finite-dimensional vector space V, $\operatorname{Lie}(V_{\mathfrak{a}}) \simeq V$ (10.9). $\qquad\square$

In particular, every commutative unipotent group over k is isomorphic to $\mathbb{G}_a^r$ for some r, and the only algebraic subgroups of $\mathbb{G}_a$ are e and $\mathbb{G}_a$ itself.

It remains to describe the group structure on $\mathfrak{g}_{\mathfrak{a}} \simeq G$ when G is not commutative. For this, we shall need some preliminaries.

14.34. A finite-dimensional Lie algebra $\mathfrak{g}$ is said to be ***nilpotent*** if it admits a filtration

$$\mathfrak{g} = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_{r-1} \supset \mathfrak{a}_r = 0$$

by ideals such that $[\mathfrak{g}, \mathfrak{a}_i] \subset \mathfrak{a}_{i+1}$ for all i. Note that then

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

for all $x_1, \ldots, x_r, y \in \mathfrak{g}$; in other words,

$$\mathrm{ad}(x_1) \circ \cdots \circ \mathrm{ad}(x_r) = 0$$

for all $x_1, \ldots, x_r \in \mathfrak{g}$. We shall need the following two statements:

  (a) 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, then there exists a basis of V for which $\rho(V) \subset \mathfrak{n}_n$ (Engel's theorem; Jacobson 1962, II, 3);

  (b) every finite-dimensional Lie algebra admits a finite-dimensional faithful representation; when $\mathfrak{g}$ is nilpotent, (V, ρ) can be chosen so that $\rho(\mathfrak{g})$ consists of nilpotent endomorphisms (Ado–Iwasawa theorem; Jacobson 1962, VI).

14.35. Let

$$\exp(U) = 1 + U + U^2/2 + U^3/3! + \cdots \quad \in \mathbb{Q}[[U]].$$

The ***Campbell–Hausdorff series***[3] is a formal power series $H(U, V)$ in the non-commuting symbols U and V with coefficients in $\mathbb{Q}$ such that

$$\exp(U) \cdot \exp(V) = \exp(H(U, V)).$$

It can be defined as

$$\log(\exp(U) \cdot \exp(V)),$$

where

$$\log(T) = \log(1 - (1 - T)) = -\left(\frac{1-T}{1} + \frac{(1-T)^2}{2} + \frac{(1-T)^3}{3} + \cdots \right).$$

Write

$$H(U, V) = \sum_{m \geq 0} H^m(U, V)$$

with $H^m(U, V)$ a homogeneous polynomial of degree m. Then

$$H^0(U, V) = 0$$
$$H^1(U, V) = U + V$$
$$H^2(U, V) = \frac{1}{2}[U, V] = \frac{1}{2}(\mathrm{ad}U)(V)$$

---

[3] Bourbaki writes "Hausdorff", Demazure and Gabriel write "Campbell–Hausdorff", and others write "Baker–Campbell–Hausdorff".

and $H^m(U,V)$, $m \geq 3$, is a sum of terms each of which is a scalar multiple of

$$\mathrm{ad}(U)^r \mathrm{ad}(V)^s(V), \qquad r+s = m,$$

or

$$\mathrm{ad}(U)^r \mathrm{ad}(V)^s(U), \qquad r+s = m-1,$$

([Bourbaki 1972](), II, §6, no. 4, Thm 2). Here

$$\mathrm{ad}(V)(U) \overset{\mathrm{def}}{=} [V,U] \overset{\mathrm{def}}{=} VU - UV.$$

For a nilpotent matrix X in $M_n(k)$,

$$\exp(X) \overset{\mathrm{def}}{=} 1 + X + X^2/2 + X^3/3! + \cdots$$

is a well-defined element of $\mathrm{GL}_n(k)$. If $X,Y \in \mathfrak{n}_n$, then $\mathrm{ad}(X)^n = 0 = \mathrm{ad}(Y)^n$, and so $H^m(X,Y) = 0$ for all m sufficiently large; therefore $H(X,Y)$ is a well-defined element of $\mathfrak{n}_n$, and

$$\exp(X) \cdot \exp(Y) = \exp(H(X,Y)).$$

PROPOSITION 14.36. *Let G be a unipotent algebraic group. Then*

$$\exp(x) \cdot \exp(y) = \exp(H(x,y)) \tag{94}$$

for all k-algebras R and $x,y \in \mathfrak{g}_R$.

PROOF. We may identify G with an algebraic subgroup of GL_V (V a finite-dimensional k-vector space). Then $\mathfrak{g} \subset \mathfrak{n}_n$ for a suitable basis of V (see [14.31]()), and so, for $x,y \in \mathfrak{g}_R$,

$$H(x,y) \overset{\mathrm{def}}{=} \sum H^m(x,y)$$

is a well-defined element of $\mathfrak{g}$, and (94) holds because it holds in $\mathfrak{n}_n$. $\qquad\square$

THEOREM 14.37. *(a) Let $\mathfrak{g}$ be a finite-dimensional nilpotent Lie algebra $\mathfrak{g}$ over k. The maps*

$$(x,y) \mapsto H(x,y) \colon \mathfrak{g}(R) \times \mathfrak{g}(R) \to \mathfrak{g}(R) \quad (R \text{ a } k\text{-algebra})$$

make $\mathfrak{g}_\mathfrak{a}$ into a unipotent algebraic group over k.

(b) The functor $\mathfrak{g} \rightsquigarrow \mathfrak{g}_\mathfrak{a}$ defined in (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. (a) For the Lie algebra $\mathfrak{n}_n$, Proposition [14.36]() shows that the maps make $(\mathfrak{n}_n)_\mathfrak{a}$ into the algebraic group $\mathbb{U}_n$. It follows that the maps make every Lie subalgebra of $\mathfrak{g}$ into an algebraic subgroup of $\mathbb{U}_n$. Now the theorems of Ado and Engel show that every nilpotent Lie algebra arises as a subalgebra of $\mathfrak{n}_n$ for some n.

(b) The two functors are quasi-inverse: $\mathrm{Lie}(\mathfrak{g}_\mathfrak{a}) \simeq \mathfrak{g}$ and $\mathrm{Lie}(G)_\mathfrak{a} \simeq G$. $\qquad\square$

COROLLARY 14.38. *Every Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}_V$ consisting of nilpotent endomorphisms is the Lie algebra of an algebraic group (V finite-dimensional).*

PROOF. According to Engel's theorem, $\mathfrak{g}$ is nilpotent, and so $\mathfrak{g} = \mathrm{Lie}(\mathfrak{g}_a)$. $\qquad \square$

ASIDE 14.39. (a) Theorem 14.37 reduces the problem of classifying unipotent algebraic groups in characteristic zero to that of classifying nilpotent Lie algebras. In dimensions greater than 6, there are families of nilpotent Lie algebras depending on parameters, and so the classification becomes a question of studying the moduli schemes. Up to dimension 6, there are complete lists (see, for example, de Graaf 2007).

(b) Some of the above theory holds also in characteristic p for "large p". Moreover, under some hypotheses on G and k, there are Springer isomorphisms of algebraic varieties $G^u \to \mathfrak{g}^n$, where G^u (resp. $\mathfrak{g}^n$) is the reduced subscheme of G (resp. $\mathfrak{g}_a$) whose points are the unipotent (resp. nilpotent) elements. See the discussions in Balaji et al. 2016, 2.2, and McNinch 2005, §4,

NOTES. This section follows DG, IV, §2, no. 4.

e. Unipotent algebraic groups in nonzero characteristic

In this section, k is a field of characteristic $p \neq 0$. We let σ denote the endomorphism $x \mapsto x^p$ of k, and we let $k_\sigma[F]$ denote the ring of polynomials

$$c_0 + c_1 F + \cdots + c_m F^m, \quad c_i \in k,$$

with multiplication defined by

$$Fc = c^\sigma F, \quad c \in k.$$

When we set $x^{[p]} = Fx$, a $k_\sigma[F]$-module becomes a p-Lie algebra with trivial bracket (see 10.39).

Recall (2.1) that $\mathcal{O}(\mathbb{G}_a) = k[T]$ with $\Delta(T) = T \otimes 1 + 1 \otimes T$. Therefore, to give a homomorphism $G \to \mathbb{G}_a$ amounts to giving an element $f \in \mathcal{O}(G)$ such that

$$\Delta_G(f) = f \otimes 1 + 1 \otimes f. \tag{95}$$

Such an f is said to be **primitive**, and we write $P(G)$ for the set of primitive elements in G; thus

$$\mathrm{Hom}(G, \mathbb{G}_a) \simeq P(G). \tag{96}$$

EXAMPLE 14.40. Let $f = \sum c_i T^i \in \mathcal{O}(\mathbb{G}_a)$. The condition (95) becomes

$$c_i (T \otimes 1 + 1 \otimes T)^i = c_i (T^i \otimes 1 + 1 \otimes T^i)$$

for all i. Let $T_1 = T \otimes 1$ and $T_2 = 1 \otimes T$; then the condition becomes that

$$c_i (T_1 + T_2)^i = c_i (T_1^i + T_2^i) \quad \text{(equality in } k[T_1, T_2]).$$

In particular, $c_0 = 0$. For $i \geq 1$, write $i = mp^j$ with m prime to p; then

$$(T_1 + T_2)^i = (T_1^{p^j} + T_2^{p^j})^m,$$

which equals $T_1^{mp^j} + T_2^{mp^j}$ if and only if $m = 1$. Thus $c_i = 0$ unless $m = 1$, and so the primitive elements in $\mathcal{O}(\mathbb{G}_a)$ are the polynomials

$$\sum_{j \geq 0} b_j T^{p^j} = b_0 T + b_1 T^p + \cdots + b_n T^{p^n}, \quad b_j \in k.$$

For $c \in k$, let c (resp. F) denote the endomorphism of $\mathbb{G}_a$ acting on R-points as $x \mapsto cx$ (resp. $x \mapsto x^p$). Then $Fc = c^\sigma F$, and so we have a homomorphism

$$k_\sigma[F] \to \mathrm{End}(\mathbb{G}_a) \simeq P(\mathbb{G}_a).$$

This sends $\sum b_j F^j$ to the primitive element $\sum b_j T^{p^j}$, and so it is an isomorphism:

$$k_\sigma[F] \simeq \mathrm{End}(\mathbb{G}_a) \simeq P(\mathbb{G}_a). \tag{97}$$

Note that $\sum b_j F^j$ acts on $\mathbb{G}_a(R) = R$ as $c \mapsto \sum b_j c^{p^j}$.

Let G be an algebraic group. From the isomorphism $k_\sigma[F] \simeq \mathrm{End}(\mathbb{G}_a)$, we get an action of $k_\sigma[F]$ on $P(G) \simeq \mathrm{Hom}(G, \mathbb{G}_a)$. Explicitly, for $f \in \mathcal{O}(G)$ and $c \in k$, $cf = c \circ f$ and $Ff = f^p$. The reader should check directly that these actions preserve the primitive elements. Now P is a contravariant functor from algebraic groups to $k_\sigma[F]$-modules.

PROPOSITION 14.41. *Let M be a finitely generated $k_\sigma[F]$-module. Among the pairs consisting of an algebraic group G and a $k_\sigma[F]$-module homomorphism $u: M \to P(G)$ there is one $(U(M), u_M)$ that is universal: for each pair (G, u), there exists a unique homomorphism $\alpha: G \to U(M)$ such that $P(\alpha) \circ u_M = u$:*

$$
\begin{array}{ccc}
U(M) & M \xrightarrow{\;u_M\;} P(U(M)) \\
\big\uparrow{\scriptstyle \exists! \alpha} & \quad\searrow{\scriptstyle u} \quad \big\downarrow{\scriptstyle P(\alpha)} \\
G & P(G).
\end{array}
$$

PROOF. Let M be a finitely generated $k_\sigma[F]$-module. Regard M as a p-Lie algebra with trivial bracket. The universal enveloping p-algebra $U^{[p]}(M)$ is a Hopf algebra, and we define

$$U(M) = \mathrm{Spm}(U^{[p]}(M), \Delta).$$

Let $u_M: M \to P(U(M))$ denote the map defined by $j: M \to U^{[p]}(M)$. The pair $(U(M), u_M)$ is universal, because

$$\mathrm{Hom}(G, U(M)) \simeq \mathrm{Hom}((U^{[p]}(M), \Delta), (\mathcal{O}(G), \Delta_G))$$
$$\simeq \mathrm{Hom}_{k_\sigma[F]}(M, P(G)).$$

The second isomorphism states the universal property of $j: M \to U^{[p]}(M)$ (see p.). $\qquad\square$

The proposition says that the functor P has an adjoint functor U:

$$\operatorname{Hom}_{k_\sigma[F]}(M, P(G)) \simeq \operatorname{Hom}(G, U(M)). \tag{98}$$

Hence P and U map direct limits to inverse limits (in particular, they map right exact sequences to left exact sequences).

REMARK 14.42. From the bijections

$$
\begin{aligned}
\operatorname{Hom}(G, U(k_\sigma[F])) &\simeq \operatorname{Hom}_{k_\sigma[F]}(k_\sigma[F], P(G)) &&\text{(see (98))} \\
&\simeq P(G) &&\text{(obvious)} \\
&\simeq \operatorname{Hom}(G, \mathbb{G}_a) &&\text{(see (96))}
\end{aligned}
$$

we see that $U(k_\sigma[F]) \simeq \mathbb{G}_a$. Every finitely generated $k_\sigma[F]$-module M is a quotient of a free $k_\sigma[F]$-module of finite rank, and so $U(M)$ is an algebraic subgroup of $\mathbb{G}_a^r$ for some r. In particular, it is algebraic, unipotent, and commutative.

LEMMA 14.43. *For a finitely generated $k_\sigma[F]$-module M, the canonical map $u_M: M \to P(U(M))$ is bijective.*

PROOF. We have to show that the canonical map $j: M \to U^{[p]}(M)$ induces a bijection from M onto the set of primitive elements of $U^{[p]}(M)$. Let $(e_i)_{i \in I}$ be a basis for M as a k-vector space. The PBW Theorem 10.36 shows that the finite products

$$u_n = \prod_{i \in I} \frac{j(e_i)^{n_i}}{n_i!}, \quad n = (n_i)_{i \in I}, \quad 0 \le n_i < p,$$

form a basis for $U^{[p]}(M)$ as a k-vector space (see 10.40). As the $j(e_i)$ are primitive,

$$\Delta u_n = \sum_{r+s=n} u_r \otimes u_s,$$

which shows that the only primitive elements of $U^{[p]}(M)$ are the linear combinations of the u_n with $\sum n_i = 1$.   □

For a commutative algebraic group G, let $v_G: G \to U(P(G))$ denote the adjunction map; by definition, $P(v_G) \circ u_{P(G)} = \operatorname{id}_{P(G)}$. As $u_{P(G)}$ is bijective, so also is $P(v_G)$.

LEMMA 14.44. *For a commutative algebraic group G over k, the homomorphism $v_G: G \to U(P(G))$ is a quotient map.*

PROOF. On applying P to the right exact sequence

$$G \xrightarrow{v_G} U(P(G)) \to Q \to 0, \quad Q \overset{\text{def}}{=} \operatorname{Coker}(v_G),$$

we get a left exact sequence

$$0 \to P(Q) \to P(U(P(G)) \xrightarrow{P(v_G)} P(G).$$

As $P(v)$ is bijective, $P(Q) = 0$, and so Q is multiplicative (12.18). As it is also the quotient of a unipotent algebraic group, it is trivial (14.18).   □

DEFINITION 14.45. An algebraic group is ***elementary unipotent***[4] if it embeds into a vector group $V_{\mathfrak{a}}$.

Equivalently, G is elementary unipotent if and only if $\mathcal{O}(G)$ is generated by the homomorphisms $G \to \mathbb{G}_a$. Note that an algebraic group is unipotent if and only if it has a normal series whose quotients are elementary unipotent algebraic groups (14.21).

THEOREM 14.46. *The functor $G \rightsquigarrow P(G)$ defines a contravariant equivalence from the category of elementary unipotent algebraic groups to the category of finitely generated $k_{\sigma}[F]$-modules, with quasi-inverse $M \rightsquigarrow U(M)$.*

PROOF. Because of Lemma 14.43, the adjoint functors P and U define an equivalence of the essential image of U with the category of finitely generated $k_{\sigma}[M]$-modules. We have seen (14.42) that every algebraic group in the essential image of U is elementary unipotent. Conversely, let $i\colon G \to \mathbb{G}_a^r$ be an algebraic subgroup of $\mathbb{G}_a^r$. In the commutative diagram

$$
\begin{array}{ccc}
G & \xrightarrow{\ \ i\ \ } & \mathbb{G}_a^r \\
\ \downarrow{v_G} & & \ \downarrow{v} \\
U(P(G)) & \longrightarrow & U(P(\mathbb{G}_a^r)),
\end{array}
$$

the map i is an embedding and v is an isomorphism. Therefore v_G is an embedding. As it is also a quotient map (14.44), it must be an isomorphism (5.33), and so G is in the essential image of the functor U.   □

COROLLARY 14.47. *Let G be an elementary unipotent group. Every algebraic subgroup of G isomorphic to $\mathbb{G}_a$ is a direct factor of G.*

PROOF. An exact sequence

$$e \to \mathbb{G}_a \to G \to Q \to e$$

corresponds to an exact sequence

$$0 \to P(Q) \to P(G) \to k_{\sigma}[F] \to 0$$

of $k_{\sigma}[F]$-modules, which obviously splits (choose a $p \in P(G)$ mapping to $1 \in k_{\sigma}[F]$, and send $a \in k_{\sigma}[F]$ to ap).   □

PROPOSITION 14.48. *A commutative algebraic group G is elementary unipotent if and only if $V_G = 0$.*

---

[4]Springer 1998, 3.4.1, 3.4.8, and others use this terminology for group varieties. For Demazure and Gabriel, they are the "groupes annulés par décalage", i.e., killed by the Verschiebung (DG, IV §3, 6.6, p. 521).

PROOF. The necessity follows from 11.41. For the sufficiency, let G be a commutative algebraic group G such that $V_G = 0$. To show that G is elementary unipotent, it suffices to show that the homomorphism $v_G \colon G \to U(P(G))$ is an isomorphism, and it suffices to do this after an extension of k. Therefore, we may suppose that k is perfect. We shall need to use that, for an algebraic subgroup Q of $\mathbb{G}_a$, every nontrivial commutative extension of Q by $\mathbb{G}_a$ comes by pull-back from the extension

$$0 \to \mathbb{G}_a \xrightarrow{V} W_2 \to \mathbb{G}_a \to 0 \tag{99}$$

(15.27 below). Arguing by induction on the length of a subnormal series for G, we may suppose that G contains a subgroup N such that $Q = G/N$ embeds into $\mathbb{G}_a$ and N embeds into $\mathbb{G}_a^r$. If we show that every homomorphism $N \to \mathbb{G}_a$ extends to G, then the homomorphism $N \hookrightarrow \mathbb{G}_a^r$ extends to G (because its components do), and we will have an embedding of G into $\mathbb{G}_a^r \times \mathbb{G}_a$, as required. Let $\varphi \colon N \to \mathbb{G}_a$ be a homomorphism, and form the diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \| & & \\
0 & \longrightarrow & \mathbb{G}_a & \longrightarrow & G' & \longrightarrow & Q & \longrightarrow & 0
\end{array}
$$

with the bottom row the pushout of the top row. If the extension in the lower row splits, then φ extends to G. Otherwise, the lower row comes by pull-back from (99). But $V_{G'} = 0$ because G' is a quotient of $G \times \mathbb{G}_a$, and so the homomorphism $G' \to W_2$ factors through $\mathbb{G}_a \subset W_2$, and so again φ extends to G. For more details, see DG, IV, §3, 6.6.   □

PROPOSITION 14.49. *Every smooth commutative algebraic group G of exponent p is elementary unipotent.*

PROOF. Because G is smooth, $V_G = 0$ (see 11.41), and so G is elementary unipotent by 14.48.   □

The ring $k_\sigma[F]$ behaves somewhat like the usual polynomial ring $k[T]$. In particular, the right division algorithm holds: given f and g in $k_\sigma[F]$ with $g \neq 0$, there exist unique elements q, r with $r = 0$ or $\deg(r) < \deg(g)$ such that $f = qg + r$. The proof is the same as for the usual division algorithm.

PROPOSITION 14.50. *The left ideals in $k_\sigma[F]$ are principal. Every submodule of a free finitely generated left $k_\sigma[F]$-module is free.*

PROOF. The proofs are similar to those for $k[T]$. See Berrick and Keating 2000, Theorem 3.2.10 and Lemma 3.3.5.   □

When k is perfect, the map $\sigma \colon k \to k$ is an automorphism, and the left division algorithm also holds: given f and g in $k_\sigma[F]$ with $g \neq 0$, there exist unique elements q, r with $r = 0$ or $\deg(r) < \deg(g)$ such that $f = gq + r$.

PROPOSITION 14.51. *When k is perfect, every finitely generated left $k_\sigma[F]$-module M is a direct sum of cyclic modules $k_\sigma[F]/k_\sigma[F]g$ with $g = 0$ or irreducible; if, moreover, M has no torsion, then it is free.*

PROOF. The proof is similar to that for $k[T]$. See Berrick and Keating 2000, Theorem 3.3.6. □

PROPOSITION 14.52. *When k is perfect, every elementary unipotent algebraic group G over k is a product of algebraic groups of the form $\mathbb{G}_a$, α_{p^r} for some r, or an étale group of order a power of p.*

PROOF. Let $A = k_\sigma[F]$. According to Proposition 14.51, $P(G)$ is a finite direct sum of cyclic modules A/Ag, $g \in A$. Correspondingly, G is a product of algebraic groups G' such that $P(G')$ is cyclic. Let G' be the algebraic group with $P(G) = A/Ag$. If $g = 0$, then $G \approx \mathbb{G}_a$; if $g = F^r$, then $G \approx \alpha_{p^r}$; and if g is not divisible by F, then G is étale. □

COROLLARY 14.53. *When k is perfect, every smooth connected elementary unipotent group is isomorphic to $(\mathbb{G}_a)^d$ for some d. The proper connected subgroups of $\mathbb{G}_a$ are the groups α_{p^r}, $r \geq 0$.*

PROOF. Immediate consequence of Proposition 14.52. □

PROPOSITION 14.54. *When k is perfect, every smooth connected commutative group G of exponent p over a perfect field k is isomorphic to $\mathbb{G}_a^r$.*

PROOF. Such a group G is elementary unipotent (14.48). Therefore it corresponds in Theorem 14.46 to the $k_\sigma[F]$-module $P(G) \simeq \mathrm{Hom}(G, \mathbb{G}_a)$, which is torsion-free because G is connected and smooth. Because k is perfect, this implies that $P(G)$ is free, of rank r say, and so G is isomorphic to $\mathbb{G}_a^r$. □

COROLLARY 14.55. *When k is perfect, every nontrivial connected unipotent group variety U over k contains a central subgroup variety isomorphic to $\mathbb{G}_a$.*

PROOF. As U is nilpotent (14.21), it contains a nontrivial connected group variety U' in its centre (6.40). Now apply (14.54) to $(U'')^\circ_{\mathrm{red}}$ where U'' is the kernel of $p\colon U' \to U'$. □

COROLLARY 14.56. *Every smooth connected commutative algebraic group of exponent p is a form of $\mathbb{G}_a^r$ for some r.*

PROOF. It becomes isomorphic to $\mathbb{G}_a^r$ over a perfect closure of the base field. □

EXAMPLE 14.57. Let k be a nonperfect field of characteristic p. For every finite sequence $a_0, \ldots, a_m$ of elements of k with $a_0 \neq 0$ and $m \geq 1$, the algebraic subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^{p^n} = a_0 X + a_1 X^p + \cdots + a_m X^{p^m}$$

is a form of $\mathbb{G}_a$, and every form of $\mathbb{G}_a$ arises in this way (Russell 1970, 2.1). Rosenlicht's group (1.56) can be expressed in this form. Note that G is the fibred product

$$
\begin{array}{ccc}
G & \longrightarrow & \mathbb{G}_a \\
\downarrow & & \downarrow {\scriptstyle a_0 F + \cdots + a_m F^{p^m}} \\
\mathbb{G}_a & \xrightarrow{\ F^n\ } & \mathbb{G}_a.
\end{array}
$$

In particular, G is an extension of $\mathbb{G}_a$ by a finite subgroup of $\mathbb{G}_a$ (so it does satisfy 14.21). There is a criterion for when two forms are isomorphic (Russell 1970, 2.3). In the case $a_0 = 1$, G becomes isomorphic to $\mathbb{G}_a$ over an extension K of k if and only if K contains a p^nth root of each a_i.

For a classification of the forms of $\mathbb{G}_a^r$, in which the elements a_i are replaced by matrices, see Kambayashi et al. 1974, 2.6.

NOTES. This section follows DG, IV, §3, no. 6. See also Springer 1998, 3.3, 3.4.

f.   Algebraic groups isomorphic to $\mathbb{G}_a$

14.58. Let G be an algebraic group over k. If G is isomorphic to $\mathbb{G}_a$, then G is smooth, connected, unipotent, and one-dimensional, and the converse is true when k is perfect (14.53). Every nontrivial quotient of a group isomorphic to $\mathbb{G}_a$ is isomorphic to $\mathbb{G}_a$ (Exercise 14-3a).

14.59. Every regular map $\mathbb{A}_k^1 \to \mathbb{A}_k^1$ is of the form $c \mapsto f(c)$ for a unique polynomial $f \in k[T]$. An elementary calculation shows that the map is an isomorphism if and only if $f(T) = a_0 + a_1 T$ with a_1 invertible. Let R be a k-algebra. Every map $\mathbb{A}_R^1 \to \mathbb{A}_R^1$ of R-schemes is of the form $c \mapsto f(c)$ for a unique polynomial $f(T) = \sum_{i \geq 0} a_i T^i$, $a_i \in R$. If the map is an automorphism, then, for all maximal ideals $\mathfrak{m}$ in R, we have $a_1 \notin \mathfrak{m}$ and $a_i \in \mathfrak{m}$ for $i > 1$; hence $a_1 \in R^\times$ and a_i is nilpotent for $i > 1$. In particular, if R is reduced, then the only automorphisms of $\mathbb{A}_R^1$ are the maps $c \mapsto f(c)$ with $f(T) = a_0 + a_1 T$, $a_0 \in R$, $a_1 \in R^\times$. It follows that, if R is reduced, then the only automorphisms of the group scheme $\mathbb{G}_{aR}$ over R are the maps $c \mapsto ac$, $a \in R^\times$.

14.60. Let X be an algebraic variety over k. In this paragraph we let $\tilde{X}$ denote the functor $R \rightsquigarrow X(R)$ of *reduced* small k-algebras. The Yoneda lemma in this context says that the functor $X \rightsquigarrow \tilde{X}$ is fully faithful. Let $\underline{\mathrm{Aut}}(\mathbb{G}_a)$ denote the functor $R \rightsquigarrow \mathrm{Aut}_R(\mathbb{G}_{aR})$ of *reduced* small k-algebras. We saw in the last paragraph that $\underline{\mathrm{Aut}}(\mathbb{G}_a) \simeq \mathbb{G}_m$. Let U be an algebraic group over k isomorphic to $\mathbb{G}_a$. The choice of an isomorphism $i \colon \mathbb{G}_a \to U$ determines an isomorphism $\underline{\mathrm{Aut}}(U) \simeq \mathbb{G}_m$ which is *independent of the choice of i* (because the automorphism group is commutative). Therefore, to give an action of a group variety G on $\mathbb{G}_a$ by group homomorphisms is the same as giving a homomorphism $G \to \mathbb{G}_m$.

g.   Split and wound unipotent groups

Recall (14.21) that unipotent groups are solvable, and so the next definition is a special case of Definition 6.33.

DEFINITION 14.61. A unipotent algebraic group G over k is ***split*** if it admits a subnormal series each of whose quotients is isomorphic to $\mathbb{G}_a$.

14.62. A split unipotent algebraic group is automatically smooth and connected (8.1). If G is split over k, then $G_{k'}$ is split over k' for all fields k' containing k.

14.63. Recall (14.21) that every unipotent algebraic group admits a normal series whose quotients are *subgroups* of $\mathbb{G}_a$. In characteristic zero, $\mathbb{G}_a$ has no proper subgroups (14.24), and so all connected unipotent algebraic groups are split. In characteristic p, a connected unipotent group variety need not be split, but it is if the ground field is perfect – this follows by induction from 14.55. Hence every connected unipotent group variety splits over a finite purely inseparable extension of the ground field.

14.64. An elementary unipotent group G over k is split if and only if it iso-morphic to $\mathbb{G}_a^r$ for some r. This follows by induction from 14.47.

14.65. A unipotent group G over k is split if it splits over a separable field extension k' of k. In proving this, we may suppose that G is elementary and that k' is finite over k. If $\{x_1,\dots,x_n\}$ is a basis for k' as a k-vector space, then so also is $\{x_1^{p^r},\dots,x_n^{p^r}\}$ for all r (here we use that k' is separable over k), and it follows that $\{x_1,\dots,x_n\}$ is a basis for $k'_\sigma[F]$ as a $k_\sigma[F]$-module. We know that $P(G_{k'})$ is a free $k'_\sigma[F]$-module, and so $P(G)$ is a submodule of a free $k_\sigma[F]$-module. This implies that it is free (14.50).

14.66. Let G be a split unipotent algebraic group of dimension n. Then the underlying scheme of U is isomorphic to $\mathbb{A}^n$. Indeed, inductively, G is a $\mathbb{G}_a$-torsor over $\mathbb{A}^{n-1}$ (2.68), and such a torsor is trivial (2.72).

14.67. A form of $\mathbb{G}_a^r$ over k is split if and only if it is trivial (i.e., isomorphic to $\mathbb{G}_a^r$ over k). This follows from 14.64. In particular, every nontrivial form of $\mathbb{G}_a$, e.g., Rosenlicht's group $Y^p - Y = tX^p$ (see 1.56), is nonsplit. Moreover, every split smooth connected commutative algebraic group of exponent p is isomorphic to $\mathbb{G}_a^r$ for some r (see 14.56).

14.68. The algebraic group $\mathbb{U}_n$ is split (6.49). Every connected group variety admitting an action by a split torus with only nonzero weights is a split unipotent group (16.63 below). For example, the unipotent radical of a parabolic subgroup of a reductive algebraic groups is split.

DEFINITION 14.69. A connected unipotent group variety G is ***wound*** if every morphism from the affine line to G is constant.

Just as split unipotent groups are the additive analogue of split tori, wound unipotent groups are the additive analogue of anisotropic tori (compare the definition with Exercise 12-5). This rest of this section is only a brief summary.

14.70. In characteristic zero, the only wound unipotent group is the trivial group. Over a perfect field of characteristic p, the wound unipotent groups are those that are finite.

14.71. A unipotent group variety G is wound if and only if G does not contain a subgroup variety isomorphic to $\mathbb{G}_a$. Hence every nontrivial (hence nonsplit) form of $\mathbb{G}_a$ is wound.

14.72. If G is wound, then it admits a subnormal series formed of wound characteristic subgroups whose quotients are wound commutative and killed by p. Proofs of this are complicated by the fact that quotients of wound unipotent groups by smooth connected proper subgroups can be split. See Conrad et al. 2015, B.2.3, B.3.2, and B.3.3.

14.73. Subgroups and extensions of wound group varieties are wound, but not necessarily quotients – for example, every form of $\mathbb{G}_a$ admits $\mathbb{G}_a$ as a quotient.

14.74. Every unipotent group variety G is isomorphic to a subgroup variety of a split unipotent group variety H (see 14.3). If G is commutative, H can be chosen commutative. If G is commutative of exponent p, then it is elementary unipotent (14.48; see also Tits 1968, 3.3.1). In general, it is not possible to choose H so that G is a normal subgroup.

14.75. (Structure theorem). Let G be a connected unipotent group variety. Then G contains a unique normal connected split subgroup variety G_{split} such that $W = G/G_{\mathrm{split}}$ is wound:

$$e \to G_{\mathrm{split}} \to G \to W \to e.$$

The subgroup variety G_{split} contains all connected split subgroup varieties of G, and its formation commutes with separable (not necessarily inseparable) extensions (Tits 1968, 4.2).

14.76. Tits (1968, p. 3) remarks that he knows of no connected wound group that is not commutative and of exponent p. An example of a noncommutative such group was found by Gabber (Conrad et al. 2015, B.2.9).

NOTES. (a) In the literature, one usually finds "k-split" and "k-wound" for "split" and "wound" (e.g., Tits 1968, 4.1). We can omit the "k" because of our convention that statements concerning an algebraic group G over k are intrinsic to G over k. Oesterlé (1984, 3.1) writes "déployé" and "totalement ployé" for "split" and "wound".

(b) To paraphrase Oesterlé (1984), the paternity of the results in this section is not always easy to attribute. Most of the questions were considered for the first time by Rosenlicht (1963), reconsidered and developed in detail by Tits (1968), and extended to group schemes by Demazure and Gabriel (1970).

(c) For a modern exposition of the material in this section, see Conrad et al. 2015, Appendix B.

Exercises

EXERCISE 14-1. Prove or disprove the following statement: every algebraic group contains a largest connected unipotent normal algebraic subgroup.

EXERCISE 14-2. Use Theorem 14.46 to prove Russell's theorem, 14.57.

EXERCISE 14-3 (DG, IV, §2, 1.1). Let H be an algebraic subgroup of $\mathbb{G}_a$ over k such that $H \neq \mathbb{G}_a$. If $\mathrm{char}(k) = 0$, then $H = e$, and so we suppose that $\mathrm{char}(k) = p \neq 0$ and we let F denote the endomorphism $a \mapsto a^p$ of $\mathbb{G}_a$. Prove the following statements.

(a) There exists an endomorphism φ of $\mathbb{G}_a$ such that the sequence

$$e \to H \to \mathbb{G}_a \xrightarrow{\varphi} \mathbb{G}_a \to e$$

is exact.

(b) Write

$$\varphi = a_r F^r + a_{r+1} F^{r+1} + \cdots + a_s F^s$$

with $r, s \in \mathbb{N}$, $a_r, \ldots, a_s \in k$, and $a_r \neq 0 \neq a_s$ (cf. 14.40). Then $H^\circ \approx \alpha_{p^r}$,

$$\pi_0(H) = \mathrm{Ker}(a_r \,\mathrm{id} + a_{r+1} F + \cdots + a_s F^{s-r}),$$

and $\pi_0(H)(k^s) \approx (\mathbb{Z}/p\mathbb{Z})^{s-r}$.

(c) If H is stable under the natural action of $\mathbb{G}_m$ on $\mathbb{G}_a$, then it is connected.

EXERCISE 14-4. Prove directly that there is no nontrivial homomorphism $\mu_\ell \to \mathbb{G}_a$. Deduce another proof of Proposition 14.16.

EXERCISE 14-5. Let G be a connected group variety over a finite extension k' of k. Show that if G is unipotent (resp. split unipotent), then so is $(G)_{k'/k}$.

Cohomology and Extensions

All schemes are algebraic over a base field k unless indicated otherwise. All functors are from the category of small k-algebras to sets or groups. By an action of a group on a group we mean an action by group homomorphisms. Recall that all algebraic groups are affine over the base field k.

a. Crossed homomorphisms

Let $G \times M \to M$ be an action of a group functor G on a group functor M by group homomorphisms. Such an action corresponds to a homomorphism $G \to \underline{\mathrm{Aut}}(M)$, where $\underline{\mathrm{Aut}}(M)$ is the functor sending R to the group of automorphisms of M_R (as a group functor of R-algebras). A map of functors $f \colon G \to M$ is a *crossed homomorphism* if

$$f(gg') = f(g) \cdot g f(g')$$

for all small k-algebras R and $g, g' \in G(R)$. When G is a smooth algebraic group and M is representable, it suffices to check the condition for $g, g' \in G(k^{\mathrm{s}})$ (see 1.17, 1.22). For $m \in M(k)$, the map

$$g \mapsto m^{-1} \cdot g m \colon G \to M$$

is a crossed homomorphism. The crossed homomorphisms of this form are said to be *principal*.

EXAMPLE 15.1. Let $G \times M \to M$ be an action of a group functor G on a group functor M, and let $\theta \colon G \to \underline{\mathrm{Aut}}(M)$ be the corresponding homomorphism. Let $M \rtimes_\theta G$ denote the semidirect product defined by θ. There is an exact sequence

$$e \to M \to M \rtimes_\theta G \to G \to e,$$

and the group sections to the homomorphism $M \rtimes_\theta G \to G$ are the maps $g \mapsto (f(g), g)$ with f a crossed homomorphism. For example, there is always a

group section $g \mapsto (e,g)$. The sections of the form $g \mapsto (m,e)^{-1} \cdot (e,g) \cdot (m,e)$ correspond to principal crossed homomorphisms.

LEMMA 15.2. *Let U be a unipotent algebraic group, and let e be an integer not divisible by the characteristic of k. Then the map $x \mapsto x^e : U(k^a) \to U(k^a)$ is bijective.*

PROOF. This is obviously true for $\mathbb{G}_a$. A proper algebraic subgroup N of $\mathbb{G}_a$ is finite, and the map on $N(k^a)$ is injective, and so it is bijective. As every unipotent group admits a filtration whose quotients are subgroups of $\mathbb{G}_a$ (see 14.21), and the functor $U \rightsquigarrow U(k^a)$ is exact (5.48), the general case follows. □

PROPOSITION 15.3. *Let G be a diagonalizable group variety over an algebraically closed field k and M a commutative unipotent group variety on which it acts. Then every crossed homomorphism $f : G \to M$ is principal.*

PROOF. Let $n > 1$ be an integer not divisible by the characteristic of k, and let G_n denote the kernel of multiplication by n on G. Then $G_n(k)$ is finite, of order e_n not divisible by the characteristic of k.

Let $f : G \to M$ be a crossed homomorphism, so that

$$f(x) = f(xy) - x \cdot f(y)$$

for all $x, y \in G(k)$. When we sum this identity over all $y \in G_n(k)$, we find that

$$e_n f(x) = s - x \cdot s, \quad s = \sum f(y).$$

Since we can divide by e_n in M, this shows that the restriction of f to G_n is principal. In other words, the set

$$M(n) = \{m \in M(k) \mid f(x) = x \cdot m - m \text{ for all } x \in G_n(k)\}$$

is nonempty. The set $M(n)$ is closed in $M = M(k)$, and so the descending sequence

$$\cdots \supset M(n) \supset M(n+1) \supset \cdots$$

eventually becomes constant (and nonempty). This implies that there exists an $m \in M(k)$ such that

$$f(x) = x \cdot m - m$$

for all $x \in \bigcup G_n(k)$. It follows from Theorem 12.32 that f agrees with the principal crossed homomorphism $x \mapsto x \cdot m - m$ on G. □

b. Hochschild cohomology

Let G be a group functor. A **G-module** is a commutative group functor M equipped with an action of G by group homomorphisms. Thus $M(R)$ is a $G(R)$-module in the usual sense for each k-algebra R. Much of the basic formalism of group cohomology carries over to this setting. We first define the standard complex.

Let M be a G-module. Define

$$C^n(G, M) = \mathrm{Map}(G^n, M)$$

(maps of set-valued functors). By definition, $G^0 = e$, and so $C^0(G, M) = M(k)$. The set $C^n(G, M)$ acquires a commutative group structure from that on M. If G is an algebraic group with coordinate ring A, then $C^n(G, M) = M(A^{\otimes n})$.

An element f of $C^n(G, M)$ defines an n-cochain $f(R)$ for $G(R)$ with values in $M(R)$ for each k-algebra R. The coboundary map

$$\partial^n : C^n(G, M) \to C^{n+1}(G, M)$$

is defined by the usual formula: let $g_1, \dots, g_{n+1} \in G(R)$; then

$$\begin{aligned}
(\partial^n f)(g_1, \dots, g_{n+1}) = {} & g_1 f(g_2, \dots, g_{n+1}) \\
& + \sum_{j=1}^{n} (-1)^j f(g_1, \dots, g_j g_{j+1}, \dots, g_{n+1}) \\
& + (-1)^{n+1} f(g_1, \dots, g_n).
\end{aligned}$$

Define

$$\begin{aligned}
&Z^n(G, M) = \mathrm{Ker}(\partial^n) && \text{(group of } n\text{-cocycles)} \\
&B^n(G, M) = \mathrm{Im}(\partial^{n-1}) && \text{(group of } n\text{-coboundaries)} \\
&H_0^n(G, M) = Z^n(G, M)/B^n(G, M).
\end{aligned}$$

For example,

$$H_0^0(G, M) = M(k)^G$$

$$H_0^1(G, M) = \frac{\text{crossed homomorphisms } G \to M}{\text{principal crossed homomorphisms}}.$$

If G acts trivially on M, then

$$H_0^0(G, M) = M(k)$$

$$H_0^1(G, M) = \mathrm{Hom}(G, M) \quad \text{(homomorphisms of group functors)}.$$

The group $H_0^n(G, M)$ is called the **nth Hochschild cohomology group** of G in M.

Let

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of G-modules. By this we mean that

$$0 \to M'(R) \to M(R) \to M''(R) \to 0 \qquad (100)$$

is exact for all small k-algebras R. Then

$$0 \to C^\bullet(G, M') \to C^\bullet(G, M) \to C^\bullet(G, M'') \to 0 \qquad (101)$$

is an exact sequence of complexes. For example, if G is an algebraic group, then the degree n part of (101) is obtained from (100) by replacing R with $\mathcal{O}(G)^{\otimes n}$. By a standard argument, (101) gives rise to a long exact sequence of cohomology groups

$$0 \to H_0^0(G, M') \to \cdots \to H_0^n(G, M'') \to H_0^{n+1}(G, M') \to H_0^{n+1}(G, M) \to \cdots.$$

More generally, even when M and M'' are not assumed to be commutative, there is an exact sequence (DG, II, §3, 1.4)

$$0 \to M'^G(k) \to M^G(k) \to M''^G(k) \to H_0^1(G, M'). \qquad (102)$$

Let M be a commutative group functor, and let $\mathrm{Ind}^G(M)$ denote the functor $R \rightsquigarrow \mathrm{Map}(G_R, M_R)$ (maps of set-valued functors). Then $\mathrm{Ind}^G(M)$ becomes a G-module when we set

$$(gf)(h) = f(hg), \quad g, h \in G, \quad f \in \mathrm{Ind}^G(M).$$

PROPOSITION 15.4 (SHAPIRO'S LEMMA). *Let M be a functor to commutative groups. For all $n > 0$,*

$$H_0^n(G, \mathrm{Ind}^G(M)) = 0.$$

PROOF. Note that

$$C^n(G, \mathrm{Ind}^G(M)) \simeq \mathrm{Map}(G \times G^n, M) = C^{n+1}(G, M).$$

Define

$$s^n : \mathrm{Map}(G^{n+2}, M) \to \mathrm{Map}(G^{n+1}, M)$$

by

$$(s^n f)(g, g_1, \dots, g_n) = f(e, g, g_1, \dots, g_n).$$

When we regard s^n as a map $C^{n+1}(G, \mathrm{Ind}^G(M)) \to C^n(G, \mathrm{Ind}^G(M))$, we find (by direct calculation) that

$$s^n \partial^n + \partial^{n-1} s^{n-1} = \mathrm{id} \text{ for } n > 0.$$

Therefore $(s^n)_n$ is a homotopy operator, and the cohomology groups vanish. $\qquad \square$

REMARK 15.5. In the above discussion, we did not use that k is a field. Let R_0 be a k-algebra. From an algebraic group G over R_0 and a G-module M over R_0 we obtain, as above, cohomology groups $H_0^n(G, M)$.

Now let G be an algebraic group over k with coordinate ring A, and let $M = V_a$ be the G-module defined by a linear representation (V, r) of G over k. From the description $C^n(G, M) = M(A^{\otimes n}) = V \otimes A^{\otimes n}$, we see that

$$C^\bullet(G_{R_0}, M_{R_0}) \simeq R_0 \otimes C^\bullet(G, M).$$

As $k \to R_0$ is flat, it follows that

$$H_0^n(G_{R_0}, M_{R_0}) \simeq R_0 \otimes H_0^n(G, M).$$

Examples.

PROPOSITION 15.6. *Let Γ_k be the constant algebraic group defined by a finite abstract group Γ. For all Γ_k-modules M,*

$$H_0^n(\Gamma_k, M) \simeq H^n(\Gamma, M(k)) \qquad \text{(usual group cohomology)}.$$

PROOF. The standard complexes $C^\bullet(\Gamma_k, M)$ and $C^\bullet(\Gamma, M(k))$ are equal. $\qquad \square$

PROPOSITION 15.7. *Every action of $\mathbb{G}_a$ on $\mathbb{G}_m$ is trivial, and*

$$H_0^n(\mathbb{G}_a, \mathbb{G}_m) = \begin{cases} k^\times & \text{if } n = 0 \\ 0 & \text{if } n > 0. \end{cases}$$

PROOF. The first assertion follows from Corollary 12.37. We have

$$C^n(\mathbb{G}_a, \mathbb{G}_m) \stackrel{\text{def}}{=} \text{Map}(\mathbb{G}_a^n, \mathbb{G}_m) \simeq \mathbb{G}_m(k[T]^{\otimes n}) \simeq k[T_1, \dots, T_n]^\times = k^\times$$

and $\partial^n = \sum_0^{n+1} (-1)^j \, \text{id}$. Therefore,

$$\partial^n = \begin{cases} \text{id} & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even}, \end{cases}$$

from which the statement follows. $\qquad \square$

PROPOSITION 15.8. *Let r be an integer ≥ 0. Every action of $\mathbb{G}_m^r$ on $\mathbb{G}_m$ is trivial, and*

$$H_0^i(\mathbb{G}_m^r, \mathbb{G}_m) = 0 \text{ for } i \geq 2.$$

PROOF. The first assertion follows from Corollary 12.37. The Hochschild complex has

$$C^n(\mathbb{G}_m^r, \mathbb{G}_m) = k[T_{11}, T_{11}^{-1}, \dots, T_{1n}, T_{1,n}^{-1}, \dots, T_{rn}, T_{rn}^{-1}]^\times \simeq k^\times \times \mathbb{Z}^{nr}.$$

When the boundary maps are made explicit, one finds that $C^\bullet(\mathbb{G}_m^r, \mathbb{G}_m)$ is a direct sum of a complex $\cdots \to k^\times \to k^\times \to \cdots$ and r copies of a complex $\cdots \to \mathbb{Z}^n \to \mathbb{Z}^{n+1} \to \cdots$. A direct calculation now gives the required statement (DG, III, §6, 6.1). $\qquad \square$

PROPOSITION 15.9. *Let $\mu: G \times H \to H$ be an action of an algebraic group G of height $\leq n$ on a commutative algebraic group H, and let H_n denote the kernel of $F_H^n: H \to H^{(p^n)}$. Then the induced action of G on H/H_n is trivial, and the canonical map*

$$H_0^i(G, H_n) \to H_0^i(G, H)$$

is bijective for all $i \geq 2$.

PROOF. From the functoriality of the Frobenius map (2.27), we obtain a commutative diagram

$$
\begin{array}{ccc}
G \times H & \xrightarrow{\ \mu\ } & H \\
{\scriptstyle F_G^n \times F_H^n}\big\downarrow & & \big\downarrow{\scriptstyle F_H^n} \\
G^{(p^n)} \times H^{(p^n)} & \xrightarrow{\ \mu^{(p^n)}\ } & H^{(p^n)}
\end{array}
$$

As F_G^n is the trivial homomorphism, this shows that the induced action of G on $H^{(p^n)}$, hence on H/H_n, is trivial.

For the second assertion, we define a functor $X \rightsquigarrow X(n)$ of schemes as follows. The underlying set of the scheme $X(n)$ is $X(k)$ endowed with its discrete topology. For $x \in X(k)$, set $\mathcal{O}_{X(n),x} = \mathcal{O}_{X,x}/\mathfrak{m}_x^{p^n}$. Then $X(n)$ is a subfunctor of X; moreover, $(X \times Y)(n) \simeq X(n) \times Y(n)$ and $G(n) = G$. It follows that $H(n)$ is stable under G. As $\mathrm{Map}(G^i, H(n)) \simeq \mathrm{Map}(G^i, H)$ (maps of schemes) for all i, we deduce that $H_0^i(G, H(n)) \simeq H_0^i(G, H)$ for all $i \geq 0$. Now note that there is a canonical exact sequence of G-modules

$$0 \to H_n \to H(n) \to H(k)_k \to 0. \tag{103}$$

Here $H(k)_k$ is the constant algebraic group equipped with the trivial G-action. As $\mathrm{Map}(G^i, H(k)_k) = H(k)$ for all i, we see that $H_0^i(G, H(k)_k) = 0$ for $i \geq 1$, and so the required statement follows from the cohomology sequence of (103). $\square$

For example, $H_0^i(\alpha_p, \mu_p) \simeq H_0^i(\alpha_p, \mathbb{G}_m)$ for all $i \geq 2$.

c. Hochschild extensions

Let G be a group functor. Let M be a commutative group functor, and let

$$0 \to M \xrightarrow{\ i\ } E \xrightarrow{\ \pi\ } G \tag{104}$$

be an exact sequence of group functors, i.e.,

$$0 \to M(R) \xrightarrow{\ i(R)\ } E(R) \xrightarrow{\ \pi(R)\ } G(R)$$

is exact for all (small) k-algebras R. A sequence (104) is a ***Hochschild extension*** if there exists a map of set-valued functors $s: G \to E$ such that $\pi \circ s = \mathrm{id}_G$. For a Hochschild extension, the sequence

$$0 \to M(R) \xrightarrow{i(R)} E(R) \xrightarrow{\pi(R)} G(R) \to 0$$

is exact for all k-algebras R. Conversely, if $\pi(R)$ is surjective with $R = \mathcal{O}(G)$, then (104) is a Hochschild extension. Two Hochschild extensions (E, i, π) and (E', i', π') of G by M are ***equivalent*** if there exists a homomorphism $f: E \to E'$ making the following diagram commute

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\ i\ } & E & \xrightarrow{\ \pi\ } & G & \longrightarrow & 0 \\
  &   & \| &   & \downarrow{\scriptstyle f} & & \| & & \\
0 & \longrightarrow & M & \xrightarrow{\ i'\ } & E' & \xrightarrow{\ \pi'\ } & G & \longrightarrow & 0.
\end{array}
$$

Let (E, i, π) be a Hochschild extension of G by M. In the action of E on M by conjugation, M acts trivially, and so (E, i, π) defines a G-module structure on M. Equivalent extensions define the same G-module structure on M. For a G-module M, we define $E(G, M)$ to be the set of equivalence classes of Hochschild extensions of G by M inducing the given action of G on M.

A Hochschild extension (E, i, π) is ***trivial*** if there exists a homomorphism of *group* functors $s: G \to E$ such that $\pi \circ s = \mathrm{id}_G$. This means that E is isomorphic to the semidirect product $M \rtimes_\theta G$ for the action θ of G on M defined by the extension.

PROPOSITION 15.10. *Let M be a G-module. There is a canonical bijection*

$$E(G, M) \simeq H_0^2(G, M). \tag{105}$$

PROOF. Let (E, i, π) be a Hochschild extension of G by M, and let $s: G \to E$ be a section to π. Define $f: G^2 \to M$ by the formula

$$s(g)s(g') = i(f(g, g')) \cdot s(gg'), \quad g, g' \in G(R).$$

Then f is a 2-cocycle, whose cohomology class is independent of the choice of s. In this way, we get a map from the set of equivalence classes of Hochschild extensions to $H_0^2(G, M)$. On the other hand, a 2-cocycle defines an extension, as for abstract groups. One checks without difficulty that the two maps obtained are inverse (DG, II, §3, 2.3). □

A Hochschild extension (E, i, π) of G by M is ***central*** if $i(M)$ is contained in the centre of E, or, in other words, if the action of G on M is trivial.

Let G act trivially on M. A 2-cocycle f is ***symmetric*** if $f(g, g') = f(g', g)$ for all $g, g' \in G(R)$. Let $Z_s^2(G, M)$ denote the group of symmetric 2-cocycles, and define

$$H_s^2(G, M) = Z_s^2(G, M) / B^2(G, M).$$

COROLLARY 15.11. *Let G and M be commutative group functors and regard M as a G-module with trivial action. There is a canonical one-to-one correspondence between the equivalence classes of Hochschild extensions $M \to E \to G$ with E commutative and the elements of $H_s^2(G, M)$.*

PROOF. This follows without difficulty from Proposition 15.10. □

Higher Hochschild extensions

We wish to define a connected sequence of functors $E^0(G, -)$, $E^1(G, -)$,... such that $E^1(G, -) = E(G, -)$. We examine this question first for an abstract group G. Consider the group ring $\mathbb{Z}[G]$ of G and let $J = \text{Ker}(\mathbb{Z}[G] \xrightarrow{g \mapsto 1} \mathbb{Z})$ be its augmentation ideal; thus $\mathbb{Z}[G] \simeq \mathbb{Z} \oplus J$. The map

$$\delta: G \to J, \quad \delta(g) = g - 1$$

is a crossed homomorphism, and it is universal, i.e.,

$$\varphi \leftrightarrow \varphi \circ \delta: \text{Hom}_{G\text{-module}}(J, M) \simeq Z^1(G, M) \quad \text{for all } G\text{-modules } M.$$

From an exact sequence of G-modules,

$$\mathcal{E}: \quad 0 \to M \xrightarrow{i} E \xrightarrow{\pi} J \to 0,$$

we can construct a diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M & \longrightarrow & E(\mathcal{E}) & \longrightarrow & G & \longrightarrow & e \\
 & & \| & & \downarrow & & \downarrow{\scriptstyle g \mapsto (g-1, g)} & & \\
0 & \longrightarrow & M & \xrightarrow{m \mapsto (i(m), 1)} & M \rtimes G & \xrightarrow{\pi \times \text{id}} & J \rtimes G & \longrightarrow & 0
\end{array}
$$

by taking the top row to be the pull-back by $G \to J \rtimes G$ of the bottom row. Let $F(\mathcal{E})$ denote the top row. Then the map $\mathcal{E} \mapsto F(\mathcal{E})$ defines a bijection from $\text{Ext}^1_{G\text{-module}}(J, M)$ onto the set $E(G, M)$ of equivalence classes of extensions of G by M (DG, III, §6, no. 1). We define

$$E^n(G, M) = \text{Ext}^n_{G\text{-module}}(J, M). \tag{106}$$

Then $E^0(G, M) = Z^1(G, M)$ and $E^1(G, M) = E(G, M)$.

A similar discussion applies to group functors. Let G be a group functor. The G-modules form an abelian category and, for a G-module M, we define $E^n(G, M)$ by (106). Then $E^0(G, -)$, $E^1(G, -)$, ... is a connected sequence of functors of G-modules such that

$$\begin{cases} E^0(G, M) \simeq Z^1(G, M) & \text{set of crossed homomorphisms} \\ E^1(G, M) \simeq E(G, M) & \text{set of Hochschild extensions} \end{cases} \tag{107}$$

(see DG, III, §6, 1.4). Moreover, when G is an algebraic group, $E^n(G, M) \simeq H_0^{n+1}(G, M)$ for $n \geq 1$ (DG, III, §6, 2.1).

d.   The cohomology of linear representations

Let G be an algebraic group over k, and let (V,r) be a linear representation of G. Then r defines an action of G on the group functor $V_{\mathfrak{a}} : R \rightsquigarrow V \otimes R$, and we set

$$H^n(G,V) = H_0^n(G,V_{\mathfrak{a}}).$$

Let $A = \mathcal{O}(G)$, and let $\rho : V \to V \otimes A$ be the corresponding co-action. Then

$$C^n(G,V_{\mathfrak{a}}) \overset{\text{def}}{=} \mathrm{Map}(G^n, V) \simeq V(A^{\otimes n}) = V \otimes A^{\otimes n}.$$

Thus, $C^{\bullet}(G,V_{\mathfrak{a}})$ is a complex

$$0 \to V \to V \otimes A \to \cdots \to V \otimes A^{\otimes n} \xrightarrow{\partial^n} V \otimes A^{\otimes (n+1)} \to \cdots.$$

The map ∂^n has the following description (DG, II, §3, 3.1): let $v \in V$ and $a_1, \ldots, a_n \in A$; then

$$\partial^n(v \otimes a_1 \otimes \cdots \otimes a_n) = \rho(v) \otimes a_1 \otimes \cdots \otimes a_n$$

$$+ \sum_{j=1}^{n} (-1)^j v \otimes a_1 \otimes \cdots \otimes \rho(a_j) \otimes \cdots \otimes a_n$$

$$+ (-1)^{n+1} v \otimes a_1 \otimes \cdots \otimes a_n \otimes 1.$$

An exact sequence of representations

$$0 \to V' \to V \to V'' \to 0$$

gives an exact sequence of complexes

$$0 \to C^{\bullet}(G,V'_{\mathfrak{a}}) \to C^{\bullet}(G,V_{\mathfrak{a}}) \to C^{\bullet}(G,V''_{\mathfrak{a}}) \to 0,$$

and so there is a long exact sequence of cohomology groups

$$0 \to H^0(G,V') \to \cdots \to H^n(G,V'') \to H^{n+1}(G,V') \to H^{n+1}(G,V) \to \cdots.$$

PROPOSITION 15.12. *Let V be a k-vector space, and let $V \otimes A$ be the free comodule on V (see p. 88). Then*

$$H^n(G,V \otimes A) = 0 \text{ for } n > 0.$$

PROOF. For a (small) k-algebra R,

$$\begin{aligned}
(V \otimes A)_{\mathfrak{a}}(R) &= V \otimes A \otimes R && \text{(definition)} \\
&\simeq (V \otimes R) \otimes_R (A \otimes R) && \text{(linear algebra)} \\
&= (V_{\mathfrak{a}})_R(A_R) && \text{(change of notation)} \\
&\simeq \mathrm{Nat}(h^{A_R}, (V_{\mathfrak{a}})_R) && \text{(Yoneda lemma A.32)} \\
&= \mathrm{Ind}^G(V_{\mathfrak{a}})(R) && \text{(definition)}.
\end{aligned}$$

As these isomorphisms are natural in R, they form an isomorphism of functors

$$(V \otimes A)_{\mathfrak{a}} \simeq \mathrm{Ind}^G(V_{\mathfrak{a}}).$$

Therefore the statement follows from Shapiro's lemma (15.4).   □

REMARK 15.13. The functors $H^n(G,\cdot)$ are the derived functors of the functor $H^0(G,\cdot)$ on the category of all linear representations of G (not necessarily finite-dimensional). To prove this, it remains to show that the functors $H^n(G,\cdot)$ are effaceable, i.e., for each V, there exists an injective homomorphism $V \to W$ such that $H^n(G,W) = 0$ for $n > 0$, but the homomorphism $V \to V_0 \otimes A$ in Proposition 4.12 has this property because of Proposition 15.12.

As the category of representations of G is isomorphic to the category of A-comodules, and $H^0(G,V) = \mathrm{Hom}_A(k,V)$ (homomorphisms of A-comodules), we see that, for all n, $H^n(G,V) \simeq \mathrm{Ext}^n_A(k,V)$ (Exts in the category of A-comodules).

e. Linearly reductive groups

Let G be an algebraic group over k, and let (V,r) be a linear representation of G on a k-vector space V. Then (V,r) is a directed union of its finite-dimensional subrepresentations, $(V,r) = \bigcup_{\dim(W)<\infty}(W,r|W)$ (see 4.8). Correspondingly,

$$H^n(G,V) = \varinjlim H^n(G,W) \tag{108}$$

because direct limits are exact in the category of abelian groups.

LEMMA 15.14. *Let $x \in H^n(G,V)$, $n > 0$. Then x maps to zero in $H^n(G,W)$ for some finite-dimensional representation W containing V.*

PROOF. Recall (4.12) that the co-action $\rho\colon V \to V_0 \otimes A$ is an injective homomorphism of A-comodules. According to Proposition 15.12, the element x maps to zero in $H^n(G,V_0 \otimes A)$, and it follows from (108) that x maps to zero in $H^n(G,W)$ for some finite-dimensional G-submodule W of $V_0 \otimes A$ containing $\rho(V)$. □

PROPOSITION 15.15. *An algebraic group G is linearly reductive if and only if $H^1(G,V) = 0$ for all finite-dimensional representations (V,r) of G.*

PROOF. $\Rightarrow$: Let $x \in H^1(G,V)$. According to the lemma, x maps to zero in $H^i(G,W)$ for some finite-dimensional representation W of G containing V. Hence x lifts to an element of $(W/V)^G$ in the cohomology sequence

$$0 \to V^G \to W^G \to (W/V)^G \to H^1(G,V) \to H^1(G,W).$$

But, because G is linearly reductive, the sequence $0 \to V \to W \to W/V \to 0$ splits as a sequence of G-modules, and so $W^G \to (W/V)^G$ is surjective. Therefore $x = 0$.

$\Leftarrow$: When (V,r) and (W,s) are finite-dimensional representations of G, we let $\mathrm{Hom}(V,W)$ denote the space of k-linear maps $V \to W$ equipped with the G-action given by the rule

$$(gf)(v) = g(f(g^{-1}v)).$$

We have to show that every exact sequence

$$0 \to V' \to V \to V'' \to 0 \tag{109}$$

of finite-dimensional representations of G splits. From (109), we get an exact sequence of G-modules

$$0 \to \operatorname{Hom}(V'', V') \to \operatorname{Hom}(V'', V) \to \operatorname{Hom}(V'', V'') \to 0,$$

and hence an exact cohomology sequence

$$\cdots \to \operatorname{Hom}(V'', V)^G \to \operatorname{Hom}(V'', V'')^G \to H^1(G, \operatorname{Hom}(V'', V')).$$

By assumption, the last group is zero, and so $\operatorname{id}_{V''}$ lifts to an element of the space $\operatorname{Hom}(V'', V)^G$. This element splits the original sequence (109). □

PROPOSITION 15.16. *If G is linearly reductive, then $H^n(G, V) = 0$ for all $n > 0$ and all representations V of G.*

PROOF. Because of (108), it suffices to prove this for finite-dimensional representations. We use induction on n. We know the statement for $n = 1$, and so we may suppose that $n > 1$ and that $H^i(G, W) = 0$ for $1 \le i < n$ and all finite-dimensional representations W. Let $x \in H^n(G, V)$. Then x maps to zero in $H^n(G, W)$ for some finite-dimensional W containing V (15.14), and so x lifts to an element of $H^{n-1}(G, V/W)$ in the cohomology sequence

$$H^{n-1}(G, V/W) \to H^n(G, V) \to H^n(G, W).$$

But $H^{n-1}(G, V/W) = 0$ (induction), and so $x = 0$. □

REMARK 15.17. In particular, $H^n(G, V) = 0$ $(n > 0)$ for groups G of multiplicative type (12.30).

f. Applications to homomorphisms

We can now prove a stronger form of Corollary 14.18(b).

PROPOSITION 15.18. *Let G and U be algebraic groups over k with G of multiplicative type and U unipotent, and let R be a k-algebra. Every homomorphism $G_R \to U_R$ is trivial.*

PROOF. Let α be such a homomorphism, and let H be minimal among the algebraic subgroups of U such that $\alpha(G_R) \subset H_R$. If $H \neq e$, then there exists a nontrivial homomorphism $\beta: H \to \mathbb{G}_a$ (see 14.22), and the composite map $\beta_R \circ \alpha: G_R \to (\mathbb{G}_a)_R$ is nontrivial because otherwise $\alpha(G_R)$ would be contained in the kernel of β_R and H would not be minimal. But when we endow $\mathbb{G}_{aR}$ with the trivial action of G_R, so that crossed homomorphisms are homomorphisms, we find that

$$\operatorname{Hom}_R(G_R, \mathbb{G}_{aR}) = H_0^1(G_R, \mathbb{G}_{aR}) \overset{15.5}{\simeq} R \otimes H_0^1(G, \mathbb{G}_a) \overset{15.15}{=} 0,$$

giving a contradiction. Therefore $H = e$ and α is trivial. □

REMARK 15.19. We saw in Exercise 1-1 that there may exist nontrivial homomorphisms $U_R \to G_R$ even in characteristic zero. In characteristic $p \neq 0$,

$$\underline{\mathrm{Hom}}((\mathbb{Z}/p\mathbb{Z})_k, \mathbb{G}_m) \simeq \mu_p \quad \underline{\mathrm{Hom}}(\alpha_p, \mathbb{G}_m) \simeq \alpha_p$$

(11.13), and so

$$\mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})_R, \mathbb{G}_{mR}) \neq 0 \neq \mathrm{Hom}(\alpha_{pR}, \mathbb{G}_{mR})$$

if R contains a nonzero element whose pth power is 0.

g. Applications to centralizers

The traditional approach to the smoothness of centralizers uses cohomology and Lie algebras. An action of an algebraic group H on an algebraic group G defines a representation of H on the Lie algebra $\mathfrak{g}$ of G, and hence cohomology groups $H^n(G, \mathfrak{g})$.

THEOREM 15.20 (SMOOTHNESS OF CENTRALIZERS). *Let H be an algebraic group acting on a smooth algebraic group G by group homomorphisms. If $H^1(H, \mathfrak{g}) = 0$, then G^H is smooth.*

PROOF. See DG, II, §5, 2.8. □

Linearly reductive groups H (not necessarily smooth) satisfy the hypothesis (15.15),

h. Calculation of some extensions

We compute (following DG, III, §6) some extension groups. Throughout, p denotes the characteristic exponent of k.

Preliminaries

Let G be an algebraic group over k. Recall that a G-module is a commutative group functor M on which G acts by group homomorphisms. A *G-module sheaf* is a G-module whose underlying functor is a sheaf for the flat topology.

Let M be a sheaf of commutative groups. A *sheaf extension* of G by M is a sequence

$$e \to M \xrightarrow{i} E \xrightarrow{\pi} G \to e \tag{110}$$

that is exact as a sequence of sheaves of groups. This means that the sequence

$$e \to M(R) \to E(R) \to G(R)$$

is exact for all small k-algebras and π is a quotient map of sheaves (see 5.73). Equivalence of sheaf extensions is defined as for Hochschild extensions. An extension of G by M defines an action of G on M, and equivalent extensions define the same action.

DEFINITION 15.21. For a G-module sheaf M, $\mathrm{Ext}(G,M)$ denotes the set of equivalence classes of sheaf extensions of G by M inducing the given action of G on M.

When M is an algebraic group, $\mathrm{Ext}(G,M)$ is equal to the set of equivalence classes of extensions (110) with E an algebraic group (Exercise 5-10).

Let M be a G-module sheaf, and let $(E,i.\pi)$ be a Hochschild extension of G by M. Then E is a sheaf, and (E,i,π) is a sheaf extension of G by M. In this way, we get an injective map

$$E(G,M) \to \mathrm{Ext}(G,M)$$

whose image consists of the classes of extensions (110) such that π has a section as a map of functors. One strategy for computing $\mathrm{Ext}(G,M)$ is to show that every extension is a Hochschild extension, and then use the description of $E(G,M)$ in terms of Hochschild cohomology (see 15.10). Let

$$e \to N \to E \to G \to e \qquad (111)$$

be an extension of algebraic groups. Then E is an N-torsor over G (see 2.68), and (111) is a Hochschild extension if this torsor is trivial.

More generally, we define $\mathrm{Ext}^i(G,-)$ to be the ith right derived functor of

$$M \rightsquigarrow \mathrm{Hom}(G,M) \quad \text{(functor of } G\text{-module } sheaves).$$

Then (DG, III, §6, no. 2)

$$\begin{cases} \mathrm{Ext}^0(G,M) = Z^1(G,M) & \text{group of crossed homomorphisms} \\ \mathrm{Ext}^1(G,M) \simeq \mathrm{Ext}(G,M) & \text{group of sheaf extensions.} \end{cases}$$

NOTES. Demazure and Gabriel (1970, III, §6, no. 2) write Ex^i and $\mathrm{E\tilde{x}}^i$ where we write E^i and Ext^i.

Extensions with étale quotient

PROPOSITION 15.22. *Suppose that k is algebraically closed. Let Γ_k be the constant algebraic group over k defined by a finite group Γ, and let M be a Γ_k-module sheaf. For all $i \geq 1$,*

$$\mathrm{Ext}^i(\Gamma_k,M) \simeq H^{i+1}(\Gamma,M(k)) \quad \text{(usual group cohomology).}$$

PROOF. Because k is algebraically closed, the functor $M \rightsquigarrow M(k)$ is exact (5.48). Hence the functor $M \rightsquigarrow C^\bullet(\Gamma,M(k))$ is exact, and so an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of sheaves of commutative groups gives rise to an exact sequence

$$0 \to Z^1(\Gamma,M'(k)) \to Z^1(\Gamma,M(k)) \to Z^1(\Gamma,M''(k)) \to H^2(\Gamma,M'(k)) \to \cdots$$

of commutative groups. As

$$\text{Ext}^0(\Gamma_k, M) = Z^1(\Gamma_k, M) \simeq Z^1(\Gamma, M(k)),$$

it remains to show that $H^{i+1}(\Gamma, M(k)) = 0$ for $i > 0$ when M is injective. But the functor $M \rightsquigarrow M(k)$ is right adjoint to the functor $N \rightsquigarrow N_k$, i.e.,

$$\text{Hom}(N, M(k)) \simeq \text{Hom}(N_k, M).$$

If M is injective, then the functor $N \rightsquigarrow \text{Hom}(N_k, M) \simeq \text{Hom}(N, M(k))$ is exact, and so $M(k)$ is injective. □

COROLLARY 15.23. *Let k, Γ, and M be as in the proposition. If Γ is of finite order n and $x \mapsto nx \colon M(k) \to M(k)$ is an isomorphism, then*

$$\text{Ext}^i(\Gamma_k, M) = 0 \text{ for all } i \geq 0.$$

PROOF. Let N be a Γ-module. If Γ has order n, then the cohomology group $H^i(\Gamma, N)$ is killed by n for all $i > 0$ (Serre 1962, VIII, §2). If $x \mapsto nx \colon N \to N$ is bijective, then n acts bijectively on $H^i(\Gamma, N)$. If both are true, then $H^i(\Gamma, N) = 0$ for $i > 0$, and so the statement follows from (15.22). □

COROLLARY 15.24. *Let D be a diagonalizable algebraic group over k. If k is algebraically closed, then $\text{Ext}^i(\mathbb{Z}/p\mathbb{Z}, D) = 0$ for all $i > 0$.*

PROOF. It suffices to show that $p \colon D(k) \to D(k)$ is an isomorphism. This is obviously true if $D = \mathbb{G}_m$, $D = \mu_{p^r}$, or $D = \mu_n$ with $\gcd(p, n) = 1$, and every diagonalizable group is a product of such groups (12.3). □

Extensions with additive quotient

PROPOSITION 15.25. *Let D be a diagonalizable group. Every action of $\mathbb{G}_a$ on D is trivial, and*
$$\text{Ext}^0(\mathbb{G}_a, D) = 0 = \text{Ext}^1(\mathbb{G}_a, D).$$

PROOF. The first assertion follows from Corollary 12.37. For the second assertion, we first consider the case $D = D(\mathbb{Z}) = \mathbb{G}_m$. Because the action is trivial, $\text{Ext}^0(\mathbb{G}_a, \mathbb{G}_m) = \text{Hom}(\mathbb{G}_a, \mathbb{G}_m)$, which is 0 (see 14.18). Consider a sheaf extension

$$0 \to \mathbb{G}_m \to E \to \mathbb{G}_a \to 0. \tag{112}$$

Then E is a $\mathbb{G}_m$-torsor over $\mathbb{A}^1$ (see 2.68), and hence corresponds to an element of $\text{Pic}(\mathbb{A}^1)$, which is zero (A.79). Therefore (112) is a Hochschild extension, and

$$E(\mathbb{G}_a, \mathbb{G}_m) \overset{15.10}{\simeq} H_0^2(\mathbb{G}_a, \mathbb{G}_m) \overset{15.7}{=} 0.$$

In the general case, $D = D(M)$, and there exists an exact sequence

$$0 \to \mathbb{Z}^s \to \mathbb{Z}^r \to M \to 0$$

for some $r, s \in \mathbb{N}$, which gives an exact sequence of algebraic groups

$$0 \to D(M) \to \mathbb{G}_m^r \to \mathbb{G}_m^s \to 0$$

(12.9b). This is exact as a sequence of sheaves of commutative groups, and so there is a long exact sequence

$$0 \to \mathrm{Ext}^0(\mathbb{G}_a, D(M)) \to \mathrm{Ext}^0(\mathbb{G}_a, \mathbb{G}_m)^r \to \mathrm{Ext}^0(\mathbb{G}_a, \mathbb{G}_m)^s \to \cdots.$$

Thus the statement follows from the case $D = \mathbb{G}_m$. □

Define $f_1: \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$ by

$$f_1(x, y) = \frac{x^p + y^p - (x+y)^p}{p}$$

$$= -x^{p-1}y - \tfrac{p-1}{2}x^{p-2}y^2 - \cdots - xy^{p-1}.$$

It is a symmetric 2-cocycle for the trivial action of $\mathbb{G}_a$ on $\mathbb{G}_a$.

LEMMA 15.26. *Every element of $H_s^2(\mathbb{G}_a, \mathbb{G}_a)$ has a unique representative of the form $f = \sum_{i \geq 0} a_i f_1^{p^i}$ ($a_i \in k$). Therefore $H_s^2(\mathbb{G}_a, \mathbb{G}_a)$ is a free $k_\sigma[F]$-module with basis f_1.*

PROOF. When we substitute $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ into

$$f(y, z) - f(x+y, z) + f(x, y+z) - f(x, y) = 0$$

we obtain the identities that the a_{ij} must satisfy in order for f to be a 2-cocycle. From these identities, it is possible to deduce the statement of the lemma (Lazard 1955, Lemme 3; DG, II, §2, 4.6). □

PROPOSITION 15.27. *Let H be an algebraic subgroup of $\mathbb{G}_a$. Every extension $\mathbb{G}_a \to E \to H$ with E commutative comes by pull-back from the extension*

$$0 \to \mathbb{G}_a \to W_2 \to \mathbb{G}_a \to 0. \tag{113}$$

PROOF. Let

$$0 \to \mathbb{G}_a \to E \to H \to 0$$

be an extension of H by $\mathbb{G}_a$ with E commutative. The extension is Hochschild because E is a $\mathbb{G}_a$-torsor over H (see 2.68) and hence is trivial (2.72). Thus the extension corresponds to an element of $H_s^2(H, \mathbb{G}_a)$ (see 15.11). The extension (113) corresponds to the 2-cocycle $f_1 \in Z_s^2(\mathbb{G}_a, \mathbb{G}_a)$. Thus, the proposition for $H = \mathbb{G}_a$ follows from the lemma using the isomorphism $\mathrm{End}(\mathbb{G}_a) \simeq k_\sigma[F]$ in 14.40. For an $H \neq \mathbb{G}_a$, it remains to show that the canonical map $H_s^2(\mathbb{G}_a, \mathbb{G}_a) \to H_s^2(H, \mathbb{G}_a)$ is surjective. Let $\mathcal{O}(\mathbb{G}_a) = k[T]$ and let $\mathcal{O}(H) = k[T]/I$ with I generated by a polynomial of degree n. Let U be the subspace of $k[T]$ spanned by $1, \ldots, T^{n-1}$. Every $f \in Z_s^2(H, \mathbb{G}_a) \subset (k[T]/I)^{\otimes 2}$ lifts to an $f' \in U^{\otimes 2} \subset k[T]^{\otimes 2}$. This f' is a symmetric 2-cocycle whose class in $H_s^2(\mathbb{G}_a, \mathbb{G}_a)$ maps to the class of f in $H_s^2(H, \mathbb{G}_a)$ (DG, II, §3, 4.7). □

Extensions with multiplicative quotient

PROPOSITION 15.28. *Let $D = D(M)$ be a diagonalizable algebraic group. Every action of $\mathbb{G}_m^r$ on $D(M)$ is trivial, and the functor D induces isomorphisms*

$$\operatorname{Ext}^i(M, \mathbb{Z}^r) \simeq \operatorname{Ext}^i(\mathbb{G}_m^r, D(M))$$

for $i = 0, 1$.

PROOF. The first assertion follows from Corollary 12.37. The contravariant equivalence in Theorem 12.9 gives isomorphisms

$$\operatorname{Hom}_{\mathbb{Z}\text{-modules}}(M, \mathbb{Z}^r) \simeq \operatorname{Hom}(\mathbb{G}_m^r, D(M))$$
$$\operatorname{Ext}^1_{\mathbb{Z}\text{-modules}}(M, \mathbb{Z}^r) \simeq \operatorname{Ex}^1(\mathbb{G}_m^r, D(M))$$

where $\operatorname{Ex}^1(\mathbb{G}_m^r, D(M))$ denotes extensions in the category of *commutative* algebraic groups (equivalently *commutative* group functors). Because the action of $\mathbb{G}_m^r$ on $D(M)$ is trivial,

$$\operatorname{Ext}^0(\mathbb{G}_m^r, D(M)) = \operatorname{Hom}(\mathbb{G}_m^r, D(M)).$$

The map

$$\operatorname{Ex}^1(\mathbb{G}_m^r, D(M)) \to \operatorname{Ext}^1(\mathbb{G}_m^r, D(M))$$

is injective, and it remains to show that it is surjective. By a five-lemma argument, it suffices to do this with $M = \mathbb{Z}$ (so $D(M) = \mathbb{G}_m$).

Consider an extension

$$0 \to \mathbb{G}_m \to E \to \mathbb{G}_m^r \to 0.$$

Then E is a $\mathbb{G}_m$-torsor over $\mathbb{G}_m^r$, and so corresponds to an element of $\operatorname{Pic}(\mathbb{G}_m^r)$, which is zero. Therefore, the extension is a Hochschild extension, and so

$$\operatorname{Ext}^1(\mathbb{G}_m^r, \mathbb{G}_m) = E(\mathbb{G}_m^r, \mathbb{G}_m) \overset{15.10}{=} H_0^2(\mathbb{G}_m^r, \mathbb{G}_m) \overset{15.8}{=} 0. \qquad \square$$

Recall (10.12) that an action of an algebraic group G on $\mathbb{G}_a$ is said to be linear if it arises from a linear representation of G on a one-dimensional vector space.

PROPOSITION 15.29. *Let G be of multiplicative type, and let N be an algebraic subgroup of $\mathbb{G}_a$ such that G acts on N through a linear action on $\mathbb{G}_a$. Then*

$$H_0^1(G, N) = 0 = H_0^2(G, N).$$

PROOF. Let V be such that $V_{\mathfrak{a}} = \mathbb{G}_a$. Then $H^i(G, V) = H_0^i(G, \mathbb{G}_a)$ by definition, and $H^i(G, V) = 0$ for $i > 0$ by 15.16. Consider the exact sequence

$$0 \to N \to \mathbb{G}_a \to \mathbb{G}_a/N \to 0. \tag{114}$$

Either $\mathbb{G}_a/N = 0$ or it is isomorphic to $\mathbb{G}_a$ (Exercise 14-3). In the first case, $N \simeq \mathbb{G}_a$ and so $H_0^i(G,N) = 0$ for $i > 0$. In the second case, (114) becomes an exact sequence

$$0 \to N \to \mathbb{G}_a \to \mathbb{G}_a \to 0,$$

whose exact cohomology sequence gives the result.   □

COROLLARY 15.30. *Let G be of multiplicative type. Then $H_0^i(G,\alpha_p) = 0$ for $i > 0$.*

PROOF. The automorphism group of α_p is $\mathbb{G}_m$, and so every action of G on α_p extends to a linear action on $\mathbb{G}_a$. Thus, we can regard

$$0 \to \alpha_p \to \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \to 0$$

as an exact sequence of G-modules. Its cohomology sequence gives the result.□

PROPOSITION 15.31. *Let G be an algebraic group of multiplicative type, and let (V,r) be a finite-dimensional representation of G. Then $E^0(G,V_a) \simeq V/V^G$ and $\mathrm{Ext}^i(G,V_a) = 0$ all $i > 0$.*

PROOF. By definition, $H^i(G,V) = H_0^i(G,V_a)$, and $H^i(G,V) = 0$ for $i > 0$ (see 15.17).   □

PROPOSITION 15.32. *Let G be an algebraic group of multiplicative type, acting trivially on a commutative unipotent group U. Then $\mathrm{Ext}^i(G,U) = 0$ for all $i \geq 0$.*

PROOF. For $U = \mathbb{G}_a$, this follows from (15.31). Every algebraic subgroup of $\mathbb{G}_a$ is the kernel of an epimorphism $\mathbb{G}_a \to \mathbb{G}_a$ (Exercise 14-3), and so the statement is true for such groups. Now use that U has a filtration whose quotients are of these types (14.21).   □

COROLLARY 15.33. *Let G be of multiplicative type, and let $\varphi\colon G \to \underline{\mathrm{Aut}}(\alpha_p) \simeq \mathbb{G}_m$ be a nontrivial homomorphism. Then $\mathrm{Ext}^i(G,\alpha_p) = 0$ for $i \geq 2$. If φ factors through $\mu_p \subset \mathbb{G}_m$, then*

$$\begin{cases} \mathrm{Ext}^0(G,\alpha_p) \simeq k \\ \mathrm{Ext}^1(G,\alpha_p) = 0; \end{cases} \quad \textit{otherwise} \quad \begin{cases} \mathrm{Ext}^0(G,\alpha_p) = 0 \\ \mathrm{Ext}^1(G,\alpha_p) \simeq k/k^p. \end{cases}$$

PROOF. As $\underline{\mathrm{Aut}}(\alpha_p) \simeq \mathbb{G}_m$, every action of D on α_p extends to a linear action of D on $\mathbb{G}_a$. We have an exact sequence

$$0 \to \alpha_p \to \mathbb{G}_a' \xrightarrow{F} \mathbb{G}_a'' \to 0$$

in which $\mathbb{G}_a' = \mathbb{G}_a = \mathbb{G}_a''$ as algebraic groups but may have different G-module structures. In the corresponding long exact sequence,

$$\mathrm{Ext}^i(G,\mathbb{G}_a') = 0 = \mathrm{Ext}^i(G,\mathbb{G}_a''), \quad i \geq 1.$$

Now the exact sequence

$$\mathrm{Hom}(D,\mathbb{G}_a) \to \mathrm{Ext}^1(D,\alpha_p) \to \mathrm{Ext}^1(D,\mathbb{G}_a)$$

and (15.31) show that $\mathrm{Ext}^1(D,\alpha_p) = 0$. □

THEOREM 15.34. *Let U be an algebraic subgroup of $\mathbb{G}_a$, and let G be an algebraic group of multiplicative type acting on U by group homomorphisms. Then $\mathrm{Ext}^1(G,U) = 0$ in each of the following cases:*

(a) $U = \mathbb{G}_a$ *and the action of G on U is linear (for example, trivial);*

(b) k *is perfect and $U = \alpha_{p^r}$;*

(c) U *is étale and G is connected;*

(d) k *is algebraically closed and the action of G on U is the restriction of a linear action on $\mathbb{G}_a$;*

(e) G *acts trivially on U.*

PROOF. (a) This was proved in Proposition 15.31.

(b) This follows from Proposition 15.32 using the exact sequences

$$0 \to \alpha_p \to \alpha_{p^r} \to \alpha_{p^{r-1}} \to 0.$$

(c) The action of G on U is trivial, and so we have an exact sequence of G-modules with trivial action,

$$0 \to U \to \mathbb{G}_a \to \mathbb{G}_a \to 0$$

(see Exercise 14-3). In the exact sequence

$$\mathrm{Ext}^0(G,\mathbb{G}_a) \to \mathrm{Ext}^1(G,U) \to \mathrm{Ext}^1(G,\mathbb{G}_a),$$

the two end terms are zero (15.29).

(d, e) If $U = \mathbb{G}_a$, then this is proved in (a). Otherwise, there is an exact sequence

$$0 \to U \to \mathbb{G}_a \xrightarrow{\alpha} \mathbb{G}_a \to 0,$$

(see Exercise 14-3), and hence an exact sequence

$$\mathrm{Ext}^0(G,\mathbb{G}_a) \to \mathrm{Ext}^0(G,\mathbb{G}_a) \to \mathrm{Ext}^1(G,U) \to \mathrm{Ext}^1(G,\mathbb{G}_a).$$

But $\mathrm{Ext}^1(G,\mathbb{G}_a) = 0$, and $\mathrm{Hom}(G,\mathbb{G}_a)$ equals 0 if the action is trivial (12.18) and k otherwise. Therefore $\mathrm{Ext}^1(G,U) = 0$ or $\mathrm{Ext}^1(G,U) = k/k^p$, from which the statements (d) and (e) follow. □

Extensions of unipotent groups by diagonalizable groups

PROPOSITION 15.35. *We have*

$$H_0^2(\alpha_p, \mu_p) \simeq H_0^2(\alpha_p, \mathbb{G}_m) \simeq \mathrm{Ext}^1(\alpha_p, \mathbb{G}_m).$$

PROOF. The first isomorphism is a special case of Proposition 15.9. For the second isomorphism, it suffices (after 15.10) to show that every extension

$$0 \to \mathbb{G}_m \xrightarrow{i} E \xrightarrow{\pi} \alpha_p \to 0$$

is a Hochschild extension, i.e., there exists a map $s\colon \alpha_p \to E$ of schemes such that $\pi \circ s = \mathrm{id}$. But E is a $\mathbb{G}_m$-torsor over α_p, and hence corresponds to an element of $\mathrm{Pic}(\alpha_p)$, which is zero because α_p is the spectrum of a local ring.   □

PROPOSITION 15.36. *Every action of α_p on a diagonalizable group D is trivial, and*

$$\mathrm{Ext}^1(\alpha_p, \mu_p) \simeq \mathrm{Ext}^1(\alpha_p, \mathbb{G}_m) \simeq k/k^p.$$

If k is perfect, then $\mathrm{Ext}^1(\alpha_p, D) = 0$.

PROOF. The first assertion follows from Corollary 12.37. We now prove the second assertion. As $\mathrm{Hom}(\alpha_p, \mathbb{G}_m) = 0$, from the Ext-sequence of

$$0 \to \mu_p \to \mathbb{G}_m \xrightarrow{x \mapsto x^p} \mathbb{G}_m \to 0,$$

we find that

$$\mathrm{Ext}^1(\alpha_p, \mu_p) \to \mathrm{Ext}^1(\alpha_p, \mathbb{G}_m)$$

is injective. From Proposition 15.35, we find that

$$\mathrm{Ext}^1(\alpha_p, \mu_p) \simeq \mathrm{Ext}^1(\alpha_p, \mathbb{G}_m) \simeq H_0^2(\alpha_p, \mu_p) \simeq \mathrm{Ext}^1(\mathrm{Lie}(\alpha_p), \mathrm{Lie}(\mu_p)).$$

The p-Lie algebra of α_p is kf with $f^{[p]} = 0$, and the p-Lie algebra of $\mu_p = ke$ with $e^{[p]} = e$. Every extension of $\mathrm{Lie}(\alpha_p)$ by $\mathrm{Lie}(\mu_p)$ splits as an extension of vector spaces, and so it is equivalent to an extension

$$\mathcal{L}_\lambda\colon \quad 0 \to ke \xrightarrow{j} ke \oplus kf_\lambda \xrightarrow{q} kf \to 0$$

where $j(e) = e$, $q(e) = 0$, $q(f_\lambda) = f$ and $ke \oplus kf_\lambda$ is a p-Lie algebra with $e^{[p]} = e$ and $f_\lambda^{[p]} = \lambda f_\lambda$. A homomorphism of extensions of p-Lie algebras

$$
\begin{array}{ccccccccc}
\mathcal{L}_\lambda\colon & 0 & \longrightarrow & ke & \xrightarrow{\ j\ } & ke \oplus kf_\lambda & \longrightarrow & kf & \xrightarrow{\ q\ } 0 \\
& & & \Big\| & & \Big\downarrow{\scriptstyle u} & & \Big\| & \\
\mathcal{L}_\mu\colon & 0 & \longrightarrow & ke & \xrightarrow{\ j\ } & ke \oplus kf_\mu & \longrightarrow & kf & \xrightarrow{\ q\ } 0
\end{array}
$$

maps e to e and f_λ onto $\alpha e + f_\mu$ with $\alpha \in k$. The equality

$$\lambda e = u(f_\lambda^{[p]}) = (\alpha e + f_\mu)^{[p]} = \alpha^p e + \mu e$$

shows that the extensions $\mathcal{L}_\lambda$ and $\mathcal{L}_\mu$ are equivalent if and only if $\lambda - \mu \in k^p$.

Finally, let Γ^0 be the quotient of Γ by the prime-to-p torsion in Γ. Then $D(\Gamma)^\circ = D(\Gamma^0)$. As Γ^0 has a normal series whose quotients are isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$, the final assertion follows from the second. $\square$

NOTES. See DG, III, §6, 7.2; 8.6; 8.7 for more details.

THEOREM 15.37. *Let D and U be algebraic groups over an algebraically closed field k with D diagonalizable and U unipotent. Then $\mathrm{Ext}^1(U, D) = 0$.*

PROOF. Consider an exact sequence

$$e \to D \xrightarrow{i} G \xrightarrow{\pi} U \to e$$

where D is diagonalizable and U is unipotent. We shall show that i admits a retraction r. This assertion is trivial if $U = e$. Otherwise, U contains a normal algebraic subgroup U_1 such that U/U_1 is isomorphic to $\mathbb{G}_a$ ($p = 1$) or $\mathbb{G}_a, \alpha_p$, or $(\mathbb{Z}/p\mathbb{Z})_k$ ($p \neq 1$) (see 14.22, 14.52). Consider the commutative diagram

Arguing by induction on the length of a subnormal series for U, we may suppose that i_1 admits a retraction $r_1 : \pi^{-1}(U_1) \to D$. We form the pushout of the middle column of the diagram by r_1:

On combining Corollary 15.24 with the Propositions 15.25 and 15.36, we find that $\mathrm{Ext}^1(H, D) = 0$, and so i_2 admits a retraction r_2. Now $r = r_2 \circ u : G \to D$ is a retraction of i, which completes the proof. $\square$

Extensions of multiplicative groups by multiplicative groups

PROPOSITION 15.38. *Every action of μ_p on $\mathbb{G}_m$ or μ_p is trivial, and*

$$\mathrm{Ext}^1(\mu_p, \mathbb{G}_m) \simeq k/\wp(k), \quad \text{where } \wp(x) = x^p - x$$
$$\mathrm{Ext}^1(\mu_p, \mu_p) \simeq \mathbb{Z}/p\mathbb{Z} \oplus k/\wp(k).$$

PROOF. The proof is similar to that of Proposition 15.36.   □

THEOREM 15.39. *Every extension of a connected algebraic group of multiplicative type by an algebraic group of multiplicative type is of multiplicative type.*

PROOF. We may suppose that k is algebraically closed. Let $A(G'', G')$ denote the following statement: for every exact sequence

$$e \to G' \to G \to G'' \to e, \tag{115}$$

the algebraic group G is diagonalizable. We prove that $A(G'', G')$ holds for all connected groups G'' and G' of multiplicative type by using induction on the dimension of G''. We may suppose $G'' \neq e$.

Consider an extension (115) with G' and G'' connected of multiplicative type. To show that G is diagonalizable, it suffices to show that every finite-dimensional representation (V, r) of G is diagonalizable (12.12). As G' is diagonalizable,

$$(V, r|G') = \bigoplus_{\chi \in X^*(G')} V_\chi.$$

Moreover, G' is contained in the centre of G (see 12.38), and so each V_χ is stable under G. Therefore, we may replace V with V_χ and assume that G' acts through χ. We now have a diagram

$$
\begin{array}{ccccccccc}
e & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & e \\
& & \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle \bar{r}} & & \\
e & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_V & \xrightarrow{\ q\ } & \mathrm{GL}_V/\mathbb{G}_m & \longrightarrow & e,
\end{array}
$$

and it suffices to show that the representation of $q^{-1}(\bar{r}(G''))$ on V is diagonalizable. This will be true if $q^{-1}(\bar{r}(G''))$ is diagonalizable. But $q^{-1}(\bar{r}(G''))$ is an extension of $\bar{r}(G'')$ by $\mathbb{G}_m$. Therefore, in order to prove $A(G'', G')$, it suffices to prove $A(H, \mathbb{G}_m)$ where H runs over the quotients of G''.

For the case $G'' = \mathbb{G}_m$ or μ_p, where p is the characteristic exponent of k, it suffices to prove $A(\mathbb{G}_m, \mathbb{G}_m)$ and $A(\mu_p, \mathbb{G}_m)$. In Proposition 15.28 (resp. Proposition 15.38) we prove that every extension of $\mathbb{G}_m$ by $\mathbb{G}_m$ (resp. μ_p by $\mathbb{G}_m$) is commutative, and hence of multiplicative type (12.12).

If G'' is neither $\mathbb{G}_m$ or μ_p, then it contains one or the other as a proper normal algebraic subgroup N (this is obvious from 12.9). Let G_1 denote the inverse image of N in G, and consider the diagram

$$
\begin{array}{ccccccccc}
& & & & e & & e & & \\
& & & & \downarrow & & \downarrow & & \\
e & \longrightarrow & G' & \longrightarrow & G_1 & \longrightarrow & N & \longrightarrow & e \\
& & \| & & \downarrow & & \downarrow & & \\
e & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & e \\
& & & & \downarrow & & \downarrow & & \\
& & & & G/G_1 & \overset{\simeq}{\longrightarrow} & G''/N & & \\
& & & & \downarrow & & \downarrow & & \\
& & & & e & & e. & &
\end{array}
$$

The group G_1 is diagonalizable by the last case, and so G, being an extension of G''/N by G_1, is diagonalizable by the induction hypothesis. $\qquad\square$

COROLLARY 15.40. *Let G and G' be algebraic groups of multiplicative type with G connected. The map*

$$
\mathrm{Ext}^1(G, G') \to \mathrm{Ext}^1_{\mathbb{Z}\Gamma\text{-}modules}(X^*(G'), X^*(G)), \quad \Gamma = \mathrm{Gal}(k^s/k),
$$

defined by the functor X^* is a bijection.

Exercises

EXERCISE 15-1. Proposition 15.36 shows that there are no noncommutative extensions of α_p by $\mathbb{G}_m$ over k (because this is true over k^a). Can you prove this without using p-Lie algebras? See https://mathoverflow.net/, question 183139.

The Structure of Solvable Algebraic Groups

In this chapter, we study solvable algebraic groups. Of special interest are the groups G satisfying the following condition:

(*) there exists a normal unipotent algebraic subgroup G_u such that G/G_u is of multiplicative type.

When it exists, G_u contains *every* unipotent algebraic subgroup, and so it is unique (see 16.6). Algebraic groups satisfying (*) are solvable, and conversely smooth connected solvable groups over a perfect field satisfy (*) (see 16.33). An algebraic group G satisfies (*) if and only if it becomes diagonalizable over a separable field extension (see 16.6).

As usual, R is a (variable) k-algebra. Recall that all algebraic groups are affine over a base field k.

a.   Trigonalizable algebraic groups

DEFINITION 16.1. An algebraic group G is ***trigonalizable*** if every simple representation has dimension one.

In other words, G is trigonalizable if every nonzero representation of G contains an eigenvector. In terms of the associated comodule (V, ρ), the condition means that there exists a nonzero vector $v \in V$ such that $\rho(v) = v \otimes a$ for some $a \in \mathcal{O}(G)$. Both unipotent and diagonalizable algebraic groups are trigonalizable (6.45, 12.12).

A finite-dimensional representation (V, r) of an algebraic group G is said to be ***trigonalizable*** if there exists a basis of V for which $r(G) \subset \mathbb{T}_n$. Equivalently, (V, r) is trigonalizable if G stabilizes a maximal flag in V.

PROPOSITION 16.2. *The following conditions on an algebraic group G are equivalent:*

(a) G is trigonalizable;

(b) every finite-dimensional representation (V,r) of G is trigonalizable;

(c) G is isomorphic to an algebraic subgroup of $\mathbb{T}_n$ for some n;

(d) there exists a normal unipotent algebraic subgroup U of G such that G/U is diagonalizable.

PROOF. (a)$\Rightarrow$(b). We use induction on the dimension of V, assumed nonzero. By hypothesis, V contains a one-dimensional subspace V_1 stable under G. From the induction hypothesis, V/V_1 contains a maximal flag $V/V_1 \supset V_{n-1}/V_1 \supset \cdots \supset V_1/V_1 = 0$ stable under G. Now $V \supset V_{n-1} \supset \cdots \supset V_1 \supset 0$ is a maximal flag in V stable under G.

(b)$\Rightarrow$(c). Apply (b) to a faithful finite-dimensional representation of G (which exists by 4.9), and use that every monomorphism is a closed immersion (3.35).

(c)$\Rightarrow$(d). Embed G into $\mathbb{T}_n$, and let $U = \mathbb{U}_n \cap G$. Then U is normal because $\mathbb{U}_n$ is normal in $\mathbb{T}_n$, and it is unipotent because it is isomorphic to a subgroup of $\mathbb{U}_n$ (see 14.5). Finally, G/U embeds into the split torus $\mathbb{T}_n/\mathbb{U}_n$, and so it is diagonalizable (12.9c).

(d)$\Rightarrow$(a). Let U be as in (d), and let (V,r) be a representation of G on a nonzero vector space. Then V^U is nonzero because U is unipotent, and it is stable under G because U is normal (5.15). Now G acts on V^U through G/U, and so V^U is a sum of one-dimensional subrepresentations (12.12). In particular, it contains a one-dimensional subrepresentation. $\qquad\square$

COROLLARY 16.3. *Subgroups and quotients of trigonalizable algebraic groups are trigonalizable.*

PROOF. Let G be a trigonalizable algebraic group. As G admits a faithful trigonalizable representation, so does every algebraic subgroup. Let Q be a quotient of G. A nonzero representation of Q can be regarded as a representation of G, and so it has a one-dimensional subrepresentation. $\qquad\square$

COROLLARY 16.4. *Let G be an algebraic group over k, and let k' be a field containing k. If G is trigonalizable, then so also is $G_{k'}$.*

PROOF. An embedding $G \hookrightarrow \mathbb{T}_n$ gives an embedding $G_{k'} \hookrightarrow \mathbb{T}_{nk'}$ by extension of scalars. $\qquad\square$

REMARK 16.5. Extensions of trigonalizable groups need not be trigonalizable. For example, commutative algebraic groups over algebraically closed fields are trigonalizable (16.14), but solvable algebraic groups need not be (16.36, 16.37).

THEOREM 16.6. *The following conditions on an algebraic group G over k are equivalent:*

(a) G becomes trigonalizable over a separable field extension of k;

(b) G contains a normal unipotent algebraic subgroup G_u such that G/G_u is of multiplicative type.

When these conditions hold, G_u is unique and contains every unipotent algebraic subgroup of G.

PROOF. Let G be an algebraic group over k. A normal unipotent subgroup U of G such that G/U is multiplicative contains every unipotent subgroup V of G, because the composite $V \to G \to G/U$ is trivial (14.18); in particular, there exists at most one such U.

(a)$\Rightarrow$(b). Let k' be a finite Galois extension of k such that $G_{k'}$ is trigonalizable. According to Proposition 16.2(d), $G_{k'}$ contains a U as in the first paragraph, which, being unique, is stable under $\mathrm{Gal}(k'/k)$, and therefore arises from an algebraic subgroup G_u of G (see 1.54). Now G_u is unipotent because it becomes so over k', and G/G_u is of multiplicative type because it becomes diagonalizable over k'.

(b)$\Rightarrow$(a). The quotient G/G_u becomes diagonalizable over some finite separable extension k' of k (see 12.18). As G_u remains unipotent over k' (see 14.9), it follows that G becomes trigonalizable over k' (see 16.2d). $\qquad\square$

NOTATION 16.7. When G is an algebraic group, we use G_u exclusively to denote a normal algebraic subgroup such that G_u is unipotent and G/G_u is of multiplicative type.

Notes

Let G be an algebraic group over k satisfying the equivalent conditions of Theorem 16.6.

16.8. The algebraic subgroup G_u is characterized by each of the following properties: (a) it is the largest unipotent algebraic subgroup of G; (b) it is a normal unipotent algebraic subgroup U of G such that G/U is of multiplicative type; (c) it is the smallest normal algebraic subgroup U such that G/U is of multiplicative type. From (b), it follows that the formation of G_u commutes with extension of the base field.

16.9. Assume that k is perfect. Let (V, r) be a faithful representation of G. By assumption, there exists a basis of V_{k^a} for which $r(G)_{k^a} \subset \mathbb{T}_n$, and then

$$r(G_u)_{k^a} = \mathbb{U}_n \cap r(G)_{k^a}.$$

As $\mathbb{U}_n(k^a)$ consists of the unipotent elements of $\mathbb{T}_n(k^a)$, it follows that $G_u(k^a)$ consists of the unipotent elements of $G(k^a)$:

$$G_u(k^a) = G(k^a)_u.$$

If G_u is smooth, this equality characterizes G_u (1.18).

16.10. If G is smooth (resp. connected), then G_u is smooth (resp. connected) because it becomes a quotient of G over k^a (see 16.26a below).

b.   Commutative algebraic groups

Let u be an endomorphism of a finite-dimensional vector space V over k. If the eigenvalues of u lie in k, then there exists a basis of V for which the matrix of u lies in

$$
\mathbb{T}_n(k) = \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\}
$$

(9.10). We extend this elementary statement to sets of commuting endomorphisms, and then to connected solvable group varieties over algebraically closed fields.

LEMMA 16.11. *Let V be a finite-dimensional vector space over an algebraically closed field k, and let S be a set of commuting endomorphisms of V. Then there exists a basis of V such that all elements of S are represented by upper triangular matrices.*

PROOF. By a standard argument (see the proof of 16.2), it suffices to show that there exists a one-dimensional subspace of V stable under S. We prove this by induction on the dimension of V. If every $u \in S$ is a scalar multiple of the identity map, then there is nothing to prove. Otherwise, there exists a $u \in S$ and an eigenvalue a for u such that the eigenspace $V_a \neq V$. As every element of S commutes with u, the space V_a is stable under the action of the elements of S. By the induction hypothesis, V_a contains a one-dimensional subspace stable under S. $\qquad\square$

PROPOSITION 16.12. *Let V be a finite-dimensional vector space over an algebraically closed field k, and let G be a smooth commutative algebraic subgroup of GL_V. Then there exists a basis of V for which G is contained in $\mathbb{T}_n$.*

PROOF. According to the lemma, there exists a basis of V for which $G(k) \subset \mathbb{T}_n(k)$. Now $G \cap \mathbb{T}_n$ is an algebraic subgroup of G such that $(G \cap \mathbb{T}_n)(k) = G(k)$. As $G(k)$ is dense in G (see 1.17), this implies that $G \cap \mathbb{T}_n = G$, and so $G \subset \mathbb{T}_n$. $\square$

Let G be an algebraic group over a perfect field k, and let $G(k)_s$ (resp. $G(k)_u$) denote the set of semisimple (resp. unipotent) elements of $G(k)$. Theorem 9.18 shows that

$$
G(k) = G(k)_s \times G(k)_u \quad \text{(product of sets).} \tag{116}
$$

This is not usually a decomposition of groups because products do not generally respect Jordan decompositions. When G is commutative, the multiplication map $m: G \times G \to G$ is a homomorphism of algebraic groups, and so it *does* respect the Jordan decompositions (9.21):

$$(gg')_s = g_s g'_s \quad (gg')_u = g_u g'_u$$

(this can also be proved directly). Thus, in this case (116) realizes $G(k)$ as a product of abstract subgroups. We can do better.

THEOREM 16.13. *Let G be a commutative algebraic group over k.*

(a) *There exists a largest algebraic subgroup G_s of G of multiplicative type; this is a characteristic subgroup of G, and the quotient G/G_s is unipotent.*

(b) *If k is perfect, then there also exists a largest unipotent algebraic subgroup G_u of G, and*

$$G \simeq G_u \times G_s$$

(unique decomposition of G into a product of a unipotent subgroup and a subgroup of multiplicative type).

PROOF. (a) Let G_s denote the intersection of the algebraic subgroups H of G such that G/H is unipotent. Then $G/G_s \to \prod G/H$ is an embedding, and so G/G_s is unipotent (14.7). Clearly, G_s is the smallest algebraic subgroup with this property.

To prove that G_s is of multiplicative type it suffices to show that every homomorphism $G_s \to \mathbb{G}_a$ is trivial (12.18). Let φ be such a homomorphism, and let N be its kernel. Then G/N is an extension of unipotent groups,

$$0 \to G_s/N \to G/N \to G/G_s \to 0,$$

and hence is unipotent (14.7). It follows that $N = G_s$, and so $\varphi = 0$.

Let H be another algebraic subgroup of G of multiplicative type. The composite $H \to G \to G/G_s$ is trivial (14.18), and so $H \subset G_s$.

Let α be an endomorphism of G_R for some k-algebra R. The composite

$$(G_s)_R \to G_R \xrightarrow{\alpha} G_R \to (G/G_s)_R$$

is trivial (15.18), and so $\alpha(G_{sR}) \subset G_{sR}$. Hence G_s is characteristic (1.53).

(b) If $G = U \times M$ with U unipotent and M multiplicative, then the decomposition is unique (and $M = G_s$). Indeed, if U' is a unipotent subgroup of G, then the map $U' \to G \to G/U \simeq M$ is trivial (14.18), and so $U' \subset U$. Similarly, M contains every subgroup of multiplicative type.

Because k^a is Galois over k, the uniqueness shows that any such decomposition over k^a arises from a decomposition over k. Thus we may suppose that k is algebraically closed. Now the extension

$$e \to G_s \to G \to G/G_s \to e$$

splits (15.37), and so $G = U \times G_s$ with $U \simeq G/G_s$ unipotent. □

Because G_s and G_u become quotients of G over k^a, they are smooth or connected if G is smooth or connected.

COROLLARY 16.14. *Every commutative algebraic group over an algebraically closed field is trigonalizable.*

PROOF. The group satisfies condition (b) of Theorem 16.6. □

COROLLARY 16.15. *A connected commutative group variety G over a perfect field k is a product of a torus and a connected commutative unipotent group variety. When k has characteristic zero, every commutative unipotent algebraic group is a vector group.*

PROOF. Write $G = G_u \times G_s$ (as in 16.13). A smooth connected algebraic group of multiplicative type is a torus, and a connected commutative unipotent algebraic group in characteristic zero is a vector group (14.33). □

COROLLARY 16.16. *Let G be a smooth connected algebraic group of dimension 1 over a field k. Either G becomes isomorphic to $\mathbb{G}_m$ over a finite separable extension of k or it becomes isomorphic to $\mathbb{G}_a$ over a finite purely inseparable extension of k. Over an algebraically closed field, $\mathbb{G}_a$ and $\mathbb{G}_m$ are the only connected group varieties of dimension 1.*

PROOF. The group G is commutative (14.25), and so it contains a multiplicative subgroup G_s such that G/G_s is unipotent. Either $G = G_s$, which gives the first case, or $G = G_u$, which gives the second case (14.53). □

Notes

16.17. Let G be a commutative algebraic group over k. The algebraic subgroup G_s of G in Theorem 16.13 is characterized by each of the following properties: (a) it is the largest algebraic subgroup of G of multiplicative type; (b) it is an algebraic subgroup H of G of multiplicative type such that G/H is unipotent; (c) it is the smallest algebraic subgroup H of G such that G/H is unipotent. It follows from (b) that the formation of G_s commutes with extension of the base field.

16.18. If G is a commutative group variety over a perfect field k, then G_s and G_u are the unique subgroup varieties of G such that $G_s(k^a) = G(k^a)_s$ and $G_u(k^a) = G(k^a)_u$. Thus, we have realized the decomposition (116) on the level of group varieties.

16.19. The subgroup G_u of G in Theorem 16.13(b) is weakly characteristic in G but in general it is not a characteristic subgroup. The argument in the proof of the theorem for G_s fails because there may exist nontrivial homomorphisms $G_{uR} \to G_{sR}$ (see 15.19).

16.20. Statement (b) of Theorem 16.13 fails when k is nonperfect. For example, the group in 11.4 is a commutative nonsplit extension of $(\mathbb{Z}/p\mathbb{Z})_k$ by μ_p. As another example, let $c \in k \smallsetminus k^p$, and let G be the restriction of scalars of $\mathbb{G}_m$ from $k[c^{1/p}]$ to k. Then G is smooth, connected, and commutative and there is a natural inclusion $\mathbb{G}_m \hookrightarrow G$ with smooth unipotent quotient $G/\mathbb{G}_m$. If G contained a nontrivial smooth unipotent subgroup, then $G(k)$ would contain an element of order p because $G(k)$ is dense in G (Exercise 12-10), but $G(k) = k'^{\times}$, which has no such elements.

NOTES. The first published proof that the only connected group varieties of dimension 1 over an algebraically closed field are $\mathbb{G}_a$ and $\mathbb{G}_m$ is that given by Grothendieck in Chevalley 1956–58.

c.　Structure of trigonalizable algebraic groups

THEOREM 16.21. *Let G be a trigonalizable algebraic group over a field k. There exists a normal series,*

$$G \supset G_0 \supset G_1 \supset \cdots \supset G_r = e$$

with the following properties:

(a) $G_0 = G_u$;

(b) *for each $i \geq 0$, the action of G on G_i/G_{i+1} by inner automorphisms factors through G/G_u, and there exists an embedding*

$$G_i/G_{i+1} \hookrightarrow \mathbb{G}_a$$

which is equivariant for some linear action of G/G_u on $\mathbb{G}_a$.

PROOF. Choose an embedding of G in $\mathbb{T}_n$. From the exact sequence

$$e \to \mathbb{U}_n \to \mathbb{T}_n \xrightarrow{q} \mathbb{D}_n \to e,$$

we obtain an exact sequence

$$e \to G \cap \mathbb{U}_n \to G \to q(G) \to e.$$

Let U be a unipotent subgroup of G. Then $q(U)$ is unipotent and diagonalizable, hence trivial. Therefore $U \subset G \cap \mathbb{U}_n$, and so $G \cap \mathbb{U}_n$ is the largest unipotent subgroup G_u of G.

The group $\mathbb{U}_n$ has a normal series

$$\mathbb{U}_n = U^{(0)} \supset \cdots \supset U^{(i)} \supset U^{(i+1)} \supset \cdots \supset U^{(\frac{n(n-1)}{2})} = 0$$

such that each quotient $U^{(i)}/U^{(i+1)}$ is canonically isomorphic to $\mathbb{G}_a$; moreover, $\mathbb{T}_n$ acts linearly on $U^{(i)}/U^{(i+1)}$ through the quotient $\mathbb{T}_n/\mathbb{U}_n$ (see 6.49).

Let $G^{(i)} = U^{(i)} \cap G$. Then $G^{(i)}$ is a normal subgroup of G and $G^{(i)}/G^{(i+1)}$ is an algebraic subgroup of $U^{(i)}/U^{(i+1)} \simeq \mathbb{G}_a$. Therefore, we obtain an embedding of $G^{(i)}/G^{(i+1)}$ into $\mathbb{G}_a$, the group G acts on $G^{(i)}/G^{(i+1)}$ through an action that extends to a linear action on $\mathbb{G}_a$, and the action of $G_u \subset G$ is trivial.　□

COROLLARY 16.22. *If G is smooth, G_u is smooth and connected, and k is perfect, then the sequence in the theorem can be chosen so that each G_i is smooth and connected and each embedding $G_i/G_{i+1} \to \mathbb{G}_a$ is an isomorphism.*

PROOF. Let $G^{(i)}$ be as in the proof of the theorem. Then $(G^{(i)})^\circ_{\mathrm{red}}$ is a smooth connected unipotent subgroup of G_u (see 1.39). Moreover, $(G^{(i)})^\circ$ is normal in G (see 1.52), and so $(G^{(i)})^\circ_{\mathrm{red}}$ is normal in G (see 1.87). The quotient group $(G^{(i)})^\circ_{\mathrm{red}}/(G^{(i+1)})^\circ_{\mathrm{red}}$ is a smooth connected subgroup of $U^{(i)}/U^{(i+1)}$, which is canonically isomorphic to $\mathbb{G}_a$ (see the proof of the theorem). Therefore either $(G^{(i)})^\circ_{\mathrm{red}}/(G^{(i+1)})^\circ_{\mathrm{red}}$ is trivial or it maps isomorphically onto $U^{(i)}/U^{(i+1)}$ (Exercise 14-3). When we omit duplicates from the sequence $G_u = (G^{(0)})^\circ_{\mathrm{red}} \supset (G^{(1)})^\circ_{\mathrm{red}} \supset \cdots$, we obtain a sequence with the required properties. □

In fact, G_u is automatically smooth and connected if G is (16.10).

COROLLARY 16.23. *Let U be a smooth connected unipotent group over a perfect field, and let T be a split torus acting on U. If $U \neq e$, then there exists a central subgroup N of U that is stable under T and equivariantly isomorphic to $\mathbb{G}_a$ for some linear action of T on $\mathbb{G}_a$.*

PROOF. Form the trigonalizable group $U \rtimes T$. The last nontrivial group in the sequence in Corollary 16.22 has the required properties. □

COROLLARY 16.24. *Every smooth connected unipotent algebraic group U over a perfect field k has a central normal series with quotients isomorphic to $\mathbb{G}_a$. Moreover, if a split torus T acts on U, then it is possible to choose the normal series to be stable under T and such that the action of T on the quotients is linear.*

PROOF. This follows by induction from Corollary 16.23. □

COROLLARY 16.25. *Let U be a connected unipotent algebraic group acted on by a torus T. Every algebraic subgroup H of U stable under T and containing U^T is connected. In particular, U^T is connected.*

PROOF. It suffices to show that H_{k^a} is connnected, and so we may suppose that k is algebraically closed. As $H_{\mathrm{red}}(k) = H(k)$, it is stable under $T(k)$. Let $N = N_{U \rtimes T}(H_{\mathrm{red}})$. Then $N(k)$ consists of the elements of $(U \rtimes T)(k)$ normalizing $H_{\mathrm{red}}(k)$ (see 1.84), and so $N(k) \supset T(k)$, which implies that $N \supset T$ because T is smooth. We have shown that H_{red} is stable under T. In particular, U_{red} is stable under T. As $H \supset (U_{\mathrm{red}})^T$ and $(U_{\mathrm{red}})^T$ is smooth (13.1), $H_{\mathrm{red}} \supset (U_{\mathrm{red}})^T$. Therefore, we may replace U and H with U_{red} and H_{red}, and so assume that both are smooth.

We argue by induction on the dimension of U. We may suppose that $U \neq e$. Let N be as in Corollary 16.23. The sequences

$$0 \to N(R) \to U(R) \to (U/N)(R) \to 0$$

are exact because $H^1(R, \mathbb{G}_a) = 0$ (see 2.72), and so there is an exact sequence ((102), p. 305),

$$\cdots \to U^T(k) \to (U/N)^T(k) \to H_0^1(T, N) \overset{15.3}{=\!=} 0.$$

Hence $U^T \to (U/N)^T$ is surjective, and so it is a quotient map (1.71). It follows that HN/N contains $(U/N)^T$, and so HN/N is connected by the induction hypothesis. As $HN/N \simeq H/H \cap N$ (see 5.52), it remains (by 5.59) to prove that $H \cap N$ is connected. Now T acts on N through a character $\chi \colon T \to \mathbb{G}_m$. If $\chi = 0$, then $N \subset U^T \subset H$, and $H \cap N = N$ is connected. Otherwise χ is a quotient map, and $H \cap N$ is stable under the natural action of $\mathbb{G}_m$ on N; this implies that it is connected (Exercise 14-3c).   □

THEOREM 16.26. *Let G be a trigonalizable algebraic group over a field k. The extension*

$$e \to G_u \longrightarrow G \overset{\pi}{\longrightarrow} D \to e$$

splits in each of the following cases:

   (a) *the field k is algebraically closed;*

   (b) *the field k is perfect and G_u is smooth and connected;*

   (c) *the field k is perfect and D is connected.*

PROOF. If $G = D$, there is nothing to prove, and so we may suppose that $G_u \neq e$. Let N be the last nontrivial group in the normal series for G_u defined in Theorem 16.21. Then G/N is trigonalizable, and we have an exact sequence

$$e \to G_u/N \to G/N \to D \to e \tag{117}$$

with $(G_u/N) = (G/N)_u$. By induction on the length of the normal series, we may suppose that the theorem holds for G/N.

By construction, N admits a D-equivariant embedding in $\mathbb{G}_a$ for some linear action of D on $\mathbb{G}_a$, and so there is an exact sequence

$$e \to N \to \mathbb{G}_a \to \mathbb{G}_a/N \to e$$

on which D acts linearly. The quotient $\mathbb{G}_a/N$ is either trivial or isomorphic to $\mathbb{G}_a$ (Exercise 14-3a).

We now prove the theorem. Let $\bar{s} \colon D \to G/N$ be a section of (117). In the following exact commutative diagram, the top row is the pull-back of the bottom row by $\bar{s}$:

$$
\begin{array}{ccccccccc}
e & \longrightarrow & N & \longrightarrow & G \times_{G/N} D & \longrightarrow & D & \longrightarrow & e \\
 & & \big\| & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \bar{s}} & & \\
e & \longrightarrow & N & \longrightarrow & G & \overset{p}{\longrightarrow} & G/N & \longrightarrow & e.
\end{array}
\tag{118}
$$

It remains to show that the top extension splits, because, if $d \mapsto (s(d), g)$ is a section of $G \times_{G/N} D \to D$, then $d \mapsto s(d)$ is a section of $G \to D$.

In case (a), the top extension splits because of Theorem 15.34(d).

In case (b), we choose N as in Corollary 16.23, and then the top extension splits because of 15.34(a).

In case (c), the top extension splits if $N \approx \mathbb{G}_a$ by 15.34(a). If N is finite, then we apply 15.34(c) to $\pi_0(N)$ and then 15.34(b) to N°. $\square$

THEOREM 16.27. *Let G be a trigonalizable algebraic group over an algebraically closed field k, and let $q: G \to D$ be the quotient of G by G_u.*

(a) *Let $s_1, s_2: D \to G$ be sections of q (as a homomorphism of algebraic groups). Then there exists a $u \in G_u(k)$ such that $s_2 = \mathrm{inn}(u) \circ s_1$.*

(b) *The maximal diagonalizable subgroups of G are those of the form $s(D)$ with s a section of q; any two are conjugate by an element of $G_u(k)$.*

PROOF. We begin with an observation. Let $s: D \to G$ be a section to $G \to D$. When we use s to write G as a semidirect product $G = U \rtimes D$, the remaining sections to $G \to D$ are of the form $d \mapsto (f(d), d)$ with $f: D \to U$ a crossed homomorphism. Such a section is of the form $\mathrm{inn}(u) \circ s$ if and only if the crossed homomorphism f is principal (see 15.1).

Let s and s_1 be two sections to $G \to D$. Let N be the last nontrivial term in the normal series Theorem 16.21 for G, and let $\bar{s}$ be the composite of s with the quotient map $p: G \to G/N$. Form the diagram (118) as above. Now $\bar{s}$ and $p \circ s_1$ are two sections of $G/N \to D$. By induction on the length of the normal series of G, there exists a $\bar{u} \in (U/N)(k)$ such that $\mathrm{inn}(\bar{u}) \circ p \circ s_1 = \bar{s}$. Let $u \in U(k)$ lift $\bar{u}$; then

$$p \circ \mathrm{inn}(u) \circ s_1 = \bar{s},$$

and, by replacing s_1 with $\mathrm{inn}(u) \circ s_1$, we may suppose that $p \circ s_1 = \bar{s}$. From the construction of G' as a pull-back, we see that there exist sections $\sigma, \sigma_1: D \to G'$ such that $s = h \circ \sigma$ and $s_1 = h \circ \sigma_1$. As $H^1(D, N) = 0$ (see 15.3), there exists a $u \in N(k)$ such that $\mathrm{inn}(u) \circ \sigma = \sigma_1$, and therefore $\mathrm{inn}(u) \circ s = s_1$, which completes the proof.

(b) Let s be a section of $q: G \to D$ and let S be a diagonalizable subgroup of G. Then $S \cap G_u = e$ (see 14.17), and so q induces an isomorphism of S onto $q(S)$. Let $G' = q^{-1}(q(S))$ and $q' = q|G'$. The sequence

$$e \to G_u \to G' \xrightarrow{q'} q(S) \to e$$

is split by $s' = s|q(S)$. As S gives a section of q', there exists by Theorem 16.26 a $u \in G_u(k)$ such that $S = \mathrm{inn}(u)s'q(S)$. We deduce that $S \subset \mathrm{inn}(u)s(D)$. As S was arbitrary, it follows that $s(D)$ is a maximal diagonalizable subgroup of G, and that any two such subgroups are conjugate by an element of $G_u(k)$. $\square$

PROPOSITION 16.28. *Let*

$$e \to D \to G \to U \to e \tag{119}$$

be an exact sequence of algebraic groups over a perfect field. If D is diagonaliz-able and U is smooth, connected, and unipotent, then the sequence has a unique splitting: $G \simeq D \times U$.

PROOF. Because U is connected, it acts trivially on D (see 12.37). If $s: U \to G$ is a section, then $s(U) = G_u$, and s is uniquely determined. To prove the existence of a section, we use induction on the dimension of U. If $\dim(U) > 0$, then U contains a central subgroup N isomorphic to $\mathbb{G}_a$ (16.23). The pull-back of (119) by the map $N \to U$ splits (15.25), and so (119) comes by pull-back from an extension of U/N by D, which splits by the induction hypothesis. $\square$

SUMMARY 16.29. Similar arguments to those in the proofs Theorems 16.26 and 16.27 suffice to prove the following statement (SGA 3, XVII, 5.2.3, 5.3.1). Let

$$e \to G_u \to G \xrightarrow{\ q\ } D \to e$$

be an exact sequence of algebraic groups with G_u unipotent and D a smooth group of multiplicative type. The sequence splits in each of the following cases:

(a) G_u is commutative and q admits a section as a map of schemes;

(b) k is algebraically closed;

(c) k is perfect and G_u is connected;

(d) G_u is split (as a unipotent group).

Moreover, in each of these cases, any two sections $s_1, s_2: D \to G$ of q as a homomorphism of algebraic groups are conjugate by an element of $G_u(k)$; the maximal subgroups of multiplicative type in G are those of the form $s(D)$ with s a section of q (and so any two such subgroups are conjugate by an element of $G_u(k)$).

d.   Solvable algebraic groups

THEOREM 16.30 (LIE–KOLCHIN). *Let G be a smooth connected solvable algebraic group over k. If k is algebraically closed, then G is trigonalizable.*

PROOF. Let (V, r) be a simple representation of G. We shall use induction on the dimension of G to show that $\dim(V) = 1$. We already know this when G is commutative (16.14), and so we may suppose that G is not commutative.

Because G is solvable, it contains a smooth connected normal algebraic subgroup N such that $\dim(N) < \dim(G)$ (see 6.19). The induction hypothesis applied to N shows that, for some character χ of N, the eigenspace V_χ for N is nonzero. Let W denote the sum of the nonzero eigenspaces for N in V. According to Theorem 4.25, the sum is direct, $W = \bigoplus V_\chi$, and so the set S of characters χ of N such that $V_\chi \neq 0$ is finite.

Let x be a nonzero element of V_χ for some χ, and let $g \in G(k)$. For $n \in N(k)$,

$$ngx = g(g^{-1}ng)x = g \cdot \chi(g^{-1}ng)x = \chi(g^{-1}ng) \cdot gx.$$

The middle equality used that N is normal in G. Thus, gx lies in the eigenspace for the character $\chi^g \overset{\text{def}}{=} (n \mapsto \chi(g^{-1}ng))$ of N. This shows that $G(k)$ permutes the finite set S.

Choose a χ such that $V_\chi \neq 0$, and let $H \subset G(k)$ be the stabilizer of V_χ. Then H consists of the $g \in G(k)$ such that $\chi^g = \chi$, i.e., such that

$$\chi(n) = \chi(g^{-1}ng) \text{ for all } n \in N(k). \tag{120}$$

Clearly H is a subgroup of finite index in $G(k)$, and it is closed for the Zariski topology on $G(k)$ because (120) is a polynomial condition on g for each n. Therefore $H = G(k)$ because otherwise its cosets would disconnect $G(k)$. This shows that $G(k)$ (hence G) stabilizes V_χ.

As V is simple, $V = V_\chi$, and so each $n \in N(k)$ acts on V as a homothety $x \mapsto \chi(n)x$, $\chi(n) \in k$. But each element n of $N(k)$ is a product of commutators $[x, y]$ of elements of $G(k)$ (see 6.20), and so n acts on V as an automorphism of determinant 1. The determinant of $x \mapsto \chi(n)x$ is $\chi(n)^d$, $d = \dim(V)$, and so the image of $\chi \colon N \to \mathbb{G}_m$ is contained in μ_d. As N is smooth and connected, this implies that $\chi(N) = e$ (see 6.8), and so G acts on V through the quotient G/N. Now V is a simple representation of the commutative algebraic group G/N, and so it has dimension 1 (see 16.14). □

Thus, every smooth connected solvable algebraic group over k becomes trigonalizable over a finite extension of k.

COROLLARY 16.31. *A smooth connected solvable algebraic group G over k becomes trigonalizable over a separable field extension of k if and only if $(G_{k^a})_u$ is defined over k.*

PROOF. Because G_{k^a} is trigonalizable, it contains a normal unipotent subgroup $(G_{k^a})_u$ such that $G/(G_{k^a})_u$ is of multiplicative type. If $(G_{k^a})_u$ is defined over k, say, $(G_{k^a})_u = (G_u)_{k^a}$ with G_u an algebraic subgroup of G, then G_u is unipotent and G/G_u is of multiplicative type. Now Theorem 16.6 shows that G becomes trigonalizable over a separable extension of k. Conversely, if G becomes trigonalizable over a separable extension of k, then it contains a normal unipotent subgroup G_u such that G/G_u is of multiplicative type (16.6). Then $(G_u)_{k^a} = (G_{k^a})_u$ because both are normal unipotent subgroups of G with quotient of multiplicative type. □

COROLLARY 16.32. *Let G be a solvable algebraic group over an algebraically closed field k, and let (V, r) be a finite-dimensional representation of G. Then there exists a basis of V for which $r(G^\circ(k)) \subset \mathbb{T}_n(k)$.*

PROOF. The subgroup G°_{red} smooth, connected, and solvable, hence trigonalizable, and $G^\circ_{\mathrm{red}}(k) = G^\circ(k)$. □

THEOREM 16.33. *Let G be a smooth connected solvable algebraic group over a perfect field k.*

(a) *There exists a normal unipotent subgroup G_u of G such that G/G_u is of multiplicative type.*

(b) *The subgroup G_u in (a) contains all unipotent algebraic subgroups of G, and its formation commutes with extension of the base field.*

(c) *The subgroup G_u in (a) is smooth and connected, and G/G_u is a torus; moreover, G_u is the unique smooth algebraic subgroup of G such that $G_u(k^a) = G(k^a)_u$.*

(d) *Suppose that k is algebraically closed, and let T be a maximal torus in G. Then*

$$G = G_u \rtimes T,$$

and every algebraic subgroup of multiplicative type in G is conjugate by an element of $G_u(k)$ to a subgroup of T.

PROOF. Theorem 16.30 shows that G becomes trigonalizable over a finite extension of k, which is separable because k is perfect. Now (a), (b), and (c) follow from 16.6, 16.8, 16.9, and 16.10. When k is algebraically closed, Theorem 16.27 implies that the quotient map $G \to G/G_u$ induces an isomorphism from T onto G/G_u, and so $G \simeq G_u \rtimes T$ (see 2.34). Theorem 16.27 also implies the second part of (d).   □

PROPOSITION 16.34. *Let G be an algebraic group over an algebraically closed field k. The following conditions are equivalent:*

  (a) *G is smooth, connected, and trigonalizable;*

  (b) *G is a split solvable algebraic group;*

  (c) *G is smooth and connected, and the abstract group $G(k)$ is solvable;*

  (d) *G is smooth, connected, and solvable.*

PROOF. (a)$\Rightarrow$(b). As G is smooth and connected, so also is G_u, and so this follows from Corollary 16.22.

(b)$\Rightarrow$(c). We are given that G admits a subnormal series $G \supset G_1 \supset \cdots$ such that each quotient G_i/G_{i+1} is isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. It follows that G is smooth and connected, and $G(k)$ is solvable because $G(k) \supset G_1(k) \supset \cdots$ is a subnormal series for $G(k)$ with commutative quotients.

(c)$\Rightarrow$(d). Recall (p. 132) that the derived series for G is the normal series

$$G \supset \mathcal{D}G \supset \mathcal{D}^2 G \supset \cdots.$$

Each group $\mathcal{D}^i G$ is smooth and connected (6.19), and $\mathcal{D}^{i+1}(G)(k)$ is the derived group of $\mathcal{D}^i(G)(k)$ (6.20). Therefore $\mathcal{D}^i(G)(k) = e$ for i large, which implies that $\mathcal{D}^i(G) = e$ for i large. Hence the derived series terminates with e, and so G is solvable.

(d)$\Rightarrow$(a). This is the Lie–Kolchin theorem (16.30).   □

PROPOSITION 16.35. *Let G be a smooth connected solvable algebraic group over k, and let $U_G(\lambda)$ and $P_G(\lambda)$ be the subgroup varieties of G attached to a cocharacter λ of G (see 13.30). Then the multiplication map*

$$U_G(-\lambda) \times P_G(\lambda) \to G$$

is an isomorphism of algebraic varieties.

PROOF. We may suppose that k is algebraically closed. The map is an open immersion (13.33d), and so it suffices to show that

$$G = U(-\lambda) \cdot Z(\lambda) \cdot U(\lambda)$$

as a set. Fix a maximal torus T containing the image of λ. We may suppose that $G \neq T$. As G is trigonalizable (16.30), Corollary 16.22 and the following comment show that there exists a normal subgroup N of G, isomorphic to $\mathbb{G}_a$, contained in the centre of G_u. By induction on $\dim(G)$, we may suppose that the proposition holds for $G' = G/N$ and the cocharacter λ' induced by λ. Then Proposition 13.34 implies that $G = U(-\lambda) \cdot P_G(\lambda) \cdot N$. On applying Theorem 13.33(c) to the group $N \cdot T$ and the cocharacter λ, we see that N is a subgroup of one of the groups $Z(\lambda)$, $U(\lambda)$, $U(-\lambda)$, which completes the proof. □

NOTES. The proof of Theorem 16.30 is essentially Kolchin's original proof (Kolchin 1948, §7, Theorem 1). For a shorter proof, see 17.4 below. Lie proved the analogous result for Lie algebras in 1876. The implication (c)⟹(a) in Proposition 16.34 is sometimes called the Lie–Kolchin theorem.

Examples

The following examples illustrate the various ways that a solvable algebraic group G over a field k can fail to be trigonalizable.

16.36. Nonconnected. The algebraic group of monomial $n \times n$ matrices is smooth, and it is solvable if $n \leq 4$ (see 2.41), but it is not trigonalizable if $n \geq 2$. Indeed, let G be the group of monomial 2×2 matrices. The eigenvectors of $\mathbb{D}_2(k) \subset G(k)$ in k^2 are $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and their multiples, but the monomial matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ interchanges e_1 and e_2, and so the elements of $G(k)$ have no common eigenvector in k^2.

16.37. Nonsmooth. Let k have characteristic 2, and let G be the algebraic subgroup of SL_2 such that

$$G(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(R) \,\middle|\, a^2 = 1 = d^2,\, b^2 = 0 = c^2 \right\}$$

for all k-algebras R. Then G is a connected finite algebraic group, and

$$e \longrightarrow \mu_2 \xrightarrow{a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}} G \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (ab, cd)} \alpha_2 \times \alpha_2 \longrightarrow e$$

is an exact sequence of homomorphisms. Moreover, $\mu_2 = Z(G) \neq G$ and so G is solvable but not commutative. It is even nilpotent. In the natural action of G on k^2, no line through the origin is fixed by G, and so G is not trigonalizable. Note that $G(k) = e$.

16.38. **Base field not algebraically closed.** If k is perfect, then a smooth connected solvable group G contains a normal unipotent subgroup G_u such that G/G_u is of multiplicative type, but G/G_u need not be split. For example, the matrices $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix} \right)$ such that $a^2 + b^2 = 1$ form a connected commutative algebraic subgroup G of $\mathrm{SL}_{2,\mathbb{R}}$ but have no common eigenvector in $\mathbb{R}^2$. Therefore, G is not trigonalizable over $\mathbb{R}$.

If k is not perfect, then G need not contain a normal unipotent subgroup G_u such that G/G_u is of multiplicative type, even when G is smooth, connected, and commutative. The group $G = (\mathbb{G}_m)_{k'/k}$ with k' purely inseparable over k provides such an example (16.20).

e. Connectedness

In this section, we prove that centralizers of semisimple elements in solvable groups are connected. Throughout, G is a connected group variety and k is algebraically closed.

LEMMA 16.39. *Let N be a connected normal subgroup variety of G, and let $s \in G(k)$. If s is semisimple and N is commutative and unipotent, then $C_N(s)$ is connected; moreover, the map $N \times C_N(s) \to N$, $u, v \mapsto [s,u] \cdot v$ is surjective.*

PROOF. As N is commutative, the regular map $u \mapsto [s,u] \colon N \to N$ is a homomorphism of algebraic groups. Its kernel is $C_N(s)$, and we let M denote its image; thus

$$\dim N = \dim M + \dim C_N(s) \tag{121}$$

(by 5.23). If $x \in (M \cap C_N(s))(k)$, then $x = sus^{-1}u^{-1}$ for some $u \in N$, and $sx^{-1} = x^{-1}s = usu^{-1}$. As usu^{-1} is semisimple and x is unipotent, the uniqueness of Jordan decompositions implies that $x = e$. Hence the multiplication map

$$\mu \colon M \times C_N(s) \to N$$

has finite connected kernel, and so (121) implies that it is surjective. Now $C_N(s)$ is connected because both the kernel of μ and its image are connected (apply 5.59). As μ is surjective, so is its composite with $(u \mapsto [s,u] \colon N \to M) \times C_N(s)$. □

THEOREM 16.40. *Let G be a connected solvable group variety, and let s be a semisimple element of $G(k)$. Then $C_G(s)$ is connected and $G = U \cdot C_G(s)$ with U a unipotent subgroup of G.*

PROOF. We use induction on $\dim G$. If G is commutative, then there is nothing to prove. Otherwise, we let N denote the last nontrivial term in the derived series of G. The Lie–Kolchin theorem implies that the derived group of G is unipotent, and so N is unipotent; it is also connected, normal, and commutative.

Write $x \mapsto \bar{x}$ for the quotient map $G \to G/N$. Let $z \in G(k)$ be such that $\bar{z} \in C_{\bar{G}}(\bar{s})$. Then $[s, z] \in N$, and so $[s, z] = [s, u] \cdot v$ for some $u \in N$ and $v \in C_N(s)$ (see 16.39). In other words,

$$szs^{-1}z^{-1} = sus^{-1}u^{-1} \cdot v,$$

and so

$$zs^{-1}z^{-1} = us^{-1}u^{-1} \cdot v.$$

As v is unipotent and commutes with u and s, this implies that $v = e$ because of the uniqueness of the Jordan decomposition. Thus $u^{-1}z \in C_G(s)$. We have shown that $C_G(s)(k) \to C_{\bar{G}}(\bar{s})(k)$ is surjective, which implies that $C_G(s) \to C_{\bar{G}}(\bar{s})$ a quotient map because $C_{\bar{G}}(\bar{s})$ is smooth (1.71, 13.8) Therefore, the sequence

$$e \to C_N(s) \to C_G(s) \to C_{\bar{G}}(\bar{s}) \to e$$

is exact. By the induction hypothesis, $C_{\bar{G}}(\bar{s})$ is connected; as $C_N(s)$ is connected, so also is $C_G(s)$ (apply 5.59).

By the induction hypothesis, $\bar{G} = U \cdot C_{\bar{G}}(\bar{s})$ with U unipotent. Let $\tilde{U}$ denote the inverse image of U in G. Then $G = \tilde{U} \cdot C_G(s)$, and $\tilde{U}$ is unipotent because it is the extension of a unipotent group U by a unipotent group N. □

THEOREM 16.41. *Let S be a torus in a connected solvable group variety G. Then $C_G(S)$ is connected and $G = U \cdot C_G(S)$ with U unipotent subgroup of G.*

PROOF. As S is diagonalizable, every element of $S(k)$ is semisimple. Therefore, the theorem follows from Theorem 16.40 and the next lemma. □

LEMMA 16.42. *Let S be a torus in a connected group variety G. There exists an $s \in S(k)$ such that $C_G(s) = C_G(S)$.*

PROOF. Choose a faithful finite-dimensional representation (V, r) of G, and write V as a sum of eigenspaces $V = \bigoplus V_{\chi_i}$ of S (see 12.12). For each pair (i, j) with $i \neq j$, let $S_{ij} = \{s \in S(k) \mid \chi_i(s) = \chi_j(s)\}$. Then S_{ij} is a proper closed subset of $S(k)$, and so there exists an $s \in S(k) \smallsetminus \bigcup_{i \neq j} S_{ij}$. It is semisimple, and so $C_G(s)$ is smooth (13.8). An element of $G(k)$ commutes with s if and only if it stabilizes each V_{χ_i}, in which case it centralizes S. Therefore $C_G(s)(k) \subset C_G(S)(k)$. As $C_G(S) \subset C_G(s)$, the smoothness of $C_G(s)$ now implies that the two are equal. □

NOTES. The short elementary proof of Theorem 16.41 follows Doković 1988. The standard proof deduces it from Corollary 16.25.

f. Nilpotent algebraic groups

We extend earlier results from commutative algebraic groups to nilpotent algebraic groups.

Recall (6.34) that an algebraic group is nilpotent if it has a central normal series. The last nontrivial term in such a series is contained in the centre of the group. Therefore, a nontrivial nilpotent algebraic group G has nontrivial centre. If G is smooth and connected, then so are the terms in its descending central series, and so $Z(G)$ contains a connected group variety of dimension > 0.

LEMMA 16.43. *Let $H' \subset H$ be normal algebraic subgroups of a connected algebraic group G. If H' and H/H' are both of multiplicative type, then H is central and of multiplicative type.*

PROOF. It follows from Corollary 12.41 that the action of G on H by inner automorphisms is trivial. Therefore H is central, in particular, commutative, and so it is multiplicative (12.22).   □

LEMMA 16.44. *Let G be an algebraic group, and let T and U be normal algebraic subgroups of G. If T is of multiplicative type and G/T is unipotent, while U is unipotent and G/U is of multiplicative type, then the map*

$$(t,u) \mapsto t u : T \times U \to G \tag{122}$$

is an isomorphism

PROOF. Note that $T \cap U = e$ (see 14.17). Elements $t \in T(R)$ and $u \in U(R)$ commute because $tut^{-1}u^{-1} \in (T \cap U)(R) = e$, and so the map (122) is a homomorphism. Its kernel is $T \cap U = e$, and its cokernel is a quotient of both G/T and G/U. Hence it is both unipotent and multiplicative, which implies that it is trivial (14.17).   □

LEMMA 16.45. *Let G be a connected nilpotent algebraic group, and let $Z(G)_s$ be the largest multiplicative subgroup of its centre (16.13). Then the centre of $G/Z(G)_s$ is unipotent.*

PROOF. Let $G' = G/Z(G)_s$, and let N be the inverse image of $Z(G')_s$ in G. Then N and $Z(G)_s$ are normal subgroups of G (recall that $Z(G)_s$ is characteristic in $Z(G)$), and $N/Z(G)_s \simeq Z(G')_s$ is of multiplicative type, and so N is central and of multiplicative type (16.43). Therefore $N \subset Z(G)_s$, and so $Z(G')_s = e$.□

LEMMA 16.46. *A connected nilpotent algebraic group is unipotent if its centre is.*

PROOF. Let G be a connected nilpotent algebraic group over k with unipotent centre $Z(G)$. It suffices to show that G_{k^a} is unipotent (14.9). This allows us to assume that k is algebraically closed. We prove that G is unipotent by induction on its dimension.

Because G is nilpotent, $Z(G) \neq e$, and we may suppose that $Z(G) \neq G$. Let $G' = G/Z(G)$, and let N be the inverse image of $Z(G')_s$ in G. It suffices so show that (a) G/N is unipotent, and (b) N is unipotent.

(a) The group $G/N \simeq G'/Z(G')_s$, which has unipotent centre (16.45), and so is unipotent by the induction hypothesis.

(b) In the exact sequences

$$e \to Z(N)_s \to N \to N/Z(N)_s \to e$$
$$e \to Z(G) \to N \to Z(G')_s \to e,$$

$Z(N)_s$ and $Z(G')_s$ are of multiplicative type and $Z(G)$ and $N/Z(N)_s$ are unipotent. Therefore $N \simeq Z(N)_s \times Z(G)$ (see 16.44), which is commutative. As $Z(N)_s$ is characteristic in N (16.13), it is normal in G, and hence central in G (see 12.37). But $Z(G)$ is unipotent, and so $Z(N)_s = 0$. We have shown that $Z(N)$ is unipotent, and so N is unipotent (by induction). □

THEOREM 16.47. *Let G be a connected nilpotent algebraic group over k.*

(a) $Z(G)_s$ is the largest algebraic subgroup of G of multiplicative type; it is characteristic and central, and the quotient $G/Z(G)_s$ is unipotent.

(b) If G becomes trigonalizable over a separable extension of k, then it has a unique decomposition into a product $G = G_u \times Z(G)_s$ with G_u unipotent and $Z(G)_s$ of multiplicative type.

(c) If G is smooth, then $Z(G)_s$ is a torus.

PROOF. (a) The quotient $G/Z(G)_s$ has unipotent centre (16.45), and so it is unipotent (16.46). Therefore, every multiplicative algebraic subgroup of G maps to e in the quotient $G/Z(G)_s$ (see 14.18), and so is contained in $Z(G)_s$. Therefore $Z(G)_s$ is the largest algebraic subgroup of G of multiplicative type. It is obviously central. The same argument as in the proof of Theorem 16.13 shows that it is characteristic.

(b) Because G becomes trigonalizable over k^s, it contains a normal unipotent subgroup G_u such that G/G_u is of multiplicative type (16.6). Therefore the statement follows from (16.44) applied to G_u and $Z(G)_s$.

(c) The formation of $Z(G)_s$ commutes with extension of the base field, and so we may suppose that k is perfect. Then G becomes trigonalizable over k^s by the Lie–Kolchin theorem, and so $G = G_u \times Z(G)_s$. It follows that $Z(G)_s$ is smooth and connected. □

COROLLARY 16.48. *The connected nilpotent group varieties over a perfect field k are exactly those of the form $U \times T$ with U a connected unipotent group variety and T a torus.*

PROOF. Certainly, a group of this form is nilpotent (14.21). Conversely, if G is smooth, connected, and nilpotent, then it becomes trigonalizable over a finite extension of k (see 16.30), which is separable if k is perfect. In this case, $G = U \times D$ with U unipotent and D of multiplicative type (16.47b). As G is smooth and connected, so are U and D. □

PROPOSITION 16.49. *Let G be an algebraic group over an algebraically closed field k. The following conditions are equivalent:*

(a) *G is smooth, connected, and nilpotent;*

(b) *G admits a normal series with quotients $\mathbb{G}_a$ or $\mathbb{G}_m$ on which the action of G by inner automorphisms is trivial;*

(c) *G is smooth and connected, and the abstract group $G(k)$ is nilpotent.*

PROOF. (a)$\Rightarrow$(b). In fact, $G = U \times T$ with U smooth, connected, and unipotent and T a torus. Now (b) follows from Corollary 16.24 and the fact that T is a split torus.

(b)$\Rightarrow$(c). The group G is smooth and connected because it is obtained from smooth connected groups by successive extension. The group $G(k)$ has a normal series with quotients $\mathbb{G}_a(k)$ or $\mathbb{G}_m(k)$ on which the action of $G(k)$ is trivial, and so it is nilpotent.

(c)$\Rightarrow$(a). According to Proposition 16.34, G is trigonalizable. As it is smooth and connected, so also is G_u. After Corollary 16.22, it remains to show that action of the torus $D = G/G_u$ on G_u is trivial. We argue by induction on the dimension of G_u. From Corollary 16.22 again, we see that there exists a normal subgroup U of G, contained in G_u and isomorphic to $\mathbb{G}_a$, on which G acts linearly. We claim that D acts trivially on U. By assumption, it acts through a character χ, and so, for $t \in D(k)$ and $x \in U(k) \approx k$,

$$txt^{-1}x^{-1} = (\chi(t) - 1)x.$$

As $G(k)$ is nilpotent, there exists an n such that $(\chi(t) - 1)^n = 0$ for all $t \in D(k)$. As D is smooth, this implies that $\chi(t) = 1$ for all $t \in D(k)$, and so $\chi = 1$. Thus D acts trivially on U. It acts trivially on G/U by the induction hypothesis, and so the statement follows from the next lemma. □

LEMMA 16.50. *Let D be a diagonalizable group acting on an exact sequence of smooth unipotent groups*

$$e \to \mathbb{G}_a \to U \to V \to e.$$

If D acts trivially on $\mathbb{G}_a$ and V, then it acts trivially on U.

PROOF. There is an exact sequence

$$1 \to \mathbb{G}_a(k) \to U^D(k) \to V(k) \to H_0^1(D, \mathbb{G}_a)$$

((102), p. 305). Now $H_0^1(D, \mathbb{G}_a) = 0$ (see 15.34), and so $U^D(k) = U(k)$. As U is reduced, this implies that $U^D = U$. □

g. Split solvable groups

Recall (6.33) that a solvable algebraic group is said to be split if it admits a subnormal series with quotients isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. Every split solvable algebraic group is smooth and connected. Quotients of split solvable groups are split because nontrivial quotients of $\mathbb{G}_a$ and $\mathbb{G}_m$ are isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$ (Exercise 14-3). Extensions of split solvable groups are obviously split, but subgroups of split solvable groups, even normal subgroups, need not be split. For example, there are many nonsplit subgroups of $\mathbb{G}_a \times \mathbb{G}_a$ (see 14.57).

THEOREM 16.51 (FIXED POINT THEOREM). *Let G be a split solvable algebraic group acting on a complete algebraic scheme X. If $X(k)$ is nonempty, then $X^G(k)$ is nonempty.*

PROOF. Suppose first that G is $\mathbb{G}_a$, and identify $\mathbb{G}_a$ with the complement of ∞ in $\mathbb{P}^1$. Let $x \in X(k)$. If x is not fixed by G, then the map $g \mapsto gx \colon G \to X$ extends uniquely to $\mathbb{P}^1$ (because X is complete). Let $\lim_{t \to \infty} t \cdot x$ denote the image of ∞. Then $\lim_{t \to \infty} t \cdot x \in X(k)$, and, for every $t' \in T(k^{\mathrm{a}})$,

$$t'(\lim_{t \to \infty} t \cdot x) = \lim_{t \to \infty} t't \cdot x = \lim_{t \to \infty} t \cdot x,$$

and so $\lim_{t \to \infty} t \cdot x$ is the required fixed point. A similar argument applies if $G = \mathbb{G}_m$. In the general case, G has a subnormal series $G \rhd G_1 \rhd \cdots \rhd G_r \rhd e$ with quotients $\mathbb{G}_a$ or $\mathbb{G}_m$, and

$$X(k) \neq \emptyset \Rightarrow X^{G_r}(k) \neq \emptyset \Rightarrow \cdots \Rightarrow X^G(k) \neq \emptyset. \qquad \square$$

PROPOSITION 16.52. *Let G be a smooth connected algebraic group over k. If G is split solvable, then it is trigonalizable, and the converse is true when k is perfect.*

PROOF. Suppose that G is split solvable. Choose a faithful representation of G, and let G act on the algebraic variety of maximal flags (7.29). Then G fixes a flag (16.51), and so the representation is trigonalizable. Conversely, if k is perfect and G is trigonalizable, then we can apply Corollary 16.24 to the split torus G/G_u acting on G_u. $\qquad \square$

In particular, smooth connected unipotent groups over perfect fields are split solvable groups.

COROLLARY 16.53. *Every smooth connected solvable algebraic group over an algebraically closed field is split.*

PROOF. According to the Lie–Kolchin theorem (16.30), G is trigonalizable. $\quad \square$

PROPOSITION 16.54. *Let G be a split solvable algebraic group over a field k. The canonical extension*

$$e \to G_u \longrightarrow G \xrightarrow{q} D \to e$$

splits, and any two sections $s_1, s_2 \colon D \to G$ of q are conjugate by an element of $G_u(k)$. The maximal split tori in G are those of the form $s(D)$ with s a section of q (and so any two such tori are conjugate by an element of $G_u(k)$).

PROOF. As G is trigonalizable (16.52), there does exist such an exact sequence. The unipotent subgroup G_u is split and the quotient D is smooth, and so the rest of the statement follows from 16.29(d). □

PROPOSITION 16.55. *Let G be a split solvable algebraic group over a field k.*

(a) *If X is an affine algebraic scheme over k such that $\mathrm{Pic}(X) = 0$, then every G-torsor over X is trivial.*

(b) *If X is an affine algebraic scheme over k and G is unipotent, then every G-torsor over X is trivial.*

(c) *Every G-torsor is locally split for the Zariski topology.*

PROOF. According to Example 2.72, statements (a) and (c) are true for $\mathbb{G}_m$ and $\mathbb{G}_a$ and (b) is true for $\mathbb{G}_a$. It follows that they are true for G. □

COROLLARY 16.56. *Let G be a split solvable algebraic group over k. The underlying scheme of G is isomorphic to $\mathbb{A}^r \times (\mathbb{A}^1 \smallsetminus 0)^{n-r}$, where $n = \dim G$ and $r = \dim G_u$. Hence $\mathrm{Pic}(G) = 0$.*

PROOF. The scheme G is a G_u-torsor over G/G_u (see 2.68). This torsor is trivial by (b) of the proposition, and so $G \approx G_u \times G/G_u$ as algebraic schemes. Here G/G_u is a split torus, and so it is isomorphic to $\mathbb{G}_m^{n-r}$. On the other hand, G_u has a subnormal series with quotients isomorphic to $\mathbb{G}_a$. An induction argument using (b) of the proposition shows that $G_u \approx \mathbb{A}^r$ (as a scheme). The second statement follows from the fact that the polynomial ring $k[T_1, \ldots, T_n]$ is a unique factorization domain (see A.79 and CA 4.10). □

For example, the underlying scheme of a smooth connected unipotent group U over a perfect field is isomorphic to $\mathbb{A}^{\dim(U)}$.

COROLLARY 16.57. *Every connected nilpotent group variety over a perfect field is unirational.*

PROOF. Such a group variety is a product of a torus and a connected unipotent group variety (16.48). The first is unirational (12.64) and the second is rational (16.56). □

In particular, if a solvable algebraic group G is split, then there exists a dominant map $(\mathbb{A}^1 \smallsetminus 0)^n \to G$ for some integer n. We prove a converse.

THEOREM 16.58 (ROSENLICHT). *A solvable group variety G is split if there exists a dominant map of schemes $\varphi \colon (\mathbb{A}^1 \smallsetminus 0)^n \to G$ for some integer n.*

PROOF. We first prove this in three special cases.

Case G is of multiplicative type. After composing φ with a translation, we may suppose that $\varphi(e) = e$. Now φ is a surjective homomorphism $\mathbb{G}_m^n \to G$ (see 12.49), and so G is a split torus.

Case G is commutative and unipotent and $\operatorname{char}(k) = 0$. Without any hypotheses, G is isomorphic to $\mathbb{G}_a^{\dim(G)}$ (see 14.33).

Case G is elementary unipotent and $\operatorname{char}(k) = p$. It suffices to show that

$$P(G) \overset{\text{def}}{=} \{ f \in \mathcal{O}(G) \mid \varDelta(f) = f \otimes 1 + 1 \otimes f \}$$

is a free $k_\sigma[F]$-module because then G will be a product of copies of $\mathbb{G}_a$ (see 14.46). Let $X = (\mathbb{A}^1 \smallsetminus 0)^n$, and endow $\mathcal{O}(X)$ with the structure of a left $k_\sigma[F]$-module by setting $Fa = a^p$. Then

$$\mathcal{O}(X) = k[T_1, \dots, T_n, T_1^{-1}, \dots, T_n^{-1}]$$

is a direct sum of k and a free $k_\sigma[F]$-module with basis the set of monomials $T_1^{r_1} \cdots T_n^{r_n}$ for which the exponents r_i are integers such that $\mathbb{Z}p + \mathbb{Z}r_1 + \cdots + \mathbb{Z}r_n = \mathbb{Z}$. Now the maps

$$P(G) \hookrightarrow \mathcal{O}(G)/k \hookrightarrow \mathcal{O}(X)/k$$

realize $P(G)$ as a $k_\sigma[F]$-submodule of a free $k_\sigma[F]$-module, and so it is free (14.50).

General case. We use induction on $\dim(G)$. First observe that if G contains a normal subgroup variety N satisfying the hypothesis of the theorem and such that $\dim(G) > \dim(N) > 0$, then each of G/N and N is split (induction), and so G is split. The derived group of G satisfies the hypothesis of the theorem because the map $G^{2n} \to \mathcal{D}(G)$ is dominant for some n (6.20a), and so we may suppose that G is commutative. If $\operatorname{char}(k) = 0$, then G is a product of a multiplicative group and unipotent group (16.13), and so this case follows from the special cases proved above. If $\operatorname{char}(k) = p \neq 0$, then the image of the homomorphism $p \colon G \to G$ satisfies the hypothesis of the theorem. From the exact sequence $0 \to pG \to G \to G/pG \to 0$ we see that we need consider only the cases $G = pG$ and $pG = e$. If $G = pG$, then G is multiplicative because otherwise p will not be surjective on the unipotent quotient G/G_s in (16.13). If $pG = e$, then $V_G = 0$ because F_G is surjective (2.29), and so G is elementary unipotent (14.48). This completes the proof. □

Concretely, this says that G is split if and only if there exists an injective homomorphism of k-algebras

$$\mathcal{O}(G) \to k[T_1, \dots, T_n, T_1^{-1}, \dots, T_n^{-1}].$$

THEOREM 16.59 (LAZARD). *Let G be an algebraic group over k. The following conditions on G are equivalent:*

(a) *there exists an isomorphism of k-schemes $G \to \mathbb{A}^{\dim(G)}$;*

(b) *G is a split unipotent group;*

(c) *G is reduced and solvable, and there exists a dominant map of k-schemes $\mathbb{A}^N \to G$ for some integer N.*

PROOF. See DG, IV, §4, 4.1.   □

NOTES. This section follows DG, IV, §4, no. 3.

h.   Complements on unipotent algebraic groups

PROPOSITION 16.60. *A connected group variety G over an algebraically closed field is unipotent if it contains no nontrivial torus.*

PROOF. Let (V, r) be a finite-dimensional faithful representation of G, and let $\mathcal{B}$ be the algebraic variety of maximal flags in V (see 7.29). Then G acts on $\mathcal{B}$, and there exists a closed orbit (1.66), say $O \simeq G/U$. The variety G/U is complete, and the map $G/U \to G/U_{\mathrm{red}}^\circ$ is finite (7.15), and so G/U_{red}° is complete (A.75). The group U_{red}° is smooth, connected, and solvable, and so it is the semidirect product of a unipotent group and a torus (16.33d). The torus is trivial because of the hypothesis on G. Therefore U_{red}° is unipotent. Now G/U_{red}° is a subscheme of an affine scheme (14.26). As it is also complete and connected, it is a point. Hence $G = U_{\mathrm{red}}^\circ$ is unipotent.   □

COROLLARY 16.61. *Let G be a connected group variety. The following conditions are equivalent:*

(a) *G is unipotent;*

(b) *The centre of G is unipotent and $\mathfrak{g}$ is nilpotent;*

(c) *For every representation (V, r) of G, dr maps the elements of $\mathfrak{g}$ to nilpotent endomorphisms of V;*

(d) *The condition in (c) holds for one faithful representation (V, r) of G.*

PROOF. (a)⇒(b). Every algebraic subgroup, in particular, the centre, of a unipotent algebraic group is unipotent (14.7). An embedding of G into $\mathbb{U}_n$ (see 14.5) defines an embedding of $\mathfrak{g}$ into $\mathfrak{n}_n$.

(b)⇒(a). We may suppose that k is algebraically closed (14.9). If the centre of G is unipotent, then the kernel of the adjoint representation is an extension of unipotent algebraic groups (14.23), and so it is unipotent (14.7). Therefore, if G contains a subgroup H isomorphic to $\mathbb{G}_m$, then H acts faithfully on $\mathfrak{g}$. Let $\mathfrak{g} = \bigoplus_{n \in \mathbb{Z}} \mathfrak{g}_n$ where $h \in H(k)$ acts on $\mathfrak{g}_n$ as h^n. A nonzero element x of $\mathfrak{h}$ acts on each $\mathfrak{g}_n$ as multiplication by nx, and so it acts semisimply on $\mathfrak{g}$, contradicting the nilpotence of $\mathfrak{g}$.

(a)$\Rightarrow$(c). There exists a basis for V such that G maps into $\mathbb{U}_n$ (see 14.3).

(c)$\Rightarrow$(d). Trivial.

(d)$\Rightarrow$(a). We may suppose that k is algebraically closed (14.9). Let (V, r) be a faithful representation as in (d). If G contains a subgroup H isomorphic to $\mathbb{G}_m$, then $V = \bigoplus_{n \in \mathbb{Z}} V_n$ where $h \in H(k)$ acts on V_n as h^n. A nonzero element x of $\mathfrak{h}$ acts on each V_n as multiplication by nx, contradicting the hypothesis. □

i. Tori acting on algebraic groups

Unipotent groups

Let G be a smooth connected algebraic group over an algebraically closed field, and let T be a maximal torus of G. When G is solvable, we showed in Theorem 16.33(d) that every subtorus of G of multiplicative type is conjugate by an element of G to a subgroup of T. In Theorem 17.10 below we show, as a consequence of the Borel fixed point theorem, that any two maximal solvable subgroups of G are conjugate by an element of $G(k)$, from which it follows that the preceding statement holds also for nonsolvable G. In the next proposition, we assume this as it strengthens the statement and the proof of 17.10 is independent of the proposition.

PROPOSITION 16.62. *Let G be a smooth connected algebraic group with an action of a torus T. If $\mathfrak{g}^T = 0$, then G is unipotent and the action of T on $\mathfrak{g}$ is strictly definite (13.40).*

PROOF. We may suppose that k is algebraically closed.

If G is not unipotent, then it contains a nontrivial torus S (see 16.60). Let T' be a maximal torus of $G \rtimes T$ containing S. Some conjugate $gT'g^{-1}$ of T' contains T (see above). Now both gSg^{-1} and T are contained in the torus $gT'g^{-1}$, and so T normalizes gSg^{-1} and acts trivially on it and its Lie algebra. As $gSg^{-1} \subset G$, this contradicts the hypothesis.

Thus G is unipotent. Therefore there exists an embedding of $G \rtimes T$ into $\mathbb{T}_n$ for some n such that G maps into $\mathbb{U}_n$ and T maps into $\mathbb{D}_n$. The action of $\mathbb{D}_n$ on $\mathfrak{u}_n$ is definite, and it follows that the action of T on $\mathfrak{g}$ is definite. As $\mathfrak{g}^T = 0$, it is strictly definite. □

PROPOSITION 16.63. *Let G be a smooth connected algebraic group with an action of a split torus T. If $\mathfrak{g}^T = 0$, then $G^T = e$ and every Luna map $G \to \mathrm{Tgt}_e(G)_{\mathfrak{a}}$ is an equivariant isomorphism of schemes over k; moreover, G is a split unipotent group.*

PROOF. According to Proposition 16.62, the action of T on $\mathfrak{g}$ is strictly definite, and so the first part of the statement follows from Theorem 13.41. Again 16.62 implies that G is unipotent, and it is split because of Rosenlicht's theorem (16.58). □

The algebraic subgroup attached to a semigroup of characters

Let G be a connected group variety with an action of a split torus T, and let $\Phi = \Phi(G, T)$ denote the set of nonzero weights of T on $\mathrm{Lie}(G)$, so

$$\mathfrak{g} = \mathfrak{g}^T \oplus \bigoplus \{\mathfrak{g}_\beta \mid \beta \in \Phi\}.$$

Let α be a nonzero character of T, and let $T_\alpha = \mathrm{Ker}(\alpha)_t$. Then T_α is the subtorus of T such that $X(T_\alpha) = (X(T)/\mathbb{Z}\alpha)/\mathrm{torsion}$. Let $G_\alpha = G_\alpha^{T_\alpha}$. Then G_α is a connected group variety (17.38), with Lie algebra

$$\mathrm{Lie}(G_\alpha) \overset{10.34}{=} \mathfrak{g}^{T_\alpha} = \mathfrak{g}^T \oplus \bigoplus \{\mathfrak{g}_\beta \mid \beta \in \mathbb{Q}\alpha \cap \Phi\}. \tag{123}$$

Let (α) denote the set of the strictly positive rational multiples of α in $X(T)$. Then (α) is a cyclic subsemigroup of $X(T)$. Let λ be a cocharacter of T such that $\langle \alpha, \lambda \rangle > 0$, and let

$$U_{(\alpha)} = U_{G_\alpha}(\lambda).$$

Thus $U_{(\alpha)}$ is the unique subgroup variety of G such that

$$U_{(\alpha)}(k^a) = \{g \in G(k^a) \mid g \text{ centralizes } T_\alpha(k^a) \text{ and } \lim_{t \to 0} \lambda(t)g = e\} \tag{124}$$

(see 13.30). Clearly, T_α, G_α, and $U_{(\alpha)}$ depend only on the semigroup (α).

PROPOSITION 16.64. *The subgroup variety $U_{(\alpha)}$ of G is stable under T and has Lie algebra*

$$\mathrm{Lie}(U_{(\alpha)}) = \bigoplus \{\mathfrak{g}_\beta \mid \beta \in (\alpha) \cap \Phi(G, T)\}. \tag{125}$$

  (a) *Every T-stable subgroup variety of G whose Lie algebra contains the Lie algebra of $U_{(\alpha)}$ contains $U_{(\alpha)}$.*

  (b) *Every T-stable subgroup variety of G whose Lie algebra is contained in the Lie algebra of $U_{(\alpha)}$ is contained in $U_{(\alpha)}$.*

PROOF. That $U_{(\alpha)}$ is stable under T follows from the description (124). To determine its Lie algebra, apply Theorem 13.33(c) to (123).

  (a) Let H be a T-stable subgroup variety of G such that $\mathrm{Lie}(H) \supset \mathrm{Lie}(U_{(\alpha)})$. Let $H_\alpha = (HT)^{T_\alpha}$, and let $U = U_{H_\alpha}(\lambda_\alpha)$. Then U is the subgroup variety of HT such that

$$U(k^s) = \{h \in (HT)(k^s) \mid h \text{ centralizes } T_\alpha(k^s) \text{ and } \lim_{t \to 0} \lambda_\alpha(t)h = e\}$$

$$\mathrm{Lie}(U) = \bigoplus \{\mathfrak{g}_\beta \mid \beta \in (\alpha) \cap \Phi(H, T)\} = \mathrm{Lie}(U_{(\alpha)}).$$

Hence $U(k^s) \subset U_{(\alpha)}(k^s)$, and so $U \subset U_{(\alpha)}$. As they have the same dimension, they are equal. Thus $U_{(\alpha)} = U \subset H$. Finally, G is generated by $C_G(T)$ and the $U_{(\alpha)}$ because its Lie algebra is generated by their Lie algebras.

  (b) Let H be a T-stable subgroup variety of G such that $\mathrm{Lie}(H) \subset \mathrm{Lie}(U_{(\alpha)})$. Then the algebraic subgroup H' generated by H and $U_{(\alpha)}$ has Lie algebra $\mathrm{Lie}(U_{(\alpha)})$. As H' is smooth, it equals $U_{(\alpha)}$ (see 10.15). Therefore $H \subset U_{(\alpha)}$. $\square$

Thus $U_{(\alpha)}$ is the unique connected T-stable subgroup variety of G satisfying (125).

Let G be a connected group variety with an action of a split torus T, and let $\Psi = \Psi(G,T)$ denote the set of weights of T on $\mathfrak{g}$, so $\mathfrak{g} = \bigoplus\{\mathfrak{g}_\alpha \mid \alpha \in \Psi\}$.

THEOREM 16.65. *Let G be a connected group variety with an action of a split torus T, and let A be a subsemigroup of $X(T)$. There is a unique connected T-stable subgroup variety H_A of G such that*

$$\mathrm{Lie}(H_A) = \bigoplus\{\mathfrak{g}_\alpha \mid \alpha \in A \cap \Psi(G,T)\}.$$

A T-stable subgroup variety H of G is contained in H_A if and only if $\Psi(H,T)$ is contained in A.

We first need a lemma. For a subset A of $X(T)$, we let $\langle A \rangle$ denote the subsemigroup generated by A. For example, if A is empty, then $\langle A \rangle$ is the empty semigroup.

LEMMA 16.66. *Let G be a connected group variety with an action of a split torus T. Let H_1 and H_2 be connected subgroup varieties of G stable under T, and let H be the algebraic subgroup of G generated by H_1 and H_2. Then H is smooth and connected and $\langle \Psi(H,T) \rangle$ is the semigroup generated by $\Psi(H_1,T)$ and $\Psi(H_2,T)$.*

PROOF. That H is smooth and connected follows from Propositions 2.51 and 2.53).

Obviously $\Psi(H,T)$ contains $\Psi(H_1,T)$ and $\Psi(H_2,T)$, and so $\langle \Psi(H,T) \rangle$ contains the semigroup generated by $\Psi(H_1,T)$ and $\Psi(H_2,T)\rangle$.

We let T act on $\mathcal{O}(H)$ by $(tf)(h) = f(th)$. If $I_H \subset \mathcal{O}(H)$ is the augmentation ideal of H, then $\mathrm{Lie}(H) = \mathrm{Hom}(I_H/I_H^2, k)$ and so $\Psi(H,T)$ is the set of weights of T acting on I_H/I_H^2. It follows that $\langle \Psi(H,T) \rangle$ is the set of weights of T acting on I_H.

Let $H_1 \cdot H_2$ be the closure of the image of the multiplication map $H_1 \times H_2 \to G$. From the dominant map $H_1 \times H_2 \to H$ we get an inclusion $\mathcal{O}(H) \hookrightarrow \mathcal{O}(H_1) \otimes \mathcal{O}(H_2)$, and hence a T-equivariant embedding

$$I_{H_1 \cdot H_2} \hookrightarrow I_{H_1} \oplus I_{H_2} \oplus (I_{H_1} \otimes I_{H_2}).$$

Therefore the weights of T on $I_{H_1 \cdot H_2}$ are contained in $\langle \Psi(H_1,T) \cup \Psi(H_2,T) \rangle$. On repeating this with H_1^n and H_2^n for H_1 and H_2, we find that the weights of T on $I_{H_1^n \cdot H_2^n}$ are contained in $\langle \Psi(H_1,T) \cup \Psi(H_2,T) \rangle$. For large enough n, $H = H_1^n \cdot H_2^n$ (see 2.46) and so $\langle \Psi(H,T) \rangle \subset \langle \Psi(H_1,T) \cup \Psi(H_2,T) \rangle$ (see Conrad et al. 2015, 3.3.5). $\qquad\square$

We now prove Theorem 16.65. When A is empty, we let $H_A = e$. When $A = (\alpha)$, we let $H_A = U_{(\alpha)}$ (see 16.64). In the general case, we let H_A be the algebraic subgroup generated by the $U_{(\alpha)}$ as α runs over a set of generators for

$A \cap \Psi(G,T)$. This is smooth and connected (2.51, 2.53), obviously T-stable, and (16.66) shows that its Lie algebra is as described.

Let H be a T-stable connected subgroup variety of G. If $\Psi(H,T) \subset A$, then the subgroup variety H' generated by H and H_A is a T-stable connected subgroup variety with $\Psi(H',T) \subset A$. Now $H_A \subset H'$ and $\mathrm{Lie}(H_A) = \mathrm{Lie}(H')$, and so $H_A = H'$. This shows that $H \subset H_A$. Conversely, if $H \subset H_A$, then obviously $\Psi(H,T) \subset A$.

The uniqueness of H_A follows from the second statement.

REMARK 16.67. If $0 \notin A$, then H_A is a split unipotent group, $H_A^T = e$, and every Luna map $G \to \mathrm{Tgt}_e(H_A)_{\mathfrak{a}}$ is a T-equivariant isomorphism of algebraic varieties (16.63). We often denote it by U_A in this case.

The decomposition of a solvable group variety under the action of a torus

THEOREM 16.68. *Let G be a connected solvable group variety over k equipped with an action of a split torus T, and let $A_1,\dots,A_n$ be subsemigroups of $X(T)$. If Ψ is the disjoint union of the sets $A_i \cap \Psi$, then the multiplication map*

$$H_{A_1} \times \cdots \times H_{A_n} \to G$$

is an isomorphism of algebraic varieties.

PROOF. We may suppose that k is algebraically closed. Suppose first that all the A_i are definite. In this case, we get a commutative diagram

$$
\begin{array}{ccc}
H_{A_1} \times \cdots \times H_{A_n} & \xrightarrow{\quad m \quad} & G \\
\downarrow & & \downarrow \\
\mathrm{Tgt}_e(H_{A_1})_{\mathfrak{a}} \times \cdots \times \mathrm{Tgt}_e(H_{A_n})_{\mathfrak{a}} & \xrightarrow{\mathrm{Tgt}_e(m)} & \mathrm{Tgt}_e(G)_{\mathfrak{a}}
\end{array}
$$

in which the vertical maps are isomorphisms – the first is a product of Luna maps and the second is a Luna map. As $\mathrm{Tgt}_e(m)$ is an isomorphism of algebraic varieties, so also is m.

If 0 lies in some A_i, then it lies in exactly one, say A_n. By replacing G with $G \rtimes T$, we may suppose that $T \subset G$ and then that $G = G_u \rtimes T$. For $i \neq n$, the group $H_{A_i}(G)$ is unipotent and $H_{A_i}(G) = H_{A_i}(G_u)$. Clearly, $T \subset H_{A_n}(G)$ and so inside $G = G_u \rtimes T$ we have

$$H_{A_n}(G) = (G_u \cap H_{A_n}(G)) \rtimes T = H_{A_n}(G_u) \rtimes T.$$

Now

$$G \simeq G_u \rtimes T \simeq H_{A_1}(G_u) \times \cdots \times H_{A_n}(G_u) \rtimes T$$
$$\simeq H_{A_1}(G) \times \cdots \times H_{A_n}(G). \qquad \square$$

NOTES. Theorem 16.68 is Theorem 3.3.11 of Conrad et al. 2015. It generalizes earlier statements of Borel, Chevalley, and Tits.

Exercises

EXERCISE 16-1. (Waterhouse 1979, Chapter 10, Exercise 3). Verify the statements in Example 16.37.

EXERCISE 16-2. (Waterhouse 1979, Chapter 9, Exercise 5). Show that an algebraic group G is trigonalizable if and only if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \cdots$ of $\mathcal{O}(G)$ by subspaces C_i such that

$$\begin{cases} C_0 \text{ is spanned by group-like elements,} \\ \bigcup_{r \geq 0} C_r = \mathcal{O}(G), \\ \Delta C_r \subset \sum_{0 \leq i \leq r} C_i \otimes C_{r-i}. \end{cases}$$

EXERCISE 16-3. Let G be an algebraic group over a field k, and let k' be a finite field extension of k. Show that $(G_{k'})_{k'/k}$ is solvable if G is solvable. [By Corollary 6.31 we may suppose that k is algebraically closed. Now use Exercise 2-10.]

EXERCISE 16-4. Show that a connected solvable group variety G over an algebraically closed field k is nilpotent if and only if one (hence every) maximal torus in G is contained in $Z(G)$.

EXERCISE 16-5. (Conrad et al. 2015, 3.3, p. 107). Let $G = \mathbb{G}_a \times \mathbb{G}_a$ over a field of k of characteristic $p \neq 0$, and let $T = \mathbb{G}_m \times \mathbb{G}_m$ act on G by the rule $(t_1, t_2)(x_1, x_2) = (t_1 x_1, t_2 x_2)$. Let H be the subgroup $\mathbb{G}_a \times e$ of G and H' the graph of the relative Frobenius map $F_{\mathbb{G}_a/k}$, so $H'(k) = \{(x, x^p)\}$.

  (a) Show that H is T-stable and $\mathrm{Lie}(H) = \mathrm{Lie}(H')$, but that H' is not T-stable.

  (b) Show that H and H' generate G, but their Lie algebras do not generate $\mathrm{Lie}(G)$.

Borel Subgroups and Applications

In this chapter, we introduce Borel subgroups. Recall that, when k is algebraically closed, we can identify the underlying topological space $|G|$ of an algebraic group G with $G(k)$. Recall also that all algebraic groups are affine over a base field k.

a. The Borel fixed point theorem

Let H be an algebraic subgroup of an algebraic group G. If G is commutative, then H is normal, and so G/H is affine (5.18). When G is solvable, we have only the following weaker result.

THEOREM 17.1. *Let H be an algebraic subgroup of a smooth connected algebraic group G over k. If G is solvable, then G/H does not contain a complete subscheme of dimension > 0. In particular, $H = G$ if G/H is complete.*

PROOF. We may suppose that k is algebraically closed, and then that H is smooth because the map $G/H_{\text{red}} \to G/H$ is finite (7.15). We prove the statement by induction on the dimension of G. We may suppose that $\dim(G/H) > 0$.

The derived group G' of G is a smooth connected algebraic subgroup of G (see 6.19), which is distinct from G because G is solvable. If $G = G' \cdot H$, then $G/H \simeq G'/(G' \cap H)$ (see 5.52), and so the statement follows from the induction hypothesis applied to G'.

In the contrary case, $N \stackrel{\text{def}}{=} G' \cdot H$ is a proper normal algebraic subgroup of G, which is smooth and connected (6.41).

Let Z be a complete subscheme of G/H – we have to show that $\dim(Z) = 0$. We may suppose that Z is connected. Consider the quotient map $q: G/H \to G/N$. Because N is normal, G/N is affine, and so the image of Z in G/N is a point (A.75g). Therefore Z is contained in one of the fibres of the map q, but these are all isomorphic to N/H, and so we can conclude again from the induction hypothesis. $\qquad\square$

In the next two corollaries, G is a smooth connected algebraic group acting on a separated algebraic scheme X over k.

COROLLARY 17.2. *If G is solvable, then no orbit in X contains a complete subscheme of dimension > 0.*

PROOF. Let $x \in X(k)$, and let O_x be its orbit under G. Because G is reduced, the orbit map defines an isomorphism $G/G_x \to O_x$, and so the statement follows from the theorem. □

COROLLARY 17.3 (BOREL FIXED POINT THEOREM). *If G is solvable and X is complete and nonempty, then X^G is nonempty; hence there is a fixed point in $X(k^a)$.*

PROOF. The formation of X^G commutes with extension of the base field, and so we may suppose that k is algebraically closed and that X is reduced. Every orbit of minimum dimension is closed (1.66), hence complete (A.75a), and hence consists of a single fixed point (17.2). □

The Borel fixed point theorem gives an alternative proof of the Lie–Kolchin theorem.

THEOREM 17.4. *Let G be a smooth connected solvable algebraic group over k. If k is algebraically closed, then G is trigonalizable.*

PROOF. Let (V, r) be a faithful finite-dimensional representation of G, and let X denote the collection of maximal flags in V. This has a natural structure of a projective variety on which G acts (7.29). According to Corollary 17.3, there is a fixed point in $X(k^a)$. This is a maximal flag in V stabilized by G. Hence the representation (V, r) is trigonalizable, which implies that G is trigonalizable (16.2). □

REMARK 17.5. Readers tempted to drop the smoothness condition on G in the above statements should note that it is possible for a connected solvable algebraic group to act on $\mathbb{P}^1$ without fixed points (16.37).

NOTES. Borel's original theorem (Borel 1956, 15.5, 16.4) is Corollary 17.3. The generalization to noncomplete X (see 17.1, 17.2) is from Allcock 2009.

b. Borel subgroups and maximal tori

In this section, G is a connected group variety over an algebraically closed field k.

DEFINITION 17.6. A ***Borel subgroup*** of G is a maximal connected solvable subgroup variety of G.

For example, every connected solvable subgroup variety of largest possible dimension is a Borel subgroup.

EXAMPLE 17.7. Let V be a finite-dimensional vector space over k, and let B be a Borel subgroup in GL_V. Because B is solvable, there exists a basis of V for which $B \subset \mathbb{T}_n$ (see 16.30), and because B is maximal, $B = \mathbb{T}_n$. Thus, we see that the Borel subgroups of GL_V are exactly the subgroup varieties B such that $B = \mathbb{T}_n$ relative to some basis of V. More canonically, the Borel subgroups of GL_V are exactly the stabilizers of maximal flags in V. Because $\mathrm{GL}_V(k)$ acts transitively on the set of bases for V, any two Borel subgroups of GL_V are conjugate by an element of $\mathrm{GL}_V(k)$.

EXAMPLE 17.8. Suppose that $\mathrm{char}(k) \neq 2$, and let ϕ be a bilinear form on a vector space V over k. A subspace of V is ***totally isotropic*** if the restriction of ϕ to it is zero, and a flag in V is ***totally isotropic*** if each of its subspaces is totally isotropic. The Borel subgroups in each of the algebraic groups SO_{2n+1}, Sp_{2n}, SO_{2n} (see 2.10) are the stabilizers of the maximal totally isotropic flags in V (and each such flag has length n). See Exercise 17-1.

THEOREM 17.9.   (a) *If B is a Borel subgroup of G, then G/B is complete.*

  (b) *Any two Borel subgroups of G are conjugate by an element of $G(k)$.*

PROOF. We first prove that G/B is complete when B is a Borel subgroup of maximum dimension. According to Chevalley's theorem (4.27), there exists a representation (V, r) of G such that B is the stabilizer of a one-dimensional subspace L in V. Now the Lie–Kolchin theorem 16.30 shows that B stabilizes some maximal flag in V/L, which we pull back to a maximal flag,

$$F_0: \quad V = V_n \supset V_{n-1} \supset \cdots \supset V_1 = L \supset 0,$$

in V. Not only does B stabilize F_0, but, because of our choice of V_1, it equals its stabilizer.

  In general, the stabilizer in G of a maximal flag F in V is a solvable subgroup G_F of G, and the orbit of F in the space of maximal flags has dimension $\dim G - \dim G_F$. As B has the maximum possible dimension, the orbit $G \cdot F_0$ has minimum possible dimension, and so it is a closed (1.66) subvariety of the variety of maximal flags in V. As flag varieties are complete (7.30), this shows that $G \cdot F_0$ is complete, and as G/B is isomorphic to $G \cdot F_0$, it also is complete.

  To complete the proof of the theorem, it remains to show that for any Borel subgroups B and B' with B of maximum dimension, $B' \subset gBg^{-1}$ for some $g \in G(k)$ (the maximality of B' will then imply that $B' = gBg^{-1}$). Let B' act on G/B by left multiplication $(b', gB) \mapsto b'gB$. According to (17.3), there is a fixed point, i.e., for some $g \in G(k)$, $B'gB \subset gB$. Then $B'g \subset gB$, and so $B' \subset gBg^{-1}$ as required.   □

THEOREM 17.10. *Any two maximal tori in G are conjugate by an element of $G(k)$.*

PROOF. When G is solvable, this was proved in Theorem 16.33(d). Let T and T' be maximal tori in G. Being smooth, connected, and solvable, they are contained in Borel subgroups, say, $T \subset B$ and $T' \subset B'$. For some $g \in G(k)$, $gB'g^{-1} = B$ (see 17.9), and so $gT'g^{-1} \subset B$. Now T and $gT'g^{-1}$ are maximal tori in B, and so $T = bgT'g^{-1}b^{-1}$ for some $b \in B(k)$. □

COROLLARY 17.11. *Let T be a maximal torus in G, and let H be a subgroup variety of G containing T. Then $N_G(T)(k)$ acts transitively on the set of conjugates of H containing T, and the number of such conjugates is*

$$\frac{(N_G(T)(k):N_G(T)(k) \cap H(k))}{(N_G(H)(k):H(k))}.$$

In particular, $N_G(T)$ acts transitively on the set of Borel subgroups of G containing T.

PROOF. Let gHg^{-1}, $g \in G(k)$, be a conjugate of H containing T. Then gTg^{-1} and T are maximal tori in gHg^{-1}, and so there exists an $h \in gH(k)g^{-1}$ such that $hgTg^{-1}h^{-1} = T$ (see 17.10). Now $hg \in N_G(T)(k)$ and $gHg^{-1} = hgHg^{-1}h^{-1}$, and so this shows that $N_G(T)(k)$ acts transitively on the set of conjugates of H containing T.

We now write $N(*)$ for $N_G(*)(k)$. The number of conjugates of H containing T is

$$(N(T):(N(T) \cap N(H))) = \frac{(N(T):(N(T) \cap H(k)))}{(N(T) \cap N(H):N(T) \cap H(k))}.$$

Let $g \in N(H)$; then T and gTg^{-1} are maximal tori in H, and so there exists an $h \in H(k)$ such that $hgTg^{-1}h^{-1} = T$ (see 17.10), i.e., such that $hg \in N(T)$. As $hg \in N(H)$, this shows that $N(H) = H(k) \cdot (N(T) \cap N(H))$, and so the canonical injection

$$\frac{N(T) \cap N(H)}{N(T) \cap H(k)} \to \frac{N(H)}{H(k)}$$

is a bijection. Therefore

$$(N(T) \cap N(H):N(T) \cap H(k)) = (N(H):H(k)),$$

which completes the proof of the formula. □

DEFINITION 17.12. A pair (B,T) with T a maximal torus of G and B a Borel subgroup of G containing T is called a **Borel pair**.[1]

Every maximal torus T of G, being connected and solvable, is contained in a Borel subgroup B and so is part of a Borel pair. As one Borel subgroup is part of a Borel pair, and any two Borel subgroups are conjugate, every Borel subgroup is part of a Borel pair.

---

[1]In SGA 3, XXII, 5.3.13, such a pair is called a Killing pair (*couple de Killing*).

PROPOSITION 17.13. *Any two Borel pairs of G are conjugate by an element of $G(k)$.*

PROOF. Let (B, T) and (B', T') be Borel pairs in G. Then $gB'g^{-1} = B$ for some $g \in G(k)$ and $bgT'g^{-1}b^{-1} = T$ for some $b \in B(k)$, and so

$$bg \cdot (B', T') \cdot (bg)^{-1} = (B, T).$$
$\square$

Recall (16.33) that a connected solvable group variety H over a perfect field contains a unique normal unipotent algebraic subgroup such that H/H_u is of multiplicative type. Moreover, H_u is smooth and connected, and it is the largest unipotent algebraic subgroup of H.

PROPOSITION 17.14. *The maximal connected unipotent subgroup varieties of G are those of the form B_u with B a Borel subgroup of G. Any two are conjugate by an element of $G(k)$.*

PROOF. Let U be a maximal connected unipotent subgroup variety of G. It is solvable (14.21), and so it is contained in a Borel subgroup B. By maximality, it equals B_u. Let $U' = B'_u$ be a second such subgroup. Then $B' = gBg^{-1}$ for some $g \in G(k)$, and so $B'_u = (gBg^{-1})_u = gB_ug^{-1}$. $\square$

DEFINITION 17.15. Let G be a connected group variety over a field k (not necessarily algebraically closed). A subgroup variety P of G is **parabolic** if G/P is complete.

THEOREM 17.16. *A subgroup variety P of G is parabolic if and only if it contains a Borel subgroup.*

PROOF. If P contains the Borel subgroup B, then the quotient map $G \to G/P$ factors through G/B (see 5.22). Now G/P is complete because G/B is complete and $G/B \to G/P$ is surjective (A.75d).

Conversely, suppose that G/P is complete, and let B be a Borel subgroup of G. According to 17.3, B fixes a point xP in G/P. In other words, $BxP = xP$, which implies that P contains the Borel subgroup $x^{-1}Bx$ of G. $\square$

COROLLARY 17.17. *A connected group variety contains a proper parabolic subgroup if and only if it is not solvable.*

PROOF. Let H be a connected group variety. If H is solvable, the only Borel subgroup of H is H itself, and so H contains no proper parabolic subgroup. If is not solvable, then the Borel subgroups of H are proper parabolic subgroups. $\square$

EXAMPLE 17.18. Borel subgroups are parabolic (17.9). Let V be a finite-dimensional k-vector space, and let F be a flag in V, not necessarily maximal.

The stabilizer P_F of F in GL_V is a parabolic subgroup of GL_V because it contains the Borel subgroup stabilizing a maximal flag containing F. For example,

$$P = \left\{ \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix} \right\}$$

is a parabolic subgroup of GL_4.

PROPOSITION 17.19. *Let H be a connected subgroup variety of G. The following conditions on H are equivalent:*

(a) *H is a Borel subgroup;*

(b) *H is solvable and G/H is complete;*

(c) *H is minimal parabolic.*

PROOF. (a)$\Rightarrow$(b). A Borel subgroup H is solvable by definition and G/H is complete by Theorem 17.9.

(b)$\Rightarrow$(c). If H satisfies (b), then certainly it is parabolic. Let $P \subset H$ be a parabolic subgroup P of G. Then H contains a Borel subgroup B of G (see 17.16) which, being maximal connected solvable, must equal H. Hence $P = H$, and so H is minimal.

(c)$\Rightarrow$(a). Suppose that H is minimal parabolic. Then H contains a Borel subgroup B (see 17.16), which being parabolic, must equal H. □

PROPOSITION 17.20. *Let $q: G \to Q$ be a quotient map of connected group varieties, and let H be a subgroup variety of G. If H is parabolic (resp. Borel, resp. a maximal unipotent subgroup variety, resp. a maximal torus), then so also is $q(H)$; moreover, every such subgroup of Q arises in this way.*

PROOF. From the universal property of quotients, the map $G \to Q/q(H)$ factors through G/H, and so we get a surjective map $G/H \to Q/q(H)$.

If H is parabolic, then G/H is complete. As $G/H \to Q/q(H)$ is surjective, this implies that $Q/q(H)$ is complete (A.75d), and so $q(H)$ is parabolic.

If H is a Borel subgroup, then $q(H)$ is connected (5.59) and solvable (6.27), and $Q/q(H)$ is complete, and so H is a Borel subgroup (17.19).

If H is a maximal unipotent subgroup variety, then $H = B_u$ for some Borel subgroup B (see 17.14). Now $q(B_u)$ is a normal subgroup of the Borel subgroup $q(B)$ in Q. It is unipotent and $q(B)/q(B_u)$ is of multiplicative type (because quotients of unipotent and multiplicative groups have the same property), and so $q(B_u) = q(B)_u$, which is a maximal unipotent subgroup variety of G (see 17.14).

If H is a maximal torus, then H is contained in a Borel subgroup B and $B = B_u \cdot H$ (see 16.33). Now

$$q(B) = q(B_u) \cdot q(H) = q(B)_u \cdot q(H),$$

which implies that $q(H)$ is a maximal torus in the Borel subgroup $q(B)$, and hence in Q.

Let B' be a Borel subgroup of Q, and let B be a Borel subgroup of G. Then $q(B)$ is a Borel subgroup of Q, and so there exists a $g \in G(k)$ such that

$$B' = q(g)q(B)q(g)^{-1} = q(gBg^{-1})$$

by Theorem 17.9. This exhibits B' as the image of a Borel subgroup of G. The same argument applies to maximal unipotent subgroup varieties and maximal tori of Q.

Let H' be a parabolic subgroup of Q. Then H' contains a Borel subgroup B', which we can write $B' = q(B)$ with B a Borel subgroup of G. Now $H \overset{\text{def}}{=} q^{-1}(H')_{\text{red}}$ contains B, and so it is parabolic, but $q(H) = H'$. ☐

PROPOSITION 17.21. *Let G and G' be connected group varieties over k, let R be a k-algebra, and let $\varphi_1, \varphi_2 : G_R \to G'_R$ be homomorphisms. If φ_1 and φ_2 agree on B_R for some Borel subgroup B of G, then they agree on G_R.*

PROOF. We prove this first in the case $R = k$. The regular map $\delta : G \to G'$ sending x to $\varphi_1(x) \cdot \varphi_2(x)^{-1}$ is constant on the cosets of B, and so it factors through a regular map $\delta^B : G/B \to G$ (see 5.21). As G/B is complete and G' is affine, δ^B is constant (A.75g), with value e. This shows that φ_1 and φ_2 agree on G.

In proving the general case, we use that, for an algebraic scheme X over k and a k-algebra R,

$$\mathcal{O}_{X_R}(X_R) \simeq R \otimes \mathcal{O}_X(X).$$

When X is affine, this is obvious, and the general case can be proved by covering X with open affine subschemes and applying the sheaf condition.

Let $\delta : G_R \to G'_R$ be the morphism such that $\delta(R') : G(R') \to G'(R')$ sends x to $\varphi_1(x) \cdot \varphi_2(x)^{-1}$ for every R-algebra R'. Then $\delta(R')$ is constant on each coset of $B_R(R')$, and so we have a map of functors $\tilde{G}_R/\tilde{B}_R \to \tilde{G}'_R$. As $\tilde{G}/\tilde{B}$ is fat in $\tilde{G}/\tilde{B} = \widetilde{G/B}$, this extends to a regular map

$$(G/B)_R \simeq G_R/B_R \overset{\delta^B}{\longrightarrow} G'_R.$$

Let $X = G/B$. As G' is affine, we can embed it in $\mathbb{A}^n$ for some n. The composite of the maps

$$X_R \overset{\delta^B}{\longrightarrow} G'_R \longrightarrow \mathbb{A}^n_R \overset{p_i}{\longrightarrow} \mathbb{A}_R \qquad (p_i \text{ is the } i\text{th projection})$$

is an element of $\mathcal{O}_{X_R}(X_R) \simeq R \otimes \mathcal{O}_X(X)$. Because X is complete, $\mathcal{O}_X(X) = k$, and so the composite map is constant. Hence δ^B is constant, with value e. This shows that φ_1 and φ_2 agree on $G(R')$ for all R-algebras R', and hence on G_R (Yoneda lemma A.33). ☐

In particular, an automorphism of G_R is the identity map if it agrees with the identity map on B_R for some Borel subgroup B of G.

PROPOSITION 17.22. *Let B be a Borel subgroup of G. Then*

$$Z(B) \subset C_G(B) = Z(G).$$

PROOF. The inclusions $Z(B) \subset C_G(B)$ and $Z(G) \subset C_G(B)$ are obvious. Let $g \in C_G(B)(R)$ for some k-algebra R. Then $\mathrm{inn}(g)$ acts as the identity map on B_R, and so it is the identity map on G_R (17.21). Thus $C_G(B)(R) \subset Z(G)(R)$. As this is true for all k-algebras R, $C_G(B) \subset Z(G)$. □

PROPOSITION 17.23. *The following conditions on G are equivalent:*

  (a) *G has only one maximal torus;*
  (b) *some Borel subgroup of G is nilpotent;*
  (c) *G is nilpotent;*
  (d) *every maximal torus T of G is contained in the centre of G.*

PROOF. (a)$\Rightarrow$(b). Let (B, T) be a Borel pair in G. Then T is normal in B, because otherwise $gTg^{-1} \neq T$ for some $g \in B(k)$ (see 1.85) and G would contain a second maximal torus. Because T is maximal, the quotient B/T contains no copy of $\mathbb{G}_m$ (see 15.39), and so it is unipotent (16.60). Now $B \simeq T \times U$ with U unipotent (16.28), and both T and U are nilpotent (14.21).

(b)$\Rightarrow$(c). We use induction on the dimension of a nilpotent Borel subgroup B to show that $G = B$. If $\dim(B) = 0$, then $G = G/B$ is both affine and complete, hence trivial (A.75g). Thus, we may suppose that $\dim(B) > 0$, and hence that $\dim(Z(B)) > 0$ (see 6.40). But $Z(B) \subset Z(G)$ (see 17.22), and so $Z(B)$ is normal in G. The quotient $B/Z(B)$ is a Borel subgroup of $G/Z(B)$ (17.20). By the induction hypothesis, $G/Z(B) = B/Z(B)$, and so $G = B$.

(c)$\Rightarrow$(d). The centre of a connected nilpotent group variety contains *every* algebraic subgroup of multiplicative type (16.47a).

(d)$\Rightarrow$(a). Any two would be conjugate by an element of $G(k)$ (17.10). □

EXAMPLE 17.24. In particular, a connected solvable group variety is nilpotent if and only it has exactly one maximal torus. For $n > 1$, the group $\mathbb{T}_n$ is solvable but not nilpotent because the maximal torus of diagonal matrices is not normal:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b-a \\ 0 & b \end{pmatrix}.$$

COROLLARY 17.25. *If G contains no nontrivial connected unipotent subgroup variety, then it is a torus. This is true, for example, if all elements of $G(k)$ are semisimple.*

PROOF. Let (B, T) be a Borel pair in G. Then $B = B_u \cdot T$ (see 16.33), and the hypothesis implies that $B_u = e$. Hence B is nilpotent, and so $G = B = T$. □

COROLLARY 17.26. *(a) A maximal torus of G is contained in only finitely many Borel subgroups.*

(b) For a Borel subgroup B of G, $B = N_G(B)^\circ_{\mathrm{red}}$.

PROOF. (a) Let T be a maximal torus in G, and let B be a Borel subgroup containing T. The Borel subgroups containing T are conjugates of B, and so (17.11) shows that $N_G(T)(k)$ acts transitively on the Borel subgroups containing T. As $N_G(T)^\circ$ is smooth (13.10) and contains the maximal torus T in its centre (12.38), it is nilpotent (17.23), and so it lies in some Borel subgroup B' containing T. As $B = gB'g^{-1}$ with $g \in N_G(T)(k)$, we see that $N_G(T)^\circ$ lies in B, and so the number of Borel subgroups containing T is at most

$$(N_G(T)(k):N_G(T)(k) \cap B(k)) \le (N_G(T)(k):N_G(T)^\circ(k)) < \infty.$$

(b) Let B be a Borel subgroup of G, and let T be a maximal torus of G contained in B. According to (17.11), $(N_G(B)(k):B(k))$ divides

$$(N_G(T)(k):N_G(T)(k) \cap B(k)),$$

which is finite. This implies that $N_G(B)^\circ_{\mathrm{red}} = B$.   □

COROLLARY 17.27. *If $\dim G \le 2$, then G is solvable.*

PROOF. Let B be a Borel subgroup of G – we have to show that $G = B$. If $\dim B = 0$, then B is nilpotent, and so $G = B = e$ (see 17.23). If $\dim B = 1$, then, in the decomposition $B = B_u \cdot T$ (see 16.33), either $B = B_u$ or $B = T$. In each case, B is nilpotent, and so $G = B$ (see 17.23). Finally, if $\dim B = 2$, then certainly $G = B$.   □

Note that SL_3 has dimension 3 and is not solvable.

PROPOSITION 17.28. *Let T be a maximal torus of G. Then $C_G(T)^\circ$ is smooth, nilpotent, and equals $N_G(C)^\circ$.*

PROOF. Let $C = C_G(T)^\circ$. Then C is smooth (13.10), and, as C contains T in its centre, it is nilpotent (17.23). Therefore C has a unique decomposition $C = U \times T$ with U unipotent (16.47), which is preserved by every automorphism of C. In particular, the action of $N_G(C)^\circ$ on C by inner automorphisms preserves T. By rigidity (12.37), $N_G(C)^\circ$ acts trivially on T, and so it centralizes T. Therefore $C \subset N_G(C)^\circ \subset C_G(T)^\circ = C$.   □

COROLLARY 17.29. *Let T be a maximal torus of G. Then $C_G(T)^\circ$ is contained in every Borel subgroup of G containing T.*

PROOF. Let B be a Borel subgroup containing T. As $C_G(T)^\circ$ is connected and nilpotent, it is contained in some Borel subgroup B' of G. According to (17.11), $B = gB'g^{-1}$ for some $g \in N_G(T)(k)$, and so

$$C_G(T)^\circ = C_G(gTg^{-1})^\circ = g(C_G(T)^\circ)g^{-1} \subset gB'g^{-1} = B.$$ □

REMARK 17.30. In the above, G was assumed to be connected. For a noncon-nected group variety G, the definition of Borel and parabolic subgroups is the same. In particular, Borel subgroups are connected, and so the Borel subgroups of G are just the Borel subgroups of G°. A subgroup variety P of G is parabolic in G if and only if P° is parabolic in G° (i.e., G/P is complete if and only if G°/P° is complete). Parabolic subgroups of connected group varieties are automatically connected (17.49 below).

REMARK 17.31. Let I denote the reduced identity component of the intersec-tion of the Borel subgroups of G. Thus I is a connected subgroup variety of G. It is solvable because it is contained in a solvable group, and it is normal because the collection of Borel subgroups is closed under conjugation. Every connected solvable subgroup variety is contained in a Borel subgroup, and, if it is normal, then it is contained in all Borel subgroups (17.9), and so it is contained in I. Therefore I is the largest connected solvable normal subgroup variety of G, i.e.,

$$R(G) = \left(\bigcap_{B \subset G \text{ Borel}} B \right)^\circ_{\text{red}}.$$

This is sometimes adopted as the definition of $R(G)$ (e.g., in Chevalley 1956–58, 9.4).

c. The density theorem

In this section, G is a connected group variety over k algebraically closed.

LEMMA 17.32. *Let H be a connected subgroup variety of G.*

(a) *If G/H is complete, then $\bigcup_{g \in G(k)} g|H|g^{-1}$ is a closed subset of $|G|$.*

(b) *If there exists an element of $H(k)$ fixing only finitely many elements of $(G/H)(k)$, then $\bigcup_{g \in G(k)} g|H|g^{-1}$ contains a nonempty open subset of $|G|$.*

PROOF. Consider the composite of the maps

$$
\begin{array}{ccccc}
G \times G & \xrightarrow{\tau} & G \times G & \xrightarrow{q \times \text{id}} & G/H \times G \\
(g, h) & \mapsto & (g, ghg^{-1}) & &
\end{array}
$$

where q is the quotient map. We claim that the image S of $G \times H$ in $G/H \times G$ is closed. As $q \times \text{id}$ is open (5.25), it suffices to show that $(q \times \text{id})^{-1}(S)$ is closed in $G \times G$. But this set coincides with $\tau(G \times H)$, which is closed because τ is an automorphism of $G \times G$ and H is closed in G (see 1.41).

(a) Now assume that G/H is complete. Then (by definition) the projection map $p_2: G/H \times G \to G$ is closed. In particular, the image of S under this map is closed, but this image is exactly $\bigcup_{g \in G(k)} gHg^{-1}$.

(b) Now suppose that there exists an $h_0 \in H(k)$ whose fixed points in $|G/H|$ are finite in number. The preimage of h_0 with respect $p_2: S \to G$ is the set of

pairs $(\bar{g}, ghg^{-1})$ with $\bar{g}$ fixed by h_0 and $ghg^{-1} = h_0$. This set is finite, which implies that the dimension of S is the same as the dimension of the closure of its image in G (see A.72). As S has dimension $\dim(G)$, it follows that the regular map $S \to G$ is dominant, and this implies the second statement (A.15).   □

For $G = \mathrm{GL}_n$, the next theorem says that the set of diagonalizable matrices in $\mathrm{GL}_n(k)$ contains an open subset that every matrix is trigonalizable.

THEOREM 17.33.   (a) *Let T be a maximal torus in G, and let $C = C_G(T)^\circ$. Then $\bigcup_{g \in G(k)} g \,|C| \, g^{-1}$ contains a nonempty open subset of $|G|$.*

(b) *Let B be a Borel subgroup of G. Then $|G| = \bigcup_{g \in G(k)} g \,|B| \, g^{-1}$.*

PROOF. (a) As C is smooth, connected, and nilpotent (17.28) and T is a maximal torus in C,
$$C = C_u \times T$$
(see 16.47). Let $t \in T(k)$ be as in (16.42). We shall show that t fixes only finitely many elements of G/C; then (17.32) will imply (a).

Let x be an element of $G(k)$ such that $txC = xC$. As $x^{-1}tx$ is a semisimple element of C, it lies in T. Hence, every element of T commutes with $x^{-1}tx$ or, equivalently, every element of xTx^{-1} commutes with t. By the choice of t, this implies that $xTx^{-1} \subset C$, whence $xTx^{-1} = T$. As conjugation by x on G stabilizes T, it also stabilizes C, and so $x \in N_G(C)$. From (17.28), we know that $N_G(C)^\circ = C$. Therefore the map $xC \mapsto xN_G(C)^\circ$ is an injection from the fixed point set of t in G/C to the finite set $N_G(C)/N_G(C)^\circ$.

(b) Let T be a maximal torus of G contained in B, and let $C = C_G(T)^\circ$. Then $C \subset B$ (see 17.29), and so $\bigcup_{g \in G(k)} gBg^{-1}$ contains a nonempty open subset of G. As G/B is complete, $\bigcup_{g \in G(k)} gBg^{-1}$ is closed in G (see 17.32), and so it equals G.   □

COROLLARY 17.34. *Every element of $G(k)$ is contained in a Borel subgroup of G. Every normal Borel subgroup of G equals G.*

PROOF. Let B be a Borel subgroup of G. Conjugates of B are Borel and the theorem says that $G(k) = \bigcup_{g \in G(k)} (gBg^{-1})(k)$. If B is normal, then $G(k) = B(k)$, which implies that $G = B$ because G is reduced.   □

As B is a normal Borel subgroup of $N_G(B)^\circ_{\mathrm{red}}$, we see again that $B = N_G(B)^\circ_{\mathrm{red}}$.

COROLLARY 17.35. *Let B be a Borel subgroup of G. Then B is the only Borel subgroup of G contained in $N_G(B)$.*

PROOF. Suppose $B' \subset N_G(B)$. Then $B' \subset N_G(B)^\circ_{\mathrm{red}} = B$, and so $B' = B$.   □

Later (17.48) we shall see that $B = N_G(B)$.

COROLLARY 17.36. *Every semisimple element s of $G(k)$ lies in a maximal torus.*

PROOF. Let B be a Borel subgroup of G containing s, and let T be a maximal torus of G in B. The Zariski closure S of the subgroup of $G(k)$ generated by s is diagonalizable (because every representation of S is diagonalizable). Therefore, s is contained in a conjugate of T (by 16.33d). □

d. Centralizers of tori

In this section, we prove that the centralizer of a torus in a connected group variety is connected (hence smooth and connected, 13.10). The base field k need not be algebraically closed. An algebraic subgroup of a connected group variety G over k is ***Borel*** if it becomes Borel over k^a. In this section we define a maximal torus in G to be a torus T such that T_{k^a} is maximal in G_{k^a}. Later (17.82) we shall see that this agrees with the obvious definition.

LEMMA 17.37. *Let T be a torus in a connected group variety G over an algebraically closed field k. Then*

$$C_G(T) \subset \bigcup\nolimits_{B \supset T} B$$

(finite union over the Borel subgroups of G containing T).

PROOF. Let $c \in C_G(T)(k)$. It suffices to show that c lies in a Borel subgroup containing T. Let B be a Borel subgroup of G. Then G acts on the scheme G/B, and we let $(G/B)^c$ denote the subscheme fixed by c. As c is contained in a Borel subgroup of G (see 17.33), the Borel fixed point theorem (17.3) shows that $(G/B)^c$ is nonempty. It is also closed, being the subset where the regular maps $gB \mapsto cgB$ and $gB \mapsto gB$ agree. As T commutes with c, it stabilizes $(G/B)^c$, and the Borel fixed point theorem shows that it has a fixed point in $(G/B)^c$. This means that there exists a $g \in G$ such that

$$cgB = gB \quad \text{(hence } cg \in gB\text{)}$$
$$TgB = gB \quad \text{(hence } Tg \subset gB\text{).}$$

Thus c lies in the Borel subgroup gBg^{-1}, which contains T. □

THEOREM 17.38. *Let T be a torus in a connected group variety G. Then $C_G(T)$ is connected.*

PROOF. We may suppose that k is algebraically closed. From the lemma, we deduce that

$$C_G(T) = \bigcup\nolimits_{T \subset B} C_B(T).$$

As each $C_B(T)$ is connected (16.41) and contains T, their union is connected. □

COROLLARY 17.39. *Let T be a maximal torus in a connected group variety G over k. Then*

(a) $C_G(T) = N_G(T)^\circ$;

(b) $C_G(T)$ *is contained in every Borel subgroup containing T;*

(c) $C_G(T) = C_G(T)_u \times T$ *if k is perfect.*

PROOF. In proving (a) and (b), we may suppose k to be algebraically closed. Then the statements follow from Corollaries 12.40 and 17.29. As $C_G(T)$ is nilpotent (17.28) and connected, (c) follows from Theorem 16.47(b). □

REMARK 17.40. (a) More generally, if T is a torus acting on a connected group variety G, then G^T is connected. This follows from Lemma 17.38 applied to $G \rtimes T$.

(b) Centralizers of tori in nonsmooth algebraic groups are also connected. This can be deduced from the smooth case (SHS, Exposé 13, §4, p. 358).

(c) Theorem 17.38 fails for subgroups of multiplicative type (see 17.51).

DEFINITION 17.41. Let T be a maximal torus in a connected group variety G. The ***Weyl group*** $W(G, T)$ of G with respect to T is the étale group scheme $\pi_0(N_G(T))$.

Thus
$$W(G, T) \overset{\text{def}}{=} N_G(T)/N_G(T)^\circ \overset{17.39}{=} N_G(T)/C_G(T).$$

By definition, $W(G, T)$ acts faithfully on T, and hence on $X^*(T)$ and $X_*(T)$.

EXAMPLE 17.42. Let $G = \mathrm{GL}_V$ and let T be a split maximal torus in G. Then V decomposes into a direct sum $V = \bigoplus_{i \in I} V_i$ of one-dimensional eigenspaces for the action of T, and T is the algebraic subgroup of G of automorphisms α of V preserving the decomposition including the ordering, i.e., such that $\alpha(V_i) \subset V_i$ for all i. Let $g \in G(k)$. The algebraic subgroup of G preserving the decomposition $V = \bigoplus_{i \in I} gV_i$ (including the ordering) is gTg^{-1}. Therefore g normalizes T if and only if it preserves the decomposition $V = \bigoplus_{i \in I} V_i$ except for the ordering, i.e., $g(V_i) = V_{\sigma(i)}$ for some permutation σ of I. When we choose a basis for V consisting of an element from each V_i, we find that $N_G(T)$ consists of the monomial matrices (see 2.41). Therefore $N_G(T) = C_G(T) \cdot (S_n)_k$, and so $W(G, T) \simeq (S_n)_k$ (finite constant algebraic group attached to the symmetric group on n symbols).

DEFINITION 17.43. A ***Cartan subgroup*** of a connected group variety is the centralizer of a maximal torus.

PROPOSITION 17.44. *Let G be a connected group variety over k. Every Cartan subgroup of G is smooth, connected, and nilpotent. If k is algebraically closed, then any two are conjugate by an element of $G(k)$, and the union of the Cartan subgroups of G contains a dense open subset of G.*

PROOF. We may suppose that k is algebraically closed. Let $C = C_G(T)$ be a Cartan subgroup of G. Then C is smooth (13.10), connected (17.38), and nilpotent (17.28). Let $C' = C_G(T')$ be a second Cartan subgroup of G. Then $T' = gTg^{-1}$ for some $g \in G(k)$ (see 17.10), and so

$$C' = C_G(gTg^{-1}) = g \cdot C_G(T) \cdot g^{-1} = g \cdot C \cdot g^{-1}.$$

Finally, every conjugate of C is a Cartan subgroup of G, and we showed in Theorem 17.33 that $\bigcup_{g \in G(k)} g|C|g^{-1}$ contains a nonempty open subset of G.□

PROPOSITION 17.45. *Let B be a Borel subgroup in a connected group variety G. Then $Z(G) = Z(B)$.*

PROOF. We may suppose that k is algebraically closed. As $Z(G) = C_G(B)$ (17.22) and $Z(B) = C_G(B) \cap B$, it suffices to show that $Z(G) \subset B$. Let T be a maximal torus of G contained in B. Then $Z(G) \subset C_G(T)$, which is contained in B (17.39b). □

THEOREM 17.46. *Let G be a connected group variety over k. Let S be a torus in G and B a Borel subgroup containing S. Then $C_G(S) \cap B$ is a Borel subgroup of $C_G(S)$. If k is algebraically closed, then every Borel subgroup of $C_G(S)$ is of this form.*

PROOF. We may suppose that k is algebraically closed. Let $C = C_G(S)$. Then $C \cap B = C_B(S)$, which is smooth (13.10), connected (17.38), and solvable (because it is a subgroup of B). To show that it is a Borel subgroup of C, it remains to show that $C/C \cap B$ is complete (17.19). Let $q: G \to G/B$ denote the quotient map. Then $C/C \cap B \simeq q(C)$, and so it suffices to show that $q(C)$ complete. As G/B is complete, it suffices to show that $q(C)$ is closed, and as q is open, it suffices to show that CB is closed in G. Let $\overline{CB}$ denote the closure of CB in G. It is connected because CB is the image of $C \times B$ under the multiplication map. We regard it as a closed subvariety of G.

Let $y = cb \in CB$ (by this we mean that $y \in (CB)(k)$). Then

$$y^{-1}Sy = b^{-1}c^{-1}Scb = b^{-1}Sb \subset B$$

because $S \subset B$, and so (by continuity[2])

$$y \in \overline{CB} \implies y^{-1}Sy \subset B. \tag{126}$$

Let $\varphi: B \to B/B_u$ denote the quotient map, and consider the regular map $(y,s) \mapsto \varphi(y^{-1}sy): \overline{CB} \times S \to B/B_u$. As $\overline{CB}$ is connected and B/B_u is diagonalizable, the rigidity theorem (12.36) shows that $\varphi(y^{-1}sy)$ is independent of y. Hence

$$\varphi(y^{-1}sy) = \varphi(s) \text{ for all } y \in \overline{CB} \text{ and } s \in S. \tag{127}$$

---

[2]More formally, in the action of G on itself by conjugation, the transporter of S into B is a closed subscheme of G (1.79) containing CB and hence $\overline{CB}$.

Let $y \in \overline{CB}$, and let T be a maximal torus of B containing S. Then $y^{-1}Sy \subset B$ (by (126)), and so there exists a $u \in B_u$ such that $u^{-1}y^{-1}Syu \subset T$ (see 16.33d). As $CB \cdot B \subset CB$, we have $\overline{CB} \cdot B \subset \overline{CB}$ (by continuity). Therefore $yu \in \overline{CB}$, and so

$$\varphi((yu)^{-1}s(yu)) = \varphi(s) \text{ for all } s \in S$$

(by (127)). But $(yu)^{-1}s(yu)$ and s both lie in T and φ is injective on T, and so

$$(yu)^{-1}s(yu) = s \text{ for all } s \in S.$$

Therefore $yu \in C$ (see 1.93), and so $y \in CB$. We have shown that CB is closed.

For the second part of the statement, let B_0 be a Borel subgroup of C, and let B be a Borel subgroup of G containing S. Because $B \cap C$ is a Borel subgroup of C, there exists $c \in C(k)$ such that $B_0 = c(B \cap C)c^{-1}$ (see 17.9). But $c(B \cap C)c^{-1} = cBc^{-1} \cap cCc^{-1} = cBc^{-1} \cap C$, which proves the assertion. $\quad\square$

e.   The normalizer of a Borel subgroup

In this section, we prove the normalizer theorem: every Borel subgroup is equal to its own normalizer.[3] Throughout, G is a connected group variety over a field k (not necessarily algebraically closed field).

LEMMA 17.47. *Let H be a subgroup variety of G. If H contains a Cartan subgroup of G, then $N_G(H)^\circ = H^\circ$ (and so $N_G(H)$ is smooth).*

PROOF. We may suppose that k is algebraically closed. Let $N = N_G(H)$. Then $N \supset H$ and

$$\dim \mathfrak{h} = \dim H \leq \dim N \leq \dim \mathfrak{n}$$

(see 1.37). If $\mathfrak{n} = \mathfrak{h}$, then N is smooth and $H^\circ = N^\circ$.

Let H contain the Cartan subgroup $C = C_G(T)$. Recall (10.34) that $\mathfrak{c} = \mathfrak{g}^T$ and $\mathfrak{n}/\mathfrak{h} = (\mathfrak{g}/\mathfrak{h})^H$. Because H contains C, its Lie algebra $\mathfrak{h}$ contains $\mathfrak{c}$, and there is an exact sequence

$$0 \to \mathfrak{h}/\mathfrak{g}^T \to \mathfrak{g}/\mathfrak{g}^T \to \mathfrak{g}/\mathfrak{h} \to 0.$$

As T is diagonalizable, it is linearly reductive (12.54), and so the map $(\mathfrak{g}/\mathfrak{g}^T)^T \to (\mathfrak{g}/\mathfrak{h})^T$ is surjective and $(\mathfrak{g}/\mathfrak{g}^T)^T = 0$. Therefore $(\mathfrak{g}/\mathfrak{h})^T = 0$. But

$$(\mathfrak{g}/\mathfrak{h})^T \supset (\mathfrak{g}/\mathfrak{h})^H = \mathfrak{n}/\mathfrak{h},$$

and so $\mathfrak{n} = \mathfrak{h}$. $\quad\square$

---

[3]Chevalley always said that, once the normalizer theorem had been proved, it was all downhill (Cartier 2005, 25.7).

THEOREM 17.48 (NORMALIZER THEOREM). *Let B be a Borel subgroup of G. Then*

$$B = N_G(B).$$

PROOF. We may suppose that k is algebraically closed. We use induction on the dimension of G. If $\dim(G) \leq 2$, then G is solvable (17.27), and so $G = B = N_G(B)$.

Every Borel subgroup contains a maximal torus and therefore a Cartan subgroup (17.39), and so the lemma shows that $N_G(B)$ is smooth. Therefore it suffices to show that $N_G(B)(k) \subset B(k)$.

Let $x \in N_G(B)(k)$, which we wish to prove lies in $B(k)$. Let T be a maximal torus in B. Then xTx^{-1} is also a maximal torus in B and hence is conjugate to T by an element b of $B(k)$ (see 17.9). After replacing x with bx, we may suppose that $T = xTx^{-1}$. The map

$$\varphi: T \to T, \quad t \mapsto [x,t] = xtx^{-1}t^{-1}$$

is a homomorphism because $\varphi(t_1)\varphi(t_2) = t_1^x t_1^{-1} \cdot t_2^x t_2^{-1} = t_1^x t_2^x t_2^{-1} t_1^{-1} = \varphi(t_1 t_2)$.

If $\varphi(T) \neq T$, then the kernel of φ contains a nontrivial torus S such that $x \in C_G(S)$. Note that x normalizes $C_G(S) \cap B$, which is a Borel subgroup of C (see 17.46). If $C_G(S) \neq G$, then $x \in B(k)$ by the induction hypothesis applied to $C_G(S)$. On the other hand, if $C_G(S) = G$, then $S \subset Z(G)$, and $x \in B(k)$ by the induction hypothesis applied to G/S.

If $\varphi(T) = T$, then T acts trivially on any one-dimensional representation of G. Let (V,r) be a representation of G such that $N_G(B)$ is the stabilizer of a line $L = \langle v \rangle$ in V (see 4.27). Then T fixes v, and B_u fixes v because it is unipotent. Therefore $B = B_u \cdot T$ fixes v, and the map $g \mapsto r(g) \cdot v: G \to V$ factors through G/B. As G/B is complete and connected, the map has image $\{v\}$ (see A.75g), and so G fixes v. Hence $G = N_G(B)$, which implies that $G = B$ (17.33b). □

COROLLARY 17.49. *Let P be a subgroup variety of G. If P contains a Borel subgroup of G, then P is connected and $P = N_G(P)$.*

PROOF. We may suppose that k is algebraically closed. As P contains a Borel subgroup of G, it contains a Cartan subgroup (17.39), and so $N_G(P)$ is smooth (17.47). As $P^\circ \subset P \subset N_G(P)$, it suffices to show that $P^\circ(k) = N_G(P)(k)$.

Let $x \in N_G(P)(k)$, and let $B \subset P$ be a Borel subgroup of G. Then B and xBx^{-1} are Borel subgroups of P°, and so there exists a $p \in P^\circ(k)$ such that

$$B = p(xBx^{-1})p^{-1} = (px)B(px)^{-1}$$

(17.10). As px normalizes B, it lies in $B(k)$ (see 17.48), and so

$$x = p^{-1} \cdot px \in P^\circ(k) \cdot B(k) = P^\circ(k),$$

as required. □

COROLLARY 17.50. *Let B be a Borel subgroup of G and assume that B contains a subgroup B_u as in 16.7. Then $B = N_G(B_u)$.*

PROOF. We may suppose that k is algebraically closed. Let $P = N_G(B_u)_{\mathrm{red}}$. Then P contains B, and so it is connected (17.49). From the conjugacy of Borel subgroups, it follows that B_u is maximal among the connected unipotent subgroup varieties of G. Hence P/B_u has no nontrivial connected unipotent subgroup variety, and so it is a torus (17.25). Therefore P is solvable, and so $P = B$. Now,

$$B = N_G(B_u)_{\mathrm{red}} \subset N_G(B_u) \subset N_G(B) = B,$$

and so $N_G(B_u) = B$. □

Recall (16.33) that B contains a subgroup B_u if k is perfect.

REMARK 17.51. It follows from Corollary 17.49 that the Borel subgroups of G are maximal among the solvable subgroup varieties (not necessarily connected) of G.[4] However, not every solvable subgroup variety is contained in a Borel subgroup of G. For example, the diagonal in SO_n is a commutative subgroup variety not contained in any Borel subgroup (we assume that $n > 2$ and that the characteristic $\neq 2$). Indeed, it is a product of copies of $(\mathbb{Z}/2\mathbb{Z})_k$, and equals it own centralizer. If it were contained in a Borel subgroup of G, it would be contained in a torus (16.33), which would centralize it.

f. The variety of Borel subgroups

In this section, G is a connected group variety over an algebraically closed field k. Let $\mathcal{B}$ denote the set of Borel subgroups in G. The group $G(k)$ acts transitively on $\mathcal{B}$ by conjugation,

$$(g, B) \mapsto gBg^{-1} : G(k) \times \mathcal{B} \to \mathcal{B}$$

(see 17.9). Let B be a Borel subgroup of G. As $B = N_G(B)$ (17.47), the orbit map $g \mapsto gBg^{-1}$ induces a bijection

$$\phi_B : (G/B)(k) \to \mathcal{B}.$$

We endow $\mathcal{B}$ with the structure of an algebraic variety for which ϕ_B is an isomorphism. Then the action of G on $\mathcal{B}$ is regular and $\mathcal{B}$ is a smooth connected projective variety.

Let $B' = gBg^{-1}$ be a second Borel subgroup of G. The map $G \xrightarrow{\mathrm{inn}(g)} G \longrightarrow G/B'$ factors through G/B, and gives top map in the following diagram:

$$
\begin{array}{ccc}
G/B & \xrightarrow{\mathrm{inn}(g)} & G/B' \\
\downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi_{B'}} \\
\mathcal{B} & \xrightarrow{B'' \mapsto gB''} & \mathcal{B}.
\end{array}
$$

[4]In fact, $B(k)$ is a maximal solvable (abstract) subgroup of $G(k)$.

The diagram commutes, and all maps except possibly $\phi_{B'}$ are regular isomorphisms, and so $\phi_{B'}$ is also a regular isomorphism. In particular, the structure of an algebraic variety on $\mathcal{B}$ does not depend on the choice of B.

The variety $\mathcal{B} = \mathcal{B}(G)$, equipped with its G-action, is called the **flag variety** of G. For example, the flag variety of GL_V is the set of maximal flags in V equipped with its natural structure of an algebraic variety (Section 7g).

LEMMA 17.52. *Let S be a subset of $G(k^a)$, and let $\mathcal{B}^S = \{B \in \mathcal{B} \mid s \cdot B = B$ for all $s \in S\}$. Then $\mathcal{B}^S$ is a closed subset of $\mathcal{B}$, equal to $\{B \in \mathcal{B} \mid B \supset S\}$.*

PROOF. We have $\mathcal{B}^S = \bigcap_s \mathcal{B}^s$, where $\mathcal{B}^s$ is the subset of $\mathcal{B}$ on which the maps $x \mapsto x$ and $x \mapsto sx$ agree. As $\mathcal{B}^s$ is closed, so also is $\mathcal{B}^S$. By definition, $s \cdot B = sBs^{-1}$. Hence $s \cdot B = B \iff s \in N_G(B) \overset{17.48}{=} B$, from which the second part of the statement follows. $\qquad\square$

For example, if T is a torus in G, then $\mathcal{B}^T$ consists of the Borel subgroups of G containing T.

PROPOSITION 17.53. *Let T be a maximal torus of G. The Weyl group $W(G,T)$ acts simply transitively on the set $\mathcal{B}^T$ of Borel subgroups of G containing T.*

PROOF. The set $\mathcal{B}^T$ is finite by 17.11. As $C_G(T)$ is connected (17.38), it acts trivially on the corresponding finite subset $(G/B)^T$ of G/B, and so the action factors through $W(G,T)$. Let x be an element of $N_G(T)$ such that $xBx^{-1} = B$. Then $x \in B$ by (17.48). Thus $x \in N_B(T)$. Hence, for every $t \in T$, we have

$$x t x^{-1} t^{-1} \in T \cap B^{\mathrm{der}} \subset T \cap B_u = e,$$

so that $x \in C_G(T)$. $\qquad\square$

The essence of the proof was to show that $N_G(T) \cap B = N_G(T)^\circ$; cf. 17.11.

PROPOSITION 17.54. *Let $\phi: G \to G'$ be a quotient map of connected group varieties.*

(a) The map $B \mapsto \phi(B)$ is a surjective regular map

$$\phi_{\mathcal{B}}: \mathcal{B} \longrightarrow \mathcal{B}'$$

of flag varieties. If $\mathrm{Ker}(\phi)$ is contained in some Borel subgroup of G, then $\phi_{\mathcal{B}}$ is bijective.

(b) Let T be a maximal torus of G, and let $T' = \phi(T)$. Then ϕ induces a surjective homomorphism $W(\phi): W(G,T) \to W(G',T')$. If $\mathrm{Ker}(\phi)$ is contained in some Borel subgroup of G, then $W(\phi)$ is an isomorphism.

PROOF. (a) That ϕ induces a surjective map of sets is proved in 17.20. The regularity of $\phi_{\mathcal{B}}$ follows from the definition of the algebraic structure on the flag varieties. If $\mathrm{Ker}(\phi)$ is contained in a Borel subgroup, then, since it is normal, it

is contained in every Borel subgroup, and so $B = \phi^{-1}(\phi(B))$ for every $B \in \mathcal{B}$. This proves the injectivity.

(b) Recall (17.20) that $T' \stackrel{\text{def}}{=} \phi(T)$ is a maximal torus in G'. Let $n \in N_G(T)$. Then

$$\phi(n)\phi(T)\phi(n)^{-1} = \phi(nTn^{-1}) = \phi(T)$$

and so $\phi(n) \in N_{G'}(T')$. If $n \in C_G(T)$, then a similar computation shows that $\phi(n) \in C_{G'}(T')$, and so the map sending n to $\phi(n)$ induces a homomorphism $W(G,T) \to W(G',T')$.

If $B \supset T$, then $\phi(B) \supset \phi(T) \stackrel{\text{def}}{=} T'$, and so $\phi_{\mathcal{B}}$ maps $\mathcal{B}^T$ into $\mathcal{B}'^{T'}$. For any $B \in \mathcal{B}^T$, we get a commutative diagram

$$
\begin{array}{ccc}
W(G,T) & \xrightarrow{\ W(\phi)\ } & W(G',T') \\
{\scriptstyle 1:1}\big\downarrow{\scriptstyle n \mapsto n\cdot B} & & {\scriptstyle 1:1}\big\downarrow{\scriptstyle n \mapsto n\cdot\phi(B)} \\
\mathcal{B}^T & \xrightarrow{\ \ \phi_{\mathcal{B}}\ \ } & \mathcal{B}'^{T'}
\end{array}
$$

Therefore $W(\phi): W(G,T) \to W(G',T')$ is surjective (resp. bijective) if and only if $\phi_{\mathcal{B}}: \mathcal{B}^T \to \mathcal{B}'^{T'}$ is surjective (resp. bijective).

Let $B_0' \in \mathcal{B}'^{T'}$. There exists a $B_0 \in \mathcal{B}$ such that $\phi(B_0) \in \mathcal{B}'^{T'}$. Then $\phi(T) \in \phi(B_0)$, and so $T \in \phi^{-1}(\phi(B_0)) = P$, which is a parabolic subgroup of G containing B_0. Now T is a maximal torus of P, and so it is contained in a Borel subgroup B of P. But B_0 is also a Borel subgroup of P, and so B and B_0 are conjugate in P, which implies that B is a Borel subgroup of G. This proves the surjectivity.

Finally, if $\mathrm{Ker}(\phi)$ is contained in a Borel subgroup, then $\phi_{\mathcal{B}}: \mathcal{B} \to \mathcal{B}'$ is injective, which implies that its restriction to $\mathcal{B}^T \to \mathcal{B}'^{T'}$ is injective.   □

In the course of proving (17.54), we showed that, if B is a Borel subgroup of a parabolic subgroup of G, then it is a Borel subgroup of G.

REMARK 17.55. Let G be a connected group variety, and let X be a projective variety of maximum dimension on which G acts transitively. Let $o \in X$, and let G_o be the isotropy group at o. Then $G/G_o \simeq X$. As X is projective of maximum dimension, G_o is parabolic of minimum dimension, and hence is a Borel subgroup of G (see 17.19). The map $x \mapsto G_x$ is a G-equivariant isomorphism of algebraic varieties $X \to \mathcal{B}$.

If X is not of maximum dimension, then its points correspond to the elements of a conjugacy class of parabolic subgroups of G (see 17.49).

g.   Chevalley's description of the unipotent radical

In this section, G is a connected group variety over k. Recall (17.31) that, when k is algebraically closed, the radical of G is the reduced identity component of the intersection of the Borel subgroups of G. Chevalley proved a more precise statement.

THEOREM 17.56 (CHEVALLEY'S THEOREM). *Assume that k is algebraically closed, and let T be a maximal torus in G. Then*

$$R_u(G) \cdot T = \left(\bigcap_{B \in \mathcal{B}^T} B \right)^{\circ}_{\text{red}}$$

$$R_u(G) = \left(\bigcap_{B \in \mathcal{B}^T} B_u \right)^{\circ}_{\text{red}}.$$

The intersection is over the (finite set of) Borel subgroups of G containing T.

Before proving the theorem, we list some consequences.

COROLLARY 17.57. *Assume that k is algebraically closed, and let S be a torus in G. Then*

$$R_u(C_G(S)) = R_u(G) \cap C_G(S).$$

PROOF. Let S act on G by conjugation. Then $C_G(S) = G^S$, and so $R_u(G) \cap C_G(S) = R_u(G)^S$, which is smooth and connected (13.9, 17.40). As it is unipotent (14.7) and normal in $C_G(S)$, it is contained in $R_u(C_G(S))$.

For the reverse inclusion, it suffices to prove that $R_u(C_G(S)) \subset R_u(G)$. Let T be a maximal torus of G containing S. The intersection with $C_G(S)$ of a Borel subgroup B of G containing T is a Borel subgroup of $C_G(S)$ (see 17.46), and so $B \supset R_u(C_G(S))$. Therefore

$$R_u(C_G(S)) \subset \left(\bigcap_{B \in \mathcal{B}^T} B \right)^{\circ}_{\text{red}} \overset{17.56}{=} R_u(G) \cdot T,$$

and so

$$R_u(C_G(S)) \subset (R_u(G) \cdot T)_u = R_u(G). \qquad \square$$

COROLLARY 17.58. *Assume that k is algebraically closed, and let S be a torus acting on G. Then*

$$R_u(G^S) = R_u(G)^S.$$

PROOF. Let $G' = G \rtimes S$. Then $C_{G'}(S) = G^S$ and $R_u(G') = R_u(G)$, and so

$$R_u(G^S) = R_u(C_{G'}(S)) \overset{17.57}{=} R_u(G') \cap C_{G'}(S) = R_u(G)^S. \qquad \square$$

COROLLARY 17.59. *Let S be a torus acting on G. If G is reductive, then so also is G^S. In particular, the centralizer of a torus in a reductive group is reductive.*

PROOF. The group G^S is smooth and connected (13.9, 17.40), and Corollary 17.57 applied to G_{k^a} shows that $R_u(G^S_{k^a}) = R_u(G)^S_{k^a} = e$. $\qquad \square$

More generally, the identity component of G^S is reductive if G is reductive and S_{k^a} is linearly reductive (Conrad et al. 2015, A.8.12). The proof uses Matsushima's criterion (5.30).

PROPOSITION 17.60. *Let λ be a cocharacter of G. The unipotent group $U(\lambda)$ is split. If G is reductive, then the quotient $P(\lambda)/U(\lambda)$ is reductive and*

$$R_u(P(\lambda)) = U(\lambda), \quad R_u(P(\lambda)_{k^a}) = U(\lambda)_{k^a}.$$

PROOF. Recall (13.33) that $U(\lambda)$ and $P(\lambda)$ are smooth and connected, and that $U(\lambda)$ is unipotent. According to (13.33c), $\mathrm{Lie}(U(\lambda))^{\mathbb{G}_m} = 0$ and so $U(\lambda)$ is split by (16.63). The quotient $P(\lambda)/U(\lambda)$ is isomorphic to $C_G(\lambda\mathbb{G}_m)$ (see 13.33b), which is reductive if G is reductive (17.59). The remaining statements follow from the definitions.   □

PROPOSITION 17.61. *Let G be a reductive group.*

(a) *Let T be a torus in G such that T_{k^a} is maximal in G_{k^a}. Then $C_G(T) = T$.*

(b) *The centre $Z(G)$ of G is contained in all maximal tori T in G, and $Z(G)(k^a) = \bigcap_{T\ maximal} T(k^a)$.*

PROOF. (a) We may suppose that k is algebraically closed. Every Borel subgroup containing T contains $C_G(T)$ (see 17.39), and $C_G(T)$ is smooth and connected (13.10, 17.38), and so

$$C_G(T) \subset \left(\bigcap_{B\in\mathcal{B}^T} B\right)^{\circ}_{\mathrm{red}} \overset{17.56}{=} R_u(G)\cdot T = T.$$

(b) Certainly, $Z(G) \subset \bigcap_{T\ maximal} C_G(T) = \bigcap_{T\ maximal} T$. Conversely, if $g \in G(k^a)$ lies in $\bigcap_{T\ maximal} T(k^a)$, then it commutes with all elements of all Cartan subgroups, but these elements contain a dense open subset of G (see 17.44), and so $g \in Z(G)(k)$.   □

Later (17.82) we show that if T is a maximal torus in a group variety G, then T_{k^a} is maximal in G_{k^a}. Therefore (a) holds for all maximal tori in G.

COROLLARY 17.62. *Let G be a reductive group.*

(a) *The centre $Z(G)$ of G is of multiplicative type.*

(b) *$R(G) = Z(G)_t$ (largest subtorus of $Z(G)$).*

(c) *The formation of $R(G)$ commutes with extension of the base field.*

(d) *The quotient $G/R(G)$ is semisimple.*

(e) *The quotient $G/Z(G)$ has trivial centre.*

PROOF. (a) Let T be a maximal torus in G; then $Z(G) \subset C_G(T) = T$, and so $Z(G)$ is of multiplicative type.

(b) The subgroup variety $Z(G)_t$ is normal in G (see 12.29). It is also connected and commutative (by definition), and so $Z(G)_t \subset R(G)$. Conversely, $R(G)_{k^a} \subset R(G_{k^a})$, which is a torus because $R_u(G_{k^a}) = e$. Therefore $R(G)$ is a torus. Rigidity (12.37) implies that the action of G on $R(G)$ by inner automorphisms is trivial, and so $R(G) \subset Z(G)$. Hence $R(G) \subset Z(G)_t$.

(c) The formation of the centre, and the largest subtorus, commute with extension of the base field, and so this follows from (b).

(d) We have

$$(G/R(G))_{k^{\mathrm{a}}} \simeq G_{k^{\mathrm{a}}}/R(G)_{k^{\mathrm{a}}} \overset{(c)}{\simeq} G_{k^{\mathrm{a}}}/R(G_{k^{\mathrm{a}}}),$$

which is semisimple (6.44). By definition, this means that $G/R(G)$ is semisimple.

(e) Let Z' be the inverse image of the centre of $G/Z(G)$ in G. Then Z' is a normal subgroup of G, and the action of G on it by conjugation is trivial by (12.41). Therefore $Z' = Z(G)$. □

REMARK 17.63. Let G be an algebraic group over k. The action of G on itself by inner automorphisms

$$(x, y) \mapsto xyx^{-1}: G \times G \to G$$

is invariant under $Z(G) \times e$ acting by translation, and so it factors through $G/Z(G)$. The automorphisms of G defined by elements of $(G/Z)(k)$ are exactly the inner automorphisms of G, i.e., over k^{a} they become of the form $\mathrm{inn}(g)$ with $g \in G(k^{\mathrm{a}})$ (see 3.51). An inner automorphism need not be of the form $\mathrm{inn}(g)$ with $g \in G(k)$. For example, the automorphism

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & tb \\ t^{-1}c & d \end{pmatrix}, \quad t \in k^{\times},$$

of SL_2 is inner (it is conjugation by the matrix $\mathrm{diag}(t, 1)$ regarded as an element of $\mathrm{PGL}_2(k)$), but it need not be of the form $\mathrm{inn}(g)$ with $g \in \mathrm{SL}_2(k)$ (see 20.29).

We write $\mathrm{inn}(g)$ for the inner automorphism of G defined by an element $g \in G^{\mathrm{ad}}(k)$.

An ***adjoint group*** is a semisimple group with trivial centre. The quotient of a reductive group G by its centre is an adjoint group (17.62e), called the ***adjoint group*** G^{ad} of G.

h. Proof of Chevalley's theorem

Chevalley's theorem is important for the description of algebraic groups in terms of root data. The traditional proof (Chevalley 1956–58, Exp. 12; Springer 1998, 7.6.3) also uses root data. We give a proof (due to Luna) that avoids using root data. The field k is algebraically closed.

THEOREM 17.64 (KOSTANT–ROSENLICHT). *Let G be a unipotent group variety acting on an affine algebraic scheme X over k. Every orbit of G in X is closed.*

PROOF. Let O be an orbit of G in X. After replacing X with the closure of O, we may suppose that O is dense in X. Let $Z = (X \smallsetminus O)_{\mathrm{red}}$. Then Z is stable

under G (see 7.5), and so its ideal $I(Z)$ in $\mathcal{O}(X)$ is stable under G. The scheme Z is not dense in X because its complement contains a nonempty open subset of X, and so $I(Z) \neq 0$. As G is unipotent, there is a nonzero f in $I(Z)$ fixed by G. Now f is constant on O, and hence also on X. Thus $I(Z)$ contains a nonzero scalar, which implies that Z is empty. $\qquad\square$

For example, the orbits of $\mathbb{U}_2$ acting on k^2 are the horizontal lines, which are closed.

THEOREM 17.65. *Let G be a connected group variety, and let (B, T) be a Borel pair in G. The set*

$$\mathcal{B}(B) = \{B' \in \mathcal{B} \mid B \in \overline{T \cdot B'}\}$$

is open and affine in $\mathcal{B}$, and it is stable under $I_u(T)$.

PROOF. According to Theorem 4.27, there exists a representation (V, r) of G such that B is the stabilizer of a line $[v]$. There is then a projective embedding $G/B \to \mathbb{P}(V)$, which we may suppose to be nondegenerate. The image of $\mathcal{B}$ in $\mathbb{P}(V)$ is a closed irreducible subvariety X stable under G. Let x denote the image of B in X. Then x is fixed by T, and $\mathcal{B}(B)$ maps onto the set

$$U(x) = \{y \in X \mid x \in \overline{T \cdot y}\}.$$

According to Proposition 13.52, for each cocharacter λ of G satisfying certain conditions, there is an $x_- \in \mathcal{B}^T(k)$ such that $U(x_-)$ is an open affine subset of $\mathcal{B}$. There exists an $n \in N_G(T)$ such that $n(x_-) = x$ (see 17.53), and the point x is the "x_-" for $n(\lambda)$. Therefore $U(x)$ is an open affine subset of X, and it remains to show that it is stable under $I_u(T)$.

Let $V = \bigoplus_{\chi \in \Xi} V_\chi$ be the decomposition of V into eigenspaces for the action of T, and let $\lambda : \mathbb{G}_m \to T$ be a cocharacter of T such that the integers $\langle \lambda, \chi \rangle$, $\chi \in \Xi$, are distinct.

Let $\chi_- \in \Xi$ be such that $\langle \lambda, \chi_- \rangle$ is minimum. Then V_{χ_-} has dimension 1 and V_- is the unique attracting point x_- of X (see 13.53). Moreover, $U(x_-)$ is the open cell $X(x_-, \lambda)$. It is the set of $[v] \in X$ such that $v = \sum v_\chi$ with $v_{\chi_-} \neq 0$.

Let $(V^\vee, r^\vee)$ be the contragredient of r. Let $V_-^\perp$ be the hyperplane in $V^\vee$ orthogonal to $v_- \in V$. If there exists a vector $v^\vee$ such that the orbit $Gv^\vee$ is entirely contained in this hyperplane, then $\langle gv_-, v^\vee \rangle = 0$ for all g, which implies that $v^\vee = 0$ because the vectors gv_- generated V. It follows that every orbit $G[v^\vee]$ in $\mathbb{P}(V^\vee)$ meets the affine complement $\mathbb{P}(V^\vee) \smallsetminus V_-^\perp$. But the action of $\lambda^{-1}(z)$, $z \in \mathbb{G}_m$, contracts this affine space to $[v_-^\vee]$, which shows that the orbit $G[v_-^\vee]$ is closed. Let P denote the stabilizer of $v_-^\vee$. It is a parabolic subgroup of G containing T. It contains a Borel subgroup B such that $T \subset B \subset P$. Therefore $I_u(T) \subset P$. Therefore, it fixes the line $[v^\vee]$ and dually it leaves invariant the open $X_{x_-}(\lambda)$. $\qquad\square$

We now prove Chevalley's Theorem 17.56. It suffices to show that $I_u(T)$ acts trivially on $\mathcal{B}$, i.e., that $\mathcal{B} = \mathcal{B}^{I_u(T)}$, because then $I_u(T)$ is contained in all

Borel subgroups of G, and so

$$I_u(T) \subset \left(\bigcap\nolimits_{B \subset G \text{ Borel}} B \right)^{\circ}_{\text{red}} \stackrel{17.31}{=} R(G);$$

as $I_u(T)$ is unipotent, this implies that

$$I_u(T) \subset R(G)_u = R_u(G).$$

We now show that $I_u(T)$ acts trivially on $\mathcal{B}$. Any nonempty closed orbit of T acting on $\mathcal{B}$ is complete, and so contains a fixed point (17.3), and so the orbit itself is a fixed point.

Note that the (open affine) varieties $\mathcal{B}(B)$, $B \in \mathcal{B}^T$, cover $\mathcal{B}$. Indeed, for any $B' \in \mathcal{B}$, the closure of its T-orbit $\overline{T \cdot B'}$ contains a closed T-orbit and hence T-fixed point; i.e., there exists a $B \in \mathcal{B}^T$ such that $B \in \overline{T \cdot B'}$. This means that $B' \in \mathcal{B}(B)$.

Let $B' \in \mathcal{B}$; we have to show that the orbit $I_u(T) \cdot B'$ consists of a single point. Because $I_u(T)$ is solvable and connected, there is an $I_u(T)$-fixed point B'' in $\overline{I_u(T) \cdot B'}$ (see 17.3). This point is contained in some $\mathcal{B}(B)$ for $B \in \mathcal{B}^T$. The set $\mathcal{B} \smallsetminus \mathcal{B}(B)$ is closed and $I_u(T)$-stable and so, if it meets the orbit $I_u(T) \cdot B'$, then it has to contain $\overline{I_u(T) \cdot B'}$ and hence also B'', which is a contradiction. Thus $I_u(T) \cdot B'$ is contained in $\mathcal{B}(B)$. As $I_u(T)$ is unipotent and $\mathcal{B}(B)$ is affine, the Kostant–Rosenlicht theorem shows that $I_u(T) \cdot B'$ is closed in $\mathcal{B}(B)$. But B'' lies in the closure of $I_u(T) \cdot B'$ and in $\mathcal{B}(B)$, and so B'' lies in the $I_u(T) \cdot B'$. As it was a fixed point, the orbit $I_u(T) \cdot B'$ is trivial.

i.   Borel and parabolic subgroups over an arbitrary base field

In this section, we explain how to extend some of the above material to an arbitrary base field k.

17.66. A ***Borel subgroup*** of a connected group variety G over k is a connected solvable subgroup variety B such that G/B is complete. According to (17.19), this definition agrees with the earlier definition (17.6) when k is algebraically closed. Let k' be a field containing k; then a subgroup variety B of G is Borel if and only if $B_{k'}$ is a Borel subgroup of $G_{k'}$ (see 1.34, 6.31). Therefore the Borel subgroups of G are exactly those algebraic subgroups that become Borel in the sense of (17.6) over an algebraic closure of k. A ***Borel pair*** of G is a pair that becomes a Borel pair over k^{a} in the sense of (17.12).

17.67. A connected group variety G over k need not contain a Borel subgroup. In other words, it is possible that no Borel subgroup of $G_{k^{\mathrm{a}}}$ is defined over k. A connected group variety containing a Borel subgroup is said to be ***quasi-split***. A connected group variety is quasi-split if and only if some maximal connected solvable subgroup variety H has a complete quotient G/H or, equivalently, if and only if some parabolic subgroup is solvable.

17.68. A parabolic subgroup of a connected group variety G need not contain a Borel subgroup. A Borel subgroup of G (if it exists) is a minimal parabolic subgroup (17.19). For reductive groups without Borel subgroups, the minimal parabolic subgroups play the role that Borel subgroups otherwise play.

17.69. Let $q: G \to Q$ be a quotient map of connected group varieties, and let H be a subgroup variety of G. If H is parabolic (resp. Borel), then so also is $q(H)$. This follows from Proposition 17.20.

Let G be a connected group variety over k. Because the formation of centralizers and normalizers commutes with extension of the base field, the following statements can be deduced from the algebraically closed case.

17.70. Let B be a Borel subgroup of G. Then $Z(B) = C_G(B) = Z(G)$ (17.22, 17.45).

17.71. Let P be a subgroup variety of G. If P contains a Borel subgroup of G, then P is connected and $P = N_G(P)$; in particular, $B = N_G(B)$ (see 17.49).

17.72. Let S be a torus acting on G. Then G^S is smooth and connected (13.9, 17.40). In particular, the centralizer of a torus in G is a smooth connected subgroup of G. If S is contained in a Borel subgroup B of G, then $C_G(S) \cap B$ is a Borel subgroup of $C_G(S)$ (17.46).

ASIDE 17.73. Let G be a reductive group over an arbitrary field k. Any two minimal parabolic subgroups of G are conjugate by an element of $G(k)$ (25.8 below). If G has a Borel subgroup, then the minimal parabolic subgroups of G coincide with the Borel subgroups, and so any two Borel subgroups are conjugate by an element of $G(k)$. A Borel subgroup B in G defines a k-structure on the flag variety $\mathcal{B}$ of G_{k^a},

$$(G/B)_{k^a} \xrightarrow{\simeq} G_{k^a}/B_{k^a} \simeq \mathcal{B},$$

which the preceding statement shows to be independent of B.

j. Maximal tori and Cartan subgroups over an arbitrary base field

Preliminaries

Every endomorphism α of a finite-dimensional vector space V over a perfect field k has a unique additive Jordan decomposition $\alpha = \alpha_s + \alpha_n$ with α_s and α_n commuting semisimple and nilpotent endomorphisms respectively. Indeed, when the eigenvalues of α lie in k, we can define α_s as in the proof of Theorem 9.11 and take $\alpha_n = \alpha - \alpha_s$. The rest of the proof is the same as that of 9.11. When α lies in a Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}_V$, its semisimple and nilpotent parts α_s and α_n need not lie in $\mathfrak{g}$. However, this is true if $\mathfrak{g}$ is the Lie algebra of an algebraic group. More precisely, the following is true.

PROPOSITION 17.74. *Let k be a perfect field.*

(a) *Let G be an algebraic group over k, and let $X \in \mathfrak{g}$. Then X has a unique decomposition $X = X_s + X_n$ such that $\rho(X_s) = \rho(X)_s$ and $\rho(X_n) = \rho(X)_n$ for every representation ρ of $\mathfrak{g}$.*

(b) *Let $\varphi \colon G \to G'$ be a homomorphism of algebraic groups. Then $(d\varphi)(X_s) = (d\varphi)(X)_s$ and $(d\varphi)(X_n) = (d\varphi)(X)_n$ for all $X \in \mathfrak{g}$.*

PROOF. Exercise (cf. Springer 1998, 4.4.20). □

EXAMPLE 17.75. If G is unipotent, then all element of $\mathfrak{g}$ are nilpotent because an embedding of G into $\mathbb{U}_n$ defines an embedding of $\mathfrak{u}$ into $\mathfrak{n}_n$ (strictly upper triangular matrices). Similarly, if G is a torus, then all elements of $\mathfrak{g}$ are semisimple.

Let $\mathfrak{g}$ be a Lie algebra over a field k (not necessarily perfect). We say that an element X of $\mathfrak{g}$ is **semisimple** if $\rho(X)$ is semisimple for all representations ρ of $\mathfrak{g}$. When k is perfect, X is semisimple if and only if $X = X_s$.

Let G be a connected group variety over a field k, and let $X \in \mathfrak{g}$. Then G acts on $\mathfrak{g}$ through the adjoint representation, and we let $C_G(X)$ denote the subgroup of G fixing X.

PROPOSITION 17.76. *If X is semisimple, then $C_G(X)$ is a smooth algebraic subgroup of G, and*

$$\operatorname{Lie}(C_G(X)) = z_{\mathfrak{g}}(X) \overset{\text{def}}{=} \{Y \in \mathfrak{g} \mid [Y, X] = 0\}.$$

PROOF. The smoothness can be proved by a modification of the proof of 13.6 (decompose $\mathfrak{m}/\mathfrak{m}^2$ into a sum of simple representations for the action of X). It suffices to prove the remaining statement with $G = \mathrm{GL}_n$. Let $A \in \mathfrak{gl}_n$. Then

$$\begin{aligned}
I + A\varepsilon \in L(C_G(X)) &\iff I + A\varepsilon \in C_G(X)(k[\varepsilon]) \\
&\iff (I + A\varepsilon)X(I - A\varepsilon) = X \\
&\iff AX - XA = 0.
\end{aligned}$$

□

COROLLARY 17.77. *A semisimple element X of $\mathfrak{g}$ is central if and only if $C_G(X) = G$.*

PROOF. By definition, X is central if and only if $z_{\mathfrak{g}}(X) = \mathfrak{g}$. As $C_G(X)$ is smooth and G is connected, $C_G(X) = G$ if and only if $\operatorname{Lie}(C_G(X)) = \operatorname{Lie}(G)$ (see 10.15), i.e., if and only if $z_{\mathfrak{g}}(X) = \mathfrak{g}$. □

PROPOSITION 17.78. *Let G be a group variety over an algebraically closed field k. The elements of $\mathfrak{g}$ with noncentral semisimple part form an open subset of $\mathfrak{g}$ (for the Zariski topology).*

PROOF. For $X \in \mathfrak{g}$, let $P(T, X)$ denote the characteristic polynomial of the linear map $\mathrm{ad}(X): \mathfrak{g} \to \mathfrak{g}$, and write

$$P(T, X) = T^d + f_1(X)T^{d-1} + \cdots + f_d, \quad d = \dim G, \quad f_i(X) \in k.$$

When we vary X, the f_i become regular functions on $\mathfrak{g}_a$. From the definition of the semisimple part of an element of $\mathfrak{g}$, we see that $P(T, X) = P(T, X_s)$. The element X_s is central if and only if $f_i(X) = 0$ for all i. Thus, the elements of $\mathfrak{g}$ with noncentral semisimple part are those in the open sets $D(f_i)$, $i = 1, \ldots, d$. For more details, see Springer 1998, 13.3.4. □

PROPOSITION 17.79. *Let G be a group variety over an infinite field k. If $\mathfrak{g}_{k^a}$ contains a noncentral semisimple element, then so does $\mathfrak{g}$, and the centralizers of these elements in $\mathfrak{g}$ span $\mathfrak{g}$.*

PROOF. As $\mathfrak{g}_{k^a}$ contains a noncentral semisimple element, the elements of $\mathfrak{g}_{k^a}$ with noncentral semisimple part form a *nonempty* open subset U of $\mathfrak{g}_{k^a}$ (see 17.78). Because k is infinite, $\mathfrak{g}$ is dense in $\mathfrak{g}_{k^a}$ (because $\mathfrak{g}_a \approx \mathbb{A}^{\dim(\mathfrak{g})}$), and so $U \cap \mathfrak{g}$ is dense in $\mathfrak{g}_{k^a}$. Therefore, there exists a noncentral semisimple element in $\mathfrak{g}$. The set spanned by the centralizers of such elements is a closed subset of $\mathfrak{g}$ containing $U \cap \mathfrak{g}$, and so equals $\mathfrak{g}$. □

Let G be a group variety over a field k. If G is nilpotent, then all semisimple elements of $G(k^a)$ are contained in its centre (16.47). For certain "bad" nonnilpotent groups this may still be true. These groups cause problems, which the next result allows us to avoid.

PROPOSITION 17.80. *Let G be a group variety over a field k. Then there exists an isogeny $\varphi: G \to G'$ such that*
   (a) *either G' is nilpotent or $\mathfrak{g}'_{k^a}$ contains a noncentral semisimple element;*
   (b) *every torus T' in G' is the image of a torus in G.*

PROOF. If G satisfies (a), there is nothing to prove. Otherwise, G is not nilpotent and all semisimple elements of $\mathfrak{g}_{k^a}$ are central. Then k has nonzero characteristic p, and the set of semisimple elements of $\mathfrak{g}$ form a p-Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ stable under $\mathrm{Ad}(G)$. There exists an infinitesimal isogeny $\varphi: G \to G_1$ such that $d\varphi$ has kernel $\mathfrak{h}$ (see 11.38). If G_1 also fails (a), then we repeat the process. Eventually we arrive at an algebraic group G_r and an isogeny $G \to G_r$ satisfying (a) and (b). For more details, see Springer 1998, 13.3.5. □

Maximal tori

We first generalize Proposition 16.60 to an arbitrary base field.

PROPOSITION 17.81. *A connected group variety is unipotent if it contains no nontrivial torus.*

PROOF. Let G be a nonunipotent group over k. We shall show by induction on $\dim(G)$ that G contains a nontrivial torus. We first assume that k is infinite.

Suppose G is nilpotent. Then $Z(G)_s$ is a central torus such that $G/Z(G)_s$ is unipotent (16.47). As G is not unipotent, $Z(G)_s$ is not trivial.

Suppose $\mathfrak{g}_{k^a}$ contains a noncentral semisimple element. As k is infinite, $\mathfrak{g}$ contains a noncentral semisimple element (17.79). Then $C_G(X) \neq G$ and it is nonunipotent (because its Lie algebra contains the semisimple element X). By the induction hypothesis, $C_G(X)$ contains a nontrivial torus.

If neither condition holds, then we choose an isogeny $G \to G'$ as in (17.80). Then G' is not unipotent, and the previous argument shows that it contains a nontrivial torus. It follows that G contains a nontrivial torus.

The proof of the proposition when k is finite requires a different argument. In (17.99) below, we show that a connected group variety G over a finite field k contains a torus T such that T_{k^a} is maximal in G_{k^a}. If G is not unipotent, then neither is G_{k^a}, and T_{k^a} is nontrivial by (16.60). Therefore T is nontrivial. □

THEOREM 17.82. *Let G be a group variety over k and let k' be a field containing k. A torus T in G is maximal if and only if $T_{k'}$ is maximal in $G_{k'}$.*

PROOF. After replacing G with its identity component, we may suppose it to be connected. Clearly T is maximal in G if and only if it is maximal in its centralizer $C_G(T)$, which is again a connected group variety (17.72), and T is maximal in $C_G(T)$ if and only if $C_G(T)/T$ contains no nontrivial torus (16.43). Therefore,

$$T \text{ is maximal in } G \overset{17.81}{\Longleftrightarrow} C_G(T)/T \text{ is unipotent.}$$

The statement on the right holds over k if and only if it holds over k' (see 14.9).□

COROLLARY 17.83. *There exists a maximal torus in G_{k^a} defined over k.*

PROOF. If T is any maximal torus in G, then T_{k^a} is such a torus in G_{k^a}. □

COROLLARY 17.84. *A torus T in a reductive group G is maximal if and only if $C_G(T) = T$.*

PROOF. If T is maximal in G, then T_{k^a} is maximal in G_{k^a}, and so $C_{G_{k^a}}(T_{k^a}) = T_{k^a}$ by Proposition 17.61. But the formation of centralizers commutes with extension of the base field, and so this implies that $C_G(T) = T$. The converse is obvious. □

Recall (12.29) that D_t denotes the reduced connected component (largest subtorus) of a multiplicative group D.

COROLLARY 17.85. *Let G be a connected group variety and N a normal subgroup variety. If T is a maximal torus in G, then $(T \cap N)_t$ is a maximal torus in N, and every maximal torus in N is of this form.*

PROOF. Let T be a maximal torus in G. Let T' be a maximal torus in N and T'' a maximal torus in G containing T'. Then T''_{k^a} is maximal in G_{k^a} (17.82), and so $T_{k^a} = gT''_{k^a}g^{-1}$ for some $g \in G(k^a)$ (see 17.10). Now

$$((T \cap N)_t)_{k^a} = (T_{k^a} \cap N_{k^a})_t = g(T''_{k^a} \cap N_{k^a})_t g^{-1} = gT'_{k^a}g^{-1},$$

which is maximal in N_{k^a}. Therefore $(T \cap N)_t$ is maximal in N. For the second part of the statement, note that $T' = (T'' \cap N)_t$.   □

COROLLARY 17.86. *Let G be a connected group variety over a field k. If G is an almost-direct product of connected subgroup varieties, $G = G_1 \cdots G_n$, then every maximal torus T in G is an almost-direct product $T = T_1 \cdots T_n$ with $T_i = (T \cap G_i)_t$ a maximal torus in G_i.*

PROOF. Let $T_i = (T \cap G_i)_t$. Then T_i is a maximal torus in G_i and $T_1 \cdots T_n \subset T$. Certainly, $T_1 \times \cdots \times T_n$ is a maximal torus in $G_1 \times \cdots \times G_n$, and so its image $T_1 \cdots T_n$ in G is maximal (17.20). Therefore, $T_1 \cdots T_n$ equals T.   □

THEOREM 17.87. *Let G be a group variety over a field k, and let T_1 and T_2 be maximal tori in G. Then T_1 and T_2 are conjugate by an element of $G(k')$ for some finite separable field extension k' of k, i.e., $(T_2)_{k'} = g \cdot (T_1)_{k'} \cdot g^{-1}$ for some $g \in G(k')$.*

PROOF. Consider the functor

$$X \colon R \rightsquigarrow \{g \in G(R) \mid gT_{1R}g^{-1} = T_{2R}\}.$$

When we let G act on itself by inner automorphisms, X is represented by a closed subscheme of G (see 1.80). According to Theorem 17.10, there exists a $g \in X(k^a)$. The map $h \mapsto gh \colon N_G(T_1)_{k^a} \to X_{k^a}$ is an isomorphism of functors of k^a-algebras, and hence of k^a-schemes. Therefore X is smooth and nonempty, and so $X(k') \neq \emptyset$ for some finite separable field extension k' of k (see A.48). □

In particular, any two maximal tori in a group variety G over a separably closed field k are conjugate by an element of $G(k)$.

EXAMPLE 17.88. The torus $\mathbb{D}_n$ is maximal in GL_n because $\mathbb{D}_n$ is its own centralizer in GL_n. To see this, let E_{ij} denote the matrix with a 1 in the ijth position and zeros elsewhere, and let $A \in M_n(R)$ for some k-algebra R. If

$$(I + E_{ii})A = A(I + E_{ii})$$

then $a_{ij} = 0 = a_{ji}$ for all $j \neq i$, and so A must be diagonal if it commutes with the matrices $I + E_{ii}$.

EXAMPLE 17.89. Let V be a vector space of dimension n over k. The conjugacy classes of maximal tori in GL_n are in natural one-to-one correspondence with the isomorphism classes of étale k-algebras of degree n.

To see this, let T be a maximal torus in GL_V. As a T-module, V decomposes into a direct sum of simple T-modules, $V = \bigoplus_i V_i$, and the endomorphism ring of V_i (as a T-module) is a separable extension k_i of k such that $\dim_{k_i} V_i = 1$ (12.30). Now $\prod_i k_i$ is an étale k-algebra of degree n, and $T(k) = \prod_i k_i^\times$.

Conversely, let $A = \prod_i k_i$ be an étale k-algebra of degree n. The choice of a nonzero element of V defines on V the structure of a free A-module of rank 1. Then $V = \bigoplus_i V_i$ with V_i a one-dimensional k_i-vector space. The automorphisms of V preserving this gradation and commuting with the action of A form a maximal subtorus T of GL_V such that $T(k) = A^\times = \prod_i k_i^\times$.

In particular, the split maximal tori in GL_V are in natural one-to-one correspondence with the decompositions $V = V_1 \oplus \cdots \oplus V_n$ of V into a direct sum of one-dimensional subspaces. From this it follows that they are all conjugate. The (unique) conjugacy class of split maximal tori corresponds to the étale k-algebra $k \times \cdots \times k$ (n copies).

Cartan subgroups

Let G be a connected group variety. Recall (17.43, 17.44) that the Cartan subgroups of G are the centralizers of maximal tori of G, and that they are smooth, connected, and nilpotent.

PROPOSITION 17.90. *Let X be a semisimple element of $\mathfrak{g}$. Then every maximal torus of $C_G(X)$ is maximal in G.*

PROOF. Let $H = C_G(X)^\circ$ – it is a smooth connected group variety (17.76). Its Lie algebra contains X, and so H is not unipotent (17.75). Therefore H contains nontrivial maximal tori (17.81) – let T be one. The centralizer $C = C_H(T)$ of T in H is a Cartan subgroup of H, and its Lie algebra $\mathfrak{c}$ contains X (10.31). As C is smooth, connected, and nilpotent, $Z(C)_s$ is the only maximal torus in C and the quotient $C/Z(C)_s$ is unipotent (16.47). Therefore $T = Z(C)_s$ and C/T is unipotent, which implies that $X \in \mathfrak{t}$ (see 17.75). Let T' be a maximal torus T' of G containing T. Then T' centralizes X, and so $T' \subset H$. Thus $T = T'$.   □

THEOREM 17.91. *Every connected group variety G is generated by its Cartan subgroups.*

PROOF. If G is nilpotent, then $Z(G)_s$ is a maximal torus (16.47), and so G itself is a Cartan subgroup. We prove the general case by induction on $\dim(G)$. Suppose first that k is infinite. If $\mathfrak{g}_{k^a}$ contains a noncentral semisimple element, then G is generated by the groups $C_G(X)^\circ$ as X runs over the noncentral semisimple elements of $\mathfrak{g}$ because $\mathrm{Lie}(G)$ is spanned by their Lie algebras (17.79). Each $C_G(X)^\circ$ is a proper algebraic subgroup of G whose maximal tori are maximal in G (see 17.90). The induction hypothesis allows us to assume that each group $C_G(X)^\circ$ is generated by its Cartan subgroups, and it follows that the same is true of G. The proof of the theorem when k is finite requires a different argument, which we omit (Borel and Springer 1968, 2.9).   □

COROLLARY 17.92. *Let G be a connected group variety over an infinite field. If the Cartan subgroups of the maximal tori in G are unirational over k, then G is unirational over k (and $G(k)$ is dense in G if k is infinite).*

PROOF. The hypothesis implies that there exists a dominant morphism $C_1 \times \cdots \times C_m \to G$ with the C_i unirational, and so G is unirational. □

THEOREM 17.93. *Let G be a connected group variety over k. Then G is unirational over k (and $G(k)$ is dense in G if k is infinite) under each of the following hypotheses:*

  (a) *k is perfect;*

  (b) *G is reductive.*

PROOF. (a) The Cartan subgroups are smooth, connected, and nilpotent. As k is perfect, they are products of tori with connected unipotent groups (16.48). All tori are unirational (12.64), and all connected unipotent groups over perfect fields are unirational (14.66).

    (b) According to (17.84), the Cartan subgroups of a reductive group are tori, which are unirational over k (see 12.64). □

REMARK 17.94. (a) Let k be a perfect field. Then the formation of $R_u(G)$ commutes with extension of the base field, and so there is an exact sequence

$$e \to R_u(G) \to G \to G/R_u(G) \to e$$

with $G/R_u(G)$ reductive. Using the exact sequence, it possible to deduce the unirationality of G from that of $G/R_u(G)$.

    (b) There exist tori, even over fields of characteristic zero, that are not rational. However, a connected group variety over a perfect field is rational if its "generic torus" is rational (Voskresenskiĭ 1998, p. 42).

k. Algebraic groups over finite fields

Let X be an affine scheme over $\mathbb{F}_q$. The $\mathbb{F}_q$-algebra homomorphism $f \mapsto f^q : \mathcal{O}(X) \to \mathcal{O}(X)$ defines a Frobenius morphism $\sigma : X \to X$. If $X \subset \mathbb{A}^n$, then σ acts on $X(\mathbb{F})$ as $(a_1, \ldots) \mapsto (a_1^q, \ldots)$.

DEFINITION 17.95. Let G be a connected group variety over $\mathbb{F}$ (an algebraic closure of $\mathbb{F}_p$). A ***Steinberg endomorphism*** of G is an endomorphism F such that some power of F is equal to the Frobenius endomorphism of G defined by a model of G over a finite subfield of $\mathbb{F}$.

    In other words, relative to some model G_0 of G over $\mathbb{F}_q \subset \mathbb{F}$ and embedding $G_0 \hookrightarrow \mathrm{GL}_n$, a power F^m of F acts as $(a_1, \ldots) \mapsto (a_1^q, \ldots)$. Let F be a Steinberg endomorphism of G. Then the set G^F of fixed points of F acting on $G(\mathbb{F})$ is finite, and $G(\mathbb{F}) = \bigcup_{m \geq 1} G^{F^m}$ (because this is true of a Frobenius endomorphism).

THEOREM 17.96. *Let $F\colon G \to G$ be a Steinberg endomorphism of a connected group variety G over $\mathbb{F}$. Then the morphism $g \mapsto g \cdot F(g^{-1})\colon G \to G$ is surjective.*

PROOF. Let G act on itself (on the right) by $(x,g) \mapsto g^{-1} \cdot x \cdot F(g)$. There exists an $x \in G(\mathbb{F})$ such that the orbit O_x through x is closed (1.66). If we can show that $\dim(O_x) = \dim(G)$, then $O_x = G$ (because G is smooth and connected); then $e \in O_x$, and so $G = O_e$, which is the required statement. For this, it suffices to show that the fibre of the orbit map $\mu_x\colon G \to O_x$ over x is finite (A.72), and even that the equation $g^{-1}xF(g) = x$ has only finitely many solutions with g in $G(\mathbb{F})$. Rewrite this equation as $f(g) = g$, where $f(g) = xF(g)x^{-1}$. Because F is a Steinberg endomorphism, some multiple F^m of it is a Frobenius endomorphism fixing x. A direct calculation shows that $f^m(g) = yF^m(g)y^{-1}$ with $y = xF(x)\cdots F^{m-1}(x)$, and then that $f^{mm'}(g) = y^{m'}F^{mm'}(g)y^{-m'}$ for every $m' \in \mathbb{N}$. Take m' to be the order of y in $G(\mathbb{F})$. Then $f^{mm'}(g) = F^{mm'}(g)$, and so $f^{mm'}(g) = g$ has only finitely many solutions in $G(\mathbb{F})$; a fortiori, $f(g) = g$ has only finitely many solutions in $G(\mathbb{F})$. □

COROLLARY 17.97. *Let G be a connected group variety over a finite field k, and let $F\colon G \to G$ be the Frobenius map relative to k. Then the morphism $g \mapsto g \cdot F(g^{-1})\colon G \to G$ is surjective.*

PROOF. The proposition shows that the morphism becomes surjective after passage to $\mathbb{F}$, and hence is surjective. □

The corollary fails for nonconnected groups. For example, let $G = \mu_n$ with $n = q - 1$. Then $g \cdot F(g^{-1}) = g \cdot g^{-q} = e$ for all $x \in \mu(k^a)$.

COROLLARY 17.98. *For a connected group variety G over a finite field k, the cohomology group $H^1(k, G) = 1$.*

PROOF. Let $\Gamma = \mathrm{Gal}(k^s/k)$. Then Γ is generated (as a topological group) by the element $\sigma\colon a \mapsto a^q$, $q = |k|$. Let $f\colon \Gamma \to G(\mathbb{F})$ be a crossed homomorphism. Then σ acts on $G(\mathbb{F})$ as F, and so there exists a $g \in G(\mathbb{F})$ such that $g^{-1} \cdot \sigma g = f(\sigma)$. Thus f agrees on σ with the principal crossed homomorphism defined by g. It follows that the two crossed homomorphisms agree on all powers of σ, and hence on $\mathrm{Gal}(k^s/k)$ (by continuity). □

The corollary fails already for the disconnected group $G = \mathbb{Z}/n\mathbb{Z}$, $n > 1$, because

$$H^1(k, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z}) \quad \text{(continuous homomorphisms)}$$
$$\simeq \mathbb{Z}/n\mathbb{Z}.$$

PROPOSITION 17.99. *Let G be a connected group variety over k. There exists a Borel pair (B, T) in G, and any two Borel pairs are conjugate by an element of $G(k)$.*

PROOF. Let B be a Borel subgroup of G_{k^a}. Then $\sigma B = h B h^{-1}$ for some $h \in G(k^a)$. According to (17.96), $h = g^{-1} \cdot \sigma g$ for some $g \in G(k^a)$. Now gBg^{-1} is fixed by σ, and so it arises from a subgroup B_0 of G. This is a Borel subgroup in G. The existence of a maximal torus in B is proved similarly.

Let (B, T) and (B_1, T_1) be Borel pairs in G. Then $(B_1, T_1)_{k^a} = g(B, T)_{k^a} g^{-1}$ for some $g \in G(k^a)$. Now $g^{-1} \cdot \sigma g \in T(k^a)$, and so $g^{-1} \cdot \sigma g = t \cdot \sigma t^{-1}$ for some $t \in T(k^a)$. Then $gt \in G(k)$ and $(B_1, T_1) = gt(B, T)t^{-1}g^{-1}$. $\qquad\square$

In particular, every reductive group over a finite field is quasi-split.

ASIDE 17.100. Let $F: G \to G$ be a Steinberg endomorphism of a connected group variety G over $\mathbb{F}$. Then the set G^F of fixed points of F acting on $G(\mathbb{F})$ is a finite group. A group arising in this way from a semisimple G is called a ***finite group of Lie type.*** If the group variety G is almost-simple and simply connected, then the finite group G^F is simple modulo its centre except in exactly eight cases (Malle and Testerman 2011, 24.17). Every nonabelian finite simple group is a quotient of a finite group of Lie type, an alternating group, the Tits group, or one of 26 sporadic groups.

NOTES. Corollary 17.97 was first proved in Lang 1956. Each of the three statements 17.96, 17.97, 17.98 is referred to as Lang's theorem. The above proof of Theorem 17.96 is from Müller 2003.

l.   Split algebraic groups

Recall (6.33) that a solvable algebraic group G over k is split if it has a subnormal series such that each quotient is isomorphic either to $\mathbb{G}_a$ or to $\mathbb{G}_m$. Extensions of split solvable groups are obviously split, and quotients of split solvable groups are split because nontrivial quotients of $\mathbb{G}_a$ and $\mathbb{G}_m$ are isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$ (Exercise 14-3). A split solvable group G is trigonalizable (16.52), and the canonical exact sequence $e \to G_u \to G \to D \to e$ splits (16.26, 16.29).

DEFINITION 17.101. A group variety over k is ***split*** if it has a Borel subgroup that is split (as a solvable group).

17.102. A split group variety is quasi-split, but there exist quasi-split groups that are not split, for example, the special orthogonal group of $x_1^2 + x_2^2 + x_3^2 - x_4^2$ over $k = \mathbb{R}$.

17.103. Every quotient of a split group variety is split because the image of a Borel subgroup is Borel (17.69) and a quotient of a split solvable group is split.

17.104. Clearly, a solvable group variety is split as a group variety if and only if it is split as a solvable algebraic group. For example, a torus is split as a group variety if and only if it is split as a torus. We shall see that a reductive algebraic group over k is split if and only if it has a split maximal torus (21.64).

THEOREM 17.105. *Let G be a group variety over a field k.*

(a) *If H is a split solvable subgroup of G and B is a split Borel subgroup, then $H \subset gBg^{-1}$ for some $g \in G(k)$.*

(b) *Any two split Borel subgroups of G are conjugate by an element of $G(k)$.*

(c) *If G is split, then any two split maximal tori are conjugate by an element of $G(k)$.*

PROOF. (a) As H is split solvable and G/B is complete, when we let H act on G/B by left multiplication, there is a fixed point $P \in (G/B)(k)$ (16.51). The inverse image of P in G is a B-torsor over k, which is trivial because B is split (16.55). Therefore $HgB \subset gB$ for some $g \in G(k)$, and so $H \subset gBg^{-1}$.

(b) This follows from (a) because all Borel subgroups of G have the same dimension (they do over k^a).

(c) Let T and T' be split maximal tori in G, and let B be a split Borel subgroup of G. According to (a), $gTg^{-1} \subset B$ and $g'T'g'^{-1} \subset B$ for some $g, g' \in G(k)$, and so we may suppose that T and T' are both contained in B. Now we can apply (16.29d) to the extension

$$e \to B_u \to B \to B/B_u \to e.$$

$\square$

NOTES. The original source for most of the rationality theorems in the last four sections is Borel and Springer 1966, 1968.

Exercises

Except for 17-7, the exercises are from Springer 1998, Chapter 6.

EXERCISE 17-1. Prove the statements in Example 17.8 (this may require using results on quadratic and alternating forms from Jacobson 1985, Chapter 6).

In the remaining exercises, G is a connected group variety over an algebraically closed field.

EXERCISE 17-2. Let H be a subgroup variety of G containing a maximal torus T. Show that $N_G(H) \subset H^{\circ} \cdot N_G(T)$.

EXERCISE 17-3. Call an $s \in G(k)$ **regular** if the multiplicity of 1 as a root of the characteristic polynomial of the linear map $\mathrm{Ad}(s) \colon \mathfrak{g} \to \mathfrak{g}$ is a minimum.

(a) Show that the regular elements form a nonempty open subset of $G(k)$.

(b) Show that an element s is regular if and only if its semisimple part is regular.

(c) Show that a semisimple element s is regular if and only if its centralizer has minimum dimension (use that $\mathrm{Lie}(G^s) = \mathrm{Lie}(G)^s$).

(d) Show that a semisimple element s is regular if and only if $C_G(s)^{\circ}$ is a Cartan subgroup (use 16.42 and 17.36).

EXERCISE 17-4. (a) Show that a maximal nilpotent subgroup variety C of G such that $C = N_G(C)^\circ$ is a Cartan subgroup.

(b) Let A be a maximal nilpotent abstract subgroup of $G(k)$ such that every subgroup of finite index in A has finite index in its normalizer. Show that $A = C(k)$ for a Cartan subgroup C. [This is the group-theoretic characterization of Cartan subgroups; Chevalley 1956–58, 7.1. For the proof, show that the Zariski closure of an abstract nilpotent subgroup of $G(k)$ is nilpotent, and deduce that A is closed and satisfies the condition in (a).]

EXERCISE 17-5. Let $x = x_s x_u$ be the Jordan decomposition of $x \in G(k)$. Show that $x \in C_G(x_s)^\circ(k)$.

EXERCISE 17-6. Assume that $\mathrm{char}(k) \neq 2$, and let $G = \mathrm{SO}_n$ with $n \geq 3$. Show that there exist semisimple elements in $G(k)$ whose centralizer is not connected (consider elements of order 2; cf. 17.51). (By contrast, Steinberg showed that the centralizers of semisimple elements in *simply connected* semisimple algebraic groups are connected; see Humphreys 1995, 2.11.)

EXERCISE 17-7. (Steinberg 1968, 7.2). Let (B, T) be a Borel pair in G, and let $C = C_G(T)$ (so $C \subset B$ 17.39). Let $\alpha \colon G \to G$ be a surjective homomorphism such that $\alpha(B) = B$.

(a) Consider the regular map
$$\phi_b \colon G \times B \to G, \quad \phi_b(x, c) = (\alpha x) b^{-1} c x^{-1} b.$$

Show that $\phi_b(e, e) = e$, and that the image of $(d\phi_b)_{(e,e)}$ in $\mathfrak{g}$ contains both $\mathfrak{b}$ and $(\mathrm{Ad}(b)d\alpha - 1)\mathfrak{g}$.

(b) Show that there exists a $b \in B$ such that $\alpha(T) = b^{-1}Tb$, and that the linear endomorphism of $\mathfrak{g}/\mathfrak{b}$ induced by $\mathrm{Ad}(b)d\alpha$ does not have 1 as an eigenvalue (first choose b to satisfy the first condition and then modify it by an element of T).

(c) Show that, if b is as in (b), then ϕ_b is dominant.

(d) Show that ϕ_e is surjective.

(e) Deduce from (c) that every surjective endomorphism of G fixes a Borel subgroup.

The Geometry of Algebraic Groups

In this chapter, following Iversen 1976, we show that, by using a little algebraic geometry, it is possible to prove results about algebraic groups that are normally deduced only from the classification theorems. Those unfamiliar with the theory of line bundles may skip the details. Recall that all algebraic groups are affine over a base field k.

a. Central and multiplicative isogenies

In this section, G' and G are connected group varieties. Recall (2.23, 6.6) that an isogeny $\varphi: G' \to G$ is a surjective homomorphism with finite kernel. The degree of φ is the order of its kernel.

DEFINITION 18.1. An isogeny is ***central*** (resp. ***multiplicative***[1]) if its kernel is central (resp. of multiplicative type).

A multiplicative isogeny is central by rigidity (12.38). Conversely, if G' is reductive, then a central isogeny $\varphi: G' \to G$ is multiplicative because the centre of a reductive group is of multiplicative type (17.62).

An isogeny of degree prime to the characteristic has étale kernel (11.31), and so it is central (12.39). In nonzero characteristic, there exist noncentral isogenies, for example, the Frobenius map (2.24). The isogenies in nonzero characteristic that behave as the isogenies in characteristic zero are the multiplicative isogenies.

PROPOSITION 18.2. *A composite of multiplicative isogenies is multiplicative.*

PROOF. Let φ_1 and φ_2 be composable multiplicative isogenies. Then

$$e \to \operatorname{Ker}(\varphi_1) \to \operatorname{Ker}(\varphi_2 \circ \varphi_1) \xrightarrow{\varphi_1} \operatorname{Ker}(\varphi_2) \to e$$

is exact (Exercise 5-8). Corollary 12.41 shows that $\operatorname{Ker}(\varphi_2 \circ \varphi_1)$ is central, and hence of multiplicative type (12.22). □

[1]Iversen 1976 says central.

EXAMPLE 18.3. Let k be a field of characteristic 2. Let $G = SO_{2n+1}$ be the group variety attached to the quadratic form $x_0^2 + \sum_{i=1}^{n} x_i x_{n+i}$ on k^{2n+1} and $G' = Sp_{2n}$ that attached to the skew-symmetric form $\sum_{i=1}^{n} (x_i x'_{n+i} - x_{n+i} x'_i)$ on k^{2n}. These are semisimple algebraic groups, and the diagonal tori in each are split maximal tori. The group G fixes the basis vector e_0 in k^{2n+1} (only because the characteristic is 2) and hence acts on $k^{2n+1}/ke_0 \simeq k^{2n}$. From this isomorphism, we get an isogeny from G to G' that restricts to an isomorphism on the diagonal maximal tori. It is not central because the centre of a reductive group is contained in every maximal torus (because of 17.84).

REMARK 18.4. Borel and Tits (1972) call a homomorphism $\varphi \colon G \to G'$ of group varieties **quasi-central** if the kernel of $\varphi(k^a)$ is central. This amounts to requiring that the commutator map $G(k^a) \times G(k^a) \to G(k^a)$ factor through $\varphi(G(k^a)) \times \varphi(G(k^a))$. If this factorization takes place on the level of group varieties, then they say that φ is central (same article 2.2). This agrees with our definition (12.44). A homomorphism φ of group varieties is central if and only if it is quasi-central and the kernel of $\mathrm{Lie}(\varphi)$ is contained in the centre of $\mathrm{Lie}(G)$, i.e., if and only if $\varphi(k^a)$ and $\mathrm{Lie}(\varphi)$ are both central (Borel and Tits 1972, 2.15).

b.   The universal covering

DEFINITION 18.5. A connected group variety G is **simply connected** if every multiplicative isogeny $G' \to G$ of connected group varieties is an isomorphism.

PROPOSITION 18.6. *Let G be a simply connected connected group variety over k, and let $\varphi \colon G' \to G$ be a surjective homomorphism with finite kernel of multiplicative type (G' not necessarily smooth or connected). Then φ admits a section in each of the following two cases:*

(a) *k is perfect, i.e., $k = k^p$;*
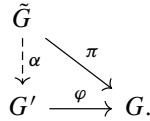
(b) *G is perfect, i.e., $G = \mathcal{D}G$.*

PROOF. (a) Suppose that k is perfect. Then $(G')^{\circ}_{\mathrm{red}}$ is a connected subgroup variety of G', and $(G')^{\circ}_{\mathrm{red}} \xrightarrow{\varphi} G$ is a multiplicative isogeny, and hence an isomorphism. The inverse of this isomorphism is the required section.

(b)[2] We may suppose that G' is connected, and hence that the kernel N of φ is central (12.38). Any two sections of φ_R over a k-algebra R differ by a homomorphism $G_R \to N_R$, which is trivial because G is perfect (6.19d). Hence the sections are equal. We know from (a) that φ has a section over a purely inseparable extension k' of k, which we may take to be finite. The two inverse images of s over $k' \otimes_k k'$ are both sections of $\varphi_{k' \otimes_k k'}$, and hence are equal. By flat descent (A.81), this implies that s arises from a section over k.   □

---

[2]I thank Brian Conrad for this argument.

DEFINITION 18.7. A ***universal covering*** of a connected group variety G is a multiplicative isogeny $\tilde{G} \to G$ with $\tilde{G}$ a simply connected connected group variety. We also call it the ***simply connected covering***. When the universal covering exists, its kernel is called the ***fundamental group*** $\pi_1(G)$ of G.

PROPOSITION 18.8. *Let $\pi: \tilde{G} \to G$ be a universal covering of a connected group variety G over k. Assume that either k or G is perfect, and let $\varphi: G' \to G$ be a multiplicative isogeny of connected group varieties. Then there exists a unique homomorphism $\alpha: \tilde{G} \to G$ such that $\pi = \varphi \circ \alpha$.*

$$\begin{array}{ccc} \tilde{G} & & \\ {\scriptstyle\alpha}\downarrow & \searrow^{\pi} & \\ G' & \xrightarrow{\varphi} & G. \end{array}$$

In particular, $(\tilde{G}, \pi)$ is uniquely determined up to a unique isomorphism.

PROOF. As $\tilde{G}$ is smooth and connected, it has no nontrivial finite quotient. It follows that if G is perfect, i.e., has no nontrivial commutative quotient, then the same is true of $\tilde{G}$.

The map $G' \times_G \tilde{G} \to \tilde{G}$ is surjective with finite kernel of multiplicative type. Therefore it has a section (18.6). The composite α of this section with the map $G' \times_G \tilde{G} \to G'$ is such that $\pi = \varphi \circ \alpha$.

If $\beta: \tilde{G} \to G'$ is a second homomorphism such that $\pi = \varphi \circ \beta$, then $g \mapsto \alpha(g)/\beta(g)$ maps $\tilde{G}$ to $\mathrm{Ker}(\varphi)$, and is therefore trivial (because $\tilde{G}$ is smooth and connected). Hence $\alpha = \beta$. $\qquad\square$

c. Line bundles and characters

In this section, G is a connected group variety over k and $X(G) = \mathrm{Hom}(G, \mathbb{G}_m)$. We begin with some definitions from Iversen 1976.

18.9. A principal $\mathbb{G}_m$-bundle on an algebraic variety is a right $\mathbb{G}_m$-torsor for the Zariski topology. From a line bundle, we get a principal $\mathbb{G}_m$-bundle by removing the zero section, and every $\mathbb{G}_m$-bundle arises in this way from an essentially unique line bundle. The isomorphism classes of line bundles on a variety X form a group, called the Picard group $\mathrm{Pic}(X)$ of X (see A.77).

18.10. Let $G \times X \to X$ be an action of G on a variety X over k. A G-homogeneous principal $\mathbb{G}_m$-bundle on X is a principal $\mathbb{G}_m$-bundle $E \to X$ together with a left action of G on E commuting with the action of $\mathbb{G}_m$ and such that $E \to X$ is G-equivariant. A line bundle arising from such a $\mathbb{G}_m$-bundle is said to be G-homogeneous.

18.11. Let $\pi: X \to S$ be a G-torsor for the Zariski topology. The functor $L \rightsquigarrow \pi^{-1}L$ is an equivalence from the category of line bundles on S to the category of G-homogeneous line bundles on X.[3]

---

[3]If X is only locally trivial for the flat topology, then the line bundle on S corresponding to a G-homogeneous line bundle on X is only locally trivial for the flat topology on S, but this implies that it is locally trivial for the Zariski topology by descent theory.

18.12. Let V be a finite-dimensional vector space over k. The natural projection $V^{\vee} \smallsetminus 0 \to \mathbb{P}(V)$ is a principal $\mathbb{G}_m$-bundle on $\mathbb{P}(V)$ with a natural structure of an SL_V-homogeneous bundle (Iversen 1976, 1.2). The associated line bundle is denoted L_{univ}.

18.13. A homomorphism $f : G \to \mathrm{PGL}_V$ defines an action of G on $\mathbb{P}(V)$. A lifting of f to GL_V defines the structure of a G-homogeneous line bundle on L_{univ}. In this way, we get a one-to-one correspondence between the liftings of f to GL_V and such structures on L_{univ} (Iversen 1976, 1.3).

We now assume that G is split. Recall (17.101) that this means that G contains a Borel subgroup B that is split as a solvable algebraic group, which is automatically so if k is algebraically closed. In particular, B is trigonalizable (16.52). We let $T = B/B_u$. It is a split torus.

The map $\pi : G \to G/B$ is a B-torsor. Let χ be a character of B, and let B act on $G \times \mathbb{A}^1$ according to the rule

$$(g, x)b = (gb, \chi(b^{-1})x), \quad g \in G, \quad x \in \mathbb{A}^1, \quad b \in B.$$

This is a B-homogeneous line bundle on G, and we let $L(\chi)$ denote the corresponding line bundle on G/B (see 18.11). It is G-homogeneous for the natural action of G on G/B.

PROPOSITION 18.14. *The map $\chi \mapsto L(\chi)$ defines a bijection from $X(B)$ to the set of isomorphism classes of G-homogeneous line bundles on G/B.*

PROOF. Let L be a G-homogeneous line bundle on G/B. The point $\pi(e)$ is fixed for the action of B on G/B, and so B acts on the fibre of L at $\pi(e)$. This action defines a character χ_L of B, which depends only on the isomorphism class of L. The map $L \mapsto \chi_L$ is inverse to the map sending χ to the isomorphism class of $L(\chi)$. $\qquad\square$

Every character of B factors uniquely through T, and so $X(B) \simeq X(T)$. Therefore, we have a linear map

$$\chi \mapsto L(\chi) : X(T) \to \mathrm{Pic}(G/B).$$

This is called the ***characteristic map*** for G.

The basic fact we need is the following.

THEOREM 18.15. *With the above assumptions, the following sequence is exact:*

$$0 \to X(G) \to X(T) \to \mathrm{Pic}(G/B) \to \mathrm{Pic}(G) \to 0. \qquad (128)$$

The proof, being mainly algebraic geometry, is deferred to the last section of this chapter.

REMARK 18.16. From (18.14) we see that the image of $X(T)$ in $\mathrm{Pic}(G/B)$ consists of the line bundles that admit a G-homogeneous structure.

EXAMPLE 18.17. Let T be the diagonal maximal torus in $G = \mathrm{SL}_2$, and let B be the standard (upper triangular) Borel subgroup. The natural action of G on $\mathbb{A}^2$ defines an action of G on $\mathbb{P}^1$, and B is the stabilizer of the point $(1:0)$ in $\mathbb{P}^1$. The canonical line bundle L_{univ} on $\mathrm{SL}_2/B \simeq \mathbb{P}^1$ is equipped with an SL_2-action, and B acts on the fibre over $(1:0)$ through the character

$$\begin{pmatrix} z & x \\ 0 & z^{-1} \end{pmatrix} \mapsto z^{-1}.$$

In this case the characteristic map $X(T) \to \mathrm{Pic}(\mathrm{SL}_2/B)$ is an isomorphism and $X(\mathrm{SL}_2) = 0 = \mathrm{Pic}(\mathrm{SL}_2)$ (see 20.24 and 20.25 for direct proofs of these equalities).

PROPOSITION 18.18. *Let* $\varphi: G' \to G$ *be a surjective homomorphism of split connected group varieties with kernel of multiplicative type. Then there is an exact sequence*

$$0 \to X(G) \to X(G') \to X(\mathrm{Ker}(\varphi)) \to \mathrm{Pic}(G) \to \mathrm{Pic}(G') \to 0. \qquad (129)$$

PROOF. Let B be a Borel subgroup of G, and let B' be its inverse image in G'. Then B' is solvable, and $G/B \simeq G'/B'$, and so B' is a Borel subgroup of G'. The columns in the following commutative diagram are the exact sequences in (18.15) for (G, B) and (G', B'):

$$
\begin{array}{ccccccc}
& 0 & & 0 & & & \\
& \downarrow & & \downarrow & & & \\
& X(G) & \longrightarrow & X(G') & & & \\
& \downarrow & & \downarrow & & & \\
0 \longrightarrow & X(T) & \longrightarrow & X(T') & \longrightarrow & X(\mathrm{Ker}\,\varphi) & \longrightarrow 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \longrightarrow & \mathrm{Pic}(G/B) & \overset{\simeq}{\longrightarrow} & \mathrm{Pic}(G'/B') & \longrightarrow & 0 & \longrightarrow 0 \\
& \downarrow & & \downarrow & & & \\
& \mathrm{Pic}(G) & \longrightarrow & \mathrm{Pic}(G') & & & \\
& \downarrow & & \downarrow & & & \\
& 0 & & 0 & & &
\end{array}
$$

Now the snake lemma gives the required exact sequence. $\qquad\square$

PROPOSITION 18.19. *Let* G *be a split connected group variety. If* $X(G) = 0$ *and* $\mathrm{Pic}(G) = 0$, *then* G *is simply connected.*

PROOF. Let $\varphi\colon G' \to G$ be a multiplicative isogeny of connected group varieties. In the exact sequence in (129)

$$X(G) \to X(G') \to X(\operatorname{Ker}\varphi) \to \operatorname{Pic}(G),$$

the groups $X(G)$ and $\operatorname{Pic}(G)$ are zero, the group $X(\operatorname{Ker}\varphi)$ is finite, and the group $X(G')$ is torsion-free (because G' is smooth and connected). Therefore $X(\operatorname{Ker}\varphi) = 0$, which implies that $\operatorname{Ker}(\varphi) = e$.   □

EXAMPLE 18.20. The algebraic group SL_2 is simply connected (18.17).

d.   Existence of a universal covering

The existence of a universal covering $\tilde{G} \to G$ for a semisimple group G is usually deduced from the classification theorems (including the existence and isogeny theorems) for reductive groups. But the proof of such a basic fact should not require knowing the whole theory. In the rest of this section we sketch the proof in Iversen 1976.

   Throughout this section, G is a split connected group variety and B is a Borel subgroup of G that is split as a solvable algebraic group.

LEMMA 18.21. *The group* $\operatorname{Pic}(G/B)$ *is finitely generated, and its generators can be chosen to be line bundles* L *with* $\Gamma(G/B, L) \neq 0$.

PROOF. For a smooth algebraic variety, the Picard group can also be defined as the group of Weil divisors modulo principal divisors (A.78). It follows from Proposition 13.52 that G/B contains an open subvariety U isomorphic to $\mathbb{A}^n$ (see the proof of 17.65). Because $k[T_1, \ldots, T_n]$ is a unique factorization domain (CA 4.10), the Picard group of $\mathbb{A}^n$ is zero. It follows that the group of Weil divisor classes on G/B is generated by those with support on the boundary $\bar{U} \smallsetminus U$, which is a finite union of proper closed subvarieties. This implies the statement.   □

   See Iversen 1976 for an explicit description of $\operatorname{Pic}(G/B)$.

PROPOSITION 18.22 (IVERSEN 1976, 2.7). *There exists a multiplicative isogeny* $\tilde{G} \to G$ *with* $\tilde{G}$ *a connected group variety such that* $\operatorname{Pic}(\tilde{G}) = 0$.

PROOF. Let $\varphi\colon G' \to G$ be a multiplicative isogeny. Because $\operatorname{Pic}(G) \to \operatorname{Pic}(G')$ is surjective (18.18), it suffices to find a φ such that $\operatorname{Pic}(\varphi)$ is zero. Let B' be the inverse image of B in G', and consider the diagram

$$
\begin{array}{ccccc}
\operatorname{Pic}(G/B) & \longrightarrow & \operatorname{Pic}(G) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \\
X(B') \longrightarrow \operatorname{Pic}(G'/B') & \longrightarrow & \operatorname{Pic}(G'). & &
\end{array}
$$

After 18.21 and 18.16, it suffices to prove the following statement:

Let L be a line bundle on G/B with $\Gamma(G/B, L) \neq 0$; then there exists a φ such that the pull-back of L to G'/B' admits a G'-homogeneous structure.

Let $V = \Gamma(G/B, L)$. In the setting of 18.13, we have canonical maps $f: G \to \mathrm{PGL}_V$ and $t: G/B \to \mathbb{P}(V)$ such that $t^* L_{\mathrm{univ}} = L$. Let $\varphi: G' \to G$ denote the pull-back of the multiplicative isogeny $\mathrm{SL}_V \to \mathrm{PGL}_V$ along f. Because L_{univ} is an SL_V-homogeneous line bundle, its pull-back to G'/B' is a G'-homogeneous line bundle, as required. $\qquad\square$

COROLLARY 18.23. *The group* $\mathrm{Pic}(G)$ *is finite.*

PROOF. Let $\varphi: \tilde{G} \to G$ be as in Proposition 18.22. Then the exact sequence

$$X(\mathrm{Ker}(\varphi)) \to \mathrm{Pic}(G) \to \mathrm{Pic}(\tilde{G}) = 0$$

(see 18.18) shows that $\mathrm{Pic}(G)$ is finite. $\qquad\square$

COROLLARY 18.24. *If* G *is simply connected, then* $\mathrm{Pic}(G) = 0$.

PROOF. If G is simply connected, then the isogeny in Proposition 18.22 is an isomorphism, and so $\mathrm{Pic}(G) \simeq \mathrm{Pic}(\tilde{G}) = 0$. $\qquad\square$

THEOREM 18.25. *If* $X(G) = 0$, *then* G *admits a universal covering.*

PROOF. Let $\varphi: \tilde{G} \to G$ be as in Proposition 18.22. Because $\tilde{G}$ is smooth and connected, $X(\tilde{G})$ is torsion-free. Now the exact sequence in 18.18 shows that $X(\tilde{G}) = 0 = \mathrm{Pic}(\tilde{G})$, and so $\tilde{G}$ is simply connected (18.19). $\qquad\square$

COROLLARY 18.26. *If* $X(G) = 0$, *then* $\mathrm{Pic}(G) \simeq X(\pi_1 G)$.

PROOF. For the universal covering $\tilde{G} \to G$, the exact sequence in Proposition 18.18 becomes $0 \to X(\pi_1 G) \to \mathrm{Pic}(G) \to 0$. $\qquad\square$

REMARK 18.27. Let G be a connected group variety (not necessarily split) over k. If G splits over a separable extension of k and $X^*(G) = 0$, then G admits a universal covering. Indeed, Theorem 18.25 shows that G admits a universal covering over some finite Galois extension of k, and the uniqueness property of the universal covering shows that it descends to k. In particular, all semisimple algebraic groups admit universal coverings.

e. Applications

PROPOSITION 18.28. *An extension of algebraic groups*

$$e \to D \to G' \to G \to e$$

splits if (a) D *is of multiplicative type and (b)* G *is smooth, connected, and perfect, and* G_{k^a} *is simply connected.*

PROOF. Suppose first that D is a torus. From Proposition 18.18 applied to $G'_{k^a} \to G_{k^a}$, we have an exact sequence

$$X^*(G) \to X^*(G') \to X^*(D) \to \mathrm{Pic}(G_{k^a}).$$

As G_{k^a} is simply connected, $\mathrm{Pic}(G_{k^a}) = 0$ (see 18.24), and as G is perfect, $X^*(G) = 0$. Therefore the restriction map $X^*(G') \to X^*(D)$ is an isomorphism. As D is a central torus in G' and G'/D is perfect, the quotient $T = G'/\mathcal{D}G'$ is a torus (12.46). Consider the maps

$$D \to G' \to T.$$

The maps on the character groups

$$X^*(T) \to X^*(G') \to X^*(D)$$

are isomorphisms and so the homomorphism $D \to T$ is an isomorphism. This shows that the complex splits.

    In the general case, there is an exact sequence

$$e \to D' \to D \to D'' \to e$$

with D' a torus and D'' finite (12.24). This gives an exact sequence

$$\mathrm{Ext}^1(G, D'') \to \mathrm{Ext}^1(G, D) \to \mathrm{Ext}^1(G, D'),$$

and so it suffices to prove the proposition in the two cases (a) D is finite, and (b) D is a torus. The first case was proved in 18.6 and the second was proved in the above paragraph.   □

REMARK 18.29. The proposition applies to extensions of simply connected semisimple algebraic groups by groups of multiplicative type (21.50).

PROPOSITION 18.30. *Let G be a reductive algebraic group. If there exists a multiplicative isogeny $H \to G/RG$ with H perfect and H_{k^a} simply connected, then there is a multiplicative isogeny $RG \times H \to G$.*

PROOF. On pulling back the extension

$$e \to RG \to G \to G/RG \to e$$

by the map $H \to G/RG$, we get an exact sequence

$$e \to RG \to G' \to H \to e$$

and a multiplicative isogeny $G' \to G$. According to (18.28), the extension splits, and so $G' \approx RG \times H$.   □

PROPOSITION 18.31. *Let G be a semisimple algebraic group. Assume that there exists a multiplicative isogeny $\tilde{G} \to G$ with $\tilde{G}$ perfect and $\tilde{G}_{k^a}$ simply connected. For any torus D,*

$$\text{Hom}(\pi_1(G), D) \simeq \text{Ext}^1(G, D).$$

PROOF. Let $f: \pi_1(G) \to D$ be a homomorphism. Define $E(f)$ to be the cokernel of the homomorphism

$$x \mapsto (x, f(x^{-1})): \pi_1(G) \to \tilde{G} \times D.$$

Then $E(f)$ is an extension of G by D. On the other hand, let $h: G' \to G$ be an extension of G by D. Then $\pi: \tilde{G} \to G$ factors through h, say,

$$\tilde{G} \xrightarrow{f} G' \xrightarrow{h} G,$$

and the factorization is unique (cf. 18.7). Then f restricts to a map $\pi_1(G) \to D$. These operations are inverse.   □

f.   Proof of theorem 18.15

Recall (12.50) that we let $U(X) = \Gamma(X, \mathcal{O}_X^\times)/k^\times$ for X an algebraic variety over k. If G is a connected group variety, then $U(G) \simeq X(G)$ (see 12.49).

   Let H be a smooth connected algebraic group, let X be a smooth algebraic variety, and let $f: Y \to X$ be a right H-torsor over X for the Zariski topology. Fix a $y_0 \in Y(k)$ (assumed to exist), and let $i: H \to Y$ denote the map $h \mapsto hy_0$. A character χ of H defines an action of H on $Y \times \mathbb{G}_m$:

$$(y_0, g)h = (y_0 h, \chi(h^{-1})g), \quad y_0 \in Y, g \in \mathbb{G}_m, h \in H.$$

Then $X = Y/H$ and $L(\chi) \overset{\text{def}}{=} Y \times \mathbb{G}_m/H$ is a principal $\mathbb{G}_m$-bundle on X.

THEOREM 18.32. *The following sequence is exact:*

$$U(X) \to U(Y) \xrightarrow{U(i)} X(H) \xrightarrow{\chi \mapsto L(\chi)} \text{Pic}(X) \xrightarrow{\text{Pic}(f)} \text{Pic}(Y) \xrightarrow{\text{Pic}(i_y)} \text{Pic}(H).$$

PROOF (FOSSUM AND IVERSEN 1973, 3.1). Exactness at $X(H)$. An extension of χ to all of Y gives a global section of $L(\chi)$, and so the composite of the two maps is 0. Conversely, suppose that $L(\chi)$ admits a global section over X. The corresponding section over Y of the pull-back of $L(\chi)$ along f (which we may identify with $Y \times \mathbb{G}_m$) has the form $y \mapsto (y, t(y))$, where $t: Y \to \mathbb{G}_m$ satisfies $t(yh) = t(y)\chi(h^{-1})$. Substitute $y = y_0$ to obtain the desired extension of χ.

   Exactness at $\text{Pic}(X)$. Let L be a principal $\mathbb{G}_m$-bundle on X. If $L = L(\chi)$ for some $\chi \in X(H)$, it obviously has a section over Y. Conversely, suppose that f^*L has a section s. Interpret s as a map from Y to L, and consider the

map $a: Y \times H \to \mathbb{G}_m$ defined by $s(yh) = s(y)a(y,h)$. According to (12.50), a has the form $a(y,h) = b(y)\chi(h)$ with $b \in U(Y)$ and $\chi \in X(H)$. In sum, $s(yh) = s(y)b(y)\chi(h)$. Substituting $h = e$, one sees that b is the constant 1. The map $(y,z) \mapsto s(y)\chi(z)$ now induces an isomorphism $L \to L(\chi)$.

The proof of the exactness at $U(Y)$ and $\mathrm{Pic}(Y)$ is similarly straightforward.□

Now let G be a split connected group variety over k, and let B be a Borel subgroup of G. Then G is a B-torsor over G/B, which is locally split for the Zariski topology because B is split solvable (16.55). Hence we can apply (18.32) to the map $G \to G/B$. As $\mathrm{Pic}(B) = 0$ (16.56), in this case the exact sequence becomes

$$0 \to X(G) \to X(B) \to \mathrm{Pic}(G/B) \to \mathrm{Pic}(G) \to 0.$$

Because B is split solvable, it is trigonalizable (16.52). Let $T = B/B_u$. Then $X(B) = X(T)$, and the sequence becomes (128).

More generally, let P be a parabolic subgroup of G. In this case the exact sequence in (18.32) becomes

$$0 \to X(G) \to X(P) \to \mathrm{Pic}(G/P) \to \mathrm{Pic}(G) \to \mathrm{Pic}(P) \to 0$$

(Fossum and Iversen 1973, p. 276).

Exercises

EXERCISE 18-1. Let $\varphi: G \to G'$ be a homomorphism of connected group varieties. Show that the following conditions on φ are equivalent:

(a) φ is central[4];

(b) $\varphi(k^a)$ and $\mathrm{Lie}(\varphi)$ are both central;

(c) there exists a morphism $\kappa: \varphi(G) \times \varphi(G) \to G'$ such that

$$\kappa(\varphi(x), \varphi(y)) = xyx^{-1}y^{-1} \quad \text{all } x, y \in G(k^a).$$

---

[4] A homomorphism is **central** if its kernel is central.

Semisimple and Reductive Groups

This chapter contains generalities on semisimple and reductive groups. In particular, we explain how reductive groups are constructed from semisimple groups and groups of multiplicative type.

a. Semisimple groups

The radical

Let G be a connected group variety over k. Recall (6.44) that, among the connected normal solvable subgroup varieties of G there is a largest one, containing all others. This is the radical $R(G)$ of G. For example, if G is the algebraic subgroup of GL_{m+n} consisting of the invertible matrices $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix} \right)$ with A of size $m \times m$ and C of size $n \times n$, then $R(G)$ consists of the matrices of the form $\left(\begin{smallmatrix} aI_m & B \\ 0 & cI_n \end{smallmatrix} \right)$ with aI_m and cI_n nonzero scalar matrices. The quotient G/RG is the semisimple group $\mathrm{PGL}_m \times \mathrm{PGL}_n$.

PROPOSITION 19.1. *The formation of $R(G)$ commutes with separable algebraic field extensions.*

PROOF. Let k'/k be a finite separable extension. As $R(G)_{k'}$ is connected, normal, and solvable it is contained in $R(G_{k'})$. It suffices to prove they are equal when k' is Galois over k. By uniqueness, $R(G_{k'})$ is stable under the action of $\mathrm{Gal}(k'/k)$ on $G_{k'}$, and therefore arises from a subgroup variety H of G (see 1.54). Now $R(G)_{k'} \subset R(G_{k'}) = H_{k'}$, and so $R(G) \subset H$. But H is connected, normal, and solvable (1.36, 6.31), and so $R(G) = H$ by maximality. □

Semisimple algebraic groups

Recall (6.44) that an algebraic group over a field k is said to be semisimple if it is smooth and connected and G_{k^a} has trivial radical.

PROPOSITION 19.2. *Let G be a connected group variety over a perfect field k.*

(a) *If $R(G) = e$, then G is semisimple.*

(b) *The quotient $G/R(G)$ is semisimple.*

PROOF. (a) If $R(G) = e$, then $R(G_{k^a}) \overset{19.1}{=} R(G)_{k^a} = e$.

(b) Let N be the inverse image of $R(G/RG)$ in G. Then N is a normal algebraic subgroup of G, and it is an extension

$$e \to RG \to N \to R(G/RG) \to e$$

of smooth connected solvable algebraic groups. Therefore it is smooth, connected, and solvable (1.62, 5.59, 6.27), and so $RG = N$. Hence $R(G/RG) = e$, and G/RG is semisimple.   □

PROPOSITION 19.3. *Let G be a connected group variety over field k. If G is semisimple, then every smooth connected normal commutative algebraic subgroup is trivial; the converse is true if k is perfect.*

PROOF. Suppose that G is semisimple, and let H be a connected normal commutative subgroup variety of G. Then $H_{k^a} \subset R(G_{k^a}) = e$, and so $H = e$.

For the converse, suppose that k is perfect and that G is not semisimple. Then $R(G) \neq e$, and the last nontrivial term in the derived series for $R(G)$ is smooth, connected, and commutative (6.19b). It is normal in G because it is characteristic in $R(G)$ (see 6.19e). Hence G contains a nontrivial smooth connected normal commutative algebraic subgroup.   □

REMARK 19.4. If one of the conditions on the subgroup in Proposition 19.3 is dropped, then a semisimple group may have such an algebraic subgroup. Let $p = \mathrm{char}(k)$.

(a) The subgroup $\mathbb{Z}/2\mathbb{Z} = \{\pm I\}$ of SL_2 ($p \neq 2$) is smooth, normal, and commutative, but not connected.

(b) The subgroup μ_2 of SL_2 ($p = 2$) is connected, normal, and commutative, but not smooth.

(c) The subgroup $\mathbb{U}_2 = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}$ of SL_2 is smooth, connected, and commutative, but not normal.

(d) The subgroup $e \times \mathrm{SL}_2$ of $\mathrm{SL}_2 \times \mathrm{SL}_2$ is smooth, connected, and normal, but not commutative.

PROPOSITION 19.5. *Let G be an algebraic group over k, and let k' be a field containing k. Then G is semisimple if and only if $G_{k'}$ is semisimple.*

PROOF. Certainly G is smooth and connected if and only if $G_{k'}$ is, and so we may suppose that G is a connected group variety. By definition, G is semisimple if and only if G_{k^a} is semisimple, and so it suffices to prove the statement with k and k' both algebraically closed. The sufficiency is obvious because $R(G)_{k'} \subset$

$R(G_{k'})$. The necessity follows from a standard "spreading" argument. Let N be a nontrivial smooth connected normal commutative algebraic subgroup of $G_{k'}$. There exists a subfield k'' of k' finitely generated over k, say, $k'' = k(t_1, \ldots, t_n)$, such that N is defined (as an algebraic subgroup of G) over k''. Now G and N extend to smooth group schemes $\mathcal{G}$ and $\mathcal{N}$ over an open subscheme $U = \mathrm{Spm}(A)$ of $\mathrm{Spm}(k[t_1, \ldots, t_m])$. For some maximal ideal $\mathfrak{m}$ in A, the specialization $\mathcal{N}_{\mathfrak{m}} = \mathcal{N} \otimes_A \kappa(\mathfrak{m})$ of $\mathcal{N}$ to $\kappa(\mathfrak{m}) = k$ will be a nontrivial smooth connected normal commutative algebraic subgroup of $\mathcal{G}_{\kappa(\mathfrak{m})} = G$. □

EXAMPLE 19.6. Let $G = \mathrm{SL}_n$, and let $n = mp^r$ with p the characteristic exponent of k and m prime to p. Then $Z(G) = \mu_n$, $Z(G)^{\circ} = \mu_{p^r}$, $Z(G)_{\mathrm{red}} = \mu_m$, and $R(G) = Z(G)^{\circ}_{\mathrm{red}} = e$.

DEFINITION 19.7. An algebraic group over k is **simple** (resp. **almost-simple**) if it is semisimple and noncommutative, and every proper normal algebraic subgroup is trivial (resp. finite). It is **geometrically simple** (resp. **almost-simple**) if it is almost-simple (resp. simple) and remains so over k^{a}.

For example, SL_n is almost-simple and $\mathrm{PSL}_n = \mathrm{SL}_n / \mu_n$ is simple for $n > 1$. In Chapter 23 below, we show that every almost-simple algebraic group over a separably closed field is isogenous to one of the algebraic groups in the four families 2.10(a), 2.10(b), 2.10(c), 2.10(d), or to one of five exceptional algebraic groups.

DEFINITION 19.8. An algebraic group is **pseudo-simple** (resp. **almost pseudo-simple**) if it is smooth, connected, and noncommutative, and every proper normal algebraic subgroup is trivial (resp. finite).

NOTES. There is considerable disagreement in the literature concerning these terms. While Borel 1991, IV, 14.10, writes "almost simple" for our "almost-simple", Springer 1998, 8.1.12, writes "quasi-simple", and Conrad et al. 2015 write "simple". A geometrically almost-simple group is often said to be absolutely almost-simple. Definition 19.8 is from Tits 1993, II; that in Conrad et al. 2015, 3.1.1, differs.

b. Reductive groups

The unipotent radical

Let G be a connected group variety over k. Recall (6.46) that, among the connected normal unipotent subgroup varieties of G there is a largest one, containing all others. This is the unipotent radical $R_u(G)$ of G. For example, if G is the algebraic subgroup of GL_{m+n} consisting of the invertible matrices $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix} \right)$ with A of size $m \times m$ and C of size $n \times n$, then $R_u(G)$ consists of the matrices of the form $\left(\begin{smallmatrix} I_m & B \\ 0 & I_n \end{smallmatrix} \right)$. The quotient $G / R_u(G)$ is the reductive group $\mathrm{GL}_m \times \mathrm{GL}_n$.

PROPOSITION 19.9. *The formation of $R_u(G)$ commutes with separable algebraic field extensions.*

PROOF. The proof is the same as for $R(G)$ (see 19.1).   □

Reductive algebraic groups

Recall (6.46) that an algebraic group G over a field k is said to be reductive if it is smooth and connected and the unipotent radical of G_{k^a} is trivial. The centre $Z(G)$ of a reductive group G is of multiplicative type, and $R(G)$ is the largest subtorus of $Z(G)$; the formation of $R(G)$ commutes with all extensions of the base field, and $G/R(G)$ is semisimple (17.62). Note that the centre of a reductive group need be neither smooth nor connected (19.6).

PROPOSITION 19.10. *The following conditions on a reductive algebraic group G are equivalent: (a) G is semisimple; (b) $R(G) = e$; (c) $Z(G)$ is finite.*

PROOF. (a)⇔(b). As the formation of $R(G)$ commutes with extension of the base field, $R(G) = e$ if and only if $R(G_{k^a}) = e$.

(b)⇔(c). As $R(G)$ is the largest subtorus of the multiplicative group $Z(G)$, the quotient $Z(G)/R(G)$ is finite, and so $Z(G)$ is finite if $R(G) = e$. Conversely, if $Z(G)$ is finite, then $R(G) = e$ because it is a torus.   □

PROPOSITION 19.11. *Let G be a connected group variety over a perfect field k.*

  (a) *If $R_u(G) = e$, then G is reductive.*

  (b) *The quotient $G/R_u(G)$ is reductive.*

PROOF. The proof is the same as that of Proposition 19.2.   □

PROPOSITION 19.12. *Let G be a connected group variety over a field k. If G is reductive, then every smooth connected normal commutative algebraic subgroup is a torus; the converse is true if k is perfect.*

PROOF. The proof is the same as that of Proposition 19.3.   □

PROPOSITION 19.13. *Let G be an algebraic group variety over k, and let k' be a field containing k. Then G is reductive if and only if $G_{k'}$ is reductive.*

PROOF. The proof is similar to that of Proposition 19.5.   □

LEMMA 19.14. *Let $\varphi: G' \to G$ be an isogeny of connected group varieties. If G is reductive or semisimple, then so is G'.*

PROOF. We may suppose that k is algebraically closed. Suppose that G is reductive, and let U be a smooth connected normal unipotent subgroup of G'. Then $\varphi(U)$ is smooth, connected, and unipotent, and it is normal because φ is surjective. Therefore $\varphi(U)$ is trivial, which implies that U is finite, and hence trivial. The proof for "semisimple" is similar.   □

PROPOSITION 19.15. *A semisimple group G is simply connected if and only if every central isogeny $G' \to G$ from a semisimple group G' to G is an isomorphism.*

PROOF. When G is semisimple, to say that an isogeny $G' \to G$ is central with G' semisimple is the same as saying that it is multiplicative with G' a connected group variety. Therefore the conditions coincide. □

The second condition is the usual definition of "simply connected" for semisimple groups (see, for example, Conrad et al. 2015, p. 500).

LEMMA 19.16. *A normal unipotent algebraic subgroup U of an algebraic group G acts trivially on every semisimple representation of G.*

PROOF. Let V be a semisimple representation of G, and let W be a simple subrepresentation of V. Because U is normal, W^U is stable under G (see 5.15), and because U is unipotent, $W^U \neq 0$. Therefore $W^U = W$. As V is a sum of its simple subrepresentations, it follows that U acts trivially on V. □

PROPOSITION 19.17. *If a connected group variety G admits a faithful semisimple representation, then its unipotent radical is trivial.*

PROOF. Let (V, r) be a faithful semisimple representation of G. According to the lemma, $r(R_u(G)) = e$, and so $R_u(G) = e$. □

COROLLARY 19.18. *A connected group variety G is reductive if it admits a faithful semisimple representation that remains semisimple over k^a.*

PROOF. The hypothesis implies that the unipotent radical of G_{k^a} is trivial. □

Lemma 19.16 shows that, for a connected group variety G,

$$R_u(G) \subset \bigcap_{(V,r) \text{ simple}} \mathrm{Ker}(r).$$

When k has characteristic zero, equality holds because $G/R_u(G)$ has a faithful semisimple representation (19.11, 22.42).

EXAMPLE 19.19. The group varieties SL_n, SO_n, Sp_{2n}, and GL_n are reductive because they are connected and their standard representations are simple and faithful. The first three are semisimple because their centres are finite.

c.   The rank of a group variety

DEFINITION 19.20. The ***rank*** of a group variety G over a field k is the dimension of a maximal torus in G_{k^a}, and the ***semisimple rank*** of G is the rank of $G_{k^a}/R(G_{k^a})$. The ***k-rank*** of G is the dimension of a maximal split torus in G, and the ***semisimple k-rank*** of a reductive group G is the k-rank of the semisimple group $G/R(G)$.

Since any two maximal tori in G_{k^a} are conjugate (17.10), the rank is well-defined. It is also equal to the dimension of a maximal torus in G (17.82). The semisimple rank of a reductive group G is the rank of its semisimple quotient $G/R(G)$ because the formation of $R(G)$ commutes with extension of the base field (17.62). The k-rank is well defined but changes with extension of the base field.

PROPOSITION 19.21. *Let G be a reductive group.*

(a) *The semisimple rank of G is $\mathrm{rank}(G) - \dim Z(G)$.*

(b) *The algebraic group $Z(G) \cap G^{\mathrm{der}}$ is finite.*

(c) *The algebraic group G^{der} is semisimple of rank at most the semisimple rank of G.*

PROOF. (a) Let T be a maximal torus of G. Then T contains $Z(G)$ (see 17.61), and the semisimple rank of G is $\dim(T/Z(G)) = \dim(T) - \dim Z(G)$.

(b) It follows from Proposition 12.46 that $Z(G)_t \cap G^{\mathrm{der}}$ is finite, and this implies that $Z(G) \cap G^{\mathrm{der}}$ is finite because $Z(G)_t$ has finite index in $Z(G)$.

(c) We may suppose that k is algebraically closed. The radical $R(G^{\mathrm{der}})$ of G^{der} is weakly characteristic in G^{der}, and so it is normal in G (see 1.90). Therefore $R(G^{\mathrm{der}}) \subset R(G) = Z(G)_t$. Now (b) implies that $R(G^{\mathrm{der}})$ is finite, and hence trivial (being smooth and connected). Therefore G^{der} is semisimple, and the restriction of the quotient map $G \to G/R(G)$ to G^{der} has finite kernel. It follows that $\mathrm{rank}(G^{\mathrm{der}}) \le \mathrm{rank}(G/R(G))$.   □

In fact, the map $G^{\mathrm{der}} \to G^{\mathrm{ad}} \overset{\text{def}}{=} G/Z(G)$ is an isogeny (12.46, 21.50) and so the rank of G^{der} equals the semisimple rank of G.

DEFINITION 19.22. A reductive group is ***splittable*** if it contains a split maximal torus. A ***split reductive group*** over k is a pair (G,T) consisting of a reductive group G over k and a split maximal torus T in G. A ***homomorphism of split reductive groups*** $(G,T) \to (G',T')$ is a homomorphism $\varphi \colon G \to G'$ such that $\varphi(T) \subset T'$.

We often loosely refer to a splittable reductive group as a split reductive group. When the base field k is separably closed, all reductive groups are splittable because all tori are split (12.20). Therefore every reductive group splits over a finite separable extension of the base field.[1]

---

[1] It may also split over a purely inseparable extension. For example, a quaternion algebra over the local field $\mathbb{F}_p((T))$ splits over every quadratic extension of $\mathbb{F}_p((T))$, even a purely inseparable quadratic extension (Serre 1962, XIII, §3), and the same is true of the algebraic groups attached to the algebra (Section 20i).

d. Deconstructing reductive groups

We begin with an ugly lemma.

LEMMA 19.23. *Let*

$$
\begin{array}{ccc}
A & \xrightarrow{\;\alpha\;} & B \\
\downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\
C & \xrightarrow{\;\delta\;} & D
\end{array}
$$

be a commutative diagram of algebraic groups satisfying the following conditions:

(a) *the images of α and β are central subgroups of B and C;*

(b) *the images of γ and δ are commuting normal subgroups of D;*

(c) *the sequence*

$$
A \xrightarrow{\;a\mapsto(\alpha(a),\beta(a^{-1}))\;} B\times C \xrightarrow{\;(b,c)\mapsto\gamma(b)\delta(c)\;} D \longrightarrow e \qquad (130)
$$

is exact.

Then the maps $B/A \to D/C$ and $C/A \to D/B$ defined by γ and δ are isomorphisms. (Strictly, we should write $B/\alpha(A)$ for B/A and so on.)

PROOF. To obtain the first isomorphism, apply the snake lemma (Exercise) to the diagram

$$
\begin{array}{ccccccc}
A & \xrightarrow{\;a\mapsto(a,\beta(a^{-1}))\;} & A\times C & \xrightarrow{\;(a,c)\mapsto\beta(a)c\;} & C & \longrightarrow & e \\
\downarrow & & \downarrow{\scriptstyle\alpha\times\mathrm{id}} & & \downarrow{\scriptstyle\delta} & & \\
e \longrightarrow \bar{A} & \longrightarrow & B\times C & \xrightarrow{\;(b,c)\mapsto\gamma(b)\delta(c)\;} & D & \longrightarrow & e
\end{array}
$$

in which the bottom row is obtained from the sequence (130) by replacing A with its image in $B\times C$. The second isomorphism is obtained similarly. □

Note that, in the situation of the lemma, there are exact sequences

$$
C \xrightarrow{\;\delta\;} D \to B/A \to e
$$
$$
B \xrightarrow{\;\gamma\;} D \to C/A \to e.
$$

EXAMPLE 19.24. Consider the commutative diagram

$$
\begin{array}{ccc}
\mu_n & \longrightarrow & \mathbb{G}_m \\
\downarrow & & \downarrow \\
\mathrm{SL}_n & \longrightarrow & \mathrm{GL}_n
\end{array}
$$

in which the horizontal maps are the obvious inclusions and the vertical maps send x to $\mathrm{diag}(x, x, \ldots)$. Then

$$e \to \mu_n \to \mathbb{G}_m \times \mathrm{SL}_n \to \mathrm{GL}_n \to e$$

is exact, and the diagram satisfies the hypotheses of the lemma. Let $T = \mathrm{GL}_n / \mathrm{SL}_n$ and $\mathrm{PGL}_n = \mathrm{GL}_n / \mathbb{G}_m$. According to the lemma, the homomorphisms $\mathbb{G}_m \to T$ and $\mathrm{SL}_n \to \mathrm{PGL}_n$ given by the diagram are isogenies with kernel μ_n.

EXAMPLE 19.25. Let G be a reductive group such that the semisimple group G^{ad} is perfect.[2] Then $G/(Z(G) \cdot G^{\mathrm{der}})$ is a quotient of G^{ad} (which is perfect) and G/G^{der} (which is commutative), and so it is trivial, i.e., $G = Z(G) \cdot G^{\mathrm{der}}$. It follows that $Z(G) \cap G^{\mathrm{der}} = Z(G^{\mathrm{der}})$ and that the sequence

$$e \to Z(G^{\mathrm{der}}) \to Z(G) \times G^{\mathrm{der}} \to G \to e$$

is exact. Therefore the diagram of natural inclusions

$$
\begin{array}{ccc}
Z(G^{\mathrm{der}}) & \longrightarrow & Z(G) \\
\downarrow & & \downarrow \\
G^{\mathrm{der}} & \longrightarrow & G
\end{array}
$$

satisfies the hypotheses of the lemma. Let $T = G/G^{\mathrm{der}}$ and $G^{\mathrm{ad}} = G/Z(G)$. According to the lemma, the homomorphisms $Z(G) \to T$ and $G^{\mathrm{der}} \to G^{\mathrm{ad}}$ given by the diagram are isogenies with kernel $Z(G^{\mathrm{der}})$.

DEFINITION 19.26. Consider a triple (H, D, φ) with H a perfect semisimple algebraic group, D an algebraic group of multiplicative type, and $\varphi \colon Z(H) \to D$ a homomorphism whose cokernel is a torus. The homomorphism

$$z \mapsto (z, \varphi(z)^{-1}) \colon Z(H) \to H \times D$$

is normal, and we define $G(\varphi)$ to be its cokernel.

PROPOSITION 19.27. *The algebraic group* $G = G(\varphi)$ *is reductive with*

$$Z(G) \simeq D, \quad G^{\mathrm{der}} \simeq H/\mathrm{Ker}(\varphi), \quad G^{\mathrm{ad}} \simeq H^{\mathrm{ad}}, \quad G/G^{\mathrm{der}} \simeq D/\mathrm{Im}(\varphi).$$

PROOF. Let $Z = \mathrm{Ker}(\varphi)$ (a finite group scheme) and $T = \mathrm{Coker}(\varphi)$ (a torus). The commutative diagram

$$
\begin{array}{ccc}
Z(H) & \xrightarrow{\varphi} & D \\
\downarrow & & \downarrow{\scriptstyle d \mapsto [e,d]} \\
H/Z & \xrightarrow{h \mapsto [h,e]} & G(\varphi)
\end{array}
$$

[2]In fact, all semisimple algebraic groups are perfect (21.50), and so this condition, here and elsewhere in this section, is superfluous.

satisfies the hypotheses of the lemma. Moreover, both homomorphisms with target $G(\varphi)$ are injective, and so the lemma gives exact sequences

$$e \to Z \to H \to G(\varphi) \to T \to e$$
$$e \to D \to G(\varphi) \to H/Z(H) \to e.$$

The first sequence realizes $G(\varphi)$ as an extension of smooth connected groups, and so $G(\varphi)$ is smooth and connected (8.1). From the first sequence, we see that $G(\varphi)^{\mathrm{der}} \subset H/Z$, and so $(H/Z)^{\mathrm{der}} \subset G(\varphi)^{\mathrm{der}} \subset H/Z$. But $H/Z = (H/Z)^{\mathrm{der}}$ because H is perfect, and so $G(\varphi)^{\mathrm{der}} \simeq H/Z$ and $G(\varphi)/G(\varphi)^{\mathrm{der}} \simeq T$. As $H/Z(H)$ has trivial centre (17.62e), the second sequence shows that $Z(G(\varphi)) \simeq D$ and $G(\varphi)^{\mathrm{ad}} \simeq H^{\mathrm{ad}}$. □

EXAMPLE 19.28. From the triple $(\mathrm{SL}_n, \mathbb{G}_m, \mu_n \hookrightarrow \mathbb{G}_m)$ we recover the group $G = \mathrm{GL}_n$.

PROPOSITION 19.29. *Let G be a reductive algebraic group such that the semisimple group G^{ad} is perfect. Then $G = G(\varphi)$ for a triple (H, D, φ) as (19.26).*

PROOF. In fact, we showed in Example 19.25 that G^{der} is semi simple and that G is the reductive group attached to the triple $(G^{\mathrm{der}}, Z(G), Z(G^{\mathrm{der}}) \hookrightarrow Z(G))$. □

Thus, to give a reductive group G amounts to giving a triple (H, D, φ) with H semisimple, D of multiplicative type, and the cokernel of $\varphi \colon Z(H) \to D$ a torus. (Without the last condition, $G(\varphi)$ need not be connected.)

REMARK 19.30. In fact, every reductive group G arises from a triple (G', D, φ) with $G' \to G^{\mathrm{ad}}$ the simply connected covering group of G^{ad} and $D = Z(G)$. Indeed, the homomorphism $G^{\mathrm{der}} \to G^{\mathrm{ad}}$ is a multiplicative isogeny, and so $G' \to G^{\mathrm{ad}}$ lifts to a homomorphism $G' \to G^{\mathrm{der}} \subset G$ (see 18.8). The restriction φ of this homomorphism to $Z(G')$ maps into D, and $G(\varphi) \simeq G$. In more detail, there is an exact commutative diagram

$$
\begin{array}{ccccccccc}
e & \longrightarrow & Z & \longrightarrow & Z(G') & \longrightarrow & Z(G) & \longrightarrow & Z(G/G') & \longrightarrow & e \\
& & \downarrow{\simeq} & & \downarrow & & \downarrow & & \downarrow{\simeq} & & \\
e & \longrightarrow & Z & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G/G' & \longrightarrow & e.
\end{array}
$$

ASIDE 19.31. Semisimple algebraic groups obviously form an important class. Reductive (and even pseudo-reductive) groups arise in inductive arguments involving parabolic subgroups of semisimple groups. They are also important in their own right – for example, they play a fundamental role in the work of Langlands. Most of the theory of semisimple groups extends without serious difficulty to reductive groups. In characteristic zero, reductive groups are those whose representations are "completely reducible" to simple representations (22.42), which perhaps justifies the name. The name was popularized in the foundational paper Borel and Tits 1965.

Exercises

EXERCISE 19-1. Show that a semisimple algebraic group G is simply connected if and only if every homomorphism $G \to \mathrm{PGL}_V$ lifts to a homomorphism $G \to \mathrm{GL}_V$ (Borel 1975, p. 362).

EXERCISE 19-2. Show that an isogeny $\varphi: G \to G'$ of reductive groups is central if and only if the kernel of $\mathrm{Lie}(\varphi): \mathrm{Lie}(G) \to \mathrm{Lie}(G')$ is central.

EXERCISE 19-3. Let G be a reductive group over a field k, and let k' be a finite Galois extension of k splitting some maximal torus in G. Let $G' \to G^{\mathrm{der}}$ be a central isogeny. Show that there exists a central extension

$$e \to N \to G_1 \to G \to e$$

such that G_1 is a reductive group, N is a product of copies of $(\mathbb{G}_m)_{k'/k}$, and $G_1^{\mathrm{der}} \to G^{\mathrm{der}}$ is the given isogeny $G' \to G^{\mathrm{der}}$ (Milne and Shih 1982, 3.1).

Algebraic Groups of Semisimple Rank One

This chapter contains preliminaries for the general study of reductive groups in the next chapter. In particular, we show that every split reductive group of semisimple rank 1 is isomorphic to exactly one of the following groups:

$$\mathbb{G}_m^r \times \mathrm{SL}_2, \quad \mathbb{G}_m^r \times \mathrm{PGL}_2, \quad \mathbb{G}_m^{r-1} \times \mathrm{GL}_2, \quad r \in \mathbb{N}.$$

a. Group varieties of semisimple rank 0

Recall (19.20) that the rank of a group variety is the dimension of a maximal torus, and that this does not change under extension of the base field. The semisimple rank of G is the rank of the largest semisimple quotient of G_{k^a}.

THEOREM 20.1. *Let G be a connected group variety over a field k.*

(a) *G has rank 0 if and only if it is unipotent.*

(b) *G has semisimple rank 0 if and only if it is solvable.*

(c) *G is reductive of semisimple rank 0 if and only if it is a torus.*

PROOF. We may suppose that k is algebraically closed.

(a) This is a restatement of Proposition 16.60.

(b) If G is solvable, then $G = R(G)$, and so it has semisimple rank 0. Conversely, if G has semisimple rank 0, then $G/R(G)$ is unipotent (by (a)) and semisimple (19.2), and hence trivial. Thus $G = R(G)$, and so G is solvable.

(c) A torus is certainly reductive of semisimple rank 0. Conversely, if G is reductive of semisimple rank 0, then it is solvable. As $R_u(G) = e$, this implies that G is a torus (16.33d). □

b.   Homogeneous curves

20.2. Let C be a regular complete algebraic curve over k. The local ring $\mathcal{O}_P$ at a point $P \in |C|$ is a discrete valuation ring containing k with field of fractions $k(C)$, and every such discrete valuation ring arises from a unique P. Therefore, we can identify $|C|$ with the set of such discrete valuation rings in $k(C)$ endowed with the topology for which the proper closed subsets are the finite sets. For an open subset U, the ring $\mathcal{O}_C(U) = \bigcap_{P \in U} \mathcal{O}_P$. Thus, we can recover C from its function field $k(C)$. In particular, two regular complete connected curves over k are isomorphic if they have isomorphic function fields. (Cf. Hartshorne 1977, I, §6, and II, 6.7.)

20.3. According to the last remark, a regular complete algebraic curve C over k is isomorphic to $\mathbb{P}^1$ if and only if $k(C)$ is the field $k(T)$ of rational functions in a single symbol T. Lüroth's theorem states that every subfield of $k(T)$ properly containing k is of the form $k(u)$ for some $u \in k(T)$ transcendental over k (Jacobson 1989, Section 8.14).

20.4. Let C be an algebraic curve over k. If C becomes isomorphic to $\mathbb{P}^1$ over k^{a} and $C(k) \neq \emptyset$, then C is isomorphic to $\mathbb{P}^1$ over k. To see this, note that C is a smooth complete curve over k of genus 0 because it becomes so over k^{a}. Embed C in a projective space. Repeatedly projecting from a point $P \in C(k)$ onto a hyperplane will eventually give a birational map from C onto $\mathbb{P}^1$.

PROPOSITION 20.5. *Let C be a smooth complete algebraic curve over an algebraically closed field. If C admits a nontrivial action by a connected group variety G, then it is isomorphic to $\mathbb{P}^1$.*

PROOF. Suppose first that C admits a nontrivial action by a solvable G. As G is split (16.53), C admits a nontrivial action by $\mathbb{G}_a$ or $\mathbb{G}_m$ (see 16.34). If $\mathbb{G}_a$ acts nontrivially on C, then, for some $x \in C(k)$, the orbit map $\mu_x \colon \mathbb{G}_a \to C$ is nonconstant, and hence dominant. Now

$$k(C) \hookrightarrow k(\mathbb{G}_a) = k(T),$$

and so $k(C) \approx k(\mathbb{P}^1)$ by Lüroth's theorem (20.3). Hence $C \approx \mathbb{P}^1$ (see 20.2). The same argument applies with $\mathbb{G}_m$ for $\mathbb{G}_a$.

     We now prove the general case. If all the Borel subgroups B of G act trivially on C, then $G(k)$ acts trivially on C because $G(k) = \bigcup B(k)$ (see 17.33). As G is reduced, this implies that G acts trivially on C, contrary to the hypothesis. Therefore some Borel subgroup acts nontrivially on C, and we have seen that this implies that C is isomorphic to $\mathbb{P}^1$.   □

REMARK 20.6. There are several different proofs of the proposition, none completely elementary. If the genus of C is nonzero, then a nontrivial action of G on C defines a nontrivial action of G on the jacobian variety of C fixing 0, but abelian varieties are "rigid" (Borel 1991, 10.7). In fact, the automorphism group of a curve of genus $g > 1$ is finite (and even of order $\leq 84(g-1)$ in characteristic zero).

c. The automorphism group of the projective line

The projective line represents the functor

$$R \rightsquigarrow \mathbb{P}^1(R) = \{P \subset R^2 \mid P \text{ is a direct summand of } R^2 \text{ of rank } 1\}.$$

Each $P \in \mathbb{P}^1(R)$ is a projective R-module, and hence is locally free for the Zariski topology on $\text{spm}(R)$ (CA §12). Given $x, y \in R$, we write $(x:y)$ for the submodule $R\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ of R^2 when this is an element of $\mathbb{P}^1(R)$. Locally for the Zariski topology on $\text{spm}(R)$, every point of $\mathbb{P}^1(R)$ is of the form $(x:y)$. For example, $0 = (0:1)$, $1 = (1:1)$, and $\infty = (1:0)$.

We let $\underline{\text{Aut}}(\mathbb{P}^1)$ denote the functor $R \rightsquigarrow \text{Aut}_R(\mathbb{P}^1_R)$. For a k-algebra R, the natural action of $\text{GL}_2(R)$ on R^2 defines an action of $\text{GL}_2(R)$ on $\mathbb{P}^1(R)$, and hence a homomorphism $\text{GL}_2 \to \underline{\text{Aut}}(\mathbb{P}^1)$. This factors through PGL_2.

PROPOSITION 20.7. *The homomorphism* $\text{PGL}_2 \to \underline{\text{Aut}}(\mathbb{P}^1)$ *just defined is an isomorphism.*

We need two lemmas.

LEMMA 20.8. *Let* $\alpha \in \underline{\text{Aut}}(\mathbb{P}^1)(R) = \text{Aut}(\mathbb{P}^1_R)$. *If* $\alpha(0_R) = 0_R$, $\alpha(1_R) = 1_R$, *and* $\alpha(\infty_R) = \infty_R$, *then* α *is the identity map.*

PROOF. Let U_0 (resp. U_1) denote the complement of 0 (resp. ∞) in $\mathbb{P}^1_k$. Then $\mathbb{P}^1_R = U_{0R} \cup U_{1R}$ with $U_{0R} = \text{Spec } R[T]$ and $U_{1R} = \text{Spec } R[T^{-1}]$. The diagram

$$U_{0R} \hookleftarrow U_{0R} \cap U_{1R} \hookrightarrow U_{1R}$$

corresponds to

$$R[T] \hookrightarrow R[T, T^{-1}] \hookleftarrow R[T^{-1}].$$

The automorphism α preserves U_{0R} and U_{1R}, and its restrictions to U_{0R} and U_{1R} correspond to R-algebra homomorphisms

$$T \mapsto P(T) = a_0 + a_1 T + P_2(T)T^2$$
$$T^{-1} \mapsto Q(T^{-1}) = b_0 + b_1 T^{-1} + Q_2(T^{-1})T^{-2}$$

such that $P(T)Q(T^{-1}) = 1$ (equality in $R[T, T^{-1}]$). The coefficient $a_0 = 0$ because α fixes 0_R, and $b_0 = 0$ because α fixes ∞_R. The equality $PQ = 1$ expands to

$$a_1 b_1 + P_2(T)Q_2(T^{-1}) + b_1 P_2(T)T + a_1 Q_2(T)T^{-1} = 1.$$

This implies that $P_2(T) = 0$ because otherwise the degree of $b_1 P_2(T)T$ is greater than that of $P_2(T)Q_2(T^{-1})$. Similarly, $Q_2(T^{-1}) = 0$. Finally, $a_1 = 1 = b_1$ because α fixes 1_R, and so α is the identity map. □

LEMMA 20.9. *Let P_0, P_1, P_∞ be distinct points on $\mathbb{P}^1$ with coordinates in R. If P_0, P_1, P_∞ remain distinct in $\mathbb{P}^1(R/\mathfrak{m})$ for all maximal ideals $\mathfrak{m}$ in R, then there exists a unique $\gamma \in \mathrm{PGL}_2(R)$ such that $\gamma \cdot 0_R = P_0$, $\gamma \cdot 1_R = P_1$, and $\gamma \cdot \infty_R = P_\infty$.*

PROOF. One sees easily that the only elements of $\mathrm{GL}_2(R)$ fixing 0_R, 1_R, and ∞_R are the scalar matrices. Therefore γ is unique if it exists, and it follows that it suffices to prove the existence of γ locally. Thus we may suppose that $P_0 = (x_0 : y_0)$, $P_1 = (x_1 : y_1)$, and $P_\infty = (x_\infty : y_\infty)$. Let $\mathfrak{m}$ be a maximal ideal in R. Because P_0 and P_∞ are distinct modulo $\mathfrak{m}$, $(x_\infty y_0 - x_0 y_\infty) \neq 1$ modulo $\mathfrak{m}$. As this is true for all $\mathfrak{m}$, the matrix $A = \left(\begin{smallmatrix} x_\infty & x_0 \\ y_\infty & y_0 \end{smallmatrix}\right)$ lies in $\mathrm{GL}_2(R)$. Note that $A \cdot 0_R = P_0$ and $A \cdot \infty_R = P_\infty$. Let $A^{-1}\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)$. Then $x, y \in R^\times$ because $(x : y)$ is distinct from $(0 : 1)$ and $(1 : 0)$ modulo every maximal ideal in R. The matrix $B = \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$ fixes 0_R and ∞_R and maps $(1 : 1)$ to $(x : y)$. The image of AB in $\mathrm{PGL}_2(R)$ is the required element.   □

We now prove the proposition. Let $\alpha \in \mathrm{Aut}(\mathbb{P}^1_R)$. The points $\alpha(0)$, $\alpha(1)$, and $\alpha(\infty)$ satisfy the hypothesis of Lemma 20.9, and so there is a unique $\gamma \in \mathrm{PGL}_2(R)$ such that $\gamma \cdot 0 = \alpha(0)$, $\gamma \cdot 1 = \alpha(1)$, and $\gamma \cdot \infty = \alpha(\infty)$. Lemma 20.8 now shows that γ acts as α on the whole of $\mathbb{P}^1_R$.

d. A fixed point theorem for actions of tori

According to the Borel fixed point theorem, a torus acting on a complete variety X has at least one fixed point. We shall need to know that it has at least $\dim(X) + 1$ fixed points.

LEMMA 20.10. *Let X be an irreducible closed subvariety of $\mathbb{P}^n$ of dimension ≥ 1, and let H be a hyperplane in $\mathbb{P}^n$. Then $X \cap H$ is nonempty, and either $X \subset H$ or the irreducible components of $X \cap H$ all have dimension $\dim(X) - 1$.*

PROOF. If $X \cap H$ were empty, then X would be a complete subvariety of the affine variety $X \smallsetminus H$, and hence of dimension 0 (see A.75), contradicting the hypothesis. The rest of the statement is a special case of Krull's principal ideal theorem (CA 21.3).   □

PROPOSITION 20.11. *Let (V, r) be a finite-dimensional representation of a torus T over k, and let X be a closed subvariety of $\mathbb{P}(V)$ stable under the action of T on $\mathbb{P}(V)$. In $X(k^a)$ there are at least $\dim(X) + 1$ points fixed by T.*

PROOF. We may suppose that k is algebraically closed. As T is connected, it leaves stable each irreducible component of X, and so we may suppose that X is irreducible. Lemma 13.51 allows us to replace T with $\mathbb{G}_m$. We prove the statement by induction on $d = \dim X$.

Let $\{e_0, \ldots, e_n\}$ be a basis of V consisting of eigenvectors for $\mathbb{G}_m$, say,

$$\lambda(t)e_i = t^{m_i} e_i, \quad m_i \in \mathbb{Z}, \quad t \in \mathbb{G}_m(k),$$

numbered so that $m_0 = \min_i(m_i)$. Let W be the subspace of V spanned by $\{e_1,\ldots,e_n\}$. If $X \subset \mathbb{P}(W)$, we replace V with W and start over. If not, we apply the induction hypothesis to deduce that $\mathbb{G}_m$ has at least d fixed points in $X \cap \mathbb{P}(W)$. Let $[v] \in X \smallsetminus \mathbb{P}(W)$, and write

$$v = e_0 + a_1 e_1 + \cdots + a_n e_n, \quad a_0 \neq 0.$$

If $[v]$ is fixed by the action of $\mathbb{G}_m$, then we have at least $d + 1$ fixed points. Otherwise, $\mathbb{G}_m$ acts on the affine space $D(e_0^\vee) = \mathbb{P}(V) \smallsetminus \mathbb{P}(W)$ with nonnegative weights $0,\ldots, m_n - m_0$, and so there exists a fixed point $\lim_{t\to 0} t[v]$ in $D(e_0^\vee) \cap X$ (see 13.17). Again we have at least $d + 1$ fixed points. $\square$

COROLLARY 20.12. *Let P be an algebraic subgroup of a smooth connected algebraic group G such that G/P is complete, and let T be a torus in G. In $(G/P)(k^a)$ there are at least $\dim(G/P) + 1$ points fixed by T.*

PROOF. There exists a representation $G \to \mathrm{GL}_V$ of V and an $o \in \mathbb{P}(V)$ such that the map $g \mapsto go \colon G \to \mathbb{P}(V)$ defines a G-equivariant isomorphism of G/P onto the orbit $G \cdot o$ (see the proof of 7.18). Now $G \cdot o$ is a complete subvariety of $\mathbb{P}(V)$ to which we can apply the proposition. $\square$

EXAMPLE 20.13. The bound $\dim(X) + 1$ in Proposition 20.11 cannot be improved. When $\mathbb{G}_m$ acts on $\mathbb{P}^n$ according to the rule

$$t(x_0 \colon \cdots \colon x_i \colon \cdots \colon x_n) = (t^0 x_0 \colon \cdots \colon t^i x_i \colon \cdots \colon t^n x_n),$$

the fixed points are $P_0,\ldots,P_n$ with $P_i = (0\colon\cdots\colon 0 \colon \overset{i}{1} \colon 0 \colon\cdots\colon 0)$.

ASIDE 20.14. There is an alternative explanation of the proposition using étale cohomology. Consider a torus T acting linearly on a projective variety X over an algebraically closed field. For some $t \in T(k)$, X^T is the set of fixed points of t, and so

$$\#X^T = \sum_{i=0}^{2\dim X} (-1)^i \,\mathrm{Tr}(t \mid H^i(X))$$

(Lefschetz trace formula). On letting $t \to 1$, we find that $\mathrm{Tr}(t \mid H^i(X)) = \dim H^i(X)$. It follows from the Białynicki-Birula decomposition (13.47) that the cohomology groups of X can be expressed in terms of the cohomology groups of the connected components of X^T with an even shift in degree. Therefore, the odd-degree groups vanish when X^T is finite. On the other hand $H^{2i}(X)$ has dimension at least 1 because it contains the class of an intersection of hyperplane sections. Therefore,

$$\#X^T = \sum_{i=0}^{\dim X} \dim H^{2i}(X) \geq \dim(X) + 1.$$

e. Group varieties of semisimple rank 1.

In this section, k is algebraically closed.

Let G be a connected group variety over k and λ a cocharacter of G. In Section 13d we defined connected subgroup varieties $U(\lambda)$, $Z(\lambda)$, and $P(\lambda)$ of G. Recall that $U(\lambda)$ is a normal unipotent subgroup of $P(\lambda)$ and

$$U(\lambda) \rtimes Z(\lambda) \simeq P(\lambda)$$

(13.33, 14.13). Let T be a maximal torus containing $\lambda\mathbb{G}_m$. A Borel subgroup of G containing T is said to be *positive* if it contains $U(\lambda)$ and *negative* if it contains $U(-\lambda)$.

LEMMA 20.15. *Let G be a connected nonsolvable group variety of rank* 1, *and let $\lambda: \mathbb{G}_m \to T$ be an isomorphism from $\mathbb{G}_m$ onto a maximal torus T in G.*

(a) *There are both positive and negative Borel subgroups containing T.*

(b) *No Borel subgroup containing T is both positive and negative.*

(c) *The normalizer of T in G contains an element acting on T as $t \mapsto t^{-1}$.*

PROOF. (a) By definition, $Z(\lambda) = C_G(T)$, which equals T (see 17.61), and so $P(\lambda)$ is solvable. As it is connected, $P(\lambda)$ is contained in a Borel subgroup, which is positive (by definition). Similarly, $P(-\lambda)$ is contained in a negative Borel subgroup.

(b) The subgroups $U(-\lambda)$, $Z(\lambda)$, and $U(\lambda)$ generate G because their Lie algebras generate $\mathfrak{g}$. A Borel subgroup containing them would equal G, but G is not solvable.

(c) The normalizer of T in G acts transitively on the set of Borel subgroups containing T (see 17.11), and an element of the normalizer mapping a positive Borel subgroup to a negative Borel subgroup acts as $t \mapsto t^{-1}$ on T (this is the only nontrivial automorphism of T). □

THEOREM 20.16. *Let G be a connected nonsolvable group variety G over k, and let T be a maximal torus in G. The following are equivalent:*

(a) *the semisimple rank of G is* 1;

(b) *T lies in exactly two Borel subgroups;*

(c) *$\dim(G/B) = 1$ if B is a Borel subgroup containing T;*

(d) *there exists an isogeny $G/R(G) \to \mathrm{PGL}_2$.*

PROOF. Proposition 17.20 allows us to replace G with $G/R(G)$. Then G is semisimple.

(a)$\Rightarrow$(b). The Weyl group of T acts faithfully on T (by definition) and transitively on the set of Borel groups containing T (see 17.11). As $T \approx \mathbb{G}_m$ and $\mathrm{Aut}(\mathbb{G}_m) = \{\pm 1\}$, we see that there are most two such Borel groups. As G has rank 1, the lemma shows that there are exactly two.

(b)$\Rightarrow$(c). Let $\mathcal{B}$ denote the variety of Borel subgroups in G (Section 17f). Then $\mathcal{B} \simeq G/B$ and the Borel subgroups containing T are the fixed points for T acting on $\mathcal{B}$. According to (20.12), there are at least $\dim(G/B) + 1$ fixed points, and so $\dim(G/B) = 1$.

(c)$\Rightarrow$(d). The variety G/B is smooth and complete with a nontrivial action of G. If it has dimension 1, then it is isomorphic to $\mathbb{P}^1$ (see 20.5). On choosing an isomorphism $G/B \to \mathbb{P}^1$, we get an action of G on $\mathbb{P}^1$, and hence a homomorphism $G \to \underline{\mathrm{Aut}}(\mathbb{P}^1)$. On composing this with the isomorphism $\underline{\mathrm{Aut}}(\mathbb{P}^1) \simeq \mathrm{PGL}_2$ in Proposition 20.7, we get a homomorphism $\varphi: G \to \mathrm{PGL}_2$ whose kernel is the intersection of the Borel subgroups containing T. This kernel is finite (17.56), and φ is surjective because every proper subgroup of PGL_2 is solvable (17.27).

(d)$\Rightarrow$(a). As PGL_2 is the quotient of GL_2 by its radical, it is semisimple (Section 19b). The diagonal torus in PGL_2 is maximal and has dimension 1. Now apply Lemma 19.14. $\qquad\square$

Let G be a connected reductive group over k of semisimple rank 1. Let T be a maximal torus in G, and let B^+ and B^- be the two Borel subgroups containing T. Choose the isomorphism $G/B^+ \to \mathbb{P}^1$ so that B^+ fixes 0 and B^- fixes ∞, and let φ denote the resulting homomorphism $\varphi: G \to \underline{\mathrm{Aut}}(\mathbb{P}^1) \simeq \mathrm{PGL}_2$.

As G is not solvable, B^+ is not nilpotent (17.23), and so its unipotent part B_u^+ is nonzero. The kernel of φ contains the torus $R(G)$ as a subgroup of finite index, and so the restriction of φ to B_u^+ has finite kernel. Therefore φ is an isogeny from B_u^+ onto the unipotent part of the stabilizer of 0 in PGL_2, and so B_u^+ is a smooth connected unipotent group of dimension 1. Hence B_u^+ is isomorphic to $\mathbb{G}_a$, and the action of T on B_u^+ by inner automorphisms determines a character α^+ of T such that, for every isomorphism $i: \mathbb{G}_a \to B_u^+$,

$$i(\alpha^+(t) \cdot x) = t \cdot i(x) \cdot t^{-1}, \quad t \in T(R), \quad x \in \mathbb{G}_a(R) = R$$

(see 14.58, 14.69). Similarly, T acts on B_u^- through a character α^-.

LEMMA 20.17. *Let $n \in G(k)$ normalize T and map B^- onto B^+. Then*

(a) $\alpha^+ \circ \mathrm{inn}(n)|T = \alpha^-$;

(b) $\mathrm{Ker}(\alpha^+) = Z(B^+) = Z(G)$;

(c) $\alpha^+ \circ \mathrm{inn}(n)|T = -\alpha^+$.

PROOF. (a) Fix an isomorphism $i: \mathbb{G}_a \to B_u^+$, and let $i^-: \mathbb{G}_a \to B_u^-$ be the composite of i with $\mathrm{inn}(n^{-1})$. For $x \in B_u^+(R)$ and $t \in T(R)$ (R a k-algebra),

$$
\begin{aligned}
i(\alpha^+(ntn^{-1}) \cdot x) &= ntn^{-1} \cdot i(x) \cdot nt^{-1}n^{-1} && \text{(definition of } \alpha^+) \\
&= nt \cdot i^-(x) \cdot t^{-1}n^{-1} && \text{(definition of } i^-) \\
&= n \cdot i^-(\alpha^-(t) \cdot x) \cdot n^{-1} && \text{(definition of } \alpha^-) \\
&= i(\alpha^-(t) \cdot x) && \text{(definition of } i^-),
\end{aligned}
$$

and so $\alpha^+(ntn^{-1}) = \alpha^-(t)$, as required.

(b) Note that $B^+ = B_u^+ \rtimes_{\alpha^+} T$. As B^+ is not nilpotent, α^+ is nonzero, and it follows that $Z(B^+) = \mathrm{Ker}\,\alpha^+$. The equality $Z(B^+) = Z(G)$ was proved in Proposition 17.45.

(c) Conjugation by n restricts to the identity map on $Z(G) = \mathrm{Ker}(\alpha^+)$, and so $\mathrm{inn}(n)|T$ induces an automorphism ν of $\mathbb{G}_m$:

$$
\begin{array}{ccccccccc}
e & \longrightarrow & \mathrm{Ker}(\alpha^+) & \longrightarrow & T & \xrightarrow{\ \alpha^+\ } & \mathbb{G}_m & \longrightarrow & e \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{inn}(n)} & & \vdots{\scriptstyle \nu} & & \\
e & \longrightarrow & \mathrm{Ker}(\alpha^+) & \longrightarrow & T & \xrightarrow{\ \alpha^+\ } & \mathbb{G}_m & \longrightarrow & e
\end{array}
$$

If $\nu = \mathrm{id}$, then $ntn^{-1} = t \cdot \lambda(t)$ with λ a homomorphism $T \to \mathrm{Ker}(\alpha^+)$. As $\mathrm{inn}(n)^2 = \mathrm{id}$, we have $\lambda^2 = \mathrm{id}$. But $\mathrm{Hom}(T, \mathrm{Ker}(\alpha^+))$ is torsion-free, and so this implies that $\mathrm{inn}(n)|T = \mathrm{id}$, which contradicts the definition of n. Therefore $\nu = -\mathrm{id}$, and so (c) holds. $\qquad\square$

PROPOSITION 20.18. *With the above notation, the intersection*

$$B_u^+ \cap B_u^- = e.$$

PROOF. Clearly $B_u^+ \cap B_u^-$ is stable under the action of T on G by inner automorphisms. The torus T acts on B_u^+ through the character α^+. As α^+ is surjective, $B_u^+ \cap B_u^-$ is a finite subscheme of B_u^+ stable under $\mathbb{G}_m$. If we identify B_u^+ with $\mathbb{G}_a$, then $B_u^+ \cap B_u^-$ is identified with the finite group scheme α_{p^r} for some $r \in \mathbb{N}$ (Exercise 14-3). If $r \neq 0$, then T acts on $\alpha_p \subset \alpha_{p^r}$ through $\alpha^+ \colon T \to \mathbb{G}_m = \underline{\mathrm{Aut}}(\alpha_p)$ and also through $\alpha^- = -\alpha^+$, which is impossible. $\quad\square$

REMARK 20.19. The proof of (a)$\Rightarrow$(b) in Theorem 20.16 uses (i) that $C_G(T)$ is connected (so the Weyl group acts on $\mathcal{B}^T$), and the proof of (a)$\Rightarrow$(b)$\Rightarrow$(c) uses (ii) that $N_G(B) = B$ (so we can identify $\mathcal{B}$ with G/B). In fact, Theorem 20.16 can be proved without either (i) or (ii) by using Corollary 17.2 to prove (a)$\Rightarrow$(b) and by using the following weaker statement to prove (b)$\Rightarrow$(c): $N_G(B)_{\mathrm{red}}$ contains B as a subgroup of finite index and is equal to its own normalizer. After this more elementary proof of Theorem 20.16, it is possible to prove the Bruhat decomposition and then go back and prove (i) and (ii). See Allcock 2009. We did not follow this path because we found it convenient to be able to identify $\mathcal{B}$ with G/B at an early stage.

f.   Split reductive groups of semisimple rank 1.

In this section, G is a reductive group of semisimple rank 1 over a field k (not necessarily algebraically closed) with a split maximal torus T.

LEMMA 20.20. *The torus T is contained in exactly two Borel subgroups, namely, in $B^+ = P(\lambda)$ and $B^- = P(-\lambda)$ for any cocharacter λ of T mapping $\mathbb{G}_m$ isomorphically onto $(T \cap G^{\mathrm{der}})_t$.*

PROOF. Suppose first that G is semisimple. Over k^a, the radical of G is trivial and so there exists an isogeny from G onto PGL$_2$ (see 20.16). Hence G has dimension 3 and every Borel subgroup has dimension 2. Choose an isomorphism $\lambda: \mathbb{G}_m \to T$. Then $P(\lambda) = U(\lambda) \cdot T$ is a connected solvable algebraic subgroup of G of maximum dimension, and hence is a Borel subgroup containing T (and $P(-\lambda)$ is the only other Borel subgroup of G containing T).

We now consider the general case. The derived group G' of G is semisimple of rank ≤ 1 (see 19.21). If G' had rank 0, then it would be trivial, and G would be solvable, contradicting the hypothesis. Thus, G' is a split semisimple group of rank 1. Let T' be a maximal torus of G' contained in T (which exists by 17.85), and choose an isomorphism $\lambda: \mathbb{G}_m \to T'$. Then $U(\lambda) \cdot T$ and $U(-\lambda) \cdot T$ are Borel subgroups of G containing T. $\qquad\square$

LEMMA 20.21. *We have*

$$B_u^+ \cap B_u^- = e$$
$$B^+ \cap B^- = T.$$

PROOF. We may suppose that k is algebraically closed. Then the first equality was proved in Proposition 20.18, and the second follows because $B^+ = B_u^+ \cdot T$ and $B^- = B_u^- \cdot T$. $\qquad\square$

THEOREM 20.22. *Let B be a Borel subgroup of G. Then G/B is isomorphic to* $\mathbb{P}^1$*, and the homomorphism*

$$\varphi: G \to \underline{\mathrm{Aut}}(G/B) \approx \mathrm{PGL}_2$$

is surjective with kernel $Z(G)$.

PROOF. The algebraic group G_{k^a} is reductive of semisimple rank 1, and B_{k^a} is a Borel subgroup of G_{k^a}. Moreover, $(G/B)_{k^a} \simeq G_{k^a}/B_{k^a} \approx \mathbb{P}^1$, and so $G/B \approx \mathbb{P}^1$ because it has a k-point (20.4). The map $G \to \underline{\mathrm{Aut}}(G/B)$ is surjective because this is true after a base change to k^a. It remains to prove that the kernel of $G \to \underline{\mathrm{Aut}}(G/B)$ is $Z(G)$.

The kernel of φ is contained in $B^+ \cap B^- = T$, and is therefore a diagonalizable normal subgroup of a connected group G. Hence the kernel is contained in the centre of G (see 12.38). On the other hand, because φ is surjective, $Z(G)$ maps into $Z(\mathrm{PGL}_2) = e$, and so $Z(G) \subset \mathrm{Ker}(\varphi)$. $\qquad\square$

g. Properties of SL$_2$

We use the following notation: T is the diagonal torus in SL$_2$; n is the element $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ of the normalizer of T; U^+ and U^- are the algebraic subgroups $\left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$ and $\left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\}$ of SL$_2$.

PROPOSITION 20.23. *The algebraic group* SL$_2$ *is generated by its subgroups* U^+ *and* U^-.

PROOF. Its Lie algebra is generated by the Lie algebras of U^+ and U^- (10.2).□

PROPOSITION 20.24. *The algebraic groups* SL_2 *and* PGL_2 *are perfect.*

PROOF. It suffices to show that SL_2 is perfect. As SL_2 is smooth, it suffices to show that the abstract group $\mathrm{SL}_2(k^a)$ is perfect (6.21). In fact, we shall show that $\mathrm{SL}_2(k)$ is perfect whenever k has at least three elements. For $a \in k^\times$, let

$$E_{1,2}(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad E_{2,1}(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

An algorithm in elementary linear algebra shows that $\mathrm{SL}_2(k)$ is generated by these matrices. On the other hand, the commutator

$$\left[\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (b^2 - 1)c \\ 0 & 1 \end{pmatrix}.$$

Take $b \neq \pm 1$, and then c can be chosen so that $(b^2 - 1)c = a$. Thus $E_{1,2}(a)$ is a commutator. On taking transposes, we find that $E_{2,1}(a)$ is also a commutator. □

For $t \in k^\times$, the inner automorphism

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & tb \\ t^{-1}c & d \end{pmatrix} = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & 1 \end{pmatrix}$$

of GL_2 induces an automorphism γ_t of SL_2 with the property that $\gamma_t(T) = T$. Recall that $\mathrm{End}(\mathbb{G}_m) \simeq \mathbb{Z}$ and $\mathrm{Aut}(\mathbb{G}_m) \simeq \{\pm 1\}$.

PROPOSITION 20.25. *Let* γ *be an automorphism of* (SL_2, T). *Then* γ *maps* U^+ *isomorphically onto* U^+ *or* U^- *according as* γ *acts as* $+1$ *or* -1 *on* T. *In the first case,* $\gamma = \gamma_t$ *for a unique* $t \in k^\times$, *and in the second case* $\gamma = \mathrm{inn}(n) \circ \gamma_t$ *for a unique* $t \in k^\times$.

PROOF. Let λ be the cocharacter $t \mapsto \mathrm{diag}(t, t^{-1})$ of SL_2. Then $U(\pm\lambda) = U^\pm$ (see 13.31) and γ maps $U(\lambda)$ isomorphically onto $U(\gamma \circ \lambda)$ (see 13.34). As $\gamma \circ \lambda$ equals $+\lambda$ or $-\lambda$ according as $\gamma|T$ equals $+1$ or -1, this proves the first statement. Suppose that $\gamma|T = +1$. As U^+ is isomorphic to $\mathbb{G}_a$, the restriction of γ to U^+ is multiplication by some $t \in k^\times$ (see 14.59). Now $\gamma_{t^{-1}} \circ \gamma$ acts as the identity map on $B^+ = T \cdot U^+$, and hence on G (see 17.21). This shows that $\gamma = \gamma_t$. If $\gamma|T = -1$, then $\mathrm{inn}(n) \circ \gamma|T = 1$, and so $\mathrm{inn}(n) \circ \gamma = \gamma_t$.   □

COROLLARY 20.26. *Let* γ *be an automorphism of* (SL_2, T). *If* $\gamma|T = \mathrm{id}$ *and* γ *fixes some nonzero element of* U^+, *then* γ *is the identity map.*

PROOF. We know that $\gamma = \gamma_t$ for some $t \in k^\times$, and γ_t acts on U^+ as multiplication by t.   □

The action of GL_2 on SL_2 by inner automorphisms defines an action of PGL_2 on SL_2.

THEOREM 20.27. *The action of* PGL$_2$ *on* SL$_2$ *by inner automorphisms defines isomorphisms*

$$\text{PGL}_2(k) \to \text{Aut}(\text{SL}_2),$$
$$(N/\mu_2)(k) \to \text{Aut}(\text{SL}_2, T) \text{ where } N = N_{\text{SL}_2}(T),$$
$$(T/\mu_2)(k) \to \text{Aut}(\text{SL}_2, T, U^+).$$

PROOF. The centralizer of SL$_2$ in GL$_2$ is $\mathbb{D}_2$, and so the first map is injective. Let γ be an automorphism of SL$_2$. If T' and T'' are split maximal tori in SL$_2$, then $T' \cdot \mathbb{G}_m$ and $T'' \cdot \mathbb{G}_m$ are split maximal tori in GL$_2$, and so they are conjugate by an element of GL$_2(k)$ (see 17.89). Hence T' and T'' are conjugate by an element of PGL$_2(k)$. Therefore, after possibly composing γ with conjugation by an element of PGL$_2(k)$, we may suppose that $\gamma(T) = T$. Now Proposition 20.25 shows that the first map is surjective because γ_t is the automorphism of SL$_2$ defined by the element $[\text{diag}(t, 1)]$ of PGL$_2(k)$.

We saw in Proposition 20.25 that the automorphisms of SL$_2$ mapping T into T and U^+ into U^+ are exactly the automorphisms γ_t for $t \in k^\times$. The map $\text{diag}(t, t^{-1}) \to t^2$ defines an isomorphism $T/\mu_2 \to \mathbb{G}_m$, and hence an isomorphism $(T/\mu_2)(k) \to k^\times$. If $a \in (T/\mu_2)(k)$ maps to $t \in k^\times$, then $\text{inn}(a)$ acts on SL$_2$ as γ_t. This proves that the second map is an isomorphism, and the third follows using that $N = T \sqcup Tn$ (see 17.42). □

REMARK 20.28. Similar arguments show that the natural homomorphisms

$$\text{PGL}_2(k) \to \text{Aut}(\text{GL}_2), \quad \text{PGL}_2(k) \to \text{Aut}(\text{PGL}_2)$$

are isomorphisms. In fact,

$$\text{PGL}_2 \simeq \underline{\text{Aut}}(\text{SL}_2) \simeq \underline{\text{Aut}}(\text{GL}_2) \simeq \underline{\text{Aut}}(\text{PGL}_2),$$

i.e., the functors $R \rightsquigarrow \text{Aut}(G_R)$ are representable by PGL$_2$ for $G = \text{SL}_2$, GL$_2$, or PGL$_2$. See Remark 23.50 below.

REMARK 20.29. Theorem 20.27 says that every automorphism of SL$_2$ is inner in the sense that it arises from an element of the adjoint group. For $t \in k^\times \smallsetminus k^{\times 2}$,

$$\begin{pmatrix} \sqrt{t} & 0 \\ 0 & \sqrt{t^{-1}} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \sqrt{t^{-1}} & 0 \\ 0 & \sqrt{t} \end{pmatrix} = \begin{pmatrix} a & tb \\ t^{-1}c & d \end{pmatrix}, \qquad (131)$$

and so γ_t is conjugation by an element of SL$_2(k^a)$, but not of SL$_2(k)$. In other words, it is an inner automorphism of SL$_2$ but an outer automorphism of SL$_2(k)$. This reflects the fact that the map SL$_2(k) \to \text{PGL}_2(k)$ is not surjective in general.

PROPOSITION 20.30. *The Picard groups of* SL$_n$ *and* GL$_n$ *are zero.*

PROOF. The polynomial ring $k[X_{11}, X_{12}, \ldots, X_{nn}]$ is a unique factorization domain (CA 4.10), and remains so after $\det(X_{ij})$ has been inverted. Therefore $\text{Pic}(\text{GL}_n) = 0$. In 2.42 we saw that $\text{GL}_n \simeq \text{SL}_n \times \mathbb{G}_m$ as schemes, from which it follows that $\text{Pic}(\text{SL}_n) = 0$. □

PROPOSITION 20.31. *The algebraic group* SL_2 *is simply connected, the map* $SL_2 \to PGL_2$ *is the universal covering of* PGL_2, *and* $\pi_1(PGL_2) = \mu_2$.

PROOF. This was shown in Example 18.20, but we give a direct proof. Recall that the algebraic group GL_2 is reductive and its split maximal tori are the conjugates of the diagonal torus (17.89). It follows that PGL_2 is reductive, and its split maximal tori are the conjugates of the diagonal torus; in particular, each is isomorphic to $\mathbb{G}_m$.

Let $\varphi: G \to PGL_2$ be a multiplicative isogeny of connected group varieties. Then G is reductive because $R_u(G_{k^a})$ maps isomorphically onto its image in PGL_2, which is trivial. Let T be a maximal torus in G. The kernel N of φ is central, and so it is contained in T (see 17.61). The image T/N of T in PGL_2 is isomorphic to $\mathbb{G}_m$, and so T is isomorphic to $\mathbb{G}_m$. Thus, $N \approx \mu_m$ for some m. We show that $m \le 2$. For this, we may suppose that k is algebraically closed. The image $\bar{n}$ of n in $PGL_2(k)$ normalizes the diagonal torus and acts on it as $t \mapsto t^{-1}$. Therefore, a suitable conjugate n' of $\bar{n}$ normalizes T/N and acts on it as $t \mapsto t^{-1}$. Every lift of n' to $G(k)$ acts on T as its unique nontrivial automorphism $t \mapsto t^{-1}$. As N is central, the action is trivial on it, and so $m \le 2$.

Let $\varphi: G \to SL_2$ be a multiplicative isogeny of connected group varieties. Its composite with $SL_2 \to PGL_2$ has degree at most 2, and so φ is an isomorphism. Hence SL_2 is simply connected. □

h. Classification of the split reductive groups of semisimple rank 1

We let T_2 denote the diagonal torus in SL_2 and N its normalizer.

PROPOSITION 20.32. *Let* (G, T) *be a split reductive group of semisimple rank 1. There exists a homomorphism* $v: (SL_2, T_2) \to (G, T)$ *with central kernel. Every such homomorphism is a central isogeny from* SL_2 *onto the derived group of* G, *and any two differ by the inner automorphism defined by an element of* $(N/\mu_2)(k)$.

PROOF. Recall (20.22) that there exists an exact sequence

$$e \to Z(G) \longrightarrow G \xrightarrow{q} PGL_2 \to e.$$

The homomorphism q maps T onto a maximal split torus in PGL_2. After composing q with an inner automorphism of PGL_2, we may suppose that it maps T onto the diagonal torus in PGL_2.

Let $D = Z(G)$ and $G' = \mathcal{D}G$. Then $D_t \cap G'$ is finite and the sequence

$$e \to D_t \cap G' \to D_t \times G' \to G \to e$$

is exact (12.46). Moreover, $T' \overset{\text{def}}{=} (T \cap G')_t$ is a maximal split torus in G' (see 17.85). The restriction of q to $G' \to PGL_2$ is a multiplicative isogeny

mapping T' onto the diagonal torus, and so $\mathrm{SL}_2 \to \mathrm{PGL}_2$ lifts to a central isogeny $v' : (\mathrm{SL}_2, T_2) \to (G', T')$ by Proposition 20.31. The composite of this with the inclusion $G' \hookrightarrow G$ is the required homomorphism v.

Because SL_2 is perfect, the homomorphism v maps into G', and $v : \mathrm{SL}_2 \to G'$ is an isogeny with kernel e or μ_2 according as G' is simply connected or not. Now Proposition 18.8 implies that any two v differ by an automorphism of (SL_2, T_2), and so the uniqueness statement follows from Theorem 20.27. $\quad\square$

THEOREM 20.33. *Every split reductive group is isomorphic to exactly one of the groups*

$$\mathbb{G}_m^r \times \mathrm{SL}_2, \quad \mathbb{G}_m^r \times \mathrm{PGL}_2, \quad \mathbb{G}_m^{r-1} \times \mathrm{GL}_2 \quad (r \in \mathbb{N}).$$

PROOF. Because its adjoint group is perfect, G is the reductive group $G(\varphi)$ attached to a triple $(\mathrm{SL}_2, D, \varphi)$ with D a diagonalizable group and $\varphi : \mu_2 \to D$ an injective homomorphism whose cokernel is a torus (19.29). Now $\alpha = X^*(\varphi)$ is a surjective homomorphism $X^*(D) \to \mathbb{Z}/2\mathbb{Z}$ whose kernel is torsion-free. There are three cases to consider. In the first case, there exists a decomposition $X(D) = N \oplus \mathbb{Z}/2\mathbb{Z}$ such that $\alpha|N = 0$ and $\alpha|\mathbb{Z}/2\mathbb{Z} = \mathrm{id}$. In this case

$$G(\varphi) = D(N) \times \mathrm{SL}_2.$$

In the second case $\alpha = 0$. Then D is a torus T, and $G(\varphi) = T \times \mathrm{PGL}_2$. Finally, there may exist a decomposition $X^*(D) = N \oplus \mathbb{Z}$ such that $\alpha|N = 0$ and $\alpha|\mathbb{Z}$ is the quotient map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. In this case, $G(\varphi) = D(N) \times \mathrm{GL}_2$.

These exhaust the split reductive groups over k of semisimple rank 1. The derived groups are PGL_2 in the first case, and SL_2 in the second and third cases, while the centres are tori in the first two cases but not in the third, and so no two of the groups are isomorphic. $\quad\square$

As noted earlier (17.89), a split maximal torus T in GL_V defines a decomposition $V = \bigoplus_{i \in I} V_i$ of V into a direct sum of one-dimensional eigenspaces, and T is the subgroup of GL_V preserving the decomposition. As any two bases of V are conjugate by an element of $\mathrm{GL}_V(k)$, it follows that any two split maximal tori in GL_V are conjugate by an element of $\mathrm{GL}_V(k)$. Similar statements are true for SL_V and PGL_V.

COROLLARY 20.34. *Any two split maximal tori in a reductive group G over k of semisimple rank 1 are conjugate by an element of $G(k)$.*

PROOF. This is true for $T \times \mathrm{SL}_2$, $T \times \mathrm{GL}_2$, and $T \times \mathrm{PGL}_2$. $\quad\square$

i. The forms of SL_2, GL_2, and PGL_2

Let G be a reductive group of semisimple rank 1, and let T be a maximal torus in G. Then T splits over k^s, and so G is a k^s/k-form of one of the groups in Theorem 20.33. To determine the reductive groups of semisimple rank 1 over k, it remains to determine the k-forms of these groups. We begin by finding the k-forms of GL_2.

The forms of $M_2(k)$

An algebra A over k is a ***quaternion algebra*** if $A \otimes_k k^s$ is isomorphic to $M_2(k)$. In other words, A is a quaternion algebra if it is a k^s/k-form of $M_2(k)$.

Every automorphism of $M_2(k)$ as an algebra over k is inner by the Skolem–Noether theorem (24.23 below). Therefore $\mathrm{Aut}(M_2(k)) \simeq \mathrm{PGL}_2(k)$.

Let $\varGamma = \mathrm{Gal}(k^s/k)$, and let $H^1(k, G) = H^1(\varGamma, G(k^s))$. Let A be a quaternion algebra over k, and choose an isomorphism $a: M_2(k^s) \to A \otimes_k k^s$. Then $\tau \mapsto c_\tau = a^{-1} \circ \tau a$ is a continuous 1-cocycle for $\varGamma$ with values in $\mathrm{Aut}(M_2(k^s)) = \mathrm{PGL}_2(k^s)$ whose cohomology class does not depend on the choice of a. By descent theory, every cohomology class arises from a quaternion algebra, and so the isomorphism classes of quaternion algebras over k are classified by the elements of $H^1(k, \mathrm{PGL}_2)$. See Section 2k.

Forms of GL_2

Each quaternion algebra A over k defines a group-valued functor on k-algebras,

$$G^A: R \rightsquigarrow (A \otimes R)^\times.$$

There is a well-defined reduced norm homomorphism $\mathrm{Nrd}: A \to k$, which becomes the determinant function when $A = M_2(k)$ (see 24.25 below). In terms of a basis for A, the norm homomorphism is a polynomial function, and G^A is the subfunctor of $R \rightsquigarrow A \otimes R$ determined by the nonvanishing of this function. Thus, G^A is representable, and so it is an algebraic group over k.

If $A = M_2(k)$, then $G^A = \mathrm{GL}_2$. Otherwise, G^A is a k-form of GL_2.

THEOREM 20.35. *The functor $A \rightsquigarrow G^A$ defines a bijection from the set of isomorphism classes of quaternion algebras over k to the set of isomorphism classes of k-forms of GL_2.*

PROOF. Let G' be a k-form of GL_2, and choose an isomorphism $a: \mathrm{GL}_{2k^s} \to G_{k^s}$. Then $\tau \mapsto c_\tau = a^{-1} \circ \tau a$ is a continuous 1-cocycle for $\varGamma$ with values in $\mathrm{PGL}_2(k^s)$ whose cohomology class does not depend on the choice of a. In this way, $H^1(k, \mathrm{PGL}_2)$ classifies the isomorphism classes of k-forms of GL_2 (see 3.43). Let A be a quaternion algebra over k, and choose an isomorphism $a: M_2(k^s) \to A \otimes_k k^s$. Then a defines an isomorphism $a': \mathrm{GL}_{2k'} \to G^A_{k'}$, and a and a' give rise to the same 1-cocycle $\varGamma \to \mathrm{PGL}_2(k^s)$. Therefore, we have a commutative diagram

{isomorphism classes of quaternion algebras over k} $\quad\searrow$ $\;^{1:1}$

$$H^1(k, \mathrm{PGL}_2)$$

{isomorphism classes of k-forms of GL_2} $\quad\nearrow$ $\;^{1:1}$

from which the statement follows. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Forms of SL_2 *and* PGL_2

Let A be a quaternion algebra over k. The functor

$$S^A: R \rightsquigarrow \{a \in A \otimes R \mid \mathrm{Nrd}(a) = 1\}$$

is an algebraic group over k. We let

$$P^A = G^A/Z(G^A).$$

As in the previous case, the functors $A \rightsquigarrow S^A$ and $A \rightsquigarrow P^A$ define bijections from the set of isomorphism classes of quaternion algebras over k to the sets of isomorphism classes of k-forms of SL_2 and PGL_2.

j.   Classification of reductive groups of semisimple rank one

THEOREM 20.36. *Let T be a torus and A a quaternion algebra over k. Then $T \times S^A$, $T \times P^A$, and $T \times G^A$ are reductive groups of semisimple rank 1 over k, and every reductive group of semisimple rank 1 over k is isomorphic to one of these groups.*

PROOF. Let G be a reductive group of semisimple rank 1 over k. Then G splits over k^s, and so $G/Z(G)$ is a k-form of PGL_2. In particular, G^{ad} is perfect, and so G is equals $G(\varphi)$ for some triple (H, D, φ) with H the group S^A attached to a quaternion algebra A over k, D a group of multiplicative type over k, and $\varphi: \mu_2 \to D$ an injective homomorphism whose cokernel is a torus (19.29, 19.30). Again there are three cases to consider for the map $X^*(\varphi): X^*(D) \to \mathbb{Z}/2\mathbb{Z}$ of Γ-modules, which lead to the three groups in the statement of the theorem. $\quad\square$

The classification of the quaternion algebras

It remains to classify the quaternion algebras over k. Let k be a field of characteristic $\neq 2$. Let $a, b \in k^\times$, and define $H(a, b)$ to be the algebra over k with basis 1, i, j, ij as a k-vector space and with the multiplication

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Then $H(a, b)$ is a quaternion algebra, and every quaternion algebra over k is of this form for some $a, b \in k^\times$. A quaternion algebra is either a division algebra or it is isomorphic to $M_2(k)$, in which case it is said to be ***split***.

Over a finite field or a separably closed field, there are only the split quaternion algebras, but over $\mathbb{R}$ there is also Hamilton's quaternion algebra $H(-1, -1)$. Over $\mathbb{Q}$ (or a number field), the isomorphism classes of quaternion algebras are classified by the sets of primes with finite even cardinality. We sketch a proof of this statement.

Let k be $\mathbb{R}$ or a p-adic field $\mathbb{Q}_p$. For $a, b \in k^\times$, set $(a, b) = 1$ or -1 according as $z^2 - ax^2 - by^2 = 0$ has a nontrivial solution or not. An elementary argument

shows that a quaternion algebra $H(a,b)$ is split if and only if $(a,b) = 1$, and that there is (up to isomorphism) exactly one nonsplit quaternion algebra over k.

Let $a,b \in \mathbb{Q}^\times$. In the last paragraph, we defined a symbol $(a,b)_p$ for each prime p and one symbol $(a,b)_\infty$ corresponding to $\mathbb{R}$. The Hilbert product formula says that $(a,b)_p = 1$ for almost all p, and that

$$(a,b)_\infty \cdot \prod_p (a,b)_p = 1;$$

moreover, every possible family of ± 1s arises from a pair $a,b \in \mathbb{Q}^\times$ (Serre 1970, II, §2).

A quaternion algebra $H(a,b)$ over $\mathbb{Q}$ is determined up to isomorphism by the quaternion algebras $H(a,b) \otimes \mathbb{R}$ and $H(a,b) \otimes \mathbb{Q}_p$, and hence by the Hilbert symbols $(a,b)_\infty$ and $(a,b)_p$. Thus, a quaternion algebra $H(a,b)$ is determined by the set of primes p or ∞ for which it is nonsplit, i.e., for which $(a,b) = -1$. According to the product formula, this set has a finite even number of elements and every such set arises from a quaternion algebra.

k. Review of SL_2

Every semisimple group is built up from copies of SL_2, just as every Dynkin diagram is built up from copies of the Dynkin diagram of SL_2 and line segments. We collect here for future use some notation and facts concerning SL_2.

20.37. Let $G = \mathrm{SL}_2$ and let T_2 be the torus of diagonal matrices $\mathrm{diag}(t,t^{-1})$ in G. Then $X(T_2) = \mathbb{Z}\chi$, where χ is the character $\mathrm{diag}(t,t^{-1}) \mapsto t$. The Lie algebra of SL_2 is

$$\mathfrak{sl}_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) \ \middle|\ a + d = 0 \right\},$$

and T acts on $\mathfrak{sl}_2$ by conjugation (10.24):

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} a & t^2 b \\ t^{-2}c & d \end{pmatrix}. \tag{132}$$

Therefore,

$$\mathfrak{sl}_2 = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}, \quad \mathfrak{g}_\alpha = \left\{ \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \right\}, \quad \mathfrak{g}_{-\alpha} = \left\{ \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix} \right\}$$

where T_2 acts on $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ through the characters $\alpha = 2\chi$ and $-\alpha$ respectively.

20.38. Let λ be the isomorphism $t \mapsto \mathrm{diag}(t,t^{-1}) \colon \mathbb{G}_m \to T_2$. Then

$$U^+ \overset{\mathrm{def}}{=} U(\lambda) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}, \quad \mathrm{Lie}(U^+) = \mathfrak{g}_\alpha$$

$$U^- \overset{\mathrm{def}}{=} U(-\lambda) = \left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\}, \quad \mathrm{Lie}(U^-) = \mathfrak{g}_{-\alpha}$$

(see 13.31). The map $a \mapsto \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ is an isomorphism $u_\alpha \colon \mathbb{G}_a \to U^+$ with the property that

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \quad \text{all } t \in T(R), \quad a \in \mathbb{G}_a(R)$$

(see (132)). Similarly, $a \mapsto \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$ is an isomorphism $u_{-\alpha} \colon \mathbb{G}_a \to U^-$ with the property that

$$t \cdot u_{-\alpha}(a) \cdot t^{-1} = u_{-\alpha}(-\alpha(t)a), \quad \text{all } t \in T(R), \quad a \in \mathbb{G}_a(R).$$

The Borel subgroups containing T_2 are $B^+ = U^+ \cdot T$ and $B^- = U^- \cdot T$.

20.39. Let $n_\alpha = u_\alpha(1)u_{-\alpha}(-1)u_\alpha(1)$. Then $n_\alpha = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and

$$N_G(T) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\} \sqcup \left\{ \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix} \right\} = T_2 \sqcup T_2 n_\alpha.$$

Therefore $W(G,T) = \{1, s\}$, where s is represented by n_α. Note that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

and so s acts as -1 on T_2 and swaps B^+ and B^-.

20.40. Let $\alpha^\vee$ be the cocharacter $t \mapsto \operatorname{diag}(t, t^{-1})$ of T. Then $\langle \alpha, \alpha^\vee \rangle = 2 = \langle -\alpha, -\alpha^\vee \rangle$, and

$$s(\chi) = s_\alpha(\chi) \overset{\text{def}}{=} \chi - \langle \chi, \alpha^\vee \rangle \alpha, \quad s(\chi) = s_{-\alpha}(\chi) \overset{\text{def}}{=} \chi - \langle \chi, -\alpha^\vee \rangle (-\alpha),$$

for all $\chi \in X^*(T)$. Note that $s(\alpha) = -\alpha$ and $s(-\alpha) = \alpha$.

20.41. The following identities can be checked by direct calculation

$$\begin{cases} u_\alpha(t)u_{-\alpha}(-t^{-1})u_\alpha(t) = \alpha^\vee(t)n_\alpha \\ \qquad\qquad n_\alpha^2 = \alpha^\vee(-1). \end{cases}$$

Let $n_{-\alpha} = u_{-\alpha}(1)u_\alpha(-1)u_{-\alpha}(1)$. Then $n_{-\alpha} = n_\alpha^{-1}$. For each $u \in U^+ \smallsetminus \{e\}$, there is a unique $u' \in U^- \smallsetminus \{e\}$ such that $uu'u \in N_{\mathrm{SL}_2}(T_2)$.

Exercises

EXERCISE 20-1. Show that $\mathrm{SL}_2 = T_2U^+ \cup U^+ n_\alpha T_2 U^+$; in particular, SL_2 is generated by T_2, U^+, and n_α.

Split Reductive Groups

In this chapter, we reap the reward of our hard work in the earlier chapters and determine the structure of split reductive groups. We assume some familiarity with root systems and root data (Appendix C). The field k is arbitrary.

a. Split reductive groups and their roots

Let G be a reductive algebraic group over k. Recall (17.59) that the centralizer of a torus in G is also a reductive algebraic group (in particular, it is smooth and connected), and (17.84) that a torus T in G is maximal if and only if $C_G(T) = T$. Maximal tori remain maximal after extension of the base field.

Recall also that G is split if some maximal torus T is split, in which case we refer to the pair (G, T) as a split reductive group. The centralizer of T in G equals the identity component of its normalizer, and the Weyl group $W(G, T)$ of (G, T) is defined to be the étale group scheme

$$\pi_0(N_G(T)) = N_G(T)/C_G(T) = N_G(T)/T.$$

PROPOSITION 21.1. *The Weyl group $W(G, T)$ of a split reductive group (G, T) is a finite constant algebraic group. For every field k' containing k,*

$$W(G, T)(k) = W(G, T)(k') = N(k')/T(k'), \quad N = N_G(T).$$

PROOF. By definition, $W(G, T)$ acts faithfully on T, and hence on $X^*(T)$. As T is split, $\mathrm{Gal}(k^s/k)$ acts trivially on $X^*(T)$, and hence on the subgroup $W(G, T)(k^s)$ of $\mathrm{Aut}(X^*(T))$. Therefore $W(G, T)$ is constant, and so, for all fields k' containing k, $W(G, T)(k) = W(G, T)(k') = (N/T)(k')$. As T is split, $H^1(k', T) = 1$ (see 3.47), and so the sequence

$$1 \to T(k') \to N(k') \to (N/T)(k') \to 1$$

is exact (3.45). Therefore $N(k')/T(k') \simeq (N/T)(k')$. □

Let (G, T) be a split reductive group over k, and let $\mathrm{Ad}: G \to \mathrm{GL}_{\mathfrak{g}}$ be the adjoint representation (10.20). Then T acts on $\mathfrak{g}$ and, because T is diagonalizable, $\mathfrak{g}$ decomposes into a direct sum

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in X(T)} \mathfrak{g}_\alpha$$

with $\mathfrak{g}_0 = \mathfrak{g}^T$ and $\mathfrak{g}_\alpha$ the subspace on which T acts through a nontrivial character α. The characters α of T occurring in this decomposition are called the **roots** of (G, T). They form a finite subset $\Phi(G, T)$ of $X(T)$. Note that

$$\mathfrak{g}_0 = \mathrm{Lie}(G)^T \overset{10.34}{=} \mathrm{Lie}(G^T) = \mathrm{Lie}(C_G(T)) = \mathrm{Lie}(T),$$

and so[1]

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi(G,T)} \mathfrak{g}_\alpha.$$

We next show that the action of $W(G, T)$ on $X(T)$ stabilizes $\Phi(G, T)$.

PROPOSITION 21.2. *Let $s \in W(G, T)$ and let α be a root of (G, T). Then $s\alpha$ is also a root of (G, T), and $\mathfrak{g}_{s\alpha} = s\mathfrak{g}_\alpha$.*

PROOF. Let $n \in N_G(T)(k)$ represent s, and let $t \in T(R)$ for some k-algebra R. Then s acts on $\chi \in X(T)$ by the rule $(s\chi)(t) = \chi(n^{-1}tn)$. For $x \in \mathfrak{g}_\alpha$, $t(sx) = t(nx) = n(n^{-1}tn)x = n(\alpha(n^{-1}tn)x) = \alpha(n^{-1}tn)(nx) = ((s\alpha)(t))(sx)$, and so T acts on $s\mathfrak{g}_\alpha$ through the character $s\alpha$, as claimed. □

EXAMPLE 21.3. Let $(G, T) = (\mathrm{GL}_2, T)$ with T the diagonal torus in G. Then $X(T) = \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2$, where $m_1\chi_1 + m_2\chi_2$ is the character $\mathrm{diag}(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2}$. The Lie algebra $\mathfrak{g}$ of GL_2 is $M_2(k)$ with the bracket $[A, B] = AB - BA$, and T acts on $\mathfrak{g}$ by conjugation (10.24):

$$\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{t_1}{t_2}b \\ \frac{t_2}{t_1}c & d \end{pmatrix}. \tag{133}$$

Let E_{ij} denote the matrix with a 1 in the ijth position and zeros elsewhere. Then T acts trivially on $\mathfrak{g}_0 = kE_{11} + kE_{22}$, through the character $\alpha = \chi_1 - \chi_2$ on $\mathfrak{g}_\alpha = kE_{12}$, and through the character $-\alpha = \chi_2 - \chi_1$ on $\mathfrak{g}_{-\alpha} = kE_{21}$. Thus, $\Phi(G, T) = \{\alpha, -\alpha\}$ with $\alpha = \chi_1 - \chi_2$. When we use χ_1 and χ_2 to identify $X(T)$ with $\mathbb{Z} \oplus \mathbb{Z}$, the set Φ becomes identified with $\{\pm(e_1 - e_2)\}$, where $\{e_1, e_2\}$ is the standard basis for $\mathbb{Z}^2$.

EXAMPLE 21.4. The roots of (SL_2, T_2) are $\pm\alpha$, where $\mathrm{diag}(t, t^{-1}) \overset{\alpha}{\mapsto} t^2$ (20.37).

---

[1]The Lie algebra of T is often denoted by $\mathfrak{h}$.

EXAMPLE 21.5. Let $G = \mathrm{PGL}_2$. Recall (5.49) that this is defined to be the quotient of GL_2 by its centre $\mathbb{G}_m$, and that $\mathrm{PGL}_2(k) = \mathrm{GL}_2(k)/k^\times$. We let T be the diagonal torus

$$T = \left\{ \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \,\middle|\, t_1 t_2 \neq 0 \right\} \Big/ \left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \,\middle|\, t \neq 0 \right\}.$$

Then $X(T) = \mathbb{Z}\chi$, where χ is the character $\mathrm{diag}(t_1, t_2) \mapsto t_1/t_2$. The Lie algebra of PGL_2 is

$$\mathfrak{pgl}_2 = \mathfrak{gl}_2/\{\text{scalar matrices}\},$$

and T acts on $\mathfrak{pgl}_2$ by conjugation (133). Therefore, the roots are $\alpha = \chi$ and $-\alpha = -\chi$. When we use χ to identify $X(T)$ with $\mathbb{Z}$, $\Phi(G, T)$ becomes identified with $\{1, -1\}$.

EXAMPLE 21.6. Let $G = \mathrm{GL}_n$, and let T be the diagonal torus $\mathbb{D}_n$ in G. Then $X(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i$, where χ_i is the character $\mathrm{diag}(t_1, \ldots, t_n) \mapsto t_i$. The Lie algebra of GL_n is

$$\mathfrak{gl}_n = M_n(k) \text{ with } [A, B] = AB - BA,$$

and T acts on $\mathfrak{g}$ by conjugation (10.20):

$$
\begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_n \end{pmatrix}
\begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & a_{ij} & \vdots \\ \vdots & & & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}
\begin{pmatrix} t_1^{-1} & & 0 \\ & \ddots & \\ 0 & & t_n^{-1} \end{pmatrix}
$$

$$
= \begin{pmatrix} a_{11} & \cdots & \cdots & \frac{t_1}{t_n}a_{1n} \\ \vdots & & \frac{t_i}{t_j}a_{ij} & \vdots \\ \vdots & & & \vdots \\ \frac{t_n}{t_1}a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}.
$$

Therefore T acts through the character $\alpha_{ij} = \chi_i - \chi_j$ on $\mathfrak{g}_{\alpha_{ij}} = k E_{ij}$. The set of roots is

$$\Phi(G, T) = \{\alpha_{ij} \mid 1 \leq i, j \leq n, \quad i \neq j\}.$$

When we use the χ_i to identify $X(T)$ with $\mathbb{Z}^n$, then $\Phi(G, T)$ becomes identified with

$$\{e_i - e_j \mid 1 \leq i, j \leq n, \quad i \neq j\}$$

where $e_1, \ldots, e_n$ is the standard basis for $\mathbb{Z}^n$.

b.   Centres of reductive groups

It is possible to compute the centre of a split reductive group from its roots.

PROPOSITION 21.7. *Let G be a reductive algebraic group, and let T be a maximal torus in G. The centre $Z(G)$ of G is contained in T, and is equal to the kernel of* $\mathrm{Ad}\colon T \to \mathrm{GL}_{\mathfrak{g}}$.

PROOF. As $Z(G)$ centralizes T, it is contained in $C_G(T) = T$. Certainly $Z(G)$ is contained in the kernel of the adjoint map $\mathrm{Ad}\colon G \to \mathrm{GL}_{\mathfrak{g}}$, and so $Z(G) \subset \mathrm{Ker}(\mathrm{Ad}|T)$. The quotient $\mathrm{Ker}(\mathrm{Ad})/Z(G)$ is unipotent (14.23), and so the image of $\mathrm{Ker}(\mathrm{Ad}|T)$ in $\mathrm{Ker}(\mathrm{Ad})/Z(G)$, being both multiplicative and unipotent, is trivial (14.16). Thus $\mathrm{Ker}(\mathrm{Ad}|T) \subset Z(G)$. $\qquad\square$

PROPOSITION 21.8. *Let (G,T) be a split reductive group, and let $\mathbb{Z}\Phi$ denote the $\mathbb{Z}$-submodule of $X^*(T)$ generated by the roots. Then*

$$X^*(Z(G)) = X^*(T)/\mathbb{Z}\Phi,$$

and so $Z(G)$ is the diagonalizable subgroup of T with character group $X(T)/\mathbb{Z}\Phi$.

PROOF. As T acts on $\mathfrak{g}$ through the characters $\alpha \in \Phi(G,T)$,

$$Z(G) \overset{21.7}{=} \bigcap_{\alpha \in \Phi(G,T)} \mathrm{Ker}(\alpha\colon T \to \mathbb{G}_m).$$

From this we get an exact sequence

$$0 \to Z(G) \to T \xrightarrow{t \mapsto (\alpha(t))_\alpha} \prod_{\alpha \in \Phi} \mathbb{G}_m.$$

On applying X^* to this sequence, we get an exact sequence

$$\bigoplus_{\alpha \in \Phi} \mathbb{Z} \xrightarrow{(m_\alpha)_\alpha \mapsto \sum m_\alpha \alpha} X^*(T) \to X^*(Z(G)) \to 0$$

(see 12.23), which gives the required equality. $\qquad\square$

COROLLARY 21.9. *The quotient $T/Z(G)$ of T has character group the subgroup $\mathbb{Z}\Phi$ of $X^*(T)$.*

PROOF. Because $T/Z(G)$ is the cokernel of $Z(G) \to T$, its character group is the kernel of $X^*(T) \to X^*(Z(G))$, which equals $\mathbb{Z}\Phi$. $\qquad\square$

For example (21.4, 21.5, 21.6),

$$Z(\mathrm{SL}_2) = \mathrm{Ker}(2\chi) = \{\mathrm{diag}(t,t^{-1}) \mid t^2 = 1\} = \mu_2$$
$$X^*(Z(\mathrm{SL}_2)) = \mathbb{Z}\chi/\mathbb{Z}2\chi \simeq \mathbb{Z}/2\mathbb{Z}$$
$$Z(\mathrm{PGL}_2) = \mathrm{Ker}(\chi) = 1$$
$$X^*(Z(\mathrm{PGL}_2)) = \mathbb{Z}/\mathbb{Z} = 0$$
$$Z(\mathrm{GL}_n) = \bigcap_{i \neq j} \mathrm{Ker}(\chi_i - \chi_j) = \{\mathrm{diag}(t,\dots,t) \mid t \neq 0\} = \mathbb{G}_m$$
$$X^*(Z(\mathrm{GL}_n)) = \mathbb{Z}^n \Big/ \sum_{i \neq j} \mathbb{Z}(e_i - e_j) \simeq \mathbb{Z} \quad \text{by } (a_i) \mapsto \sum a_i.$$

c.   The root datum of a split reductive group

We briefly review the notion of a root datum (see Appendix C). Let X be a free $\mathbb{Z}$-module of finite rank, let $X^\vee$ denote the linear dual $\mathrm{Hom}(X, \mathbb{Z})$ of X, and let $\langle\,,\,\rangle\colon X \times X^\vee \to \mathbb{Z}$ denote the perfect pairing $\langle x, f\rangle = f(x)$.

Let α be an element of X and $\alpha^\vee$ an element of $X^\vee$ such that $\langle \alpha, \alpha^\vee\rangle = 2$. The linear map

$$s_\alpha \colon X \to X, \quad s_\alpha(x) = x - \langle x, \alpha^\vee\rangle\alpha$$

fixes the elements of the hyperplane $H = \{x \in X \mid \langle x, \alpha^\vee\rangle = 0\}$ in X and sends α to $-\alpha$. We regard s_α as a reflection with vector α.

Let Φ be a finite subset of X and $\alpha \mapsto \alpha^\vee$ a map $\Phi \to X^\vee$. The triple $\mathcal{R} = (X, \Phi, \alpha \mapsto \alpha^\vee)$ is a root datum if (rd1) $\langle \alpha, \alpha^\vee\rangle = 2$, (rd2) $s_\alpha(\Phi) \subset \Phi$ for all $\alpha \in \Phi$, and (rd3) the group $W(\mathcal{R})$ of automorphisms of X generated by the reflections s_α is finite (it is called the Weyl group of $\mathcal{R}$). The map $\alpha \mapsto \alpha^\vee$ (if it exists) is bijective onto its image $\Phi^\vee \subset X^\vee$ and is uniquely determined by $\Phi^\vee$. We sometimes write $(X, \Phi, \Phi^\vee)$ for a root datum. The root datum is reduced if, for every $\alpha \in \Phi$, the only rational multiples of α in Φ are $\pm\alpha$.

The main theorem

Let (G, T) be a split reductive group over k. For a root α of (G, T), we let $T_\alpha = \mathrm{Ker}(\alpha)_t$ (subtorus of T of codimension 1) and $G_\alpha = C_G(T_\alpha)$.

DEFINITION 21.10. The ***root group*** U_α of α is the algebraic subgroup $U_{G_\alpha}(\lambda)$ of G, where λ is any cocharacter λ of T such that $\langle \alpha, \lambda\rangle > 0$.

In the next theorem, we show that U_α is isomorphic to $\mathbb{G}_a$. We always use u_α to denote an isomorphism $\mathbb{G}_a \to U_\alpha$.

By definition, U_α is the unique connected subgroup variety of G such that

$$U_\alpha(k^a) = \{g \in G(k^a) \mid g \text{ centralizes } T_\alpha(k^a) \text{ and } \lim_{t\to 0} \lambda(t)g = e\}$$

(see 13.30). It is also the unique connected subgroup variety of G normalized by T whose Lie algebra has weights the positive rational multiples of α in Φ (see 16.64). In particular, it is independent of λ.

THEOREM 21.11. *Let (G, T) be a split reductive group over k, and let α be a root of (G, T).*

(a) *The pair (G_α, T) is a split reductive group of semisimple rank 1.*

(b) *The Lie algebra of G_α satisfies*

$$\mathrm{Lie}(G_\alpha) = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

with $\mathfrak{t} = \mathrm{Lie}(T)$ and $\dim \mathfrak{g}_\alpha = 1 = \dim \mathfrak{g}_{-\alpha}$. The only rational multiples of α in $\Phi(G, T)$ are $\pm\alpha$.

(c) *The root group U_α is normalized by T, is isomorphic to $\mathbb{G}_a$, and has Lie algebra $\mathfrak{g}_\alpha$. Any other subgroup variety of G normalized by T contains U_α if and only if its Lie algebra contains $\mathfrak{g}_\alpha$.*

(d) *The Weyl group $W(G_\alpha, T)$ contains exactly one nontrivial element s_α, and s_α is represented by an $n_\alpha \in N_{G_\alpha}(T)(k)$.*

(e) *There is a unique $\alpha^\vee \in X_*(T)$ such that*

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad \text{for all } x \in X(T). \tag{134}$$

Moreover, $\langle \alpha, \alpha^\vee \rangle = 2$.

(f) *The algebraic group G is generated by T and its root groups U_α ($\alpha \in \Phi(G,T)$).*

PROOF. Our assumption that there exists a root implies that $G \neq T$.

(a) The group G_α is reductive because it is the centralizer of a torus in a reductive group (17.59), and T is a split maximal torus in G_α. The semisimple rank of G_α is the dimension of the image of T in $G_\alpha/R(G_\alpha)$. As $T_\alpha \subset Z(G_\alpha)^\circ = R(G_\alpha)$, this dimension is 0 or 1. If it were 0, then $T \subset R(G_\alpha) \subset Z(G_\alpha)$ and $G_\alpha \subset C_G(T) = T$, which implies that $\mathrm{Lie}(G_\alpha) \subset \mathfrak{t}$, contradicting

$$\mathrm{Lie}(G_\alpha) = \mathrm{Lie}(G^{T_\alpha}) \overset{10.34}{=} \mathfrak{g}^{T_\alpha} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \cdots.$$

(b) Because (G_α, T) is split reductive of semisimple rank 1, there exist homomorphisms $q: G_\alpha \to \mathrm{PGL}_2$ and $v_\alpha: \mathrm{SL}_2 \to G_\alpha$ with central kernels such that the diagrams

$$
\begin{array}{ccccccc}
 & & & & \mathrm{SL}_2 & & \\
 & & & \overset{v_\alpha}{\swarrow} & \downarrow & & \\
e \longrightarrow & Z(G_\alpha) & \longrightarrow & G_\alpha & \overset{}{\underset{q}{\longrightarrow}} \mathrm{PGL}_2 & \longrightarrow e
\end{array}
\qquad
\begin{array}{ccccc}
 & & & T_2 & \\
 & \overset{v_\alpha|T_2}{\swarrow} & & \downarrow 2 & \\
T & \underset{q|T}{\longrightarrow} & T_2 & &
\end{array}
$$

are exact and commutative; moreover, v_α is an isogeny from SL_2 onto the derived group G'_α of G_α (20.32). Here T_2 denotes the diagonal maximal torus in SL_2 or PGL_2. The quotient G_α/G'_α is a torus, and so $U_\alpha \subset G'_\alpha$.

Let λ be the cocharacter $t \mapsto \mathrm{diag}(t, t^{-1})$ of T_2. Then v_α maps $U^+ = U_{\mathrm{SL}_2}(\lambda)$ onto $U_{G'_\alpha}(v_\alpha \circ \lambda) = U_{G_\alpha}(v_\alpha \circ \lambda) = U_\alpha$ (see 13.34). In fact, v_α maps U^+ isomorphically onto U_α because the kernel of v_α is contained in T_2, and so $U_\alpha \approx \mathbb{G}_a$. As noted earlier, the weights of T on $\mathrm{Lie}(U_\alpha)$ are the positive multiples of α in Φ. It follows that $\mathrm{Lie}(U_\alpha) = \mathfrak{g}_\alpha$, that $\mathfrak{g}_\alpha$ has dimension 1, and that the only rational multiples of α in Φ are $\pm\alpha$.

(c) We have shown that U_α is isomorphic to $\mathbb{G}_a$, and that $\mathrm{Lie}(U_\alpha) = \mathfrak{g}_\alpha$. The rest of (c) follows from Proposition 16.64.

(d) The Weyl group $W(G_\alpha, T)$ has order 2 because it acts simply transitively on the Borel subgroups containing T, of which there are exactly two (17.53,

20.20). Let n_α be as in 20.39. Then $v_\alpha(n_\alpha) \in N_{G_\alpha}(T)(k)$ and represents a nontrivial element s_α of $W(G_\alpha, T)$.

(e) Let α' be the cocharacter $t \mapsto \mathrm{diag}(t, t^{-1})$ of T_2. Then $\alpha^\vee = v_\alpha \circ \alpha'$ is the unique cocharacter of T satisfying the condition (134); moreover, $\langle \alpha, \alpha^\vee \rangle = 2$.

(f) The Lie algebra of G is generated by the Lie algebras of T and of the U_α, and so we can apply Corollary 10.17. $\square$

COROLLARY 21.12. *The system $(X(T), \Phi(G, T), \alpha \mapsto \alpha^\vee)$ is a reduced root datum.*

PROOF. We have to show that the map $\alpha \mapsto \alpha^\vee$ satisfies the conditions (rd1), (rd2), and (rd3). The first was checked in (e) of the theorem. The reflection s_α of $X(T)$ lies in $W(G_\alpha, T) \subset W(G, T)$, and so it stabilizes Φ by Proposition 21.2. We have $W(\mathcal{R}) \subset W(G, T)$ (as groups of automorphisms of $X(T)$), and $W(G, T)$ is finite by definition. Thus, $(X, \Phi, \alpha \mapsto \alpha^\vee)$ is a root datum, and (b) of the theorem shows that it is reduced. $\square$

COROLLARY 21.13. *The dimension of G is $\dim T + |\Phi|$.*

PROOF. From $\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$ and (b) of the theorem, we see that $\dim \mathfrak{g} = \dim \mathfrak{t} + |\Phi|$. This implies the statement because G and T are smooth. $\square$

ASIDE 21.14. If $\mathrm{char}(k) \neq 2$, then the map $\mathrm{Lie}(SL_2) \to \mathrm{Lie}(PGL_2)$ is an isomorphism, and so the first diagram gives a T-equivariant decomposition

$$\mathrm{Lie}(G_\alpha) = \mathrm{Lie}(Z(G_\alpha)) \oplus \mathrm{Lie}(SL_2).$$

This simplifies the proof.

EXAMPLE 21.15. The only root data of semisimple rank 1 are the systems $(\mathbb{Z}^r, \{\pm\alpha\}, \{\pm\alpha^\vee\})$ with

$$\begin{cases} \alpha = 2e_1 \\ \alpha^\vee = e_1', \end{cases} \qquad \begin{cases} \alpha = e_1 \\ \alpha^\vee = 2e_1', \end{cases} \quad \text{or} \quad \begin{cases} \alpha = e_1 + e_2 \\ \alpha^\vee = e_1' + e_2'. \end{cases}$$

Here $e_1, e_2, \ldots$ and $e_1', e_2', \ldots$ are the standard dual bases, and $r \geq 2$ in the third case. These are the root data of the groups

$$\mathbb{G}_m^{r-1} \times SL_2, \quad \mathbb{G}_m^{r-1} \times PGL_2, \quad \mathbb{G}_m^{r-2} \times GL_2.$$

EXAMPLE 21.16. Let $(G, T) = (GL_n, \mathbb{D}_n)$, and let $\alpha = \alpha_{12} = \chi_1 - \chi_2$ (see 21.6). Then $T_\alpha = \{\mathrm{diag}(x, x, x_3, \ldots, x_n) \mid xxx_3 \cdots x_n \neq 1\}$ and

$$G_\alpha = \left\{ \begin{pmatrix} * & * & 0 & & 0 \\ * & * & 0 & & 0 \\ 0 & 0 & * & & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & * \end{pmatrix} \in GL_n \right\}.$$

Moreover

$$
n_\alpha =
\begin{pmatrix}
0 & 1 & 0 & & & 0 \\
1 & 0 & 0 & & & 0 \\
0 & 0 & 1 & & & 0 \\
& & & \ddots & & \vdots \\
0 & 0 & 0 & \cdots & & 1
\end{pmatrix}
$$

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 (134), p. 429, holds if and only if $\alpha^\vee$ is taken to be $\lambda_1 - \lambda_2$. In general, the coroot $\alpha_{ij}^\vee$ of α_{ij} is

$$
t \mapsto \mathrm{diag}(1, \ldots, 1, \overset{i}{t}, 1, \ldots, 1, \overset{j}{t^{-1}}, 1, \ldots, 1).
$$

Clearly $\langle \alpha_{ij}, \alpha_{ij}^\vee \rangle = \alpha_{ij} \circ \alpha_{ij}^\vee = 2$. The associated root system is that in (C.16).

Notes

21.17. The root datum attached to a split reductive group does not change under extension of the base field. This is obvious from its definition.

21.18. Let T and T' be split maximal tori in a reductive group G. Then $T' = \mathrm{inn}(g)(T)$ for some $g \in G(k)$ (see 17.105). The isomorphism $\mathrm{inn}(g) \colon (G, T) \to (G, T')$ induces an isomorphism of root data $\mathcal{R}(G, T) \to \mathcal{R}(G, T')$ – we explain this in 23.5 below. Therefore the isomorphism class of $\mathcal{R}(G, T)$ depends only on G, not on the maximal torus.

21.19. Recall (14.59) that an algebraic group U isomorphic to $\mathbb{G}_a$ has a canonical action of $\mathbb{G}_m$. The root group U_α is the unique T-stable algebraic subgroup of G isomorphic to $\mathbb{G}_a$ on which T acts through the character α. The last condition means that, for every isomorphism $u \colon \mathbb{G}_a \to U_\alpha$,

$$
t \cdot u(a) \cdot t^{-1} = u(\alpha(t)a), \text{ all } t \in T(R), a \in \mathbb{G}_a(R). \tag{135}
$$

There is a unique isomorphism of algebraic groups $u_\alpha \colon (\mathfrak{g}_\alpha)_a \to U_\alpha \subset G$ such that $\mathrm{Lie}(u_\alpha)$ is the given inclusion $\mathfrak{g}_\alpha \hookrightarrow \mathfrak{g}$.

21.20. It follows from Theorem 21.11(c) that the root groups of (G, T) are exactly the T-stable algebraic subgroups of G isomorphic to $\mathbb{G}_a$. As the roots (G, T) are exactly the characters of T arising root groups, this gives a description of the root system of (G, T) not involving Lie algebras.

21.21. Let α and β be roots for (G,T). The commutator subgroup $[U_\alpha, U_\beta]$ is a smooth connected unipotent subgroup of G on which T acts through the character $\alpha + \beta$. Therefore $[U_\alpha, U_\beta] = e$ if $\alpha + \beta$ is not a root.

21.22. The centre Z of G is contained in T, and the action of T on G by inner automorphisms factors through T/Z (see 17.63). Hence every root $\alpha: T \to \mathbb{G}_m$ factors through T/Z. The action of T/Z on G preserves the root group U_α, and for every isomorphism $u: \mathbb{G}_a \to U_\alpha$,

$$\mathrm{inn}(t)(u(a)) = u(\alpha(t)a), \quad \text{all } t \in (T/Z)(k), a \in G(R).$$

It suffices to prove this after an extension of the base field, and so we may suppose that t is the image of an element of $T(k)$, in which case the statement follows from 21.19.

21.23. The algebraic group G_α of G is generated by its subgroups U_α, $U_{-\alpha}$, and T because this is true on the level of Lie algebras. Its derived group G^α is generated by U_α and $U_{-\alpha}$, because SL_2 is generated by U^+ and U^- (see 20.23). By construction, $n_\alpha \in G^\alpha(k)$.

21.24. As before, let γ_t for $t \in k^\times$ denote the inner automorphism $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & tb \\ t^{-1}c & d \end{smallmatrix}\right)$ of SL_2. In the proof of Theorem 21.11 we constructed, for each root α of (G,T), a central isogeny

$$v_\alpha: \mathrm{SL}_2 \to G^\alpha$$

such that $v_\alpha(\mathrm{diag}(x, x^{-1})) = \alpha^\vee(x)$ and $v_\alpha(U^+) \subset U_\alpha$. Such an isogeny v_α is uniquely determined by its restriction u_α to U^+ (see 20.26). If v'_α is a second such isogeny, then $v'_\alpha = v_\alpha \circ \gamma_t$ for a unique $t \in k^\times$ (see 20.25). Because the kernel of v_α is contained in T, v_α restricts to an isomorphism $U^+ \to U_\alpha$ (and also $U^- \to U_{-\alpha}$).

21.25. When k has characteristic zero, we can define a canonical homomorphism v_α. The subalgebra $\mathfrak{s}_\alpha = \mathfrak{g}_{-\alpha} \oplus [\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] \oplus \mathfrak{g}_\alpha$ of $\mathfrak{g}$ is semisimple (it is isomorphic to $\mathfrak{sl}_2$). According to Theorem 23.70 below, there exists an algebraic group S_α such that $\mathrm{Rep}(S_\alpha) = \mathrm{Rep}(\mathfrak{s}_\alpha)$. Define

$$v_\alpha: S_\alpha \to G$$

to be the homomorphism dual to the exact tensor functor

$$\mathrm{Rep}(G) \to \mathrm{Rep}(\mathfrak{g}) \to \mathrm{Rep}(\mathfrak{s}_\alpha) = \mathrm{Rep}(S_\alpha).$$

The choice of a nonzero element of $\mathfrak{g}_\alpha$ determines an isomorphism $\mathfrak{s}_\alpha \to \mathfrak{sl}_2$, and hence an isomorphism $S_\alpha \to \mathrm{SL}_2$.

d. Borel subgroups; Weyl groups; Tits systems

In this section, (G,T) is a split reductive group over k with root datum $\mathcal{R} = (X, \Phi, \Phi^\vee)$. As before, $\mathcal{B}$ denotes the collection of Borel subgroups of G and $\mathcal{B}^T$ the subset of $\mathcal{B}$ fixed by T (consisting of the Borel subgroups containing T).

Borel subgroups

Let $V = X^*(T)_\mathbb{Q}$ and $V^\vee = X_*(T)_\mathbb{Q}$. For a root $\alpha \in \Phi$, we let

$$H_\alpha = \{f \in V^\vee \mid \langle \alpha, f \rangle = 0\}.$$

It is a hyperplane in $V^\vee$. The **Weyl chambers** of the root datum $\mathcal{R} = (X, \Phi, \Phi^\vee)$ are the connected components of

$$V^\vee \smallsetminus \bigcup\nolimits_{\alpha \in \Phi} H_\alpha.$$

DEFINITION 21.26. A cocharacter λ of T is **regular** if it is contained in a Weyl chamber, i.e., for all roots α, $\langle \alpha, \lambda \rangle \neq 0$.

PROPOSITION 21.27. *If λ is regular, then $\mathcal{B}^{\lambda(\mathbb{G}_m)} = \mathcal{B}^T$.*

PROOF. We may suppose that k is algebraically closed. Recall (Section 17f) that $\mathcal{B}$ has the structure of a smooth complete algebraic variety with an action of T. The subvariety $\mathcal{B}^{\lambda(\mathbb{G}_m)}$ contains $\mathcal{B}^T$ and is stable under T. Let Y be a connected component of $\mathcal{B}^{\lambda(\mathbb{G}_m)}$. Then Y is stable under T (because T is connected) and complete, and so it contains a fixed point B (see 17.3). From the isomorphism $G/B \simeq \mathcal{B}$ we deduce that $\mathrm{Tgt}_B(\mathcal{B}) \simeq \mathfrak{g}/\mathfrak{b}$. As $\mathfrak{b} \supset \mathfrak{t}$, $\mathrm{Tgt}_B(\mathcal{B}) \subset \bigoplus_{\alpha \in \Phi(G,T)} \mathfrak{g}_\alpha$, and so the weights of $\mathbb{G}_m$ on $\mathrm{Tgt}_B(\mathcal{B})$ are nonzero integers $\langle \alpha, \lambda \rangle$. But $\mathbb{G}_m$ acts trivially on Y and hence on $\mathrm{Tgt}_B(Y)$, which is a subspace of $\mathrm{Tgt}_B(\mathcal{B})$, and so $\mathrm{Tgt}_B(Y) = 0$. Therefore Y has dimension 0, and so $\mathcal{B}^{\lambda(\mathbb{G}_m)}$ is finite. As it is stable under T and T is connected, it is fixed by T. □

LEMMA 21.28. *Let α be a root of (G,T). Every Borel subgroup of G containing T contains exactly one of U_α or $U_{-\alpha}$.*

PROOF. As before, let $T_\alpha = (\mathrm{Ker}\,\alpha)_t$ and $G_\alpha = C_G(T_\alpha)$. Then G_α has exactly two Borel subgroups containing T, namely, $U_\alpha \cdot T$ and $U_{-\alpha} \cdot T$ (see 20.20). If B is a Borel subgroup of G containing T, then $B \cap G_\alpha$ is a Borel subgroup of G_α (see 17.72), and so it equals one of $U_\alpha \cdot T$ and $U_{-\alpha} \cdot T$. □

PROPOSITION 21.29. *Let λ be a regular cocharacter of T. Then $P(\lambda)$ is a Borel subgroup of G containing T. It is the only Borel subgroup of G containing T and having Lie algebra*

$$\mathfrak{t} \oplus \bigoplus\nolimits_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_\alpha.$$

PROOF. We may suppose that k is algebraically closed. We shall use 13.33 and
14.13. By definition, $Z(\lambda)$ is the centralizer of $\lambda \mathbb{G}_m$ in G. It contains T, has
Lie algebra $\mathfrak{g}_0(\lambda) = \mathfrak{t}$, and is connected, and so it equals T. Now $P(\lambda)$ is the
semidirect product $P(\lambda) = U(\lambda) \rtimes T$ of a torus T with a unipotent group $U(\lambda)$,
and so it is solvable. As it is connected, it is contained in a Borel subgroup B.

The torus $\mathbb{G}_m$ acts on $\mathfrak{g}_\alpha$ through the character $t \mapsto t^{\langle \alpha, \lambda \rangle}$, and so (see 13.33c)

$$\text{Lie}(P(\lambda)) = \mathfrak{t} \oplus \bigoplus\nolimits_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_\alpha.$$

The Lie algebra of B contains $\text{Lie}(P(\lambda))$. According to the lemma, it contains
exactly one of $\mathfrak{g}_\alpha$ or $\mathfrak{g}_{-\alpha}$ for each α, and so it equals $\text{Lie}(P(\lambda))$. Therefore
$B = P(\lambda)$ (apply 10.15). In particular, $P(\lambda)$ is a Borel subgroup.

Let B' be a second element of $\mathcal{B}^T$ with Lie algebra $\mathfrak{t} \oplus \bigoplus_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_\alpha$. Then
B' contains the root group U_α for all α with $\langle \alpha, \lambda \rangle > 0$ (21.11c). These groups,
together with T, generate $P(\lambda)$, and so $B' \supset P(\lambda)$. As before, this implies that
$P(\lambda) = B$.   □

COROLLARY 21.30. *Every split maximal torus of a reductive group is contained
in a Borel subgroup.*

PROOF. The torus admits a regular cocharacter λ, and so it is contained in the
Borel subgroup $P(\lambda)$.   □

PROPOSITION 21.31. *Let λ and λ' be regular cocharacters of T. Then $P(\lambda) =
P(\lambda')$ if and only if λ and λ' lie in the same Weyl chamber.*

PROOF. Obviously, λ and λ' lie in the same Weyl chamber

$$\begin{aligned}
&\Longleftrightarrow \{\alpha \in \Phi \mid \langle \alpha, \lambda \rangle > 0\} = \{\alpha \in \Phi \mid \langle \alpha, \lambda' \rangle > 0\} \\
&\Longleftrightarrow \text{Lie } P(\lambda) = \text{Lie } P(\lambda') \\
&\Longleftrightarrow P(\lambda) = P(\lambda').
\end{aligned}$$
                                                                                     □

In particular, $P(\lambda)$ depends only on the Weyl chamber C of λ; we denote it by
$B(C)$.

THEOREM 21.32. *The map $C \mapsto B(C)$ is a bijection from the set of Weyl
chambers of (G, T) onto the set of Borel subgroups of G containing T.*

In particular, every Borel subgroup containing T is of the form $P(\lambda)$ for
some regular cocharacter λ of T.

PROOF. Proposition 21.31 shows that the map $C \mapsto B(C)$ is injective. In proving
that it is surjective, we initially assume that k is algebraically closed. Let $B \in \mathcal{B}^T$
and let λ be a regular cocharacter of T. There exists an $n \in N_G(T)(k)$ such that
$B = nP(\lambda)n^{-1}$ (see 17.11). Let w be the class of n in $W(G, T)$. Then

$$\text{Lie}(B) = \text{Lie}(nP(\lambda)n^{-1}) = \mathfrak{t} \oplus \bigoplus_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_{w(\alpha)} = \mathfrak{t} \oplus \bigoplus_{\langle \alpha, w^{-1}(\lambda) \rangle > 0} \mathfrak{g}_\alpha = \mathfrak{b}_{w^{-1}(\lambda)},$$

and so $B = P(w^{-1}(\lambda))$. For a general k, we have maps

$$\{\text{Weyl chambers}\} \xrightarrow{\mathcal{B}} \mathcal{B}(G)^T \to \mathcal{B}(G_{k^a})^{T_{k^a}} \xrightarrow{\mathcal{B}^{-1}} \{\text{Weyl chambers}\}.$$

Their composite is the identity map and all are injective, which implies that all the maps are bijective. □

COROLLARY 21.33. *Every Borel subgroup of* G_{k^a} *containing* T_{k^a} *is defined over* k.

PROOF. We saw in the proof of Theorem 21.32 that the map $\mathcal{B}(G)^T \to \mathcal{B}(G_{k^a})^{T_{k^a}}$ is bijective. □

COROLLARY 21.34. *Every Borel subgroup of* G *containing* T *is split as a solvable algebraic group.*

PROOF. The Borel subgroup is of the form $P(\lambda)$ for some regular cocharacter λ of T. Now $P(\lambda) = U(\lambda) \rtimes Z(\lambda)$ with $U(\lambda)$ unipotent and $Z(\lambda) = T$ (see 13.33). As $U(\lambda)$ is split (16.63) and T is split, $P(\lambda)$ is split . □

DEFINITION 21.35. For a Borel subgroup B of G containing T, let

$$\Phi^+(B) = \{\alpha \in \Phi \mid \mathfrak{g}_\alpha \subset \mathfrak{b}\} \text{ and}$$
$$C(B) = \{\lambda \in X_*(T)_{\mathbb{Q}} \mid \langle \alpha, \lambda \rangle > 0 \text{ for all } \alpha \in \Phi^+(B)\}.$$

Then $C(B)$ is a Weyl chamber, called the **dominant Weyl chamber** for B. If $B = P(\lambda)$, then $\Phi^+(B) = \{\alpha \in \Phi \mid \langle \alpha, \lambda \rangle > 0\}$ and so it is a system of positive roots, called the **system of positive roots attached to** B.

Note that $\Phi^+(B) = \{\alpha \in \Phi \mid U_\alpha \subset B\}$ and $\text{Lie}(B) = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi^+(B)} \mathfrak{g}_\alpha$.

EXAMPLE 21.36. Let $(G, T) = (\text{GL}_n, \mathbb{D}_n)$, and let χ_i denote the character of T sending $\text{diag}(x_1, \ldots, x_n)$ to x_i. The roots of (G, T) are the characters $\chi_i - \chi_j$, $i \neq j$ (see 21.6). If B is the Borel subgroup of upper triangular matrices, then

$$\Phi^+(B) = \{\chi_i - \chi_j \mid i < j\}.$$

Weyl groups

Recall (21.11d) that there is a distinguished element $s_\alpha \in W(G, T)$ for each root α of (G, T).

THEOREM 21.37. *The Weyl group* $W(G, T)$ *of* (G, T) *is generated by the elements* $s_\alpha, \alpha \in \Phi$.

PROOF. We may suppose that k is algebraically closed (21.1). By definition, $W(G,T)$ acts faithfully on T, and hence on $X(T)$. When we identify $W(G,T)$ with a subgroup of $\mathrm{Aut}(X(T))$, the element s_α becomes identified with the reflection map $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$. By definition, the Weyl group $W(\mathcal{R})$ of the root system $\mathcal{R}$ of (G,T) is the subgroup of $\mathrm{Aut}(X(T))$ generated by these reflection maps. It acts simply transitively on the set of Weyl chambers (C.22, C.30). On the other hand, $W(G,T)$ acts simply transitively on the set of Borel subgroups of G containing T (17.53). Thus, it suffices to construct a bijection from the set of Weyl chambers of the root datum $\mathcal{R}$ to the set of Borel subgroups of G containing T compatible with the actions of the two Weyl groups. This Theorem 21.32 does.   □

COROLLARY 21.38. *There is a canonical isomorphism $W(\mathcal{R}) \to W(G,T)$.*

PROOF. Such an isomorphism was constructed in the proof of Theorem 21.37.□

COROLLARY 21.39. *Let Δ be a base for the root system (G,T). Then $W(G,T)$ is generated by the elements s_α for $\alpha \in \Delta$.*

PROOF. This is true for $W(G,T)$ because it is true for $W(\mathcal{R})$ (see C.11).   □

EXAMPLE 21.40. Let $(G,T) = (\mathrm{GL}_n, \mathbb{D}_n)$. The centralizer of T in G is T, but its normalizer contains the permutation matrices (those obtained from the identity matrix by permuting the rows). For example, let $E(ij)$ be the matrix obtained from the identity matrix 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 the cosets of $T(k)$ in $N_G(T)(k)$, and so $W(G,T) \simeq S_n$.

Similarly, the Weyl group of $(\mathrm{SL}_n, \mathrm{SL}_n \cap \mathbb{D}_n)$ is canonically isomorphic to S_n. However, in this case, S_n cannot be realized as a subgroup of SL_n, even in the case $n = 2$ (s has no representative of order 2 in $N_G(T)$; see 20.39).

SUMMARY 21.41. Let (G,T) be a split reductive group. There are natural one-to-one correspondences between the following sets:

(a) the set of Borel subgroups of G containing T;

(b) the set of Weyl chambers C in $X_*(T)_{\mathbb{Q}}$;

(c) the set of systems of positive roots in Φ;

(d) the set of bases Δ for Φ.

Each set is acted on simply transitively by the Weyl group.

"The" root system of a splittable reductive group

21.42. Let G be a splittable reductive group over k. We say that a Borel pair (B,T) is split if T is split. Choose a split Borel pair (B,T), and let $\mathcal{R}(G,T)$ be the root datum of (G,T). Any other split Borel pair (B',T') in G equals $g(B,T)g^{-1}$ for some $g \in G(k)$. If (B',T') also equals $g'(B,T)g'^{-1}$, then we can write $g' = gh$ for some $h \in G(k)$. Now $h \in N_G(T)(k)$ because $hTh^{-1} = T$, and $h \in T(k)$ because $hBh^{-1} = B$ (see 21.41). Hence $\mathrm{inn}(h)$ induces the identity map on $\mathcal{R}(G,T)$, and so the isomorphism $\mathrm{inn}(g)\colon \mathcal{R}(G,T) \to \mathcal{R}(G',T')$ is *independent* of the choice of g. This allows us to define the root datum of G to be $\mathcal{R}(G,T)$ for any choice of a split Borel pair (B,T) with T split. It is well-defined up to a unique isomorphism. The map sending G to its root datum is functorial for isomorphisms of reductive groups.

21.43. We can exploit the same idea to define "the" maximal torus and "the" Weyl group of a splittable reductive group. For most purposes, knowing an object up to a unique isomorphism is as good as knowing the object itself. For example, for most purposes it suffices to know that there exists an object with a certain universal property without having a specific object in mind. We can state this more formally as follows.

Suppose that we are given a family $(X_i)_{i \in I}$ of objects and a system of isomorphisms $\varphi_{ji}\colon X_i \longrightarrow X_j$ such that $\varphi_{ii} = \mathrm{id}$ and $\varphi_{lj} \circ \varphi_{ji} = \varphi_{li}$ for all $i,j,l \in I$. A projective limit of the family is an object X equipped with isomorphisms $\varphi_i\colon X \to X_i$ such that $\varphi_{ji} \circ \varphi_i = \varphi_j$ for all i,j.

Now let G be a splittable reductive group over k. As index set I, we take the set of split Borel pairs (B,T) in G. For an index $i = (B,T)$, we set $T_i = T$ and $B_i = B$. We take φ_{ji} to be the isomorphism $T_i \to T_j$ induced by $\mathrm{inn}(g)$, where g is any element of $G(k)$ such that $g(B_i,T_i)g^{-1} = (B_j,T_j)$. As before, the elements g form a single right $T_i(k)$-coset, and so φ_{ji} is independent of the choice of g. The projective limit of the system is "the" maximal torus T in G. Similarly, we can define *the* Weyl group W of G, *the* action of W on T, *the* root datum of G, and its set of simple roots (see Deligne and Lusztig 1976, 1.1).

Tits systems

DEFINITION 21.44. Let G be an abstract group with subgroups B and N, and let S be a subset of $N/(B \cap N)$. Then (G, B, N, S) is a ***Tits system***[2] if it satisfies the following axioms:

(T1) G is generated by B and N, and $B \cap N$ is a normal subgroup of N;

(T2) the elements of S are involutions generating the group $W = N/(B \cap N)$;

(T3) if $s \in S$ and $w \in W$, then $sBw \subset BwB \cup BswB$;

---

[2]We follow Bourbaki 1968, IV, §2. The set S is uniquely determined by (G, B, N) (*ibid.* no. 5). A pair (B, N) such that (G, B, N, S) is a Tits system for some S is called a ***BN-pair*** in G.

(T4) for all $s \in S$, sBs is not contained in B.

THEOREM 21.45 (BRUHAT DECOMPOSITION). *Let (G, B, N, S) be a Tits system. Then*

$$G = \bigsqcup_{w \in W} BwB \qquad \text{(disjoint union).}$$

PROOF. The set BWB is stable under the formation of inverses (obviously) and products. As it contains B and N, it equals G. It remains to show that the double cosets BwB are disjoint. For this, see Exercise 21-5 or Bourbaki 1968, IV, §2, Théorème 1.   □

EXAMPLE 21.46 (BOURBAKI 1981, IV, §2). Let $G = \mathrm{GL}_n(k)$ for some $n \geq 0$. Let B be the standard (upper triangular) Borel subgroup, T the standard (diagonal) maximal torus, and N the subgroup of G consisting of the matrices having exactly one nonzero element in each row and column. Then N permutes the lines ke_i in k^n, and the resulting surjection $N \to S_n$ has kernel $T = B \cap N$. Thus $W \stackrel{\text{def}}{=} N/T \simeq S_n$. Let $s_i \in W$ correspond to the transposition $(i, i+1)$, and let $S = \{s_1, \ldots, s_{n-1}\}$. The quadruple (G, B, N, S) is a Tits system.

Axiom (T1) is a consequence of the following elementary statement from linear algebra: the group $\mathrm{GL}_n(k)$ is generated by the permutation matrices, the matrices $\mathrm{diag}(a, 1, \ldots, 1)$, and the matrices $I + \lambda E_{ij}$.

Axiom (T2) holds because the transpositions $(i, i+1)$ are involutions generating S_n.

Axiom (T4) is equally obvious.

It remains to prove (T3), namely, that

$$s_j Bw \subset BwB \cup Bs_j wB \quad \text{for } 1 \leq j \leq n-1, \quad w \in W.$$

This amounts to showing that

$$s_j B \subset BB' \cup Bs_j B' \quad \text{with } B' = wBw^{-1}.$$

Let G_j be the subgroup of G consisting of the elements fixing e_i for $i \neq j$, $j+1$ and stabilizing the plane spanned by e_j and e_{j+1} (for example, G_1 is a subgroup of the group G_α in 21.16). Then $G_j \simeq \mathrm{GL}_2(k)$, and $G_j B = BG_j$. As $s_j \in G_j$, we have $s_j B \subset BG_j$, and so it suffices to prove that

$$G_j \subset (B_j \cdot B_j') \cup (B_j s_j B_j') \text{ with } B_j = B \cap G_j \text{ and } B_j' = B' \cap G_j.$$

Identify G_j with GL_2. This identifies B_j with the Borel subgroup B^+ of GL_2 and B_j' with B^+ when $w(j) < w(j+1)$ and with B^- otherwise. In the first case, we have to show that

$$\mathrm{GL}_2(k) = B^+ \cup B^+ s B^+, \quad s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This follows from the fact that B^+ is the stabilizer of the point $(1{:}0)$ in the natural action of $\mathrm{GL}_2(k)$ on $\mathbb{P}^1(k)$ and acts transitively on the complement of $(1{:}0)$. In the second case, we have to show that

$$\mathrm{GL}_2(k) = B^+B^- \cup B^+sB^-;$$

as $B^- = sB^+s$, this follows from the preceding equality by multiplying on the right by s.

Thus (21.45),

$$\mathrm{GL}_n(k) = \bigsqcup\nolimits_{w \in W} B(k)wB(k) \quad \text{(Bruhat decomposition)}.$$

This just says that every matrix can be written uniquely as a product $U_1 P U_2$ with U_1, U_2 in B and P a permutation matrix. For another proof, see Exercise 21-6.

EXAMPLE 21.47. Let (G, T) be a split reductive group over k. Let B be a Borel subgroup of G containing T, and let Δ be the corresponding base for the root system (21.41). The quadruple $(G(k), B(k), N(k), S)$ with $N = N_G(T)$ and S the set of reflections s_α, $\alpha \in \Delta$, is a Tits system. See Proposition 21.75 below.

The Tits systems of many classical groups are described in Borel 1991, V.23.

e. Complements on semisimple groups

Recall (C.34) that a root datum $(X, \Phi, \Phi^\vee)$ is semisimple if $\mathbb{Z}\Phi$ is of finite index in X.

PROPOSITION 21.48. *A split reductive group is semisimple if and only if its root datum is semisimple.*

PROOF. A reductive group is semisimple if and only if its centre is finite (19.10), and so this follows from Proposition 21.8. □

PROPOSITION 21.49. *Let (G, T) be a split semisimple algebraic group.*
  (a) *G is generated by its root groups U_α (see 21.10), $\alpha \in \Phi(G, T)$.*
  (b) *G is generated by the subgroups G^α (see 21.23), $\alpha \in \Phi(G, T)$.*

PROOF. (a) We may suppose the base field is algebraically closed. We know (21.11) that G is generated by T and the root groups U_α. Let H be the algebraic subgroup of G generated by the U_α. Because the identity

$$u_\alpha(t)u_{-\alpha}(-t^{-1})u_\alpha(t) = \alpha^\vee(t)n_\alpha$$

holds in SL_2 (see 20.41), it holds in G (21.24). As $\alpha^\vee(t) = \alpha^\vee(t)n_\alpha\alpha^\vee(-1)n_\alpha$, it lies in $H(k)$, and so H contains $\alpha^\vee(\mathbb{G}_m)$ for every root α. By duality the $\alpha^\vee$ generate a subgroup of $X_*(T)$ of finite index, and so H contains T.

(b) Every group G^α contains U_α, and so this is obvious. □

COROLLARY 21.50. *Every semisimple algebraic group is perfect.*

PROOF. We may suppose that the base field k is algebraically closed. Then the semisimple group G is split. As each group G^α is perfect (20.24), it is contained in the derived group of G, which therefore equals G. □

Recall (19.7) that a nontrivial algebraic group is almost-simple if it is semisimple and every proper normal subgroup is finite. Also (2.31) that an algebraic group G is the almost-direct product of its algebraic subgroups $G_1, \ldots, G_r$ if the multiplication map $G_1 \times \cdots \times G_r \to G$ is a surjective homomorphism with finite kernel. In particular, this means that the G_i commute in pairs and that each G_i is normal in G.

THEOREM 21.51. *A semisimple algebraic group G has only finitely many almost-simple normal subgroup varieties $G_1, \ldots, G_r$ and is the almost-direct product of them. Every connected normal subgroup variety of G is a product of those G_i that it contains, and is centralized by the remaining ones.*

PROOF. Let $G_1, \ldots, G_r$ be subgroup varieties of G that are minimal among the nonfinite normal subgroup varieties of G. They are almost-simple.

For $i \neq j$, $[G_i, G_j]$ is the algebraic subgroup generated by the commutator map
$$G_i \times G_j \to G, \quad (a, b) \mapsto aba^{-1}b^{-1}$$
(see 6.24). It is a connected normal subgroup variety of G, properly contained in G_i, and so it is trivial (by the minimality of G_i). Thus, the multiplication map
$$u: G_1 \times \cdots \times G_r \to G$$
is a homomorphism of algebraic groups, and $H \overset{\text{def}}{=} G_1 \cdots G_r$ is a connected normal subgroup variety of G; it is also semisimple. The kernel of u is finite, and so
$$\dim G \geq \sum_{i=1}^{r} \dim G_i.$$

Thus r is bounded and we may suppose that our family $(G_i)_{1 \leq i \leq r}$ contains all minimal nonfinite normal subgroup varieties of G.

It remains to show that $H = G$. For this we may suppose that k is algebraically closed. The torus $T_H \overset{\text{def}}{=} (T \cap H)_t$ is maximal in H (see 17.85). Suppose that there exists $\beta \in \Phi(G, T) \smallsetminus \Phi(H, T_H)$, and let $\alpha \in \Phi(H, T_H)$. Consider the map
$$u: \mathbb{A}^1 \times \mathbb{A}^1 \to G, \quad x, y \mapsto u_\beta(y) u_\alpha(x) u_\beta(y)^{-1}.$$
Then $u(x, y) \in H$ and $t \cdot u(x, y) \cdot t^{-1} = y(\alpha(t)x, y)$ for $t \in T_H(k)$. For a fixed y, the map $x \mapsto u(x, y)$ is a homomorphism $\mathbb{G}_a \to U_\alpha$, and so it is a nonzero multiple, $f(y)$ say, of u_α. Now f is a regular map $\mathbb{A}^1 \to \mathbb{A}^1 \smallsetminus 0$, and so it is constant: $f(y) = f(0) = 1$. We deduce that
$$u_\beta(y) u_\alpha(x) u_\beta(y)^{-1} = u_\alpha(x), \quad \text{all } x, y \in \mathbb{G}_a(k),$$

and so u_α and u_β commute. As this is true for all $\alpha \in \Phi(H, T_H)$ and the groups U_α generate H, we see that U_β centralizes H. Hence the algebraic subgroup H' generated by the U_β for $\beta \in \Phi(G, T) \smallsetminus \Phi(H, T_H)$ is a connected subgroup variety of G centralizing H. Let N be minimal among the nonfinite normal subgroup varieties of H'. Then N is normal in G (because $G = H \cdot H'$ and H centralizes H'), and so it equals one of the G_i. This contradicts the definition of H, and so we conclude that $\Phi(H, T_H) = \Phi(G, T)$ and H contains U_α for every $\alpha \in \Phi(G, T)$. Thus $H = G$. □

The G_i in the theorem are called the ***almost-simple factors*** of G.

COROLLARY 21.52. *Quotients and connected normal subgroup varieties of a semisimple algebraic groups are semisimple.*

PROOF. Every such group is an almost-direct product of almost-simple (hence semisimple) algebraic groups. □

COROLLARY 21.53. *Every connected normal subgroup variety N of a reductive group G is reductive.*

PROOF. We may suppose that k is algebraically closed. The quotient $N/N \cap R(G)$ is a normal subgroup variety of the semisimple group $G/R(G)$, and so it is semisimple. Therefore $R_u(G) \subset N \cap R(G)$, which is of multiplicative type, and so $R_u(G) = e$. □

SUMMARY 21.54. The following conditions on a connected reductive group G are equivalent:

(a) G is semisimple;

(b) G is equal to its derived group;

(c) (G split) G is generated by the root groups U_α;

(d) (G split) if T is split, then the roots of (G, T) generate $X^*(T)_{\mathbb{Q}}$.

Notes

21.55. Theorem 21.51 shows that every semisimple algebraic group is generated by its almost-simple subgroups. As these are obviously perfect, this gives another proof that semisimple algebraic groups are perfect.

21.56. When k has characteristic zero, Theorem 21.51 is most easily proved using Lie algebras. The Lie algebra of a semisimple algebraic group G is semisimple, and so it is a direct sum $\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r$ of its simple ideals $\mathfrak{g}_i$. Correspondingly, G is an almost-direct product of almost-simple subgroups G_i with G_i equal to the centralizer of $\bigoplus_{j \neq i} \mathfrak{g}_i$ in G.

21.57. There is a more general form of Theorem 21.51. An ***almost pseudo-simple group*** is a smooth connected noncommutative algebraic group such that every proper normal subgroup is finite. A connected group variety G (not necessarily semisimple) has only finitely many minimal perfect nontrivial normal subgroup varieties $G_1, \ldots, G_r$. Each G_i is almost pseudo-simple, and the multiplication map $G_1 \times \cdots \times G_r \to G$ is a homomorphism with image the largest perfect connected normal subgroup variety of G. Its kernel is central and contains no nontrivial connected subgroup variety. See Conrad et al. 2015, 3.1.8.

21.58. For a semisimple group G over an algebraically closed field k, every element of $G(k)$ is a commutator (not merely a product of commutators); see Ree 1964.

f.   Complements on reductive groups

LEMMA 21.59. *Every almost-simple algebraic group has a simple representation with finite kernel*

PROOF. Every simple subrepresentation of a faithful representation on which the group acts nontrivially has finite kernel.   □

Such an algebraic group need not have a faithful simple representation, essentially because noncyclic commutative groups do not (see Exercise 22-2).

PROPOSITION 21.60. *Let G be a connected group variety over a perfect field k. The following conditions on G are equivalent:*
  (a) *G is reductive;*
  (b) *The radical $R(G)$ of G is a torus;*
  (c) *G is an almost-direct product of a torus and a semisimple group;*
  (d) *G admits a semisimple representation with finite kernel.*

PROOF. (a)$\Rightarrow$(b). If G is reductive, then $R(G) = Z(G)_t$ is a torus (17.62).

(b)$\Rightarrow$(c). Let $S = R(G)$. Then S is a central torus in G and G/S is semisimple (19.2). Hence G/S is perfect (21.50), and so G is the almost-product of S and G^{der} (see 12.46). The latter is semisimple because it is isogenous to G/S.

(c)$\Rightarrow$(d). The group G is an almost-direct product

$$G_0 \times G_1 \times \cdots \times G_n \to G$$

of subgroup varieties G_i with G_0 a torus and each G_i, $i \geq 1$, an almost-simple group (21.51). Each quotient $G/(G_0 \cdots G_{i-1}G_{i+1} \cdots G_n)$ is either a torus or an almost-simple group, and therefore admits a semisimple representation with finite kernel. Choose such a representation for each i, and take the direct sum of them.

(d)$\Rightarrow$(a). The unipotent radical of G acts trivially on semisimple representations of G (see 19.16). Hence (d) implies that it is finite, but, by definition it is connected and smooth, and so it is trivial (2.17). As k is perfect, this implies that G is reductive (19.11).   □

PROPOSITION 21.61. *Let G be a connected group variety over a field k (not necessarily perfect). The following conditions are equivalent:*

(a) *G is reductive;*

(b) *the geometric radical $R(G_{k^a})$ of G is a torus;*

(c) *G is an almost-direct product of a torus and a semisimple group.*

PROOF. (a)$\Rightarrow$(b). If G is reductive, then G_{k^a} is reductive, and so $R(G_{k^a})$ is a torus (21.60).

(b)$\Rightarrow$(c). As $R(G)_{k^a} \subset R(G_{k^a})$, we see that $R(G)$ is a torus. Now the same argument as in the proof of Proposition 21.60 proves (c).

(c)$\Rightarrow$(a). As G_{k^a} is also an almost-direct product of a torus and a semisimple algebraic group, its unipotent radical is obviously zero. □

Recall (21.23) that, for a root α of (G, T), G^α (resp. G_α) is the algebraic subgroup of G generated by $U_{\pm\alpha}$ (resp. T and $U_{\pm\alpha}$).

PROPOSITION 21.62. *Let (G, T) be a split reductive group, and let Δ be a base for the root system of (G, T). Then G^{der} is generated by the algebraic subgroups G^α, $\alpha \in \Delta$, and G is generated by the algebraic subgroups G_α, $\alpha \in \Delta$.*

PROOF. As $G = G^{\mathrm{der}} \cdot T$ and each group G_α contains T, it suffices to show that G^{der} is generated by the groups G^α. Thus, we may suppose that G is semisimple.

Let H be the algebraic subgroup of G generated by the G^α. As each G^α is normalized by T, so also is H. As G^α contains U_α and $U_{-\alpha}$, we see that H contains $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ for all $\alpha \in \Delta$.

In characteristic zero, $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$ if α, β, and $\alpha + \beta$ are all roots (Serre 1966, VI, Thm 2) and so $\mathrm{Lie}(H)$ contains $\mathfrak{g}_\alpha$ for all $\alpha \in \Phi$.

In the general case, we use that the Weyl group of (G, T) is generated by the reflections s_α for $\alpha \in \Delta$ (see 21.39). As $G^\alpha(k)$ contains a representative for n_α for s_α (see 21.11d), we see that $H(k)$ contains a set of representatives for the elements of $W(G, T)$. Therefore, for all $s \in W(G, T)$ and $\alpha \in \Delta$, the Lie algebra of H contains $s\mathfrak{g}_\alpha = \mathfrak{g}_{s\alpha}$ (see 21.2) and so H contains the root group $U_{s\alpha}$. As $W \cdot \Delta = \Phi$ (see C.30), it follows that H contains U_α for all $\alpha \in \Phi$, and so $H = G$ (see 21.49). □

COROLLARY 21.63. *Let $\varphi_1, \varphi_2 : (G, T) \rightrightarrows (G', T')$ be isogenies of split reductive groups, and let Δ be a base for $\Phi(G, T)$. If φ_1 and φ_2 agree on T and on U_α for all $\alpha \in \Delta$, then they agree on G.*

PROOF. As φ_1 and φ_2 agree on the Borel subgroup $U_\alpha \cdot T$ of G_α, they agree on G_α (see 17.21), and these groups generated G (see 21.62). □

PROPOSITION 21.64. *A reductive group G is splittable (19.22) if and only if it is split as a group variety (17.101).*

PROOF. If G contains a split maximal torus, then it contains a split Borel subgroup (21.30, 21.34). Conversely, if G contains a Borel subgroup B that is split as a solvable group, then (16.29d) applied to the extension

$$e \to B_u \to B \to B/B_u \to e$$

shows that B contains a split maximal torus, which is also split maximal in G. $\quad\square$

COROLLARY 21.65. *Let G be a reductive group over k. Any two split maximal tori in G are conjugate by an element of $G(k)$.*

PROOF. If G is not split, there is nothing to prove. Otherwise, G is split as an algebraic group, and so we can apply Theorem 17.105(c). $\quad\square$

NOTES. Proposition 21.60 is Proposition 2.2 of Borel and Tits 1965[3] except that there k is implicitly assumed to be algebraically closed (the assumption is hidden in the terminology).

g.   Unipotent subgroups normalized by T

21.66. Let (G, T) be a split reductive group, and let H be a connected subgroup variety of G normalized by T. Then

$$\mathrm{Lie}(G)^T \overset{10.34}{=} \mathrm{Lie}(C_G(T)) \overset{17.84}{=} \mathrm{Lie}(T),$$

and so

$$\mathrm{Lie}(H)^T = \mathrm{Lie}(G)^T \cap \mathrm{Lie}(H) = \mathrm{Lie}(T) \cap \mathrm{Lie}(H) \overset{10.14}{=} \mathrm{Lie}(T \cap H).$$

Let Φ_H be the set of roots α such that $H \supset U_\alpha$. This is also the set of roots α such that $\mathrm{Lie}(H) \supset \mathfrak{g}_\alpha$ (see 21.11c). As H is stable under T, its Lie algebra is a direct sum of eigenspaces for T, and so

$$\mathrm{Lie}(H) = \mathrm{Lie}(T \cap H) \oplus \bigoplus\nolimits_{\alpha \in \Phi_H} \mathfrak{g}_\alpha.$$

Therefore H is generated by $T \cap H$ and the root groups U_α it contains (10.17).

PROPOSITION 21.67. *Let G be a reductive group over k, and let H_1 and H_2 be smooth connected subgroups of G. If $H_1 \cap H_2$ is connected and contains a maximal torus T of G, then it is smooth.*

---

[3]These authors (see 0.3 of their paper) offer the reader three different definitions of "groupe algébrique sur k". However, many of the statements in their paper take on different meanings according to which definition is adopted, and some become false. For example, Proposition 2.2 is false as stated for "schémas en groupes affine absolument réduit sur k".

PROOF. We may suppose that k is algebraically closed. From 21.66,

$$\text{Lie}(H_i) = \text{Lie}(T) \oplus \bigoplus \{\mathfrak{g}_\alpha \mid \alpha \in \Phi_{H_i}\} \quad \text{for } i = 1, 2,$$

$$\text{Lie}((H_1 \cap H_2)_{\text{red}}) = \text{Lie}(T) \oplus \bigoplus \{\mathfrak{g}_\alpha \mid \alpha \in \Phi_{H_1} \cap \Phi_{H_2}\}.$$

Now $\text{Lie}(H_1 \cap H_2) \overset{10.14}{=} \text{Lie}(H_1) \cap \text{Lie}(H_2) = \text{Lie}((H_1 \cap H_2)_{\text{red}})$, and so $H_1 \cap H_2$ is smooth (3.19). □

THEOREM 21.68. *Let (G, T) be a split reductive group. Let B be a Borel subgroup of G containing T, and let $\Phi^+(B) = \{\alpha_1, \ldots, \alpha_r\}$ be its system of positive roots.*

(a) *The multiplication map*

$$\varphi: U_{\alpha_1} \times \cdots \times U_{\alpha_r} \to B_u$$

is a T-equivariant isomorphism of algebraic varieties with T-action.

(b) *The morphism $B_u \rtimes T \to B$ is an isomorphism.*

(c) *Let U be a subgroup variety of B_u normalized by T, and let $\{\beta_1, \ldots \beta_s\}$ be the weights of T on $\text{Lie}(U)$. Then U is connected and the multiplication map*

$$U_{\beta_1} \times \cdots \times U_{\beta_s} \to U$$

is a T-equivariant isomorphism of algebraic varieties with T-action. In particular, U is generated by the U_α for which $\mathfrak{g}_\alpha \subset \text{Lie}(U)$.

(d) *A subset Φ' of Φ is the set of weights of a subgroup U as in (c) if and only if $\Phi' \cap -\Phi' = \emptyset$ and $(\mathbb{N}\alpha + \mathbb{N}\beta) \cap \Phi \subset \Phi'$ for all $\alpha, \beta \in \Phi'$.*

PROOF. (a) Let $U = U_{\alpha_1} \times \cdots \times U_{\alpha_r}$. The map φ is equivariant for the actions of T by conjugation, and it induces an isomorphism $\text{Tgt}_e(U) \to \text{Tgt}_e(B_u)$ on the tangent spaces. Let λ lie in the dominant Weyl chamber of B. Then the weights of $\lambda(\mathbb{G}_m)$ on $\text{Tgt}_e(U)$ and $\text{Tgt}_e(B_u)$ are strictly positive, and so the Luna maps $U \to \text{Tgt}_e(U)$ and $B_u \to \text{Tgt}_e(B_u)$ are isomorphisms (13.41). Therefore φ is an isomorphism (cf. 13.42).

(b) Every Borel subgroup B containing T is of the form $P(\lambda)$ for some regular character λ (see 21.32). Then $B_u = U(\lambda)$ and $T = Z(\lambda)$, and so the required isomorphism is the isomorphism $U(\lambda) \rtimes Z(\lambda) \to P(\lambda)$ of Theorem 13.33(b).

(c) The same argument as in (a) shows that the multiplication map

$$U_{\beta_1} \times \cdots \times U_{\beta_s} \to U^\circ$$

is an isomorphism. It remains to show that $U = U^\circ$. From (a) we get an isomorphism

$$U^\circ \times U' \to B_u$$

with $U' = \prod\{U_\alpha \mid \alpha \in \Phi^+, U_\alpha \not\subset U^\circ\}$. This isomorphism restricts to an iso-
morphism
$$U^\circ \times U \cap U' \to U.$$

On passing to the quotient by U°, we get an isomorphism $U \cap U' \to U/U^\circ$.
Now $U \cap U'$ is stable under T (because U and U' are), and the map is T-
equivariant. As T is connected and U/U° is étale, the action of T is trivial, and
so $U \cap U' \subset C_G(T) = T$. Therefore $U \cap U' \subset B_u \cap T = e$, and so $U = U^\circ$.

(d) The necessity is obvious, and the sufficiency follows from Theorem 16.65
applied to the subsemigroup of X generated by Φ'.   □

REMARK 21.69. In order to write down the map φ, we had to choose an ordering
of the set Φ^+. However, the theorem is true whichever ordering we choose.
Similar remarks apply elsewhere.

h.   The Bruhat decomposition

Let (G, T) be a split reductive group over k and B a Borel subgroup of G
containing T. The Bruhat decomposition for $G(k)$ is
$$G(k) = \bigsqcup_{w \in W} B(k) w B(k)$$

(see 21.46 for GL_n). In this section, we prove that the Bruhat decomposition
exists on the level of schemes.

Recall (21.1) that every $w \in W$ has a representative $n_w \in N_G(T)(k)$. As
$n_w B$ is independent of the choice of n_w, we usually denote it by wB. Similarly,
BwB denotes the double coset $Bn_w B$. For $w \in W$, we let e_w denote the point
wB/B in G/B – it is fixed by T. Recall that $(G/B)^T(k)$ is equal to the set of
Borel subgroups of G containing B, which is acted on simply transitively by W
(see 21.41). It follows that
$$(G/B)^T(k) = \{e_w \mid w \in W\}.$$

In particular, $(G/B)^T$ is a finite constant scheme.

As usual, we choose a representation (V, r) of G such that B is the stabilizer
of a line in V and regard G/B as a closed subvariety of $\mathbb{P}(V)$. Fix a cocharacter
λ of T in the dominant Weyl chamber $C(B)$ with the property that the numbers
$\langle \chi, \lambda \rangle$ as χ runs over the weights of T on V are distinct, and let $\mathbb{G}_m$ act on G and
G/B through λ. Then $B = P(\lambda)$ (21.29) and $(G/B)^{\mathbb{G}_m} = (G/B)^T$ (13.51).

PROPOSITION 21.70. *For each $w \in W$, there is a unique smooth subscheme
$Y(w)$ of G/B such that*
$$Y(w)(k^{\mathrm{a}}) = \{x \in (G/B)(k^{\mathrm{a}}) \mid \lim_{t \to 0} \lambda(t) \cdot x = e_w\}.$$

Each $Y(w)$ is an affine space, and
$$G/B = \bigsqcup_{w \in W} Y(w) \quad \text{(disjoint union of locally closed subvarieties).}$$

For a unique (attracting) point, $Y(w)$ is open and dense in G/B, and for unique (repelling) point, $Y(w)$ is a single point.

PROOF. As $(G/B)^{\lambda(\mathbb{G}_m)}$ is the finite constant scheme $\{e_w \mid w \in W\}$, this is the Białynicki-Birula decomposition (13.49). □

PROPOSITION 21.71. *The cell $Y(w)$ is the B_u-orbit of e_w in G/B.*

PROOF. If $b \in B_u(k^a)$, then $\lim_{t\to 0} \lambda(t) \cdot b \cdot \lambda(t)^{-1} = 1$ because $B_u = U(\lambda)$, and so $\lim_{t\to 0} \lambda(t)bx = e_w$ for all $x \in Y(w)(k^a)$. Therefore $Y(w)$ is stable under the action of B_u. In particular, $B_u e_w \subset Y(w)$. As $Y(w)$ is smooth, it remains to show that $(B_u e_w)(k^a) = Y(w)(k^a)$. We may suppose that k is algebraically closed. Let $B_u x$ be a nonempty orbit of B_u in $Y(w)$. Then $B_u x$ is closed by the Kostant–Rosenlicht theorem (17.64). Therefore $e_w \in B_u x$ and $B_u e_w = B_u x = Y(w)$. □

DEFINITION 21.72. The **symmetry with respect to B** is the element $w_0 \in W$ such that $w_0(\Phi^+) = -\Phi^+$ (equivalently, $w_0(C(B)) = -C(B)$).

As the Weyl group acts simply transitively on the set of Weyl chambers (21.41), there is a unique such element. Note that w_0 is an involution because $w_0^2(C(B)) = C(B)$.

THEOREM 21.73. *(a) There are decompositions (of smooth algebraic varieties)*

$$G/B = \bigsqcup_{w \in W} B_u w B/B \quad \text{(cellular decomposition)}$$

$$G = \bigsqcup_{w \in W} B_u w B \quad \text{(Bruhat decomposition)}.$$

(b) The dense open orbit for the action of B_u on G/B is $B_u w_0 B/B$ and the dense open orbit for the action of $B_u \times B$ on G is $B_u w_0 B$.

PROOF. (a) The first equality follows from Propositions 21.70 and 21.71, and the second equality follows from the first.
(c) Let $n_0 \in N(k)$ represent w_0. Then

$$\mathrm{Tgt}_{e_{w_0}}(G/B) \simeq \mathfrak{g}/n_0(\mathfrak{b}) \simeq \bigoplus \{\mathfrak{g}_\alpha \mid \alpha \in \Phi^+(B)\},$$

and so the weights of $\mathbb{G}_m$ on $\mathrm{Tgt}_{e_{w_0}}(G/B)$ are strictly positive (by our choice of λ). Therefore the orbit $Y(w_0) = B_u n_0 B/B$ is open and dense (13.49). □

When $k = \mathbb{C}$, the cellular decomposition in the theorem becomes a cellular decomposition of the manifold $(G/B)(\mathbb{C})$ in the sense of geometric topology, which explains the name.

REMARK 21.74. As $B = B_u \cdot T$ and W normalizes T, we have $BwB = B_u wB$ and $BwB/B = B_u wB/B$. Therefore, the decompositions in (a) can be written

$$G/B = \bigsqcup_{w \in W} BwB/B$$

$$G = \bigsqcup_{w \in W} BwB.$$

PROPOSITION 21.75. *The quadruple* $(G(k), B(k), N(k), S)$ *arising, as in Example* 21.47, *from a split reductive group* (G, T) *over* k *is a Tits system.*

PROOF. Note that $B \cap N = T$, and so the group $W = N(k)/(B \cap N)(k)$ is equal to the Weyl group $W(G, T) = N(k)/T(k)$ (see 21.1). Therefore (T2) holds, and (T1) holds because the equality (21.73)

$$G(k) = \bigsqcup_{w \in W} B_u(k) n_w B(k)$$

shows that $G(k)$ is generated by $B(k)$ and $N(k)$.

For (T3), we have to show that

$$s_\alpha B(k) w \subset B(k) w B(k) \cup B(k) s_\alpha w B(k).$$

According to Theorem 21.68, $B(k) = T(k) \cdot \prod_{\beta \in \Phi^+} U_\beta(k)$, and so

$$s_\alpha B(k) w = T(k) \cdot \prod_{\beta \in \Phi^+, \beta \neq \alpha} U_\beta(k) U_{-\alpha}(k) s_\alpha w.$$

Therefore, it suffices to prove the inclusion

$$U_{-\alpha}(k) s_\alpha w \subset B(k) w B(k) \cup B(k) s_\alpha w B(k).$$

If $w^{-1}(\alpha) \in \Phi^+$, then

$$U_{-\alpha}(k) s_\alpha w = s_\alpha w U_{w^{-1}(\alpha)}(k) \subset B(k) s_\alpha w B(k).$$

If not, then using the Bruhat decomposition in G_α, we have $U_{-\alpha}(k) \subset B(k) \cup B(k) s_\alpha B(k)$. We deduce the inclusion

$$U_{-\alpha}(k) s_\alpha w \subset B(k) s_\alpha w \cup B(k) s_\alpha B(k) s_\alpha w.$$

But we have $B(k) s_\alpha B(k) s_\alpha w = B(k) U_{-\alpha}(k) w = B(k) U_{-w^{-1}(\alpha)}(k) \subset B(k)$.

Finally, (T4) is obvious.   □

The subgroups U_w and U^w

Let $U = B_u$. Let $\Phi^- = -\Phi^+$ and $U^- = n_0(U)$. Each of U and U^- is equal to the product of the root groups it contains (21.68), and

$$\begin{cases} U_\alpha \subset U & \Longleftrightarrow \quad \alpha \in \Phi^+ \\ U_\alpha \subset U^- & \Longleftrightarrow \quad \alpha \in \Phi^-. \end{cases}$$

DEFINITION 21.76. For $w \in W$, define $U_w = U \cap n_w(U)$ and $U^w = U \cap n_w(U^-)$.

PROPOSITION 21.77. *For all* $w \in W$, *the groups* U_w *and* U^w *are smooth and connected; moreover*

$$\begin{cases} U_w \simeq \prod \{U_\alpha \mid \alpha \in \Phi^+ \cap w(\Phi^+) \\ U^w \simeq \prod \{U_\alpha \mid \alpha \in \Phi^+ \cap w(\Phi^-). \end{cases} \tag{136}$$

PROOF. Once we prove that U_w and U^w are smooth, the remaining statements will follow from Theorem 21.68(c). We may suppose that k is algebraically closed. As $(U_w)_{\mathrm{red}}$ is a subgroup variety of B_u normalized by T, it is connected (21.68c). Now U_w is connected, and hence smooth by Proposition 21.67. The proof that U^w is smooth is similar. □

LEMMA 21.78. *For all $w \in W$, the multiplication map*

$$U_w \times U^w \to U$$

is an isomorphism.

PROOF. We may suppose k to be algebraically closed. We first show that $U_w \cap U^w = e$. The subgroup variety $(U_w \cap U^w)_{\mathrm{red}}$ is normalized by T, and so it is equal to the product of the U_α that it contains. But

$$U_\alpha \subset U_w \iff \alpha \in \Phi^+ \cap w(\Phi^+)$$
$$U_\alpha \subset U^w \iff \alpha \in \Phi^+ \cap w(\Phi^-).$$

These conditions are exclusive, which proves that $(U_w \cap U^w)_{\mathrm{red}} = e$. On the other hand, $\mathrm{Lie}(U_w \cap U^w) = \mathrm{Lie}(U_w) \cap \mathrm{Lie}(U^w) = 0$, and so $U_w \cap U^w$ is smooth, and hence trivial.

Every root α satisfies one of the above conditions and U is smooth, and so the homomorphism $U_w \times U^w \to U$ is surjective. Its kernel is $U_w \cap U^w = e$. □

PROPOSITION 21.79. *Let $w \in W$.*

(a) *The isotropy group at e_w in G (resp. U) is $n_w(B)$ (resp. U_w).*

(b) *The orbits $U^w e_w \subset U e_w$ are equal, and the orbit map*

$$U^w \to U^w e_w = U e_w$$

is an isomorphism.

(c) *The dimension of $U e_w$ is $n(w) \overset{\mathrm{def}}{=} |\Phi^+ \cap w(\Phi^-)|$.*

PROOF. (a) Consider the quotient map $\pi : G \to G/B$. The isotropy group at eB/B in G is obviously B. When we translate π by n_w, we get a quotient map $\pi_w : G \to G/B$ defined by $\pi_w(g) = g n_w B/B$. The isotropy group at $n_w B/B$ is the fibre of this map, which is $n_w(B)$.

The stabilizer of e_w in U is $U \cap n_w(B) = U \cap n_w(U) = U_w$.

(b) The kernel of the restriction of $(d\pi_w)_e$ to $\mathrm{Lie}(U)$ is

$$\mathrm{Ker}((d\pi_w)_e) \cap \mathrm{Lie}(U) = n_w(\mathfrak{b}) \cap \mathrm{Lie}(U) = \mathrm{Lie}(U_w).$$

As $U_w \times U^w \simeq U$, the morphism $U^w \to U^w e_w$ is bijective on k^{a}-points and the kernel of its differential is $\mathrm{Lie}(U^w) \cap \mathrm{Lie}(U_w) = 0$. Therefore it is étale and an isomorphism.

(c) From (b) we have $\dim(U e_w) = \dim U^w$, which equals $n(w)$ by (136). □

THEOREM 21.80 (BRUHAT DECOMPOSITION).   (a) *There are decomposi-tions (of smooth algebraic varieties)*

$$G/B = \bigsqcup_{w \in W} U^w n_w B/B \quad \text{(cellular decomposition of } G/B)$$

$$G = \bigsqcup_{w \in W} U^w n_w B \quad \text{(Bruhat decomposition of } G).$$

(b) *For every $w \in W$, the morphism*

$$U^w \times B \to U^w n_w B, \quad (u,b) \mapsto u n_w b$$

is an isomorphism.

(c) *There are open coverings*

$$G = \bigcup_{w \in W} n_w U^- B$$

$$G/B = \bigcup_{w \in W} n_w U^- B/B.$$

PROOF. (a, b) These statements summarize what was proved above.

(c) Theorem 21.73b implies that $U^- B$ and $U^- B/B$ are dense open subsets of G and G/B containing e and eB. Therefore, their translates by n_w are dense open subsets containing n_w and $n_w B$. Their unions are all of G or G/B because

$$n_w U^- B = (n_w U^- n_w^{-1}) n_w B \supset U^w n_w B$$

and because of the decompositions in (a).   □

DEFINITION 21.81. For $w \in W$, define

$$N(w) = \{ \alpha \in \Phi^+ \mid w^{-1}(\alpha) \in \Phi^- \} = \Phi^+ \cap w(\Phi^-).$$

Thus $n(w) = |N(w)|$.

REMARK 21.82. For $w \in W$,

(a) $\dim Y(w) = \dim U^w = n(w)$,

(b) $n(w) = n(w^{-1})$, and

(c) $n(w_0 w) = n(w w_0) = |\Phi^+| - n(w)$.

EXAMPLE 21.83. Let B be a Borel subgroup in a reductive group G. The map $gB, g'B \mapsto Bg^{-1}g'B$ induces a bijection

$$G \backslash (G/B \times G/B) \to B \backslash G/B$$

and so the Bruhat decomposition says that the orbits of pairs of maximal flags under simultaneous translation by G are indexed by the elements W.

Let $G = \mathrm{GL}_n$, and let B be the Borel subgroup of upper triangular matrices. We can view G/B as the variety of maximal flags in $V = k^n$. Let $w \in S_n$. Maximal flags $(V_1, \ldots, V_n)$ and $(V_1', \ldots, V_n')$ are said to be in relative position w if there exists a basis $\{e_1, \ldots, e_n\}$ for V such that, for every $i = 1, \ldots, n-1$, we have $V_i = \langle e_1, \ldots, e_i \rangle$ and $V_i' = \langle e_{w(1)}, \ldots, e_{w(i)} \rangle$. The subvariety $Y(w)$ consists of the maximal flags in relative position w. For a direct proof of the Bruhat decomposition from this perspective, see Exercise 21-6.

The big cell

THEOREM 21.84. *Let (G, T) be a split reductive group over k, and let B be a Borel subgroup containing T. Then there exists a unique Borel subgroup B' of G such that $B \cap B' = T$. The multiplication map*

$$B_u' \times T \times B_u \to G \qquad (137)$$

is an open immersion (of algebraic varieties).

PROOF. Choose a $\lambda \in X_*(T)$ such that $\langle \alpha, \lambda \rangle > 0$ for all $\alpha \in \Phi^+(B)$. Then $B = P(\lambda)$. Let $B' = P(-\lambda)$. The map (137) is an open immersion by Theorem 13.33. The rest is obvious. □

DEFINITION 21.85. The dense open subvariety $B_u' \cdot T \cdot B_u$ of G is called the **big cell** in G.

We often write B^- for B', and U^- for B_u^-. Then the big cell becomes $U^- B$. It is also equal to the dense open subset $B_u w_0 B$ of G in Theorem 21.73.

Borel subgroups B and B' of G such that $B \cap B'$ is a maximal torus are said to be **opposite**. Thus Borel subgroups are opposite if their intersection is as small as possible. If w_0 is the symmetry with respect to B (see 21.72), then $w_0 B = B'$.

SUMMARY 21.86. Let (G, T) be a split reductive group over k, and let Φ^+ be a positive system of roots. Then $U = \prod_{\alpha \in \Phi^+} U_\alpha$ and $U^- = \prod_{\alpha \in \Phi^+} U_{-\alpha}$ are maximal connected unipotent subgroup varieties of G. Each of U and U^- is isomorphic as an algebraic variety to the product of the factors in its definition. The subgroups $B = UT$ and $B^- = U^- T$ are opposite Borel subgroups of G. Finally, $C = U^- T U$ (the big cell) is a dense open subvariety of G.

EXAMPLE 21.87. Let $(G, T) = (\mathrm{GL}_n, \mathbb{D}_n)$. Its roots are

$$\alpha_{ij} : \mathrm{diag}(t_1, \ldots, t_n) \mapsto t_i t_j^{-1}, \quad i, j = 1, \ldots, n, \quad i \neq j.$$

The corresponding root groups are $U_{ij} = \{I + a E_{ij} \mid a \in k\}$. Let $\Phi^+ = \{\alpha_{ij} \mid i < j\}$. Then U and U^- are, respectively, the subgroups of superdiagonal and subdiagonal unipotent matrices, and the big cell is the set of matrices for which the $i \times i$ matrix in the upper left-hand corner is invertible for all i.

NOTES. The existence of a Bruhat decomposition was proved for a number of classical groups by Bruhat in 1956, and extended to the general case by Chevalley in his 1956–58 seminar.

i. Parabolic subgroups

In this section, (G, T) is a split reductive group and B is a Borel subgroup of G containing T. We determine the parabolic subgroups containing B. As a consequence, we find that the parabolic subgroups of G are exactly the groups $P(\lambda)$ with λ a cocharacter of G. As the parabolic subgroups of G and its semisimple quotient $G/R(G)$ are in natural one-to-one correspondence, we assume throughout that G is semisimple.

Maximal parabolic subgroups

Fix a Borel subgroup B of G containing T, and let Δ be the base corresponding to B. Recall (13.30) that, for every cocharacter λ of G, there is a subgroup variety $P(\lambda)$ whose k^a-points are the $x \in G(k^a)$ such that $\lim_{t \to 0} \lambda(t) \cdot x \cdot \lambda(t)^{-1}$ exists.

Let $(X, \Phi, \Phi^\vee)$ be the root system of (G, T). Because G is semisimple, Δ is a basis for $X_{\mathbb{Q}}$. The **fundamental cocharacters** (relative to Δ) are the elements λ_α of the dual basis for $X_{\mathbb{Q}}^\vee = X_*(T)_{\mathbb{Q}}$. Thus, $\langle \alpha, \lambda_\beta \rangle = \delta_{\alpha,\beta}$ for $\alpha, \beta \in \Delta$. For $\alpha \in \Delta$, let $P_\alpha = P(\lambda_\alpha)$.

PROPOSITION 21.88. *The group P_α is a proper parabolic subgroup of G containing B. Let $s_\beta \in W$ be the reflection corresponding to $\beta \in \Delta \smallsetminus \{\alpha\}$; then every element of $N_G(T)(k)$ representing $s_\beta \in W$ lies in $P_\alpha(k)$.*

PROOF. We may suppose that k is algebraically closed. Obviously $T \subset P_\alpha$ because $\lambda_\alpha(t) \cdot x \cdot \lambda_\alpha(t)^{-1} = x$ if $x, t \in T(k)$. For a root β and isomorphism $u_\beta : \mathbb{G}_a \to U_\beta$,

$$\lambda_\alpha(t) \cdot u_\beta(x) \cdot \lambda_\alpha(t)^{-1} = u_\beta(t^{\langle \beta, \lambda_\alpha \rangle} x), \quad \text{all } x \in U_\beta(k). \tag{138}$$

If $\beta \in \Phi^+$, then $\langle \beta, \lambda_\alpha \rangle \geq 0$, and so $u_\beta(x) \in P_\alpha(k)$. Hence $U_\beta \subset P_\alpha$ for all $\beta \in \Phi^+$, which implies that $B \subset P_\alpha$ (see 21.68). Therefore P_α is parabolic (17.16), and it is proper because it does not contain $U_{-\alpha}$ (this is clear from (138)). If $\beta \in \Delta \smallsetminus \{\alpha\}$ and $n \in N_G(T)(k)$ represents s_β, then

$$n \cdot \lambda_\alpha(t) \cdot n^{-1} = s_\beta(\lambda_\alpha)(t) = (\lambda_\alpha - \langle \beta, \lambda_\alpha \rangle \beta)(t) = \lambda_\alpha(t),$$

and so $\lambda_\alpha(t) \cdot n \cdot \lambda_\alpha(t)^{-1} = n \cdot \lambda_\alpha(t) \cdot n^{-1} \cdot n \cdot \lambda_\alpha(t)^{-1} = n$. It follows that $n \in P_\alpha(k)$.   □

From the formula (138), we see that $U_{-\beta}$ is contained in P_α if $\beta \in \Delta \smallsetminus \{\alpha\}$ but not if $\beta = \alpha$. It follows that P_α contains the semisimple subgroup G^β generated by U_β and $U_{-\beta}$ if β is a simple root $\neq \alpha$.

Description of the parabolic subgroups containing B

As before, (G, T) is a split semisimple group over k, B is a Borel subgroup of G containing T, and Δ is the base for $\Phi = \Phi(G, T)$ corresponding to B.

NOTATION 21.89. Let I be a subset of Δ. We define the following objects:

(a) W_I is the subgroup of W generated by the elements s_α, $\alpha \in I$;

(b) $\Phi_I = \mathbb{Z}I \cap \Phi$ (set of roots that are linear combinations of elements of I);

(c) $T_I = \left(\bigcap_{\alpha \in I} \mathrm{Ker}(\alpha)\right)_t$ (largest subtorus of T such that $\alpha(T_I) = 1$ if $\alpha \in I$);

(d) $L_I = C_G(T_I)$.

PROPOSITION 21.90. (a) *The pair* (L_I, T) *is a split reductive group with root datum* $(X(T), \Phi_I, \alpha \mapsto \alpha^\vee)$ *and Weyl group* W_I.

(b) *The intersection* $B \cap L_I$ *is a Borel subgroup* B_I *of* L_I *with* $\Phi^+(B_I) = \Phi_I \cap \Phi^+(B)$; *this has base* I.

PROOF. We may suppose that k is algebraically closed.

(a) The group L_I is reductive because it is the centralizer of a torus in a reductive group (17.59). Clearly, T is maximal in L_I and it is split, and so (L_I, T) is a split reductive group.

The root groups U_α contained in L_I are those centralizing the torus T_I. Let u_α be an isomorphism $\mathbb{G}_a \to U_\alpha$. For $t \in T(k)$ and $x \in \mathbb{G}_a(k)$,

$$u_\alpha(x) \cdot t \cdot u_\alpha(x)^{-1} = t t^{-1} \cdot u_\alpha(x) \cdot t \cdot u_\alpha(-x) = t \cdot u_\alpha(\alpha(t^{-1})x) \cdot u_\alpha(-x)$$
$$= t \cdot u_\alpha(\alpha(t^{-1})x - x).$$

If $\alpha \in \Phi_I$, then $\alpha(t^{-1}) = 1$ for all $t \in T_I$, and so $U_\alpha \subset L_I$. Conversely, if $U_\alpha \subset L_I$, then $u_\alpha(x) \cdot t \cdot u_\alpha(x)^{-1} = t$ for $t \in T_I(k)$, and so $\alpha(t^{-1}) = 1$; thus $\alpha(T_I) = 1$ and $\alpha \in \Phi_I$. It follows that (L_I, T) has root datum $(X, \Phi_I, \alpha \mapsto \alpha^\vee)$ (cf. 21.20), and this has Weyl group W_I.

(b) The intersection $B \cap L_I$ is a Borel subgroup of L_I (see 17.72). The associated system of positive roots is obviously $\Phi_I \cap \Phi^+(B)$. The set I is contained in a base for Φ_I, and it has the correct order to be a base. $\quad\square$

Let $w \in W(G, T)$. Recall from the last section that $C(w)$ is the smooth subscheme of G/B whose points x satisfy $\lim_{t \to 0} \lambda(t) \cdot x = wB/B$ for any (one or all) λ in the dominant Weyl chamber for B. It is the B_u-orbit of wB/B, and there is a Białynicki-Birula decomposition $G/B = \bigsqcup_{w \in W} C(w)/B$ where $C(w) = BwB$.

THEOREM 21.91. *For each subset* I *of* Δ, *there is a unique parabolic subgroup* P_I *of* G *containing* B *such that*

$$P_I = \bigsqcup_{w \in W_I} C(w).$$

The unipotent radical of P_I *is generated by the* U_α *with* $\alpha \in \Phi^+ \smallsetminus \Phi_I$, *and the map*

$$R_u(P_I) \rtimes L_I \to P_I$$

is an isomorphism. Every parabolic subgroup P *of* G *containing* B *is of the form* P_I *for a unique subset* I *of* Δ.

PROOF. Let $Z_I = \{wB/B \mid w \in W_I\}$, and let $X(Z_I)$ be the concentrator sub-scheme (see 13.58). We define P_I to the inverse image of $X(Z_I)$ in G. Then P_I is a smooth subscheme of G such that $|P_I| = \bigsqcup_{w \in W_I} |C(w)|$. To show that P_I is an algebraic subgroup of G, it suffices to show that $P_I(k^a)$ is a subgroup of $G(k^a)$. It is obviously stable under the formation of inverses and under left multiplication by elements of $B(k^a)$. It remains to show that it is stable under left multiplication by s_α, $\alpha \in \Phi_I$, but this follows from

$$s_\alpha B(k^a) w \subset B(k^a) w B(k^a) \cup B(k^a) s_\alpha w B(k^a)$$

(see 21.75). As $P_I(k^a) \supset C(e)(k^a)$, we have $C(e) = B$.

We have proved the first statement, and in proving the remainder, we may suppose that k is algebraically closed. Let $T_\alpha = \mathrm{Ker}(\alpha)_t$ and $G_\alpha = C_G(T_\alpha)$. The Bruhat decomposition of G_α is

$$G_\alpha = C(e) \cup C(s_\alpha),$$

and so U_α and $U_{-\alpha}$ are contained in $C(e) \cup C(s_\alpha)$. This implies that P_I contains L_I.

Let $U = B_u$. Then U is a maximal unipotent subgroup of P_I, and so $R_u(P_I)$ is the reduced identity component of $\bigcap_{w \in W_I} w(U)$ (see 17.56). We can write $U = U_I \cdot U^I$ with $U_I = \prod_{\alpha \in \Phi_I^+} U_\alpha$ and $U_I = \prod_{\alpha \in \Phi^+ \smallsetminus \Phi_I} U_\alpha$. The elements $w \in W_I$ map $\Phi^+ \smallsetminus \Phi_I$ onto itself, and so

$$\bigcap_{w \in W_I} w(U) = \left(\bigcap_{w \in W_I} w(U_I) \right) \cdot U^I.$$

But L_I is reductive, U_I is a maximal unipotent subgroup of L_I, and W_I the Weyl group of L_I, and so $\bigcap_{w \in W_I} w(U_I) = e$. Thus $R_u(P_I) = U^I$.

For $w \in W$,
$$C(w) = U^w w B = U^w w T U_I U^I.$$

As $U^w \subset L_I$ if $w \in W_I$, we deduce that $C(w) \subset L_I \cdot R_u(P_I)$. The homomorphism $R_u(P_I) \times L_I \to P_I$ is therefore surjective, and it is easily seen to be injective on k^a-points. It is an isomorphism because it is an isomorphism on the Lie algebras.

It remains to prove the third statement. Let P be a subgroup variety containing B, and let Φ_P be the set of weights of T on $\mathrm{Lie}(P/R_u(P))$. Let $I = \Phi_P \cap \Delta$. For $\alpha \in I$, the image in $P/R_u(P)$ of the intersection of G_α with P has the same Lie algebra as G_α, hence the same dimension, and so $G_\alpha \subset P$ (because G_α is connected). In particular, $U_{\pm\alpha} \subset P$, and so $L_I \subset P$. As $R_u(P_I) \subset B \subset P$, we find that $P_I \subset P$.

Conversely, the root systems of L_I and $P/R_u(P)$ are the same, and so $\dim L_I = \dim P/R_u(P)$. As L_I is reductive, $L_I \cap R_u(P) = e$, and so

$$P \hookrightarrow L_I \cdot R_u(P) \subset L_I \cdot B \subset L_I \cdot R_u(P_I) \subset P_I. \qquad \square$$

COROLLARY 21.92. *Let λ be a cocharacter of T. Then $P(\lambda)$ contains B if and only if $\langle \alpha, \lambda \rangle \geq 0$ for all $\alpha \in \Phi^+(B)$, in which case $P(\lambda) = P_I$ with $I = \{\alpha \in \Delta \mid \langle \alpha, \lambda \rangle = 0\}$.*

PROOF. From the definitions of the two groups, we see that $P(\lambda)$ contains U_α if and only if $\langle \alpha, \lambda \rangle \geq 0$. As B is generated by the U_α with $\alpha \in \Phi^+(B)$ (see 21.68a), this proves the first part of the statement. We saw in the proof of the theorem that $P(\lambda) = P_I$ with I the set of simple roots occurring as weights on $\mathrm{Lie}(P(\lambda)/R_u P(\lambda))$. As the weight of T on $\mathrm{Lie}(P(\lambda))$ (resp. $\mathrm{Lie}(R_u P(\lambda))$) are the roots α such that $\langle \alpha, \lambda \rangle \geq 0$ (resp. $\langle \alpha, \lambda \rangle > 0$), the set I is as described. $\square$

EXAMPLE 21.93. Let $G = \mathrm{GL}_n$ with its standard Borel pair (B, T). The corresponding base Δ for $\Phi(G, T)$ consists of the characters

$$\alpha_i \colon \mathrm{diag}(t_1, \ldots, t_n) \mapsto t_i/t_{i+1}, \quad i = 1, \ldots, n-1.$$

Let I be a subset of Δ. Identify Δ with $\{1, \ldots, n-1\}$, and set

$$\Delta \smallsetminus I = \{a_1, a_1 + a_2, \ldots, a_1 + \cdots + a_{s-1}\}.$$

Then P_I, L_I, and $R_u(P_I)$ consist respectively of the matrices of the form

$$\begin{pmatrix} A_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & A_s \end{pmatrix}, \quad \begin{pmatrix} A_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_s \end{pmatrix}, \quad \begin{pmatrix} I & * & * \\ 0 & \ddots & * \\ 0 & 0 & I \end{pmatrix}$$

with A_i an $a_i \times a_i$ matrix. Note that there are 2^{n-1} parabolic subgroups of this shape. As there are 2^{n-1} subsets I of Δ, these subgroups must exhaust the parabolic subgroups containing $B = P_\emptyset$.

REMARK 21.94. In 21.90, we attached a reductive group $L(I)$ to a subset I of Δ. More generally, we say that a subset Φ' of Φ is **closed** if $(\mathbb{N}\alpha + \mathbb{N}\beta) \cap \Phi \subset \Phi'$ for all $\alpha, \beta \in \Phi'$ and **symmetric** if $\Phi' = -\Phi'$. Given a symmetric closed subset Φ' of Φ, let $G(\Phi')$ denote the algebraic subgroup of G generated by T and the U_α with $\alpha \in \Phi'$. Then $(G(\Phi'), T)$ is a split reductive group, and

$$\mathrm{Lie}(G(\Phi')) = \mathrm{Lie}(T) \oplus \bigoplus_{\alpha \in \Phi'} \mathrm{Lie}(G)_\alpha.$$

Therefore, its root system is $(X, \Phi', \ldots)$, and its Weyl group is the subgroup of $W(G, T)$ generated by s_α with $\alpha \in \Phi'$. See Jantzen 2003, II, 1.7.

ASIDE 21.95. Let (G, T) be a split reductive group. Much is known about the lattice group subvarieties of G containing T – see, for example, the tables in Harebov and Vavilov 1996. In Sopkina 2009, the lattice of connected algebraic subgroups (not necessarily smooth) of G containing T is described in terms of the root system of (G, T). In particular, the smooth subgroups correspond to certain "quasi-closed" sets of roots (Borel and Tits 1965).

j.   The root data of the classical semisimple groups

We compute the root system attached to each of the classical split almost-simple groups. In each case we work with a convenient form of the group G in GL_n and find the eigenspaces of a maximal split torus acting on $\mathrm{Lie}(G)$. This determines the roots, and either we find the coroots directly, as we did for GL_n, or we deduce them from the fact that we have a root system. We obtain groups for each of the Dynkin diagrams A_n, B_n, C_n, D_n. As the Dynkin diagram determines the group up to isogeny (23.9 below), we obtain in this way a complete list of split geometrically almost-simple groups over k with Dynkin diagram A_n, B_n, C_n, or D_n.

Example (A_n): SL_{n+1}, $n \geq 1$

The diagonal torus $T = \{\mathrm{diag}(t_1,\ldots,t_{n+1}) \mid t_1 \cdots t_{n+1} = 1\}$ is a split maximal torus in SL_{n+1}. Its character group is

$$X^*(T) = \bigoplus_i \mathbb{Z}\chi_i \big/ \mathbb{Z}\chi,$$

where χ_i is the character $\mathrm{diag}(t_1,\ldots,t_{n+1}) \mapsto t_i$ and $\chi = \sum \chi_i$, and

$$X_*(T) = \left\{ \sum a_i \lambda_i \in \bigoplus_i \mathbb{Z}\lambda_i \mid \sum a_i = 0 \right\},$$

where $\sum a_i \lambda_i$ is the cocharacter $t \mapsto \mathrm{diag}(t^{a_1},\ldots,t^{a_n})$. The canonical pairing $X^*(T) \times X_*(T) \to \mathbb{Z}$ is $\langle \chi_j, \sum a_i \lambda_i \rangle = a_j$. The Lie algebra of SL_{n+1} is

$$\mathfrak{sl}_{n+1} = \{(a_{ij}) \in M_{n+1}(k) \mid \sum a_{ii} = 0\},$$

and SL_{n+1} acts on it by conjugation. Let $\bar{\chi}_i$ denote the class of χ_i in $X^*(T)$. Then T acts trivially on the set $\mathfrak{g}_0$ of diagonal matrices in $\mathfrak{g}$, and it acts through the character $\alpha_{ij} \overset{\text{def}}{=} \bar{\chi}_i - \bar{\chi}_j$ on $kE_{i,j}$, $i \neq j$ (see 21.6). Therefore,

$$\mathfrak{sl}_{n+1} = \mathfrak{g}_0 + \bigoplus_{i \neq j} \mathfrak{g}_{\alpha_{ij}}, \quad \mathfrak{g}_{\alpha_{ij}} = kE_{i,j},$$

and

$$\Phi = \{\alpha_{ij} \mid 1 \leq i,j \leq n+1, \quad i \neq j\}.$$

It remains to compute the coroots. Consider, for example, the root $\alpha = \alpha_{12}$. With the notation of Theorem 21.11,

$$T_\alpha = \{\mathrm{diag}(x,x,x_3,\ldots,x_n) \mid xxx_3 \cdots x_n = 1\}$$

and

$$G_\alpha = \left\{ \begin{pmatrix} * & * & 0 & & 0 \\ * & * & 0 & & 0 \\ 0 & 0 & * & & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & * \end{pmatrix} \in SL_n \right\}.$$

As in Example 21.16, $W(G_\alpha, T) = \{1, s_\alpha\}$, where s_α acts on T by interchanging the first two coordinates – it is represented by

$$
n_\alpha = \begin{pmatrix}
0 & 1 & 0 & & & 0 \\
-1 & 0 & 0 & & & 0 \\
0 & 0 & 1 & & & 0 \\
& & & \ddots & & \vdots \\
0 & 0 & 0 & & \cdots & 1
\end{pmatrix} \in N_G(T)(k).
$$

Let $\chi = \sum_{i=1}^{n+1} a_i \bar{\chi}_i \in X^*(T)$. Then

$$
s_\alpha(\chi) = a_2 \bar{\chi}_1 + a_1 \bar{\chi}_2 + \sum_{i=3}^{n+1} a_i \bar{\chi}_i = \chi - \langle \chi, \lambda_1 - \lambda_2 \rangle (\bar{\chi}_1 - \bar{\chi}_2).
$$

In other words,

$$
s_{\alpha_{12}}(\chi) = \chi - \langle \chi, \alpha_{12}^\vee \rangle \alpha_{12}
$$

with $\alpha_{12}^\vee = \lambda_1 - \lambda_2$, which proves that $\lambda_1 - \lambda_2$ is the coroot of α_{12}.

When the ordered index set $\{1, 2, \ldots, n+1\}$ is replaced with an unordered set, everything becomes symmetric among the roots, and so the coroot of α_{ij} is

$$
\alpha_{ij}^\vee = \lambda_i - \lambda_j, \quad \text{all } i \neq j.
$$

Let B be the standard (upper triangular) Borel subgroup of SL_{n+1}. The corresponding system of positive roots is $\Phi^+ = \{\chi_i - \chi_j \mid i < j\}$, which has base $\{\chi_1 - \chi_2, \ldots, \chi_n - \chi_{n+1}\}$.

The set Φ is a root system in the vector space $X^*(T) \otimes \mathbb{Q} \simeq \mathbb{Q}^{n+1}/\langle e_1 + \cdots + e_{n+1} \rangle$. We can transfer it to a root system in the hyperplane $H: \sum_{i=1}^{n+1} a_i X_i = 0$ by noticing that each element of $\mathbb{Q}^{n+1}/\langle e_1 + \cdots + e_{n+1} \rangle$ has a unique representative in H.

SUMMARY 21.96. Let V be the hyperplane in $\mathbb{Q}^{n+1}$ of $(n+1)$-tuples (a_i) such that $\sum a_i = 0$. Let $\{\varepsilon_1, \ldots, \varepsilon_{n+1}\}$ be the standard basis for $\mathbb{Q}^{n+1}$, and consider

roots	$\Phi = \{\varepsilon_i - \varepsilon_j \mid 1 \leq i, j \leq n+1, i \neq j\}$
root lattice	$Q(\Phi) = \{\sum a_i \varepsilon_i \mid a_i \in \mathbb{Z}, \sum a_i = 0\}$
weight lattice	$P(\Phi) = Q(\Phi) + \langle \varepsilon_1 - (\varepsilon_1 + \cdots + \varepsilon_{n+1})/(n+1) \rangle\}$
base	$\Delta = \{\varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_n - \varepsilon_{n+1}\}$.

The pair (V, Φ) is an indecomposable root system with Dynkin diagram of type A_n (see p. 626). The group SL_n is split and geometrically almost-simple with root system (V, Φ). It is simply connected because $X = P(\Phi)$, and its centre is μ_{n+1} because $P(\Phi)/Q(\Phi) \simeq \mathbb{Z}/n\mathbb{Z}$.

Example (B_n): SO_{2n+1}, $n \geq 2$

Let O_{2n+1} denote the algebraic subgroup of GL_{2n+1} preserving the quadratic form

$$q = x_0^2 + x_1 x_{n+1} + \cdots + x_n x_{2n},$$

i.e., $O_{2n+1}(R) = \{g \in GL_{2n+1}(R) \mid q(gx) = x \text{ for all } x \in R^{2n}\}$. Define SO_{2n+1} to be the kernel of the determinant map $O_{2n+1} \to \mathbb{G}_m$. When $\mathrm{char}(k) \neq 2$, SO_{2n+1} is the special orthogonal group of the symmetric bilinear form

$$\phi = 2x_0 y_0 + x_1 y_{n+1} + x_{n+1} y_1 + \cdots + x_n y_{2n} + x_{2n} y_n,$$

i.e., it consists of the $2n + 1 \times 2n + 1$ matrices A of determinant 1 such that

$$A^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix}.$$

The subgroup $T = \{\mathrm{diag}(1, t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1})\}$ is a split maximal torus in SO_{2n+1} and

$$X^*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i, \quad \chi_i : \mathrm{diag}(1, t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}) \mapsto t_i$$

$$X_*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\lambda_i, \quad \lambda_i : t \mapsto \mathrm{diag}(1, \ldots, \overset{i+1}{t}, \ldots, t^{-1}, \ldots 1)$$

$$\langle \chi_i, \lambda_j \rangle = \delta_{ij}, \quad \chi_i \in X^*(T), \quad \lambda_j \in X_*(T).$$

The Lie algebra $\mathfrak{so}_{2n+1}$ of SO_{2n+1} consists of the $2n + 1 \times 2n + 1$ matrices A of trace zero such that $\phi(x, Ax) = 0$ for all x. When $\mathrm{char}(k) \neq 2$, the second condition becomes

$$A^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} A = 0.$$

In the adjoint action of T on $\mathfrak{so}_{2n+1}$, there are the following nonzero eigenvectors,

Weight	Eigenvector	
$\chi_i + \chi_j$	$E_{i,n+j} - E_{j,n+i}$	$1 \leq i < j \leq n$
$-\chi_i - \chi_j$	$E_{n+i,j} - E_{n+j,i}$	$1 \leq i < j \leq n$
$\chi_i - \chi_j$	$E_{i,j} - E_{n+j,n+i}$	$1 \leq i \neq j \leq n$
$-\chi_i$	$E_{0,i} - 2E_{n+i,0}$	$1 \leq i \leq n$
χ_i	$E_{0,n+i} - 2E_{i,0}$	$1 \leq i \leq n.$

SUMMARY 21.97. Let $V = \mathbb{Q}^n$ with standard basis $\{\varepsilon_1, \ldots \varepsilon_n\}$, and consider

roots	$\Phi = \pm\varepsilon_i \ (1 \le i \le n), \pm\varepsilon_i \pm \varepsilon_j \ (1 \le i < j \le n)$
root lattice	$Q(\Phi) = \bigoplus_{i=1}^{n} \mathbb{Z}\varepsilon_i$
weight lattice	$P(\Phi) = \bigoplus_{i=1}^{n} \mathbb{Z}\varepsilon_i + \mathbb{Z}(\frac{1}{2}\sum_{i=1}^{n}\varepsilon_i)$
base	$\Delta = \varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_{n-1} - \varepsilon_n, \varepsilon_n.$

The pair (V, Φ) is an indecomposable root system with Dynkin diagram of type
B_n (see p. 626). The group SO_{2n+1} is split and geometrically almost-simple
with root system (V, Φ). It is an adjoint group because $X = Q(\Phi)$. Its simply
connected covering group is the spin group $Spin_{2n+1}$ (see Section 24i below),
which has center μ_2 because $P(\Phi)/Q(\Phi) \simeq \mathbb{Z}/2\mathbb{Z}$.

Example (C_n): $Sp_{2n}, n \ge 3$

Let Sp_{2n} denote the algebraic subgroup of GL_{2n} of matrices preserving the
skew-symmetric bilinear

$$\phi = x_1 y_{n+1} - x_{n+1} y_1 + \cdots + x_n y_{2n} - x_{2n} y_n.$$

Thus Sp_{2n} consists of the $2n \times 2n$ matrices A such that $\phi(Ax, Ay) = \phi(x, y)$,
i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The subgroup $T = \text{diag}(t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1})$ is a split maximal torus in
SO_{2n+1}, and

$$X^*(T) = \bigoplus_{1 \le i \le n} \mathbb{Z}\chi_i, \quad \chi_i : \text{diag}(t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}) \mapsto t_i$$

$$X_*(T) = \bigoplus_{1 \le i \le n} \mathbb{Z}\lambda_i, \quad \lambda_i : t \mapsto \text{diag}(1, \ldots, \overset{i}{t}, \ldots, t^{-1}, \ldots 1).$$

The Lie algebra $\mathfrak{sp}_n$ of Sp_n consists of the $2n \times 2n$ matrices A such that
$\phi(Ax, y) + \phi(x, Ay) = 0$, i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} + \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = 0.$$

In the adjoint action of T on $\mathfrak{sp}_n$, there are the following nonzero eigenvectors,

Weight	Eigenvector	
$2\chi_i$	$E_{i,n+i}$	$1 \le i \le n$
$-2\chi_i$	$E_{n+i,i}$	$1 \le i \le n$
$\chi_i + \chi_j$	$E_{i,n+j} + E_{j,n+i}$	$1 \le i < j \le n$
$-\chi_i - \chi_j$	$E_{n+i.j} + E_{n+j,i}$	$1 \le i < j \le n$
$\chi_i - \chi_j$	$E_{i,j} - E_{n+j,n+i}$	$1 \le i \ne j \le n.$

SUMMARY 21.98. Let $V = \mathbb{Q}^n$ with standard basis $\{\varepsilon_1, \ldots \varepsilon_n\}$, and consider

roots	$\Phi = \pm 2\varepsilon_i \ (1 \le i \le n), \pm\varepsilon_i \pm \varepsilon_j, (1 \le i < j \le n)$
root lattice	$Q(\Phi) = \{\sum a_i e_i \mid a_i \in \mathbb{Z}, \ \sum a_i \in 2\mathbb{Z}\}$
weight lattice	$P(\Phi) = \{\sum a_i e_i \mid a_i \in \mathbb{Z}\}$
base	$\Delta \ \varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_{n-1} - \varepsilon_n, 2\varepsilon_n.$

The pair (V, Φ) is an indecomposable root system with Dynkin diagram of type C_n (see p. 626). The group Sp_n is split and geometrically almost-simple. It is simply connected because $X = P(\Phi)$, and its centre is μ_2 because $P(\Phi)/Q(\Phi)$ equals $\mathbb{Z}/2\mathbb{Z}$.

Example (D_n): $\mathrm{SO}_{2n}, n \ge 4$

Let O_{2n} denote the algebraic subgroup of GL_{2n} of matrices preserving the quadratic form

$$q = x_1 x_{n+1} + \cdots + x_n x_{2n}.$$

When $\mathrm{char}(k) \ne 2$, we define SO_{2n} to be the kernel of the determinant map $O_{2n} \to \mathbb{G}_m$; it is the special orthogonal group of the symmetric bilinear form

$$\phi = x_1 y_{n+1} + x_{n+1} y_1 + \cdots + x_n y_{2n} + x_{2n} y_{2n}.$$

Otherwise, we define SO_n as in Section 24i below.

The subgroup $T = \{\mathrm{diag}(t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1})\}$ is a split maximal torus in SO_{2n+1} and

$$X^*(T) = \bigoplus_{1 \le i \le n} \mathbb{Z}\chi_i, \quad \chi_i: \mathrm{diag}(1, t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}) \mapsto t_i$$

$$X_*(T) = \bigoplus_{1 \le i \le n} \mathbb{Z}\lambda_i, \quad \lambda_i: t \mapsto \mathrm{diag}(1, \ldots, \overset{i}{t}, \ldots, t^{-1}, \ldots 1).$$

The Lie algebra $\mathfrak{so}_{2n}$ of SO_{2n} consists of the $2n+1 \times 2n+1$ matrices A of trace zero such that $\phi(x, Ax) = 0$ for all x. When $\mathrm{char}(k) \ne 2$, the second condition becomes

$$A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} + \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = 0.$$

In the adjoint action of T on $\mathfrak{so}_{2n}$, there are the following nonzero eigenvectors:

Weight	Eigenvector	
$\chi_i + \chi_j$	$E_{i,n+j} - E_{j,n+i}$	$1 \le i < j \le n$
$-\chi_i - \chi_j$	$E_{n+i,j} - E_{n+j,i}$	$1 \le i < j \le n$
$\chi_i - \chi_j$	$E_{ij} - E_{n+j,n+i}$	$1 \le i \ne j \le n.$

SUMMARY 21.99. Let $V = \mathbb{Q}^n$, and let $\varepsilon_1, \ldots \varepsilon_n$ be the standard basis for $\mathbb{Q}^n$. Then

roots	$\Phi = \pm\varepsilon_i \pm \varepsilon_j \ (1 \leq i < j \leq n)$
root lattice	$Q(\Phi) = \{\sum a_i e_i \mid a_i \in \mathbb{Z}, \ \sum a_i \in 2\mathbb{Z}\}$
weight lattice	$P(\Phi) = \bigoplus_{i=1}^n \mathbb{Z}\varepsilon_i + \mathbb{Z}(\frac{1}{2}\sum_{i=1}^n \varepsilon_i)$
base	$\Delta = \varepsilon_1 - \varepsilon_2, \ldots, \varepsilon_{n-1} - \varepsilon_n, \varepsilon_{n-1} + \varepsilon_n.$

The pair (V, Φ) is an indecomposable root system with Dynkin diagram of type D_n (see p. 626). The group SO_{2n} is split and geometrically almost-simple. It is neither adjoint nor simply connected because $Q(\Phi) \subsetneqq X \subsetneqq P(\Phi)$. Its simply connected covering group is the spin group Spin_{2n} (see Section 24i below). When n is even, the centre of Spin_{2n} is $\mu_2 \times \mu_2$ because $P(\Phi)/Q(\Phi) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and when n is odd, its centre is μ_4 because $P(\Phi)/Q(\Phi) \simeq \mathbb{Z}/4\mathbb{Z}$.

The subscript on A_n, B_n, C_n, D_n denotes the rank of the group.

Exercises

EXERCISE 21-1. Verify the statements in Example 21.15 (root data of semisimple rank 1).

EXERCISE 21-2. Show that a reductive group contains no nontrivial normal connected unipotent algebraic subgroup.

EXERCISE 21-3. Show that $X \mapsto (X^t)^{-1}: \mathrm{SL}_{n+1}(R) \to \mathrm{SL}_{n+1}(R)$ is an automorphism of SL_{n+1}, and that it acts on the Dynkin diagram of SL_{n+1} as the obvious nontrivial symmetry (X^t is the transpose of X).

EXERCISE 21-4. Let $(X, \Phi, \Phi^\vee)$ be a root datum. Let $X_0 = \{x \in X \mid \langle x, \Phi^\vee \rangle = 0\}$, and let $X' = X/X_0$. Let Φ' denote the image of Φ in X', and let $Q = Q(\Phi) \simeq Q(\Phi')$ (see C.43). Then (X', Φ') is a semisimple root datum. Assume that there exists a split semisimple group (H, T) with root datum (X', Φ'). Then $Z(H)$ has character group X'/Q. Let $\varphi: Z(H) \to D$ be the homomorphism of diagonalizable groups corresponding to the homomorphism $X/Q \to X'/Q$. Define $G(\varphi)$ and $T(\varphi)$ to be the cokernels

$$Z(H) \to H \times D \to G(\varphi)$$
$$Z(H) \to T \times D \to T(\varphi)$$

(see 19.27). Show that $(G(\varphi), T(\varphi))$ is a split reductive group with root datum $(X, \Phi, \Phi^\vee)$.

EXERCISE 21-5. Let (G, B, N, S) be a Tits system.
  (a) Show that the union $BwB \cup BswB$ is disjoint for all $s \in S$, $w \in W$.

(b) Show that $wBs \subset BwB \cup BwsB$ for all $s \in S$, $w \in W$.

Let $w \in W$. An expression $w = s_1 \cdots s_n$ ($s_i \in S$) for w is said to be **reduced** if it is as short as possible; we then set $l(w) = n$.

(c) Show that $l(w) = 1$ if and only if $w = e$. Show that

$$-1 \leq l(ws) - l(w) \leq 1$$
$$-1 \leq l(sw) - l(w) \leq 1$$

for all $s \in S$, $w \in W$.

For a subset I of S, let W_I denote the subgroup of W generated by I, and let $P_I = BW_I B$.

(d) Show that $P_\emptyset = B$.

(e) Show that P_I is a subgroup of G, and deduce that $P_S = G$.

(f) Show that $BwB = B$ implies that $w = e$.

(g) Let w and w' be elements of W with $l(w) \leq l(w')$. Prove by induction on $l(w)$ that $BwB = Bw'B$ implies that $w = w'$. [Write $w = sv$ with $l(v) = l(w) - 1$.]

(h) Deduce that $G = \bigsqcup_{w \in W} BwB$ (Bruhat decomposition).

EXERCISE 21-6. This exercise gives a direct proof of the Bruhat decomposition for GL_n. We write G for $GL_n(k)$ and B for $B(k)$.[4]

(a) Let $F_n \supset \cdots \supset F_1 \supset F_0$ and $F'_n \supset \cdots \supset F'_1 \supset F'_0$ be two maximal flags (in some vector space of dimension n), and let $d_{ij} = \dim F_i \cap F'_j$. Show that the numbers d_{ij} determine the orbit of the pair (F, F'), i.e., if a pair (E, E') has the same numbers, then $(E, E') = g(F, F')$ for some $g \in GL_n(k)$. (Hint: choose suitable bases.)

(b) Let $w_{ij} = d_{ij} - d_{i-1,j} - d_{i,j-1} + d_{i-1,j-1}$. Show that (w_{ij}) is a permutation matrix and that the d_{ij} can be recovered from the w_{ij} (note that the w_{ij} determine where the jump from 0 to 1 occurs in the filtration of F_i/F_{i-1} induced by F').

(c) Show that every permutation matrix w arises in this way, for example, from the pair $(F, w \cdot F)$.

(d) Deduce that, for any maximal flag F,

$$G/B \times G/B = \bigsqcup_{w \in W} G \cdot (F, w \cdot F)$$

(we have identified W with the group of permutation matrices in GL_n).

---

[4]For this and other proofs, see https://mathoverflow.net/, question 15438.

Representations of Reductive Groups

We begin by classifying the semisimple representations of a split reductive group over a field k (see 22.2). When k has characteristic zero, this includes all of them (22.42). Throughout, representations are finite-dimensional unless it is specified otherwise. As usual, R is a (variable) k-algebra.

a.   The semisimple representations of a split reductive group

Let (G, T) be a split reductive group over k, and let $(X, \Phi, \Phi^\vee)$ be its root datum. Because T is split, every representation (V, r) of G decomposes into a direct sum $V = \bigoplus_{\lambda \in X(T)} V_\lambda$ of its weight spaces V_λ for the action of T (see 12.12). The λ for which $V_\lambda \neq 0$ are called the weights of (V, r).

Statement of the fundamental theorem

To classify the semisimple representations of G, it suffices to classify the simple representations. For this, we fix a Borel subgroup B of G containing T. Let Φ^+ denote the corresponding system of positive roots and Δ the set of simple roots in Φ^+. Define an order relation on X by setting $\lambda \geq \mu$ if $\lambda - \mu = \sum_{\alpha \in \Delta} m_\alpha \alpha$ with $m_\alpha \in \mathbb{N}$. Thus $\Phi^+ = \{\alpha \in \Phi \mid \alpha > 0\}$.

DEFINITION 22.1.   An element λ of X is said to be **dominant** if $\langle \lambda, \alpha^\vee \rangle \geq 0$ for all $\alpha \in \Phi^+$.

THEOREM 22.2 (FUNDAMENTAL THEOREM).   *For each dominant $\lambda \in X$, there exists a simple representation $V(\lambda)$ of G, unique up to isomorphism, that decomposes as a representation of T into*

$$V(\lambda) = V(\lambda)_\lambda \oplus \bigoplus_\mu V(\lambda)_\mu$$

with $V(\lambda)_\lambda$ of dimension 1 and all $\mu < \lambda$. Every simple representation is isomorphic to $V(\lambda)$ for a unique dominant λ.

Before proving the theorem, we list some complements.

22.3. Every simple representation (V, r) has a unique weight $\lambda(r)$ (called the **highest weight**) such that $\mu < \lambda(r)$ for all other weights. The map $(V, r) \mapsto \lambda(r)$ defines a bijection from the set of isomorphism classes of simple representations of G to the set of dominant $\lambda \in X$.

22.4. The only endomorphisms of $V(\lambda)$ are the scalar multiplications by elements of k, i.e., $\mathrm{End}(V(\lambda)) \simeq k$ (Exercise 22-1). Therefore, $V(\lambda)$ remains simple under extension of the base field (4.19). It follows that if (V, r) is a simple representation of G of highest weight λ over k, then $(V, r) \otimes k'$ is a simple representation of $G_{k'}$ of highest weight λ over k'.

22.5. Let G be a split reductive group over k, and let k' be an extension of k. For every semisimple representation (V', r') of $G_{k'}$ over k', there exists a semisimple representation (V, r) of G over k and an isomorphism $(V, r) \otimes k' \to (V', r')$. This follows from 22.4.

22.6. Let $V(\lambda)$ and $V(\lambda')$ be simple representations of split reductive groups G and G' with highest weights λ and λ'. Because $\mathrm{End}(V(\lambda)) \simeq k$, the representation $V(\lambda) \otimes V(\lambda')$ of $G \times G'$ is simple (4.21), and it obviously has highest weight $\lambda + \lambda'$.

22.7. Let G be a reductive group over k (not necessarily split). Every semisimple representation of G over k^{a} is defined over k^{s}. Indeed, G splits over k^{s}, and so we can apply 22.5.

The dominant characters

Let (G, B, T) be as before, and let $X(T)^+$, or just X^+, denote the set of dominant $\lambda \in X(T)$. We describe X^+ and make the fundamental theorem more explicit.

22.8. Recall that the root lattice $Q = Q(\Phi)$ of $(X, \Phi, \Phi^\vee)$ is the $\mathbb{Z}$-submodule of X generated by the roots. The pair $(Q \otimes_{\mathbb{Z}} \mathbb{Q}, \Phi)$ is a root system, and the weight lattice $P(\Phi)$ consists of the $\lambda \in Q \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $\langle \lambda, \alpha^\vee \rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$ (see C.26). Then Q and P are lattices in $Q \otimes_{\mathbb{Z}} \mathbb{Q}$, and

$$X \subset X_0 + P(\Phi),$$

where $X_0 = \{x \in X \mid \langle x, \alpha^\vee \rangle = 0 \text{ for all } \alpha \in \Phi\}$. Let $\Delta = \{\alpha_1, \ldots, \alpha_n\}$. Then $\{\alpha_1^\vee, \ldots, \alpha_n^\vee\}$ is a base for $\Phi^\vee$, and

$$Q(\Phi) = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$
$$P(\Phi) = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n,$$

where $\{\lambda_1, \ldots, \lambda_n\}$ is the basis of $Q \otimes_{\mathbb{Z}} \mathbb{Q}$ dual to $\{\alpha_1^\vee, \ldots, \alpha_n^\vee\}$, i.e., λ_i in $Q \otimes_{\mathbb{Z}} \mathbb{Q}$ is such that $\langle \lambda_i, \alpha_j^\vee \rangle = \delta_{ij}$ for all j. The λ_i are called the **fundamental weights**. A dominant character λ can be written uniquely in the form

$$\lambda = \sum_{1 \le i \le n} m_i \lambda_i + \lambda_0, \quad m_i \in \mathbb{N}, \quad \sum m_i \lambda_i \in X, \quad \lambda_0 \in X_0. \quad (139)$$

22.9. If G is semisimple, then (V, Φ) is a root system with $V = X_{\mathbb{Q}}$, and X is a lattice in V such that $Q \subset X \subset P$ (see C.35). In particular, $X_0 = 0$, and the dominant λ in $X_{\mathbb{Q}}$ form a cone C with the fundamental weights $\lambda_1, \ldots, \lambda_n$ as a base (i.e., every $\lambda \in C$ can be written uniquely $\lambda = \sum a_i \lambda_i$, $a_i \ge 0$).

Choose an inner product $(\ ,\ )$ on V for which the s_α, $\alpha \in \Phi$, act as orthogonal transformations. Then, for $\lambda \in V$, $\langle \lambda, \alpha^\vee \rangle = 2(\lambda, \alpha)/(\alpha, \alpha)$. Hence,

$$P(\Phi) = \left\{ \lambda \in X_{\mathbb{Q}} \ \middle|\ 2\frac{(\lambda, \alpha)}{(\alpha, \alpha)} \in \mathbb{Z} \text{ all } \alpha \in \Phi \right\} = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n$$

where λ_i is the element of V such that $2\frac{(\lambda_i, \alpha_j)}{(\alpha_j, \alpha_j)} = \delta_{ij}$.

22.10. When G is a torus, $X^+ = X_0 = X$, and the fundamental theorem says that the simple representations of G are the one-dimensional spaces on which G acts through a character (in agreement with 12.12).

22.11. Let G be semisimple. The centre of G is the subgroup of T with character group X/Q (see 21.8). As the weights of T on $V(\lambda)$ are of the form $\lambda - \sum_{\alpha \in \Delta} m_\alpha \alpha$ with $m_\alpha \in \mathbb{N}$, the centre of G acts on $V(\lambda)$ through the character $\lambda + Q$. If G is simply connected, then $X = P$, and

$$X^+ = P^+ \overset{\text{def}}{=} \{\lambda \in P \mid \langle \lambda, \alpha^\vee \rangle \ge 0 \text{ for all } \alpha \in \Phi\}.$$

In general, $Q \subset X \subset P$ and $X^+ = X \cap P^+$. The simple representation $V(\lambda)$ of the universal covering $\tilde{G}$ of G factors through G if and only if $\lambda \in X$.

22.12. An isogeny $(G', T') \to (G, T)$ of split reductive groups realizes $X(T)$ as a subgroup of $X(T')$ of finite index. Let λ be a dominant element of $X(T')$, and let $V(\lambda)$ be a simple representation of G' whose weights other than λ are $< \lambda$. Then, as in the preceding example, $Z(G')$ acts on $V(\lambda)$ through the character $\lambda + Q$, and λ factors through G if and only if $\lambda \in X(T)$.

Proof of the fundamental theorem

We shall, in fact, prove somewhat more precise statements (22.18, 22.19, 22.20). As usual, for a root α of (G, T), u_α denotes an isomorphism $\mathbb{G}_a \to U_\alpha$, G^α is the semisimple subgroup generated by U_α and $U_{-\alpha}$, and $n_\alpha \in G^\alpha(k)$ represents the nontrivial element of $W(G^\alpha, T)$ (Section 21c).

PROPOSITION 22.13. *Every character of T occurs as a weight in some representation of G.*

PROOF. Let $\chi \in X(T)$. As the homomorphism of coordinate rings $\mathcal{O}(G) \rightarrow \mathcal{O}(T)$ is surjective, there exists an $f \in \mathcal{O}(G)$ such that $f|T = \chi$. The action of T on $\mathcal{O}(G)$ is semisimple, and so f is a sum of eigenfunctions:

$$f = f_1 + \cdots + f_r, \quad f_i \in \mathcal{O}(X)_{\chi_i}, \quad \chi_1, \ldots, \chi_r \text{ distinct characters of } T.$$

Now, for $t \in T(R)$,

$$\chi(t) = f(t) = (tf)(1) = \sum_i (tf_i)(1) = \sum_i (\chi_i(t)f)(1) = \sum_i f_i(1)\chi_i(t),$$

and so $\chi = \sum_{i=1}^r f_i(1)\chi_i$. But distinct characters are linearly independent (4.24), and so $\chi = \chi_i$ for some i. $\qquad\square$

Let V be a finite-dimensional vector space, and consider an action $\mu \colon \mathbb{G}_a \times V_a \rightarrow V_a$ of $\mathbb{G}_a$ on V_a. To say that μ is a regular function means that, when we choose a basis $(e_j)_{1 \leq j \leq n}$ for V, each coordinate of $\mu(c, \sum b_j e_j)$ is a polynomial in c and the b_j, say,

$$\sum_{i,i_1,\ldots,i_n} a_{i i_1 \cdots i_n} c^i b_1^{i_1} \cdots b_n^{i_n} = \sum_i c^i \left(\sum_{i_1,\ldots,i_n} a_{i i_1 \cdots i_n} b_1^{i_1} \cdots b_n^{i_n} \right).$$

Thus $\mu(c, v) = \sum_{i \geq 0} c^i v_i$ with $v_i \in V$ independent of c.

PROPOSITION 22.14. *Let (V, r) be a representation of G, and let v lie in the weight space V_λ. Let α be a root of (G, T). There exist $v_i \in V_{\lambda+i\alpha}, i = 1, 2, \ldots,$ such that*
$$u_\alpha(c) \cdot v = v + \sum_{i \geq 1} c^i v_i \quad \text{(finite sum)}$$
for all $c \in \mathbb{G}_a(k)$.

PROOF. We write $g \cdot v$ for $r(g)(v)$. From the above discussion, we see that

$$u_\alpha(c) \cdot v = \sum_{i \geq 0} c^i v_i. \tag{140}$$

It remains to show that $v_i \in V_{\lambda+i\alpha}$ and that $v_0 = v$. Let $t \in T(R)$. Then

$$t \cdot (u_\alpha(c) \cdot v) = \sum_{i \geq 0} c^i (t \cdot v_i),$$

but also

$$\begin{aligned} t \cdot (u_\alpha(c) \cdot v) &= (t\, u_\alpha(c)\, t^{-1}) \cdot (t \cdot v) = (u_\alpha(\alpha(t)c)) \cdot \lambda(t)v \\ &= \sum_{i \geq 0} \alpha(t)^i c^i \lambda(t) v_i. \end{aligned}$$

On comparing these equalities, we find that $t \cdot v_i = \lambda(t) \cdot \alpha(t)^i \cdot v_i$. and so $v_i \in V_{\lambda+i\alpha}$. Setting $c = 0$ in (140), we find that $v = v_0$ because $u_\alpha(0) = e$. $\quad\square$

LEMMA 22.15. *Let (V, r) be a representation of G. If $v \in V_\lambda$, then $n_\alpha \cdot v \in V_{n_\alpha(\lambda)}$.*

PROOF. For $t \in T(R)$,

$$t \cdot (n_\alpha \cdot v) = n_\alpha(n_\alpha^{-1} t \, n_\alpha) \cdot v = n_\alpha \cdot \lambda(n_\alpha^{-1} t \, n_\alpha) \, v = n_\alpha(\lambda)(t)(n_\alpha \cdot v),$$

and so, by definition, $n_\alpha \cdot v \in V_{n_\alpha(\lambda)}$. □

It follows that $\dim(V_\lambda) = \dim(V_{w(\lambda)})$ for all $w \in W(G,T)$.

DEFINITION 22.16. An element of V is **primitive** if it is an eigenvector for B, i.e., if it spans a one-dimensional subspace stable under B.

PROPOSITION 22.17. *Let (V,r) be a representation of G (not necessarily finite-dimensional). Suppose that V is generated (as a G-module) by a primitive element v of weight λ. Then λ has multiplicity 1 on V, and the remaining weights are of the form $\lambda - \sum m_\alpha \alpha$ with $m_\alpha \geq 0$ and $\alpha \in \Delta$. Moreover, λ is dominant, and V has a largest proper subspace stable under G.*

PROOF. Let $U^- B$ be the big cell (21.85). As $U^- B$ is dense in G, we see that V is spanned by $U^- B v$, and hence by $U^- v$ (because B acts as scalars on v). Let $\alpha \in \Phi^+$, and consider an element $u_{-\alpha}(c_\alpha)$ of U^-. By Proposition 22.14,

$$u_{-\alpha}(c_\alpha) \cdot v = v + \sum_{i \geq 1} c_\alpha^i v_i, \quad \text{with } v_i \in V_{\lambda - i\alpha}.$$

As U^- is generated by the $U_{-\alpha}$ with $\alpha \in \Phi^+$, we see that $u^- \cdot v \in v + \bigoplus_{\mu < \lambda} V_\mu$ if $u^- \in U^-$, and so

$$V = kv \oplus \bigoplus_{\mu < \lambda} V_\mu. \tag{141}$$

The second sum is over the weights of the form $\mu = \lambda - \sum_{\alpha > 0} m_\alpha \alpha$, $m_\alpha \in \mathbb{N}$. In the decomposition (141), V_λ is the line kv, and so λ has multiplicity 1.

If α is a simple root, then $w_\alpha(\lambda)$ is also a weight of r (see 22.15). But $w_\alpha(\lambda) = \lambda - \langle \lambda, \alpha^\vee \rangle \alpha$. Hence $\langle \lambda, \alpha^\vee \rangle \geq 0$, and so λ is dominant.

Finally, every proper G-stable subspace of V is a sum of weight spaces V_μ with $\mu \neq \lambda$, and so the sum of *all* proper G-stable subspaces is still proper. □

THEOREM 22.18. *Let (V,r) be a simple representation of G.*

(a) *There exists a primitive element v of V, unique up to scalar multiplication.*

(b) *The weight λ of v is dominant of multiplicity 1.*

(c) *The weights μ of V are of the form $\mu = \lambda - \sum_{\alpha \in \Delta} m_\alpha \alpha$ with $m_\alpha \in \mathbb{N}$ (and so λ is the highest weight of V).*

PROOF. The group B is split (21.34), hence trigonalizable (16.52), and so V contains a primitive element v. Because V is simple, v generates V, and so its weight λ has multiplicity 1 (see 22.17).

Let v and v' be primitive elements of V with weights λ and λ' respectively. Because V is simple, v generates V, and so Proposition 22.17 shows that

$$\lambda' = \lambda - \sum_{\alpha \in \Delta} m_\alpha \alpha, \quad m_\alpha \geq 0.$$

Similarly,

$$\lambda = \lambda' - \sum_{\alpha \in \Delta} m'_\alpha \alpha, \quad m'_\alpha \geq 0.$$

These equations imply that $m_\alpha = 0 = m'_\alpha$ for all α, and so $\lambda = \lambda'$. As λ has multiplicity 1, the elements v and v' span the same line. This proves (a), and the rest of the statement follows from Proposition 22.17. □

THEOREM 22.19. *Two simple representations of G are isomorphic if and only if their highest weights are equal.*

PROOF. The necessity being obvious, we prove the sufficiency. Let V_1 and V_2 be two simple representations with the same highest weight λ, and let v_1 and v_2 be primitive elements of V_1 and V_2 (of weight λ). Clearly $v = v_1 + v_2$ is a primitive element of $V_1 \oplus V_2$ of weight λ. Let V be the G-subspace of $V_1 \oplus V_2$ generated by v. The projection $V_1 \oplus V_2 \to V_2$ defines a G-homomorphism $\varphi \colon V \to V_2$. As $\varphi(v) = v_2$, the map φ is surjective. The kernel of φ is $V_1 \cap V$, which does not contain v_1 because the only elements of V of weight λ are the multiples of v. Therefore $V_1 \cap V \neq V_1$ and, as V_1 is simple, $V_1 \cap V = 0$. Therefore φ is an isomorphism $V \to V_2$. Similarly, V projects isomorphically onto V_1. Hence V_1 and V_2 are isomorphic. □

THEOREM 22.20. *Every dominant character of G is the highest weight of some simple representation of G.*

It suffices to show that there exists a representation (possibly infinite-dimensional) containing a primitive vector v of weight λ, because then the quotient of the G-submodule generated by v by its largest proper subspace stable under G (see 22.17) is a simple module with highest weight λ. Recall that simple modules are automatically finite-dimensional (4.16).

DEFINITION 22.21. For a character λ of B, let $E(\lambda)$ denote the k-subspace of $\mathcal{O}(G)$ of f satisfying

$$f(xb) = f(x)\lambda(b^{-1}) \quad x \in G, \, b \in B. \tag{142}$$

It is G-submodule of $\mathcal{O}(G)$ for the left regular representation: $^g f(x) = f(g^{-1}x)$, $g \in G$, $f \in \mathcal{O}(G)$, $x \in G$.

Let $w_0 \in W$ be the symmetry with respect to B, so that $w_0(\Phi^+) = \Phi^- = -\Phi^+$ and $w_0(B) = B^-$ (see 21.72).

PROPOSITION 22.22. *If $E(\lambda) \neq 0$, then it contains a primitive element v, unique up to scalar multiplication, and the weight of v is $w_0(\lambda)$.*

PROOF. Let $U = B_u^-$. Then the map

$$U \times B \to G, \quad (u, b) \mapsto u w_0 b$$

is an open immersion. Therefore an $f \in E(\lambda)$ is determined by the function f_U on U given by $f_U(u) = f(uw_0)$. Note that

$$({}^u f)_U(x) = f_U(u^{-1}x), \quad u \in U, \ x \in U.$$

Because U is unipotent, $E(\lambda)^U \neq 0$. If $f \in E(\lambda)^U$, then f_U is constant and it follows that $E(\lambda)^U$ is one-dimensional. Its nonzero elements are the primitive elements. That $E(\lambda)^U$ has weight $w_0(\lambda)$ follows from the equality

$$({}^t f)_U(x) = f_U(t^{-1}xt)w_0(\lambda)(t), \quad t \in T, \ u \in U.$$

To prove the equality, note that

$$({}^t f)_U(x) = ({}^t f)(xw_0) = f(t^{-1}xw_0) = f(t^{-1}xtw_0(w_0t^{-1}w_0)).$$

Now, using (142), we find that

$$({}^t f)_U(x) = f(t^{-1}xtw_0)w_0(\lambda)(t) = f_U(t^{-1}xt)w_0(\chi)(t). \qquad \square$$

LEMMA 22.23. *Let X be a normal integral affine scheme, and let U be a dense open subscheme of X. Let $f \in \mathcal{O}(U)$. If $f^d \in \mathcal{O}(X)$ for some $d \geq 1$, then $f \in \mathcal{O}(X)$.*

PROOF. We have $\mathcal{O}(X) \subset \mathcal{O}(U) \subset k(X)$. Now $f \in k(X)$ and is integral over $\mathcal{O}(X)$, and so it lies in $\mathcal{O}(X)$. $\qquad \square$

We now use the notation of 22.8. In particular, $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ and the fundamental weights are $\lambda_1, \ldots, \lambda_n$.

LEMMA 22.24. *Let λ_i be a fundamental weight of G. For some $d > 0$, $d\lambda_i$ arises as the weight of a primitive element in a representation of G.*

PROOF. Let P be a parabolic subgroup of G containing T and $U_{\pm\alpha_j}$ for every $j \neq i$ but not containing $U_{-\alpha_i}$ (see 21.88). Let (V, r) be a representation of G containing a line kv whose stabilizer in G is P. Each s_{α_j}, $j \neq i$, has a representative in $P(k)$, and so it fixes v. By construction, v is a primitive element; let $\lambda = \sum_{j=1}^n d_j \lambda_j$ be its weight. For $j \neq i$, we have $s_{\alpha_j}(\lambda) = \lambda$, and so $d_j = 0$. We conclude that $\lambda = d_i \lambda_i$. As the action of G on V is nontrivial, $d_i > 0$. $\qquad \square$

LEMMA 22.25. *If G is semisimple and simply connected, then every fundamental weight of G arises as the weight of a primitive element in a representation of G.*

PROOF. Let λ be a fundamental weight of G. For some $d > 0$, there is a simple representation V with highest weight $d\lambda$ (by 22.24). Then V embeds into $\mathcal{O}(G)$, and so $E(w_0(d\lambda)) \neq 0$. Therefore the function $f_{d\lambda} : ub \mapsto (d\lambda)(w_0 b)$ on $Uw_0 B$ extends to G. As $f_{d\lambda}(ub) = (d\lambda)(w_0 b) = f_\lambda^d(ub)$, we see from (22.23) that the function f_λ on the big cell also extends to G. Hence $E(w_0(\lambda)) \neq 0$, and so it contains a primitive element of weight λ (by 22.22). $\qquad \square$

LEMMA 22.26. *Let (V, r) and (V', r') be representations with primitive elements v and v' of weights λ and λ' respectively. Then $v \otimes v'$ is a primitive element of $V \otimes V'$ with weight $\lambda + \lambda'$.*

PROOF. Obvious. □

We now prove Theorem 22.20. Let λ be a dominant character, and write it in the form (139), p. 465. The theorem follows from Lemmas 22.25 and 22.26 when G is the product of a torus with a simply connected semisimple group. Every reductive group is an isogeny quotient of such a group, and so the general case of the theorem follows from 22.12.

PROPOSITION 22.27. *Let $\lambda \in X$.*

 (a) *The space $E(\lambda)$ is nonzero if and only if $w_0(\lambda)$ is dominant.*
 (b) *If $w_0(\lambda)$ is dominant, then $E(\lambda)$ contains a unique simple representation, which has highest weight $w_0(\lambda)$.*
 (c) *The weights of $E(\lambda)$ are $\leq w_0(\lambda)$.*

PROOF. If $E(\lambda) \neq 0$, then it contains a primitive element of weight $w_0(\lambda)$ (see 22.22), and so $w_0(\lambda)$ is dominant (22.17). Conversely, if $w_0(\lambda)$ is dominant, there exists a simple representation with highest weight $w_0(\lambda)$, which embeds into $\mathcal{O}(G)$, thereby showing the $E(\lambda) \neq 0$. The rest of the statement follows easily from the above results. □

COROLLARY 22.28. *If $E(\lambda)$ is nonzero and semisimple, then it is simple with highest weight $w_0(\lambda)$.*

PROOF. This is an obvious consequence of Proposition 22.27. □

When k has characteristic zero, $E(\lambda)$ is automatically semisimple (22.41).

Restatement of the main theorem

22.29. Let G be an algebraic group over k and H an algebraic subgroup of G. For a representation (V, r) of H over k, we define

$$\mathrm{Ind}_H^G(V) = \{ f \in \mathrm{Mor}(G, V_{\mathfrak{a}}) \mid f(gh) = h^{-1} f(g) \text{ all } g \in G(R), h \in H(R) \}.$$

This is a k-vector space on which G acts according to the rule

$$(gf)(x) = f(g^{-1}x), \quad g, x \in G(R), \quad f \in \mathrm{Ind}_H^G(V)_R.$$

In this way we obtain a functor Ind_H^G from representations of H to representations of G. As in the case of finite groups, Frobenius reciprocity holds:

 (a) the map $\varepsilon : \mathrm{Ind}_H^G(V) \to V$, $f \mapsto f(e)$, is a homomorphism of H-modules;
 (b) for every G-module W, the map $\varphi \mapsto \varepsilon \circ \varphi$ is an isomorphism

$$\mathrm{Hom}_G(W, \mathrm{Ind}_H^G(V)) \simeq \mathrm{Hom}_H(W, V).$$

See Jantzen 2003, I.3.

22.30. Let (G, T) be a split reductive group with a Borel subgroup B, and let $\mathbb{G}_a(\lambda)$ be the one-dimensional representation of B on which B acts through $\lambda \in X(T)$. Then $E(\lambda) = \mathrm{Ind}_B^G(\mathbb{G}_a(\lambda))$, and so

$$\mathrm{Hom}_G(V, E(\lambda)) \simeq \mathrm{Hom}_B(V, \mathbb{G}_\alpha(\lambda))$$

for all representations V of G. We often write $\mathrm{Ind}_B^G(\lambda)$ for $\mathrm{Ind}_B^G(\mathbb{G}_a(\lambda))$.

22.31. The *socle* $\mathrm{soc}(V)$ of a representation (V, r) of G is the sum of the simple subrepresentations of V. In other words, it is the largest semisimple subrepresentation of G. With this terminology, the fundamental theorem becomes the following statement:

The B-socle of a simple representation V of G is one-dimensional; if λ is the weight of this socle, then $V = \mathrm{Ind}_B^G(\lambda)$, and so V is uniquely determined by λ; the characters λ of T that arise in this way are exactly those that are dominant.

The highest weight of the contragredient representation

Let (G, B, T) be as before but with G semisimple, and let w_0 be the symmetry with respect to B, so that $w_0(\Phi^+) = -\Phi^+ = \Phi^-$. The automorphism $\iota : \alpha \mapsto -w_0(\alpha)$ of $X(T)$ is called the *opposition involution*. If $-\mathrm{id} \in W$, then ι is the identity map. This is the case for groups of type B_n, C_n, D_n n even, G_2, F_4, E_7, E_8.

The *contragredient* of a representation (V, r) of G is the representation $r^\vee$ on $V^\vee$ given by the rule $r^\vee(g)v^\vee = (r(g)^\vee)^{-1}v^\vee$. On writing V as a sum of eigenspaces for T, we see that the weights of $r^\vee$ are the negatives of the weights of r. If (V, r) is simple, then so is $(V^\vee, r^\vee)$, and it follows that

$$\lambda(r^\vee) = \iota\lambda(r).$$

In particular, if $w_0 = -\mathrm{id}$, then every semisimple representation is self-dual (isomorphic to its contragredient).

Examples

EXAMPLE 22.32. Let $G = \mathrm{GL}_n$ with its standard Borel pair (B, T). Then $X(T)$ has basis $\chi_1, \ldots, \chi_n$, where χ_i sends $\mathrm{diag}(x_1, \ldots, x_n)$ to x_i, and we use this to identify $X(T)$ with $\mathbb{Z}^n$. Then the roots of (G, T) are the vectors $e_i - e_j$, $i \neq j$, the positive roots are the vectors $e_i - e_j$ with $i < j$, and the simple roots are $e_1 - e_2, \ldots, e_{n-1} - e_n$. Moreover, $(e_i - e_{i+1})^\vee = (e_i - e_{i+1})$, and so the dominant weights are the expressions

$$m_1 e_1 + \cdots + m_n e_n, \quad m_i \in \mathbb{Z}, \quad m_1 \geq \cdots \geq m_n.$$

The fundamental weights are $\lambda_1, \ldots, \lambda_{n-1}$ with

$$\lambda_i = e_1 + \cdots + e_i - n^{-1} i \, (e_1 + \cdots + e_n).$$

The obvious representation of GL_n on k^n defines a representation of GL_n on $\bigwedge^i (k^n)$, $1 \le i \le n$. The nonzero weight spaces for T in $\bigwedge^i (k^n)$ are all one-dimensional, and they are permuted by the Weyl group S_n, and so the representation is simple. Its highest weight is $e_1 + \cdots + e_i$.

Note that GL_n has a representation

$$GL_n \xrightarrow{\det} \mathbb{G}_m \xrightarrow{t \mapsto t^m} GL_1 = \mathbb{G}_m$$

for each $m \in \mathbb{Z}$, and that every representation can be tensored with one of these. Thus, we can shift the weights of a simple representation of GL_n by any integer multiple of $e_1 + \cdots + e_n$.

EXAMPLE 22.33. Let $G = SL_2$. With the standard torus T and Borel subgroup $B = T \cdot U^+$, the root datum is isomorphic to $\{\mathbb{Z}, \{\pm 2\}, \mathbb{Z}, \{\pm 1\}\}$, the root lattice is $Q = 2\mathbb{Z}$, the weight lattice is $P = \mathbb{Z}$, and $P^+ = \mathbb{N}$. Therefore, there is (up to isomorphism) exactly one simple representation for each $m \ge 0$. There is a natural action of $SL_2(k)$ on the ring $k[X, Y]$, namely, let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} aX + bY \\ cX + dY \end{pmatrix}.$$

In other words,

$$f^A(X, Y) = f(aX + bY, cX + dY).$$

This is a right action, i.e., $(f^A)^B = f^{AB}$. We turn it into a left action by setting $Af = f^{A^{-1}}$. One can show that the representation of SL_2 on the set of homogeneous polynomials of degree m is simple if $\text{char}(k) = 0$ or $\text{char}(k) = p$ and $m < p$ or $m = p^h - 1$ (Springer 1977, Chapter 3).

EXAMPLE 22.34. Let $G = SL_n$. Let T_1 be the diagonal torus in SL_n. Then

$$X^*(T_1) = X^*(T) / \mathbb{Z}(\chi_1 + \cdots + \chi_n)$$

with $T = \mathbb{D}_n$. The root datum for SL_n is isomorphic to

$$(\mathbb{Z}^n / \mathbb{Z}(e_1 + \cdots + e_n), \{\varepsilon_i - \varepsilon_j \mid i \ne j\}, \ldots)$$

where ε_i is the image of e_i in $\mathbb{Z}^n / \mathbb{Z}(e_1 + \cdots + e_n)$. It follows from the GL_n case that the fundamental weights are $\lambda_1, \ldots, \lambda_{n-1}$ with

$$\lambda_i = \varepsilon_1 + \cdots + \varepsilon_i.$$

Again, the simple representation with highest weight ε_1 is the representation of SL_n on k^n, and the simple representation with highest weight $\varepsilon_1 + \cdots + \varepsilon_i$ is the representation of SL_n on $\bigwedge^i (k^n)$.

EXAMPLE 22.35. Let $G = \mathrm{PGL}_n$. Let T_1 be the diagonal in SL_n. Then

$$X^*(T_1) = X^*(T)/\mathbb{Z}(\chi_1 + \cdots + \chi_n)$$

with $T = \mathbb{D}_n$. The root datum for SL_n is isomorphic to

$$(\mathbb{Z}^n/\mathbb{Z}(e_1 + \cdots + e_n), \{\varepsilon_i - \varepsilon_j \mid i \neq j\}, \ldots)$$

where ε_i is the image of e_i in $\mathbb{Z}^n/\mathbb{Z}(e_1 + \cdots + e_n)$. It follows from the GL_n case that the fundamental weights are $\lambda_1, \ldots, \lambda_{n-1}$ with

$$\lambda_i = \varepsilon_1 + \cdots + \varepsilon_i.$$

Again, the simple representation with highest weight ε_1 is the representation of SL_n on k^n, and the simple representation with highest weight $\varepsilon_1 + \cdots + \varepsilon_i$ is the representation SL_n on $\bigwedge^i(k^n)$.

The fundamental weights for each of the almost-simple split groups are listed in the tables in Bourbaki 1968.

b. Characters and Grothendieck groups

Let A be an abelian category, and let $[A]$ denote the isomorphism class of an object A of A. The ***Grothendieck group*** $K(\mathsf{A})$ of A is the commutative group with one generator for each isomorphism class of objects of A, and one relation $[A] - [B] + [C]$ for each exact sequence

$$0 \to A \to B \to C \to 0.$$

If the objects of A have finite length, then $K(\mathsf{A})$ is generated as a $\mathbb{Z}$-module by the elements $[A]$ with A simple. If A is semisimple (i.e., every object is a finite sum of simple objects), then $K(\mathsf{A})$ is the free abelian group generated by the isomorphism classes of simple objects.

EXAMPLE 22.36. Let T be a split torus over k, and let $X = X^*(T)$. The ***group algebra*** of X is the free $\mathbb{Z}$-module $\mathbb{Z}[X]$ with basis the set of symbols $\{e^\chi \mid \chi \in X\}$ and with $e^\chi \cdot e^{\chi'} = e^{\chi + \chi'}$ (cf. 12.6). The (formal) ***character*** of a representation (V, r) of T is

$$\mathrm{ch}(V) \overset{\text{def}}{=} \sum_{\chi \in X} \dim(V_\chi) \cdot e^\chi.$$

In other words, the coefficient of e^χ is the multiplicity of χ as a weight of V. The character of V depends only on the isomorphism class of (V, r), and ch defines an isomorphism

$$K(\mathrm{Rep}(T)) \to \mathbb{Z}[X].$$

Let (G,T) be a split reductive group over k, and let $X = X^*(T)$. We define the ***character*** $\mathrm{ch}_G(V)$ of a representation (V,r) of G to be its character as a representation of T. Choose a Borel subgroup B of G containing T, and let Φ^+ be the corresponding system of positive roots. As before, we write $\lambda \geq \mu$ if $\lambda - \mu$ is a linear combination of positive roots with coefficients in $\mathbb{N}$. Recall that a $\lambda \in X$ is dominant if $\langle \lambda, \alpha^\vee \rangle \geq 0$ for all $\alpha \in \Phi^+$.

PROPOSITION 22.37. *For every dominant $\lambda \in X$, there exists a unique (up to isomorphism) simple representation $V(\lambda)$ of G such that*

$$\mathrm{ch}_G(V(\lambda)) = e^\lambda + \sum_\mu e^\mu$$

with all $\mu < \lambda$. Every simple representation of G is isomorphic to $V(\lambda)$ for some dominant λ.

PROOF. This is a restatement of the fundamental theorem (22.2). □

In particular, the elements $[V(\lambda)]$ with λ dominant generate $K(\mathsf{Rep}(G))$. The Weyl group W of (G,T) acts on X, and hence on $\mathbb{Z}[X]$.

THEOREM 22.38. *The homomorphism $\mathrm{ch}_G \colon K(\mathsf{Rep}(G)) \to \mathbb{Z}[X]$ is injective with image $\mathbb{Z}[X]^W$ (elements of $\mathbb{Z}[X]$ fixed by the action of the Weyl group).*

PROOF. We prove this by showing that the elements $\mathrm{ch}_G(V(\lambda))$ of $\mathbb{Z}[X]$ with λ dominant form a basis for $\mathbb{Z}[X]^W$.

By definition, the dominant characters are those in a fixed Weyl chamber. As W acts simply transitively on the Weyl chambers, every orbit of W in X contains exactly one dominant character. For each dominant character λ, we let x_λ denote the sum $\sum e^\mu$ as μ runs over the orbit $W \cdot \lambda$. Then the x_λ form a basis for $\mathbb{Z}[X]^W$.

The elements of $\mathrm{ch}_G(V(\lambda))$ are invariant under W because W acts by inner automorphisms of G. Clearly,

$$\mathrm{ch}_G(V(\lambda)) = x_\lambda + \sum_i x_{\lambda_i}$$

where the λ_i are dominant characters with $\lambda_i < \lambda$.

If λ is dominant, then the set $X(\lambda)$ of dominant μ such that $\mu \leq \lambda$ is *finite*. To see this, let $(x|y)$ denote a scalar product on $X_\mathbb{R}$ invariant under W. Then

$$(\mu|\mu) \leq (\mu|\lambda) \leq (\lambda|\lambda)$$

if $\mu \in X(\lambda)$, and so $X(\lambda)$ is a bounded subset of the lattice X. It follows that the partially ordered set of dominant characters satisfies the descending chain condition.

For a set J of dominant characters, we let E_J denote the $\mathbb{Z}$-submodule of $\mathbb{Z}[X]^W$ with basis $\{x_\lambda \mid \lambda \in J\}$. Let $\mathfrak{S}$ denote the collection of sets J with the following two properties:

(a) if $\lambda \in J$ and λ' is a dominant character such that $\lambda' \leq \lambda$, then $\lambda' \in J$;

(b) $\{\mathrm{ch}_G(V(\lambda)) \mid \lambda \in J\}$ is a basis for E_J.

Then $\mathfrak{S}$ is partially ordered by inclusion and it is inductive and nonempty. By Zorn's lemma, it has a maximal element J_0. Suppose that J_0 omits a dominant character, and let λ_0 be minimal among those omitted. Put $J = J_0 \cup \{\lambda_0\}$. Every dominant λ such that $\lambda < \lambda_0$ belongs to J_0, and so J satisfies (a). On the other hand, J also satisfies (b) because

$$x_{\lambda_0} = \mathrm{ch}_G(V(\lambda_0)) - \sum_i x_{\lambda_i}, \quad \lambda_i < \lambda_0.$$

Therefore $J \in \mathfrak{S}$, which contradicts the maximality of J_0. Hence J_0 contains all the dominant characters, and so $\{\mathrm{ch}_G(V(\lambda)) \mid \lambda \text{ dominant}\}$ is a basis for $\mathbb{Z}[X]^W$. $\square$

c. Semisimplicity in characteristic zero

In this section, k is a field of characteristic zero. All Lie algebras and their representations are finite-dimensional.

The Casimir operator

A Lie algebra is said to be **semisimple** if its only solvable ideal is 0. Let $\mathfrak{g}$ be a semisimple Lie algebra over k. From a representation (V, ρ) of $\mathfrak{g}$, we obtain a symmetric bilinear form B_ρ on $\mathfrak{g}$,

$$B_\rho(x, y) = \mathrm{Tr}(\rho(x) \circ \rho(y)), \quad x, y \in \mathfrak{g}.$$

When (V, ρ) is the adjoint representation $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}_\mathfrak{g}$ of $\mathfrak{g}$, this is called the **Killing form** $\kappa_\mathfrak{g}$. When (V, ρ) is faithful, Cartan's criterion (Humphreys 1972, 4.2) shows that the kernel of B_ρ is a solvable ideal, and hence is 0. Thus B_ρ is nondegenerate. Let $\{e_1, \ldots, e_n\}$ be a basis for $\mathfrak{g}$, and let $\{e_1', \ldots, e_n'\}$ be the dual basis with respect to B_ρ. The endomorphism

$$c_V \stackrel{\mathrm{def}}{=} \sum_{i=1}^n \rho(e_i) \cdot \rho(e_i')$$

of V is called the **Casimir operator** of V. It is independent of the choice of the basis, and it is an endomorphism of V as a $\mathfrak{g}$-module (Humphreys 1972, 6.2). The trace of c_V is

$$\sum_{i=1}^n \mathrm{Tr}(\rho(e_i) \cdot \rho(e_i')|V) = \sum_{i=1}^n B_\rho(e_i, e_i') = n = \dim(\mathfrak{g}).$$

When (V, ρ) is not faithful, its kernel is an ideal $\mathfrak{a}$ of $\mathfrak{g}$, and (using the Killing form) we can write $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{b}$ with $\mathfrak{a}$ and $\mathfrak{b}$ semisimple Lie subalgebras of $\mathfrak{g}$. Now (V, ρ) is a faithful representation of $\mathfrak{b}$, and we define the Casimir operator $c_V : V \to V$ by using $\mathfrak{b}$ instead of $\mathfrak{g}$.

Let G be a semisimple algebraic group over k. We sketch a proof that the Lie algebra $\mathfrak{g}$ of G is semisimple. Let $\mathfrak{n}$ be a commutative ideal in $\mathfrak{g}$. In the adjoint action of G on $\mathfrak{g}$, the centralizer H of $\mathfrak{n}$ in G has Lie algebra

$$\mathfrak{h} = \{x \in \mathfrak{g} \mid [x, \mathfrak{n}] = 0\}.$$

Note that $\mathfrak{h}$ contains $\mathfrak{n}$ (because $\mathfrak{n}$ is commutative) and is an ideal in $\mathfrak{g}$: for $y \in \mathfrak{g}$, $x \in \mathfrak{h}$, and $n \in \mathfrak{n}$, $[[y, x], n] = [y, [x, n]] - [x, [y, n]] = 0$. Because $\mathfrak{h}$ is an ideal, H° is normal in G, and so its centre $Z(H^{\circ})$ is normal in G. As G is semisimple, $Z(H^{\circ})$ is finite. Now $\mathrm{Lie}(Z(H^{\circ})) = z(\mathfrak{h})$ (see 10.33), and so $z(\mathfrak{h}) = 0$. But $z(\mathfrak{h}) \supset \mathfrak{n}$, and so $\mathfrak{n} = 0$.

Let (V, r) be a representation of G. Then r defines a representation of $\mathfrak{g}$ on V, and we let c_V denote the corresponding Casimir operator. Because it is a $\mathfrak{g}$-endomorphism, c_V is fixed under the natural action of $\mathfrak{g}$ on $\mathrm{End}(V)$, and so the subspace $\langle c_V \rangle$ is stable under the action of G (see 10.31). As $X(G) = 0$ (21.51), this implies that c_V is fixed by G, and so it is an endomorphism of V as a G-module.

Semisimplicity.

LEMMA 22.39. *Let G be an algebraic group over k. A representation of G is semisimple if it becomes semisimple after an extension of scalars to k^{a}.*

PROOF. This is a special case of (4.19).   □

LEMMA 22.40. *Let G be an algebraic group over k such that $X(G) = 0$. The following conditions on G are equivalent.*

(a) *Every finite-dimensional G-module is semisimple.*

(b) *Every submodule W of codimension 1 in a finite-dimensional G-module V is a direct summand: $V = W \oplus W'$ (direct sum of G-modules).*

(c) *Every simple submodule W of codimension 1 in a finite-dimensional G-module V is a direct summand: $V = W \oplus W'$ (direct sum of G-modules).*

PROOF. The implications (a)$\Rightarrow$(b)$\Rightarrow$(c) are trivial.

(c)$\Rightarrow$(b). We use induction on $\dim(V)$. Let $W \subset V$ have dimension $\dim V - 1$. If W is simple, we know that it has a G-complement, and so we may suppose that there is a nonzero G-submodule W' of W with W/W' simple. Then the G-submodule W/W' of V/W' has a G-complement, which we can write in the form V'/W' with V' a G-submodule of V containing W'; thus

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

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

(b)⇒(a). Let W be a G-submodule of a finite-dimensional G-module V; we have to show that it is a direct summand. The space $\text{Hom}_{k\text{-linear}}(V, W)$ of k-linear maps has a natural G-module structure: $(gf)(v) = g \cdot f(g^{-1}v)$. Let

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

They are both G-submodules of $\text{Hom}_{k\text{-linear}}(V, W)$, and V_1/W_1 has dimension 1. Therefore $V_1 = W_1 \oplus L$ for some one-dimensional G-submodule L of V_1. Let $L = \langle f \rangle$. As $X(G) = 0$, G acts trivially on L, and so f is a G-homomorphism $V \to W$. As $f|W = a\,\text{id}_W$ with $a \neq 0$, the kernel of f is a G-complement to W. □

PROPOSITION 22.41. *Let G be a semisimple algebraic group over k. Every finite-dimensional representation of G is semisimple.*

PROOF. After Lemma 22.39, we may suppose that k is algebraically closed. Let V be a nontrivial representation of G, and let W be a subrepresentation of V. We have to show that W has a G-complement. By Lemma 22.40 we may suppose that W is simple of codimension 1. Consider the Casimir operator $c_V: V \to V$ relative to the representation (V, dr) of $\mathfrak{g}$. Because (V, r) is nontrivial, the image $\bar{\mathfrak{g}}$ of $\mathfrak{g}$ in $\mathfrak{gl}_V$ is nonzero. As $X(G) = 0$ (see 21.50) and V/W is one-dimensional, G acts trivially on V/W. Therefore, $\mathfrak{g}$ acts trivially on V/W, i.e., $\mathfrak{g}V \subset W$. In particular, $c_V V \subset W$. On the other hand, c_V acts on W as a multiplication by some $a \in k$ (Schur's lemma 4.20). Now

$$a \cdot \dim W + 0 = \text{Tr}(c_V|V) = \dim(\bar{\mathfrak{g}}) \neq 0,$$

and so $a \neq 0$. Therefore the kernel of c_V is one-dimensional. It is a G-submodule of V intersecting W trivially, and so it is a G-complement for W. □

THEOREM 22.42. *The following conditions on a connected algebraic group G over k (of characteristic zero) are equivalent:*

(a) *G is reductive;*

(b) *every finite-dimensional representation of G is semisimple;*

(c) *some faithful finite-dimensional representation of G is semisimple.*

PROOF. (a)⇒(b). If G is reductive, then $G = Z \cdot G'$, where Z is the centre of G (a group of multiplicative type) and G' is the derived group of G (a semisimple group). Let $G \to \text{GL}_V$ be a representation of G. When regarded as a representation of Z, V decomposes into a direct sum $V = \bigoplus_i V_i$ of simple representations (12.54). Because Z and G' commute, each subspace V_i is stable under G'. As a G'-module, V_i decomposes into a direct sum $V_i = \bigoplus_j V_{ij}$ with each V_{ij} simple as a G'-module (22.41). Now $V = \bigoplus_{i,j} V_{ij}$ is a decomposition of V into a direct sum of simple G-modules.

(b)$\Rightarrow$(c). Obvious, because every algebraic group has a faithful finite-dimensional representation (4.9).

(c)$\Rightarrow$(a). The condition implies that the unipotent radical of G is trivial (19.17), which implies that G is reductive (because k has characteristic zero). $\quad\square$

COROLLARY 22.43. *Let G be an algebraic group over k. The finite-dimensional representations of G are all semisimple if and only if G° is reductive.*

PROOF. Assume that G° is reductive. Let (V, r) be a representation of G, and let W be G-stable subspace. As G° is reductive, there exists a G°-equivariant map $\pi: V \to W$ such that $\pi|W = \mathrm{id}$. Consider the map

$$q: V_{k^{\mathrm{a}}} \to W_{k^{\mathrm{a}}}, \quad q = \frac{1}{n} \sum_g g\pi g^{-1}$$

where $n = (G(k^{\mathrm{a}}): G^\circ(k^{\mathrm{a}}))$ and g runs over a set of coset representatives for $G^\circ(k^{\mathrm{a}})$ in $G(k^{\mathrm{a}})$. One checks easily that q is independent of the choice of coset representatives, is fixed by all elements of $\mathrm{Gal}(k^{\mathrm{a}}/k)$, restricts to the identity map on $W_{k^{\mathrm{a}}}$, and is $G(k^{\mathrm{a}})$-equivariant. Therefore, q is defined over k, restricts to the identity map on W, and is G-equivariant. This shows that (V, r) is semisimple.

For the converse, assume that $\mathsf{Rep}(G)$ is semisimple. A representation (V, r) of G° embeds in a representation of G, which we may suppose to be simple. Because G° is normal in G, the sum of the simple G°-submodules of (V, r) is stable under G, and hence equals V. Therefore (V, r) is semisimple. $\quad\square$

COROLLARY 22.44. *Let G be an algebraic group over k, and let V and W be finite-dimensional representations of G. If V and W are semisimple, then so is $V \otimes W$.*

PROOF. We may replace G with its image in $\mathrm{GL}_V \times \mathrm{GL}_W$. Then $V \oplus W$ is a faithful semisimple representation of G, and so G is reductive (possibly nonconnected). Therefore every representation of G, e.g., $V \otimes W$, is semisimple. $\quad\square$

Theorem 22.42 has the following remarkable consequence (Chevalley 1955b, p. 88).

COROLLARY 22.45. *Let G be an abstract group, and let (V, r) and (W, s) be representations of G on finite-dimensional vector spaces V and W over a field k of characteristic zero. If V and W are semisimple, then so is $V \otimes W$.*

PROOF. We may replace G with its Zariski closure G' in $\mathrm{GL}_V \times \mathrm{GL}_W$ – as G is dense in G' (as a scheme 1.9), the two have the same invariant subspaces in any representation. Thus we may suppose that G is a group variety over k, and apply the previous corollary. $\quad\square$

Notes

22.46. Let G be a reductive group over a field of characteristic $p \neq 0$. Then G has nonsemisimple representations unless G° is a torus and $(G : G^\circ)$ is prime to p. However, a representation of G is semisimple if its dimension is small relative to p. For example, if G is a connected reductive group over an algebraically closed field, then a representation (V, r) is semisimple if $\dim(V) \leq p$ (Jantzen 1997; see also McNinch 1998).

22.47. Corollary 22.44 also fails in characteristic p, except when the dimensions of the representations are small relative to p. More precisely, let G be an algebraic group (not necessarily smooth) over a field k of characteristic $p \neq 0$, and let $(V_i)_{i \in I}$ be a finite family of representations of G; if the V_i are semisimple and

$$\sum_{i \in I} (\dim(V_i) - 1) < p,$$

then $\bigotimes_{i \in I} V_i$ is semisimple (Serre 1994 for smooth G and Deligne 2014 in general). As a consequence, Corollary 22.45 is true if $\dim V + \dim W < p + 2$.

d. Weyl's character formula

In the first section of this chapter, we classified the simple representations of a split reductive group. In this section, we determine their characters.

Let (G, T) be a split reductive group over a field k, and let B be a Borel subgroup of G containing T. For a character χ of B (or T), we let $L(\chi)$ denote the line bundle on G/B defined in Section 18c.

THEOREM 22.48. *Let χ be a character of T.*
  (a) $H^0(G/B, L(\chi)) \neq 0$ *if and only if $w_0(\chi)$ is dominant.*
  (b) *If $w_0(\chi)$ is dominant, then $H^0(G/B, L(\chi))$ contains a unique simple representation, which has highest weight $w_0(\chi)$.*
  (c) *The weights of T on V are $\leq w_0(\chi)$.*

PROOF. Recall that we obtain $L(\chi) \to G/B$ by passing to the quotient in $G \times \mathbb{A}^1 \to G$ by the action of B, and that $b \in G$ acts on $G \times \mathbb{A}^1$ by $(g, x)b = (gb, \chi(b)^{-1}x)$. A section of $G \times \mathbb{A}^1 \to G$ is a map $g \mapsto (g, f(g))$ with $f \in \mathcal{O}(G)$. This section sends gb to $(gb, f(gb))$, and so it passes to the quotient if and only if

$$f(gb) = f(g)\chi(b^{-1}), \quad g \in G(R), \, b \in B(R).$$

This is the condition that f lie in $E(\chi)$, and so $H^0(G/B, L(\chi)) \simeq E(\chi)$. The statement now follows from Proposition 22.27. □

When k has characteristic zero, $H^0(G/B, L(\chi))$ itself is simple.

REMARK 22.49. In Section a, we used an argument from Steinberg 1967 to show that $E(\chi) \neq 0$ when χ is dominant. Iversen gives a more geometric argument. He constructs an explicit basis $(D_\alpha)_{\alpha \in \Delta}$ for the divisor classes on G/B, and shows that $L(\chi)$ is the line bundle attached to the divisor $\sum_{\alpha \in \Delta} \langle w_0(\chi), \alpha^\vee \rangle D_\alpha$ (Iversen 1976, Theorem 5.3). From this it follows that $H^0(G/B, L(\chi)) \neq 0$ if and only if $\langle w_0(\chi), \alpha^\vee \rangle \geq 0$ for all $\alpha \in \Delta$. (Iversen's definition the system of positive roots attached to B is opposite to our definition.)

We now assume that $\mathrm{Pic}(G) = 0$. When G is semisimple, this condition means that G is simply connected (18.19, 18.23).

Let $X = X(T)$ and let $W = W(G, T)$. We let W act on $\mathbb{Z}[X]$ on the left (see 22.36 for $\mathbb{Z}[X]$). For $w \in W$, we let $\det(w) = \det(w|X)$, and we define the antisymmetry operator

$$J:\mathbb{Z}[X] \to \mathbb{Z}[X], \quad J(e^\chi) = \sum_{w \in W} \det(w)e^{w(\chi)}.$$

The half sum of the positive roots,

$$\rho = \frac{1}{2}\sum\{\alpha \mid \alpha \in \Phi^+\},$$

lies in X – the proof of this uses that $\mathrm{Pic}(G) = 0$ (Iversen 1976, 9.2).

THEOREM 22.50. *For all* $\chi \in X(T)$,

$$\sum_i (-1)^i \mathrm{ch}_G H^i(G/B, L(\chi)) = J(e^{\chi+\rho})/J(e^\rho).$$

PROOF. This follows from the general fixed point theorem in Nielsen 1974. See Iversen 1976, 9.4.   □

THEOREM 22.51 (KEMPF'S VANISHING THEOREM). *If* χ *is dominant, then the group* $H^i(G/B, L(\chi)) = 0$ *for* $i > 0$.

PROOF. In characteristic 0, the statement follows from the Kodaira vanishing theorem. In characteristic p, it was proved in Kempf 1976. For a proof valid in all characteristics (due to Anderson and Haboush independently), see Jantzen 2003, II, 4.5.   □

The statement fails if χ is not dominant.

THEOREM 22.52 (WEYL CHARACTER FORMULA). *For a simple representation* V *of* G *with highest weight* χ,

$$\mathrm{ch}_G(V) = \frac{J(e^{\chi+\rho})}{J(e^\rho)} \stackrel{\mathrm{def}}{=} \frac{\sum_{w \in W} \det(w)e^{w(\chi+\rho)}}{\sum_{w \in W} \det(w)e^{w(\rho)}}.$$

PROOF. In characteristic zero, the representation V is isomorphic to the group $H^0(G/B, L(\chi))$ for some dominant χ, and so the statement follows from Theorems 22.50 and 22.51. For the general case, see Iversen 1976, 9.5, or Jantzen 2003, 5.10.   □

e.   **Relation to the representations of** Lie(G)

Let G be a semisimple algebraic group. A representation (W, r) of G is said to be ***infinitesimally simple*** if (W, dr) is simple. An infinitesimally simple representation is simple. The converse is true in characteristic 0, but not otherwise.

Characteristic 0

THEOREM 22.53. *Let G be a semisimple algebraic group over a field k of characteristic zero. Then $\mathfrak{g}$ is a semisimple Lie algebra, and the natural functor* Rep$(G) \to$ Rep$(\mathfrak{g})$ *is fully faithful; it is essentially surjective if G is simply connected.*

PROOF. We showed that $\mathfrak{g}$ is semisimple in Section c. According to Theorem 23.70 below, there is a semisimple algebraic group G' such that Rep$(G') \simeq$ Rep$(\mathfrak{g})$; moreover G' is the universal covering group of G. Now Rep$(G) \to$ Rep(G') is fully faithful and Rep$(G') \to$ Rep$(\mathfrak{g})$ is an equivalence of categories.   □

When G is split with diagram (V, Φ, X), a simple representation in Rep$(\mathfrak{g})$ lies in the essential image of the functor if and only if its highest weight lies in X.

Characteristic p

In this subsection, we list some of the known results for a split semisimple algebraic group (G, T) over a field k of characteristic $p \neq 0$.

Let G_F denote the kernel of the Frobenius homomorphism $F_G : G \to G^{(p)}$. Then Lie$(G) =$ Lie(G_F) and so the representations of Lie(G) depend only on the finite group scheme G_F.

22.54. *Suppose that G is simply connected. A simple representation of (V, r) of G is infinitesimally simple if and only if its highest weight $\lambda(r)$ is of the form*

$$\lambda(r) = \sum_{\alpha \in \Delta} m_\alpha(r)\alpha \quad \text{with } 0 \leq m_\alpha(r) < p.$$

Therefore, the infinitesimally simple representations fall into exactly $p^{\text{rank}(G)}$ isomorphism classes.

For a representation $r : G \to \mathrm{GL}_V$ of G, we write $r^{[p^l]}$ for the composite of r with F_G^l. For example, for a representation $r : G \to \mathrm{GL}_n$, the representation $r^{[p^l]}$ is

$$g \mapsto (r(g)_{i,j}^{p^l})_{1 \leq i, j \leq n}.$$

If (V, r) is simple with highest weight $\lambda(r)$, then $(V, r^{[p^l]})$ is simple with highest weight $p^l \cdot \lambda(r)$.

22.55. *Suppose that G is simply connected, and let $(V_0, r_0), \ldots, (V_m, r_m)$ be infinitesimally simple representations of G. Then*

$$r_0 \otimes r_1^{[p]} \otimes \cdots \otimes r_m^{[p^m]}$$

is a simple representation of G, and every nontrivial simple representation can be written uniquely in this way with $r_m \neq 1$.

Note that $r_0 \otimes r_1^{[p]} \otimes \cdots \otimes r_m^{[p^m]}$ has highest weight $\lambda = \lambda(r_0) + p\lambda(r_1) + \cdots + p^m \lambda(r_m)$.

22.56. *Suppose that G is simply connected and that k is finite, say, $k = \mathbb{F}_{p^m}$. For every family $(V_i, r_i)_{0 \leq i \leq m-1}$ of simple representations of G, the map*

$$g \mapsto r_0(g) \otimes r_1^{[p]}(g) \otimes \cdots \otimes r_{m-1}^{[p^{m-1}]}(g)$$

is a simple representation of the abstract group $G(k)$, and every simple representation of $G(k)$ is of this form; moreover, the (V_i, r_i) are unique (up to isomorphism).

Thus, the representations of $G(k)$ fall into exactly $(p^m)^{\mathrm{rank}(G)}$ isomorphism classes.

These results of Curtis and Steinberg make it possible to deduce the simple representations of the finite Chevalley groups from knowing the representations of the semisimple Lie algebras over $\mathbb{C}$. See Borel 1975 and the references therein, and Jantzen 2003, II.3.

Exercises

EXERCISE 22-1. Let λ be a dominant character of a split reductive group (G, T) relative to a Borel subgroup B, and let $E(\lambda) = \mathrm{Ind}_B^G(\mathbb{G}_a(\lambda))$. Show that $\mathrm{End}(E(\lambda)) \simeq k$. Deduce that $\mathrm{End}(V(\lambda)) \simeq k$ if $V(\lambda)$ is a simple representation with highest weight λ.

EXERCISE 22-2. Let (G, T) be a reductive group over an algebraically closed field k of characteristic zero. Show that the following are equivalent:
  (a) G admits a faithful simple representation;
  (b) either the centre of G is a one-dimensional torus or it is finite and cyclic (as an abstract group);
  (c) the character group $X(T)/\mathbb{Z}\Phi$ of the centre of G is cyclic.
(See https://mathoverflow.net/, question 29813; spin groups in even dimensions have centre a non-cyclic group of order 4 and so have no faithful simple representations.)

EXERCISE 22-3. Let G be a reductive group over a field k of characteristic zero, and let V be a faithful self-dual representation of G. Show that there exist tensors $t_1, \ldots, t_s$, $t_i \in (V^{\otimes r_i})^\vee$, such that G is the algebraic subgroup of GL_V fixing the t_i.

The Isogeny and Existence Theorems

These theorems show that the split reductive groups and their isogenies over k are classified by their (combinatorial) root data.

a. Isogenies of groups and of root data

We first define the notion of an isogeny of root data. An isogeny of split reductive groups defines an isogeny of root data, and the isogeny theorem says that every isogeny of root data arises in this way. Throughout this section, p denotes the characteristic exponent of k (so p is either 1 or a prime number).

Definition of an isogeny of root data

Recall that a root datum is a triple $(X, \Phi, \Phi^\vee)$ with X a free $\mathbb{Z}$-module of finite rank and Φ and $\Phi^\vee$ finite subsets of X and $X^\vee$ such that there exists a bijection $\alpha \mapsto \alpha^\vee \colon \Phi \to \Phi^\vee$ satisfying the conditions (rd1, rd2, rd3) of C.28. Here $X^\vee$ is the $\mathbb{Z}$-linear dual of X. The map $\alpha \mapsto \alpha^\vee$ is uniquely determined by the rest of the data. We call $\alpha^\vee$ the coroot of the root α. The triple $(X^\vee, \Phi^\vee, \Phi)$ is also a root datum (C.48). We require root data to be reduced, i.e., $\mathbb{Q}\alpha \cap \Phi = \{\pm\alpha\}$ for all $\alpha \in \Phi$.

DEFINITION 23.1. Let $\mathcal{R} = (X, \Phi, \Phi^\vee)$ and $\mathcal{R}' = (X', \Phi', \Phi'^\vee)$ be root data. An injective homomorphism $f \colon X' \to X$ with finite cokernel is an ***isogeny of root data*** $\mathcal{R}' \to \mathcal{R}$ if there exists a one-to-one correspondence $\alpha \leftrightarrow \alpha' \colon \Phi \leftrightarrow \Phi'$ and a map $q \colon \Phi \to p^{\mathbb{N}}$ satisfying

$$f(\alpha') = q(\alpha)\alpha \quad \text{and} \quad f^\vee(\alpha^\vee) = q(\alpha)\alpha'^\vee \tag{143}$$

for all $\alpha \in \Phi$.

Note that the following conditions on a homomorphism $f: X' \to X$ are equivalent: (a) f is injective with finite cokernel; (b) both f and $f^\vee$ are injective; (c) $f_{\mathbb{Q}}$ is an isomorphism.

If $f: X' \to X$ is an isogeny, then $f(\Phi') \subset p^{\mathbb{N}}\Phi$ and $f^\vee(\Phi^\vee) \subset p^{\mathbb{N}}\Phi'^\vee$. Because we require root data to be reduced, given $\alpha \in \Phi$, there exists at most one $\alpha' \in \Phi'$ such that $f(\alpha')$ is a positive multiple of α. It follows that the correspondence $\alpha \leftrightarrow \alpha'$ and the map q are uniquely determined by f. As $(-\alpha)'$ and $-\alpha'$ are both elements of Φ' such that $f((-\alpha)')$ and $f(-\alpha')$ are positive multiples of $-\alpha$, we find that $(-\alpha)' = -\alpha'$ and $q(-\alpha) = q(\alpha)$.

DEFINITION 23.2. An isogeny f of root data is **central** if $q(\alpha) = 1$ for all $\alpha \in \Phi$; it is an **isomorphism** if it is central and f is an isomorphism of $\mathbb{Z}$-modules.

Thus an isomorphism $f: X' \to X$ of $\mathbb{Z}$-modules is an isomorphism of root data if and only if there exists a one-to-one correspondence $\alpha \leftrightarrow \alpha': \Phi \leftrightarrow \Phi'$ such that $f(\alpha') = \alpha$ and $f^\vee(\alpha^\vee) = \alpha'^\vee$ for all $\alpha \in \Phi$.

EXAMPLE 23.3. Let $(X, \Phi, \Phi^\vee)$ be a root datum, and let q be a power of p. The map $x \mapsto qx: X \to X$ is an isogeny $(X, \Phi, \Phi^\vee) \to (X, \Phi, \Phi^\vee)$, called the **Frobenius isogeny** (the correspondence $\alpha \leftrightarrow \alpha'$ is the identity map, and $q(\alpha) = q$ for all α).

PROPOSITION 23.4. Let $f: (X', \Phi', \Phi'^\vee) \to (X, \Phi, \Phi^\vee)$ be an isogeny of root data, and let Φ^+ be a system of positive roots for Φ with base Δ. Then $\Phi'^+ \overset{\text{def}}{=} \{\alpha' \mid \alpha \in \Phi^+\}$ is a system of positive roots for Φ' with base $\Delta' \overset{\text{def}}{=} \{\alpha' \mid \alpha \in \Delta\}$.

PROOF. Using that f is an isogeny of root data, we find that each element of Φ' has a unique expression as a $\mathbb{Q}$-linear combination of elements of Δ' in which the coefficients all have the same sign. Clearly those elements of Φ' for which the signs are positive form a system of positive roots Φ'^+ for Φ'. From this and the fact that Φ' is reduced, it follows that a decomposition

$$\alpha' = \beta' + \gamma', \quad \alpha' \in \Delta', \quad \beta', \gamma' \in \Phi'^+$$

is impossible, and so Δ' is a base for Φ' (see C.21). □

NOTES. The definition of an isogeny of root data in (23.1) is that of Steinberg 1999. It essentially agrees with the definition of a p-morphism of root data in Springer 1998, p. 172. The definition of a p-morphism of root data in SGA 3, XXI, 6.8.1, p. 100, differs in that it does not require $f_{\mathbb{Q}}$ to be an isomorphism.

The isogeny of root data defined by an isogeny of groups

Let (G, T) be a split reductive group, and let $\Phi \subset X(T)$ be its set of roots. Let U_α denote the root group attached to a root $\alpha \in \Phi$. Recall that U_α is the unique algebraic subgroup of G isomorphic to $\mathbb{G}_a$, normalized by T, and such that T

acts on it through the character α (see 21.19). This last condition means that, for every isomorphism $u_\alpha \colon \mathbb{G}_a \to U_a$,

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \tag{144}$$

for all $t \in T(R)$, $a \in \mathbb{G}_a(R)$, R a k-algebra.

An **isogeny of split reductive groups** $(G, T) \to (G', T')$ is an isogeny $\varphi \colon G \to G'$ such that $\varphi(T) \subset T'$. We write φ_T for $\varphi | T \colon T \to T'$. In the following, u_α always denotes an isomorphism $\mathbb{G}_a \to U_\alpha$.

PROPOSITION 23.5. *If $\varphi \colon (G, T) \to (G', T')$ is an isogeny of split reductive groups, then $f \overset{\text{def}}{=} X(\varphi_T) \colon X(T') \to X(T)$ is an isogeny of root data. Roots $\alpha \in \Phi$ and $\alpha' \in \Phi'$ correspond if and only if $\varphi(U_\alpha) = U_{\alpha'}$, in which case*

$$\varphi(u_\alpha(a)) = u_{\alpha'}(c_\alpha a^{q(\alpha)}), \quad \text{all } a \in \mathbb{G}_a(k), \tag{145}$$

where $c_\alpha \in k^\times$ and $q(\alpha)$ is such that $f(\alpha') = q(\alpha)\alpha$. The isogeny φ is central (resp. an isomorphism) if and only if f is central (resp. an isomorphism).

PROOF. The restriction of φ to T is an isogeny $T \to T'$, and so $f \colon X(T') \to X(T)$ is injective with finite cokernel. By definition, $f(\chi') = \chi' \circ \varphi | T$ for $\chi' \in X(T')$. The image $\varphi(U_\alpha)$ of U_α in G' is isomorphic to $\mathbb{G}_a$ (see 14.58) and normalized by T', and so it equals the root group $U_{\alpha'}$ with α' the character of T' on $\mathrm{Lie}(\varphi(U_\alpha))$. Therefore

$$\varphi(u_\alpha(a)) = u_{\alpha'}(g(a)), \quad a \in \mathbb{G}_a(R), \ R \text{ a } k\text{-algebra}, \tag{146}$$

with $g(a)$ a polynomial $\sum c_j a^{p^j}$ in a with coefficients in k (14.40). On applying φ to (144), we find that

$$\varphi(t) \cdot \varphi(u_\alpha(a)) \cdot \varphi(t)^{-1} = \varphi(u_\alpha(\alpha(t)a)).$$

Using (146), we can rewrite this as

$$\varphi(t) \cdot u_{\alpha'}(g(a)) \cdot \varphi(t)^{-1} = u_{\alpha'}(g(\alpha(t)a)),$$

and using (144) in the group G', we find that

$$u_{\alpha'}(\alpha'(\varphi(t))g(a)) = u_{\alpha'}(g(\alpha(t)a)).$$

As $u_{\alpha'}$ is injective and $\alpha' \circ \varphi = f(\alpha')$, this implies that

$$f(\alpha')(t) \cdot g(a) = g(\alpha(t) \cdot a), \quad \text{all } a \in \mathbb{G}_a(R). \tag{147}$$

It follows that $g(T)$ is a monomial, say, $g(T) = cT^{q(\alpha)}$ with $c \in k^\times$ and $q(\alpha)$ a constant in $p^{\mathbb{N}}$. Now (146) and (147) become

$$\varphi(u_\alpha(a)) = u_{\alpha'}(ca^{q(\alpha)})$$

$$\text{and} \quad f(\alpha')(t) = \alpha(t)^{q(\alpha)}, \quad \text{i.e.,} \quad f(\alpha') = q(\alpha)\alpha.$$

Let G_α be the subgroup of G generated by $U_{\pm\alpha}$ and T. There exists an element $n_\alpha \in G_\alpha(k)$ normalizing T and acting nontrivially on T (see 21.11d). Then $\varphi(n_\alpha)$ normalizes T' in $G_{\alpha'}$ and acts nontrivially on it, and so we can take $n_{\alpha'} = \varphi(n_\alpha)$. Now

$$f \circ (1 - n_{\alpha'}) = (1 - n_\alpha) \circ f.$$

On applying this to $\chi' \in X(T')$ and using that $n_{\alpha'} \chi' = \chi' - \langle \chi', \alpha'^\vee \rangle \alpha'$, we obtain the first equality below:

$$\langle \chi', \alpha'^\vee \rangle f(\alpha') = \langle f(\chi'), \alpha^\vee \rangle \alpha = \langle \chi', f^\vee(\alpha^\vee) \rangle \alpha.$$

As this holds for all $\chi' \in X(T')$, it follows from $f(\alpha') = q(\alpha)\alpha$ that $f^\vee(\alpha^\vee) = q(\alpha)\alpha'^\vee$. Thus f is an isogeny of root data.

The isogeny φ is central if and only if its kernel is contained in T, which is true if and only if the restriction of φ to $U_\alpha \to U_{\alpha'}$ is injective, hence an isomorphism, for all α (see 21.84). In turn, this is true if and only if $q(\alpha) = 1$ for all α.

Let φ be a central isogeny. As its kernel is contained in T, it is an isomorphism if and only if φ_T is an isomorphism, which is true if and only if $f = X(\varphi_T)$ is an isomorphism.   □

It is not quite true that an isogeny $\varphi : (G, T) \to (G', T')$ is an isomorphism if φ_T is an isomorphism (it need not be central; 23.30).

EXAMPLE 23.6. We say that an isogeny $\varphi : G \to G'$ is a **Frobenius isogeny** if its kernel is equal to the kernel of the Frobenius homomorphism $F_G : G \to G^{(q)}$ for some q (see 2.28). An isogeny φ of split reductive groups is a Frobenius isogeny if and only if $X(\varphi)$ is a Frobenius isogeny of root data.

Uniqueness

The isogeny $f = X(\varphi_T)$ of root data in Proposition 23.5 does not determine φ uniquely because the inner automorphism of (G', T') defined by an element of $(T'/Z(G'))(k)$ does not change f. However, this is the only indeterminacy.

PROPOSITION 23.7. *Let* $\varphi_1, \varphi_2 : (G, T) \rightrightarrows (G', T')$ *be isogenies of split reductive groups. If they induce the same map on root data, then* $\varphi_2 = \mathrm{inn}(t) \circ \varphi_1$ *for a unique* $t \in (T'/Z(G'))(k)$.

PROOF. Let $f_1 = X(\varphi_1|T)$. Let Δ be a base for Φ, and let $\alpha \in \Delta$. The equality $f_1(\alpha') = q(\alpha)\alpha$ implies that $\varphi_1(u_\alpha(a)) = u_{\alpha'}(c_\alpha a^{q(\alpha)})$ for some $c_\alpha \in k$, and similarly $\varphi_2(u_\alpha(a)) = u_{\alpha'}(d_\alpha a^{q(\alpha)})$ for some $d_\alpha \in k$. As Δ' is a basis for the $\mathbb{Z}$-module $X(T'/Z')$ (see 21.9), there exists a $t \in T'(k)$ such that $\alpha'(t) = d_\alpha c_\alpha^{-1}$ for all $\alpha \in \Delta$. Let $\varphi = \mathrm{inn}(t) \circ \varphi_1$, then

$$\varphi(u_\alpha(a)) = \mathrm{inn}(t)(u_{\alpha'}(c_\alpha a^{q(\alpha)})) \overset{21.22}{=} u_{\alpha'}(\alpha'(t)c_\alpha a^{q(\alpha)}) = \varphi_2(u_\alpha(a)).$$

Therefore, φ_2 and φ agree on U_α for $\alpha \in \Delta$ as well as on T, and so they agree on G (see 21.63); hence $\varphi_2 = \varphi_1 \circ \mathrm{inn}(t)$.   □

PROPOSITION 23.8. *Let* $\varphi_1, \varphi_2 \colon (G, T) \rightrightarrows (G', T')$ *be isogenies of split reductive groups. If one of G or G' is semisimple and φ_1 and φ_2 induce the same correspondence $\alpha \leftrightarrow \alpha'$ on the roots, then $\varphi_1 | T = \varphi_2 | T$.*

PROOF. Let $f_1 = X(\varphi_1 | T)$ and $f_2 = X(\varphi_2 | T)$. We are given that for some one-to-one correspondence $\alpha \leftrightarrow \alpha' \colon \Phi \leftrightarrow \Phi'$,

$$f_1(\alpha') = q_1(\alpha)\alpha \quad \text{and} \quad f_2(\alpha') = q_2(\alpha)\alpha.$$

Because Φ is reduced, $q_1(\alpha) = q_2(\alpha)$. Therefore f_1 and f_2 agree on $\mathbb{Z}\Phi'$. If G' is semisimple, then $\mathbb{Z}\Phi'$ has finite index in $X(T')$, and so f_1 and f_2 agree on $X(T')$. This implies that φ_1 and φ_2 agree on T (see 12.9a). The proof when G is semisimple is similar. $\qquad\square$

Statement of the isogeny theorem

THEOREM 23.9 (ISOGENY THEOREM). *Let (G, T) and (G', T') be split reductive algebraic groups over k. An isogeny $\varphi \colon T \to T'$ of tori extends to an isogeny $G \to G'$ if and only if the map $X(\varphi) \colon X(T') \to X(T)$ is an isogeny of root data.*

In particular, every isogeny of root data $\mathcal{R}(G', T') \to \mathcal{R}(G, T)$ arises from an isogeny $(G, T) \to (G', T')$. The necessity was proved in Proposition 23.5; the sufficiency is proved in the next section.

b. Proof of the isogeny theorem

Preliminaries

The next lemma shows that it suffices to prove that every isogeny of root data arises from a *homomorphism* of algebraic groups.

LEMMA 23.10. *Let $\varphi \colon (G, T) \to (G', T')$ be a homomorphism of split reductive groups over k. If $X(\varphi_T) \colon X(T') \to X(T)$ is an isogeny of root data, then φ is an isogeny.*

PROOF. Let $f = X(\varphi_T)$. We are given that there exist a one-to-one correspondence $\alpha \leftrightarrow \alpha' \colon \Phi \leftrightarrow \Phi'$ and a map $q \colon \Phi \to p^{\mathbb{N}}$ such that

$$f(\alpha') = q(\alpha)\alpha \quad \text{and} \quad f^{\vee}(\alpha'^{\vee}) = q(\alpha)\alpha'^{\vee} \tag{148}$$

for all $\alpha \in \Phi$. As in the proof of Proposition 23.5, φ maps each U_α onto $U_{\alpha'}$. It follows that φ is surjective because G' is generated by its subgroups $U_{\alpha'}$ and T' (see 21.11f). As

$$\dim G \overset{21.13}{=} \dim T + |\Phi| = \dim T' + |\Phi'| \overset{21.13}{=} \dim G',$$

this implies that φ is an isogeny. $\qquad\square$

The next two lemmas, both due to Chevalley, prove special cases of the isogeny theorem.

LEMMA 23.11. Let $\varphi_1:(G,T) \to (G_1,T_1)$ and $\varphi_2:(G,T) \to (G_2,T_2)$ be isogenies of split reductive groups, and let $\varphi_T:T_1 \to T_2$ be a homomorphism such that $\varphi_T \circ \varphi_1|T = \varphi_2|T$. If $X(\varphi_T)$ is an isogeny of root data, then φ_T extends to a homomorphism $\varphi:G_1 \to G_2$ such that $\varphi \circ \varphi_1 = \varphi_2$:

$$
\begin{array}{ccc}
(G,T) & \xrightarrow{\ \varphi_1\ } & (G_1,T_1) \\
\ \downarrow{\scriptstyle \varphi_2} & \nearrow \varphi & \\
(G_2,T_2). & &
\end{array}
$$

PROOF. The homomorphism φ_2 factors through φ_1 (i.e., φ exists) if and only if $\mathrm{Ker}(\varphi_1) \subset \mathrm{Ker}(\varphi_2)$. If φ_1 and φ_2 are central isogenies (for example, if k has characteristic zero), then the kernels are contained in T (because $T = C_G(T)$), and so this follows from the fact that $\varphi_1|T$ factors through $\varphi_2|T$.

Clearly the statement $\mathrm{Ker}(\varphi_1) \subset \mathrm{Ker}(\varphi_2)$ is true if and only if it becomes true after an extension of the base field, and so we may suppose that k is algebraically closed. The kernels of $\varphi_1(k)$ and $\varphi_2(k)$ are central in $G(k)$, and so $\varphi_1(k):G(k) \to G_1(k)$ factors through $\varphi_2(k)$, say, $g \circ \varphi_1(k) = \varphi_2(k)$. It remains to show that $g:G_1(k) \to G_2(k)$ is a regular map.

Let α, α_1, and α_2 be roots of (G,T), (G,T_1), and (G,T_2) related in pairs by the maps $f_1 = X(\varphi_1|T)$, $f_2 = X(\varphi_2|T)$, and $f = X(\varphi)$. Then $\varphi_1(U_\alpha(k)) = U_{\alpha_1}(k)$ and $\varphi_2(U_\alpha(k)) = U_{\alpha_2}(k)$, so that $g(U_{\alpha_1}(k)) = U_{\alpha_2}$. Moreover, $g:U_{\alpha_1} \to U_{\alpha_2}$ is a regular map because, for some $c \in k$, it has the form

$$g(u_{\alpha_1}(a)) = u_{\alpha_2}(ca^{q(\alpha_1)}), \quad a \in U_{\alpha_1}(k)$$

(see (145), p. 485). It follows that g is a regular map on the big cell of G_1 (see 21.84), and hence on the union of its translates, which is G_1 itself. Thus g is an isogeny of algebraic groups.   □

LEMMA 23.12. Let $\varphi_1:(G_1,T_1) \to (G,T)$ and $\varphi_2:(G_2,T_2) \to (G,T)$ be isogenies of split reductive groups, and let $\varphi_T:T_1 \to T_2$ be a homomorphism such that $\varphi_2|T \circ \varphi_T = \varphi_1|T$. If $X(\varphi_T)$ is an isogeny of root data, then φ_T extends to a homomorphism $\varphi:G_1 \to G_2$ such that $\varphi_2 \circ \varphi = \varphi_1$.

PROOF. Let G_3 be the identity component of $G_1 \times_G G_2$, and let p_1 and p_2 be the projections of G_3 onto G_1 and G_2. It suffices to show that p_2 factors through p_1, say $\varphi \circ p_1 = p_2$, because then

$$\varphi_2 \circ \varphi \circ p_1 = \varphi_2 \circ p_2 = \varphi_1 \circ p_1,$$

and the surjectivity of p_1 implies that $\varphi_2 \circ \varphi = \varphi_1$. As in the last proof, it suffices to show that p_2 factors through p_1 after an extension of the base field, and so we may suppose that k is algebraically closed.

Replace G_3 with $(G_3)_{\mathrm{red}}$. The homomorphisms p_1 and p_2 are isogenies and so G_3 is reductive. Let T_3 be the inverse image torus of T in G_3 (under $\varphi_2 \circ p_2$ or $\varphi_1 \circ p_1$):

$$
\begin{array}{ccc}
(G_3, T_3) & \xrightarrow{\ p_2\ } & (G_2, T_2) \\
\downarrow{\scriptstyle p_1} & \overset{\varphi}{\dashrightarrow} & \downarrow{\scriptstyle \varphi_2} \\
(G_1, T_1) & \xrightarrow{\ \varphi_1\ } & (G, T).
\end{array}
$$

Then $\varphi_T \circ p_1 | T_3 = p_2 | T_3$, and Lemma 23.11 applied to p_1 and p_2 shows that φ_T extends to a homomorphism $\varphi : G_1 \to G_2$ such that $\varphi \circ p_1 = p_2$. $\qquad\square$

LEMMA 23.13. *It suffices to prove the isogeny theorem for split semisimple groups.*

PROOF. Assume the isogeny theorem for semisimple groups, and let (G, T) and (G', T') be split reductive groups. Then $G = T_0 \cdot S$ with $S = G^{\mathrm{der}}$ and $T_0 = R(G)$, and $T = T_0 \cdot T_S$ with T_S a maximal split torus of S (see 17.86). Let $X_S = X(T_S)$ and $X_0 = X(T_0)$. Similarly, let $G' = T'_0 \cdot S'$ etc. Let $\varphi_T : T \to T'$ be an isogeny such that $f = X(\varphi_T)$ is an isogeny of root data.

The roots α' of G' generate $(X_{S'})_{\mathbb{Q}}$, and so the equalities $f(\alpha') = q(\alpha)\alpha$ imply that $f(X_{S'}) \subset X_S$. The lattice X_0 (resp. X'_0) is the annihilator in X (resp. X') of $X_S^{\vee}$ (resp. $X_{S'}^{\vee}$), and so the equalities $f^{\vee}(\alpha^{\vee}) = q(\alpha)\alpha'^{\vee}$ imply that f maps X'_0 into X_0. Now $f | X'_0$ and $f | X_{S'}$ correspond to homomorphisms $\varphi_0 : T_0 \to T'_0$ and $\varphi_{T_S} : T_S \to T'_S$. Because $f | X_{S'}$ is an isogeny of root data, φ_{T_S} extends to a homomorphism $\varphi_S : S \to S'$. The homomorphisms φ_0 and φ_S agree on $T_0 \cap S$, and so $\varphi_0 \times \varphi_S$ induces an isogeny $G \to G'$ extending φ_T:

$$
\begin{array}{ccccccccc}
e & \longrightarrow & T_0 \cap S & \longrightarrow & T_0 \times S & \longrightarrow & G & \longrightarrow & e \\
& & \downarrow & & \downarrow{\scriptstyle \varphi_0 \times \varphi_S} & & \downarrow{\scriptstyle \varphi} & & \\
e & \longrightarrow & T'_0 \cap S' & \longrightarrow & T'_0 \times S' & \longrightarrow & G' & \longrightarrow & e.
\end{array}
$$

$\square$

The isogeny theorem for groups of semisimple rank at most 1

If (G, T) and (G', T') have semisimple rank 0, then $G = T$ and $G' = T'$, and so there is nothing to prove.

PROPOSITION 23.14. *The isogeny theorem holds for split reductive groups of semisimple rank 1.*

PROOF. Let (G, T) and (G', T') be split reductive groups of semisimple rank 1, and let $f : X(T') \to X(T)$ be an isogeny of root data. According to (the proof of) Lemma 23.13, we may suppose that G and G' are semisimple.

Assume first that $G' = \mathrm{PGL}_2$. According to Theorem 20.22, there exists a central isogeny $\varphi_1 : G \to G'$; let $f_1 = X(\varphi_1)$. Then $f(\alpha') = q(\alpha)\alpha = q(\alpha)f_1(\alpha')$

for all roots α of G, and so the composite of φ_1 with the $q(\alpha)$th power Frobenius homomorphism of G' (see 23.6) is an isogeny realizing f.

We now prove the general case. Let $\varphi_1 : (G', T') \to (\mathrm{PGL}_2, T_2)$ be a central isogeny, and let $f_1 = X(\varphi_1)$. By the previous case, there exists an isogeny $\varphi' : (G, T) \to (\mathrm{PGL}_2, T_2)$ with $X(\varphi') = f \circ f_1$. Now (23.12) applied to the diagram

$$
\begin{array}{ccc}
 & & (G', T') \\
 & \nearrow{\scriptstyle\varphi} & \downarrow{\scriptstyle\varphi_1} \\
(G, T) & \xrightarrow{\varphi'} & (\mathrm{PGL}_2, T_2)
\end{array}
$$

yields an isogeny $\varphi : G \to G'$ with $X(\varphi) = f$.   □

REMARK 23.15. Since we know that the only split semisimple groups of rank 1 are SL_2 and PGL_2 (see 20.33), we could have proved Proposition 20.32 by using a case-by-case argument. Alternatively, the proof of Proposition 23.14 only requires Theorem 20.22, and from it one can recover many of the later results in Chapter 20.

Proof of the isogeny theorem in the general case.

To pass to the general case from the case of semisimple rank 1, we make use of the subgroups G_α of G attached to each root α of (G, T). Recall that G_α is generated by T and the root groups U_α and $U_{-\alpha}$, and that (G_α, T) is a split reductive group of semisimple rank 1 (see 21.11).

Let (G, T) and (G', T') be split reductive groups over k, and let $\varphi_T : T \to T'$ be a homomorphism such that $f = X(\varphi_T) : X(T') \to X(T)$ is an isogeny of root data. Thus there is a one-to-one correspondence $\alpha \leftrightarrow \alpha' : \Phi \leftrightarrow \Phi'$ and a map $q : \Phi \to p^{\mathbb{N}}$ satisfying (143, p. 483). We fix a base Δ for Φ.

23.16. *For each $\alpha \in \Delta$, the isogeny φ_T extends to an isogeny $\varphi_\alpha : G_\alpha \to G_{\alpha'}$.*

PROOF. As G_α and $G_{\alpha'}$ have semisimple rank 1, this was proved in 23.14.   □

It remains to prove the following statement.

23.17. *The family of homomorphisms $(\varphi_\alpha : G_\alpha \to G')_{\alpha \in \Delta}$ extends to a homomorphism $\varphi : G \to G'$.*

We construct φ by constructing its graph.[1] Let G'' denote the algebraic subgroup of $G \times G'$ generated by the family of maps $x \mapsto (x, \varphi_\alpha(x)) : G_\alpha \to G \times G'$ (see Section 2h). It is a connected group variety because the G_α are connected group varieties. It suffices to prove the following statement (because then $p' \circ p^{-1}$ will be the map sought).

---

[1]Let $\varphi : X \to Y$ be a morphism of algebraic schemes over k. The morphism $(\mathrm{id}, \varphi) : X \to X \times Y$ is an isomorphism from X onto a subscheme of $X \times Y$, called the **graph** Γ_φ of φ. If Y is separated, then Γ_φ is a closed subscheme of $X \times Y$. The projection map $X \times Y \to X$ restricts to an isomorphism $\Gamma_\varphi \to X$ inverse to (id, φ).

23.18. *The projection* $p \colon G \times G' \to G$ *maps* G'' *isomorphically onto* G.

We prove this in several steps. We may suppose that k is algebraically closed.

23.19. *The projections of* G'' *to* G *and* G' *are both surjective.*

PROOF. The image of p contains $\bigcup_{\alpha \in \Delta} G_\alpha$, which generates G (see 21.62). Similarly, $p' \colon G'' \to G'$ is surjective because of Proposition 23.4. □

23.20. *The group* G'' *is reductive.*

PROOF. The images of $R_u(G'')$ in G and G' are smooth, connected, unipotent, and normal (because p and p' are surjective), and hence trivial. This implies that $R_u(G'')$ is trivial. □

When H is a subgroup variety of G_α, some $\alpha \in \Delta$, we let H'' denote the graph of $\varphi_\alpha | H$. It is a subgroup variety of G'', and $(\mathrm{id}, \varphi_\alpha | H)$ is an isomorphism of H onto H'' with inverse $p|H''$. In particular, U''_α, $U''_{-\alpha}$, T'', and G''_α are subgroup varieties of G'' (in $G \times G'$) isomorphic respectively to U_α, $U_{-\alpha}$, T, and G_α via p. Let U'' and V'' be the subgroup varieties of G'' generated by the families $(U''_\alpha)_{\alpha \in \Delta}$ and $(U''_{-\alpha})_{\alpha \in \Delta}$. The groups U''_α, U'', $U''_{-\alpha}$, and V'' are connected unipotent subgroup varieties of G'', and they are all normalized by the torus T''.

23.21. *The groups* $U''_{-\alpha}$ *and* U''_β *commute elementwise for all* $\alpha, \beta \in \Delta$, $\alpha \neq \beta$.

PROOF. As Δ and Δ' are bases for Φ and Φ', the similar statement holds for G and G' (see 21.21), and hence for G''. □

23.22. *The subset* $C = V'' \cdot T'' \cdot U''$ *of* G'' *is open and dense.*

PROOF. First C is open and dense in its closure $\bar{C}$ because it is the image of the multiplication map
$$V'' \times T'' \times U'' \to G''$$
and we can apply A.15. For the proof that this closure is G'', we use 23.21 and the definition of C. We first show by induction on n that
$$U''_\alpha U''_{-\alpha_1} U''_{-\alpha_2} \cdots U''_{-\alpha_n} \subset \bar{C} \tag{149}$$
for any elements $\alpha, \alpha_1, \ldots, \alpha_n$ of Δ. If $n = 0$, this is obvious. Assume that $n > 0$. If $\alpha \neq \alpha_1$, then
$$U''_\alpha U''_{-\alpha_1} = U''_{-\alpha_1} U''_\alpha$$
by 23.21, and if $\alpha = \alpha_1$, then
$$U''_\alpha U''_{-\alpha_1} \subset G''_\alpha = \overline{U''_{-\alpha} T'' U''_\alpha}.$$
Thus in both cases (149) follows from the induction hypothesis. We have $U''_\alpha V'' \subset \bar{C}$ by (149) because $V'' = U''_{-\alpha_1} U''_{-\alpha_2} \cdots$ for some elements $\alpha_1, \alpha_2, \ldots$ of Δ. It follows that $U''_\alpha \bar{C} \subset \bar{C}$ and clearly $U''_{-\alpha} \bar{C} \subset \bar{C}$ and $T'' \bar{C} \subset \bar{C}$. As the subgroups U''_α, $U''_{-\alpha}$, $\alpha \in \Delta$, and T'' generate G'', this shows that $\bar{C}$ equals G'', as required. □

23.23. *The torus T'' in G'' equals its centralizer, and so it is maximal.*

PROOF. The centralizer of T'' in C is T'' because the corresponding result is true in G and G'. It follows from 23.22 that the centralizer of T'' in G'', which is connected (17.38), contains T'' as a dense open subset and hence equals it. □

23.24. *The projection $p(k): G''(k) \to G(k)$ is bijective and the restriction of p to $T'' \to T$ is an isomorphism.*

PROOF. That $T'' \to T$ is an isomorphism was noted earlier, and $p(k)$ is surjective because p is surjective (23.19). Let $N = \mathrm{Ker}(p)_{\mathrm{red}}$. Then N is a subgroup variety of G'', which is normal in G'' because $N(k) = \mathrm{Ker}(p(k))$ is normal in $G''(k)$ and we can apply Corollary 1.86. As $N \cap T = e$, the group N maps isomorphically onto its image $\bar{N}$ in $\bar{G}'' = G''/R(G'')$. Moreover $\bar{N}$ is normal in $\bar{G}''$ and $\bar{N} \cap \bar{T} = e$, which contradicts Theorem 21.51 unless $N^\circ = e$. Thus $\mathrm{Ker}(p)^\circ(k)$ is trivial. Then $\mathrm{Ker}(p)(k)$ is also trivial because it is finite and normal, hence central, and therefore contained in T''. □

We now complete the proof of 23.18. The properties in 23.24 are not quite enough to make p an isomorphism, as shown by the examples in Proposition 23.30 below. However, in the present case, p also induces an isomorphism between all corresponding pairs of root subgroups of G'' and G, since this is true for the root subgroups U''_α and U_α ($\alpha \in \Delta$) by construction and the others are conjugate to these under the Weyl groups. It therefore induces an isomorphism between the big cells of G'' and of G. Since the translates of the big cell form an open covering, it follows that p itself is an isomorphism. Thus 23.18 is proved, and with it the isogeny theorem (23.9).

NOTES. The isogeny theorem was first proved by Chevalley (in his famous 1956–58 seminar) for semisimple groups over an algebraically closed field. Chevalley's proof works through semisimple groups of rank 2, and is long and complicated.[2] The proofs in Humphreys 1975, Springer 1998, SGA 3, and elsewhere follow Chevalley. Takeuchi (1983) gave a proof of the isogeny theorem in terms of "hyperalgebras" that avoids using systems of rank 2. This inspired Steinberg to find his simple proof for reductive groups over algebraically closed fields (Steinberg 1999). Our proof follows Steinberg except that we have rewritten it in the language of group schemes and extended it to split groups over arbitrary base fields.

c. Complements

The next theorem summarizes what we have proved so far.

THEOREM 23.25 (FULL ISOGENY THEOREM). *Let $\varphi: (G, T) \to (G', T')$ be an isogeny of split reductive groups over the field k; then φ defines an isogeny*

---

[2]See, for example, the six pages of case-by-case calculations in Humphreys 1975, pp. 209–214, or the ten pages in SGA 3, Tome III, pp. 191–200. Borel 1991 does not prove the isogeny theorem.

$f = X(\varphi|T) : \mathcal{R}(G', T') \to \mathcal{R}(G, T)$ *of root data, and every isogeny of root data arises in this way from an isogeny of split reductive groups; moreover, φ is uniquely determined by f up to an inner automorphism defined by an element of $(T'/Z')(k)$. This statement also holds with "isogeny" replaced by "central isogeny", "Frobenius isogeny", or "isomorphism".*

PROOF. Combine 23.5, 23.6, 23.7, and 23.9. □

REMARK 23.26. In particular, an isomorphism φ of split reductive groups defines an isomorphism f of root data, and every isomorphism of root data f arises from a φ, unique up to the inner automorphism defined by an element of $(T'/Z')(k)$. This statement is called the isomorphism theorem.

COROLLARY 23.27. *Let (G, T) and (G', T') be split reductive groups over k. If G and G' become isomorphic over k^a, then (G, T) and (G', T') are isomorphic over k.*

PROOF. If G_{k^a} and G'_{k^a} are isomorphic, then $(G, T)_{k^a}$ and $(G', T')_{k^a}$ are isomorphic (21.18), and so their root data are isomorphic. But it is obvious from their definition that root data do not change under extension of the base field, and so the root data of (G, T) and (G', T') are isomorphic. Hence (G, T) and (G', T') are isomorphic. □

COROLLARY 23.28. *Let G and G' be reductive groups over k. If G and G' become isomorphic over k^a, then they become isomorphic over a finite separable extension of k.*

PROOF. They split over a finite separable extension of k, and so the statement follows from the last corollary. □

PROPOSITION 23.29. *Let (G, T) be a split semisimple group with diagram (V, Φ, X). If $X = P(\Phi)$, then G is simply connected.*

PROOF. A central isogeny $\varphi : G' \to G$ gives a central isogeny $f : (X, \Phi, \Phi^\vee) \to (X', \Phi', \Phi'^\vee)$ of root data. The map $f_\mathbb{Q} : X_\mathbb{Q} \to X'_\mathbb{Q}$ is an isomorphism, and

$$Q(\Phi') = f(Q(\Phi)) \subset f(X) \subset X' \subset P(\Phi') = f_\mathbb{Q}(P(\Phi))$$

(the equalities hold because f is central). If $X = P(\Phi)$, then $f(X) = X'$, and so f is an isomorphism of root data, which implies that φ is an isomorphism (23.5). □

Noncentral isogenies

As étale subgroups of connected groups are central, and finite group schemes of order not divisible by p are étale (11.31), only isogenies of degree divisible by p in characteristic $p \neq 0$ can be noncentral. The simplest noncentral isogenies are the Frobenius isogenies, but there are others, that occur when there are two root

lengths whose ratio squared equals p. Identify $\alpha^\vee$ with $2\alpha/(\alpha,\alpha)$; then, for any long root α_0 and $n \in \mathbb{N}$, multiplication by $p^n(\alpha_0,\alpha_0)/2$ is an isogeny between $\mathcal{R} = (X,\Phi,\Phi^\vee)$ and its dual $\mathcal{R}^\vee = (X^\vee,\Phi^\vee,\Phi)$ which sends $\alpha^\vee \in \Phi^\vee$ to $p^n\alpha$ or $p^{n+1}\alpha$ according as α is a long or short root. When $\mathcal{R}^\vee$ is isomorphic to $\mathcal{R}$, we get an endomorphism φ of the given algebraic group G. These are the Steinberg endomorphisms giving rise to the Suzuki groups and the Ree groups (17.100; Malle and Testerman 2011, Chapter 22). In characteristic $p = 2$, there are also the isogenies we discussed in 18.3, where $\mathcal{R}$ is of type B_n and $\mathcal{R}^\vee$ of type C_n ($n \geq 3$).

PROPOSITION 23.30. *An isogeny $(G,T) \to (G',T')$ of geometrically almost-simple split algebraic groups is an isomorphism if it restricts to an isomorphism $T \to T'$, except for the isogenies $\mathrm{SO}_{2n+1} \to \mathrm{Sp}_{2n}$ in characteristic 2 listed in Example 18.3.*

PROOF. Steinberg 1999, 4.11. □

Generalizations

The method of proof of the isogeny theorem can be applied to obtain more general statements.

THEOREM 23.31. *Let H be a group variety, let T be a split maximal torus in H, and let Δ be a finite $\mathbb{Z}$-linearly independent subset of $X = X(T)$. Suppose that for each $\alpha \in \Delta$ we are given a split reductive subgroup (G_α,T) of (H,T) of semisimple rank 1 with roots $\pm\alpha$, and let $U_{\pm\alpha}$ be the root groups of $\pm\alpha$ in G_α. If $U_{-\alpha}$ and U_β commute for all $\alpha,\beta \in \Delta$, $\alpha \neq \beta$, then the algebraic subgroup G of H generated by the G_α is reductive with maximal torus T, and Δ is a base for the root system of (G,T).*

PROOF. See Steinberg 1999, 5.4. □

COROLLARY 23.32. *Let (G,T) be a split reductive group, and let Δ be a base for its root datum. For any subset Δ' of Δ, there exists an algebraic subgroup G' of G containing T as a maximal torus and such that Δ' is a base for the root datum of (G',T).*

PROOF. Immediate consequence of the theorem. □

REMARK 23.33. In the situation of Theorem 23.31, let $\alpha^\vee$ be the coroot of $\alpha \in \Delta$ relative to (G_α,T), and let $\Delta^\vee = \{\alpha^\vee \mid \alpha \in \Delta\}$. Let $\mathcal{R} = (X,\Phi,\Phi^\vee)$ be the root datum of (G,T). According to the theorem Δ is a base of Φ, and so $\Delta^\vee$ is the corresponding base of $\Phi^\vee$. If $\mathcal{R}' = (X,\Phi',\Phi'^\vee)$ is a second root datum such that Δ and $\Delta^\vee$ are bases for Φ and $\Phi^\vee$, then the Weyl groups of $\mathcal{R}$ and $\mathcal{R}'$ are the same because their generators w_α, $\alpha \in \Delta$, satisfy the same formulas, and so

$$\Phi = W\Delta = \Phi'$$
$$\Phi^\vee = W\Delta^\vee = \Phi'^\vee.$$

THEOREM 23.34. *Let (G,T) be a split reductive group, let Δ be a base for its root system, and let (G_α, T) be the reductive subgroup of semisimple rank 1 attached to $\alpha \in \Delta$. Let H be an algebraic group, and let $\varphi \colon \bigcup_{\alpha \in \Delta} G_\alpha \to H$ be a morphism of algebraic varieties such that $\varphi | G_\alpha$ is a homomorphism for each α. If $\varphi(U_{-\alpha})$ and $\varphi(U_\beta)$ commute for all $\alpha, \beta \in \Delta$, $\alpha \neq \beta$, then φ extends to a homomorphism $\varphi \colon G \to H$.*

PROOF. The graphs $G'_\alpha = \{(x, \varphi(x)) \mid x \in G_\alpha\}$, $\alpha \in \Delta$, in $G \times H$ satisfy the hypotheses of Theorem 23.31, and hence generate a reductive group L in $G \times H$ with $\mathcal{R}(G,T)$ as its root datum. The projection $p_1 \colon L \to G$ is an isomorphism by Theorem 23.25, and $p_2 \circ p_1^{-1}$ is the required extension of φ. □

d. Pinnings

Let (G,T) be a split reductive group over k. For a root α, we let G^α denote the subgroup of G (semisimple of rank 1) generated by U_α and $U_{-\alpha}$. The subgroup U^+ of SL_2 is $\left\{ \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix} \right) \right\}$.

LEMMA 23.35. *Let α be a root of (G,T). There are natural one-to-one correspondences between the following objects:*

(a) *nonzero elements e_α of $\mathfrak{g}_\alpha$;*

(b) *isomorphisms $u_\alpha \colon \mathbb{G}_a \to U_\alpha$;*

(c) *central isogenies $v_\alpha \colon SL_2 \to G^\alpha$ such that $v_\alpha(\mathrm{diag}(t, t^{-1})) = \alpha^\vee(t)$ and $v_\alpha(U^+) \subset U_\alpha$.*

PROOF. (a)$\leftrightarrow$(b). Given u_α, we define e_α to be $\mathrm{Lie}(u_\alpha)(1)$. Every nonzero e_α arises from a unique u_α because the map

$$\varphi \mapsto \mathrm{Lie}(\varphi) \colon \mathrm{Isom}(\mathbb{G}_a, U_\alpha) \to \mathrm{Isom}(k, \mathfrak{g}_\alpha)$$

is an isomorphism (each set is a principal homogeneous space for $k^\times$; 14.59).

(b)$\leftrightarrow$(c). Given v_α, we define u_α to be the composite of v_α with the isomorphism $a \mapsto \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix} \right) \colon \mathbb{G}_a \to U^+$. That every u_α arises from a unique v_α is proved in 21.24. □

When e_α and u_α correspond as in the lemma, we let $\exp(e_\alpha) = u_\alpha(1)$.

DEFINITION 23.36. A ***pinning***[3] of a split reductive group is a pair $(\Delta, (e_\alpha)_{\alpha \in \Delta})$ with Δ a base for the roots and e_α a nonzero element of $\mathfrak{g}_\alpha$ for every simple α. A ***pinned reductive group*** is a split reductive group equipped with a pinning. The homomorphisms u_α and v_α corresponding to e_α as in (23.44) are called the ***pinning maps***.

---

[3]The original French term is "épinglage". Some authors prefer "frame" to "pinning".

DEFINITION 23.37. Let $(G, T, \Delta, (e_\alpha)_{\alpha \in \Delta})$ and $(G', T', \Delta', (e'_\alpha)_{\alpha \in \Delta'})$ be pinned reductive groups. An isogeny $\varphi \colon (G, T) \to (G', T')$ *respects the pinnings*, or is an *isogeny of pinned groups*, if

(a) under the one-to-one correspondence $\alpha \leftrightarrow \alpha' \colon \Phi \leftrightarrow \Phi'$ defined by φ (23.5), elements of Δ correspond to elements of Δ', and

(b) $\varphi(\exp(e_\alpha)) = \exp(e_{\alpha'})$ for all $\alpha \in \Delta$.

When φ is a central isogeny the conditions become: (a) if $\alpha \in \Delta$, then $\alpha' \in \Delta'$ and φ restricts to an isomorphism $U_\alpha \to U_{\alpha'}$; (b) $(\varphi|U_\alpha) \circ u_\alpha = u_{\alpha'}$.

DEFINITION 23.38. A *based* (or *pinned*) *root datum* is a root datum $(X, \Phi, \Phi^\vee)$ equipped with a base Δ for Φ. An *isogeny of based root data* $(X, \Phi, \Phi^\vee, \Delta) \to (X', \Phi', \Phi'^\vee, \Delta')$ is an isogeny of root data such that simple roots correspond to simple roots under $\alpha \leftrightarrow \alpha'$. *Central isogenies* and *isomorphisms* of based root data are defined similarly.

Recall (23.4) that, under an isogeny $(X, \Phi, \Phi^\vee) \to (X', \Phi', \Phi'^\vee)$ of root data, bases for Φ correspond to bases for Φ'. For an isogeny of root data to be an isogeny of based root data, the *given* base for Φ must correspond to the *given* base for Φ'.

Let $(X, \Phi, \Phi^\vee, \Delta)$ be a based root datum, and let Φ^+ be the system of positive roots defined by Δ. Then $\{\alpha^\vee \mid \alpha \in \Phi^+\}$ is a system of positive roots in $\Phi^\vee$, and we let $\Delta^\vee$ denote its base. Often, the based root datum is denoted by $(X, \Phi, \Phi^\vee, \Delta, \Delta^\vee)$ or, more symmetrically, by $(X, X^\vee, \Phi, \Phi^\vee, \Delta, \Delta^\vee)$.

LEMMA 23.39. *Let (G, T) be a split reductive group over k, and let $(\Delta, (e_\alpha))$ and $(\Delta', (f_{\alpha'}))$ be pinnings of (G, T). Then there exists a $g \in (N_G(T)/Z(G))(k)$ such that* $\mathrm{inn}(g)$ *maps $(\Delta, (e_\alpha))$ onto $(\Delta', (f_{\alpha'}))$.*

PROOF. There exists a $w \in W$ such that $w\Delta' = \Delta$ (see 21.41), and w is represented by an element of $N_G(T)(k)$ (see 21.11d, 21.37). Thus, we may suppose that $\Delta' = \Delta$. As Δ is a basis for $X(T/Z(G))$ (see 21.9), there exists a $t \in (T/Z)(k)$ such that $\alpha(t)e_\alpha = f_\alpha$ for all $\alpha \in \Delta$. Now $\mathrm{inn}(t)$ acts trivially on Δ and maps e_α to f_α for all $\alpha \in \Delta$ (see 21.22). □

With these definitions, $(G, T, \Delta, (e_\alpha)) \rightsquigarrow (X, \Phi, \Phi^\vee, \Delta)$ is a contravariant functor from pinned reductive groups over k and isogenies to based root data and isogenies. The fundamental theorem says that this functor is fully faithful.

THEOREM 23.40 (FUNDAMENTAL THEOREM). *Let G and G' be pinned reductive groups over k, and let $f \colon \mathcal{R}(G') \to \mathcal{R}(G)$ be an isogeny of the corresponding based root data. There exists a unique isogeny $\varphi \colon G \to G'$ of pinned groups such that $\mathcal{R}(\varphi) = f$. This statement also holds with "isogeny" replaced by "central isogeny" or "isomorphism".*

PROOF. The uniqueness follows from Corollary 21.63. According to Theorem 23.9, there exists an isogeny $\varphi\colon(G,T)\to(G',T')$ such that $X^*(\varphi)=f$, and Lemma 23.39 shows that, after φ has been composed with an inner automorphism by an element of $(N_G(T)/Z(G))(k)$, it will preserve the pinnings. □

COROLLARY 23.41. *Let G and G' be pinned reductive groups over k. The following are equivalent:*

(a) *G and G' are isomorphic as pinned groups;*

(b) *G and G' have isomorphic based root data;*

(c) *G and G' become isomorphic over k^{a} as pinned groups.*

PROOF. The based root datum of a pinned reductive group does not change under extension of the base field, and so the statement is an immediate consequence of the fundamental theorem. □

COROLLARY 23.42. *The only automorphism of a split reductive group respecting a pinning of the group is the trivial one.*

PROOF. Immediate consequence of the theorem (with isomorphism for isogeny). □

In other words, the pinning rigidifies the group. This inspired the frontispiece.

COROLLARY 23.43. *Let $(G,T,\Delta,(e_\alpha))$ be a pinned reductive group over k, and let k_0 be a subfield of k. There exists a split model (G_0,T_0) of (G,T) over k_0, unique up to a unique isomorphism, such that $\exp(e_\alpha)\in G_0(k)$ for all $\alpha\in\Delta$.*

Specifically, there exists a split reductive group (G_0,T_0) over k_0 and an isomorphism $\varphi\colon(G_0,T_0)_k\to(G,T)$ such that e_α lies in the image of $d\varphi\colon(\mathfrak{g}_0)_k\to\mathfrak{g}$ for each $\alpha\in\Delta$. It follows that (G_0,T_0) has a pinning $(\Delta_0,(e_{0\alpha})_{\alpha\in\Delta_0})$ for which φ becomes an isomorphism of pinned reductive groups.

The proof is by descent using the fundamental theorem (Conrad et al. 2015, A.4.13).

e. Automorphisms

Let G be a reductive group over k. We write $\mathrm{Aut}(G)$ for the group of automorphisms of G as an algebraic group over k. Recall (17.63) that the inner automorphisms of G are those defined by an element of $G^{\mathrm{ad}}(k)$. There is an exact sequence

$$1\to\mathrm{Inn}(G)\to\mathrm{Aut}(G)\to\mathrm{Out}(G)\to1 \qquad (150)$$

with $\mathrm{Inn}(G)=G^{\mathrm{ad}}(k)$ and $\mathrm{Out}(G)$ the cokernel of $\mathrm{Inn}(G)\to\mathrm{Aut}(G)$.

PROPOSITION 23.44. *Let G be a pinned reductive group over k, and let f be an automorphism of the based root system of G. Then there exists a unique automorphism φ of G respecting the pinning and such that $X^*(\varphi)=f$.*

PROOF. Special case of Theorem 23.40 with "isomorphism" for "isogeny". □

More explicitly, let (G, T) be a split reductive group over k. Let Δ be a base for the root system of (G, T), and choose for each $\alpha \in \Delta$ an isomorphism $u_\alpha : \mathbb{G}_a \to U_\alpha$. If f is an automorphism of $X(T)$ permuting the simple roots, then there exists a unique automorphism φ of (G, T) such that $X(\varphi|T) = f$ and $\varphi \circ u_\alpha = u_{f(\alpha)}$ for all simple α.

PROPOSITION 23.45. *Let $(G, T, \Delta, (e_\alpha))$ be a pinned reductive group over k. The map $\mathrm{Aut}(G) \to \mathrm{Out}(G)$ induces an isomorphism*

$$\mathrm{Aut}(G, T, \Delta, (e_\alpha)) \to \mathrm{Out}(G).$$

PROOF. Immediate consequence of Theorem 23.40. □

COROLLARY 23.46. *There are canonical isomorphisms*

$$\mathrm{Aut}(X, \Phi, \Delta) \simeq \mathrm{Aut}(G, T, \Delta, (e_\alpha)) \simeq \mathrm{Out}(G).$$

PROOF. Combine Propositions 23.44 and 23.45. □

COROLLARY 23.47. *Let G be a reductive group over k. If G is splittable, then the sequence (150) splits. More precisely, the choice of a split maximal torus T and a pinning $(\Delta, (e_\alpha))$ determines an isomorphism*

$$\mathrm{Aut}(G) \simeq \mathrm{Inn}(G) \rtimes \mathrm{Aut}(X, \Phi, \Delta).$$

PROOF. The choice of (T, Φ, Δ) determines a homomorphism $G \to \mathrm{Aut}(X, \Phi, \Delta)$ whose kernel is $\mathrm{Inn}(G)$ and whose restriction to $\mathrm{Aut}(G, T, \Delta, (e_\alpha))$ is an isomorphism. □

COROLLARY 23.48. *Let G_0 be a splittable reductive group over k. The map $(G, f) \mapsto G$ sending an inner form (G, f) of G_0 to G defines a bijection from the set of equivalence classes of inner forms (G, f) of G_0 onto the set of isomorphism classes of inner forms G of G_0.*

PROOF. The map $H^1(k, \mathrm{Inn}(G)) \to H^1(k, \mathrm{Aut}(G))$ is injective, and so both sets map bijectively to $H^1(k, \mathrm{Inn}(G))$. □

COROLLARY 23.49. *Let (G, T) be a split reductive group over k, and let B be a Borel subgroup containing T. The isomorphism $G^{\mathrm{ad}}(k) \to \mathrm{Inn}(G)$ induces isomorphisms*

$$(N/Z)(k) \simeq \mathrm{Inn}(G, T)$$
$$(T/Z)(k) \simeq \mathrm{Inn}(G, B, T)$$

where $N = N_G(T)$ and $Z = Z(G)$.

PROOF. Obvious, as N/Z is the stabilizer of T in G, and T/Z is the stabilizer of B in N/Z (see 21.41). □

REMARK 23.50. For a reductive group G over k, there is an exact sequence of sheaves of groups

$$e \to \underline{\mathrm{Inn}}(G) \to \underline{\mathrm{Aut}}(G) \to \underline{\mathrm{Out}}(G) \to e \qquad (151)$$

with $\underline{\mathrm{Inn}}(G) \simeq G^{\mathrm{ad}}$ and $\underline{\mathrm{Out}}(G)$ the cokernel of $\underline{\mathrm{Inn}}(G) \to \underline{\mathrm{Aut}}(G)$ (as a map of sheaves of groups; 5.73). If G is split, then $\underline{\mathrm{Out}}(G)$ is the constant group scheme defined by a finitely generated group, and so $\underline{\mathrm{Aut}}(G)$ is an affine group scheme (not necessarily of finite type over k); it follows by descent that the same is true for nonsplit reductive groups. For example, if G is diagonalizable, say, $G = D(M)$, then $\underline{\mathrm{Aut}}(G) \simeq \mathrm{Aut}(M)_k$ as in 12.43. When G and H are algebraic groups over k, the functor $\underline{\mathrm{Hom}}(G, H)$ is representable by an affine group scheme if G is reductive (SGA 3, XXIV, 7), but not in general otherwise (Exercise 1-1).

f. Quasi-split forms

In this section, a k-form is a k^{s}/k-form and we write $\mathrm{Aut}_{k^{\mathrm{s}}}(X)$ for $\mathrm{Aut}(X_{k^{\mathrm{s}}})$. Let $\Gamma = \mathrm{Gal}(k^{\mathrm{s}}/k)$. Recall (17.67) that a connected group variety is said to be quasi-split if it contains a Borel subgroup. For a k-form H of an algebraic group G, let $\gamma(H)$ denote the image of the cohomology class of H under the map $H^1(\Gamma, \mathrm{Aut}_{k^{\mathrm{s}}}(G)) \to H^1(\Gamma, \mathrm{Out}_{k^{\mathrm{s}}}(G))$.

THEOREM 23.51. *Let G be a splittable reductive group over k. Every element of $H^1(\Gamma, \mathrm{Out}_{k^{\mathrm{s}}}(G))$ is the class of a quasi-split k-form of G, and two quasi-split k-forms of G are isomorphic if and only if they have the same class.*

In other words, the set $H^1(\Gamma, \mathrm{Out}_{k^{\mathrm{s}}}(G))$ classifies the isomorphism classes of quasi-split k-forms of G.

PROOF. Let T be a split maximal torus in G and $(\Delta, (e_\alpha))$ a pinning of (G, T). Let B be the Borel subgroup of G (containing T) corresponding to Δ.

Let H be a quasi-split k-form of G. By definition, it contains a Borel subgroup B', and we let T' be a maximal torus of B'. The isomorphism $G_{k^{\mathrm{s}}} \to H_{k^{\mathrm{s}}}$ may be chosen to map $(B, T)_{k^{\mathrm{s}}}$ to $(B', T')_{k^{\mathrm{s}}}$. It follows that classifying the quasi-split k-forms of G amounts to classifying the k-forms of (G, B, T), which are classified by $H^1(\Gamma, \mathrm{Aut}_{k^{\mathrm{s}}}(G, B, T))$.

The obvious maps

$$\mathrm{Aut}_{k^{\mathrm{s}}}(G, T, \Delta, (e_\alpha)) \xrightarrow{a} \mathrm{Aut}_{k^{\mathrm{s}}}(G, B, T) \xrightarrow{b} \mathrm{Out}_{k^{\mathrm{s}}}(G)$$

compose to an isomorphism. Therefore b is surjective with kernel $(T/Z)(k^{\mathrm{s}})$ (see 23.49). As T/Z is a split torus, we deduce (3.47) that

$$H^1(b) \colon H^1(\Gamma, \mathrm{Aut}_{k^{\mathrm{s}}}(G, B, T)) \to H^1(\Gamma, \mathrm{Out}_{k^{\mathrm{s}}}(G))$$

is injective. As $H^1(b) \circ H^1(a)$ is an isomorphism, we see that both $H^1(a)$ and $H^1(b)$ are isomorphisms. This completes the proof. $\qquad \square$

THEOREM 23.52. *Consider the cohomology sequence of (150):*

$$H^1(\Gamma, \mathrm{Inn}_{k^s}(G)) \to H^1(\Gamma, \mathrm{Aut}_{k^s}(G)) \xrightarrow{b} H^1(\Gamma, \mathrm{Out}_{k^s}(G)).$$

Let $\gamma \in H^1(\Gamma, \mathrm{Out}_{k^s}(G))$, and let G' be a quasi-split k-form of G with class γ (23.51). The fibre of b over γ classifies the isomorphism classes of inner k-forms of G'.

PROOF. By definition, the fibre of b over the neutral class classifies the isomorphism classes of inner k-forms of G. To determine the fibres over other elements of $H^1(\Gamma, \mathrm{Out}_{k^s}(G))$ we have to twist the sequence by a 1-cocycle for $\mathrm{Aut}_{k^s}(G)$, as explained in Serre 1997, I, §5.5. Let f be an isomorphism $G_{k^s} \to G'_{k^s}$, and let (a_σ) with $a_\sigma = f^{-1} \circ \sigma f : \Gamma \to \mathrm{Aut}_{k^s}(G)$ be the corresponding continuous 1-cocycle. From the exact sequence

$$1 \to \mathrm{Inn}_{k^s}(G') \to \mathrm{Aut}_{k^s}(G') \to \mathrm{Out}_{k^s}(G') \to 1$$

we get the top row of the following diagram:

$$
\begin{array}{ccccc}
H^1(\Gamma, \mathrm{Inn}_{k^s}(G')) & \longrightarrow & H^1(\Gamma, \mathrm{Aut}_{k^s}(G')) & \xrightarrow{b'} & H^1(\Gamma, \mathrm{Out}_{k^s}(G')) \\
& & \Big\downarrow{\simeq} & & \Big\downarrow{\simeq} \\
H^1(\Gamma, \mathrm{Inn}_{k^s}(G)) & \longrightarrow & H^1(\Gamma, \mathrm{Aut}_{k^s}(G)) & \xrightarrow{b} & H^1(\Gamma, \mathrm{Out}_{k^s}(G)).
\end{array}
$$

The vertical maps are canonically defined by (a_σ), and send the neutral elements to the class of (a_σ) in $H^1(\Gamma, \mathrm{Aut}_{k^s}(G))$ and its image γ in $H^1(\Gamma, \mathrm{Out}_{k^s}(G))$. Thus the fibre of b over γ is in canonical one-to-one correspondence with the fibre of b' over the neutral element, which is in canonical one-to-one correspondence with the isomorphism classes of inner forms of G'. $\qquad \square$

COROLLARY 23.53. *Each k-form of G is an inner form of a quasi-split k-form, which is uniquely determined up to isomorphism.*

PROOF. A k-form H of G is an inner form of any quasi-split form whose class in $H^1(\Gamma, \mathrm{Out}_{k^s}(G))$ is that of H. $\qquad \square$

COROLLARY 23.54. *Let H be a reductive group over k. The quasi-split inner k-forms of H form a single isomorphism class, i.e., there is a unique $\gamma \in H^1(k, H^{\mathrm{ad}})$ such that H_γ is quasi-split.*

PROOF. Immediate consequence of the theorem. $\qquad \square$

g.   Statement of the existence theorem; applications

To complete the classification of reductive groups in terms of root data, we need the existence theorem.

THEOREM 23.55 (EXISTENCE THEOREM). *Every reduced root datum arises from a split reductive group over k.*

We defer the proof to the next section (see also Chapter 24).

COROLLARY 23.56. *The functor $(G, T) \rightsquigarrow (X, \Phi, \Phi^\vee)$ is an equivalence from the category*

$$\begin{cases} \text{objects:} & \text{split reductive groups } (G, T) \text{ over } k \\ \text{morphisms:} & (T'/Z')(k)\backslash \mathrm{Isog}((G, T), (G', T')) \end{cases}$$

to the category

$$\begin{cases} \text{objects:} & \text{root data} \\ \text{morphisms:} & \text{isogenies.} \end{cases}$$

PROOF. Combine Theorems 23.25 and 23.55. □

A remarkable feature of this statement is that, while the first category appears to depend on k, the second does not. In particular, if k'/k is an extension of fields, then every split reductive group (G, T) over k' arises from a split reductive group over k.

COROLLARY 23.57. *Let G be a reductive group over k. There exists a split reductive group G_0 over k, unique up to isomorphism, such that $G_{0k^s} \simeq G_{k^s}$.*

PROOF. Let T be a maximal torus in G. Then T_{k^s} is a split maximal torus in G_{k^s} (see 17.82), and we take (G_0, T_0) to be the split reductive group over k with root datum equal to that of $(G, T)_{k^s}$. □

Semisimple groups

Recall (C.26) that a diagram is a reduced root system (V, Φ) over $\mathbb{Q}$ together with a lattice X in V such that $Q(\Phi) \subset X \subset P(\Phi)$. A split semisimple algebraic group (G, T) over k defines a diagram (V, Φ, X) with $X = X(T)$ and $V = X(T)_{\mathbb{Q}}$.

THEOREM 23.58. *The map $(G, T) \mapsto (V, \Phi, X))$ defines a bijection from the set of isomorphism classes of split semisimple groups over k to the set of isomorphism classes of diagrams.*

PROOF. The isomorphism and existence theorems give a one-to-one correspondence between the first set and the set of isomorphism classes of semisimple root data (23.26, 23.55, 21.48), but semisimple root data are essentially the same as diagrams (C.35). □

PROPOSITION 23.59. *Let (G, T) be a split semisimple group with diagram (V, Φ, X). Then G is simply connected if and only if $X = P(\Phi)$.*

PROOF. We know that G is simply connected if $X = P(\Phi)$ (see 23.29). For the converse, suppose that $X \neq P(\Phi)$. Then the inclusion $X \hookrightarrow P(\Phi)$ is a nonisomorphic central isogeny $(X, \Phi, \Phi^\vee) \to (P(\Phi), \Phi, \Phi^\vee)$. According to Corollary 23.56, this arises from a nonisomorphic central isogeny $(G', T') \to (G, T)$ and so G is not simply connected. □

The centre of a split semisimple group (G, T) is the subgroup of T with character group $X/Q(\Phi)$ (see 21.8). Therefore, the proposition says that the simply connected groups are those with the largest possible centre given the constraint $Q(\Phi) \subset X \subset P(\Phi)$. At the opposite extreme, G has trivial centre if and only if $X = Q(\Phi)$. These are the adjoint groups.

REMARK 23.60. The existence theorem implies that every semisimple group admits a universal covering. For a split group (G, T), the universal covering is the central isogeny corresponding to the isogeny of root data $(X, \Phi, \Phi^\vee) \to (P(\Phi), \Phi, \Phi^\vee)$. Every semisimple group over k splits over k^s, and descent theory then shows that the universal covering over k^s descends to k (because of the uniqueness of the universal covering 18.8). This is the usual proof (see, for example, Conrad et al. 2015, A.4.11). However, as we saw in Chapter 18, by using a little algebraic geometry, it is possible to give a direct proof that every connected group variety G such that $X(G) = 0$ admits a universal covering.

EXAMPLE 23.61. The groups SL_n, Sp_{2n}, and $Spin_n$ are simply connected, the groups SO_{2n+1} and PSL_n are adjoint, while the groups SO_{2n} are neither. The groups of type G_2, F_4, E_8 are simultaneously simply connected and adjoint. See Chapter 24.

Semisimple groups up to strict isogeny

Two semisimple algebraic group G and G' are said to be ***strictly isogenous*** if there exist central isogenies $H \to G$ and $H \to G'$. In other words, they are strictly isogenous if they have the same simply connected covering group.

THEOREM 23.62. *Two splittable semisimple groups over k are strictly isogenous if and only if they have the same Dynkin diagram, and every Dynkin diagram arises from a splittable semisimple group over k. Such a group is almost-simple if and only if its Dynkin diagram is connected.*

PROOF. Simply connected semisimple groups are classified by their root systems (23.58, 23.59), which in turn are classified by their Dynkin diagrams (Section Cf). □

h.   Proof of the existence theorem

Let k be a field. It remains to prove that every root datum arises from a split reductive group over k. In fact, by Exercise 21-4, it suffices to prove the following statement:

> for every diagram (V, Φ), there exists a split semisimple group (G, T) over k with diagram $(V, \Phi, P(\Phi))$.

One approach to proving this, which we explain in the next chapter, is to exhibit a simply connected almost-simple group for each indecomposable root system. In this section, we sketch a uniform approach that goes back in essence to Chevalley. We assume some knowledge of the theory of semisimple Lie algebras (Serre 1966).

Semisimple Lie algebras in characteristic zero

Let k be a field of characteristic zero, and let $\mathfrak{g}$ be a semisimple Lie algebra over k. A maximal abelian Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is Cartan if it consists of semisimple elements. To say that an element h of $\mathfrak{h}$ is semisimple means that the endomorphism $\mathrm{ad}_{\mathfrak{g}}(h)$, $x \mapsto [h, x]$, of $\mathfrak{g}$ becomes diagonalizable over an extension of k. The Cartan algebra is said to be splitting if these endomorphisms are diagonalizable over k itself, and a semisimple Lie algebra is said to be split if it contains a splitting Cartan subalgebra.

Let $\mathfrak{h}$ be a splitting Cartan subalgebra in $\mathfrak{g}$. The $\mathrm{ad}_{\mathfrak{g}}(h)$ for $h \in \mathfrak{h}$ form a commuting family of diagonalizable endomorphisms of $\mathfrak{g}$. From linear algebra, we know that there exists a basis of simultaneous eigenvalues. In other words, $\mathfrak{g}$ is a direct sum of the subspaces

$$\mathfrak{u}_\alpha \overset{\mathrm{def}}{=} \{x \in \mathfrak{g} \mid \mathrm{ad}_{\mathfrak{g}}(h)(x) = \alpha(h)x \text{ for all } h \in \mathfrak{h}\}$$

where α runs over the elements of the linear dual $\mathfrak{h}^\vee$ of $\mathfrak{h}$. The nonzero α such that $\mathfrak{u}_\alpha \neq 0$ form a reduced root system Φ in $\mathfrak{h}^\vee$, and we have

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{u}_\alpha.$$

Up to isomorphism, the root system $(\mathfrak{h}^\vee, \Phi)$ depends only on $\mathfrak{g}$.

THEOREM 23.63 (CARTAN–KILLING). *Every reduced root system arises from a semisimple Lie algebra over* $\mathbb{C}$.

FIRST PROOF

Let (V, Φ) be the root system, and let $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ be a base for Φ. Let $n(i, j) = \langle \alpha_j, \alpha_i^\vee \rangle$ (so $(n(i.j))_{1 \leq i,j \leq n}$ is the Cartan matrix of the root system).

Let $\mathfrak{a}$ be the algebra with generators $X_1, \ldots, X_n, Y_1, \ldots, Y_n, H_1, \ldots, H_n$ and (Weyl) relations

$$[H_i, H_j] = 0$$
$$[X_i, X_i] = H_i, \quad [X_i, Y_j] = 0 \quad \text{if } i \neq j$$
$$[H_i, X_j] = n(i, j)X_j, \quad [H_i, X_j] = -n(i, j)Y_j.$$

Let $\mathfrak{n}$ and $\mathfrak{x}$ be the Lie subalgebras generated by the Y_i and X_i respectively, and let $\mathfrak{h}$ be the Lie subalgebra with basis the H_i. Then

$$\mathfrak{a} = \mathfrak{n} \oplus \mathfrak{h} \oplus \mathfrak{x},$$

and $\mathfrak{n}$ and $\mathfrak{x}$ are the free Lie algebras generated by the Y_i and X_i respectively. For a direct proof of this, see Bourbaki 1975, VIII, §4, no. 2.

Now let $\mathfrak{g}$ be the quotient of $\mathfrak{a}$ by the relations

$$\mathrm{ad}(X_i)^{-n(i,j)+1}(X_j) = 0 \quad \text{if } i \neq j$$
$$\mathrm{ad}(Y_i)^{-n(i,j)+1}(J_j) = 0 \quad \text{if } i \neq j.$$

Then $\mathfrak{g}$ is a semisimple Lie algebra with Cartan algebra $\mathfrak{h}$, and the root system of $(\mathfrak{g}, \mathfrak{h})$ is isomorphic to (V, Φ). For a direct proof of this, see Serre 1966, VI.

SECOND PROOF

Let k be a field of characteristic zero. A Lie algebra is **reductive** if it is a product of a commutative Lie algebra and a semisimple Lie algebra.

PROPOSITION 23.64. *Let $\mathfrak{g}$ be a semisimple Lie algebra over k and $\mathfrak{h}$ a splitting Cartan subalgebra. Let Δ be a finite linearly independent subset of $\mathfrak{h}^{\vee}$. Suppose that, for each $\alpha \in \Delta$, we are given a reductive Lie subalgebra $\mathfrak{g}(\alpha)$ of G with splitting Cartan subalgebra $\mathfrak{h}$ and roots $\pm\alpha$. Let $\mathfrak{u}_\alpha = \mathfrak{g}(\alpha)_\alpha$. If $[\mathfrak{u}_{-\alpha}, \mathfrak{u}_\beta] = 0$ for all $\alpha, \beta \in \Delta$, $\alpha \neq \beta$, then the Lie subalgebra $\mathfrak{g}'$ of $\mathfrak{g}$ generated by the $\mathfrak{g}(\alpha)$ is reductive with splitting Cartan algebra $\mathfrak{h}$, and Δ is a base for the root system of $(\mathfrak{g}, \mathfrak{h})$.*

PROOF. Rewrite Steinberg's proof of (23.31) for Lie algebras. See also the arguments in Geck 2016, §4.   □

Let (V, Φ) be a root system over $\mathbb{Q}$. Given $\alpha, \beta \in \Phi$ such that $\beta \neq \pm\alpha$, the α-**string through** β is the longest sequence

$$\beta - p\alpha, \ldots, \beta - \alpha, \beta, \beta + \alpha, \ldots, \beta + q\alpha$$

consisting of roots. Let $m_\alpha^+(\beta) = q + 1$ and $m_\alpha^-(\beta) = p + 1$.

Let $\Delta = \{\alpha_i \mid i \in I\}$ be a base for (V, Φ). Let M be the vector space over k with basis $\{u_i, i \in I; v_\alpha, \alpha \in \Phi\}$. For each $i \in I$, let h_i, e_i, and f_i be the endomorphisms of M defined by the following formulas:

$$e_i(u_j) = |\langle \alpha_i, \alpha_j^\vee \rangle| v_{\alpha_i} \qquad e_i(v_\alpha) = \begin{cases} m_{\alpha_i}^-(\alpha) v_{\alpha + \alpha_i} & \text{if } \alpha + \alpha_i \in \Phi \\ u_i & \text{if } \alpha = -\alpha_i \\ 0 & \text{otherwise} \end{cases}$$

$$f_i(u_j) = |\langle \alpha_i, \alpha_j^\vee \rangle| v_{-\alpha_i} \qquad f_i(v_\alpha) = \begin{cases} m_{\alpha_i}^+(\alpha) v_{\alpha - \alpha_i} & \text{if } \alpha - \alpha_i \in \Phi \\ u_i & \text{if } \alpha = \alpha_i \\ 0 & \text{otherwise} \end{cases}$$

$$h_i(u_j) = 0 \qquad h_i(v_\alpha) = \langle \alpha, \alpha^\vee \rangle v_\alpha.$$

Regard these endomorphisms as elements of $\mathfrak{gl}_M$. The h_i act diagonally, and generate a commutative Lie subalgebra $\mathfrak{h}'$ of $\mathfrak{gl}_M$; moreover $\mathfrak{h}'^\vee \simeq k^{|I|} \simeq V$.

LEMMA 23.65. *There are the following equalities:*

$$\begin{cases} [h_j, e_i] = \langle \alpha_i, \alpha_j^\vee \rangle e_i \text{ for all } i, j, \\ [h_j, f_i] = -\langle \alpha, \alpha_j^\vee \rangle f_i \text{ for all } i, j, \end{cases} \qquad \begin{cases} [e_i, f_i] = h_i \text{ for all } i, \\ [e_i, f_j] = 0 \text{ for all } i \neq j. \end{cases}$$

PROOF. These can be proved by a direct calculation (Geck 2016, 3.3, 3.4, 3.5). □

LEMMA 23.66. *Relative to a suitable basis for M, the e_i act by strictly upper triangular matrices and the f_i by strictly lower triangular matrices.*

PROOF. The height $\mathrm{ht}(\beta)$ of a root β is $\sum m_i$ if $\beta = \sum m_i \alpha_i$. Write $\Phi^+ = \{\beta_1, \ldots, \beta_N\}$ with $\mathrm{ht}(\beta_1) \leq \mathrm{ht}(\beta_2) \leq \cdots$. Then

$$\{v_{\beta_N}, \ldots, v_{\beta_1}, u_{j_1}, \ldots, u_{j_l}, v_{-\beta_1}, \ldots, v_{-\beta_N}\}$$

is a suitable basis for M, as can be seen directly from the definitions of the e_i and f_i. □

In particular, e_i and f_i lie in $\mathfrak{sl}_M$.

THEOREM 23.67. *Let $\mathfrak{g}'$ be the Lie subalgebra of $\mathfrak{sl}_M$ generated by $\{e_i, f_i \mid i \in I\}$. Then $\mathfrak{g}'$ is a semisimple Lie algebra with splitting Cartan subalgebra $\mathfrak{h}'$, and the root system of $(\mathfrak{g}', \mathfrak{h}')$ is (V, Φ).*

PROOF. Let $\mathfrak{h}$ denote the diagonal Cartan subalgebra of $\mathfrak{sl}_M$. For $i \in I$, let $\mathfrak{g}_i$ denote the Lie subalgebra of $\mathfrak{sl}_M$ generated by e_i, f_i, and $\mathfrak{h}$. From the lemma, we see that $\mathfrak{g}_i$ is a reductive Lie algebra with splitting Cartan subalgebra $\mathfrak{h}$ and roots $\pm \alpha_i$; moreover, $[\mathfrak{u}_{-\alpha_i}, \mathfrak{u}_{\alpha_j}] = 0$ if $i \neq j$. According to the proposition, the Lie algebra $\mathfrak{g}$ generated by the $\mathfrak{g}_i$ is a reductive Lie algebra with splitting Cartan subalgebra $\mathfrak{h}$ and Δ is a base for the root system of $(\mathfrak{g}, \mathfrak{h})$. Now $\mathfrak{g}' = [\mathfrak{g}, \mathfrak{g}]$ has the required properties, and it is generated (as a Lie algebra) by $\{e_i, f_i \mid i \in I\}$. □

NOTES. The definition of the vector space M and its family of operators follows Geck 2016, which extends earlier work of Lusztig.

Semisimple algebraic groups in characteristic zero

Classically, the path from the existence theorem for Lie algebras to algebraic groups passed through compact Lie groups and complex Lie groups (Borel 1975, 1.5; Conrad 2014, Appendix D). Using Tannakian theory, it is possible to give a much simpler and more direct derivation (Milne 2007).

LEMMA 23.68. *A connected algebraic group G over a field of characteristic zero is semisimple (resp. reductive) if and only if its Lie algebra is semisimple (resp. reductive and $Z(G)$ is of multiplicative type).*

PROOF. Suppose that $\mathrm{Lie}(G)$ is semisimple, and let N be a normal commutative algebraic subgroup of G. Then $\mathrm{Lie}(N)$ is a commutative ideal in G, and so it is zero. This implies that N is finite. For the converse, see p. 475. The statements for "reductive" follow from those for "semisimple".   □

Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over a field k of characteristic zero. A ***ring of representations*** of $\mathfrak{g}$ is a collection of finite-dimensional 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

$$\alpha = (\alpha_V)_{V \in \mathcal{R}}, \quad \alpha_V \in \mathrm{End}_{k\text{-linear}}(V),$$

satisfying the following conditions:
   (a) for all $V, W \in \mathcal{R}$, $\alpha_{V \otimes W} = \alpha_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes \alpha_W$;
   (b) $\alpha_V = 0$ if $\mathfrak{g}$ acts trivially on V, and
   (c) for all $V, W \in \mathcal{R}$ and homomorphisms $\beta \colon V \to W$, $\alpha_W \circ \beta_{\mathcal{R}} = \beta_{\mathcal{R}} \circ \alpha_V$.

The set $\mathfrak{g}_{\mathcal{R}}$ of all endomorphisms of $\mathcal{R}$ becomes a Lie algebra over k (possibly infinite-dimensional) with the bracket $[\alpha, \beta]_V = [\alpha_V, \beta_V]$.

Let $\mathcal{R}$ be a ring of representations of a Lie algebra $\mathfrak{g}$. For $x \in \mathfrak{g}$, the family $(r_V(x))_{V \in \mathcal{R}}$ is an endomorphism of $\mathcal{R}$, and $x \mapsto (r_V(x))$ is a homomorphism of Lie algebras $\mathfrak{g} \to \mathfrak{g}_{\mathcal{R}}$. If $\mathcal{R}$ contains a faithful representation of $\mathfrak{g}$, then $\mathfrak{g} \to \mathfrak{g}_{\mathcal{R}}$ is injective.

LEMMA 23.69. *Let G be an affine group scheme over k, and let $\mathcal{R}$ be the collection of representations of $\mathrm{Lie}(G)$ arising from a representation of G. Then $\mathrm{Lie}(G) \simeq \mathfrak{g}_{\mathcal{R}}$.*

PROOF. We identify $\mathrm{Lie}(G)$ with the kernel of $G(k[\varepsilon]) \to G(k)$ (see 10.6). To give an element of $\mathrm{Lie}(G)$ is the same as giving 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 conditions (a, b, c) of Theorem 9.2. When written out, these conditions say exactly that the family (α_V) satisfies the conditions (a, b, c above, i.e., that $(\alpha_V)_{V \in \mathcal{R}} \in \mathfrak{g}_{\mathcal{R}}$.   □

Let $\mathsf{Rep}(\mathfrak{g})$ be the category of finite-dimensional representations of a Lie algebra $\mathfrak{g}$ over k. It has a tensor product, and the forgetful functor satisfies the conditions of Theorem 9.24, and so there is an affine group scheme $G(\mathfrak{g})$ such that

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

The set $\mathcal{R}$ of objects of $\mathsf{Rep}(\mathfrak{g})$ contains a faithful representation (Ado's theorem; 14.34), and so the homomorphism $\mathfrak{g} \to \mathfrak{g}_{\mathcal{R}}$ is injective. On composing this with the isomorphism in 23.69, we get a homomorphism $\eta \colon \mathfrak{g} \to \mathrm{Lie}(G(\mathfrak{g}))$.

THEOREM 23.70. *Let $\mathfrak{g}$ be a semisimple Lie algebra over a field k of characteristic zero.*

(a) *The homomorphism $\eta \colon \mathfrak{g} \to \mathrm{Lie}(G(\mathfrak{g}))$ is an isomorphism.*

(b) *The affine group scheme $G(\mathfrak{g})$ is a connected semisimple algebraic group.*

(c) *Let H be an algebraic group over k. The map $b \mapsto \mathrm{Lie}(b) \circ \eta$ is an isomorphism*
$$\mathrm{Hom}(G(\mathfrak{g}), H) \simeq \mathrm{Hom}(\mathfrak{g}, \mathrm{Lie}(H)).$$

(d) *If $\mathfrak{g}$ is split with root system (V, Φ), then the group G is split with diagram $(V, \Phi, P(\Phi))$.*

(e) *The group G is simply connected.*

PROOF. (a) It remains to prove that η is surjective. As $\mathfrak{g}$ is semisimple, its representations are semisimple (Weyl's theorem), and so $G(\mathfrak{g})^\circ$ is reductive (22.42). Therefore $G(\mathfrak{g})^\circ$ is an almost-direct product of almost-simple algebraic groups and a torus. Correspondingly, $\mathrm{Lie}(G(\mathfrak{g}))$ is a direct sum of simple Lie algebras and a commutative Lie algebra (21.56). If $\eta(\mathfrak{g})$ fails to contain one of these summands, there will be a nontrivial representation r of $G(\mathfrak{g})$ such that $\mathrm{Lie}(r)$ is trivial on $\mathfrak{g}$, contradicting the fact that η defines an equivalence $\mathsf{Rep}(G(\mathfrak{g})) \to \mathsf{Rep}(\mathfrak{g})$.

(b) The group scheme $G(\mathfrak{g})$ is of finite type over k because its Lie algebra is finite-dimensional. To show that it is connected, we have to show that its representations satisfy the condition in 9.50. This follows directly from the standard description of the representations of a semisimple Lie algebra (we can extend k and assume that $\mathfrak{g}$ is split). Finally, $G(\mathfrak{g})$ is semisimple because its Lie algebra is semisimple (23.68).

(c) From a we get an exact tensor functor

$$\mathsf{Rep}(H) \to \mathsf{Rep}(\mathfrak{h}) \xrightarrow{\ a^\vee\ } \mathsf{Rep}(\mathfrak{g}) \simeq \mathsf{Rep}(G(\mathfrak{g})),$$

and hence a homomorphism $b \colon G(\mathfrak{g}) \to H$, which acts as a on the Lie algebras.

(d) Let $\mathfrak{h}$ be a splitting Cartan algebra in $\mathfrak{g}$, so (V, Φ) is the root system of $(\mathfrak{g}, \mathfrak{h})$. Let T be the split torus over k with $X^*(T) = P(\Phi)$. Then $\mathsf{Rep}(T)$ can be identified with the category of finite-dimensional vector spaces with a $P(\Phi)$-gradation (12.13). Let (W, r) be a representation of $\mathfrak{g}$. The action of $\mathfrak{h}$ on

W defines a $P(\Phi)$-gradation on W. In this way we get an exact tensor functor from $\mathsf{Rep}(G)$ to the category of vector spaces with a $P(\Phi)$-gradation, which corresponds to an injective homomorphism $T \to G$ (see 9.28). This realizes T as a split maximal torus in G with character group $P(\Phi)$, and the diagram of (G,T) is $(V, \Phi, P(\Phi))$.

(e) We may extend the base field, and so assume that $\mathfrak{g}$ is split. Then the statement follows from Proposition 23.29 and (d).   □

The Cartan–Killing theorem (23.63) holds over an arbitrary field of characteristic zero (same proof, or use Chevalley bases as below), and so this completes the proof of the existence theorem over fields of characteristic zero.

Chevalley bases and adjoint groups

Let $(\mathfrak{g}, \mathfrak{t})$ be a simple Lie algebra over $\mathbb{C}$. Thus $(\mathfrak{g}, \mathfrak{t})$ corresponds to one of the Dynkin diagrams on p. 626. Let (V, Φ) be the root system of $(\mathfrak{g}, \mathfrak{t})$, and let $(\Delta, (e_\alpha)_{\alpha \in \Delta})$ be a pinning for (G, T). For each $\alpha \in \Delta$, there is a unique $e_{-\alpha}$ in $\mathfrak{g}_\alpha$ such that $t_\alpha = [e_\alpha, e_{-\alpha}]$ lies in $\mathfrak{t}$ and satisfies $\langle \alpha, t_a \rangle = 2$. For example, if $\mathfrak{g} = \mathfrak{sl}_2$, then

$$e_\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad t_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e_{-\alpha} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

are such elements, and in the general case, we let t_α and $e_{-\alpha}$ be the images of these elements under $\mathrm{Lie}(v_\alpha)$, where v_α corresponds to e_α as in (23.35).

There is a unique endomorphism θ of $\mathfrak{g}$ sending each e_α to $-e_{-\alpha}$ ($\alpha \in \Delta$) and acting as -1 on $\mathfrak{t}$. For example, if $\mathfrak{g} = \mathfrak{sl}_2$, then $\theta(X)$ is the transpose of $-X$. This is an involution of $\mathfrak{g}$, called the **opposition involution**. It is possible to extend the family $(e_\alpha)_{\alpha \in \Delta}$ to a family $(e_\alpha)_{\alpha \in \Phi}$ such that each e_α is a nonzero element of $\mathfrak{g}_\alpha$ and the equality $\theta(e_\alpha) = -e_{-\alpha}$ still holds. The family $\{t_\alpha, \alpha \in \Delta; e_\alpha, \alpha \in \Phi\}$ is then a basis for $\mathfrak{g}$, called a **Chevalley basis**. Given a pinning, the elements of a Chevalley basis are uniquely determined up to sign. This lack of uniqueness of the signs causes difficulties for the theory.

Let $\{t_\alpha, \alpha \in \Delta; e_\alpha, \alpha \in \Phi\}$ be a Chevalley basis. For $\alpha, \beta \in \Phi$, write

$$[e_\alpha, e_\beta] = \begin{cases} N_{\alpha, \beta} e_{\alpha+\beta} & \text{if } \alpha + \beta \in \Phi \\ 0 & \text{if } \alpha + \beta \notin \Phi, \quad \alpha + \beta \neq 0. \end{cases}$$

The $N_{\alpha, \beta}$ defined by these equations are the structure constants of $\mathfrak{g}$ relative to the given Chevalley basis. They determine the multiplication table for $\mathfrak{g}$.

THEOREM 23.71. *If α and β are roots such that $\alpha + \beta$ is a root, then*

$$N_{\alpha, \beta} = \pm(p+1)$$

where $p = p_{\alpha, \beta}$ is the greatest integer such that $\beta - p\alpha$ is a root.

PROOF. This was originally proved in Chevalley 1955a. For recent proofs, see Casselman 2015 and Raghunathan 2015. □

Let $\mathfrak{g}(\mathbb{Z})$ be the $\mathbb{Z}$-submodule of $\mathfrak{g}$ generated by the elements of a Chevalley basis. The theorem shows that $\mathfrak{g}(\mathbb{Z})$ is a Lie algebra over $\mathbb{Z}$ such that $\mathfrak{g}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} \simeq \mathfrak{g}$, i.e., $\mathfrak{g}(\mathbb{Z})$ is a $\mathbb{Z}$-structure on $\mathfrak{g}$. The isomorphism class of $\mathfrak{g}(\mathbb{Z})$ as a Lie algebra over $\mathbb{Z}$ does not depend on the choice of the Chevalley basis.

For every field k, there is a unique homomorphism $\mathbb{Z} \to k$, and $\mathfrak{g}(k) \overset{\text{def}}{=} \mathfrak{g}(\mathbb{Z}) \otimes_{\mathbb{Z}} k$ is a split semisimple Lie algebra over k. In this way, we obtain, for every root system (V, Φ) and field k, a split semisimple Lie algebra over k. It is called **the split semisimple Lie algebra of type** (V, Φ) over k.

The Lie algebra $\mathfrak{g}(k)$ is equipped with a family of homomorphisms $u_\alpha \colon \mathbb{G}_a \to \underline{\mathrm{Aut}}(\mathfrak{g}(k))$ indexed by the roots $\alpha \in \Phi$. The algebraic subgroup of $\underline{\mathrm{Aut}}(\mathfrak{g}(k))$ generated by the u_α is a split semisimple algebraic group over k with diagram $(V, \Phi, \mathbb{Z}\Phi)$, i.e., it is the split adjoint group with root system (V, Φ).

Semisimple algebraic groups over arbitrary fields

A remarkable feature of the classification of split semisimple algebraic groups over a field k in terms of diagrams is that it is independent of the field k. This suggests that the existence problem should have a solution over $\mathbb{Z}$. More precisely, given a diagram (V, Φ, X), there should exist a smooth group scheme G over $\mathbb{Z}$ such that, for every homomorphism $\mathbb{Z} \to k$ from $\mathbb{Z}$ into a field k, the group scheme $G_k \overset{\text{def}}{=} G \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(k)$ is a split semisimple group over k with diagram (V, Φ, X). In fact, such a G does exist.

Since the Tannakian theory works over $\mathbb{Z}$ (with some caveats) one might try to construct G by constructing its category representations. This works, but requires a heavy machinery (Mirković and Vilonen 2007; Prasad and Yu 2006). The original, more elementary, strategy of Chevalley is to choose a lattice in some representation of $G_{\mathbb{C}}$ and realize G as a group of automorphisms of the lattice.

As before, let $(\mathfrak{g}, \mathfrak{t})$ be a split semisimple Lie algebra over $\mathbb{C}$. We fix a Chevalley basis $\{t_\alpha, \alpha \in \Delta; e_\alpha, \alpha \in \Phi\}$ for $(\mathfrak{g}, \mathfrak{t})$. The choice of the Chevalley basis allows us to regard $(\mathfrak{g}, \mathfrak{t})$ as a Lie algebra over $\mathbb{Q}$.

Let (W, ρ) be a finite-dimensional faithful representation of $\mathfrak{g}$ over $\mathbb{Q}$. We know (23.70) that there exists a split almost-simple algebraic group G over $\mathbb{Q}$ such that $\mathsf{Rep}(G) = \mathsf{Rep}(\mathfrak{g})$. In particular, there exists a representation r of G on W with $dr = \rho$.

According to Lemma 23.35, the elements $e_\alpha \in \mathfrak{u}_\alpha, \alpha \in \Phi$, determine a homomorphism $u_\alpha \colon \mathbb{G}_a \to G$. Let $\exp(e_\alpha) = u_\alpha(1) \in U_\alpha(k)$. Then $\rho(e_\alpha)$ is nilpotent, and

$$r(\exp(e_\alpha)) = \mathrm{id} + \rho(e_\alpha) + \rho(e_\alpha)^2/2 + \cdots$$

(see 14.28). Let T be the subtorus of G with Lie algebra $\mathfrak{t}$, and let $\Psi(r)$ be the set of weights of T on W, so $W = \bigoplus_{\chi \in \Psi(r)} W_\chi$. Then $r(T)$ is the subtorus of GL_W whose elements act as scalars on each space W_χ.

For each $\alpha \in \Phi$, let G_α be the subgroup of GL_W generated the maps $r|T$, u_α, and $u_{-\alpha}$. Then the groups G_α satisfy the hypotheses of Theorem 23.31 and generate a semisimple group $G(r)$ over $\mathbb{Q}$ with diagram $(X(T)_\mathbb{Q}, \Phi, X(r))$, where $X(r)$ is the sublattice of $X^*(T)_\mathbb{Q}$ generated by the weights of r. In this case, it is just the image of G in GL_W.

To obtain a similar statement for base fields of nonzero characteristic, we need a result of Chevalley.

As before, let (W, ρ) be a finite-dimensional faithful representation of $\mathfrak{g}$ over $\mathbb{Q}$, and let $W(\mathbb{Z})$ be a lattice in W (so $W(\mathbb{Z}) \otimes_\mathbb{Z} \mathbb{Q} \simeq W$). Such a lattice $W(\mathbb{Z})$ is said to be **admissible** if

$$\frac{\rho(e_\alpha)^m}{m!} W(\mathbb{Z}) \subset W(\mathbb{Z}), \quad \text{all } \alpha \in \Phi, m \in \mathbb{N}.$$

Chevalley (1961) showed that an admissible lattice always exists.

Let $W(\mathbb{Z})$ be an admissible lattice. Then

$$W(\mathbb{Z}) = \bigoplus_{\chi \in \Psi(r)} W_\chi \cap W(\mathbb{Z}) \tag{152}$$

(Borel 1970, 2.3). Choose a basis for the $\mathbb{Z}$-module $W(\mathbb{Z})$ containing a basis for each submodule $W_\chi \cap W(\mathbb{Z})$. Let $\alpha \in \Phi$. For every $\mathbb{Z}$-algebra R, we have a homomorphism

$$c \mapsto \sum_{m \geq 0} \frac{\rho(e_\alpha)^m}{m!} c^m : R \to \mathrm{Aut}_R(W(\mathbb{Z}) \otimes_\mathbb{Z} R). \tag{153}$$

Now consider a homomorphism $\mathbb{Z} \to k$ with k a field, and let $W(k) = W(\mathbb{Z}) \otimes_\mathbb{Z} k$. From (152), we get a decomposition of the k-vector space

$$W(k) = \bigoplus_{\chi \in \Psi(r)} W_\chi.$$

Define $T(r)$ to be the subtorus of $\mathrm{GL}_{W(k)}$ whose elements act as scalars on the W_χ. For each α, the homomorphisms (153) for R a k-algebra determine a homomorphism

$$u_\alpha : \mathbb{G}_a \to \mathrm{GL}_{W(k)}$$

of algebraic groups over k.

THEOREM 23.72. *Let $G(r)$ be the algebraic subgroup of $\mathrm{GL}_{W(k)}$ generated by the maps u_α for $\alpha \in \Phi$. Then the pair $(G(r), T(r))$ is a split semisimple algebraic group over k with semisimple root datum $(X(r), \Phi)$, where $X(r)$ is the sublattice of $X^*(T(r)) \otimes \mathbb{Q}$ generated by the weights of r. The Lie algebra of $G(r)$ is canonically isomorphic to $\mathfrak{g}(\mathbb{Z}) \otimes_\mathbb{Z} k$.*

PROOF. The chosen $\mathbb{Z}$-basis for $W(\mathbb{Z})$ determines a k-basis for $W(k)$, and we let T denote the corresponding maximal torus of $\mathrm{GL}_{W(k)}$. For each $\alpha \in \Delta$, let G_α denote the algebraic subgroup of $\mathrm{GL}_{W(k)}$ generated by T and $u_{\pm\alpha}$. The

pairs (G_α, T) in $\mathrm{GL}_{W(k)}$ satisfy the hypotheses of Theorem 23.31, and so the G_α generate a reductive subgroup G of $\mathrm{GL}_{W(k)}$ with maximal torus T such that Δ is a base for the root system of (G, T). The derived group of G is the required algebraic subgroup $G(r)$. We omit the details. □

COROLLARY 23.73. *For every root system (V, Φ) and every field k, there exists a split semisimple algebraic group (G, T) over k with semisimple root datum $(P(\Phi), \Phi)$.*

PROOF. As the $\mathbb{Z}$-module $P(\Phi)$ is generated by the fundamental weights, Lemma 22.24 shows that a suitable sum of representations will have $X(r) = P(\Phi)$. □

NOTES. Apart from the original articles of Chevalley, the basic reference for the existence theorem is the lecture notes Steinberg 1967. Kostant (1966) suggested a more direct method of defining the Hopf algebra of $G/\mathbb{Z}$. This is elaborated in Lusztig 2009.

Reductive groups over $\mathbb{Z}$

In fact, Chevalley and Steinberg showed that, in the situation of the last subsection, there exists a smooth group scheme of finite type $G(r, \mathbb{Z})$ over $\mathbb{Z}$ such that, for every homomorphism $\mathbb{Z} \to k$, the algebraic group $G(r, k)$ is obtained from $G(r, \mathbb{Z})$ by extension of scalars. In his thesis, Demazure extended these results to reductive groups.

THEOREM 23.74. *For every reduced root datum $\mathcal{R}$, there exists a smooth group scheme G of finite type over $\mathbb{Z}$ and a split torus $T \subset G$ such that, for every homomorphism $\mathbb{Z} \to k$, the pair $(G, T)_k$ is a split reductive group over k with root datum $\mathcal{R}$. Moreover, (G, T) is unique up to isomorphism.*

PROOF. See Demazure 1965 and SGA 3, XXV. □

The starting point of the proof of Theorem 23.74 in SGA 3 is the Cartan–Killing theorem 23.63. To construct G, it suffices to define a (torsion-free) $\mathbb{Z}$-structure on the Hopf algebra $\mathcal{O}(G)$ such that $\mathrm{Spec}(\mathcal{O}(G) \otimes_{\mathbb{Z}} \mathbb{F}_p)$ is a split reductive group of the correct type for all p. The tori can be recovered from gradations on the representations.

Following Steinberg 1967, split semisimple algebraic groups over $\mathbb{Z}$ or a field k, are often called ***Chevalley groups***.

Exercises

EXERCISE 23-1. Let G and G' be reductive groups over k, and let k' be an algebraically closed field containing k. Show that every isogeny $G_{k'} \to G'_{k'}$ is defined over the algebraic closure of k in k'.

Construction of the Semisimple Groups

All reductive groups can be constructed from semisimple groups and tori (19.29). In the first section of this chapter, we explain how to express all semisimple algebraic groups in terms of those that are simply connected and geometrically almost-simple, and in the remainder of the chapter we explain how to construct all geometrically almost-simple groups. In particular, for each field k and indecomposable Dynkin diagram $\mathcal{D}$, we exhibit a split simply connected group over k with Dynkin diagram $\mathcal{D}$. Throughout, $\Gamma = \mathrm{Gal}(k^s/k)$.

a. Deconstructing semisimple algebraic groups

Recall that a semisimple group G over k is geometrically almost-simple if G_{k^a} is almost-simple.

PROPOSITION 24.1. *The following conditions on a split semisimple group G over k are equivalent: (a) G is almost-simple; (b) the root system of G is indecomposable; (c) G is geometrically almost-simple.*

PROOF. (a)$\Leftrightarrow$(b). Choose a maximal split torus T in G. If the root system of (G, T) decomposes into a product, then the root datum of (G, T) is isogenous to a product of root data, and (G, T) is isogenous to a product (23.56). Conversely, if G is isogenous to $G_1 \times G_2$, then the root system of G is isomorphic to the product of the root systems of G_1 and G_2.

(a)$\Leftrightarrow$(c). The follows from the equivalence of (a) and (b) because the root system of (G, T) equals that of $(G, T)_{k^a}$. □

COROLLARY 24.2. *An almost-simple group over a separably closed field is geometrically almost-simple.*

PROOF. It is automatically split. □

Let G be a semisimple group over k, and let $\{G_1, \ldots, G_r\}$ be the set of almost-simple normal subgroup varieties of G_{k^s}. According to Theorem 21.51, there is an isogeny

$$(g_1, \ldots, g_r) \mapsto g_1 \cdots g_r \colon G_1 \times \cdots \times G_r \to G_{k^s}. \tag{154}$$

When G is simply connected, this becomes an isomorphism

$$G_{k^s} \simeq G_1 \times \cdots \times G_r. \tag{155}$$

Let G be a simply connected semisimple group over k. When we apply an element σ of Γ to (155), it becomes $G_{k^s} \simeq \sigma G_1 \times \cdots \times \sigma G_r$ with $\{\sigma G_1, \ldots, \sigma G_r\}$ a permutation of $\{G_1, \ldots, G_r\}$. In this way, we get a continuous action of Γ on the set $\{G_1, \ldots, G_r\}$. Let $H_1, \ldots, H_s$ denote the products of the G_i in the different orbits for this action. Then $\sigma H_i = H_i$, and so H_i is defined over k as a subgroup of G (see 1.54). Now

$$G = H_1 \times \cdots \times H_s$$

is a decomposition of G into a product of almost-simple groups over k.

If G is almost-simple, then Γ acts transitively on the set $\{G_1, \ldots, G_r\}$. Let Δ be the set of $\sigma \in \Gamma$ such that $\sigma G_1 = G_1$, and let $K = (k^s)^\Delta$. Then $\operatorname{Hom}_k(K, k^s) \simeq \Gamma/\Delta$ and G_1 is defined over K as a subgroup of G_K. The Weil restriction of G_1 is an algebraic group $(G_1)_{K/k}$ over k equipped with an isomorphism

$$((G_1)_{K/k})_{k^s} \simeq G_1 \times \cdots \times G_r = G_{k^s}$$

(see 2.61). This isomorphism is Γ-equivariant, and so it is defined over k:

$$(G_1)_{K/k} \simeq G.$$

THEOREM 24.3. *Let G be a simply connected semisimple group over k. Let S be the set of almost-simple normal subgroup varieties of G_{k^s}, and let $\{G_1, \ldots, G_s\}$ be a set of representatives for the orbits of Γ acting on S. Then*

$$G \simeq (G_1)_{k_1/k} \times \cdots \times (G_s)_{k_s/k}$$

where k_i is the field of definition of G_i as a subgroup of G. Each group G_i is geometrically almost-simple and $(G_i)_{k_i/k}$ is almost-simple.

PROOF. Let H_i be the product of the groups in the orbit of G_i. According to the above discussion, H_i is defined over k (as a subgroup of G) and is almost-simple; moreover, $H_i \simeq (G_i)_{k_i/k}$ and $G \simeq H_1 \times \cdots \times H_s$. □

If G is adjoint, then the map (154) is again an isomorphism, and Theorem 24.3 holds for G with "simple" for "almost-simple". For a general semisimple group G, the best we can say is that G is the quotient by a central subgroup of an algebraic group of the form

$$(G_1)_{k_1/k} \times \cdots \times (G_s)_{k_s/k}$$

with k_i/k separable and G_i simply connected almost-simple. Therefore, to understand all semisimple groups, it suffices to understand the simply connected almost-simple groups and their centres.

ASIDE 24.4. Here is a more canonical statement of Theorem 24.3. Let G and S be as in the theorem. Then S is a finite set with a continuous action of Γ, and we let E denote the étale k-algebra with $\mathrm{Hom}_k(E, k^s) \simeq S$ (see A.62). The element G_σ of S corresponding to an element σ of $\mathrm{Hom}_k(E, k^s)$ is defined over the subfield σE of k^s (as a subgroup of G). Let G' denote the algebraic group over E such that $\sigma(G') = G_\sigma$ for all σ. Then $(G')_{E/k}$ is an algebraic group over k equipped with an isomorphism $((G')_{E/k})_{k^s} \simeq \prod_\sigma G_\sigma$ (see 2.62). The composite of this with the isomorphism (154) is Γ-equivariant, and so it is defined over k; thus $(G')_{E/k} \simeq G$.

b.   Generalities on forms of semisimple groups

24.5. Let (G, T) be a split semisimple group over k, and let B be a Borel subgroup of G containing T. The triple (G, B, T) determines a based semisimple root datum (X, Φ, Δ), which in turn determines a Dynkin diagram $\mathcal{D}$ whose nodes are indexed by the elements of Δ. Recall (23.46) that $\mathrm{Out}(G) \simeq \mathrm{Aut}(X, \Phi, \Delta)$. Assume that G is simply connected. Then $X = P(\Phi)$ and the group of automorphisms of (X, Φ, Δ) is isomorphic to the group $\mathrm{Sym}(\mathcal{D})$ of symmetries of $\mathcal{D}$ (see C.53 and the following discussion). Therefore, there is an exact sequence

$$1 \to G^{\mathrm{ad}}(k) \to \mathrm{Aut}(G) \to \mathrm{Sym}(\mathcal{D}) \to 1.$$

Any choice of a pinning for (G, T) splits the sequence (23.47).

24.6. Let G be a simply connected semisimple group G over k and T a maximal torus in G. Then $(G, T)_{k^s}$ is split and so the choice of a Borel subgroup B containing T_{k^s} determines a based semisimple root datum (X, Φ, Δ). There is a natural action of Γ on $X \overset{\mathrm{def}}{=} X^*(T)$ which preserves the subset Φ. If σ is an element of Γ, then $\sigma(\Delta)$ is also a base for Φ, and so $w_\sigma(\sigma(\Delta)) = \Delta$ for a unique $w_\sigma \in W$ (see 21.41). For $\alpha \in \Delta$, define $\sigma * \alpha = w_\sigma(\sigma\alpha)$. One checks that this defines an action of Γ on Δ, which is obviously continuous. Using that the nodes of $\mathcal{D}$ are indexed by the elements of Δ, we obtain an action of Γ on $\mathcal{D}$, called the *-**action**. When G is split, the $*$-action of Γ on $\mathcal{D}$ is trivial. When G is quasi-split, we can choose a Borel pair (B, T) in G and define (X, Φ, Δ) to be the based semisimple root datum attached to $(G, B, T)_{k^s}$. In this case, Δ is stable under the action of Γ on X, and the $*$-action on Δ is induced by the natural action of Γ on X.

24.7. Let (G, T) be as in 24.6. Because $(G, T)_{k^s}$ is split, we have an exact sequence (24.5),

$$1 \to G^{\mathrm{ad}}(k^s) \to \mathrm{Aut}(G_{k^s}) \to \mathrm{Sym}(\mathcal{D}) \to 1. \tag{156}$$

We claim that this is Γ-equivariant for the $*$-action of Γ on $\mathcal{D}$. When G is quasi-split, it is obvious that the map $\mathrm{Aut}(G_{k^s}) \to \mathrm{Sym}(\mathcal{D})$ is Γ-equivariant. In

the general case, G is an inner form of a quasi-split group G' (see 23.53), say, that defined by a 1-cocycle $f : \Gamma \to \operatorname{Aut}(G'_{k^s})$. Now the sequence (156) for G can be obtained from that for G' by twisting using f. It follows that the maps are equivariant.

The cohomology sequence of (156) is an exact sequence

$$\cdots \to \operatorname{Sym}(\mathcal{D})^{\Gamma} \to H^1(\Gamma, G^{\mathrm{ad}}(k^s)) \to H^1(\Gamma, \operatorname{Aut}(G_{k^s})) \to H^1(\Gamma, \operatorname{Sym}(\mathcal{D})).$$

When (G, T) is split, the sequence (156) splits (see 23.47), and so we get short exact sequences

$$1 \to G^{\mathrm{ad}}(k) \to \operatorname{Aut}(G) \to \operatorname{Sym}(\mathcal{D}) \to 1$$
$$1 \to H^1(\Gamma, G^{\mathrm{ad}}(k^s)) \to H^1(\Gamma, \operatorname{Aut}(G_{k^s})) \to H^1(\Gamma, \operatorname{Sym}(\mathcal{D})) \to 1.$$

24.8. Let (G, T) be as in 24.6, and let $\underline{\operatorname{Aut}}(\mathcal{D})$ denote the étale group scheme over k corresponding to the finite Γ-set $\operatorname{Sym}(\mathcal{D})$. We claim that there is an exact sequence of smooth algebraic groups over k

$$e \to G^{\mathrm{ad}} \to \underline{\operatorname{Aut}}(G) \to \underline{\operatorname{Aut}}(\mathcal{D}) \to e \tag{157}$$

that becomes (156) on k^s-points. When (G, T) is split, we define $\underline{\operatorname{Aut}}(G)$ to be a disjoint union of copies of G^{ad} indexed by the elements of $\operatorname{Sym}(\mathcal{D})$, and we endow it with the obvious extension of the multiplication on G^{ad}. In general, (G, T) can be obtained from a split pair (G', T') by twisting by a 1-cocycle $f : \Gamma \to \operatorname{Aut}(G'_{k^s})$. Then the sequence for G is obtained from the sequence for G' by twisting each term by f.

24.9. Let G be a semisimple algebraic group over k, and let $\pi : \tilde{G} \to G$ be its simply connected covering. Then

$$\operatorname{Aut}(G) \simeq \{\alpha \in \operatorname{Aut}(\tilde{G}) \mid \alpha(\operatorname{Ker}(\pi)) \subset \operatorname{Ker}(\pi)\}.$$

Certainly, an automorphism of $\tilde{G}$ induces an automorphism of G if it maps the kernel of π into itself. That all automorphisms of G arise (uniquely) in this way follows from the universality of the universal covering. If the kernel of $\tilde{G} \to G$ is characteristic in $\tilde{G}$, for example, if G is an adjoint group, then $\operatorname{Aut}(G_{k'}) \simeq \operatorname{Aut}(\tilde{G}_{k'})$ and there are exact sequences (156) and (157).

24.10. Let G be a semisimple group over k. There exists a split semisimple group G_0 over k, unique up to isomorphism, that becomes isomorphic to G over k^s (see 23.57). We call G_0 the **split form** of G, and we say that G is **inner** or **outer** according as it is an inner or outer form of its split form.

24.11. Now let G_0 be a split semisimple group over k, and assume that G_0 is simply connected and almost-simple. We know that such groups are classified by their Dynkin diagrams (23.62), which are listed on p. 626. Thus, each such group is of type 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, or

G_2. Every k-form G of G_0 defines a cohomology class in $H^1(\Gamma, \mathrm{Aut}(G_{0k^s}))$. If γ lies in the subset $H^1(\Gamma, G_0^{\mathrm{ad}}(k^s))$, then G is an inner form of G_0. Otherwise it maps to a nontrivial element in

$$H^1(k, \mathrm{Sym}(\mathcal{D})) = \mathrm{Hom}(\Gamma, \mathrm{Sym}(\mathcal{D})) \quad \text{(continuous homomorphisms).}$$

Let Δ denote the kernel of this homomorphism and L its fixed field $(k^s)^\Delta$. Then G becomes an inner form of G_0 over L. As G_0 is geometrically almost-simple, so also is G. If G_0 has type X_y, then we say that G has type ${}^zX_y$, where $z = [L{:}k] = (\Gamma{:}\Delta)$. For example, to say that G is of type ${}^3D_4$ means that it is an outer form of type D_4 and becomes an inner form over a cubic extension of k.

24.12. The indecomposable Dynkin diagrams have few symmetries:

Type	$\mathrm{Sym}(\mathcal{D})$	Nontrivial symmetries
A_n $(n > 1)$	$\mathbb{Z}/2\mathbb{Z}$	reflection about centre
D_4	S_3	permutations of three outer nodes
D_n $(n > 4)$	$\mathbb{Z}/2\mathbb{Z}$	reflection about axis
E_6	$\mathbb{Z}/2\mathbb{Z}$	reflection about centre
remainder	1	

Thus z is 1 or 2 except for D_4, for which it can be 1, 2, 3, or 6.

24.13. Let G be a semisimple group. When G is simply connected and geometrically almost-simple, we say that G is *classical* if it is of type A_n, B_n, C_n, or D_n, but not of subtype ${}^3D_4$ or ${}^6D_4$, and it is *exceptional* if it is of type E_6, E_7, E_8, F_4, or G_2. A general semisimple group G is *classical* (resp. *exceptional*) if, in the decomposition $\tilde{G} \simeq \prod(G_i)_{k_i/k}$ in 24.3, all G_i are classical (resp. exceptional). Groups of subtypes ${}^3D_4$ or ${}^6D_4$ are neither exceptional nor classical.

In more down-to-earth terms, the geometrically almost-simple simply connected classical groups over k are the k-forms of SL_{n+1}, Sp_{2n}, and Spin_n (see below), except for some k-forms of Spin_8. Each is an inner form or becomes so over a quadratic extension of k. Weil restrictions of classical groups are classical, products of classical groups are classical, and every group isogenous to a classical group is classical. In this chapter, we show that all the geometrically almost-simple classical groups can be described in terms of associative algebras.

c. The centres of semisimple groups

Let (G, T) be a split semisimple group over k. The centre $Z(G)$ of G is the diagonalizable group whose character group is $X(T)/\mathbb{Z}\Phi$ with Γ acting trivially (21.8). Thus,

$$Z(G) = \prod_i \mu_{n_i} \iff X(T)/\mathbb{Z}\Phi = \bigoplus_i \mathbb{Z}/n_i\mathbb{Z}.$$

If G is simply connected, then $X(T)$ is the weight lattice $P(\Phi)$ (23.29), and so the character group of $Z(G)$ is isomorphic to $P(\Phi)/Q(\Phi)$. Choose a base

Δ for Φ. Then $P(\Phi)/Q(\Phi)$ is canonically isomorphic to the cokernel of the map $\mathbb{Z}^n \to \mathbb{Z}^n$ defined by the Cartan matrix $(\langle \alpha, \beta^\vee \rangle)_{\alpha,\beta \in \Delta}$. From the tables in Bourbaki 1968, one arrives at the following table of centres for the simply connected split almost-simple groups:

A_n	B_n	C_n	D_{2m}	D_{2m+1}	E_6	E_7	$E_8, F_4 G_2$
μ_{n+1}	μ_2	μ_2	$\mu_2 \times \mu_2$	μ_4	μ_3	μ_2	e

For example, the simply connected split almost-simple group of type A_n is SL_{n+1}. This has centre μ_{n+1}, which is the diagonalizable group whose character group is $\mathbb{Z}/(n+1)\mathbb{Z}$ with Γ acting trivially. Note that the centre need not be étale.

Let $\Gamma = \mathrm{Gal}(k^s/k)$. Let G_0 and G be algebraic groups over k with centres Z_0 and Z. If G is obtained from G_0 by twisting by a cocycle in $Z^1(\Gamma, \mathrm{Aut}(G_{0k^s}))$, then $Z(G)$ is obtained from $Z(G_0)$ by twisting with the same cocycle. Specifically, let $f: G_{0k^s} \to G_{k^s}$ be an isomorphism over k^s. Write $a_\sigma = f^{-1} \circ \sigma f$, $\sigma \in \Gamma$. Then f restricts to an isomorphism $f|Z_0: Z_0 \to Z$ and $(f^{-1} \circ \sigma f)|Z_0 = a_\sigma|Z_0$. Note that f defines an isomorphism $f: Z_0(k^s) \to Z(k^s)$ and $f(a_\sigma \sigma x) = \sigma(f(x))$. When we use f to identify $Z_0(k^s)$ with $Z(k^s)$, this says that Γ acts on $Z(k^s)$ by the twisted action

$$^\sigma x = a_\sigma \cdot \sigma x.$$

Let (G, f) be an inner form of G_0 (see 3.52). Then the automorphism $a_\sigma = f^{-1} \circ \sigma f$ of G_0 is inner, and so it acts trivially on the centre. Hence $f|Z_0 = \sigma(f|Z_0)$ for all $\sigma \in \Gamma$, and so $f|Z_0$ is defined over k (see A.66). If (G, f) and (G', f') are equivalent inner forms, then

$$Z(G) \simeq Z(G_0) \simeq Z(G').$$

In other words, the centre of G depends only on the equivalence class of (G, f), and is canonically isomorphic to the centre of G_0.

We now have a procedure for computing the centre of any simply connected semisimple group G. Write

$$G \simeq (G_1)_{k_1/k} \times \cdots \times (G_s)_{k_s/k}$$

as in 24.3. Then G_i is the twist by a 1-cocycle of the split group H_i of the same type over k_i, and $Z(G_i)$ is the twist of $Z(H_i)$ by the same cocycle. Now

$$Z(G) \simeq (Z(G_1))_{k_1/k} \times \cdots \times (Z(G_s))_{k_s/k}.$$

The connected algebraic groups isogenous to G are the quotients of G by algebraic subgroups of $Z(G)$. These correspond to quotients of $X^*(Z(G))$ by Γ-stable subgroups.

d.   Semisimple algebras

For the remainder of the chapter, all algebras A over k and their modules are finite-dimensional as k-vector spaces. The dimension of an algebra A as a k-vector space k is called its **degree**[1] and is denoted $[A:k]$.

DEFINITION 24.14. An algebra A over k is **central** if its centre is k, and it is a **division algebra** if every nonzero element has an inverse. It is **simple** if it contains no two-sided ideals (except 0 and A), and it is **semisimple** if every A-module is semisimple.

EXAMPLE 24.15. The matrix algebra $M_n(k)$ is central and simple. For all $a, b \in k^\times$, the quaternion algebra $H(a,b)$ (see p. 421) is central and simple.

We shall need to use the following five basic theorems, which are proved, for example, in Jacobson 1989.

THEOREM 24.16. *Let A be a simple algebra over k and S a simple A-module. Then every A-module is isomorphic to S^m for some m.*

For example, every $M_n(k)$-module is isomorphic to a direct sum of copies of k^n. Note that the theorem implies that simple algebras over k are semisimple, and so finite products of simple algebras over k are semisimple.

THEOREM 24.17. *If D is a division algebra over k, then $M_n(D)$ is a simple algebra over k, and every simple algebra over k is of this form. Moreover $M_n(D) \approx M_{n'}(D')$ if and only if $n = n'$ and $D \approx D'$.*

In particular, the centre of a simple algebra over k is a field (because the centre of a division algebra D is obviously a field, and the centre of $M_n(D)$ equals that of D).

THEOREM 24.18. *A semisimple algebra A over k has only finitely many minimal two-sided ideals $A_1, \dots, A_r$. Each A_i is a simple k-algebra, and $A = A_1 \times \cdots \times A_r$.*

In particular, a semisimple k-algebra is simple if its centre is a field.

THEOREM 24.19. *A central simple algebra over k remains central simple when tensored with a field k' containing k.*

THEOREM 24.20. *Let D be a central division algebra over k, and let L be a subfield of D that is maximal among the separable extensions of k in D. Then $D \otimes_k L$ is isomorphic to a matrix algebra over L.*

PROPOSITION 24.21. *The only central simple algebras over a separably closed field k are the matrix algebras $M_n(k)$.*

---

[1]The degree of a central simple algebra A over k is a square n^2. We call n the reduced degree of A over k; some authors call it the degree of A over k.

PROOF. A central simple algebra over k is of the form $M_n(D)$ with D a central division algebra over k (see 24.17). As k is separably closed, the subfield L in 24.20 equals k, and so D is a matrix algebra over k. This implies that $D = k$. $\square$

PROPOSITION 24.22. *The k^s/k-forms of $M_n(k)$ are the central simple algebras over k of degree n^2.*

PROOF. Let A be a central simple algebra over k. Then $A \otimes k^s$ is again central simple (24.19), and so it is isomorphic to $M_n(k)$ with $n^2 = [A:k]$ (see 24.21). Conversely, if A is an algebra over k that becomes isomorphic to $M_n(k^s)$ over k^s, then it is obviously central simple of degree n^2. $\square$

THEOREM 24.23 (SKOLEM, NOETHER). *Every automorphism of a simple algebra A over k is inner, i.e., of the form $a \mapsto bab^{-1}$ for some $b \in A^{\times}$.*

PROOF. Let α be an automorphism of A. We first suppose that $A = M_n(k)$. Then $S = k^n$ is an A-module, and we let S' denote k^n with $a \in A$ acting as $\alpha(a)$. Now S and S' are both simple A-modules, and so there is an A-isomorphism $f: S \to S'$ (see 24.16). This is an isomorphism of k-vector spaces $f: k^n \to k^n$ with the property $\alpha(a) f(x) = f(ax)$ for all $a \in A$ and $x \in k^n$. Now f is multiplication by an invertible matrix b such that $\alpha(a)b = ba$, i.e., such that $\alpha(a) = bab^{-1}$.

In the general case, there exists a finite Galois extension k' of k such that $A \otimes k' \approx M_n(k')$ (see 24.19, 24.21). It follows that there exists a $b \in A_{k'}$ such that $\alpha_{k'}(a) = bab^{-1}$ for all $a \in A_{k'}$. On applying $\sigma \in \mathrm{Gal}(k'/k)$ to this equality, we find that $\sigma b = b \cdot c_{\sigma}$ with $c_{\sigma} \in k'^{\times}$. Now $\sigma \mapsto c_{\sigma}$ is a 1-cocycle, and so $c_{\sigma} = d^{-1} \cdot \sigma d$ for some $d \in k'^{\times}$ (see 3.39). The element bd^{-1} of $A_{k'}$ is fixed by all σ, and so lies in A_k, and $\alpha(a) = (bd^{-1})a(bd^{-1})^{-1}$ for all $a \in A$. $\square$

PROPOSITION 24.24. *The isomorphism classes of central simple algebras of degree n^2 over k are classified by $H^1(k, \mathrm{PGL}_n)$.*

PROOF. These are the k^s/k-forms of $M_n(k)$ (see 24.22). According to Theorem 24.23, $\mathrm{Aut}(M_n(k^s)) \simeq \mathrm{PGL}_n(k^s)$. Given an A over k, choose an isomorphism $f: M_n(k^s) \to k^s \otimes_k A$, and let $a_{\sigma} = f^{-1} \circ \sigma f$ for $\sigma \in \Gamma = \mathrm{Gal}(k^s/k)$. Then $(a_{\sigma})_{\sigma}$ is a continuous 1-cocycle whose cohomology class depends only on the k-isomorphism class of A. Conversely, given a continuous 1-cocycle $(a_{\sigma})_{\sigma}$, let

$$\sigma X = a_{\sigma} \cdot \sigma X, \quad \sigma \in \Gamma, \quad X \in M_n(k^s).$$

This defines an action of Γ on $M_n(k^s)$, and $M_n(k^s)^{\Gamma}$ is an algebra over k such that $M_n(k^s)^{\Gamma} \otimes_k k^s \simeq M_n(k^s)$ (cf. the proof of 3.37). $\square$

REMARK 24.25. Let A be a central simple algebra over k. For some n, there exists an isomorphism $f: A \otimes k^s \to M_n(k^s)$, unique up to an inner automorphism (24.22, 24.23). Let $a \in A$, and let $\mathrm{Nrd}(a) = \det(f(a))$. Then $\mathrm{Nrd}(a)$ does not depend on the choice of f. Moreover, it is fixed by Γ, and so lies in k. It is called the ***reduced norm*** of a.

Let A be an algebra over k. The **opposite algebra** A^{opp} has the same underlying k-vector space as A, but the multiplication is reversed: $a^{\mathrm{opp}}b^{\mathrm{opp}} = (ba)^{\mathrm{opp}}$. Let A_0 denote the underlying k-vector space of A. Then $A \otimes A^{\mathrm{opp}}$ acts k-linearly on A_0 by the rule

$$(a \otimes b)(x) = axb, \quad a \in A,\ b \in A^{\mathrm{opp}},\ x \in A_0.$$

PROPOSITION 24.26. *Let A be a central algebra over k. The map*

$$A \otimes A^{\mathrm{opp}} \to \mathrm{End}\,(A) \quad \text{(k-linear endomorphisms)}$$

defined by the above action is an isomorphism of algebras over k.

PROOF. The map is obviously injective and, as the source and target have the same dimension as k-vector spaces, this implies that it is an isomorphism. □

DEFINITION 24.27. An algebra over k is **separable** if it is semisimple and its centre is an étale k-algebra.

A semisimple algebra over k is separable if and only if the centre of each of its simple factors is a separable field extension of k.

PROPOSITION 24.28. *If A is separable, then $A \otimes k'$ is semisimple for all fields k' containing k.*

PROOF. We may suppose that the centre K of A is field. Then $K \otimes k' = \prod K_i$ with each K_i a separable extension of k', and

$$A \otimes_k k' \simeq A \otimes_K (K \otimes_k k') \simeq \prod_i A \otimes_K K_i.$$

Each algebra $A \otimes_K K_i$ is central and semisimple over K_i (see 24.19), and so $A \otimes_k k'$ is semisimple over k'. □

The converse is also true: if A is not separable, then either it is not semisimple or its centre K is not étale over k; in the second case, $A \otimes_k k'$ contains central nilpotents for some k', and so it is not semisimple.

e. Algebras with involution

DEFINITION 24.29. Let A be an algebra over k. An **involution** of A is a k-linear map $a \mapsto a^* \colon A \to A$ such that

$$1^* = 1, \quad (ab)^* = b^*a^*, \quad a^{**} = a, \quad \text{all } a,b \in A.$$

A **homomorphism** $(A, *) \to (B, \dagger)$ of algebras with involution over k is a homomorphism $\varphi \colon A \to B$ of algebras over k such that $\varphi(a^*) = \varphi(a)^{\dagger}$ for all $a \in A$.

An involution of A maps the centre of A into itself. If it fixes the elements of the centre, it is said to be of the **first kind**; otherwise it is of the **second kind**.

EXAMPLE 24.30. (a) On $M_n(k)$, the standard involution $X \mapsto X^t$ (transpose) is of the first kind.

(b) On a quaternion algebra $H(a,b)$, the standard involution

$$(a + bi + cj + dij)^* = a - bi - cj + dij$$

is the unique involution of the first kind such that $\alpha^* \alpha \in k$ for all α.

(c) On an étale k-algebra of degree 2, there is a unique nontrivial involution.

LEMMA 24.31. *Let $(A, *)$ be an algebra over k with involution. An inner automorphism $x \mapsto axa^{-1}$ of A commutes with $*$ if and only if $a^* a$ lies in the centre of A.*

PROOF. To say that $\mathrm{inn}(a)$ and $*$ commute means that $ax^* a^{-1} = (a^*)^{-1} x^* a^*$ for all $x \in A$, i.e., that $a^* a x^* = x^* a^* a$ for all x. As $x \mapsto x^*$ is bijective, this holds if and only if $a^* a$ lies in the centre of A. □

REMARK 24.32. Let $(A, *)$ be a simple algebra over k with involution, and let K be the centre of A. Every automorphism of A is inner (24.23), and $\mathrm{inn}(a)$ respects $*$ if and only if $a^* a \in K^\times$. When we replace a with ca for some $c \in K^\times$, the automorphism $\mathrm{inn}(a)$ is unchanged but $a^* a$ becomes $c^* c \cdot a^* a$. When $*$ is of the first kind, so $c^* c = c^2$, and every element of K is a square, we can choose c to make $a^* a = 1$.

PROPOSITION 24.33. *Let A be a simple algebra over k with centre K, and let $*$ and $\dagger$ be involutions of A that agree on K. Then there exists an $a \in A^\times$ such that*

$$x^* = a x^\dagger a^{-1}, \quad \text{all } x \in A.$$

PROOF. Apply 24.23 to the automorphism $x \mapsto (x^*)^\dagger$ of the algebra A over K. □

PROPOSITION 24.34. *Let A be a simple algebra over k with centre K, and let $\dagger$ be an involution of A.*

(a) *If $\dagger$ is of the first kind, then the involutions of the first kind on A are the maps $x \mapsto a x^\dagger a^{-1}$, $a \in A^\times$, with $a^\dagger = \pm a$.*

(b) *If $\dagger$ is of the second kind, then the involutions $*$ on A agreeing with $\dagger$ on K are the maps $x \mapsto a x^\dagger a^{-1}$, $a \in A^\times$, with $a^\dagger = a$.*

PROOF. It is easy to see that $x \mapsto a x^\dagger a^{-1}$ is an involution of the correct type in case (a) if $a^\dagger = \pm a$, or in case (b) if $a^\dagger = a$. Now let $a \in A^\times$ be such that $x \mapsto x^* = a x^\dagger a^{-1}$ is an involution. Then

$$x = x^{**} = (a^\dagger a^{-1})^{-1} x (a^\dagger a^{-1}) \quad \text{for all } x \in A,$$

and so $a^\dagger a^{-1} \in K^\times$, say, $a^\dagger = ca$, $c \in K$. Now, $a = a^{\dagger\dagger} = cc^\dagger \cdot a$, and so $cc^\dagger = 1$. When $\dagger$ is of the first kind, this says that $c^2 = 1$, and so $c = \pm 1$. When $\dagger$ is of the second kind, the condition $cc^\dagger = 1$ implies that $c = d^\dagger / d$ for some $d \in K$ (see 3.42c). Since $*$ is unchanged when we replace a with a/d, we see that in this case $x^* = a x^\dagger a^{-1}$ for some a satisfying $a^\dagger = a$. □

EXAMPLE 24.35. Let V be a finite-dimensional vector space over k, and let ϕ be a nondegenerate k-bilinear form on V. For $\alpha \in \mathrm{End}(V)$, define α^* to be the endomorphism of V such that

$$\phi(\alpha^*(v), w) = \phi(v, \alpha(w)), \quad \text{all } v, w \in V.$$

In other words,

$$\alpha^* = \hat{\phi}^{-1} \circ \alpha^\vee \circ \hat{\phi}$$

where $\hat{\phi}$ is the isomorphism $V \to V^\vee$ such that $\hat{\phi}(v)(w) = \phi(v, w)$ for $v, w \in V$ and $\alpha^\vee$ is the map $V^\vee \to V^\vee$ such that $\alpha^\vee(f) = f \circ \alpha$ for $f \in V^\vee$. The map $\alpha \mapsto \alpha^*$ is an involution of the algebra $\mathrm{End}(V)$ over k if and only if ϕ is symmetric or skew-symmetric, in which case $*$ is called the **adjoint involution** of ϕ and denoted $*_\phi$. Every involution of the first kind on $\mathrm{End}(V)$ is the adjoint involution of some ϕ, and ϕ and ϕ' define the same involution if and only if $\phi' = c\phi$ for some $c \in k^\times$. These statements can be deduced from Proposition 24.34 by taking $\dagger$ to be the adjoint involution of some nondegenerate symmetric k-bilinear form.

PROPOSITION 24.36. *Let $(A, *)$ be a central simple algebra over k with an involution of the first kind. Then $(A, *) \otimes k^s \approx (\mathrm{End}(V), *_\phi)$ for some finite-dimensional k^s-vector space V and nondegenerate symmetric or skew-symmetric bilinear form ϕ on V.*

PROOF. Choose an isomorphism $A \otimes k^s \to \mathrm{End}(V)$ (see 24.19, 24.21), and apply 24.35 to the involution induced on $\mathrm{End}(V)$. □

DEFINITION 24.37. Let A be a central simple algebra over k. An involution $*$ on A of the first kind is of **orthogonal type** (resp. **symplectic type**) if $(A, *) \otimes k^s \approx (\mathrm{End}(V), *_\phi)$ with ϕ symmetric (resp. alternating).

For an algebra $(A, *)$ with involution over k, we define

$$\mathrm{Sym}(A, *) = \{a \in A \mid a^* = a\}$$
$$\mathrm{Skew}(A, *) = \{a \in A \mid a^* = -a\}.$$

PROPOSITION 24.38. *Let $(A, *)$ be a central simple algebra of degree n^2 over k with an involution of the first kind. Assume that $\mathrm{char}(k) \neq 2$. If $*$ is of orthogonal type, then*

$$\dim_k \mathrm{Sym}(A, *) = \frac{n(n+1)}{2}, \quad \dim_k \mathrm{Skew}(A, *) = \frac{n(n-1)}{2}.$$

If $*$ is of symplectic type, then

$$\dim_k \mathrm{Sym}(A, *) = \frac{n(n-1)}{2}, \quad \dim_k \mathrm{Skew}(A, *) = \frac{n(n+1)}{2}.$$

PROOF. As the conditions $a^* = a$ and $a^* = -a$ are linear, we may extend k and so assume that $A = M_n(k)$, and even that $*$ is one of the standard involutions. The statement is then obvious. □

EXAMPLE 24.39. For every algebra A over k, the map

$$\varepsilon: A \times A^{\mathrm{opp}} \to A \times A^{\mathrm{opp}}, \quad (a,b) \mapsto (b,a),$$

is an involution of the second kind of the k-algebra $A \times A^{\mathrm{opp}}$. It is called the **transpose involution** (other names: exchange involution; switch involution).

PROPOSITION 24.40. *Let $(A, *)$ be a separable algebra over k with an involution of the second kind. Let K be the centre of A, and assume that $k = \{a \in K \mid a^* = a\}$.*

- (a) *The centre K of $(A, *)$ is an étale k-algebra of degree two.*
- (b) *Let L be an extension of k such that $K \otimes_k L = K_1 \times K_2$, and let $A_1 = A \otimes_K K_1$. Then A_1 is a central simple algebra over K_1, and*

$$a \otimes c \mapsto (a \otimes c, a^* \otimes c): (A \otimes_k L, *) \simeq (A_1 \times A_1^{\mathrm{opp}}, \varepsilon)$$

is an isomorphism of algebras over k with involution.

PROOF. (a) The k-algebra K is étale because A is separable. That its degree over k is at most 2 is a standard result in Galois theory when K is a field, and otherwise we can apply A.62.

(b) The algebra A_1 over K_1 is semisimple, and hence a product of simple K_1-algebras (24.18). But its centre is K_1, and so A_1 itself must be simple. The map is the composite of the canonical isomorphisms

$$A \otimes_k L \simeq A \otimes_K (K \otimes_k L) = A \otimes_K (K_1 \times K_2)$$
$$\simeq (A \otimes_K K_1) \times (A \otimes_K K_2) \simeq A_1 \times A_1^{\mathrm{opp}}. \qquad \square$$

COROLLARY 24.41. *Let $(A, *)$ be as in the proposition. Then*

$$(A, *) \otimes k^{\mathrm{s}} \simeq (\mathrm{End}(V) \times \mathrm{End}(V)^{\mathrm{opp}}, \varepsilon)$$

for some finite-dimensional k^{s}-vector space V.

PROOF. Apply the proposition with $L = k^{\mathrm{s}}$. Then A_1 is a central simple algebra over k^{s}, and so it is of the form $\mathrm{End}(V)$ (see 24.21). $\qquad \square$

DEFINITION 24.42. A pair $(A, *)$ as in Proposition 24.40 is said to be **simple of unitary type**. In other words, an algebra with involution $(A, *)$ over k is simple of unitary type if $*$ is an involution of the second kind on A, the centre K of A is an étale k-algebra of degree 2, and A is either simple (case K is a field) or the product of two simple algebras (case $K = k \times k$).

f. The geometrically almost-simple groups of type A

Recall (p. 456) that the split simply connected almost-simple group of type A_{n-1} is SL_n. Thus, we need to find the forms of SL_n.

The inner forms of SL_n

When we embed $\mathrm{SL}_n(k^s)$ in $M_n(k^s)$,

$$X \mapsto X : \mathrm{SL}_n(k^s) \to M_n(k^s),$$

the action of $\mathrm{PGL}_n(k^s)$ on $M_n(k^s)$ by inner automorphisms preserves $\mathrm{SL}_n(k^s)$, and identifies $\mathrm{PGL}_n(k^s)$ with the full group of inner automorphisms of SL_n:

$$\mathrm{Inn}(\mathrm{SL}_{n,k^s}) \simeq \mathrm{Aut}(M_n(k^s)) \simeq \mathrm{PGL}_n(k^s).$$

The isomorphism classes of k-forms of M_n and inner k-forms of SL_n are both classified by $H^1(k, \mathrm{PGL}_n)$, and so they are in natural one-to-one correspondence.

　　We make this explicit. Recall that the k-forms of M_n are the central simple algebras A of degree n^2 over k (see 24.22). Given such an A, we let $\mathrm{SL}_1(A)$ denote the algebraic group over k such that

$$\mathrm{SL}_1(A)(R) = \{a \in (A \otimes R)^\times \mid \mathrm{Nrd}(a) = 1\}$$

for all k-algebras R.

THEOREM 24.43. *The inner forms of* SL_n *over* k *are the algebraic groups* $\mathrm{SL}_1(A)$ *for* A *a central simple algebra of degree* n^2 *over* k; *two algebraic groups* $\mathrm{SL}_1(A)$ *and* $\mathrm{SL}_1(A')$ *are isomorphic if and only if* A *and* A' *are isomorphic as algebras over* k.

PROOF. This summarizes the above discussion (cf. the proof 20.35). □

The outer forms of SL_n

According to 24.7, there is an exact sequence

$$1 \to \mathrm{PGL}_n(k^s) \to \mathrm{Aut}(\mathrm{SL}_{nk^s}) \to \mathrm{Sym}(\mathcal{D}) \to 1,$$

and $\mathrm{Sym}(\mathcal{D})$ has order 2 if $n > 2$. In fact, $X \mapsto (X^t)^{-1}$ is an outer automorphism of SL_n inducing the obvious symmetry on the Dynkin diagram (Exercise 21-3). This does not extend to an automorphism of $M_n(k)$, and so we need to proceed differently.

　　Consider the algebra $A = M_n(k) \times M_n(k)$ over k. The two copies of $M_n(k)$ are the *only* minimal two-sided ideals in A (see 24.18). Thus, an automorphism of A either respects the pair $(M_n(k), M_n(k))$ or it swaps them. In the first case, the automorphism is inner and in the second it is the composite of an inner automorphism with $(X, Y) \mapsto (Y, X)$.

　　Now endow $M_n(k) \times M_n(k)$ with the involution

$$*: (X, Y) \mapsto (Y^t, X^t).$$

According to Lemma 24.31, the inner automorphism $\mathrm{inn}(a)$ commutes with $*$ if and only if $a^* a \in k \times k$. If $a^* a \in k \times k$, then it lies in the diagonal k of $k \times k$

because it is fixed by $*$. When we work over k^s, we can scale a so that $a^*a = 1$. Let $a = (X,Y)$. If

$$1 = a^*a = (Y^t X, X^t Y),$$

then $a = (X, (X^t)^{-1})$. It follows that the automorphisms of $(M_n(k^s) \times M_n(k^s), *)$ are the inner automorphisms by elements $(X, (X^t)^{-1})$ and the composites of such automorphisms with $(X,Y) \mapsto (Y,X)$.

When we embed $\mathrm{SL}_n(k^s)$ in the product,

$$X \mapsto (X, (X^t)^{-1}) : \mathrm{SL}_n(k^s) \hookrightarrow M_n(k^s) \times M_n(k^s), \qquad (158)$$

the image is stable under the automorphisms of $(M_n(k^s) \times M_n(k^s), *)$, and in this way we get an isomorphism

$$\mathrm{Aut}(\mathrm{SL}_{nk^s}) \simeq \mathrm{Aut}(M_n(k^s) \times M_n(k^s), *).$$

Thus, the forms of SL_n correspond to the forms of $(M_n(k) \times M_n(k), *)$, and these are the algebras with involution $(A, *)$ over k that are simple of unitary type (24.42).

The map (158) identifies $\mathrm{SL}_n(k^s)$ with the subgroup of $M_n(k^s) \times M_n(k^s)$ of elements such that $a^*a = 1$ and $\mathrm{Nrd}(a) = 1$. Define $\mathrm{SU}(A, *)$ to be the algebraic group over k such that

$$\mathrm{SU}(A, *)(R) = \{a \in A \otimes_k R \mid a^*a = 1, \mathrm{Nrd}(a) = 1\}$$

for all k-algebras R.

THEOREM 24.44. *The forms of* SL_n *over* k *are the algebraic groups* $\mathrm{SU}(A, *)$, *where* $(A, *)$ *is an algebra with involution of degree* $2n^2$ *over* k *that is simple of unitary type (24.42); two groups* $\mathrm{SU}(A, *)$ *and* $\mathrm{SU}(A', *')$ *are isomorphic if and only if* $(A, *)$ *and* $(A', *')$ *are isomorphic as algebras with involution over* k.

PROOF. This summarizes the above discussion. $\square$

REMARK 24.45. There is a commutative diagram

$$
\begin{array}{ccc}
\mathrm{Aut}(\mathrm{SL}_{nk^s}) & \longrightarrow & \mathrm{Sym}(\mathcal{D}) \\
\downarrow{\simeq} & & \downarrow{\simeq} \\
\mathrm{Aut}(M_n(k^s) \times M_n(k^s), *) & \xrightarrow{\mathrm{restrict}} & \mathrm{Aut}(k^s \times k^s).
\end{array}
$$

The centre of A is the form of $k^s \times k^s$ corresponding to the image of the cohomology class of G in $\mathrm{Sym}(\mathcal{D})$. Therefore, $\mathrm{SU}(A, *)$ is an inner or outer form of SL_n according as the centre of A is $k \times k$ or a field.

REMARK 24.46. More formally (and precisely), the functor $(A, *) \rightsquigarrow \mathrm{SU}(A, *)$ defines an equivalence from the category

$\begin{cases} \text{objects: algebras with involution of degree } 2n^2 \text{ over } k \text{ simple of unitary type,} \\ \text{morphisms: isomorphisms of algebras with involution over } k, \end{cases}$

to the category

$$\begin{cases} \text{objects: } k\text{-forms of } \mathrm{SL}_n, \\ \text{morphisms: isomorphisms of algebraic groups over } k \end{cases}$$

(Knus et al. 1998, 26.9).

g.   The geometrically almost-simple groups of type C

Recall (p. 459) that the split simply connected almost-simple group of type C_n is Sp_{2n}. Thus, we need to find the k-forms of Sp_{2n}.

Consider the algebra $M_{2n}(k)$ over k with its involution

$$X \mapsto X^* \overset{\text{def}}{=} S^{-1} X^t S, \quad S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The inner automorphism of $M_{2n}(k)$ defined by an invertible matrix U commutes with $*$ if and only if $U^* U \in k^\times$ (see 24.31). When we pass to k^s, we may scale U so that $U^* U = I$. Then $U^t S U = S$, i.e., $U \in \mathrm{Sp}_{2n}(k^s)$. As the Dynkin diagram of type C_n has no symmetries, all automorphisms of Sp_{2n} are inner. Therefore the inclusion

$$X \mapsto X : \mathrm{Sp}_{2n}(k^s) \hookrightarrow M_{2n}(k^s) \tag{159}$$

induces an isomorphism

$$\mathrm{Aut}(\mathrm{Sp}_{2nk^s}) \simeq \mathrm{Aut}(M_{2n}(k^s), *).$$

It follows that the k-forms of Sp_{2n} correspond to the k-forms of $(M_{2n}(k), *)$. These are the central simple algebras A over k equipped with an involution $*$ of symplectic type (24.37).

The map (159) identifies $\mathrm{Sp}_{2n}(k^s)$ with the subgroup of $M_{2n}(k^s)$ of elements such that $a^* a = 1$. Define $\mathrm{Sp}(A, *)$ to be the algebraic group over k such that

$$\mathrm{Sp}(A, *)(R) = \{a \in (A \otimes_k R)^\times \mid a^* a = 1\}$$

for all k-algebras R.

THEOREM 24.47. *The forms of Sp_{2n} over k are the algebraic groups $\mathrm{Sp}(A, *)$ where $(A, *)$ is a central simple algebra of degree $(2n)^2$ over k with an involution $*$ of symplectic type (24.37); two groups $\mathrm{Sp}(A, *)$ and $\mathrm{Sp}(A', *')$ are isomorphic if and only if $(A, *)$ and $(A', *')$ are isomorphic as algebras with involution over k.*

Again, this can be stated more precisely as an equivalence of categories (Knus et al. 1998, 26.14).

h. Clifford algebras

The spin groups are the simply connected coverings of the special orthogonal groups. Unusually among the classical groups, they do not have faithful representations of small dimension. For example, for the double covering of SO_{2n}, the smallest such dimension is 2^s with $s = \lfloor \frac{n-1}{2} \rfloor$. Instead, we construct them as subgroups of the Clifford algebras, which we define in this section.

Throughout, vector spaces V over k are finite-dimensional.

Graded algebras

24.48. By a graded algebra over k in this section, we mean a $\mathbb{Z}/2\mathbb{Z}$-graded algebra over k, i.e., an algebra C over k together with a k-subspaces C_0 and C_1 such that $C = C_0 \oplus C_1$, $k \subset C_0$, and $C_i C_j \subset C_{i+j}$ for $i, j \in \mathbb{Z}/2\mathbb{Z}$. When $\mathrm{char}(k) \neq 2$, a gradation on an algebra C over k determines an involution θ of C by $\theta(x) = (-1)^{\deg(x)} x$, and every gradation arises in this way from a unique involution.

24.49. Let $c_1, \dots, c_n \in k$. Define $C(c_1, \dots, c_n)$ to be the k-algebra with generators $e_1, \dots, e_n$ and relations

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

As a k-vector space, $C(c_1, \dots, c_n)$ has basis $\{e_1^{i_1} \cdots e_n^{i_n} \mid i_j \in \{0, 1\}\}$, and so it has dimension 2^n. When we set C_0 (resp. C_1) equal to the subspace spanned by the elements $e_1^{i_1} \cdots e_n^{i_n}$ with $i_1 + \cdots + i_n$ even (resp. odd), then we obtain a graded algebra.

24.50. The tensor product of two graded algebras C and D over k is the graded algebra $C \hat{\otimes} D$ over k with underlying k-vector space $C \otimes D$, multiplication

$$(c_i \otimes d_j)(c_l' \otimes d_m') = (-1)^{jl}(c_i c_l' \otimes d_j d_m'), \quad c_i \in C_i, d_j \in D_j, \dots,$$

and gradation $(C \hat{\otimes} D)_l = \bigoplus_{i+j=l} C_i \otimes D_j$.

24.51. There is an isomorphism

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

under which e_i corresponds to $1 \otimes \cdots \otimes e \otimes \cdots \otimes 1$ (e in the ith position).

Quadratic spaces

Let V be a vector space over k. A map $q: V \to k$ is a **quadratic form** if there exists a k-bilinear form $\phi: V \times V \to k$ such that $q(v) = \phi(v, v)$ for all v in V. Then the polar symmetric bilinear form

$$\phi_q(v, w) = q(v + w) - q(v) - q(w)$$

of q has the property that $\phi_q(v,v) = 2q(v)$.

A quadratic form on a space of dimension n is **nondegenerate** if over k^a it becomes equivalent to $\sum_{i=1}^{n/2} x_{2i-1}x_{2i}$ (n even) or $x_0^2 + \sum_{i=1}^{(n-1)/2} x_{2i-1}x_{2i}$ (n odd). When $\mathrm{char}(k) \neq 2$, this is equivalent to the polar form ϕ_q being nondegenerate. In characteristic 2, q is nondegenerate if either the left kernel $V^\perp$ of ϕ_q is zero, or it has dimension 1 and $q(V^\perp) \neq 0$.

A **quadratic space** is a vector space V equipped with a quadratic form. A quadratic space (V,q) is **regular** if q is nondegenerate.

NOTES. In characteristic $\neq 2$, these definitions are standard. Otherwise, we have followed Knus et al. 1998, p. xix.

Definition of the Clifford algebra

Let (V,q) be a quadratic space.

DEFINITION 24.52. The **Clifford algebra** $C(V,q)$ is the quotient of the tensor algebra $T(V)$ of V by the two-sided ideal $I(q)$ generated by the elements of the form $x \otimes x - q(x)$ with $x \in V$.

Let $\rho: V \to C(V,q)$ be the composite of the canonical map $V \to T(V)$ and the quotient map $T(V) \to C(V,q)$. Then ρ is k-linear, and

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

If $q(x) \neq 0$, then $\rho(x)$ is invertible in $C(V,q)$, because $\rho(x) \cdot (\rho(x)/q(x)) = 1$.

EXAMPLE 24.53. If V is one-dimensional with basis e and $q(e) = c$, then $T(V)$ is a polynomial algebra over k in the symbol e and $I(q) = (e^2 - c)$. Therefore, $C(V,q) \simeq C(c)$.

EXAMPLE 24.54. If $q = 0$, then $C(V,q)$ is the exterior algebra on V (quotient of $T(V)$ by the ideal generated by all squares x^2, $x \in V$).

PROPOSITION 24.55. *Let r be a k-linear map from V to an algebra D over k such that $r(x)^2 = q(x)$. Then there exists a unique homomorphism $\bar{r}: C(V,q) \to D$ of algebras over k such that $\bar{r} \circ \rho = r$.*

PROOF. According to the universal property of the tensor algebra, r extends uniquely to a homomorphism $r': T(V) \to D$ of algebras over k, namely,

$$r'(x_1 \otimes \cdots \otimes x_n) = r(x_1) \cdots r(x_n).$$

As

$$r'(x \otimes x - q(x)) = r(x)^2 - q(x) = 0,$$

r' factors uniquely through $C(V,q)$.   □

The gradation on the Clifford algebra

Decompose

$$T(V) = T(V)_0 \oplus T(V)_1, \quad T(V)_0 = \bigoplus_{m \text{ even}} V^{\otimes m}, \quad T(V)_1 = \bigoplus_{m \text{ odd}} V^{\otimes m}.$$

As $I(q)$ is generated by elements of $T(V)_0$,

$$I(q) = (I(q) \cap T(V)_0) \oplus (I(q) \cap T(V)_1),$$

and so

$$C(V,q) = C_0 \oplus C_1 \quad \text{with} \quad C_i = T(V)_i / I(q) \cap T(V)_i.$$

Clearly this decomposition makes $C(V,q)$ into a graded algebra over k.

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

If $\{f_1, \ldots, f_n\}$ is an orthogonal basis for V, then

$$\rho(f_i)^2 = q(f_i), \quad \rho(f_j)\rho(f_i) = -\rho(f_i)\rho(f_j) \quad (i \neq j).$$

Let $c_i = q(f_i)$. Then there exists a surjective homomorphism

$$e_i \mapsto \rho(f_i) : C(c_1, \ldots, c_n) \to C(V,q). \tag{160}$$

The behaviour of the Clifford algebra with respect to direct sums

If $(V,q) = (V_1, q_1) \oplus (V_2, q_2)$, then the k-linear map

$$V = V_1 \oplus V_2 \xrightarrow{r} C(V_1, q_1) \hat{\otimes} C(V_2, q_2)$$
$$x = (x_1, x_2) \mapsto \rho_1(x_1) \otimes 1 + 1 \otimes \rho_2(x_2)$$

has the property that $r(x)^2 = q_1(x_1) + q_2(x_2) = q(x)$, and so it factors uniquely through $C(V,q)$:

$$C(V,q) \to C(V_1, q_1) \hat{\otimes} C(V_2, q_2). \tag{161}$$

Extension of scalars

Let (V,q) be a quadratic space over k, and let R be a k-algebra. By definition, $q(x) = \phi(x,x)$ for some k-bilinear form ϕ on V. This ϕ extends bilinearly to an R-bilinear form ϕ_R on V_R, and we set $q_R(x) = \phi_R(x,x)$ for $x \in V_R$.

Explicit description of the Clifford algebra

In the remainder of this section, we assume that $\mathrm{char}(k) \neq 2$.

THEOREM 24.56. *Let (V,q) be a quadratic space of dimension n.*

(a) *For every orthogonal basis for (V,q), the homomorphism (160)*

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

is an isomorphism.

(b) *For every orthogonal decomposition $(V,q) = (V_1,q_1) \oplus (V_2,q_2)$, the homomorphism (161)*

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

is an isomorphism.

(c) *The dimension of $C(V,q)$ as a k-vector space is 2^n.*

PROOF. If $n = 1$, all three statements are clear from 24.53. Assume inductively that they are true for $\dim(V) < n$. Certainly, we can decompose $(V,q) = (V_1,q_1) \oplus (V_2,q_2)$ in such a way that $\dim(V_i) < n$. The homomorphism (161) is surjective because its image contains $\rho_1(V_1) \otimes 1$ and $1 \otimes \rho_2(V_2)$ which generate $C(V_1,q_1) \hat{\otimes} C(V_2,q_2)$, and so

$$\dim(C(V,q)) \geq 2^{\dim(V_1)} 2^{\dim(V_2)} = 2^n.$$

From an orthogonal basis for (V,q), we get a surjective homomorphism (160). Therefore, $\dim(C(V,q)) \leq 2^n$. It follows that $\dim(C(V,q)) = 2^n$. By comparing dimensions, we deduce that the homomorphisms (160) and (161) are isomorphisms. □

COROLLARY 24.57. *The map $\rho: V \to C(V,q)$ is injective.*

This allows us to omit the ρ and regard V as a subset of $C(V,q)$.

The structure of the Clifford algebra

Assume that (V,q) is regular, and that $n = \dim V > 0$. Let $e_1,\ldots,e_n$ be an orthogonal basis for (V,q), and let $q(e_i) = c_i$. Let

$$\delta = (-1)^{\frac{n(n-1)}{2}} c_1 \cdots c_n = (-1)^{\frac{n(n-1)}{2}} \det(\phi(e_i,e_j)).$$

We saw in Theorem 24.56 that

$$C(c_1,\ldots,c_n) \simeq C(V,q).$$

Note that $(e_1 \cdots e_n)^2 = \delta$ in $C(c_1,\ldots,c_n)$. Moreover,

$$e_i \cdot (e_1 \cdots e_n) = (-1)^{i-1} c_i (e_1 \cdots e_{i-1} e_{i+1} \cdots e_n)$$
$$(e_1 \cdots e_n) \cdot e_i = (-1)^{n-i} c_i (e_1 \cdots e_{i-1} e_{i+1} \cdots e_n).$$

Therefore, $e_1 \cdots e_n$ lies in the centre of $C(V,q)$ if and only if n is odd.

PROPOSITION 24.58. *(a) If n is even, then the centre of $C(V,q)$ is k; if n is odd, it is of degree 2 over k, generated by the element $e_1 \cdots e_n$ of square δ.*

(b) No nonzero element of C_1 centralizes C_0, and $C_0 \cap \mathrm{Centre}(C(V,q)) = k$.

PROOF. First show that a linear combination of reduced monomials is in the centre (or centralizes C_0) if and only if each monomial does, and then find the monomials that centralize the e_i (or the $e_i e_j$). □

THEOREM 24.59. *If n is even, then $C(V,q)$ is a central simple algebra over k, isomorphic to a tensor product of quaternion algebras. If n is odd, then $C(V,q)$ is a central simple algebra over the field $k[\sqrt{\delta}]$ when δ is not a square in k, and a product of two central simple algebras over k otherwise.*

PROOF. See Scharlau 1985, Chapter 9, 2.10. □

The involution ∗

Assume that (V,q) is regular (and $\mathrm{char}(k) \neq 2$). The map $\rho : V \to C(V,q)^{\mathrm{opp}}$ is k-linear and has the property that $\rho(x)^2 = q(x)$, and so it extends uniquely to a homomorphism $* : C(V,q) \to C(V,q)^{\mathrm{opp}}$. As $*$ acts as the identity map on V,

$$(x_1 \cdots x_r)^* = x_r \cdots x_1, \quad \text{all } x_1, \ldots, x_r \in V.$$

In particular, $*$ is an involution of $C(V,q)$. From $*$ we get a norm map $x \mapsto x^*x : C(V,q) \to C(V,q)$. Note that $x^*x = q(x)$ for $x \in V$, and so the norm map extends q from V to $C(V,q)$.

NOTES. For more on Clifford algebras, see Scharlau 1985, Chapter 9, and Knus et al. 1998.

i. The spin groups

Let (V,q) be a regular quadratic space over k of dimension n. Define $\mathrm{O}(V,q)$ to be the algebraic group over k such that

$$\mathrm{O}(V,q)(R) = \{\alpha \in \mathrm{GL}_V(R) \mid q_R(\alpha v) = q_R(v) \text{ for all } v \in V_R\},$$

for all k-algebras R. When $\mathrm{char}(k) \neq 2$ or n is odd, we define

$$\mathrm{SO}(V,q) = \mathrm{Ker}(\mathrm{O}(V,q) \xrightarrow{\det} \mathbb{G}_m).$$

Otherwise, we define $\mathrm{SO}(V,q)$ so that $\mathrm{SO}(V,q)(R)$ consists of the $\alpha \in \mathrm{O}(V,q)(R)$ inducing the identity map on the centre of $C(V,q)$.

When $\mathrm{char}(k) \neq 2$,

$$\dim(\mathrm{O}(V,q)) = \frac{n(n-1)}{2} = \dim(\mathrm{Lie}(\mathrm{O}(V,q))$$

and so $O(V,q)$ is smooth; thus $SO(V,q)$ is smooth and connected (Exercise 2-9). For a proof of this when $\text{char}(k) = 2$, see Knus et al. 1998, p. 348.

We now assume that $\text{char}(k) \neq 2$. Let $g \in SO(q)(k)$. Then g is an isomorphism $V \to V$, and so it extends to an isomorphism $C(V,q) \to C(V,q)$ of the Clifford algebra (by universality). It is known that this is the inner automorphism defined by an element $h \in C_0(V,q)^\times$. Conversely, if $h \in C_0(V,q)_R^\times$ is such that $hV_R h^{-1} = V_R$, then the mapping $x \mapsto hxh^{-1} \colon V_R \to V_R$ is an element of $SO(q)(R)$.

Define $GSpin(V,q)$ to be the algebraic group over k such that

$$GSpin(V,q)(R) = \{g \in C_0(V,q)_R^\times \mid gV_R g^{-1} = V_R\}.$$

From the above discussion, we see that there is a natural homomorphism $GSpin \to SO(V,q)$ sending $g \in GSpin(V,q)(R)$ to the map $v \mapsto gvg^{-1} \colon V_R \to V_R$. The kernel consists of the scalars, and so there is an exact sequence

$$e \to \mathbb{G}_m \to GSpin(V,q) \to SO(V,q) \to e.$$

Therefore $GSpin(V,q)$ is also smooth and connected; moreover, it is reductive with adjoint group the adjoint group of $SO(V,q)$.

When $g \in GSpin(V,q)(R)$, its norm $g^*g \in R^\times$. In this way, we get a homomorphism $GSpin(V,q) \to \mathbb{G}_m$, called the **spinor norm**. The group $Spin(V,q)$ is defined to be its kernel. Thus there is a diagram

$$
\begin{array}{ccc}
& Spin(V,q) & \\
& \downarrow & \searrow \\
\mathbb{G}_m \longrightarrow & GSpin(V,q) & \longrightarrow SO(V,q) \\
{\scriptstyle x \mapsto x^2} \searrow & \downarrow & \\
& \mathbb{G}_m &
\end{array}
$$

in which the column and row are short exact sequences. We can extract from the diagram an exact sequence

$$e \to \mu_2 \to Spin(V,q) \times \mathbb{G}_m \to GSpin(V,q) \to e,$$

and so the diagram

$$
\begin{array}{ccc}
\mu_2 & \longrightarrow & \mathbb{G}_m \\
\downarrow & & \downarrow \\
Spin(V,q) & \longrightarrow & GSpin(V,q)
\end{array}
\qquad (162)
$$

satisfies the hypotheses of Lemma 19.23. Thus, there are canonical isomorphisms

$$\mathbb{G}_m/\mu_2 \simeq GSpin(V,q)/Spin(V,q),$$
$$Spin(V,q)/\mu_2 \simeq GSpin(V,q)/\mathbb{G}_m \simeq SO(V,q).$$

We see that $\mathrm{Spin}(V,q)$ is the derived group of $\mathrm{GSpin}(V,q)$, and it is a two-fold covering group of $\mathrm{SO}(V,q)$. Explicitly, an element g of $\mathrm{Spin}(k)$ lies in the kernel of $\mathrm{Spin}(k) \to \mathrm{SO}(k)$ if and only if $gxg^{-1} = x$ for all $x \in V$. As V generates $C(V,q)$, this implies that $g \in C_0 \cap \mathrm{Centre}(C) = k$ (24.58); now the condition $g^*g = 1$ implies that $g^2 = 1$, and so $g = \pm 1$.

The root system $(X(T)_{\mathbb{Q}}, \Phi)$ of $\mathrm{Spin}(V,q)$ equals that of $\mathrm{SO}(V,q)$, but $X(T) = P(\Phi)$ and so $\mathrm{Spin}(V,q)$ is the simply connected covering group of $\mathrm{SO}(V,q)$ (see 23.29). The root datum of GSpin can be computed from the diagram (162) (Exercise 24-4).

REMARK 24.60. Let ϕ be the bilinear form on V such that $q(v) = \phi(v,v)$. When $\mathrm{char}(k) \neq 2$, the groups $\mathrm{O}(V,\phi)$ and $\mathrm{O}(V,q)$ coincide. When $\mathrm{char}(k) = 2$, the group $\mathrm{O}(V,\phi)$, and even its reduced subgroup, need not be smooth (Exercise 24-2). When $\mathrm{char}(k) \neq 2$ and k is perfect, $\mathrm{O}(V,\phi)_{\mathrm{red}}$ is isomorphic to the symplectic group of an alternating space of dimension $\dim(V) - 1$ if $\dim(V)$ is odd, but it need not be reductive when $\dim(V)$ is even (Exercise 24-3).

j. The geometrically almost-simple group of types B and D

For simplicity, we assume that $\mathrm{char}(k) \neq 2$. In particular, this implies that $\mathrm{O}(V,q) = \mathrm{O}(V,\phi_q)$ for a quadratic form q and its polar form ϕ_q.

Let (V,q) be a regular quadratic space of dimension m. The **Witt index** of (V,q) is the dimension of any maximal totally isotropic subspace of V. The groups $\mathrm{SO}(V,q)$ and $\mathrm{Spin}(V,q)$ are split if and only if (V,q) has the largest possible Witt index. For example, the quadratic forms

$$q = x_0^2 + \sum_{i=1}^n x_{2i-1}x_{2i} \quad (m = 2n+1 \text{ odd})$$
$$q = \sum_{i=1}^n x_{2i-1}x_{2i} \quad (m = 2n \text{ even})$$

on k^m have the largest possible Witt index, namely, $n = \lfloor \frac{m}{2} \rfloor$. We write Spin_m, O_m, and SO_m for the algebraic groups attached to these forms.

Let (V,q) be a regular quadratic space of dimension $m \geq 7$ with largest possible Witt index. Then $\mathrm{O}(V,q)$ acts on its subgroup $\mathrm{SO}(q)$ by conjugation, and every automorphism of $\mathrm{SO}(V,q)$ arises from an element of $O(V,q)(k)$. On the other hand, $O(V,q)$ acts on the Clifford algebra $C(V,q)$, and hence on $\mathrm{Spin}(V,q)$. The map $O(V,q) \to \mathrm{Aut}(\mathrm{Spin}(V,q))$ factors through an injective homomorphism

$$O(V,q)^{\mathrm{ad}} \simeq \mathrm{Aut}(\mathrm{SO}(V,q)) \to \mathrm{Aut}(\mathrm{Spin}(V,q)). \tag{163}$$

This induces an isomorphism $\mathrm{SO}(V,q)^{\mathrm{ad}} \to \mathrm{Spin}(V,q)^{\mathrm{ad}}$ on the groups of inner automorphisms. Recall that the index of $\mathrm{Spin}(V,q)^{\mathrm{ad}}$ in $\mathrm{Aut}(\mathrm{Spin}(V,q))$ is the number of symmetries of the Dynkin diagram of $\mathrm{Spin}(V,q)$, which is 1 if m is odd and 2 if m is even but $\neq 8$ (see Section b). Thus (163) is an isomorphism if m

is odd. If m is even, the automorphism of $SO(V,q)$ defined by a reflection is not inner, and so $SO(V,q)^{ad} \neq O(V,q)^{ad}$. We see that (163) is again an isomorphism if m is even and $m \neq 8$. We conclude that

$$\text{Aut}(SO(V,q)) \simeq \text{Aut}(\text{Spin}(V,q))$$

if $m \neq 8$.

THEOREM 24.61. *The k-forms of Spin_m are exactly the simply connected coverings of the k-forms of SO_m except for $m = 8$.*

PROOF. Immediate consequence of the above discussion and Theorem 3.43. $\square$

Thus, it suffices to find the k-forms of SO_m. Let S be the matrix of one of the quadratic forms on k^m displayed above, and let $*$ be the involution $X^* = X^t S X^{-1}$ on $M_m(k)$. The automorphisms of $(M_m(k), *)$ are the inner automorphisms by elements a such that $a^* a \in k$ (see 24.31). After passing to k^s, we can scale a so that $a^* a = 1$, i.e., $a \in O(k)$. The automorphisms of SO_m are also given by inner automorphisms by elements of $O(k)$. The image of the inclusion

$$X \mapsto X : SO_m(k^s) \hookrightarrow M_m(k^s)$$

is stable under the automorphisms of $(M_m(k^s), *)$, and in this way we get an isomorphism

$$\text{Aut}(SO_{m,k^s}) \simeq \text{Aut}(M_m(k^s), *).$$

It follows that the k-forms of SO_m correspond to the k-forms of $(M_m(k^s), *)$. These are the central simple algebras A over k equipped with an involution of $*$ of orthogonal type (24.37). For such a pair, define $SO(A, *)$ to be the algebraic group over k such that

$$SO(A, *)(R) = \{ a \in (A \otimes R)^\times \mid a^* a = 1, \text{Nrd}(a) = 1 \}$$

for all k-algebras R.

THEOREM 24.62. *The forms of SO_m over k are the algebraic groups $SO(A, *)$, where $(A, *)$ is a central simple algebra of degree m^2 over k with an involution $*$ of orthogonal type (24.37); two groups $SO(A, *)$ and $SO(A', *')$ are isomorphic if and only if $(A, *)$ and $(A', *')$ are isomorphic.*

NOTES. It is possible to remove the restriction char$(k) \neq 2$ in this and the preceding section, but this involves modifying some of the definitions. See Knus et al. 1998, VI, §26.

k.   The classical groups in terms of sesquilinear forms

In the above, we described the geometrically almost-simple classical groups in terms of simple algebras with involution, but every simple algebra is a matrix

algebra over a division algebra. In this section, we explain how to rewrite the previous description in terms of division algebras and sesquilinear forms.

We shall use that the standard results in the linear algebra of vector spaces over a field hold also for vector spaces over a division algebra.

DEFINITION 24.63. Let $(D, *)$ be a division algebra over k with an involution $*$, and let V be a left vector space over D.

(a) A bi-additive form $\phi: V \times V \to D$ is *sesquilinear* if it is semilinear in the first variable and linear in the second, so

$$\phi(ax, by) = a^* \phi(x, y)b \text{ for } a, b \in D, \quad x, y \in V.$$

(b) A sesquilinear form ϕ is *hermitian* if

$$\phi(x, y) = \phi(y, x)^*, \quad \text{for } x, y \in V,$$

and *skew hermitian* if

$$\phi(x, y) = -\phi(y, x)^*, \quad \text{for } x, y \in V.$$

EXAMPLE 24.64. (a) Let $D = k$ with $*$ the identity map. In this case, the hermitian and skew hermitian forms are, respectively, the symmetric and skew symmetric forms.

(b) Let $D = \mathbb{C}$ with $* = $ complex conjugation. In this case, the hermitian and skew hermitian forms are the usual objects.

Let $(D, *)$ be a central division algebra over k with involution $*$, and let ϕ be a nondegenerate sesquilinear form on a vector space V over D. For each $\alpha \in \mathrm{End}_D(V)$, there is an $\alpha^{*\phi} \in \mathrm{End}_D(V)$ uniquely characterized by the equation

$$\phi(\alpha^{*\phi} x, y) = \phi(x, \alpha y), \quad x, y \in V.$$

This can be defined as in the bilinear case (24.35) except that $\hat{\phi}$ must be regarded as a map $V \to V'$, where V' is the set $\{f' \mid f \in V^\vee)$ with the D-module structure

$$f' + g' = (f + g)', \quad cf' = (c^* f)', \quad c \in D, \quad f, g \in V^\vee.$$

If ϕ is hermitian or skew hermitian then $*_\phi$ is an involution.

THEOREM 24.65. Let $(D, *)$ and (V, ϕ) be as above, and let $A = \mathrm{End}_D(V)$. Assume that $*$ is of the first kind on D and that $\mathrm{char}(k) \neq 2$. The map $\phi \mapsto *_\phi$ defines a one-to-one correspondence

$$\{nondegenerate \ hermitian \ or \ skew \ hermitian \ forms \ on \ V\}/k^\times$$
$$\leftrightarrow \{involutions \ on \ A \ extending \ * \ on \ D\}.$$

The involutions $*_\phi$ and $*$ have the same or opposite type according as ϕ is hermitian or skew hermitian.

The following table makes the second statement explicit.

$*$	ϕ	$*_\phi$
symplectic type	hermitian	symplectic type
orthogonal type	hermitian	orthogonal type
symplectic type	skew hermitian	orthogonal type
orthogonal type	skew hermitian	symplectic type

PROOF. Let ϕ and ϕ' be nondegenerate hermitian or skew hermitian forms on V, and let $u^{-1} = \hat{\phi}^{-1} \circ \hat{\phi}' \in A^\times$. Then

$$\phi'(x, y) = \phi(u^{-1}(x), y), \quad x, y \in V, \tag{164}$$

and so

$$*_\phi = \mathrm{inn}(u^{-1}) \circ *_{\phi'}.$$

This shows that $*_\phi = *_{\phi'}$ if and only if $\phi' = c\phi$ for some $c \in k^\times$.

Let $*'$ be an involution on A extending $*$ on D. Choose a basis for V as a vector space over D, and use it to extend $*$ on D to an involution $*$ on A of the same type (identify A with $M_m(D)$ and set $(a_{ij})^* = (a_{ij}^*)^t$). Now $*' = \mathrm{inn}(u) \circ *$ for some $u \in A^\times$ such that $u^* = \pm u$ (24.34a). Define ϕ' by (164). Then ϕ' is a nondegenerate form with $*_{\phi'} = *'$, and it is hermitian or skew hermitian according as $u^* = +u$ or $-u$. This completes the proof of the first statement.

Let $*' = \mathrm{inn}(u) \circ *$. Then

$$\mathrm{Sym}(A, *') = \begin{cases} \mathrm{Sym}(A, *) & \text{if } u^* = +u \\ \mathrm{Skew}(A, *) & \text{if } u^* = -u. \end{cases}$$

Now the second statement follows from Proposition 24.38.   □

To each hermitian or skew hermitian form, we attach the group of automorphisms of (V, ϕ), and the special group of automorphisms of ϕ (the automorphisms with determinant 1, if this is not automatic).

SUMMARY 24.66. Let k be a field of characteristic $\neq 2$. The geometrically almost-simple, simply connected, classical groups over k are the following.

(A) The groups $\mathrm{SL}_m(D)$ for D a central division algebra over k (the inner forms of SL_n); the groups attached to a hermitian form for a quadratic field extension K of k (the outer forms of SL_n).

(C) The symplectic groups, and unitary groups of hermitian forms over division algebras.

(BD) The spin groups of quadratic forms, and the spin groups of skew hermitian forms over division algebras.

Special fields

Let D and D' be central division algebras over k. Then $D \otimes D'$ is again a central simple algebra over k, and so $D \otimes D' \approx M_n(D'')$ for some central division algebra D'' over k. In this way we get a binary operation $[D][D'] = [D'']$ on the set of isomorphism classes of central division algebras over k, which makes it into a commutative group (called the ***Brauer group*** of k, denoted $\mathrm{Br}(k)$). For example, $[k]$ is an identity element, and Proposition 24.26 shows that $[D^{\mathrm{opp}}]$ is an inverse to $[D]$. We define the class $[A]$ of a central simple algebra $A = M_m(D)$ over k to be $[D]$ (see 24.17). Then $[A \otimes A'] = [A][A']$.

EXAMPLE 24.67. (a) $\mathrm{Br}(k) = 1$ if k is separably closed (24.21) or finite (Wedderburn's little theorem).

(b) $\mathrm{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$. The nontrivial element is represented by the usual quaternion algebra.

(c) $\mathrm{Br}(k) \simeq \mathbb{Q}/\mathbb{Z}$ if k is a nonarchimedean local field (i.e., a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((T))$).

(d) If k is a global field (i.e., a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(T)$), then there is an exact sequence[2]

$$0 \to \mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0 \qquad (165)$$

where the direct sum is over the primes of k (including the real primes).

The statements for local and global fields are part of class field theory (Serre 1962, XIII, §3; XIV, Annexe).

PROPOSITION 24.68. *If a central simple algebra A over k admits an involution of the first kind, then $[D]$ has order dividing 2 in $\mathrm{Br}(k)$.*

PROOF. An involution of the first kind on A is an isomorphism $A \to A^{\mathrm{opp}}$. Thus Proposition 24.26 shows that

$$A \otimes A \simeq \mathrm{End}(A) \quad (k\text{-linear endomorphisms}),$$

and so $2[A] = 0$. $\qquad\square$

In particular, every quaternion algebra has order 2 in $\mathrm{Br}(k)$.

DEFINITION 24.69. We say that a field k is ***special*** if every element of order 2 in the Brauer group of k is represented by a quaternion algebra over k.

THEOREM 24.70. *The following fields are special: separably closed fields, finite fields, local fields including $\mathbb{R}$, global fields.*

---

[2]For an algebraic number field, this is related to the famous theorem of Albert, Brauer, Hasse, and Noether.

PROOF. In each case, it is possible to show directly that each class of order 2 in the Brauer group is represented by a quaternion algebra. For example, if k is a local field, then there is exactly one class of order 2 in the Brauer group, and one can exhibit a division quaternion algebra over k which must represent that class. For a global field k, the sequence (165) shows that it suffices to exhibit, for every set S of primes of k with a finite even number of elements, a quaternion algebra H over k such that $H \otimes_k k_v$ is nonsplit exactly at the primes v in S. This can be done in a similar way to the case $k = \mathbb{Q}$ (see Section 20j). □

SUMMARY 24.71. Let k be a special field of characteristic $\neq 2$. The geometrically almost-simple, simply connected, classical groups over k are the following.

(A) The groups $\mathrm{SL}_m(D)$ for D a central division algebra over k (the inner forms of SL_n); the groups attached to a hermitian form for a quadratic field extension K of k (the outer forms of SL_n).

(BD) The spin groups of quadratic forms, and the spin groups of skew hermitian forms over quaternion division algebras.

(C) The symplectic groups, and unitary groups of hermitian forms over quaternion division algebras.

l.　The exceptional groups

In this section, we describe the almost-simple groups of exceptional type F_4, E_6, E_7, E_8, and G_2. This is only a brief survey. For more details, we refer the reader to Springer 1998 and the references therein, especially Springer and Veldkamp 2000 and Knus et al. 1998. For the exceptional Lie groups, see Adams 1969, and for the corresponding root systems, see Bourbaki 1968.

The exceptional Lie algebras over $\mathbb{C}$ were discovered and classified by Killing in the 1880s. They form a chain

$$\mathfrak{g}_2 \subset \mathfrak{f}_4 \subset \mathfrak{e}_6 \subset \mathfrak{e}_7 \subset \mathfrak{e}_8.$$

In this section, an algebra A over k is a finite-dimensional k-vector space equipped with a k-bilinear map $A \times A \to A$.

Groups of type G_2

Let V be the hyperplane $x_1 + x_2 + x_3 = 0$ in $\mathbb{R}^3$ and Φ the set of elements

$$\pm(e_1 - e_2), \ \pm(e_1 - e_3), \ \pm(e_2 - e_3),$$
$$\pm(2e_1 - e_2 - e_3), \ \pm(2e_2 - e_1 - e_2), \ \pm(2e_3 - e_1 - e_2).$$

Then (V, Φ) is a root system with base $\Delta = \{e_1 - e_2, -2e_2 + e_2 + e_3)$ and Dynkin diagram G_2 (see Section Cg). It has rank 2, and there are 12 roots, and so every geometrically almost-simple group of type G_2 has dimension 14. As $P(\Phi) = Q(\Phi)$, such a group is both simply connected and adjoint.

A **Hurwitz algebra** over k is an algebra A of finite degree over k with 1 together with a nondegenerate quadratic (norm) form $N : A \to k$ such that

$$N(xy) = N(x)N(y) \text{ for all } x, y \in A.$$

If $\mathrm{char}(k) = 2$, the bilinear form attached to N is required to be nondegenerate. The possible dimensions of A are 1, 2, 4, and 8. A Hurwitz algebra of dimension 8 is called an **octonion algebra**. For such an algebra A, the functor

$$R \rightsquigarrow \mathrm{Aut}_R(R \otimes_k A)$$

is a simple group variety over k of type G_2, and all geometrically simple group varieties of type G_2 arise in this way from octonion algebras.

Consider the map

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \bar{x} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} : M_2(k) \to M_2(k).$$

The **special octonion algebra** $\mathbb{O}$ over k equals $M_2(k) \oplus M_2(k)$ as a vector space, and the multiplication and norm form on $\mathbb{O}$ are defined by

$$(x, y)(u, v) = (xu - \bar{v}y, vx + y\bar{u})$$
$$N((x, y)) = x\bar{x} - y\bar{y} = \det(x) - \det(y).$$

The group G attached to $\mathbb{O}$ is a split connected group variety of type G_2.

Every octonion algebra over k becomes isomorphic to $\mathbb{O}$ over k^s and

$$G(k^s) \simeq \mathrm{Aut}(G_{k^s}) \simeq \mathrm{Aut}(\mathbb{O} \otimes k^s).$$

Therefore there are natural bijections between the following sets: (a) isomorphism classes of octonion algebras over k; (b) isomorphism classes of geometrically simple groups of type G_2 over k; (c) $H^1(k, G)$. There is a canonical bijection from $H^1(k, G)$ onto the subset of $H^3(k, \mathbb{Z}/2\mathbb{Z})$ consisting of decomposable elements, i.e., cup products of three elements of $H^1(k, \mathbb{Z}/2\mathbb{Z})$. Thus these groups are quite well understood.

References: Springer 1998, 17.4; Serre 1997, III, Annexe.

Groups of type F_4

Let V be $\mathbb{R}^4$ and Φ the set of elements

$$\pm e_i \quad (1 \le i \le 4), \quad \pm e_i \pm e_j \quad (1 \le i < j \le 4),$$
$$\tfrac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4).$$

Then (V, Φ) is a root system with base

$$\{e_2 - e_2, \; e_3 - e_4, \; e_4, \; \tfrac{1}{2}(e_1 - e_2 - e_3 - e_4)\}$$

and Dynkin diagram F_4. It has rank 4 and there are 48 roots, and so every geometrically almost-simple group of type F_4 has dimension 52. As $P(\Phi) = Q(\Phi)$, such a group is both simply connected and adjoint.

An **Albert algebra** over k is a finite-dimensional k-vector space A equipped with a cubic (norm) form N, a nondegenerate symmetric bilinear (trace) form σ, and an element $e \in A$ satisfying certain conditions (see below). For such an algebra A, the functor

$$R \rightsquigarrow \operatorname{Aut}_R(R \otimes A, N, \sigma, e)$$

is a simple group variety over k of type F_4, and all simple group varieties of type F_4 arise in this way from Albert algebras.

Let $V = M_3(k) \times M_3(k) \times M_3(k)$ – it is a k-vector space of dimension 27. Let d and t denote the determinant and trace on $M_3(k)$, and let N_0 denote the cubic form

$$N_0((x_0, x_1, x_2)) = d(x_0) + d(x_1) + d(x_2) - t(x_0 x_1 x_2)$$

on V. For $a \in \operatorname{GL}_3(k)$, we define $\nu(a) = d(a)a^{-1}$. Then ν is a quadratic map $M_3(k) \to M_3(k)$, and we define n to be the quadratic map $V \to V$ with

$$n((x_0, x_1, x_2)) = (\nu(x_0) - x_1 x_2, \nu(x_2) - x_0 x_1, \nu(x_1) - x_2 x_0).$$

We have a symmetric bilinear map

$$V \times V \to V, \quad x \times y = n(x + y) - n(x) - n(y),$$

and a nondegenerate symmetric bilinear form

$$\sigma_0 : V \times V \to k, \quad \sigma(x, y) = t(x_0 y_0 + x_1 y_2 + x_2 y_1).$$

Finally, let $e_0 = (1, 0, 0)$. Then $A_0 = (V, N_0, \sigma_0, e_0)$ is an Albert algebra, called the **standard Albert algebra**. The group G_0 attached to A_0 is the split connected simple group variety of type F_4.

By definition, the Albert algebras over k are the quadruples (A, N, σ, e) over k that become isomorphic to $(A_0, N_0, \sigma_0, e_0)$ over k^s. As

$$G_0(k^s) \simeq \operatorname{Aut}(G_{0k^s}) \simeq \operatorname{Aut}(A \otimes k^s),$$

we see that there are natural bijections between the following sets: (a) isomorphism classes of Albert algebras over k; (b) isomorphism classes of geometrically simple groups of type F_2 over k; (c) $H^1(k, G_0)$.

There are constructions of Tits that yield all Albert algebras (up to isomorphism) over an arbitrary field.

References: Springer 1998, p. 305; Knus et al. 1998, §40.

Groups of type E_6

Let V be the subspace of $\mathbb{R}^8$ defined by the equations $x_6 = x_7 = -x_8$ and Φ the set of elements

$$\pm e_i \pm e_j \quad (1 \leq i < j \leq 5),$$
$$\pm \tfrac{1}{2}(e_8 - e_7 - e_6 + \sum_{i=1}^{5}(-1)^{\nu(i)}e_i \text{ with } \sum_{i=1}^{5}\nu(i) \text{ even.}$$

Then (V, Φ) is a root system of type E_6. It has rank 6 and there are 72 roots, and so every geometrically almost-simple group of type E_6 has dimension 78. The quotient $P(\Phi)/Q(\Phi)$ is cyclic of order 3 and so the centre of a split simply connected almost-simple group of type E_6 is isomorphic to μ_3.

Let $A = (V, N, \sigma, e)$ be an Albert algebra over k. Recall that N is a cubic form on V. Let G be the subgroup of GL_V fixing N (2.13). Then G is a simply connected group variety over k of type E_6, which is split if A is the standard Albert algebra.

Let G_0 be the split group of type E_6. From the description of G_0, we see that $H^1(k, G_0)$ classifies the isomorphism classes of cubic forms on the k-vector space $V_0 = M_3(k)^3$ becoming isomorphic to N over k^s. The group of symmetries of the Dynkin diagram of G has order 2 (the nontrivial element is the reflection about α_4), and so G has both inner and outer forms. The inner forms are classified by $H^1(k, G_0^{\mathrm{ad}})$, where $G_0^{\mathrm{ad}} = G_0/\mu_3$.

References: Springer 1998, 17.6, 17.7; Knus et al. 1998.

Groups of type E_7

Let V be the hyperplane in $\mathbb{R}^8$ orthogonal to $e_7 + e_8$ and Φ the set of vectors

$$\pm e_i \pm e_j \quad (1 \leq i < j \leq 6),$$
$$\pm \tfrac{1}{2}(e_7 - e_8 + \sum_{i=1}^{6}(-1)^{\nu(i)}e_i \text{ with } \sum_{i=1}^{6}\nu(i) \text{ even.}$$

Then (V, Φ) is a root system of type E_7. It has rank 7 and there are 126 roots, and so every geometrically almost-simple group of type E_7 has dimension 133. The quotient $P(\Phi)/Q(\Phi)$ is cyclic of order 2 and so the centre of a split simply connected group of type E_7 is isomorphic to μ_2.

Over a field k of characteristic $\neq 2, 3$, adjoint groups of type E_7 are the automorphism groups of certain objects called gifts (generalized Freudenthal triple systems). There is a natural bijection between the isomorphism classes of adjoint groups of type E_7 and the isomorphism classes of gifts (Garibaldi 2001, 3.13).

Groups of type E_8

Let V be $\mathbb{R}^8$ and Φ the set of elements

$$\pm e_i \pm e_j \quad (1 \leq i < j \leq 8),$$
$$\tfrac{1}{2}\sum_{i=1}^{8}(-1)^{\nu(i)}e_i \text{ with } \sum_{i=1}^{8}\nu(i) \text{ even.}$$

Then (V, Φ) is a root system of type E_8. It has rank 8 and there are 240 roots, and so a geometrically almost-simple group of type E_7 has dimension 248. As $P(\Phi) = Q(\Phi)$, such a group is both simply connected and adjoint.

For a recent expository article on groups of type E_8, see Garibaldi 2016.

m.   The trialitarian groups (groups of subtype $^3D_4$ and $^6D_4$)

An algebraic group over k is said to be trialitarian if it is geometrically almost-simple of type D_4 and the Galois group of k permutes the three end vertices of its Dynkin diagram. This means that the group is of subtype $^3D_4$ or $^6D_4$. Detailed studies of trialitarian groups over fields of characteristic $\neq 2$ can be found in Knus et al. 1998, Chapter X, and Garibaldi 1998.

Exercises

EXERCISE 24-1. Verify that the two descriptions of the inner forms of SL_n in Section 24f coincide.

The next two problems (Knus et al. 1998, VI, Exercises 15, 16) show that the orthogonal groups of *bilinear* forms behave badly in characteristic 2.

EXERCISE 24-2. Let k have characteristic 2, and let $a_1, a_2 \in k^\times$. Let G be the algebraic group of isometries of the bilinear form $a_1 x_1 y_1 + a_2 x_2 y_2$. Then $\mathcal{O}(G)$ is the quotient of the ring $k[x_{11}, x_{12}, x_{21}, x_{22}]$ by the ideal generated by the entries of the matrix

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}^t \cdot \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \cdot \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} - \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}.$$

(a) Show that $x_{11}x_{22} + x_{12}x_{21} + 1$ and $x_{11} + x_{22}$ are nilpotent in $\mathcal{O}(G)$.

(b) Assume that a_1/a_2 is not a square in k, and show that

$$\mathcal{O}(G_{\mathrm{red}}) = k[x_{11}, x_{21}]/(x_1^2 + a_2 a_1^{-1} x_{21}^2 + 1);$$

deduce that $(G_{\mathrm{red}})_{k^a}$ is not reduced.

(c) Assume that a_1/a_2 is a square in k, and show that $G_{\mathrm{red}} \approx \mathbb{G}_a$.

EXERCISE 24-3. Let k be perfect of characteristic 2 and let ϕ be a nondegenerate symmetric nonalternating bilinear form on a vector space V of dimension n.

(a) Show that there is a unique $e \in V$ such that $\phi(v, v) = \phi(v, e)^2$ for all $v \in V$. Let $V' = \langle e \rangle^\perp$ be the hyperplane of all vectors orthogonal to e. Show that $e \in V'$ if and only if e is even, and that the restriction ϕ' of ϕ to V' is alternating.

(b) Show that the smooth algebraic group $O(V, \phi)_{\mathrm{red}}$ fixes e.

(c) Suppose that n is odd. Show that the alternating form ϕ' is nondegenerate and that the restriction map $O(V,\phi)_{\text{red}} \to \text{Sp}(V',\phi')$ is an isomorphism.

(d) Suppose that n is even. Show that the radical $V'^{\perp}$ of ϕ' is ke, and let $V'' = V'/ke$ with its induced bilinear form ϕ''. Show that there is an exact sequence
$$e \to R(G) \to O(V,\phi)_{\text{red}} \to \text{Sp}(V'',\phi'') \to e$$
and that $R(G) \neq e$.

EXERCISE 24-4. Show that the root datum of GSpin_m, $m = 2n+1$ or $2n$, has the following description. The $\mathbb{Z}$-modules X and $X^{\vee}$ have dual bases $\{e_0,\dots,e_n\}$ and $\{e_0',\dots,e_n'\}$. If $\dim(V) = 2n+1$, then

$$\begin{array}{llll}
\text{base for the roots} & e_1 - e_2, & \dots, & e_{n-1} - e_n, \quad e_n \\
\text{base for the coroots} & e_1' - e_2', & \dots, & e_{n-1}' - e_n', \quad 2e_n' - e_0'.
\end{array}$$

If $\dim(V) = 2n$, then

$$\begin{array}{llll}
\text{base for the roots} & e_1 - e_2, & \dots, & e_{n-1} - e_n, \quad e_{n-1} + e_n \\
\text{base for the coroots} & e_1' - e_2', & \dots, & e_{n-1}' - e_n', \quad e_{n-1}' + e_n' - e_0'.
\end{array}$$

Additional Topics

In this chapter, we briefly treat some additional topics. In particular, we extend some earlier results from split groups to nonsplit groups. Much of this chapter is only a survey. Recall that all algebraic groups are affine over a base field k.

a. Parabolic subgroups of reductive groups

In this section, G is a reductive group over k.

THEOREM 25.1. *Let λ be a cocharacter of G. Then $P(\lambda)$ is a parabolic subgroup of G, and every parabolic subgroup of G is of this form.*

PROOF. In proving that $P(\lambda)$ is parabolic, we may suppose that k is algebraically closed. Let T be a maximal torus such that $\lambda \in X_*(T)$, and let $\Phi = \Phi(G, T)$. Then $P(\lambda)$ contains a root group U_α if and only if $\langle \alpha, \lambda \rangle \geq 0$. If λ is regular, then $P(\lambda)$ is a Borel subgroup (21.29). Otherwise, a regular λ' sufficiently close to λ will satisfy

$$\alpha \in \Phi, \quad \langle \alpha, \lambda' \rangle > 0 \implies \langle \alpha, \lambda \rangle \geq 0.$$

Then $P(\lambda)$ contains the Borel subgroup $P(\lambda')$, and so $P(\lambda)$ is parabolic.

For the converse, let P be a parabolic subgroup of G and let T be a maximal torus in P. For some finite Galois extension k' of k, the torus $T_{k'}$ splits and $P_{k'}$ contains a Borel subgroup B containing $T_{k'}$. Now $P_{k'} = P_I$ for some subset I of Δ (see 21.91), and $P_{k'} = P(\lambda)$ for every cocharacter λ of $T_{k'}$ such that I is the set of simple roots α of $(G, T)_{k'}$ orthogonal to λ (see 21.92).

The weights of T acting on the $\mathrm{Lie}(P_{k'})$ form a subset Φ' of $\Phi(G, T)$ stable under the action of $\Gamma = \mathrm{Gal}(k'/k)$, and $P_{k'} = P(\lambda)$ ($\lambda \in X_*(T)$) if and only if

$$\Phi' = \{\alpha \in \Phi(G, T) \mid \langle \alpha, \lambda \rangle \geq 0\}. \tag{166}$$

We showed in the last paragraph there exists a λ such that (166) holds. Now $\mu = \sum_{\sigma \in \Gamma} \sigma\lambda$ is a cocharacter of T defined over k satisfying (166), and so $P = P(\mu)$. $\qquad\square$

PROPOSITION 25.2. *The group G contains a proper parabolic subgroup if and only if it contains a noncentral split torus.*

PROOF. Let λ be a cocharacter of G. If $P(\lambda) = G$, then $U(\lambda)$ and $U(-\lambda)$ are smooth normal unipotent subgroups of G (13.33), and hence are trivial because G is reductive; therefore $G = Z(\lambda)$ and so $\lambda(\mathbb{G}_m) \subset Z(G)$. Conversely, if $\lambda(\mathbb{G}_m) \subset Z(G)$, then $P(\lambda) = G$. From this the statement follows. □

DEFINITION 25.3. *A reductive group is **isotropic** if it contains a noncentral split torus; otherwise, it is **anisotropic**.*[1]

Thus, the isotropic reductive groups are those containing a proper parabolic subgroup. A semisimple group is isotropic if and only if contains a nontrivial split torus.

EXAMPLE 25.4. Let D be a central division algebra over k, and let G be the algebraic group $R \rightsquigarrow (D \otimes R)^{\times}$. It is a k-form of GL_n, where $n = [D:k]^{1/2}$. If S is a split torus in D, then there exists a basis $e_1, e_2, \ldots$ for D as a k-vector space consisting of eigenvectors for the action of S on D by conjugation, i.e., such that $s e_i s^{-1} \in k e_i$ for all $s \in S(k^a)$ and all i. This implies that $S \subset Z(G)$, and so G is anisotropic.

EXAMPLE 25.5. Let $G = \mathrm{SO}(q)$ for some regular quadratic space (V, q), and assume $\mathrm{char}(k) \neq 2$. Recall that q is isotropic if $q(x) = 0$ for some nonzero $x \in V$, and otherwise it is anisotropic. In general, there exists a basis for V such that

$$q = x_1 x_n + \cdots + x_r x_{n-r+1} + q_0(x_{r+1}, \ldots, x_{n-r})$$

with q_0 anistropic (Witt decomposition; Scharlau 1985, Chapter 1, §5). Here r is the Witt index of q.

If G is isotropic, then q is isotropic, because $q(x) = 0$ for any eigenvector x of a split torus in G. Therefore G is anisotropic if q is anisotropic.

The subgroup S of G consisting of the matrices

$$\mathrm{diag}(s_1, \ldots, s_r, 1, \ldots, 1, s_r^{-1}, \ldots, s_1^{-1})$$

is a split subtorus of G. Its centralizer is isomorphic to $S \times \mathrm{SO}(q_0)$, and so S is maximal. Thus G is isotropic if and only if q is isotropic. More precisely, the k-rank of G is equal to the Witt index of q.

THEOREM 25.6. *Let P be a parabolic subgroup of G.*

(a) *The unipotent group $R_u P$ is split and the quotient $P/R_u P$ is reductive.*

(b) *If S is a maximal split torus of P, then $C_G(S)$ is a reductive subgroup of P, and $P \simeq R_u P \rtimes C_G(S)$.*

---

[1] We follow Springer 1994, p. 66, and Springer 1998, p. 271. Some authors define a reductive group to be isotropic if it contains a nontrivial split torus. The two definitions agree for semisimple groups.

    (c) *If S and S' are maximal split subtori of P, then $C_G(S)$ and $C_G(S')$ are conjugate by a unique element of $(R_uP)(k)$.*

PROOF. (a) As $P = P(\lambda)$ for some cocharacter λ of G, this follows from Proposition 17.60.

    (b) The centralizer $C_G(S)$ was shown to be reductive in Corollary 17.57. It is possible to choose the λ in (a) to be a cocharacter of S such that $C_G(S) = C_G(\lambda\mathbb{G}_m)$ (cf. 13.51). Then $P \simeq R_uP \rtimes C_G(S)$ by Theorem 13.33(b).

    (c) Springer 1998, 16.1.1.   □

LEMMA 25.7. *Let P and Q be parabolic subgroups of G. Then $P \cap Q$ is smooth, and $(P \cap Q)R_uP$ is a parabolic subgroup contained in P.*

PROOF. Proposition 21.67 shows that $P \cap Q$ is smooth. The second part of the statement is proved by examining root groups (Springer 1994, 5.2.5).   □

THEOREM 25.8. *Let P and Q be parabolic subgroups of G with P minimal. There exists a $g \in G(k)$ such that $gPg^{-1} \subset Q$. Consequently, any two minimal parabolic subgroups in G are conjugate by an element of $G(k)$.*

PROOF. As R_uP is split (25.6a), it has a fixed point in the complete variety G/Q (see 16.51). Therefore, after replacing P with a conjugate, we may suppose that $Q \supset R_uP$. Now $Q \supset (P \cap Q)R_uP$. Because P is minimal, the lemma shows that this last group equals P.   □

THEOREM 25.9. *Let P be a parabolic subgroup of G.*
    (a) *If k is infinite, then the map $\pi: G \to G/P$ has local sections, i.e., G/P is covered by open subsets over which the map has a section.*
    (b) *The map $G(k) \to (G/P)(k)$ is surjective.*

PROOF. (a) Let $P = P(\lambda)$. Then the multiplication map $U(-\lambda) \times P \to G$ is an open immersion (13.33). The image U of $U(-\lambda)$ in G/P is an open subvariety of G/P and π induces an isomorphism $U(-\lambda) \to U$. The inverse of this is a section over U. Now translate using that $G(k)$ is dense in $|G|$ (see 17.93).

    (b) When k is infinite, this follows from (a). When k is finite, it follows from Lang's theorem (17.98), because the fibre of $G \to G/P$ over a point $x \in (G/P)(k)$ is a torsor under P over k.   □

THEOREM 25.10. *Any two maximal split tori in G are conjugate by an element of $G(k)$.*

PROOF. We use induction on the dimension of G. If G contains no nontrivial split torus, there is nothing to prove. Otherwise G contains a proper parabolic subgroup P (see 25.2). Let S be a split solvable subgroup of G. When we let S act on G/P, there is a fixed point $x \in (G/P)(k)$ (see 16.51). According to Theorem 25.9 there exists a $g \in G(k)$ mapping to x. Then $SgP \subset gP$, and so $gSg^{-1} \subset P$. Thus, we may suppose that the two split tori S and S' are contained in P. Now Theorem 25.6 allows us to suppose that $C_G(S) = C_G(S')$. As this group is reductive, we can apply the induction hypothesis.   □

ASIDE 25.11. Much of the above theory extends to nonreductive groups. Let G be a connected group variety over k. A ***pseudo-parabolic subgroup*** of G is an algebraic subgroup of the form $R_uG \cdot P(\lambda)$ for some cocharacter λ of G. For reductive groups, parabolic and pseudo-parabolic subgroups coincide (21.92). Pseudo-parabolic subgroups are smooth and connected (13.33). There exists a proper pseudo-parabolic subgroup in G if and only if $G/R_u(G)$ contains a noncentral split torus (Springer 1998, 15.1.2). Any two minimal pseudo-parabolic subgroups of G are conjugate by an element of $G(k)$ (Conrad et al. 2015, C.2.5).

Parabolic subgroups and filtrations on $\mathsf{Rep}(G)$

Let V be a vector space. A homomorphism $\lambda \colon \mathbb{G}_m \to \mathrm{GL}_V$ defines a filtration

$$\cdots \supset F^sV \supset F^{s+1}V \supset \cdots, \quad F^sV = \bigoplus_{i \geq s} V_i$$

of V, where $V = \bigoplus_i V_i$ is the gradation defined by λ.

Let G be an algebraic group over a field k of cocharacteristic zero. A homomorphism $\lambda \colon \mathbb{G}_m \to G$ defines a filtration $F^\bullet$ on V for each representation (V, r) of G, namely, that corresponding to $r \circ \lambda$. These filtrations are compatible with the formation of tensor products and duals, and they are exact in the sense that the functor $V \rightsquigarrow \mathrm{Gr}^\bullet(V)$ is exact. Conversely, a functor $(V, r) \rightsquigarrow (V, F^\bullet)$ from representations of G to filtered vector spaces satisfying these conditions arises from a (nonunique) homomorphism $\lambda \colon \mathbb{G}_m \to G$. We call such a functor a ***filtration*** $F^\bullet$ of $\mathsf{Rep}(G)$, and a homomorphism $\lambda \colon \mathbb{G}_m \to G$ defining $F^\bullet$ is said to ***split*** $F^\bullet$. We write $\mathrm{Filt}(\lambda)$ for the filtration defined by λ.

For each s, we define F^sG to be the algebraic subgroup of G whose elements act as the identity map on $\bigoplus_i F^iV/F^{i+s}V$ for all representations V of G. Clearly, F^sG is unipotent for $s \geq 1$, and F^0G is the semidirect product of F^1G with the centralizer $Z(\lambda)$ of any cocharacter λ splitting $F^\bullet$.

THEOREM 25.12. *Let G be a reductive group over a field k, and let $F^\bullet$ be a filtration of $\mathsf{Rep}(G)$. From the adjoint action of G on $\mathfrak{g}$, we acquire a filtration of $\mathfrak{g}$.*

(a) *F^0G is the algebraic 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 algebraic subgroup of F^0G acting trivially on the graded module $\bigoplus_i F^iV/F^{i+1}V$ attached to each representation of G; it is the unipotent radical of F^0G, and $\mathrm{Lie}(F^1G) = F^1\mathfrak{g}$.*

(c) *The centralizer $Z(\lambda)$ of any cocharacter λ splitting $F^\bullet$ is a connected algebraic subgroup of F^0G such that the quotient map $q \colon F^0G \to F^0G/F^1G$ induces an isomorphism $Z(\lambda) \to F^0G/F^1G$; the composite $q \circ \lambda$ of λ with q is central.*

(d) *Two cocharacters λ and λ' of G define the same filtration of G if and only if they define the same group F^0G and $q \circ \lambda = q \circ \lambda'$; the cocharacters λ and λ' are then conjugate under F^1G.*

PROOF. The algebraic subgroups F^0G and F^1G of G equal $P(\lambda)$ and $U(\lambda)$ for any cocharacter λ splitting the filtration, and so this is a restatement of earlier results. See Saavedra Rivano 1972, especially IV 2.2.5. $\qquad\square$

b.   The small root system

In this section, G is a reductive group over k.

The relative roots

25.13. Let S be a maximal split torus in G. Under the adjoint action of S, the Lie algebra $\mathfrak{g}$ of G decomposes into a direct sum

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus\nolimits_{\alpha \in X(S)} \mathfrak{g}_\alpha$$

with $\mathfrak{g}_0$ the Lie algebra of $C_G(S)$ and $\mathfrak{g}_\alpha$ the subspace of $\mathfrak{g}$ on which S acts through a nontrivial character α. The characters α of S such that $\mathfrak{g}_\alpha \neq 0$ are called the ***relative roots***[2] of (G, S). They form a finite subset $_k\Phi = {}_k\Phi(G, S)$ of $X(S)$.

Semisimple groups of k-rank 1

25.14. The role of split semisimple groups of rank 1 in the split case is taken by semisimple groups of k-rank 1. Let G be such a group and let S be a maximal split torus. Choose an isomorphism $\lambda : \mathbb{G}_m \to S$, and let $P = P(\lambda)$. Then,

(a) there exists an $n \in N_G(S)(k)$ acting as $s \mapsto s^{-1}$ on S;

(b) $G(k) = P(k) \cup P(k)nP(k)$.

As in the split case, S has at least two fixed points in $(G/P)(k)$. On the other hand, the group $(N_G(S)/C_G(S))(k)$ acts faithfully on S and so it has order at most two. Therefore S has exactly two fixed points P and nP, and n is the required element.

25.15. The classification of semisimple groups of k-rank 1 is complicated because it includes the classification of all anisotropic semisimple groups (those of k-rank 0). For example, if q is a quadratic form of Witt index 1, then $\mathrm{SO}(q)$ has k-rank 1 (see 25.5). Fortunately, the classification is not needed for the proofs of the remaining results in this section.

---

[2] The "relative" means relative to the field k. Since, for us, everything is relative to the field k, we should omit the "relative", but this would be too confusing. With this terminology, the absolute roots of G are the roots of $(G, T)_{k^s}$, where T is a maximal torus T of G containing S. The relative roots are sometimes called restricted roots because they are the restrictions to S of the absolute roots (Exercise 25-1).

The relative (or small) root system

25.16. Let S be a maximal split torus in G. Let $_kV$ be the subspace of $X(S) \otimes \mathbb{Q}$ spanned by the relative roots of (G, S). The quotient $N_G(S)/C_G(S)$ acts faithfully on S, and we identify it with its image in GL_{kV}. Then,

   (a) the pair $(_kV, _k\Phi)$ is a root system;

   (b) every connected component of $N_G(S)$ meets $G(k)$;

   (c) the quotient $N_G(S)/C_G(S)$ is a finite constant group scheme canonically isomorphic to the Weyl group of the root system $(_kV, _k\Phi)$.

The proof is based on a study of semisimple groups of k-rank 1.

25.17. The pair $(_kV, _k\Phi)$ is the **relative** (or **small**) **root system** of (G, S). It is not, in general, reduced. This means that there may be roots $-2\alpha, -\alpha, \alpha, 2\alpha$ (see C.18). The Weyl group of $(_kV, _k\Phi)$ is called the **relative Weyl group** and is denoted $_kW$ or $_kW(G, S)$. The action of $N_G(S)$ on $_kV$ factors through an isomorphism $N_G(S)/C_G(S) \to {}_kW$ (finite constant group schemes). In particular, it preserves $_k\Phi$. Every coset of $C_G(S)$ in $N_G(S)$ is represented by an element of $N_G(S)(k)$. The set of $\alpha \in {}_k\Phi$ such that $\frac{1}{2}\alpha \notin {}_k\Phi$ is a reduced root system $_k\Phi_i$ in $_kV$. A **base** for $_k\Phi$ is defined to be a base for $_k\Phi_i$, and a **system of positive roots** in $_k\Phi$ is a set of the form $\mathbb{N}\Delta$ with Δ a base.

25.18. The centralizer $C_G(S)$ of S in G is a reductive group over k (see 17.57). Its derived group $C_G(S)'$ is an anisotropic semisimple group, called the **anisotropic semisimple kernel**. It is one ingredient in the classification of nonsplit groups.

The root groups

25.19. Let S be a maximal split in G. Let T be a maximal torus containing S, and let Φ be the set of roots of $(G, T)_{k^s}$. Then $_k\Phi$ is the set of nontrivial restrictions to S of elements of Φ (Exercise 25-1). Let $\alpha \in {}_k\Phi$. The subgroup of G_{k^s} generated by the root groups U_β in G_{k^s} such that $\beta|S = \alpha$ is defined over k. It is denoted $_kU_\alpha$ and called the **root group** of α. It is the unique unipotent subgroup of G normalized by S with Lie algebra $\mathfrak{g}_\alpha$. It is a split unipotent group.

25.20. If G is split over k, then $_kU_\alpha$ is the usual root group; in particular it has dimension 1. In general, $\dim(_kU_\alpha) = \dim \mathfrak{g}_\alpha + \dim \mathfrak{g}_{2\alpha}$.

Example: special orthogonal groups

25.21. Let $G = SO(q)$ with q as in Example 25.5. Write $q_0(x) = x^t M_0 x$. Then the Lie algebra of G consists of the matrices

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & -M_0 A_{12}^t \\ A_{31} & -A_{21}^t M_0^{-1} & -A_{11}^t \end{pmatrix}$$

with A_{13} and A_{31} skew-symmetric and $A_{22}^t = -M_0^{-1} A_{22} M_0$. The diagonal torus S acts on $\mathrm{Lie}(G)$ by conjugation. The root system ${}_k\Phi$ of (G, S) is of type B_r unless $n = 2r$, in which case it is of type D_r. The elements of G that are upper triangular in this block decomposition (so $A_{21} = 0 = A_{31}$) form a minimal parabolic subgroup of G.

Parabolic subgroups

25.22. Any two minimal parabolic subgroups of G are conjugate by an element of $G(k)$ (see 25.8). Let S be a maximal split torus in G. The minimal parabolic subgroups containing S are indexed by the Weyl chambers of the root system $({}_kV, {}_k\Phi)$, and they are permuted simply transitively by the relative Weyl group.

25.23. Let P be a minimal parabolic subgroup of G, and let S be a maximal split torus in P. Then $P = R_u(P) \rtimes C_G(S)$ (see 25.6), and P defines a base ${}_k\Delta$ for ${}_k\Phi$. For a subset $I \subset {}_k\Delta$, let P_I denote the algebraic subgroup of G generated by $C_G(S)$ and the root groups U_α such that, when α is expressed as a linear combination of the elements of ${}_k\Delta$, the roots not in I occur with nonnegative coefficients. Then
$$G = P_{{}_k\Delta} \supset P_I \supset P_\emptyset = P.$$
In particular, P is generated by $C_G(S)$ and the root groups U_α with α positive. The P_I are the **standard parabolic subgroups** of G containing P. Every parabolic subgroup is conjugate by an element of $G(k)$ to a unique P_I. The reduced identity component S_I of $\bigcap_{\alpha \in I} \mathrm{Ker}\,\alpha$ is a split torus in G, and
$$P_I = R_u(P_I) \rtimes C_G(S_I).$$
Moreover, $R_u(P_I)$ is generated by the U_α, where α runs over the positive roots that are not linear combinations of elements of I.

25.24. Let Q be a parabolic subgroup of G with unipotent radical U. A **Levi subgroup** of Q is an algebraic subgroup L such that Q is the semidirect product $Q = U \rtimes L$. Such a subgroup is reductive (25.6a). It follows from 25.23 that a Levi subgroup in Q always exists. Any two Levi subgroups of Q are conjugate by an element of $G(k)$. For any maximal split subtorus of the centre of L, we have $L = C_G(S)$.

25.25. If S is a split subtorus of G, then there is a parabolic subgroup Q of G with Levi subgroup $C_G(S)$. Two such Q are not necessarily conjugate by an element of $G(k)$ (as they are when S is a maximal split torus). Two parabolic subgroups Q_1 and Q_2 are said to be associated if they have Levi subgroups that are conjugate by an element of $G(k)$. This defines an equivalence relation on the set of parabolic subgroups.

25.26. Let P and Q be parabolic subgroups. Then $(P \cap Q) R_u(P)$ is a parabolic subgroup contained in P (see 25.26). It equals P if and only if some Levi subgroup of P contains a Levi subgroup of Q. Parabolic subgroups P and Q are said to be **opposite** if $P \cap Q$ is a Levi subgroup of P and Q.

BRUHAT DECOMPOSITION OF $G(k)$

25.27. Let P be a parabolic subgroup of G with unipotent radical U, and let S be a split torus such that $P = U \rtimes C_G(S)$. Then

$$G(k) = \bigsqcup_{w \in {}_kW} U(k)wP(k) \quad \text{(Bruhat decomposition)}.$$

As in the split case, this can be made more precise. Let $n_w \in N_G(S)(k)$ represent $w \in {}_kW$. There exist two subgroup varieties U_w and U^w of U such that

$$U \simeq U_w \times U^w \quad \text{(product of varieties)}$$

and the map

$$(u, p) \mapsto un_w p : U^w \times P \to Un_w P$$

is an isomorphism of algebraic varieties. We then have

$$G/P = \bigsqcup_{w \in {}_kW} U^w n_w P/P$$
$$G = \bigsqcup_{w \in {}_kW} U^w n_w P$$

(decompositions of smooth algebraic varieties).

The reflections s_α with $\alpha \in {}_kW$ form a set of generators ${}_kS$ of ${}_kW$, and $(G(k), P(k), N_G(S)(k), {}_kS)$ is a Tits system. This implies the above statements on the level of sets (Theorem 21.45 and Exercise 21-5).

NOTES. The original reference for most of the results in this section is Borel and Tits 1965, 1972. The exposition partly follows that in Springer 1979. For proofs, see Borel 1991, V.21, and Springer 1998, Chapter 15.

c.   The Satake–Tits classification

A theorem of Witt says that a regular quadratic space is determined up to isomorphism by its index and its anistropic direct summand (cf. 25.5). In this section, we explain a similar result for reductive groups. Throughout, G is a reductive group over k and $\Gamma = \mathrm{Gal}(k^s/k)$.

Let S be a maximal split torus in G and T a maximal torus containing S. Then $(G, T)_{k^s}$ is split, and so T_{k^s} is contained in a Borel subgroup B of G_{k^s} (see 21.30). Let $(X, \Phi, \Phi^\vee, \Delta)$ be the based root datum of (G_{k^s}, B, T_{k^s}) (see 23.38). As was explained in (21.43), this is independent of the choice of (B, T) and so, even though the action of Γ on G_{k^s} need not preserve B, it does define an action of Γ on $(X, \Phi, \Phi^\vee, \Delta)$. We make this explicit. As the action of Γ on G_{k^s} preserves T_{k^s}, there are natural actions of Γ on $X = X^*(T)$ and $X^\vee = X_*(T)$. These preserve Φ and $\Phi^\vee$. If σ is an element of Γ, then $\sigma(\Delta)$ is also a base for Φ, and so $w_\sigma(\sigma(\Delta)) = \Delta$ for a unique $w_\sigma \in W$ (see 21.41). For $\alpha \in \Delta$,

define $\sigma * \alpha = w_\sigma(\sigma\alpha)$. This does define an action of Γ on Δ, and it is obviously continuous. It is called the *-*action*.

Let Δ_0 be the set of $\alpha \in \Delta$ whose restriction to S is trivial. Then Γ stabilizes both Δ_0 and its complement in Δ (Springer 1998, 15.5.3). The elements of $\Delta \smallsetminus \Delta_0$ are called ***distinguished***.

PROPOSITION 25.28. *(a) The group G is quasi-split if and only if $\Delta_0 = \emptyset$, in which case the $*$-action is the natural action of Γ on Δ as a subset of X.*
  (b) The group G is anisotropic if and only if $\Delta_0 = \Delta$.

PROOF. If G is quasi-split, we choose B to be defined over k, and then it is obvious that Δ is stable under Γ. For the rest, see Springer 1998, 16.2.2.   □

Let $V = \mathbb{Z}\Phi \otimes \mathbb{Q}$. Then (V, Φ) is a root system, and we let $\mathcal{D}$ denote the Dynkin diagram of (V, Φ, Δ). Its nodes are indexed by the elements of Δ. We write $*$ for the $*$-action of Γ on the nodes of $\mathcal{D}$.

DEFINITION 25.29. The triple $(\mathcal{D}, \Delta_0, *)$ is called the ***index*** (or ***Tits index*** or ***Satake diagram***) of G, and is denoted by $I(G)$.

Up to isomorphism, the index depends only on G. When k is replaced by an extension field k', the Dynkin diagram $\mathcal{D}$ is unchanged, distinguished simple roots remain distinguished, and the $*$-action for $G_{k'}$ is obtained from that for G by composing with the map $\mathrm{Gal}(k'^s/k') \to \mathrm{Gal}(k^s/k)$ (here $k^s \subset k'^s$). Traditionally, the index is illustrated by marking the distinguished nodes in the Dynkin diagram and circling the Γ-orbits in $\Gamma \smallsetminus \Gamma_0$. See Tits 1966 and Selbach 1976.

As Tits (1966, pp. 40–41) explains, it is possible to recover the relative root system of (G, S) from $I(G)$.

Let G_0 denote the derived group of $C_G(S)$. It is a connected anisotropic semisimple group over k, called the semisimple anisotropic kernel of G. Its Dynkin diagram is the full subgraph $\mathcal{D}_0$ of $\mathcal{D}$ with nodes indexed by the elements of Δ_0.

THEOREM 25.30. *A reductive group G over k is determined up to isomorphism by its isomorphism class over k^s, its index, and its semisimple anisotropic kernel (as a subgroup of G).*

More precisely, let G and G' be two reductive groups over k, and let T and T' be maximal tori in G and G' containing maximal split tori S and S'. If there exists an isomorphism of algebraic groups $\varphi \colon G_{k^s} \to G'_{k^s}$ such that

(a) $\varphi(T_{k^s}) = T'_{k^s}$,

(b) φ restricts to an isomorphism $G_0 \to G'_0$ defined over k, and

(c) φ induces an isomorphism of $I(G)$ onto $I(G')$,

then there exists an isomorphism $G \to G'$ (Springer 1994, 6.1.2).

EXAMPLE 25.31. Let $G = \mathrm{SO}(q)$, S, and q_0 be as in 25.5 and 25.21. Assume that $n - 2r$ is odd. Let T_0 be a maximal torus in $\mathrm{SO}(q_0)$, and identify it with a torus in $\mathrm{SO}(q)$ by identifying A with $\mathrm{diag}(I_r, A, I_r)$. Then $T \stackrel{\text{def}}{=} S \times T_0$ is a maximal torus containing S. The set $\Delta \smallsetminus \Delta_0$ consists of the first r nodes of $\mathcal{D}$.

EXAMPLE 25.32. Let D be a central division algebra over k of degree d^2, and let $\mathrm{GL}_{r+1,D}$ be the algebraic group representing $R \rightsquigarrow \mathrm{GL}_{r+1}(D \otimes R)$. It becomes isomorphic to $\mathrm{GL}_{(r+1)d}$ over any field k' splitting D (in particular, over k^{s}; 24.20). There is a natural embedding of GL_{r+1} in $\mathrm{GL}_{r+1,D}$, and the image of any split maximal torus in GL_{r+1} is a maximal split torus in $\mathrm{GL}_{r+1,D}$. Suitably numbered $\Delta \smallsetminus \Delta_0$ is the subset $\{\alpha_d, \alpha_{2d}, \ldots\}$ of $\Delta = \{\alpha_1, \ldots, \alpha_{(r+1)d-1}\}$.

The next result extends Theorem 23.62 to the nonsplit case.

THEOREM 25.33. *Two semisimple groups over k are strictly isogenous if and only if they become strictly isogenous over k^{s}, their anistropic semisimple kernels are isogenous, and their indices are isomorphic.*

PROOF. See Tits 1966, 2.6, 2.7. □

Isogenous semisimple groups need not have isomorphic indices. Indeed, there exists a quadratic form q in characteristic 2 such that $\mathrm{SO}(q)$ is isogenous to SL_2 but the two groups have different k-ranks (18.3; Tits 1966, 2.6.4).

After Theorem 25.33, the problem of classifying the semisimple groups over a field k comes down to the following two problems:

(a) determine the indices arising from semisimple groups over k;

(b) for a given index, find all possible semisimple anistropic kernels.

As in Section 24b, we need only consider the simply connected almost-simple case. Much is known about (a), and much is known about (b) for certain fields. However, for a general field, little is known about (b), essentially because little is known about the division algebras over the field.

NOTES. The theory sketched in this section originated with Satake's article, Satake 1963, and with Tits's talk at the 1965 Boulder conference (Tits 1966). Tits's report on his talk was expanded and completed by Selbach in his 1973 Diplomarbeit (Selbach 1976). See also the 1967 lectures of Satake (Satake 1971). In addition to the original sources, the topic is treated in Springer 1998, Chapters 16 and 17.

d. Representation theory

Let T be a torus over k, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{s}}/k)$. Recall (12.30) that there is the following description of the finite-dimensional representations of T over k. For each $\chi \in X^*(T)$, the one-dimensional representation $V(\chi)$ on which T acts through χ is defined over k; it is absolutely simple, and every absolutely simple representation of T over k is isomorphic to $V(\chi)$ for a unique χ. For each orbit Ξ of Γ on $X^*(T)$, there is a representation $V(\Xi)$ of T over k such that $V(\Xi)_{k^{\mathrm{s}}}$

is a direct sum of one-dimensional eigenspaces with characters the χ in Ξ; it is simple, and every simple representation of T over k is isomorphic to $V(\Xi)$ for a unique Γ-orbit Ξ.

One can ask whether similar statements hold for an arbitrary reductive group over k. The answer is yes, but not in any naive sense unless G is quasi-split.

Let G be a reductive group over k. Choose a maximal torus T in k and a Borel subgroup B in G_{k^s} containing T_{k^s}. Let $\Delta \subset X \stackrel{\text{def}}{=} X^*(T)$ be the set of simple roots corresponding to B, and let

$$X^+ = \{\lambda \in X \mid \langle \lambda, \alpha^\vee \rangle \geq 0 \text{ for all } \alpha \in \Delta\}$$

be the set of dominant weights. For each dominant λ, there is a simple representation $V(\lambda)$ of G over k^s, and every simple representation of G over k^s is isomorphic to $V(\lambda)$ for a unique λ (see 22.2). The first problem we run into is that the natural action of Γ on X need not preserve the set of dominant weights (because the action of Γ need not preserve B or Δ). Instead, we must use the action of Γ on X^+ deduced from the $*$-action of Γ on Δ (see p. 551). The second problem is that, if a dominant λ is fixed by Γ, then $V(\lambda)$ need not be defined over k, but only over a certain division algebra $D(\lambda)$ over k. Nevertheless, it does turn out that the simple representations of G over k are classified by the Γ-orbits of dominant weights.

This theory is worked out in detail in Tits 1971 (for earlier results, see Borel and Tits 1965, 12.6, 12.7, and Satake 1967, I, II). We now sketch it.

Representations over an algebra

By an algebra A over k in this section, we mean an associative algebra over k of finite degree (not necessarily commutative). Let A be an algebra over k and M a finitely generated A-module. We define $\mathrm{GL}_{M,A}$ to be the algebraic group over k such that, for every k-algebra R, $\mathrm{GL}_{M,A}(R)$ is the group of $A \otimes R$-linear automorphisms of $M \otimes R$. It is naturally an algebraic subgroup of GL_M (M regarded as a k-vector space). When M is the free module A^m, $m \in \mathbb{N}$, we write $\mathrm{GL}_{m,A}$ for $\mathrm{GL}_{M,A}$.

Let A be a simple algebra over k, and let S be a simple A-module. The centralizer of A in the k-algebra $\mathrm{End}_k(S)$ of k-linear endomorphisms of S is a division algebra D. If S has dimension d as a D-vector space, then $A \approx M_d(D)$. As D is a division algebra, we can make S into a right D-module. Then $M \rightsquigarrow S \otimes_D M : \mathrm{Mod}_D \to \mathrm{Mod}_A$ is an equivalence of categories (A.63). Let M be an A-module, and M_1 a D-module mapped to M by this functor. Then

$$\mathrm{GL}_{M_1,D} \simeq \mathrm{GL}_{M,A}. \tag{167}$$

Let D be a central division algebra over k and M a D-module. A D-**representation** of G on M is a homomorphism $r : G \to \mathrm{GL}_{M,D}$ of algebraic groups over k. Let $A = D \otimes k^s$. Then A is a matrix algebra over k^s, and so (167)

becomes

$$\mathrm{GL}_{M_1,k^s} \simeq \mathrm{GL}_{M \otimes k^s, D \otimes k^s}$$

with M_1 a suitable k^s-vector space such that $\dim_{k^s}(M_1) = [D:k]^{1/2} \cdot \dim_D(M)$. Therefore, a D-representation $r: G \to \mathrm{GL}_{M,D}$ defines a representation $r_1: G_{k^s} \to \mathrm{GL}_{M_1}$. We say that a representation of G_{k^s} is **defined over** D if it arises in this way.

The Tits class and the Tits algebra

Let G be a simply connected semisimple algebraic group over k. There is a quasi-split group G_0 over k, unique up to isomorphism, and an isomorphism $f: G_{0k^s} \to G_{k^s}$ such that (G, f) is an inner form of G_0 (see 23.53). Let $\gamma \in H^1(k, G_0^{\mathrm{ad}})$ be the cohomology class of (G, f). From the exact sequence

$$e \to Z(G_0) \to G_0 \to G_0^{\mathrm{ad}} \to e$$

we get a boundary map $\delta: H^1(k, G_0^{\mathrm{ad}}) \to H^2(k, Z(G_0))$ (flat cohomology). As was explained in Section 24c, $Z(G_0) \simeq Z(G)$. Let t_G denote the image of $\delta(\gamma)$ under the isomorphism

$$H^2(k, Z(G_0)) \simeq H^2(k, Z(G)).$$

Then t_G is called the **Tits class** of G. When G is not simply connected, its Tits class is defined to be that of its simply connected cover (so $t_G \in H^2(k, Z(\tilde{G}))$). By definition, t_G depends only on the strict isogeny class of G. Obviously it is zero if G is quasi-split.

Let χ be a character of $Z(\tilde{G})$, and let $k(\chi)$ be its field of definition (i.e., $k(\chi)$ is the subfield of k^s fixed by the subgroup of Γ fixing χ). Then χ is a homomorphism $Z(\tilde{G})_{k(\chi)} \to \mathbb{G}_{m,k(\chi)}$, and we write $\chi(t_G)$ for the image of t_G under

$$H^2(k, Z(\tilde{G})) \to H^2(k(\chi), Z(\tilde{G})_{k(\chi)}) \overset{H^2(\chi)}{\longrightarrow} H^2(k(\chi), \mathbb{G}_m).$$

The Brauer group of $k(\chi)$ is canonically isomorphic to the cohomology group $H^2(k(\chi), \mathbb{G}_m)$ (Serre 1962, X, §5). We define the **Tits algebra** $D(\chi)$ to be the central division algebra over $k(\chi)$ whose class $[D(\chi)]$ in the Brauer group corresponds to $\chi(t_G)$ under this isomorphism. It is uniquely determined up to isomorphism.

Statements of the main theorems

Let G be a simply connected semisimple group over k and T a maximal torus in G. We fix a Borel subgroup B of G_{k^s} containing T_{k^s}. The Galois group Γ acts on the dominant weights through the $*$-action.

THEOREM 25.34. *Let λ be a dominant weight of G. If λ is fixed by Γ, then the simple representation of G_{k^s} of highest weight λ is defined over $D(\lambda)$.*

PROOF. Tits 1971, 3.3.   □

In more detail, a dominant weight λ restricts to a character of $Z(G)$, and we let $D(\lambda)$ denote the corresponding Tits algebra. The theorem says that there exists a $D(\lambda)$-module M and a representation $r: G \to \mathrm{GL}_{M,D(\lambda)}$ such that the corresponding representation $r_1: G_{k^s} \to \mathrm{GL}_{M_1}$ (see above) is simple of highest weight λ. Tits's theorem also includes a uniqueness statement. If $r': G \to \mathrm{GL}_{M',D(\lambda)}$ is a second representation with the same property, then there is an isomorphism of $D(\lambda)$-modules $M \to M'$ such that r' is the composite of r with the map $\mathrm{GL}_{M,D(\lambda)} \to \mathrm{GL}_{M',D(\lambda)}$ defined by the isomorphism.

COROLLARY 25.35. *Let λ be a dominant weight of G fixed by Γ, and let $d^2 = [D(\lambda):k]$. There exists a representation $r': G \to \mathrm{GL}_V$ such that $(V,r')_{k^s}$ is isomorphic to a direct sum of d simple representations each with highest weight λ.*

PROOF. Let $r: G \to \mathrm{GL}_{M,D}$ be the representation in Theorem 25.34. As noted above, $\mathrm{GL}_{M,D}$ is naturally an algebraic subgroup of GL_M (M regarded as a k-vector space). The composite of r with the inclusion $\mathrm{GL}_{M,D} \hookrightarrow \mathrm{GL}_M$ has the required property.   □

Let λ be a dominant weight, and let $k(\lambda)$ be its field of definition. The Tits algebra $D(\lambda)$ is a central division algebra over $k(\lambda)$, whose degree we denote by d^2. According to the corollary, there exists a representation $r_1: G_{k(\lambda)} \to \mathrm{GL}_{V_1}$ over $k(\lambda)$ such $(V_1,r_1) \otimes_{k(\lambda)} k^s \approx V(\lambda)^{\oplus d}$. By the universality of the Weil restriction functor (2.57), r_1 corresponds to a homomorphism

$$r_2: G \to \Pi_{k(\lambda)/k}(\mathrm{GL}_{V_1}) \simeq \mathrm{GL}_{V_1,k(\lambda)},$$

and there is a natural inclusion $\mathrm{GL}_{V_1,k(\lambda)} \hookrightarrow \mathrm{GL}_{V_1}$ (V_1 regarded as a k-vector space). We define $_k r(\lambda)$ to be the composite of r_2 with this homomorphism.

THEOREM 25.36. *For every dominant weight λ, the representation $_k r(\lambda)$ is simple, and every simple representation of G is equivalent to a representation of this form. The representations $_k r(\lambda)$ and $_k r(\lambda')$ corresponding to two dominant weights λ and λ' are equivalent if and only if $\sigma(\lambda) = \lambda'$ for some $\sigma \in \Gamma$.*

PROOF. Tits 1971, 7.2.   □

In particular the isomorphism classes of simple representations of G over k are classified by the orbits of Γ in X^+. Note, however, that if (V,r) is the representation corresponding to an orbit $\{\lambda_1, \ldots, \lambda_r\}$, then (V,r) becomes isomorphic over k^s, not to

$$V(\lambda_1) \oplus \cdots \oplus V(\lambda_r),$$

but to a direct sum of d copies of this representation.

EXAMPLE 25.37. If G is quasi-split, then there exists a Borel subgroup B in G and we take T to be a maximal torus in B. As B is stable under the action of Γ, the $*$-action on Δ is the natural action on it as a subset of X. Moreover, the Tits algebra $D(\lambda)$ of a dominant weight equals $k(\lambda)$. Thus,

   (a) if a fundamental weight λ is fixed by Γ, then $V(\lambda)$ is defined over k, and every absolutely simple representation of G over k is isomorphic to $V(\lambda)$ for a unique λ;

   (b) if Ξ is a Γ-orbit in X^+, then the representation $V(\Xi) \stackrel{\text{def}}{=} \bigoplus_{\lambda \in \Xi} V(\lambda)$ is defined over k, and every simple representation of G over k is isomorphic to $V(\Xi)$ for a unique Γ-orbit Ξ.

e.   Pseudo-reductive groups

We briefly summarize Conrad et al. 2015, which completes earlier work of Borel and Tits (Borel and Tits 1978; Tits 1992, 1993; Springer 1998, Chapters 13–15).

Recall (6.47) that a smooth connected algebraic group G is pseudo-reductive if $R_u(G) = e$. For example, G is pseudo-reductive if it admits a faithful semi-simple representation (19.17).

25.38. We gave an example of a nonreductive pseudo-reductive group in 6.48. We now construct another. Let $G = (\mathbb{G}_m)_{k'/k}$, where k is infinite and k'/k is purely inseparable of degree p. Then G is a smooth connected commutative algebraic group over k. The canonical map $\mathbb{G}_m \to G$ realizes $\mathbb{G}_m$ as the largest subgroup of G of multiplicative type, and the quotient $G/\mathbb{G}_m$ is unipotent (Exercise 2-10). Over k^a, G decomposes into $(\mathbb{G}_m)_{k^a} \times (G/\mathbb{G}_m)_{k^a}$ (see 16.13), and so G is not reductive. However, G contains no smooth unipotent subgroup because $G(k)$ is dense in G (Exercise 12-10) and $G(k)$ contains no element of order p (it equals $(k')^\times$).

25.39. Let k' be a finite field extension of k, and let G be a reductive group over k'. If k' is separable over k, then $(G)_{k'/k}$ is reductive, but otherwise it is only pseudo-reductive. For example, if k'/k is purely inseparable of degree p, then G is a nonreductive pseudo-reductive group as in 25.38.

25.40. Let C be a commutative connected algebraic group over k. If C is reductive, then it is a torus, and the tori are classified by the continuous actions of $\mathrm{Gal}(k^s/k)$ on free commutative groups of finite rank. By contrast, "it seems to be an impossible task to describe general commutative pseudo-reductive groups over imperfect fields" (Conrad et al. 2015, p. xvii). The main theorem of Conrad et al. 2015 describes all pseudo-reductive groups in terms of commutative pseudo-reductive groups and the Weil restrictions of reductive groups.

25.41. Let $k_1,\ldots,k_n$ be finite field extensions of k. For each i, let G_i be a reductive group over k_i, and let T_i be a maximal torus in G_i. Define algebraic groups

$$G \hookleftarrow T \twoheadrightarrow \bar{T}$$

by
$$G = \prod_i (G_i)_{k_i/k}, \quad T = \prod_i (T_i)_{k_i/k}, \quad \bar{T} = \prod_i (T_i/Z(G_i))_{k_i/k}.$$

Let $\phi: T \to C$ be a homomorphism of commutative pseudo-reductive groups that factors through the quotient map $T \to \bar{T}$:

$$T \xrightarrow{\phi} C \xrightarrow{\psi} \bar{T}.$$

Then ψ defines an action of C on G by conjugation, and so we can form the semidirect product $G \rtimes C$. The map

$$t \mapsto (t^{-1}, \phi(t)): T \to G \rtimes C$$

is an isomorphism from T onto a central subgroup of $G \rtimes C$, and the quotient $(G \rtimes C)/T$ is a pseudo-reductive group over k. The main theorem (5.1.1) of Conrad et al. 2015 says that, except possibly when k has characteristic 2 or 3, every pseudo-reductive group over k arises by such a construction (the theorem also treats the exceptional cases).

25.42. The maximal tori in reductive groups are their own centralizers. Any pseudo-reductive group with this property is reductive (except possibly in characteristic 2; Conrad et al. 2015, 11.1.1).

25.43. If G is reductive, then $G = \mathcal{D}G \cdot (ZG)_t$, where $\mathcal{D}G$ is the derived group of G and $(ZG)_t$ is the largest central connected reductive subgroup of G. This statement becomes false with "pseudo-reductive" for "reductive" (*ibid.*, 11.2.1).

25.44. For a reductive group G, the map $RG = (ZG)^\circ \to G/\mathcal{D}G$ is an isogeny, and G is semisimple if and only if one of these groups (hence both) is trivial. For a pseudo-reductive group, the condition $RG = e$ does not imply that $G = \mathcal{D}G$. Conrad et al. 2015, 11.2.2, instead adopt the following definition: an algebraic group G is **pseudo-semisimple** if it is pseudo-reductive and $G = \mathcal{D}G$. The derived group of a pseudo-reductive group is pseudo-semisimple.

25.45. Every reductive group G over a field k is unirational, and so $G(k)$ is dense in G if k is infinite. This fails for pseudo-reductive groups: over every nonperfect field k there exists a commutative pseudo-reductive group that is not unirational, and $G(k)$ need not be dense in G for infinite k (*ibid.*, 11.3.1).

f. Nonreductive groups: Levi subgroups

In the last nine chapters, we have concentrated on reductive subgroups. Every connected group variety G over a field k is an extension

$$e \to R_u(G) \to G \to G/R_u(G) \to e$$

of a pseudo-reductive group by a unipotent group. If k is perfect, then the quotient $G/R_u(G)$ is reductive and the unipotent group $R_u(G)$ is split. In good cases, the extension itself splits.

DEFINITION 25.46. Let G be a connected group variety over k. A ***Levi subgroup*** of G is a connected subgroup variety L such that the quotient map $G_{k^a} \to G_{k^a}/R_u G_{k^a}$ restricts to an isomorphism $L_{k^a} \to G_{k^a}/R_u G_{k^a}$.

In other words, L is a reductive subgroup of G such that $G_{k^a} = R_u G_{k^a} \rtimes L_{k^a}$ (see 2.34). When a Levi subgroup exists, to some extent the study of G reduces to the study of a reductive group and a unipotent group.

Notes

25.47. Let P be a parabolic subgroup of a reductive group G over k. Then P admits a Levi subgroup, and any two Levi subgroups are conjugate by a unique element of $(R_u P)(k)$ (see 25.6).

25.48. Suppose that there exists an algebraic subgroup R of G such that $R_{k^a} = R_u(G_{k^a})$ (so R is smooth, connnected, unipotent, and normal, and G/R is reductive). Then a Levi subgroup of G is a connected subgroup variety L such that the quotient map $G \to G/R$ restricts to an isomorphism $L \to G/R$. In this case, G is the semidirect product $G = R \rtimes L$ of a reductive group L with a unipotent group R.

25.49. When k is perfect, a subgroup R as in 25.48 always exists (19.9). In characteristic zero, Levi subgroups always exist and any two are conjugate by an element of the unipotent radical (Theorem of Mostow; Hochschild 1981, VIII, Theorem 4.3).

25.50. Every pseudo-reductive group with a split maximal torus has a Levi subgroup (Conrad et al. 2015, 3.4.6).

25.51. In nonzero characteristic, a connected group variety G need not have a Levi subgroup, even when the base field is algebraically closed. An example is $SL_n(W_2(k))$, $n > 1$, regarded as an algebraic group over k. Moreover, a group variety can have Levi subgroups that are not geometrically conjugate.

For recent work on Levi subgroups, see McNinch 2010, 2013, 2014a.

g. Galois cohomology

Having persuaded the reader of the usefulness of Galois cohomology groups, we now study them in their own right. Let G be an algebraic group over k. In this section, we write $H^1(k, G)$ for the flat cohomology group (2.72). When G is smooth, it is canonically isomorphic to the Galois cohomology group $H^1(\Gamma, G(k^s))$, $\Gamma = \mathrm{Gal}(k^s/k)$ (they both classify the isomorphism classes of G-torsors over k; see 3.50).

Tori

Recall (12.62) that a torus T is induced if it is a finite product of tori of the form $(\mathbb{G}_m)_{k'/k}$ with k' finite and separable over k. If $T = \prod_i (\mathbb{G}_m)_{k_i/k}$, then

$$H^1(k, T) \overset{3.44}{\simeq} \prod_i H^1(k_i, \mathbb{G}_m) \overset{3.47}{=} 1.$$

If T is induced over k, then $T_{k'}$ is induced over k' for all fields $k' \supset k$, and so $H^1(k', T_{k'}) = 1$. This property characterizes direct factors of induced tori.

Finite fields; fields of dimension ≤ 1

A field k is said to have dimension ≤ 1 if every finite-dimensional division algebra over k is commutative. An equivalent condition is that $\mathrm{Br}(k') = 0$ for all fields k' algebraic over k. Finite fields and fields of transcendence degree 1 over an algebraically closed field have dimension ≤ 1 (Tsen's theorem[3]).

The next theorem generalizes Lang's theorem (17.98).

THEOREM 25.52. *Let G be a connected group variety over a field k of dimension ≤ 1. If k is perfect or G is reductive, then $H^1(k, G) = 1$.*

PROOF. See Steinberg 1965, 1.9, and Borel and Springer 1968, 8.6.   □

COROLLARY 25.53. *Let k be a perfect field of dimension ≤ 1. Every connected group variety over k is quasi-split.*

PROOF. This follows from 25.52 in the same way that 17.99 follows from 17.98.□

The field of real numbers

THEOREM 25.54 (CARTAN). *Let G be a semisimple algebraic group over $\mathbb{R}$. If G is simply connected, then $G(\mathbb{R})$ is connected.*

PROOF. If $G = (H)_{\mathbb{C}/\mathbb{R}}$ for H a connected group variety over $\mathbb{C}$, then $G(\mathbb{R}) = H(\mathbb{C})$, which is connected for the complex topology. If G is absolutely almost-simple, then the statement is proved in Platonov and Rapinchuk 1994, Theorem 7.6, p. 407. The general case now follows from these two cases (24.3).   □

COROLLARY 25.55. *Let G be a reductive algebraic group over $\mathbb{R}$. Then $G(\mathbb{R})$ has only finitely many components for the real topology.*

---

[3]Tsen was a student of Emmy Noether, and this was part of his thesis. Let k_0 be an algebraically closed field. Tsen first proved the following statement: let $f_1, \ldots, f_r \in k_0(X)[T_1, \ldots, T_r]$ be homogeneous of degree d; if $n > rd$ then the equations $f_1 = 0, \ldots, f_r = 0$ have a common nontrivial solution in $k_0(X)$. It follows that, if D is a central division algebra over a finite extension k of $k_0(X)$, then the norm map $\mathrm{Nm} \colon D^\times \to k^\times$ is surjective. Now let $[D:k] = n^2$, and let $\mathrm{Nm}(d) = X$. Then $X = \mathrm{Nm}(d) = \mathrm{Nrd}(d)^n$, and so $X^{1/n} \in k$. Similarly, $X^{1/n^2}, X^{1/n^3}, \ldots$ $\in k$, which is impossible unless $n = 1$.

PROOF. For a torus, this can be proved directly. For a general G, there is an exact sequence

$$e \to N \to G' \times T \to G \to e \qquad (168)$$

with G' the simply connected covering of G^{der}, T the torus $Z(G)_t$, and N finite. The group $H^1(\mathbb{R}, N)$ is finite, from which the statement follows. □

THEOREM 25.56 (CARTAN). *Every semisimple algebraic group over $\mathbb{R}$ has an anisotropic form, which is unique up to isomorphism.*

PROOF. See Harder 1965, 3.3.2. □

THEOREM 25.57 (CARTAN). *Let G be an anisotropic semisimple algebraic group over $\mathbb{R}$. Then any two maximal tori in G are conjugate by an element of $G(\mathbb{R})$.*

PROOF. For a short proof, see Suzuki 1971, Theorem 2. □

THEOREM 25.58. *Let G be a reductive algebraic group over $\mathbb{R}$, and let T_0 be a maximal compact torus in G. The centralizer of T_0 in G is a torus T, and $W_0 = N_G(T_0)/T$ is a finite group acting on $H^1(\mathbb{R}, T)$. The map $H^1(\mathbb{R}, T) \to H^1(\mathbb{R}, G)$ induces an isomorphism*

$$H^1(\mathbb{R}, T)/W_0(\mathbb{R}) \to H^1(\mathbb{R}, G).$$

PROOF. See Borovoi 2014, Theorem 9. □

COROLLARY 25.59 (BOREL AND SERRE). *Let G be an anisotropic semisimple algebraic group over $\mathbb{R}$. Then*

$$T(\mathbb{R})_2/W \simeq H^1(\mathbb{R}, G),$$

where $T(\mathbb{R})_2$ denotes the set of elements of order ≤ 2 in $T(\mathbb{R})$ and W is the Weyl group.

PROOF. Special case of the theorem. □

ASIDE 25.60. Using Kac diagrams, Borovoi and Timashev (2015) describe combinatorially the cohomology sets $H^1(\mathbb{R}, G)$ for all inner forms G of an anisotropic semisimple algebraic group H over $\mathbb{R}$. See also Adams 2013.

Local fields

By a local field in this subsection, we mean a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((T))$.

THEOREM 25.61. *Let G be a semisimple group over a local field k.*
  (a) *If G is simply connected, then $H^1(k, G) = 1$.*
  (b) *If G is simply connected, almost-simple, and anisotropic, then it is isomorphic to $\mathrm{SL}_1(D)$ for some finite-dimensional division algebra D.*

PROOF. These statements were proved in characteristic zero by Kneser and extended to more general local fields by Bruhat and Tits (1987, 4.3). See Platonov and Rapinchuk 1994, Theorems 6.4, 6.5, pp. 284–285 (characteristic zero only).□

THEOREM 25.62. *Let G be a semisimple group over a local field k and let $\tilde{G} \to G$ be its simply connected covering. Then the boundary map*

$$\delta \colon H^1(k, G) \to H^2(k, Z(\tilde{G}))$$

is bijective.

PROOF. The injectivity follows from Theorem 25.61. In characteristic zero, the theorem is proved in Kneser 1969, Theorem 2, p. 60, and in nonzero characteristic, it is proved in Thăńg 2008 (in this case, $H^2(k, Z(\tilde{G}))$ is the flat group). □

Global fields

A global field is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(T)$. We let V denote the set of primes (possibly infinite) of a global field k, and k_v the completion of k at a $v \in V$.

THEOREM 25.63. *Let G be a semisimple group over a global field k and let $\tilde{G} \to G$ be its simply connected covering. Then the boundary map*

$$H^1(k, G) \xrightarrow{\ \delta\ } H^2(k, Z(\tilde{G}))$$

is surjective.

PROOF. See Harder 1975 for the number field case and Thăńg 2008 for the function field case. □

Theorem 25.63 reduces the study of the cohomology of semisimple groups over global fields to that of simply connected groups and finite group schemes.

THEOREM 25.64. *Let G be an algebraic group over a global field k. The canonical map*

$$H^1(k, G) \to \prod_v H^1(k_v, G) \tag{169}$$

is injective in each of the following cases:

(a) *G is semisimple and simply connected;*

(b) *G is semisimple with trivial centre and k is a number field;*

(c) *$G = \mathrm{O}(\phi)$ for some nondegenerate quadratic space (V, ϕ) and k is a number field.*

PROOF. In the number field case, (a) was proved in Harder 1966 except for the case E_8, which was proved in Chernousov 1989. The remaining statements can be deduced from (a) by using Theorem 25.63 and a knowledge of the cohomology of finite group schemes. See Platonov and Rapinchuk 1994, Chapter 6. The function field case of (a) is proved in Harder 1975. □

Note that (c) of the theorem implies that two quadratic spaces over a number field k are isomorphic if and only if they become isomorphic over k_v for all primes v (including the infinite primes). This is a very important result in number theory.

A group G for which the map (169) is injective is said to satisfy the ***Hasse principle for*** H^1.

THEOREM 25.65. *Let G be a simply connected semisimple group over a global field k. Then*
$$H^1(k, G) \simeq \prod_{v \text{ real}} H^1(k_v, G).$$

PROOF. Theorems 25.61 and 25.64 show that the map is injective. For the surjectivity, see Platonov and Rapinchuk 1994, Theorem 6.6, p. 286. □

Theorem 25.65 reduces the study of the cohomology of simply connected semisimple groups over global fields to that of the same groups over $\mathbb{R}$.

THEOREM 25.66. *Let G be a semisimple algebraic group over a global field k. For every nonarchimedean prime v_0 of k, the canonical map*
$$H^1(k, G) \to \prod_{v \neq v_0} H^1(k_v, G)$$
is surjective.

PROOF. In the number field case, this can be proved by the same argument as Theorem 1.7 of Borel and Harder 1978. For the function field case, see Thǎng 2012. □

COROLLARY 25.67. *In the situation of the theorem, suppose given for each $v \neq v_0$ an inner form $G^{(v)}$ of G_{k_v} over k_v; then there exists an inner form G' of G over k such that $G'_{k_v} \approx G^{(v)}$ for all $v \neq v_0$.*

PROOF. When inner forms are interpreted as pairs (G', f) (see 3.52), this is an immediate consequence of the theorem. Otherwise, we refer the reader to Prasad and Rapinchuk 2006 and Thǎng 2012 (where more complete results are proved). □

THEOREM 25.68. *Let G be a geometrically almost-simple group over a number field, and let S be a finite set of primes for k. If G is simply connected or has trivial centre, then the canonical map*
$$H^1(k, \underline{\text{Aut}}(G)) \to \prod_{v \in S} H^1(k_v, \underline{\text{Aut}}(G_{k_v}))$$
is surjective.

PROOF. See Borel and Harder 1978, Theorem B. □

COROLLARY 25.69. *In the situation of the theorem, suppose given a k_v-form $G^{(v)}$ of G_{k_v} for each $v \in S$; then there exists a k-form of G' of G such that $G'_{k_v} \approx G^{(v)}$ for all $v \in S$.*

PROOF. Immediate consequence of the theorem and Theorem 3.43.   □

THEOREM 25.70 (REAL APPROXIMATION). *For every connected group variety G over $\mathbb{Q}$, the group $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$.*

PROOF. For a torus of the form $(\mathbb{G}_m)_{k/\mathbb{Q}}$ (hence for all induced tori) the statement follows from the weak approximation theorem in algebraic number theory. Every torus T fits into an exact sequence

$$1 \to T'' \to T' \to T \to 1$$

with T' induced (see 12.63). An easy application of the Nakayama–Tate theorem (Serre 1962, IX) shows that $H^1(\mathbb{R}, T'') = 0$ and so the map $T'(\mathbb{R}) \to T(\mathbb{R})$ is surjective. Therefore the statement for T follows from the statement for T'.

Let S be a group of multiplicative type over $\mathbb{Q}$. Then $X^*(S)$ is a quotient of a direct sum of modules of the form $\mathbb{Z}[\Gamma/\Delta]$ (as in 12.63), and correspondingly there is an exact sequence

$$0 \to S \to T' \to T'' \to 0$$

with T' an induced torus and T'' a torus. From the diagram

$$
\begin{array}{ccccccc}
T'(\mathbb{Q}) & \longrightarrow & T''(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, S) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \text{dense image}} & & \downarrow & & \\
T'(\mathbb{R}) & \xrightarrow{\text{onto } T''(\mathbb{R})^+} & T''(\mathbb{R}) & \longrightarrow & H^1(\mathbb{R}, S) & \longrightarrow & 0
\end{array}
$$

we see that $H^1(\mathbb{Q}, S) \to H^1(\mathbb{R}, S)$ is surjective.

Let G be a reductive group. There exists an exact sequence

$$1 \to N \to G' \times T \to G \to 1$$

with G' simply connected, T a torus, and N a group of multiplicative type. The real approximation theorem holds for G' because it is unirational (17.93) and $G'(\mathbb{R})$ is connected (25.54). From the diagram

$$
\begin{array}{ccccccc}
G'(\mathbb{Q}) \times T(\mathbb{Q}) & \longrightarrow & G(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, N) & \longrightarrow & H^1(\mathbb{Q}, G') \\
\downarrow{\scriptstyle \text{dense image}} & & \downarrow & & \downarrow{\scriptstyle \text{onto}} & & \downarrow{\scriptstyle 25.64} \\
G'(\mathbb{R}) \times T(\mathbb{R}) & \xrightarrow{\text{onto } G(\mathbb{R})^+} & G(\mathbb{R}) & \longrightarrow & H^1(\mathbb{R}, N) & \longrightarrow & H^1(\mathbb{R}, G')
\end{array}
$$

we see that the real approximation theorem holds for G.

Finally, let G be connected group variety over $\mathbb{Q}$. Because we are in characteristic zero, G is the semidirect product of a unipotent group and a reductive group (Section f) and the underlying scheme of a unipotent group is isomorphic to $\mathbb{A}^n$ (see 14.66).   □

THEOREM 25.71. *Let G be a reductive group over $\mathbb{Q}$. If the derived group G' of G is simply connected and the torus G/G' satisfies the Hasse principle for H^1, then G satisfies the Hasse principle for H^1.*

PROOF. Let $T = G/G'$. The theorem follows from a diagram chase in

$$
\begin{array}{ccccccc}
T(\mathbb{Q}) & \to & H^1(\mathbb{Q}, G') & \longrightarrow & H^1(\mathbb{Q}, G) & \longrightarrow & H^1(T) \\
\downarrow {\scriptstyle \text{dense image}} & & \downarrow & & \downarrow & & \downarrow \\
G(\mathbb{R}) \to T(\mathbb{R}) & \to & H^1(\mathbb{R}, G') & \to & \prod_v H^1(\mathbb{Q}_v, G) & \to & \prod_v H^1(\mathbb{Q}_v, T)
\end{array}
$$

and its twists (in the sense of Serre 1997, I, 5.4 and 5.5). $\qquad\square$

Theorems 25.70 and 25.71 can be extended to groups over number fields by using Shapiro's lemma (3.44).

NOTES. For more on the cohomology of algebraic groups, see Kneser 1969 and Platonov and Rapinchuk 1994.

Exercises

EXERCISE 25-1. Let G be a reductive group over k. Let S be a maximal split torus in G and T a maximal torus containing S. Show that the following conditions on a nonzero $\alpha \in X(S)$ are equivalent:

  (a) α is a relative root (i.e., there exists a nonzero $X \in \mathfrak{g}$ such that $\mathrm{Ad}(s)(X) = \alpha(s)X$ for all $s \in S$);

  (b) there exists a nonzero $X \in \mathfrak{g} \otimes k^{\mathrm{s}}$ such that $\mathrm{Ad}(s)(X) = \alpha(s)X$ for all $s \in S$;

  (c) there exists a nonzero $X \in \mathfrak{g} \otimes k^{\mathrm{s}}$ and a character $\chi \in X(T)$ such that $\chi|S = \alpha$ and $\mathrm{Ad}(t)(X) = \chi(t)X$ for all $t \in T$.

EXERCISE 25-2. Show that a linearly reductive algebraic group has only finitely many simple representations (up to isomorphism) if and only if it is finite. Deduce that an algebraic group (not necessarily affine) has only finitely many simple representations if and only if its identity component is an extension of a unipotent algebraic group by an anti-affine algebraic group.

EXERCISE 25-3. Let k be a field of characteristic p. Show that $H^1(k, \alpha_p) \simeq k/k^p$ (hence is 0 if k is perfect).

EXERCISE 25-4. Let G be a semisimple algebraic group over k. If G is quasi-split and either simply connected or adjoint, then every maximal torus of G contained in a Borel subgroup of G is induced (https://mathoverflow.net/, question 241535).

Review of Algebraic Geometry

This is a list of the definitions and results from algebraic geometry used in the book. For commutative algebra, we refer the reader to the notes Milne 2017 (cited as CA). In this appendix, everything takes place over a fixed field k, and "k-algebra" means "finitely generated k-algebra".

As we work mostly with schemes algebraic over a field, it is convenient to ignore nonclosed points. We formalize this by working with max specs rather than specs. Those already familiar with the language of schemes can skip to A.22, where we provide a dictionary.

a. Affine algebraic schemes

Let A be a k-algebra.

A.1. Let X be the set of maximal ideals in A, and, for an ideal $\mathfrak{a}$ in A, let

$$Z(\mathfrak{a}) = \{\mathfrak{m} \mid \mathfrak{m} \supset \mathfrak{a}\}.$$

Then

◇ $Z(0) = X$, $Z(A) = \emptyset$,

◇ $Z(\mathfrak{a}\mathfrak{b}) = Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$ for every pair of ideals $\mathfrak{a}, \mathfrak{b}$, and

◇ $Z(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} Z(\mathfrak{a}_i)$ for every family of ideals $(\mathfrak{a}_i)_{i \in I}$.

For example, if $\mathfrak{m} \notin Z(\mathfrak{a}) \cup Z(\mathfrak{b})$, then there exist $f \in \mathfrak{a} \smallsetminus \mathfrak{m}$ and $g \in \mathfrak{b} \smallsetminus \mathfrak{m}$; but then $fg \notin \mathfrak{a}\mathfrak{b} \smallsetminus \mathfrak{m}$, and so $\mathfrak{m} \notin Z(\mathfrak{a}\mathfrak{b})$. These statements show that the sets $Z(\mathfrak{a})$ are the closed sets for a topology on X, called the ***Zariski topology***. We write $\operatorname{spm}(A)$ for X endowed with this topology. For example, $\mathbb{A}^n \stackrel{\text{def}}{=} \operatorname{spm}(k[T_1, \dots, T_n])$ is ***affine n-space*** over k. If k is algebraically closed, then the maximal ideals in A are exactly the ideals $(T_1 - a_1, \dots, T_n - a_n)$, and $\mathbb{A}^n$ can be identified with k^n endowed with its usual Zariski topology.

A.2. For a subset S of $\mathrm{spm}(A)$, let $I(S) = \bigcap\{\mathfrak{m} \mid \mathfrak{m} \in S\}$. The Nullstellensatz says that, for an ideal $\mathfrak{a}$ in A,

$$I(Z(\mathfrak{a})) \stackrel{\text{def}}{=} \bigcap\{\mathfrak{m} \mid \mathfrak{m} \supset \mathfrak{a}\}$$

is the radical of $\mathfrak{a}$ (CA 13.11). Using this, one sees that Z and I define inverse bijections between the radical ideals of A and the closed subsets of X. Under this bijection, prime ideals correspond to irreducible sets (nonempty sets not the union of two proper closed subsets), and maximal ideals correspond to points.

A.3. For $f \in A$, let $D(f) = \{\mathfrak{m} \mid f \notin \mathfrak{m}\}$. It is open in $\mathrm{spm}(A)$ because its complement is the closed set $Z((f))$. The sets of this form are called the **basic open subsets** of $\mathrm{spm}(A)$. Let $Z = Z(\mathfrak{a})$ be a closed subset of $\mathrm{spm}(A)$. According to the Hilbert basis theorem (CA 3.7), A is noetherian, and so $\mathfrak{a} = (f_1, \ldots, f_m)$ for some $f_i \in A$, and

$$X \smallsetminus Z = D(f_1) \cup \cdots \cup D(f_m).$$

This shows that every open subset of $\mathrm{spm}(A)$ is a finite union of basic open subsets. In particular, the basic open subsets form a base for the Zariski topology on $\mathrm{spm}(A)$.

A.4. Let $\alpha\colon A \to B$ be a homomorphism of k-algebras, and let $\mathfrak{m}$ be a maximal ideal in B. As B is finitely generated as a k-algebra, so also is $B/\mathfrak{m}$, which implies that it is a finite field extension of k (Zariski's lemma; CA 13.1). Therefore the image of A in $B/\mathfrak{m}B$ is an integral domain of finite dimension over k, and hence is a field. This image is isomorphic to $A/\alpha^{-1}(\mathfrak{m})$, and so the ideal $\alpha^{-1}(\mathfrak{m})$ is maximal in A. Hence α defines a map

$$\alpha^*\colon \mathrm{spm}(B) \to \mathrm{spm}(A), \quad \mathfrak{m} \mapsto \alpha^{-1}(\mathfrak{m}),$$

which is continuous because $(\alpha^*)^{-1}(D(f)) = D(\alpha(f))$. In this way, spm becomes a functor from k-algebras to topological spaces.

A.5. For a multiplicative subset S of A, we let $S^{-1}A$ denote the ring of fractions having the elements of S as denominators. For example, if $f \in A$, then we let $S_f = \{1, f, f^2, \ldots\}$ and

$$A_f = S_f^{-1}A \simeq A[T]/(1 - fT).$$

Let D be a basic open subset of X. We define S_D to be the multiplicative subset of A,

$$S_D = A \smallsetminus \bigcup\{\mathfrak{m} \mid \mathfrak{m} \in D\}.$$

If $D = D(f)$, then the map $S_f^{-1}A \to S_D^{-1}A$ defined by the inclusion $S_f \subset S_D$ is an isomorphism. If D' and D are both basic open subsets of X and $D' \subset D$, then $S_{D'} \supset S_D$, and so there is a canonical map

$$S_D^{-1}A \to S_{D'}^{-1}A. \tag{170}$$

A.6. There is a unique sheaf $\mathcal{O}_X$ of k-algebras on $X = \text{Spm}(A)$ such that $\mathcal{O}_X(D) = S_D^{-1}A$ for every basic open subset D of X, and the restriction map $\mathcal{O}_X(D) \to \mathcal{O}_X(D')$ is the map (170) for every pair $D' \subset D$ of basic open subsets. Note that, for every $f \in A$,

$$A_f \stackrel{\text{def}}{=} S_f^{-1}A \simeq S_{D(f)}^{-1}(A) \stackrel{\text{def}}{=} \mathcal{O}_X(D(f)).$$

We write $\text{Spm}(A)$ for $\text{spm}(A)$ endowed with this sheaf of k-algebras.

A.7. By a k-**ringed space** we mean a topological space equipped with a sheaf of k-algebras. An **affine algebraic scheme** over k is a k-ringed space isomorphic to $\text{Spm}(A)$ for some k-algebra A. A **morphism** (or **regular map**) of affine algebraic schemes over k is a morphism of k-ringed spaces (it is automatically a morphism of *locally* ringed spaces).

A.8. The functor $A \rightsquigarrow \text{Spm}(A)$ is a contravariant equivalence from the category of k-algebras to the category of affine algebraic schemes over k, with quasi-inverse $(X, \mathcal{O}_X) \rightsquigarrow \mathcal{O}_X(X)$. In particular, for all k-algebras A and B,

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

A.9. Let M be an A-module. There is a unique sheaf $\mathcal{M}$ of $\mathcal{O}_X$-modules on $X = \text{Spm}(A)$ such that $\mathcal{M}(D) = S_D^{-1}M$ for every basic open subset D of X, and the restriction map $\mathcal{M}(D) \to \mathcal{M}(D')$ is the canonical map $S_D^{-1}M \to S_{D'}^{-1}M$ for every pair $D' \subset D$ of basic open subsets. A sheaf of $\mathcal{O}_X$-modules on X is said to be **coherent** if it is isomorphic to $\mathcal{M}$ for some finitely generated A-module M. The functor $M \rightsquigarrow \mathcal{M}$ is an equivalence from the category of finitely generated A-modules to the category of coherent $\mathcal{O}_X$-modules with quasi-inverse $\mathcal{M} \rightsquigarrow \mathcal{M}(X)$. In this equivalence, finitely generated projective A-modules correspond to locally free $\mathcal{O}_X$-modules of finite rank (CA 12.6).

A.10. For fields $K \supset k$, the Zariski topology on K^n induces that on k^n. In order to prove this, we have to show (a) that every closed subset S of k^n is of the form $T \cap k^n$ for some closed subset T of K^n, and (b) that $T \cap k^n$ is closed for every closed subset of K^n.

(a) Let $S = Z(f_1, \ldots, f_m)$ with the $f_i \in k[X_1, \ldots, X_n]$. Then

$$S = k^n \cap \{\text{zero set of } f_1, \ldots, f_m \text{ in } K^n\}.$$

(b) Let $T = Z(f_1, \ldots, f_m)$ with the $f_i \in K[X_1, \ldots, X_n]$. Choose a basis $(e_j)_{j \in J}$ for K as a k-vector space, and write $f_i = \sum e_j f_{ij}$ (finite sum) with $f_{ij} \in k[X_1, \ldots, X_n]$. Then

$$Z(f_i) \cap k^n = \{\text{zero set of the family } (f_{ij})_{j \in J} \text{ in } k^n\}$$

for each i, and so $T \cap k^n$ is the zero set in k^n of the family (f_{ij}).

b.   Algebraic schemes

A.11. Let $(X, \mathcal{O}_X)$ be a k-ringed space. An open subset U of X is said to be ***affine*** if $(U, \mathcal{O}_X | U)$ is an affine algebraic scheme over k, i.e., isomorphic to $\mathrm{Spm}(A)$ for some (finitely generated) k-algebra A. An ***algebraic scheme over*** k is a k-ringed space $(X, \mathcal{O}_X)$ that admits a finite covering by open affine subsets. A ***morphism of algebraic schemes*** (also called a ***regular map***) over k is a morphism of k-ringed spaces. We often let X denote the algebraic scheme $(X, \mathcal{O}_X)$ and $|X|$ the underlying topological space of X. When the base field k is understood, we write "algebraic scheme" for "algebraic scheme over k".

The local ring at a point x of X is denoted by $\mathcal{O}_{X,x}$ or just $\mathcal{O}_x$, and the residue field at x is denoted by $\kappa(x)$. For example, if $X = \mathrm{Spm}(A)$ and $x = \mathfrak{m}$, then $\mathcal{O}_{X,x} = A_{\mathfrak{m}}$ and $\kappa(x) = A/\mathfrak{m}$. A regular map $\varphi \colon Y \to X$ induces a local homomorphism of local rings $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ for every $y \in Y$.

A.12. A morphism $\varphi \colon Y \to X$ of algebraic schemes over k is said to be ***surjective*** (resp. ***injective, open, closed***) if the map of topological spaces $|\varphi| \colon |Y| \to |X|$ is surjective (resp. injective, open, closed). A morphism φ is surjective if and only if $\varphi(k^{\mathrm{a}}) \colon Y(k^{\mathrm{a}}) \to X(k^{\mathrm{a}})$ is surjective.

A.13. Let X be an algebraic scheme over k, and let A be a k-algebra. By definition, a morphism of k-schemes $X \to \mathrm{Spm}(A)$ gives a homomorphism $A \to \mathcal{O}_X(X)$ of k-algebras (but $\mathcal{O}_X(X)$ need not be finitely generated!). In this way, we get a natural isomorphism

$$\mathrm{Hom}(X, \mathrm{Spm}\, A) \simeq \mathrm{Hom}(A, \mathcal{O}_X(X)).$$

A.14. Let X be an algebraic scheme over k. Then $|X|$ is a noetherian topological space (i.e., the open subsets of $|X|$ satisfy the ascending chain condition; equivalently, the closed subsets of $|X|$ satisfy the descending chain condition). It follows that $|X|$ can be written as a finite union of closed irreducible subsets, $|X| = W_1 \cup \cdots \cup W_r$. When we discard any W_i contained in another, the collection $\{W_1, \ldots, W_r\}$ is uniquely determined, and its elements are called the ***irreducible components*** of X.

A noetherian topological space has only finitely many connected components, each of which is open and closed, and it is a disjoint union of them.

A.15. The image of a regular map $\varphi \colon Y \to X$ of algebraic schemes is constructible; therefore it contains a dense open subset of its closure. If φ is dominant, then its image is dense in $|X|$ and so contains a dense open subset of X.

A.16. A regular map $\varphi \colon Y \to X$ of algebraic schemes is said to be ***affine*** if, for all open affine subschemes U in X, $\varphi^{-1}(U)$ is an open affine subscheme in X. It suffices to check this condition for the sets in an open affine covering of X.

A.17. A regular map $\varphi \colon Y \to X$ of algebraic schemes over k is ***finite*** if, for every open affine subscheme $U \subset X$, $\varphi^{-1}(U)$ is affine and $\mathcal{O}_Y(\varphi^{-1}(U))$ is a

finite $\mathcal{O}_X(U)$-algebra. It suffices to check this condition for the sets in an open affine covering of X. For example, the map $\mathrm{Spm}(B) \to \mathrm{Spm}(A)$ defined by a homomorphism of k-algebras $A \to B$ is finite if and only if $A \to B$ is finite.

A.18. (Extension of the base field; extension of scalars). Let K be a field containing k. There is a functor $X \rightsquigarrow X_K$ from algebraic schemes over k to algebraic schemes over K. For example, if $X = \mathrm{Spm}(A)$, then $X_K = \mathrm{Spm}(K \otimes A)$.

A.19. For an algebraic scheme X over k, we let $X(R)$ denote the set of points of X with coordinates in a k-algebra R,

$$X(R) \overset{\text{def}}{=} \mathrm{Hom}(\mathrm{Spm}(R), X).$$

For example, if $X = \mathrm{Spm}(A)$, then $X(R) = \mathrm{Hom}(A, R)$ (homomorphisms of k-algebras).

For a ring R containing k, we let $X(R) = \varinjlim X(R_i)$, where R_i runs over the (finitely generated) k-subalgebras of R. Again $X(R) = \mathrm{Hom}(A, R)$ if $X = \mathrm{Spm}(A)$. Now $R \rightsquigarrow X(R)$ is a functor from all k-algebras (not necessarily finitely generated) to sets.

A.20. Let A be a finitely generated k-algebra, and let $A_{k^{\mathrm{a}}} = k^{\mathrm{a}} \otimes_k A$. If $\mathfrak{m}$ is a maximal ideal in $A_{k^{\mathrm{a}}}$, then $\mathfrak{m} \cap A$ is maximal because $A/\mathfrak{m} \cap A \hookrightarrow A_{k^{\mathrm{a}}}/\mathfrak{m} = k^{\mathrm{a}}$. The map $\pi \colon \mathrm{spm}(A_{k^{\mathrm{a}}}) \to \mathrm{spm}(A)$ sending $\mathfrak{m}$ to $\mathfrak{m} \cap A$ is surjective,[1] continuous,[2] and closed,[3] and hence it is a quotient map.

More generally, let X be an algebraic scheme over k; then the projection map $X_{k^{\mathrm{a}}} \to X$ realizes the topological space $|X|$ as a quotient of $|X_{k^{\mathrm{a}}}|$.[4]

A.21. Let X be an algebraic scheme. An $\mathcal{O}_X$-module $\mathcal{M}$ is said to be **coherent** if, for every open affine subset U of X, the restriction of $\mathcal{M}$ to U is coherent (A.9). It suffices to check this condition for the sets in an open affine covering of X. Similarly, a sheaf $\mathcal{I}$ of ideals in $\mathcal{O}_X$ is **coherent** if its restriction to every open affine subset U is the subsheaf of $\mathcal{O}_X|U$ defined by an ideal in the ring $\mathcal{O}_X(U)$.

A.22. For those familiar with schemes in the sense of specs, we provide a short dictionary. Let X be an algebraic scheme over a field in the sense of EGA, and let X_0 be the set of closed points in X with the induced topology.

---

[1] Every maximal ideal $\mathfrak{m}$ of A is the kernel of a k-algebra homomorphism $A \to k^{\mathrm{a}}$ (CA 13.2), which extends to a k^{a}-algebra homomorphism $A_{k^{\mathrm{a}}} \to k^{\mathrm{a}}$, whose kernel is a maximal ideal lying over $\mathfrak{m}$.

[2] Let $S = Z(f_1, \ldots, f_s)$ be closed in $\mathrm{spm}(A)$. Then $\pi^{-1}(S) = Z(f_1, \ldots, f_s)$ in $\mathrm{spm}(A_{k^{\mathrm{a}}})$.

[3] Let $T = Z(f_1, \ldots, f_s)$ be a closed subset of $\mathrm{spm}(A_{k^{\mathrm{a}}})$. Choose a basis $(e_j)_{j \in J}$ for k^{a} as a k-vector space, and write $f_i = \sum_j e_j f_{ij}$ (finite sum) with $f_{ij} \in A$. Every maximal ideal of $A_{k^{\mathrm{a}}}$ is the kernel of a k-algebra homomorphism $A_{k^{\mathrm{a}}} \to k^{\mathrm{a}}$, and the f_i map to zero under such a homomorphism if and only if every f_{ij} does. Therefore $T = Z(\ldots, f_{ij}, \ldots)$ in $\mathrm{spm}(A_{k^{\mathrm{a}}})$, and it follows that $\pi(T) = Z(\ldots, f_{ij}, \ldots)$ in $\mathrm{spm}(A)$.

[4] The cognoscenti prefer to derive this statement from Corollary 2.3.12 of EGA IV 2.3.10, whose proof depends on EGA I 9.5.3 and EGA IV 1.9.5, 2.3.3, 2.3.7, which in turn depend on …

The map $S \mapsto S \cap X_0$ is an isomorphism from the lattice of closed (resp. open, constructible) subsets of X to the lattice of closed (resp. open, constructible) subsets of X_0. In particular, X is connected if and only if X_0 is connected. To recover X from X_0, add a point z for each irreducible closed subset Z of X_0 not already a point; the point z lies in an open subset U if and only if $U \cap Z$ is nonempty. The ringed spaces $(X, \mathcal{O}_X)$ and $(X_0, \mathcal{O}_X | X_0)$ have the same lattice of open subsets and the same ring for each open subset; they differ only in the underlying sets. See EGA IV, §10.

A regular map $\varphi \colon Y \to X$ of algebraic schemes over k is surjective if and only if it is surjective on closed points (DG, I, §3, 6.10).

c. Subschemes

A.23. Let X be an algebraic scheme over k. An **open subscheme** of X is a pair $(U, \mathcal{O}_X | U)$ with U open in X. It is again an algebraic scheme over k.

A.24. Let $X = \mathrm{Spm}(A)$ be an affine algebraic scheme over k, and let $\mathfrak{a}$ be an ideal in A. Then $\mathrm{Spm}(A/\mathfrak{a})$ is an affine algebraic scheme with underlying topological space $Z(\mathfrak{a})$.

Let X be an algebraic scheme over k, and let $\mathcal{I}$ be a coherent sheaf of ideals in $\mathcal{O}_X$. The support of the sheaf $\mathcal{O}_X / \mathcal{I}$ is a closed subset Z of X, and $(Z, \mathcal{O}_X / \mathcal{I})$ is an algebraic scheme, called the **closed subscheme** of X defined by the sheaf of ideals $\mathcal{I}$. Note that $Z \cap U$ is affine for every open affine subscheme U of X.

The closed subschemes of an algebraic scheme satisfy the descending chain condition. To see this, consider a chain of closed subschemes

$$Z \supset Z_1 \supset Z_2 \supset \cdots$$

of an algebraic scheme X. Because $|X|$ is noetherian (A.14), the chain $|Z| \supset |Z_1| \supset |Z_2| \supset \cdots$ becomes constant, and so we may suppose that $|Z| = |Z_1| = \cdots$. Write Z as a finite union of open affine subsets, $Z = \bigcup U_i$. For each i, the chain $Z \cap U_i \supset Z_1 \cap U_i \supset \cdots$ of closed subschemes of U_i corresponds to an ascending chain of ideals in the noetherian ring $\mathcal{O}_Z(U_i)$, and therefore becomes constant.

A.25. A **subscheme** of an algebraic scheme X is a closed subscheme of an open subscheme of X. Its underlying set is locally closed in X (i.e., open in its closure; equivalently, it is the intersection of an open subset with a closed subset).

A.26. A regular map $\varphi \colon Y \to X$ is an **immersion** if it induces an isomorphism from Y onto a subscheme Z of X. If Z is open (resp. closed), then φ is called an **open** (resp. **closed**) **immersion**. Every immersion can be written as a closed immersion into an open subscheme and also as an open immersion into a closed subscheme.

A.27. Recall that a ring A is **reduced** if it has no nonzero nilpotent elements. If A is reduced, then $S^{-1}A$ is reduced for every multiplicative subset S of A; conversely, if $A_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$ in A, then A is reduced.

An algebraic scheme X is **reduced** if $\mathcal{O}_{X,P}$ is reduced for all $P \in X$. For example, $\mathrm{Spm}(A)$ is reduced if and only if A is reduced. If X is reduced, then $\mathcal{O}_X(U)$ is reduced for all open affine subsets U of X.

A.28. A k-algebra A is reduced if and only if the intersection of the maximal ideals in A is zero (A.2). Let X be an algebraic scheme over k. For a section f of $\mathcal{O}_X$ over some open subset U of X and $u \in U$, let $f(u)$ denote the image of f in $\kappa(u) = \mathcal{O}_{X,u}/\mathfrak{m}_u$ (a finite extension of k). If X is reduced, then two sections $f_1, f_2 \in \mathcal{O}_X(U)$ are equal if and only if $f_1(u) = f_2(u)$ for all $u \in |U|$. When k is algebraically closed, $\kappa(x) = k$ for all $x \in |X|$, and so this observation allows us to identify $\mathcal{O}_X$ with a sheaf of k-valued functions on X.

A.29. An algebraic scheme X is said to be **integral** if it is reduced and irreducible. For example, $\mathrm{Spm}(A)$ is integral if and only if A is an integral domain. If X is integral, then $\mathcal{O}_X(U)$ is an integral domain for all open affine subsets U of X.

A.30. Let X be an algebraic scheme over k. There is a unique reduced algebraic subscheme X_{red} of X with the same underlying topological space as X. For example, if $X = \mathrm{Spm}(A)$, then $X_{\mathrm{red}} = \mathrm{Spm}(A/\mathfrak{N})$, where $\mathfrak{N}$ is the nilradical of A.

Every regular map $Y \to X$ from a reduced scheme Y to X factors uniquely through the inclusion map $i\colon X_{\mathrm{red}} \to X$. In particular, $X_{\mathrm{red}}(R) \simeq X(R)$ if R is a reduced k-algebra.

More generally, every locally closed subset Y of $|X|$ carries a unique structure of a reduced subscheme of X; we write Y_{red} for Y equipped with this structure.

Passage to the associated reduced scheme does *not* commute with extension of the base field. For example, an algebraic scheme X over k may be reduced without $X_{k^{\mathrm{a}}}$ being reduced.

d. Algebraic schemes as functors

A.31. Recall that Alg_k is the category of *finitely generated* k-algebras. For a k-algebra A, let h^A denote the functor $R \rightsquigarrow \mathrm{Hom}(A, R)$ from k-algebras to sets. A functor $F\colon \mathsf{Alg}_k \to \mathsf{Set}$ is **representable** if it is isomorphic to h^A for some k-algebra A. A pair (A, a), $a \in F(A)$, is said to **represent** F if the natural transformation

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

is an isomorphism. This means that, for each $x \in F(R)$, there is a unique homomorphism $A \to R$ such that $F(A) \to F(R)$ sends a to x. The element a is said to be **universal**. For example, (A, id_A) represents h^A. If (A, a) and (A', a') both represent F, then there is a unique isomorphism $A \to A'$ sending a to a'.

A.32. Let B be a k-algebra and let F be a functor $\mathsf{Alg}_k \to \mathsf{Set}$. An element $x \in F(B)$ defines a homomorphism

$$\mathrm{Hom}(B, R) \to F(R)$$

sending an f to the image of x under $F(f)$. This homomorphism is natural in R, and so we have a map of sets

$$F(B) \to \mathsf{Nat}(h^B, F).$$

The Yoneda lemma says that this is a bijection, natural in both B and F. For $F = h^A$, this says that

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

In other words, the contravariant functor $A \rightsquigarrow h^A$ is fully faithful. Its essential image consists of the representable functors.

A.33. Let h_X denote the functor $\mathrm{Hom}(-, X)$ from algebraic schemes over k to sets. The Yoneda lemma in this situation says that, for algebraic schemes X, Y,

$$\mathrm{Hom}(X, Y) \simeq \mathsf{Nat}(h_X, h_Y).$$

Let h_X^{aff} denote the functor $R \rightsquigarrow X(R) \colon \mathsf{Alg}_k \to \mathsf{Set}$. Then $h_X^{\mathrm{aff}} = h_X \circ \mathrm{Spm}$, and can be regarded as the restriction of h_X to affine algebraic schemes.

Let X and Y be algebraic schemes over k. Every natural transformation $h_X^{\mathrm{aff}} \to h_Y^{\mathrm{aff}}$ extends uniquely to a natural transformation $h_X \to h_Y$,

$$\mathsf{Nat}(h_X^{\mathrm{aff}}, h_Y^{\mathrm{aff}}) \simeq \mathsf{Nat}(h_X, h_Y),$$

and so

$$\mathrm{Hom}(X, Y) \simeq \mathsf{Nat}(h_X^{\mathrm{aff}}, h_Y^{\mathrm{aff}}).$$

In other words, the functor $X \rightsquigarrow h_X^{\mathrm{aff}}$ is fully faithful. We shall also refer to this statement as the *Yoneda lemma*. It allows us to identify an algebraic scheme over k with its "points-functor" $\mathsf{Alg}_k \to \mathsf{Set}$.

Recall (p. 4) that Alg_k^0 denotes the category of "small" k-algebras. We let $\tilde{X}$ denote the functor $\mathsf{Alg}_k^0 \to \mathsf{Set}$ defined by an algebraic scheme. Then $X \rightsquigarrow \tilde{X}$ is fully faithful. We shall also refer to this statement as the *Yoneda lemma*.

Let F be a functor $\mathsf{Alg}_k^0 \to \mathsf{Set}$. If F is representable by an algebraic scheme X, then X is uniquely determined up to a unique isomorphism, and h_X extends F to a functor $\mathsf{Alg}_k \to \mathsf{Set}$.

A.34. By a functor in this paragraph and the next we mean a functor $\mathsf{Alg}_k^0 \to \mathsf{Set}$. A subfunctor U of a functor X is **open** if, for all maps $\varphi \colon h^A \to X$, the subfunctor $\varphi^{-1}(U)$ of h^A is defined by an open subscheme of $\mathrm{Spm}(A)$. A family $(U_i)_{i \in I}$ of open subfunctors of X is an **open covering** of X if each U_i is open in X and $X = \bigcup U_i(K)$ for every field K. A functor X is **local** if, for all k-algebras R and

all finite families $(f_i)_i$ of elements of A generating the ideal A, the sequence of sets

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

is exact. Let $\mathbb{A}^1$ denote the functor sending a k-algebra R to its underlying set. For a functor U, let $\mathcal{O}(U) = \mathrm{Nat}(U, \mathbb{A}^1)$ – it is a k-algebra, not necessarily finitely generated.[5] A functor U is said to be **affine** if $\mathcal{O}(U)$ is finitely generated and the canonical map $U \to h^{\mathcal{O}(U)}$ is an isomorphism. A local functor admitting a finite covering by open affine functors is represented by an algebraic scheme.[6]

A.35. A morphism $\varphi: X \to Y$ of functors is a **monomorphism** if $\varphi(R)$ is injective for all R. A morphism φ is an **open immersion** if it is open and a monomorphism (DG, I, §1, 3.6). Let $\varphi: X \to Y$ be a regular map of algebraic schemes. If $\tilde{X} \to \tilde{Y}$ is a monomorphism, then it is injective (DG, I, §1, 5.3). If X is irreducible and $\tilde{X} \to \tilde{Y}$ is a monomorphism, then there exists a dense open subset U of X such that $\varphi|U$ is an immersion (DG, I, §3, 4.5, 4.6).

A.36. Let R be a k-algebra (finitely generated as always). An R-algebra is small if it is small as a k-algebra. An **algebraic R-scheme** is a pair (X, φ) consisting of an algebraic k-scheme X and a morphism $\varphi: X \to \mathrm{Spm}(R)$. For example, if $f: R \to R'$ is a finitely generated R-algebra, then $\mathrm{Spm}(f): \mathrm{Spm}(R') \to \mathrm{Spm}(R)$ is an algebraic R-scheme. The algebraic R-schemes form a category in an obvious way. Moreover, the Yoneda lemma still holds: for an algebraic R-scheme X, let $\tilde{X}$ denote the functor sending a small R-algebra R' to the set $\mathrm{Hom}_R(\mathrm{Spm}(R'), X)$; then $X \rightsquigarrow \tilde{X}$ is fully faithful.

e. Fibred products of algebraic schemes

A.37. Let $\varphi: X \to Z$ and $\psi: Y \to Z$ be regular maps of algebraic schemes over k. The functor

$$R \rightsquigarrow X(R) \times_{Z(R)} Y(R) \overset{\mathrm{def}}{=} \{(x, y) \in X(R) \times Y(R) \mid \varphi(x) = \psi(y)\}$$

is representable by an algebraic scheme $X \times_Z Y$ over k, and $X \times_Z Y$ is the fibred product of (φ, ψ) in the category of algebraic k-schemes, i.e., the diagram

$$
\begin{array}{ccc}
X \times_Z Y & \longrightarrow & Y \\
\downarrow & & \downarrow{\psi} \\
X & \overset{\varphi}{\longrightarrow} & Z
\end{array}
$$

is cartesian. For example, if $R \to A$ and $R \to B$ are homomorphisms of k-algebras, then $A \otimes_R B$ is a finitely generated k-algebra, and

$$\mathrm{Spm}(A) \times_{\mathrm{Spm}(R)} \mathrm{Spm}(B) = \mathrm{Spm}(A \otimes_R B).$$

[5]Here it is important that we consider functors on Alg_k^0, not Alg_k, in order to know that $\mathcal{O}(U)$ is a set.

[6]This is the *definition* of a scheme in DG, I, §1, 3.11.

When φ and ψ are the structure maps $X \to \mathrm{Spm}(k)$ and $Y \to \mathrm{Spm}(k)$, the fibred product becomes the product, denoted $X \times Y$, and

$$\mathrm{Hom}(T, X \times Y) \simeq \mathrm{Hom}(T, X) \times \mathrm{Hom}(T, Y).$$

The diagonal map $\Delta_X \colon X \to X \times X$ is the regular map whose composites with the projection maps equal id_X.

The **fibre** $\varphi^{-1}(x)$ over x of a regular map $\varphi \colon Y \to X$ of algebraic schemes is defined to be the fibred product of the maps $x \hookrightarrow X$ and φ:

$$\begin{array}{ccc}
Y & \longleftarrow & Y \times_X x \stackrel{\mathrm{def}}{=} \varphi^{-1}(x) \\
\downarrow{\scriptstyle\varphi} & & \downarrow \\
X & \longleftarrow & x = \mathrm{Spm}(\kappa(x)).
\end{array}$$

Thus, it is an algebraic scheme over the field $\kappa(x)$. It need not be reduced even if both X and Y are reduced (see A.44).

A.38. For a pair of regular maps $\varphi_1, \varphi_2 \colon X \rightrightarrows Y$, the functor

$$R \rightsquigarrow \{x \in X(R) \mid \varphi_1(x) = \varphi_2(x)\}$$

is represented by a subscheme of X, called the **equalizer** $\mathrm{Eq}(\varphi_1, \varphi_2)$ of φ_1 and φ_2. It is the fibred product of the maps $(\varphi_1, \varphi_2) \colon X \to Y \times Y$ and $\Delta_Y \colon Y \to Y \times Y$. Its underlying set is $\{x \in |X| \mid \varphi_1(x) = \varphi_2(x)\}$.

A.39. The intersection of two closed subschemes Z_1 and Z_2 of an algebraic scheme X is defined to be $Z_1 \times_X Z_2$ regarded as a closed subscheme of X with underlying set $|Z_1| \cap |Z_2|$. For example, if $X = \mathrm{Spm}(A)$, $Z_1 = \mathrm{Spm}(A/\mathfrak{a}_1)$, and $Z_1 = \mathrm{Spm}(A/\mathfrak{a}_2)$, then $Z_1 \cap Z_2 = \mathrm{Spm}(A/\mathfrak{a}_1 + \mathfrak{a}_2)$. This definition extends in an obvious way to finite, or even infinite, sets of closed subschemes. Because X has the descending chain condition on closed subschemes (A.24), every infinite intersection is equal to a finite intersection. An intersection of reduced subschemes of a reduced scheme need not be reduced.

A.40. A regular map $\varphi \colon Y \to X$ of algebraic schemes over k is **quasi-finite** if the fibre $\varphi^{-1}(x)$ is a finite scheme over $\kappa(x)$ for $x \in |X|$. For example, a finite map is quasi-finite. For $x \in X$, we let Y_x denote the fibre $\varphi^{-1}(x)$ and $\deg_x(\varphi)$ the dimension of $\mathcal{O}(Y_x)$ as a k-vector space. When X is integral, a finite map $\varphi \colon Y \to X$ is flat if and only if $\deg_x(\varphi)$ is independent of x (CA 12.6).

f. Algebraic varieties

A.41. An algebraic scheme X over k is said to be **separated** if the diagonal in $X \times X$ is closed (so Δ_X is a *closed* immersion). Then any two regular maps $\varphi_1, \varphi_2 \colon Y \rightrightarrows X$ agree on a closed subset of $|Y|$, and so $\mathrm{Eq}(\varphi_1, \varphi_2)$ is a *closed* subscheme of Y.

A.42. An **affine** k-algebra is a k-algebra A such that $k^{\mathrm{a}} \otimes A$ is reduced. If A is an affine k-algebra and B is a reduced ring containing k, then $A \otimes B$ is reduced; in particular $A \otimes K$ is reduced for every field K containing k. The tensor product of two affine k-algebras is affine. If k is perfect, then every reduced k-algebra is affine.

A.43. An algebraic scheme X is said to be **geometrically reduced** if $X_{k^{\mathrm{a}}}$ is reduced. For example, $\mathrm{Spm}(A)$ is geometrically reduced if and only if A is an affine k-algebra. If X is geometrically reduced, then X_K is reduced for every field K containing k. If X is geometrically reduced and Y is reduced (resp. geometrically reduced), then $X \times Y$ is reduced (resp. geometrically reduced). If k is perfect, then every reduced algebraic scheme over k is geometrically reduced. These statements all follow from the affine case (A.42).

A.44. An **algebraic variety over** k is an algebraic scheme over k that is both separated and geometrically reduced. Algebraic varieties remain algebraic varieties under extension of the base field, and products of algebraic varieties are again algebraic varieties, but a fibred product of algebraic varieties need not be an algebraic variety. Consider, for example,

$$
\begin{array}{ccc}
\mathbb{A}^1 & \longleftarrow & \mathbb{A}^1 \times_{\mathbb{A}^1} \{a\} = \mathrm{Spm}(k[T]/(T^p - a)) \\
{\scriptstyle x \mapsto x^p} \downarrow & & \downarrow \\
\mathbb{A}^1 & \longleftarrow & \{a\}.
\end{array}
$$

This is one reason for working with algebraic schemes rather than varieties.

Let X be an irreducible algebraic variety over k. The rings $\mathcal{O}_X(U)$ for U an affine open subset of X have a common field of fractions, which is denoted $k(X)$. Its elements are the **rational functions** on X.

Two irreducible varieties X and X' over k are said to be **birationally equivalent** if some dense open subset of X is isomorphic to a dense open subset of X'. The varieties X and X' are birationally equivalent if and only if $k(X) \approx k(X')$ as k-algebras.

g. The dimension of an algebraic scheme

A.45. Let A be a noetherian ring. The **height** of a prime ideal $\mathfrak{p}$ is the greatest length d of a chain of distinct prime ideals

$$
\mathfrak{p} = \mathfrak{p}_d \supset \cdots \supset \mathfrak{p}_1 \supset \mathfrak{p}_0.
$$

Let $\mathfrak{p}$ be minimal among the prime ideals containing an ideal $(a_1, \ldots, a_m)$; then $\mathrm{height}(\mathfrak{p}) \leq m$. Conversely, if $\mathrm{height}(\mathfrak{p}) = m$, then there exist $a_1, \ldots, a_m \in \mathfrak{p}$ such that $\mathfrak{p}$ is minimal among the prime ideals containing $(a_1, \ldots, a_m)$. See CA 21.5, 21.7.

The *(Krull) dimension* of A is $\sup\{\text{height}(\mathfrak{p})\}$, where $\mathfrak{p}$ runs over the prime ideals of A (or just the maximal ideals – the two obviously give the same answer). Clearly, the dimension of a local ring with maximal ideal $\mathfrak{m}$ is the height of $\mathfrak{m}$, and $\dim(A) = \sup(\dim(A_\mathfrak{m}))$. Since all prime ideals of A contain the nilradical $\mathfrak{N}$ of A, we have $\dim(A) = \dim(A/\mathfrak{N})$.

A.46. Let A be a finitely generated k-algebra, and assume that $A/\mathfrak{N}$ is an integral domain. According to the Noether normalization theorem, A contains a polynomial ring $k[t_1,\ldots,t_r]$ such that A is a finitely generated $k[t_1,\ldots,t_r]$-module. We call r the *transcendence degree* of A over k – it is equal to the transcendence degree of the field of fractions of $A/\mathfrak{N}$ over k. The length of every maximal chain of distinct prime ideals in A is $\operatorname{tr\,deg}_k(A)$. In particular, every maximal ideal in A has height $\operatorname{tr\,deg}_k(A)$, and so A has dimension $\operatorname{tr\,deg}_k(A)$. See CA, §18.

A.47. Let X be an irreducible algebraic scheme over k. The *dimension* of X is the greatest length d of a chain of irreducible closed subschemes

$$Z = Z_d \subset \cdots \subset Z_1 \subset Z_0.$$

It is equal to the Krull dimension of $\mathcal{O}_{X,x}$ for every $x \in |X|$, and to the Krull dimension of $\mathcal{O}_X(U)$ for every open affine subset U of X. We have $\dim(X) = \dim(X_{\text{red}})$, and if X is reduced, then $\dim(X)$ is equal to the transcendence degree of $k(X)$ over k. These statements follow from the affine case (A.45, A.46).

The dimension of a general algebraic scheme is defined to be the maximum dimension of an irreducible component. When the irreducible components all have the same dimensions, the scheme is said to be *equidimensional*.

A.48. Assume that X is irreducible and geometrically reduced. Then there exists a transcendence basis $t_1,\ldots,t_d$ for $k(X)$ over k such that $k(X)$ is separable over $k(t_1,\ldots,t_d)$. This means that X is birationally equivalent to a hypersurface

$$f(T_1,\ldots,T_{d+1}) = 0 \quad (d = \dim(X))$$

in $\mathbb{A}^{d+1}$ with the property that $\partial f/\partial T_{d+1} \neq 0$. It follows that the points x in X such that $\kappa(x)$ is separable over k form a dense subset of $|X|$. In particular, $X(k)$ is dense in $|X|$ when k is separably closed.

h. Tangent spaces; smooth points; regular points

A.49. Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. The dimension of A is the height of $\mathfrak{m}$, and so (A.45)

$$\dim A \leq \text{minimum number of generators for } \mathfrak{m}.$$

When equality holds, A is said to be *regular*. Nakayama's lemma (CA 3.9) shows that a set of elements of $\mathfrak{m}$ generates $\mathfrak{m}$ if and only if it spans the κ-vector space $\mathfrak{m}/\mathfrak{m}^2$, where $\kappa = A/\mathfrak{m}$. Therefore

$$\dim(A) \leq \dim_\kappa(\mathfrak{m}/\mathfrak{m}^2)$$

with equality if and only if A is regular. Every regular noetherian local ring is a unique factorization domain; in particular, it is an integrally closed integral domain. For every ideal $\mathfrak{p}$ in a regular local ring A, the ring $A_\mathfrak{p}$ is regular. See CA 22.5.

A.50. Let X be an algebraic scheme over k. A point $x \in |X|$ is *regular* if $\mathcal{O}_{X,x}$ is a regular local ring. The scheme X is *regular* if every point of $|X|$ is regular. A connected regular algebraic scheme is integral but not necessarily geometrically reduced.

A.51. Let $k[\varepsilon]$ be the k-algebra generated by an element ε with $\varepsilon^2 = 0$, and let X be an algebraic scheme over k. From the map $\varepsilon \mapsto 0 : k[\varepsilon] \to k$, we get a map $X(k[\varepsilon]) \to X(k)$. The fibre of this over a point $x \in X(k)$ is the *tangent space* $\mathrm{Tgt}_x(X)$ of X at x. Thus $\mathrm{Tgt}_x(X)$ is defined for all $x \in |X|$ with $\kappa(x) = k$. To give a tangent vector at x amounts to giving a local homomorphism $\alpha : \mathcal{O}_{X,x} \to k[\varepsilon]$ of k-algebras. Such a homomorphism can be written

$$\alpha(f) = f(x) + D_\alpha(f)\varepsilon, \quad f \in \mathcal{O}_x, \quad f(x), \ D_\alpha(f) \in k.$$

Then D_α is a k-derivation $\mathcal{O}_x \to k$, which induces a k-linear map $\mathfrak{m}/\mathfrak{m}^2 \to k$. In this way, we get canonical isomorphisms

$$\mathrm{Tgt}_x(X) \simeq \mathrm{Der}_k(\mathcal{O}_x, k) \simeq \mathrm{Hom}_{k\text{-linear}}(\mathfrak{m}/\mathfrak{m}^2, k). \qquad (171)$$

The formation of the tangent space commutes with extension of the base field.

A.52. Let X be an irreducible algebraic scheme over k, and let x be a point on X such that $\kappa(x) = k$. Then

$$\dim \mathrm{Tgt}_x(X) \geq \dim X$$

with equality if and only if x is regular. This follows from (171).

A.53. Let X be a closed subscheme of $\mathbb{A}^n$, say

$$X = \mathrm{Spm}\, A, \quad A = k[T_1, \ldots, T_n]/\mathfrak{a}, \quad \mathfrak{a} = \mathfrak{a} = (f_1, \ldots, f_r).$$

Let $t_i = T_i + \mathfrak{a}$, and consider the Jacobian matrix

$$\mathrm{Jac}(f_1, f_2, \ldots, f_r) = \begin{pmatrix} \frac{\partial f_1}{\partial t_1} & \frac{\partial f_1}{\partial t_2} & \cdots & \frac{\partial f_1}{\partial t_n} \\ \frac{\partial f_2}{\partial t_1} & & & \\ \vdots & & & \\ \frac{\partial f_r}{\partial t_1} & & & \frac{\partial f_r}{\partial t_n} \end{pmatrix} \in M_{r,n}(A).$$

Let $d = \dim X$. The *singular locus* X_{sing} of X is the closed subscheme of X defined by the $(n-d) \times (n-d)$ minors of this matrix. This is independent of the embedding of X into $\mathbb{A}^n$. For example, if X is the hypersurface defined by a polynomial $f(T_1, \ldots, T_{d+1})$, then

$$\text{Jac}(f) = \begin{matrix} \frac{\partial f}{\partial t_1} & \frac{\partial f}{\partial t_2} & \cdots & \frac{\partial f}{\partial t_{d+1}} \end{matrix} \in M_{1,d+1}(A),$$

and X_{sing} is the closed subscheme of X defined by the equations

$$\frac{\partial f}{\partial T_1} = 0, \ldots, \frac{\partial f}{\partial T_{d+1}} = 0.$$

For a general algebraic scheme X over k, the *singular locus* X_{sing} is the closed subscheme such that $X_{\text{sing}} \cap U$ has this description for every open affine subset U of X. From its definition, one sees that the formation of the singular locus commutes with extension of the base field.

A.54. Let X be an algebraic scheme over k. A point x of X is *singular* or *nonsingular* according as x lies in the singular locus or not, and X is *nonsingular* (= *smooth*) or *singular* according as X_{sing} is empty or not. If x is such that $\kappa(x) = k$, then x is nonsingular if and only if it is regular. A smooth variety is regular, and a regular variety is smooth if k is perfect.

A.55. A smooth scheme is geometrically reduced. Conversely, if X is geometrically reduced and irreducible, then X_{sing} is a proper closed subset of X (because X is birationally equivalent to a hypersurface $f(T_1, \ldots, T_{d+1}) = 0$ with $\partial f / \partial T_{d+1} \neq 0$; see A.48).

A.56. An algebraic scheme X over a field k is smooth if and only if, for all k-algebras R and ideals I in R such that $I^2 = 0$, the map $X(R) \to X(R/I)$ is surjective (DG, I, §4, 4.6).

i. Étale schemes

A.57. A k-algebra A is said to be *diagonalizable* if it is isomorphic to the product algebra k^n for some $n \in \mathbb{N}$, and it is *étale* if $A \otimes k'$ is diagonalizable for some field k' containing k. In particular, an étale k-algebra is finite.

A.58. A k-algebra $k[T]/(f(T))$ is étale if and only if the polynomial $f(T)$ is separable, i.e., has distinct roots in k^{a}. Every étale k-algebra is a finite product of such algebras.

A.59. The following conditions on a finite k-algebra A are equivalent: (a) A is étale; (b) A is a product of separable field extensions of k; (c) $A \otimes k'$ is reduced for all fields k' containing k; (d) $A \otimes k^{\text{s}}$ is diagonalizable.

A.60. A scheme X finite over k is said to be ***étale*** over k if it satisfies each of the following equivalent conditions: (a) the k-algebra $\mathcal{O}(X)$ is étale (recall that X is affine); (b) X is smooth; (c) X is geometrically reduced; (d) X is an algebraic variety. The equivalence is an immediate consequence of (A.59).

A.61. The following conditions on an algebraic scheme X over k are equivalent: (a) X is étale over k; (b) X is an algebraic variety over k of dimension zero; (c) the space $|X|$ is discrete and the local rings $\mathcal{O}_{X,x}$ for $x \in |X|$ are finite separable field extensions of k.

A.62. Fix a separable closure k^s of k, and let $\Gamma = \mathrm{Gal}(k^s/k)$. The functor $X \rightsquigarrow X(k^s)$ is an equivalence from the category of étale schemes over k to the category of finite discrete Γ-sets. This is an easy consequence of standard Galois theory. By a discrete Γ-set we mean a set X equipped with a continuous action $\Gamma \times X \to X$ of Γ (Krull topology on Γ; discrete topology on X). An action of Γ on a finite discrete set is continuous if and only if it factors through $\mathrm{Gal}(K/k)$ for some finite Galois extension K of k contained in k^s.

j. Galois descent for closed subschemes

A.63. Let A and B be rings (not necessarily commutative), and let S be an A-B-bimodule (this means that A acts on S on the left, B acts on S on the right, and two actions commute). When the functor $M \rightsquigarrow S \otimes_B M \colon \mathsf{Mod}_B \to \mathsf{Mod}_A$ is an equivalence of categories, A and B are said to be ***Morita equivalent through*** S. For example, let D be a division algebra over k of finite degree, and let $A = M_r(D)$. Let $S = D^r$ with A acting by left multiplication and D acting by right multiplication. Then S is a simple A-module, and every A-module is a direct sum of copies of S (24.16). It follows that A and D are Morita equivalent through S.

A.64. Let K be a Galois extension of k with Galois group Γ. Recall that an action of Γ on a K-vector space V is semilinear if $\sigma(cv) = \sigma c \cdot \sigma v$ for all $\sigma \in \Gamma$, $c \in K$, and $v \in V$. For example, if V is a k-vector space, then $\sigma(c \otimes v) = \sigma c \otimes v$ is a semilinear action of Γ on $K \otimes V$. We claim that the functor $V \rightsquigarrow K \otimes_k V$ from k-vector spaces over k to K-vector spaces equipped with a continuous semilinear action of Γ is an equivalence of categories.

It suffices to prove this with K a finite Galois extension. Let $K[\Gamma]$ be the K-vector space with basis Γ. It becomes a K-algebra with the multiplication $(\sum a_\sigma \sigma)(\sum b_\tau \tau) = \sum a_\sigma \sigma(b_\tau)\sigma\tau$. Then $K[\Gamma]$ acts k-linearly on K by the rule $(\sum a_\sigma \sigma)c = \sum a_\sigma \cdot \sigma c$ and Dedekind's theorem on the independence of characters shows that the homomorphism

$$K[\Gamma] \to \mathrm{End}_{k\text{-linear}}(K) \approx M_{\dim(V)}(k)$$

is injective. It is an isomorphism because the two sides have the same dimension as k-vector spaces. Now A.63 shows that $K[\Gamma]$ and k are Morita equivalent through K, which is the required statement.

It follows that the functor $A \rightsquigarrow K \otimes A$ from Hopf algebras over k to Hopf algebras over K equipped with a continuous semilinear action of Γ compatible with the Hopf algebra structure is an equivalence of categories.

A.65. Let X be an algebraic scheme over a field k, and let $X' = X_{k'}$ for some field k' containing k. Let Y' be a closed subscheme of X'. There exists at most one closed subscheme Y of X such that $Y_{k'} = Y'$ (as a subscheme of X'). For example, if $X = \mathrm{Spm}(A)$ and $\mathfrak{a}'$ is an ideal in $A \otimes k'$, then there is at most one ideal $\mathfrak{a}$ in A such that $\mathfrak{a} \otimes k'$ maps isomorphically onto $\mathfrak{a}'$ (the ideal $\mathfrak{a}$ exists if and only if A contains a set of generators for $\mathfrak{a}'$, in which case $\mathfrak{a} = \mathfrak{a}' \cap A$).

Now assume that k' is Galois over k with Galois group Γ. Then Γ acts on X' and Y' arises from an algebraic subscheme of X if and only if it is stable under this action. When X is affine, the action of Γ on X' corresponds to the natural semilinear action of Γ on $\mathcal{O}(X')$, and the statement follows from (A.64). In this case, if $\mathcal{O}(Y') = \mathcal{O}(X')/\mathfrak{a}'$, then Y' is stable under Γ if and only if $\mathfrak{a}'$ is stable under Γ.

Let k' be the separable closure of k. An algebraic subvariety Y' of X' is stable under the action of Γ on X' if and only if the set $Y'(k')$ is stable under the action of Γ on $X(k')$ (because $Y'(k')$ is dense in Y; see A.48).

A.66. Let X and Y be algebraic schemes over k with Y separated, and let $X' = X_{k'}$ and $Y' = Y_{k'}$ for some field k' containing k. Let $\varphi' \colon X' \to Y'$ be a regular map. Because Y' is separated, the graph $\Gamma_{\varphi'}$ of φ' is closed in $X \times Y$, and so we can apply A.65 to it. We deduce the following:

◇ There exists at most one regular map $\varphi \colon X \to Y$ such that $\varphi' = \varphi_{k'}$.

◇ Assume k' is Galois over k, and let $\Gamma = \mathrm{Aut}(k'/k)$. Then $\varphi' \colon X' \to Y'$ arises from a regular map over k if and only if its graph is stable under the action of Γ on $X' \times Y'$.

◇ Let $k' = k^{\mathrm{s}}$, and assume that X and Y are algebraic varieties. Then φ' arises from a regular map over k if and only if the map

$$\varphi'(k') \colon X(k') \to Y(k')$$

commutes with the actions of Γ on $X(k')$ and $Y(k')$.

k. Flat and smooth morphisms

We assume that the reader is familiar with the basic properties of flatness for rings (CA, §11).

A.67. Let $A \to B$ be a local homomorphism of local noetherian rings, and let $u \colon M' \to M$ be a homomorphism of finitely generated B-modules. If M is flat over A and $u \otimes_A (A/\mathfrak{m}_A)$ is injective, then u is injective and $\mathrm{Coker}(u)$ is flat over A (Matsumura 1986, 22.5).

A.68. A regular map $\varphi: Y \to X$ of algebraic schemes over k is said to be **flat** if, for all $y \in |Y|$, the map $\mathcal{O}_{X,\varphi(y)} \to \mathcal{O}_{Y,y}$ is flat. A flat map φ is said to be **faithfully flat** if it is flat and $|\varphi|$ is surjective. The map $\mathrm{Spm}(B) \to \mathrm{Spm}(A)$ defined by a homomorphism of k-algebras $A \to B$ is flat (resp. faithfully flat) if and only if $A \to B$ is flat (resp. faithfully flat).

A.69. A flat map $\varphi: Y \to X$ of algebraic schemes over k is open. This follows from the affine case, proved in CA 23.4.

A.70 (GENERIC FLATNESS). Let $\varphi: Y \to X$ be a regular map of algebraic schemes over k. If X is integral, then there exists a dense open subset U of X such that $\varphi^{-1}(U) \xrightarrow{\varphi} U$ is faithfully flat. This follows from the affine case, proved in CA 21.10.

A.71. A morphism $\varphi: Y \to X$ of algebraic schemes over k is said to be **smooth** (of relative dimension n) if it is flat and the fibres $\varphi^{-1}(x)$ are smooth (of equidimension n) for all $x \in X$. Let k' be an extension of k; then φ is smooth if and only if $\varphi_{k'}$ is smooth. A morphism $\varphi: Y \to X$ of smooth algebraic varieties over an algebraically closed field k is smooth if and only if the map $(d\varphi)_y: \mathrm{Tgt}_y(Y) \to T_{\varphi(y)}(X)$ is surjective for all $y \in Y(k)$ (Hartshorne 1977, III, 10.4). If $\varphi: Y \to X$ is smooth and X is smooth, then Y is smooth (pass to the algebraic closure of k and check that the tangent spaces at points in $Y(k)$ have the correct dimension).

l. The fibres of regular maps

A.72. Let $\varphi: Y \to X$ be a dominant map of integral schemes. For all $P \in \varphi(Y)$,

$$\dim(\varphi^{-1}(P)) \geq \dim(Y) - \dim(X).$$

Equality holds for all P if φ is flat, and hence it always holds for P in a dense open subset of X contained in $\varphi(Y)$ (A.70). These statements follow from the corresponding local statements (CA 23.1, 23.2).

A.73. Let $\varphi: Y \to X$ be a dominant map of integral schemes. Let S be an irreducible closed subset of X, and let T be an irreducible component of $\varphi^{-1}(S)$ such that $\varphi(T)$ is dense in S. Then

$$\dim(T) \geq \dim(S) + \dim(Y) - \dim(X).$$

There exists a dense open subset U of Y such that $\varphi(U)$ is open, $U = \varphi^{-1}(\varphi(U))$, and $U \xrightarrow{\varphi} \varphi(U)$ is flat. If S meets $\varphi(U)$ and T meets U, then

$$\dim(T) = \dim(S) + \dim(Y) - \dim(X).$$

A.74. A surjective morphism of smooth algebraic k-schemes is flat (hence faithfully flat) if its fibres all have the same dimension.

m.   Complete schemes; proper maps

A.75. An algebraic scheme X is said to be ***complete*** if it is separated and if, for all algebraic schemes T, the projection map $q: X \times T \to T$ is closed. (It suffices to check this with $T = \mathbb{A}^n$.)

(a) Closed subschemes of complete schemes are complete.

(b) An algebraic scheme is complete if and only if its irreducible components are complete.

(c) Products of complete schemes are complete.

(d) Let $\varphi: X \to S$ be a regular map of algebraic varieties. If X is complete, then $\varphi(X)$ is a complete closed subvariety of S. In particular,

   (i) if $\varphi: X \to S$ is dominant and X is complete, then φ is surjective and S is complete;

   (ii) complete subvarieties of algebraic varieties are closed.

(e) A regular map $X \to \mathbb{P}^1$ from a complete connected algebraic variety X is either constant or surjective (special case of (d)).

(f) The only regular functions on a complete connected algebraic variety are the constant functions (consequence of (e)).

(g) The image of a regular map from a complete connected algebraic scheme to an affine algebraic scheme is a point. The only complete affine algebraic schemes are the finite schemes.

(h) Projective space $\mathbb{P}^n$ is complete (hence projective varieties are complete).

(i) Every quasi-finite map $Y \to X$ with Y complete is finite.

A.76. A regular map $\varphi: X \to S$ of algebraic schemes is ***proper*** if it is separated and universally closed (i.e., for all regular maps $T \to S$, the projection map $q: X \times_S T \to T$ is closed).

(a) A finite map is proper.

(b) An algebraic scheme X is complete if and only if the map $X \to \mathrm{Spm}(k)$ is proper. The base change of a proper map is proper. In particular, if $\pi: X \to S$ is proper, then $\pi^{-1}(P)$ is a complete subscheme of X for all $P \in S$.

(c) If $X \to S$ is a proper map and S is complete, then X is complete.

(d) The inverse image of a complete algebraic scheme under a proper map is complete.

(e) Let $\varphi: X \to S$ be a proper map. The image of every complete algebraic subscheme of X is a complete algebraic subscheme of S.

n.   The Picard group

A.77. Let X be an algebraic scheme over k. An ***invertible sheaf*** on X is a locally free $\mathcal{O}_X$-module of rank 1. The isomorphism classes of invertible sheaves on X form a group under tensor product, called the ***Picard group*** of X. It is denoted $\mathrm{Pic}(X)$. There is a canonical isomorphism

$$\mathrm{Pic}(X) \simeq H^1(X, \mathcal{O}_X^\times)$$

(Zariski, étale, or flat cohomology). The Picard group of X can also be described as the group of isomorphism classes of line bundles on X.

A.78. An integral domain A is said to be ***normal*** if it is integrally closed in its field of fractions. An algebraic scheme X over k is ***normal*** if $\mathcal{O}_{X,x}$ is normal for all $x \in |X|$. This is equivalent to requiring that $\mathcal{O}_X(U)$ be a normal integral domain for every connected open affine subset U of X (see CA, §6).

Let X be an irreducible variety over k. A ***prime divisor*** on X is an irreducible closed subvariety of codimension 1, and a ***(Weil) divisor*** is an element of the free abelian group $\mathrm{Div}(X)$ generated by the prime divisors. When Z is a prime divisor on X, we define $\mathcal{O}_{X,Z}$ to be the set of rational functions on X that are defined on an open subset U of X with $U \cap Z \neq \emptyset$. For example, if $X = \mathrm{Spm}(A)$, then a prime divisor Z corresponds to a prime ideal $\mathfrak{p}$ of height 1 in A and $\mathcal{O}_{X,Z} = A_\mathfrak{p}$.

Assume that X is normal. Then $\mathcal{O}_{X,Z}$ is a discrete valuation ring (CA 20.2), and we let ord_Z denote the corresponding valuation on $k(X)$. The divisor of a nonzero rational function f on X is defined to be

$$\mathrm{div}(f) = \sum \mathrm{ord}_Z(f) \cdot Z \in \mathrm{Div}(X).$$

There is an exact sequence

$$k(X)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(X) \longrightarrow \mathrm{Pic}(X) \to 0. \tag{172}$$

If f is a regular function defined on the whole of X, then $\mathrm{ord}_Z(f) \geq 0$ for all Z. If, in addition, f is nowhere zero, then $\mathrm{div}(f) = 0$. A rational function on a complete normal variety is constant if its divisor is zero.

A.79. When A is a k-algebra, we let $\mathrm{Pic}(A) = \mathrm{Pic}(\mathrm{Spm}(A))$. The invertible sheaves on X correspond to finitely generated projective A-modules of rank 1 (CA 12.6). If A is a Dedekind domain, then the exact sequence (172) shows that $\mathrm{Pic}(A)$ is the ideal class group of A. If A is a unique factorization domain, then every prime ideal of height 1 is principal (CA 4.2), and so $\mathrm{Pic}(A) = 0$.

o.   Flat descent

A.80. Let $\varphi \colon Y \to X$ be a regular map, and let $X' \to X$ be faithfully flat. If $\varphi' \colon Y \times_X X' \to X'$ is affine (resp. finite, flat, smooth), then φ is affine (resp. finite, flat, smooth).

A.81. Let $Y \to X$ be a faithfully flat morphism of algebraic schemes over k. A ***descent datum*** on a scheme Z' over Y is an isomorphism $\phi \colon p_1^* Z' \to p_2^* Z'$ satisfying

$$p_{31}^*(\phi) = p_{32}^*(\phi) \circ p_{21}^*(\phi),$$

where the p_i are the projections $Y \times_X Y \to Y$ and the p_{ij} are the projections $Y \times_X Y \times_X Y \to Y \times_X Y$. A scheme Z over X defines, in an obvious way, a descent datum on $Z' = Z \times_X X$. Conversely, a scheme Z' over Y equipped with a descent datum arises from an essentially unique scheme Z over X if, for example, Z' admits a projective embedding compatible with the descent datum. More precisely, the map sending a scheme Z over X equipped with an ample invertible sheaf to Z' equipped with its canonical descent datum is an equivalence of categories. See Bosch et al. 1990, Chapter 6.

Existence of Quotients of Algebraic Groups

Let H be an algebraic subgroup of an algebraic group G over a field k. In this appendix, we prove that G/H exists as an algebraic scheme over k.

Because of the additional flexibility it gives us, we consider the problem of quotients in the more general setting of equivalence relations on algebraic schemes. First we prove the existence of a quotient when the equivalence classes are finite (B.18, B.26). From this, we deduce that quotients exist whenever there exists a "quasi-section" (i.e., a one-to-finite section) (see B.32). In general, there will exist a quasi-section for an equivalence relation over a dense open subset (B.35). Using this and homogeneity, we deduce the existence of G/H (see B.37).

In this appendix, we work over a noetherian base ring R_0, and we ignore set-theoretic questions. Points of schemes are not required to be closed. All R_0-algebras are finitely generated, and all rings are noetherian. An algebraic scheme over R_0 is a scheme of finite type over $\operatorname{Spec}(R_0)$. Throughout, "functor" means "functor from R_0-algebras to sets representable by an algebraic scheme over R_0". An algebraic scheme X over R_0 defines such a functor, $R \rightsquigarrow X(R)$, which we denote by $\tilde{X}$ or h_X (or h^A if $X = \operatorname{Spec}(A)$). The functor $X \rightsquigarrow \tilde{X}$ is fully faithful.

This appendix is more technical than the rest of the book. It is used only to prove Theorems 5.14 and 5.34 for nonaffine groups.

a. Equivalence relations

DEFINITION B.1. A pair of morphisms $u_0, u_1 \colon F_1 \rightrightarrows F_0$ of functors is an *equivalence relation* if, for all k-algebras R, the map

$$F_1(R) \xrightarrow{(u_0, u_1)} F_0(R) \times F_0(R)$$

is a bijection from $F_1(R)$ onto the graph of an equivalence relation on $F_0(R)$.

Explicitly, the condition means the following: let R be an R_0-algebra; for $x, x' \in F_0(R)$, write $x \sim x'$ if there exists a $y \in F_1(R)$ such that $u_0(y) = x$ and $u_1(y) = x'$; then $\sim$ is an equivalence relation on the set $F_0(R)$ in the usual sense and y, if it exists, is unique.

Note that the equivalence class of $x \in F_0(R)$ is $u_1(u_0^{-1}(x))$. We say that a subfunctor F_0' of F_0 is **saturated** with respect to an equivalence relation if $F_0'(R)$ is a union of equivalence classes for all R (i.e., $u_1(u_0^{-1}(F')) \subset F'$). Then $F_1' \rightrightarrows F_0'$ is an equivalence relation with $F_1' = u_0^{-1}(F_0') = u_1^{-1}(F_0')$.

EXAMPLE B.2. Recall that an (abstract) group acts *freely* on a set if no element of the group except e has a fixed element. An action of a group functor G on a functor F is said to be *free* if $G(R)$ acts freely on $F(R)$ for all R_0-algebras R. Let $G \times F \to F$ be a free action. Then

$$G \times F \mathrel{\substack{(g,x) \mapsto gx \\ \longrightarrow \\ \longrightarrow \\ (g,x) \mapsto x}} F$$

is an equivalence relation because the freeness means that the map

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

is injective for all R. The graph of the equivalence relation on $F(R)$ is

$$\{(gx, x) \mid g \in G(R),\ x \in F(R)\}$$

and so the equivalence classes are the orbits.

EXAMPLE B.3. For any map of functors $u \colon F_0 \to F$, the pair

$$F_1 = F_0 \times_{u,F,u} F_0 \mathrel{\substack{p_1 \\ \longrightarrow \\ \longrightarrow \\ p_2}} F_0 \qquad (p_1, p_2 \text{ are the projections})$$

is an equivalence relation (two elements of $F_0(R)$ are equivalent if and only if they have the same image in $F(R)$).

DEFINITION B.4. Let $u_0, u_1 \colon F_1 \rightrightarrows F_0$ be an equivalence relation on F_0, and let $f \colon F_0' \to F_0$ be a morphism. Form the fibred product

$$
\begin{array}{ccc}
F_1' & \xrightarrow{(u_0', u_1')} & F_0' \times F_0' \\
\downarrow & & \downarrow{\scriptstyle f \times f} \\
F_1 & \xrightarrow{(u_0, u_1)} & F_0 \times F_0.
\end{array}
$$

Then u_0' and u_1' define an equivalence relation on F_0', called the **inverse image** of (u_0, u_1) with respect to f. Note that $x_0, x_1 \in F_0'(R)$ are equivalent with respect to the inverse image relation if and only if $f(x_0), f(x_1)$ are equivalent with respect to (u_0, u_1).

EXAMPLE B.5. Let $u_0, u_1: F_1 \rightrightarrows F_0$ be an equivalence relation. Then the inverse images of (u_0, u_1) with respect to u_0 and u_1 coincide (as subfunctors of $F_1 \times F_1$). (Identify $F_1(R)$ with the set of pairs $(x_0, x_1) \in F_0(R)$ such that $x_0 \sim x_1$. Then $(x_0, x_1) \sim (x'_0, x'_1)$ with respect to the inverse image by u_0 (resp. u_1) if and only if $x_0 \sim x'_0$ (resp. $x_1 \sim x'_1$). These conditions are the same.)

DEFINITION B.6. Suppose given a diagram

$$F_1 \underset{u_1}{\overset{u_0}{\rightrightarrows}} F_0 \overset{u}{\longrightarrow} F$$

in which (u_0, u_1) is an equivalence relation. We say that u (or by an abuse of language F) is a **quotient** of (u_0, u_1) if the following hold:

(a) $u \circ u_0 = u \circ u_1$;

(b) the map $(u_0, u_1): F_1 \rightarrow F_0 \times_F F_0$ is an isomorphism;

(c) for all functors T, the sequence

$$\mathrm{Hom}(F, T) \longrightarrow \mathrm{Hom}(F_0, T) \rightrightarrows \mathrm{Hom}(F_1, T)$$

is exact, i.e., $\mathrm{Hom}(F, T) \simeq \{v: F_0 \rightarrow T \mid v \circ u_0 = v \circ u_1\}$.

REMARK B.7. Condition (a) says that (u_0, u_1) maps into the fibred product, so that (b) makes sense. Condition (c) implies (a), but (b) and (c) are completely independent. Condition (c) implies that the quotient, if it exists, is unique up to a unique isomorphism.

REMARK B.8. Let $u_0, u_1: X_1 \rightrightarrows X_0$ be morphisms in some category $\mathcal{C}$ with fibred products. A morphism $u: X_0 \rightarrow X$ is a **cokernel** of (u_0, u_1) in $\mathcal{C}$ if $u \circ u_0 = u \circ u_1$ and u is universal with this property:

$$X_1 \underset{u_1}{\overset{u_0}{\rightrightarrows}} X_0 \overset{u}{\longrightarrow} X$$

$$v \circ u_0 = v \circ u_1$$

$$T.$$

In other words, u is the cokernel of (u_0, u_1) if

$$\mathrm{Hom}(X, T) \rightarrow \mathrm{Hom}(X_0, T) \rightrightarrows \mathrm{Hom}(X_1, T)$$

is exact for all objects T in $\mathcal{C}$. A morphism $u: X_0 \rightarrow X$ is an **effective epimorphism** if it is a cokernel of the projection maps $X_0 \times_X X_0 \rightrightarrows X$. Conditions (a) and (c) in B.6 say that u is a cokernel of (u_0, u_1) in the category of functors, and (b) then says that u is an effective epimorphism.

PROPOSITION B.9. *A pair of maps $u_0, u_1: F_1 \rightrightarrows F_0$ is an equivalence relation if and only if*

(a) $F_1(R) \xrightarrow{(u_0, u_1)} (F_0 \times F_0)(R)$ *is injective for all R;*

(b) *there exists a map $s: F_0 \to F_1$ such that $u_0 \circ s = \mathrm{id}_{F_0} = u_1 \circ s$ (i.e., there exists a common section to u_0 and u_1);*

(c) *there exist maps $v_0, v_1, v_2: F_2 \to F_1$ (of functors) such that*

$$
\begin{array}{ccc}
F_2 \underset{v_1}{\overset{v_0}{\rightrightarrows}} F_1 & \xrightarrow{\ u_0\ } & F_0 \\
\Big\downarrow{\scriptstyle v_2} \qquad \Big\downarrow{\scriptstyle u_1} & & \\
F_1 \underset{u_1}{\overset{u_0}{\rightrightarrows}} F_0 & &
\end{array}
$$

commutes (i.e., $u_0 \circ v_0 = u_0 \circ v_1$, $u_1 \circ v_0 = u_0 \circ v_2$, $u_1 \circ v_1 = u_1 \circ v_2$) and the two squares

$$
\begin{array}{ccc}
F_2 & \xrightarrow{\ v_0\ } & F_1 \\
\downarrow{\scriptstyle v_2} & & \downarrow{\scriptstyle u_1} \\
F_1 & \xrightarrow{\ u_0\ } & F_0
\end{array}
\qquad\qquad
\begin{array}{ccc}
F_2 & \xrightarrow{\ v_1\ } & F_1 \\
\downarrow{\scriptstyle v_2} & & \downarrow{\scriptstyle u_1} \\
F_1 & \xrightarrow{\ u_1\ } & F_0
\end{array}
$$

are cartesian.

PROOF. $\Longrightarrow$: (a) is part of the definition of an equivalence relation.

(b) Let S denote the image of (u_0, u_1) in $F_0 \times F_0$. It contains the diagonal, and we define s to be the composite of the maps

$$
F_0 \xrightarrow{(\mathrm{id}, \mathrm{id})} S \xrightarrow{(u_0, u_1)^{-1}} F_1.
$$

In other words, let $x \in F_0(R)$; then $x \sim x$, and so there is a unique $y \in F_1(R)$ such that $u_0(y) = x = u_1(y)$; set $s(x) = y$. Clearly this has the required properties.

(c) Set

$$
F_2(R) = \{(x, y, z) \in (F_0 \times F_0 \times F_0)(R) \mid x \sim y, \ y \sim z\}
$$

and

$$
\left.
\begin{array}{lll}
v_0 : & (x, y, z) \mapsto (y, z) \\
v_1 : & (x, y, z) \mapsto (x, z) \\
v_2 : & (x, y, z) \mapsto (x, y)
\end{array}
\right\} \in F_1(R) = \{(z, w) \in (F_0 \times F_0)(R) \mid z \sim w\}.
$$

With the last identification,

$$u_0(z, w) = w$$
$$u_1(z, w) = z.$$

Now

$$u_0 \circ v_0 \text{ and } u_0 \circ v_1 \text{ both map } (x, y, z) \text{ to } z$$
$$u_1 \circ v_0 \text{ and } u_0 \circ v_2 \text{ both map } (x, y, z) \text{ to } y$$
$$u_1 \circ v_1 \text{ and } u_1 \circ v_2 \text{ both map } (x, y, z) \text{ to } x.$$

This proves the commutativity, and the first square is cartesian because

$$F_1 \times_{F_0} F_1 = \{(x, y), (x', y') \mid x \sim y, \ x' \sim y', \ y = x'\}$$
$$= \{(x, y, y') \mid x \sim y, \ y \sim y'\}.$$

Similarly, the second square is cartesian.

$\Longleftarrow$: For $x \in F_0(R)$,

$$x = u_0(s(x)) = u_1(s(x)) = x,$$

and so

$$x \sim x.$$

Suppose that $x \sim y$ and $x \sim z$ in $F_0(R)$; then

$$\begin{cases} x = u_1(x') \\ y = u_0(x') \end{cases} \text{ some } x' \in F_1(R) \qquad \begin{cases} x = u_1(x'') \\ z = u_0(x'') \end{cases} \text{ some } x'' \in F_1(R).$$

Now $u_1(x') = u_1(x'')$, and so there exists an $x''' \in F_2(R)$ such that

$$v_1(x''') = x' \text{ and } v_2(x''') = x''$$

(the second square is cartesian). Consider $v_0(x''')$. Firstly,

$$u_0(v_0(x''')) = u_0(v_1(x''')) = y.$$

Secondly,

$$u_1(v_0(x''')) = u_0(v_2(x''')) = z,$$

and so $y \sim z$. This shows that $\sim$ is an equivalence relation (if $x \sim y$ then $y \sim x$ because $x \sim x$). $\qquad\square$

REMARK B.10. Let $u_0, u_1 \colon F_1 \rightrightarrows F_0$ be an equivalence relation. From the symmetry of the equivalence relation, we obtain an automorphism $s' \colon F_0 \to F_0$ such that $u_0 \circ s' = u_1$ and $u_1 \circ s' = u_0$. (Let $y \in F_1(R)$; then $u_0(y) \sim u_1(y)$ and so $u_1(y) \sim u_0(y)$; this means that there exists a (unique) $y' \in F_1(R)$ such that $u_0(y') = u_1(y)$ and $u_1(y') = u_0(y)$; set $s'(y) = y'$.) Thus, if F_1 and F_0 are schemes and the morphism u_0 has some property, then the morphism u_1 will have the same property.

b.   Existence of quotients in the finite affine case

Preliminaries

B.11. Let A be a ring and M an A-module. We say that M is ***locally free of finite rank*** if there exists a finite family $(f_i)_{i \in I}$ of elements of A generating the unit ideal A and such that, for all $i \in I$, the A_{f_i}-module M_{f_i} is free of finite rank. Equivalent conditions: M is finitely generated and projective; M is finitely presented and flat (CA 12.6). We say that an A-algebra is ***locally free of finite rank*** if it is so as an A-module.

B.12. Let B be a locally free A-algebra of finite rank r, and let $b \in B$. If B is free over A, then we define the characteristic polynomial of b over A in the usual way. Now let $(f_i)_{i \in I}$ be a family of elements generating the unit ideal and such that B_{f_i} is free over A_{f_i}. Then we have a well-defined characteristic polynomial in $A_{f_i}[T]$ for each i. These agree in $A_{f_i f_j}[T]$ for all $i, j \in I$. Using the exact sequence[1]

$$A \longrightarrow \prod_{i \in I} A_{f_i} \rightrightarrows \prod_{(i,j) \in I \times I} A_{f_i f_j}$$

we obtain a well-defined characteristic polynomial of b in $A[T]$. In particular, the norm of b is a well-defined element of A.

B.13. Let A be a ring and B a faithfully flat A-algebra. Then an A-module M is locally free of finite rank if and only if the B-module $B \otimes_A M$ is locally free of finite rank (because this is true with "flat" or "finitely presented" in place of "locally free of finite rank"; CA 11.9, 12.4).

B.14. Let A be a ring and $u : M \to N$ a homomorphism of A-modules. Then u is injective (resp. surjective, bijective, zero) if and only if $u_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective, zero) for all maximal ideals $\mathfrak{m}$ in A (CA 5.17).

B.15. Let A be a ring. An A-module M is flat (resp. faithfully flat) if and only if the $A_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$ is flat (resp. faithfully flat) for all maximal ideals $\mathfrak{m}$ in A (CA 11.17).

B.16. A locally free module of finite constant rank over a semilocal ring is free (CA 12.9).

B.17. If B is faithfully flat over A and $M \otimes_A B$ is faithfully flat over B, then M faithfully flat over A (CA 11.9).

---

[1]This exists because there is a sheaf $\mathcal{O}$ on $\mathrm{spec}(A)$ with $\mathcal{O}(D(f)) = A_f$ for all $f \in A$; alternatively, use that $A \to \prod_i A_{f_i}$ is faithfully flat.

The theorem

Let A_0 and A_1 be R_0-algebras. We say that the pair of maps $u_0, u_1 \colon A_0 \rightrightarrows A_1$ is an equivalence relation if the pair $h^{u_0}, h^{u_1} \colon h^{A_1} \rightrightarrows h^{A_0}$ is an equivalence relation, and that $u \colon A \to A_0$ is a quotient if $h^u \colon h^{A_0} \to h^A$ is a quotient.

THEOREM B.18. *Let $u_0, u_1 \colon A_0 \rightrightarrows A_1$ be an equivalence relation. If u_0 is locally free of constant rank r, then a quotient $u \colon A \to A_0$ exists, and A_0 is locally free of rank r as an A-module.*

The proof will require several steps. Consider the diagram

$$
\begin{array}{ccccc}
A_2 & \underset{v_1}{\overset{v_0}{\rightleftarrows}} & A_1 & \overset{u_0}{\longleftarrow} & A_0 \\
\big\uparrow{\scriptstyle v_2} & & \big\uparrow{\scriptstyle u_1} & & \big\uparrow{\scriptstyle u} \\
A_1 & \underset{u_1}{\overset{u_0}{\rightleftarrows}} & A_0 & \overset{u}{\longleftarrow} & A.
\end{array}
$$

Condition (c) for a quotient says that, for all R_0-algebras R,

$$
\mathrm{Hom}(R, A) \longrightarrow \mathrm{Hom}(R, A_0) \underset{u_1}{\overset{u_0}{\rightrightarrows}} \mathrm{Hom}(R, A_1)
$$

is exact. With $R = R_0$, this says that $A = \mathrm{Ker}(u_0, u_1)$ and that u equals the inclusion map – define them in this way. Then,

(a) the map $h^{A_1}(R) \to \left(h^{A_0} \times h^{A_0}\right)(R) = h^{A_0 \otimes_R A_0}(R)$ is injective for all R (because (u_0, u_1) is an equivalence relation);

(b) there exists an s such that $s \circ u_0 = s \circ u_1$ (see B.10);

(c) the undashed part of the diagram is commutative, and the two left-hand squares are cocartesian (see B.9);

(d) u_1 is locally free of rank r (hypothesis and (b));

(e) $u = \mathrm{Ker}(u_0, u_1)$ (construction);

and we have to show

(f) the right-hand square is cocartesian ($\Rightarrow u$ is a quotient);

(g) u is locally free of rank r.

STEP 0. *Statement (a) is equivalent to (a'): $A_0 \otimes_A A_0 \to A_1$ is surjective.*

PROOF. First note that we have a factorization

$$
A_0 \otimes_{R_0} A_0 \longrightarrow A_0 \otimes_A A_0 \longrightarrow A_1
$$

$$
h^{A_0} \times h^{A_0} \longleftarrow h^{A_0} \times_{h^A} h^{A_0} \longleftarrow h^{A_1}
$$

and so (a) is equivalent to the map $h^{A_1} \to h^{A_0 \otimes_A A_0}$ being injective. Certainly, (a′) implies that this map is injective, and the converse follows from the next (general) lemma. ☐

LEMMA B.19. *Let A be a ring and B a finite A-algebra. If $h^B \to h^A$ is injective, then the map $A \to B$ is surjective.*

PROOF. First note that $h^B \to h^A$ is injective if and only if $h^B \times_{h^A} h^B \simeq h^B$, i.e., the map $b \mapsto b \otimes 1 - 1 \otimes b \colon B \to B \otimes_A B$ is an isomorphism. The map $A \to B$ is surjective if $A_{\mathfrak{m}} \to B_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ of A (see B.14). After localizing at $\mathfrak{m}$, we still have that $B_{\mathfrak{m}}$ is a finite $A_{\mathfrak{m}}$-algebra and that $B_{\mathfrak{m}} \simeq B_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} B_{\mathfrak{m}}$. Thus, we may assume that A is local (with maximal ideal $\mathfrak{m}$). Then, by Nakayama's lemma, it suffices to prove that

$$A/\mathfrak{m}A \to B/\mathfrak{m}B$$

is surjective. Let $k = A/\mathfrak{m}A$ (a field) and $C = B/\mathfrak{m}B$. The hypothesis implies that $C \simeq C \otimes_k C$, but this implies that $\dim_k(C) = 1$, and so $k \simeq C$. ☐

As R_0 has dropped out of all the hypotheses, we may forget about it.

STEP 1. *It suffices to prove (f) and (g′): u is faithfully flat.*

PROOF. These conditions imply that u is locally free (of rank r), because after a faithfully flat base change it is and so we can apply (B.13). ☐

STEP 2. *We may suppose that A is local.*

PROOF. Note that tensoring the diagram with $A_{\mathfrak{p}}$ (over A) preserves all the hypotheses (because $A_{\mathfrak{p}}$ is flat over A). Suppose that the theorem has been proved for $A_{\mathfrak{p}}$ with $\mathfrak{p}$ arbitrary. Then (f) follows from (B.14) and (g′) follows from (B.15). ☐

STEP 3. *We may suppose that A is local with infinite residue field.*

PROOF. Suppose that A is local with maximal ideal $\mathfrak{m}$; then $\mathfrak{p} = \mathfrak{m}A[T]$ is prime in $A[T]$ because $A[T]/\mathfrak{p} = (A/\mathfrak{m})[T]$. Moreover, $A \to (A[T])_{\mathfrak{p}}$ is flat (because $A \to A[T]$ is) and is local, therefore faithfully flat. All the hypotheses are preserved by a faithfully flat base change, and also the conclusions. For (g′) this follows from B.17. ☐

STEP 4. *The ring A_0 is integral over A.*

PROOF. Let $x \in A_0$ and let $y = u_0(x) \in A_1$. We shall show that the characteristic polynomial
$$F(T) = T^r - \sigma_1 T^{r-1} + \cdots + (-)^r \sigma_r$$
of y over A_0 (via u_1) has coefficients in A and that $F(x) = 0$.

Let $z = v_0(y) = v_1(y) \in A_2$. The characteristic polynomial is preserved by base change, and so $u_0(F)$ and $u_1(F)$ both equal the characteristic polynomial of z (over A_1 via v_2):

$$
\begin{array}{ccccc}
A_2 & \xleftleftarrows{v_0} & A_1 & \xleftarrow{u_0} & A_0 \\
\big\uparrow{\scriptstyle v_2} & & \big\uparrow{\scriptstyle u_1} & & \big\uparrow{\scriptstyle u} \\
A_1 & \xleftleftarrows[u_1]{u_0} & A_0 & \xleftarrow{\quad u \quad} & A
\end{array}
\qquad
\begin{array}{ccccc}
z & \xleftleftarrows{v_0} & y & \xleftarrow{u} & x \\
{\scriptstyle u_0(F), u_1(F)}\big\updownarrow{\scriptstyle v_2} & & F\big\updownarrow{\scriptstyle u_1} & & \\
* & \xleftleftarrows[u_1]{u_0} & * .
\end{array}
$$

Therefore, $u_0(F) = u_1(F)$, and so $F = u(F_0)$ with $F_0 \in A[T]$. But $F(y) = 0$, i.e., $(uF_0)(u_0x) = 0$, and so $u_0(F_0(x)) = 0$. Now apply s to get $F_0(x) = 0$. $\quad\square$

STEP 5. *The ring A_0 is semilocal.*

PROOF. Because A_0 is integral over A, every maximal ideal of A_0 lies over the maximal ideal of A. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_N$ be distinct maximal ideals of A_0, and let $a_1, \ldots, a_N \in A$ be distinct modulo $\mathfrak{m}$ (recall that the residue field is infinite). Take $x \in A_0$ such that $x \equiv a_i \bmod \mathfrak{m}_i$ (exists by the Chinese remainder theorem). Then the characteristic polynomial of x, modulo $\mathfrak{m}$, has N distinct roots, namely, $a_1, \ldots, a_N$, and so $N \le r$. $\quad\square$

STEP 6. *Completion of the proof.*

Now apply B.16:

$$
\left.
\begin{array}{l}
A_1 \text{ locally free of rank } r \text{ over } A_0 \text{ (via } u_1) \\
A_0 \text{ semilocal}
\end{array}
\right\} \implies A_1 \text{ free over } A_0 \text{ (via } u_1).
$$

Note that the set $u_0(A_0)$ generates A_1 as a (u_1, A_0)-module (because $A_0 \otimes_A A_0 \to A_1$ is surjective). Therefore Lemma B.20 below shows that there exist $x_1, \ldots, x_r \in A_0$ such that $u_0(x_1), \ldots, u_0(x_r)$ form a basis for A_1 over A_0 (via u_1).

We shall complete the proof by showing that A_0 is free over A with basis $\{x_1, \ldots, x_r\}$ and that $A_1 = A_0 \otimes_A A_0$. Let $y_i = u_0(x_i)$.

If $\sum a_i x_i = 0$, $a_i \in A$, then $\sum a_i y_i = 0$, and so $a_i = 0$ all i. Therefore the x_i are linearly independent.

Let $x \in A_0$, and let $y = u_0(x)$. By assumption, there exist $b_i \in A_0$ such that

$$
y = \sum u_1(b_i) y_i = \sum b_i y_i.
$$

In the last expression, we regard A_1 as an A_0-module via u_1. Let

$$
z = v_0(y) = v_1(y)
$$
$$
z_i = v_0(y_i) = v_1(y_i).
$$

Then the z_i form a basis A_2 over A_1 (via v_2), and so

$$z = \sum u_0(b_i)z_i = \sum u_1(b_i)z_i \implies u_0(b_i) = u_1(b_i) \text{ all } i \implies b_i \in A, \text{ all } i.$$

On applying s to $y = \sum b_i y_i$, we find that $x = \sum b_i x_i$, and so the x_i generate.

LEMMA B.20. *Let $u: A \to B$ be a homomorphism with A local and B semilocal. Assume that u maps the maximal ideal $\mathfrak{m}$ of A into every maximal ideal of B. Let N be a free B-module of rank r, and let M be an A-submodule of N such that $N = BM$. If the residue field of A is infinite, then M contains a B-basis for N.*

PROOF. Let $\mathfrak{r}$ be the radical of B (intersection of the maximal ideals). Elements $n_1, \dots, n_r$ of N form a B-basis for N if (and only if) their images in $N/\mathfrak{r}N$ form a $B/\mathfrak{r}$-basis – by Nakayama's lemma, they will generate N, and there are r of them. Thus we may replace N with $N/\mathfrak{r}N$, M with $M/M \cap \mathfrak{r}N$, and so on. Then A is a field, and B is a finite product of finite field extensions $B = \prod_{j=1}^{s} k_j$ of k. Correspondingly, $N = \prod_{j=1}^{s} N_j$ with N_j a k_j-vector space of dimension r. To complete the proof, we use induction on r, the case $r = 0$ being trivial.

We claim that there exists an $m \in M$ whose image in N_j is zero for no j. By hypothesis there exists an $m_j \in M$ whose image in N_j is not zero. Consider

$$m = c_1 m_1 + \dots + c_s m_s, \quad c_j \in k.$$

The set of families $(c_j)_{1 \le j \le s}$ for which $m = 0$ in N_j is a proper subspace of k^s, and a finite union of proper subspaces of a finite-dimensional vector space over an infinite field cannot equal the whole space[2] – hence there exists an appropriate family (c_j).

The B-module $N/Bm = \prod_j N_j/k_j m_j$ is free of rank $r - 1$, and the k-subspace M/km still generates it. By the induction hypothesis, there exist elements $m_1, \dots, m_{r-1}$ in M forming a B-basis for N/Bm. Now $m_1, \dots, m_{r-1}$ together with m form a B-basis for N. □

REMARK B.21. Let $u: A \to A_0$ be faithfully flat. Then $u = \mathrm{Ker}(u_0, u_1)$, and so the maps

$$x \mapsto x \otimes 1, 1 \otimes x: A_0 \rightrightarrows A_0 \otimes_A A_0$$

are an equivalence relation on A_0 with quotient $u: A \to A_0$. The theorem says that every equivalence relation with A_1 locally free of constant rank over A_0 is isomorphic to one of this form.

REMARK B.22. (a) The system

$$A \xrightarrow{\ u\ } A_0 \underset{u_1}{\overset{u_0}{\rightrightarrows}} A_0 \otimes_A A_0 \qquad \begin{cases} u \text{ faithfully flat} \\ u = \mathrm{Ker}(u_0, u_1) \end{cases}$$

[2] Suppose $V = \bigcup_{i=1}^{n} V_i$ with $V_i \ne V$. Let $f_i: V \to k$ be a nonzero linear map zero on V_i. Then $\prod f_j$ is a nonzero polynomial function on V vanishing identically, which is impossible because k is infinite.

retains its properties under extension of scalars (because u stays faithfully flat).

(b) The above system retains its properties under tensor products, i.e.,

$$
\begin{array}{ccc}
A \longrightarrow & A_0 \rightrightarrows & A_0 \otimes_A A_0 \\
\otimes R_0 & \otimes R_0 & \otimes R_0 \\
B \longrightarrow & B_0 \rightrightarrows & B_0 \otimes_B B_0
\end{array}
$$

has the same properties.

(c) A map $\varphi \colon A_0 \to B_0$ defines a map $A \to B$ if $\varphi \otimes \varphi$ satisfies the obvious commutativity condition:

$$
\begin{array}{ccc}
A \xrightarrow{\ u\ } & A_0 \rightrightarrows & A_0 \otimes A_0 \\
\downarrow & \downarrow{\varphi} & \downarrow{\varphi \otimes \varphi} \\
B \longrightarrow & B_0 \rightrightarrows & B_0 \otimes V_0.
\end{array}
$$

In other words, given equivalence relations $A_0 \rightrightarrows A_1$ and $B_0 \rightrightarrows B_1$ as in B.18, we have a map

$$
\mathrm{Hom}((A_0, A_1), (B_0, B_1)) \to \mathrm{Hom}(A, B).
$$

c. Existence of quotients in the finite case

Preliminaries

B.23. *Let Z be a closed subset of $X = \mathrm{Spec}(A)$ and let S be a finite set of points of $X \smallsetminus Z$. Then there exists an $f \in A$ that is zero on Z but not zero at any point in S.*

PROOF. This is the prime avoidance lemma (CA 2.8) □

B.24. *Let B be a locally free A-algebra of rank r. Let $\mathfrak{p}$ be a prime ideal in A, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be the prime ideals of B lying over it. An element b of B lies in $\mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n$ if and only if its norm $\mathrm{Nm}(b) \in \mathfrak{p}$.*

PROOF. After replacing A and B with $A_\mathfrak{p}$ and $B_\mathfrak{p}$, we may suppose that A is local with maximal ideal $\mathfrak{p}$ and that B is semilocal with maximal ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$. Then B is free of rank r (see B.16), and $\mathrm{Nm}(b)$ is the determinant of an A-linear map $\ell_b \colon B \to B$, $x \mapsto bx$. Now

$$
\mathrm{Nm}(b) \notin \mathfrak{p} \Leftrightarrow \mathrm{Nm}(b) \text{ is invertible} \quad (\mathfrak{p} \text{ is the only maximal ideal of } A)
$$
$$
\Leftrightarrow \ell_b \text{ is invertible} \quad (\text{linear algebra})
$$
$$
\Leftrightarrow b \text{ is invertible in } B
$$
$$
\Leftrightarrow b \notin \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n \quad (\mathfrak{q}_1, \ldots, \mathfrak{q}_n \text{ are the only maximal ideals of } B). \ \square
$$

B.25. According to the prime avoidance lemma, b lies in $\mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n$ if and only if it lies in some $\mathfrak{q}_i$. Therefore, B.24 says the zero set of $\mathrm{Nm}(b)$ in $\mathrm{spec}(A)$ is the image under $\mathrm{spec}(B) \to \mathrm{spec}(A)$ of the zero set of b in $\mathrm{spec}(B)$. More generally, let $\pi\colon Y \to X$ be a morphism of schemes that is finite and locally free of constant rank r, and let $b \in \Gamma(Y, \mathcal{O}_Y)$; then $\pi(Z(b)) = Z(\mathrm{Nm}(b))$.

The theorem

Let X_0 be an algebraic scheme over R_0. By an equivalence relation on X_0, we mean a pair of morphisms $X_1 \rightrightarrows X_0$ such that $\tilde{X}_1 \rightrightarrows \tilde{X}_0$ is an equivalence relation on $\tilde{X}_0$. We say that $X_0 \to X$ is a quotient if $\tilde{X}_0 \to \tilde{X}$ is a quotient; in particular, $X_1 \simeq X_0 \times_X X_0$. A subscheme U_0 of X_0 is saturated if $\tilde{U}_0$ is saturated in $\tilde{X}_0$; then $U_1 \rightrightarrows U_0$ is an equivalence relation on U_0 with $U_1 = u_0^{-1}(U) = u_1^{-1}(U)$.

THEOREM B.26. *Let $u_0, u_1\colon X_1 \rightrightarrows X_0$ be an equivalence relation on the algebraic scheme X_0 over R_0. Assume*

(a) *$u_0\colon X_1 \to X_0$ is locally free of constant rank r;*

(b) *for all $x \in X_0$, the set $u_0(u_1^{-1}(x))$ is contained in an open affine subscheme of X_0.*

Then a quotient $u\colon X_0 \to X$ exists; moreover, u is locally free of rank r.

When X_0 and X_1 are affine, this is a restatement of Theorem B.18. The idea of the general proof is to construct the quotient in the category of R_0-ringed spaces, and then use the affine case to show that the ringed space quotient is a scheme quotient.

STEP 1. *Every $x \in X_0$ has a saturated open affine neighbourhood.*

PROOF. By hypothesis, there exists an open affine neighbourhood U of x containing its equivalence class $u_1 u_0^{-1}(x)$. Let U' denote the union of the equivalence classes contained in U, i.e., U' is the complement in U of $u_1 u_0^{-1}(X_0 \smallsetminus U)$. This last set is closed because u_1 is finite, and so U' is open. Moreover U' is saturated by construction. It contains x and is contained in U, and it is quasi-affine, but it need not be affine.

As U is affine and the set $u_1 u_0^{-1}(x)$ is finite and contained in U', there exists an $f \in \mathcal{O}_{X_0}(U)$ that is zero on $U \smallsetminus U'$ but is not zero at any of the points of $u_1 u_0^{-1}(x)$ (see B.23). In other words, the principal open subset $D(f)$ of U is contained in U' and contains $u_1 u_0^{-1}(x)$. Let U'' denote the union of the equivalence classes contained in $D(f)$, i.e., U'' is the complement in $D(f)$ of $u_1 u_0^{-1}(U' \smallsetminus D(f))$. As before, this is a saturated open set. It contains x and is contained in $D(f)$. It remains to show that it is affine.

Let $Z(f) = U' \smallsetminus D(f)$ be the zero set of f in U'. Then $u_0^{-1}(Z(f))$ is the zero set of $u_0^*(f)$ in $u_0^{-1}(U') = u_1^{-1}(U')$. Therefore $u_1 u_0^{-1}(Z(f))$ is the zero set of $\mathrm{Nm}(u_0^*(f))$ in U' (B.24). By construction, its complement in $D(f)$ is exactly U'', and so U'' is the set of points of $D(f)$ where $\mathrm{Nm}(u_0^*(f))$ is not zero, which is an open affine subset of $D(f)$. □

STEP 2. *Let $u_0, u_1 : X_1 \rightrightarrows X_0$ be a pair of morphisms of R_0-ringed spaces.*

  (a) *There exists a cokernel $u : X_0 \to X$ in the category of R_0-ringed spaces.*

  (b) *If u_0, u_1, and u are morphisms of schemes, then $u : X_0 \to X$ is a cokernel in the category of R_0-schemes.*

PROOF. (a) Let $|X|$ be the topological space obtained from $|X_0|$ by identifying $u_0(x)$ and $u_1(x)$ for all $x \in |X_1|$, and let u be the quotient map. For an open subset U of X, define $\mathcal{O}_X(U)$ so that

$$\mathcal{O}_X(U) \to \mathcal{O}_{X_0}(u^{-1}(U)) \rightrightarrows \mathcal{O}_{X_1}((u_0 \circ u)^{-1}U)$$

is exact. A routine verification shows that $\mathcal{O}_X$ is a sheaf of R_0-algebras on X, and that $u : X_0 \to X$ is a cokernel of (u_0, u_1) in the category of ringed spaces.

    (b) Assume that u_0, u_1, and u are morphisms of schemes, and let $v : X_0 \to T$ be a morphism of R_0-schemes such that $v \circ u_0 = v \circ u_1$. By hypothesis, there exists a unique morphism of ringed spaces $r : X \to T$ such that $r \circ u = v$. It remains to show that, for all $x \in X$, the homomorphism $\mathcal{O}_{r(x)} \to \mathcal{O}_x$ induced by r is local. But $x = u(x_0)$ for some $x_0 \in X_0$, and $\mathcal{O}_x \to \mathcal{O}_{x_0}$ and the composite map

$$\mathcal{O}_{r(x)} \to \mathcal{O}_x \to \mathcal{O}_{x_0}$$

are local, which implies the statement.   □

STEP 3. *Completion of the proof*

PROOF. Let $u_0, u_1 : X_1 \rightrightarrows X_0$ be as in the statement of the theorem, and let $u : X_0 \to X$ of (u_0, u_1) be the cokernel in the category of R_0-ringed spaces. Let U_0 be a saturated open affine subset of X_0, and let $U_1 = u_0^{-1}(U_0) = u_1^{-1}(U_0)$. Then $(u_0, u_1) : U_1 \rightrightarrows U_0$ is an equivalence relation, and $V = u(U_0) \subset X$ is the cokernel of $(u_0, u_1)|U_1$ in the category of R_0-ringed spaces. From the affine case (B.18), we see that V is an affine scheme. From Step 1, we see that X is covered by finitely many such V, and so X is an algebraic scheme over R_0 and u is a morphism of R_0-schemes. It follows from Step 2 that u is the cokernel of (u_0, u_1) in the category of schemes over R_0. Finally, $X_1 \simeq X_0 \times_X X_0$ because this condition is local on X.   □

REMARK B.27. It is possible to weaken the hypothesis (a) to

     (a′) $u_0 : X_1 \to X_0$ is locally free of finite rank,

because such an equivalence relation decomposes into a finite disjoint union of equivalence relations of constant rank. Indeed, for $r \in \mathbb{N}$, let X_0^r denote the set of points over which u_0 has rank r. As u_0 is locally free of finite rank, each X_0^r is open in X_0, and X_0 is a finite disjoint union of the X_0^r. Using the associativity of the equivalence relation, one sees that each X_0^r is saturated, from which the claim follows.

Application

PROPOSITION B.28. *Let G be an algebraic group over R_0 and H an algebraic subgroup of G. Assume that H is locally free of rank r over R_0. Then the quotient sheaf $G\widetilde{/}H$ is representable by an algebraic scheme G/H over R_0, and the morphism $G \to G/H$ is locally free of rank r; moreover, $G \times H \simeq G \times_{G/H} G$.*

PROOF. Apply the theorem to the following equivalence relation on G:

$$G \times H \xrightarrow[\ (g,h) \mapsto g\ ]{\ (g,h) \mapsto gh\ } G.$$

□

d.   Existence of quotients in the presence of quasi-sections

Preliminaries

We shall need the following technical lemma.

LEMMA B.29. *Let*

$$
\begin{array}{ccc}
Y_1 & \overset{v_0}{\underset{v_1}{\rightrightarrows}} & Y_0 \\
\downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} \\
X_1 & \overset{u_0}{\underset{u_1}{\rightrightarrows}} & X_0
\end{array}
$$

be a commutative diagram in some category $\mathcal{C}$ with fibred products. Assume that f_0 and f_1 are effective epimorphisms, and that there exists a morphism $\Delta: Y_0 \times_{X_0} Y_0 \to Y_1$ such that $v_0 \circ \Delta = p_1$ and $v_1 \circ \Delta = p_2$. Then the cokernel of (u_0, u_1) exists if and only if the cokernel of (v_0, v_1) exists, in which case f_0 induces an isomorphism

$$\mathrm{Coker}(v_0, v_1) \to \mathrm{Coker}(u_0, u_1).$$

PROOF. Let T be an object of $\mathcal{C}$, and consider the diagram

$$
\begin{array}{ccc}
C(u_0,u_1)(T) \overset{u}{\longrightarrow} \mathrm{Hom}(X_0,T) & \rightrightarrows & \mathrm{Hom}(X_1,T) \\
\Big\downarrow{\scriptstyle f(T)} \qquad \Big\downarrow{\scriptstyle T(f_0)} & & \Big\downarrow{\scriptstyle T(f_1)} \\
C(v_0,v_1)(T) \overset{v}{\longrightarrow} \mathrm{Hom}(Y_0,T) & \rightrightarrows & \mathrm{Hom}(Y_1,T)
\end{array}
$$

in which the left-hand terms are defined to make the rows exact. Here $T(f_i)$ is the map defined by $f_i: Y_i \to X_i$. The cokernel of (u_0, u_1) exists if and only if the

functor $T \rightsquigarrow C(u_0, u_1)(T) : \mathcal{C} \to \mathsf{Set}$ is representable, in which case it represents the functor.

The map $T(f_0)$ is injective because f_0 is an epimorphism. As $f(T)$ is induced by $T(f_0)$, it also is injective. We shall show that $f(T)$ is surjective for all T, and so f is an isomorphism of functors on $\mathcal{C}$. Thus $C(u_0, u_1)$ is representable by an object of $\mathcal{C}$ if and only if $C(v_0, v_1)$ is. This will complete the proof of the lemma because we will have shown that f_0 induces an isomorphism of functors.

Let $g \in C(v_0, v_1)(T)$. Thus g is a map $Y_0 \to T$ such that $g \circ v_0 = g \circ v_1$:
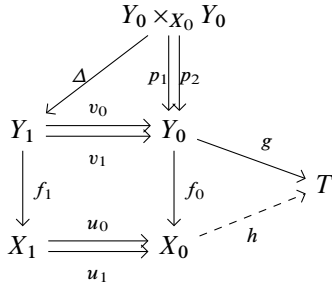
Then $g \circ v_0 \circ \Delta = g \circ v_1 \circ \Delta$, and so $g \circ p_1 = g \circ p_2$. As f_0 is an effective epimorphism, $g = h \circ f_0$ for some $h : X_0 \to T$, i.e., $g = T(f_0)(h)$. It remains to show that $h \circ u_0 = h \circ u_1$. But

$$h \circ u_0 \circ f_1 = h \circ f_0 \circ v_0 = g \circ v_0 = g \circ v_1 = h \circ f_0 \circ v_1 = h \circ u_1 \circ f_1,$$

which implies that $h \circ u_0 = h \circ u_1$ because f_1 is an epimorphism. $\square$

LEMMA B.30. *Let $u_0, u_1 : X_1 \rightrightarrows X_0$ be an equivalence relation on an algebraic scheme X_0 over R_0, and let $v_1, v_0 : Y_1 \rightrightarrows Y_0$ be its inverse image with respect to a morphism $f_0 : Y_0 \to X_0$. Assume that f_0 is faithfully flat or that it admits a section. Then the cokernel of (u_0, u_1) exists if and only if the cokernel of (v_0, v_1) exists, in which case f_0 induces an isomorphism*

$$\mathrm{Coker}(v_0, v_1) \to \mathrm{Coker}(u_0, u_1).$$

PROOF. Assume that f_0 is faithfully flat. Recall (B.4) that the inverse image equivalence relation is defined by the cartesian square

$$
\begin{array}{ccc}
Y_1 & \xrightarrow{(v_1, v_0)} & Y_0 \times Y_0 \\
\downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0 \times f_0} \\
X_1 & \xrightarrow{(u_1, u_0)} & X_0 \times X_0.
\end{array}
$$

Therefore $f_1 : Y_1 \to X_1$ is also faithfully flat, and so both f_0 and f_1 are effective epimorphisms (Appendix A). There exists a morphism $s : X_0 \to X_1$ such that $u_0 \circ$

$s = \mathrm{id}_{X_0} = u_1 \circ s$ (see B.9) and we let Δ denote the map $Y_0 \times_{X_0} Y_0 \to Y_1$ defined by the inclusion $Y_0 \times_{X_0} Y_0 \hookrightarrow Y_0 \times Y_0$ and the map $s \circ f_0 \circ p_1 : Y_0 \times_{X_0} Y_0 \to X_1$. Then $v_0 \circ \Delta = p_1$ and $v_1 \circ \Delta = p_2$, and so we can apply Lemma B.29 to obtain the result. The proof when f_0 admits a section is similar. □

The theorem

DEFINITION B.31. Let $u_0, u_1 : X_1 \rightrightarrows X_0$ be an equivalence relation on an algebraic scheme X_0 over R_0. A **quasi-section** of (u_0, u_1) is a subscheme Y_0 of X_0 such that

(a) the restriction of u_1 to $u_0^{-1}(Y_0)$ is finite, locally free, and surjective onto X_0;

(b) for all $x \in Y_0$, the set $u_1 u_0^{-1}(x) \cap Y_0$ is contained in an open affine subscheme of Y_0.

Condition (a) implies that every equivalence class meets Y_0 in a finite nonempty set, and (b) then says that each of these sets is contained in an open affine subset of Y_0.

THEOREM B.32. *Let $u_0, u_1 : X_1 \rightrightarrows X_0$ be an equivalence relation on an algebraic scheme X_0 over R_0. If (u_0, u_1) admits a quasi-section, then a quotient $u : X_0 \to X$ exists; moreover, u is surjective, and if u_0 is open (resp. universally closed, flat) then u is also.*

PROOF. We shall need the following diagrams:

(a) Let Y_0 be a quasi-section. Let $i : Y_0 \hookrightarrow X_0$ denote the inclusion map, and let $v_0, v_1 : Y_1 \rightrightarrows Y_0$ be the inverse image of (u_0, u_1) with respect to i. According to the definition (B.4), Y_1 is the intersection $u_0^{-1}(Y_0) \cap u_1^{-1}(Y_0)$, and so we have a cartesian square:

$$
\begin{array}{ccc}
Y_1 & \longrightarrow & u_0^{-1}(Y_0) \\
\downarrow{\scriptstyle v_1} & & \downarrow{\scriptstyle f} \\
Y_0 & \xrightarrow{\ i\ } & X_0.
\end{array}
\qquad f = \text{restriction of } u_1 \text{ to } u_0^{-1}(Y_0).
$$

Hence v_1 is finite, locally free, and surjective. According to Theorem B.26 (and B.27), the equivalence relation $v_0, v_1 : Y_1 \rightrightarrows Y_0$ admits a quotient $v : Y_0 \to Y$.

(b) Let $Z_0 = u_0^{-1}(Y_0) \subset X_1$, and let $(w_0, w_1): Z_1 \rightrightarrows Z_0$ be the inverse image of (v_0, v_1) with respect to the restriction $u_0|Z_0$ of u_0 to Z_0. The map $u_0|Z_0$ admits a section (because u_0 does by B.9b), and so B.30 shows that the pair of maps $(w_0, w_1): Z_1 \rightrightarrows Z_0$ admits a cokernel $w: Z_0 \to Z$ isomorphic (by $u_0|Z_0$) to $v: Y_0 \to Y$. The map $Z_1 \to Z_0 \times_Z Z_0$ is an isomorphism because it is a pull-back of the isomorphism $Y_1 \to Y_0 \times_Y Y_0$. Thus w is a quotient of (w_0, w_1).

(c) Note that (w_0, w_1) is the inverse image of (u_0, u_1) with respect to $i \circ (u_0|Z_0)$, which equals the map $Z_0 \hookrightarrow X_1 \xrightarrow{u_0} X_0$. Therefore, according to Example B.5, it is also the inverse image of (u_0, u_1) with respect to the map $Z_0 \hookrightarrow X_1 \xrightarrow{u_1} X_0$. But this last map is the restriction f of u_1 to $u_0^{-1}(Y_0)$, which is finite and locally free (by assumption), and hence faithfully flat. Lemma B.30 now shows that (u_0, u_1) admits a cokernel $u: X_0 \to X$ isomorphic (by f) to $w: Z_0 \to Z$. The map $X_1 \to X_0 \times_X X_0$ because its pull-back by the faithfully flat map $f \times f$ is the isomorphism $Z_1 \to Z_0 \times_Z Z_0$. Thus $u: X_0 \to X$ is a quotient of (u_0, u_1).

Finally, u is obviously surjective. The morphism v is finite and locally free (B.26), and it follows easily that u is open (resp. universally closed, flat) if u_0 is. □

REMARK B.33. The map $u: X_0 \to X$ is the cokernel of (u_0, u_1) in the category of ringed spaces.

e.　Existence generically of a quotient

For simplicity, in this section we take the base ring R_0 to be a field k.

Preliminaries

B.34. *Let X and Y be algebraic schemes over k. Let x be a closed point of $|X|$ and let y be a point of $|Y|$. There exist only finitely many points of $|X \times Y|$ mapping to both x and y under the projection maps $X \times Y \to X$ and $X \times Y \to Y$.*

PROOF. The points in question are in one-to-one correspondence with the points mapping to y under the projection map $\mathrm{Spec}(\kappa(x)) \times Y \to Y$. As $\kappa(x)$ is a finite extension of k, this set is obviously finite. □

The theorem

THEOREM B.35. *Let $u_0, u_1: X_1 \rightrightarrows X_0$ be an equivalence relation on an algebraic scheme X_0 over k. Suppose that u_0 is flat and that X_0 is quasi-projective over k. Then there exists a saturated dense open subscheme W of X such that the induced equivalence relation on W admits a quotient.*

After B.32 it suffices to show that we can choose W so that the equivalence relation induced on it has a quasi-section.

STEP 1. *For every closed point z of X_0, there exists a closed subset Z of X_0 such that*

(a) *the restriction of u_1 to $u_0^{-1}(Z)$ is flat at the points of $u_1^{-1}(z)$;*

(b) *$Z \cap u_1 u_0^{-1}(z)$ is finite and nonempty.*

PROOF. We construct a Z satisfying (b), and then show that the Z we have constructed also satisfies (a).

To obtain Z, we construct a strictly decreasing sequence $Z_0 \supset Z_1 \supset \cdots$ of closed subsets of X_0 such that $Z_n \cap u_1 u_0^{-1}(z)$ is nonempty. Let $Z_0 = X_0$, and suppose that Z_n has been constructed. If $Z_n \cap u_1 u_0^{-1}(z)$ is finite, then Z_n satisfies (b). Otherwise we construct Z_{n+1} as follows. The set $u_0^{-1}(Z_n) \cap u_1^{-1}(z)$ is closed in X_1, and we let $y_1, \ldots, y_r$ denote the generic points of its irreducible components. The image $Z_n \cap u_0 u_1^{-1}(z)$ of $u_0^{-1}(Z_n) \cap u_1^{-1}(z)$ in X_0 is infinite by hypothesis; it is also constructible, and so it contains infinitely many closed points. We can therefore choose a closed point x of $Z_n \cap u_0 u_1^{-1}(z)$ distinct from the points $u_0(y_1), \ldots, u_0(y_r)$. By hypothesis, X_0 can be realized as a subscheme of $\mathbb{P}^m$ for some m. As x is closed in X_0, its closure in $\mathbb{P}^m$ does not contain any point $u_0(y_i)$, and so there exists a homogeneous polynomial $f \in k[X_0, \ldots, X_m]$ which is zero at x but not at any point $u_0(y_i)$ (homogeneous prime avoidance lemma; cf. B.23). We put $Z_{n+1} = Z_n \cap V_+(f)$. It is a closed subset of X, strictly contained in Z_n, and $Z_{n+1} \cap u_1 u_0^{-1}(z)$ is nonempty because it contains x.

Eventually, $Z_{n+1} \cap u_1 u_0^{-1}(z)$ will be finite, and it remains to show (inductively) that the restriction of u_1 to $u_0^{-1}(Z_{n+1})$ is flat at the points of $u_1^{-1}(z)$. Let y be such a point. Let $\mathcal{O}_z$ (resp. $\mathcal{O}_y$, $\mathcal{O}_y'$) be the local ring of z in X (resp. of y in $u_0^{-1}(Z_n)$, of y in $u_0^{-1}(Z_{n+1})$). By induction $\mathcal{O}_y$ is flat over $\mathcal{O}_z$. The local ring $\mathcal{O}_y'$ of y in $u_0^{-1}(Z_{n+1})$ can be described as follows. Let g be a homogeneous polynomial of degree 1 such that $D_+(g)$ is a neighbourhood of $u_0(y)$ in $\mathbb{P}^m$. In a neighbourhood of $u_0(y)$ (in Z_n), Z_{n+1} has equation $f/g^d = 0$ for some homogeneous polynomial f of degree d. Therefore in a neighbourhood of y (in $u_0^{-1}(Z_n)$), $u_0^{-1}(Z_{n+1})$ has equation $h = 0$, where h is the image f/g^d in $\mathcal{O}_y$, and so $\mathcal{O}_y' = \mathcal{O}_y/h\mathcal{O}_y$. By construction, h is not a zero-divisor on $\mathcal{O}_y$, and so (A.67) implies that $\mathcal{O}_y'$ is flat over $\mathcal{O}_z$. □

STEP 2. *For every closed point z of X_0, there exists a saturated open subset W_z of X_0 admitting a quasi-section and meeting every irreducible component of X_0 passing through z.*

PROOF. Let Z be as in Step 1, and let $u_1' : u_0^{-1}(Z) \to X_0$ be the restriction of u_1. The fibre $u_1'^{-1}(z)$ is finite (B.34). Let U be the open subset of $u_0^{-1}(Z)$ formed of the points where u_1' is both flat and quasi-finite. Let W_z denote the largest open subset of $u_1'(U)$ above which u_1' is finite and flat. Then W_z contains the generic points of the irreducible components passing through z. By using the associativity of the equivalence relation, one shows that W_z is saturated, and that $u_1'^{-1}(W_z) = u_0'^{-1}(U)$ for some open subset U of Z. Note that W_z contains U because it is saturated. It follows from the construction of W_z that U is a

quasi-section for the induced equivalence relation on W_z (see SGA 3, V, §8, p. 281 for more details).   □

STEP 3. *There exists a saturated dense open subscheme W of X such that the equivalence relation induced on W has a quasi-section.*

PROOF. Let z be a closed point of X, and let W_z be as in Step 2. Its exterior $u_0^{-1}(X_0 \smallsetminus \bar{W}_z)$ is then saturated (because $u_1(u_0^{-1}(X_0 \smallsetminus \bar{W}_z))$ is open and doesn't meet W_z). If this exterior is nonempty, then it contains a closed point z', and we have a set $W_{z'}$, which we may suppose to be contained in $X_0 \smallsetminus \bar{W}_z$. Then W_z and $W_{z'}$ are disjoint, and the equivalence relation induced on $W_z \sqcup W_{z'}$ admits a quasi-section. Continuing in this way, we arrive at the required W in finitely many steps because X_0 has only finitely many components.   □

As noted earlier, this completes the proof of the theorem.

f. Existence of quotients of algebraic groups

In this section, we work over a base field k.

Preliminaries

LEMMA B.36. *Let X be an algebraic scheme over a field k. Suppose that we are given, for each finite extension k' of k in fixed algebraic closure k^a of k, an open subset $U[k']$ of $X_{k'}$ containing $X(k')$. Assume that $U[k']_{k''} \subset U[k'']$ whenever $k' \subset k''$. Then $U[k'] = X_{k'}$ for some finite extension k' of k.*

PROOF. Let $Z[k']$ denote the complement of $U[k']$ in $X_{k'}$. If $Z[k]$ is nonempty, we choose a closed point x_i in each irreducible component of $Z[k]$, and we let k_1 be a finite normal extension of k in k^a containing a conjugate of every field $\kappa(x_i)$. Every point of X_{k_1} above an x_i is k_1-rational and so lies in $U[k_1]$; hence $\dim Z[k_1] < \dim Z[k]$. If $Z[k_1]$ is nonempty, we repeat the argument with k_1 for k to obtain a finite extension k_2/k_1 such that

$$\dim Z[k_2] < \dim Z[k_1] < \dim Z[k].$$

Eventually this process stops with an empty scheme $Z[k']$.   □

The theorem

Recall that a homomorphism $i \colon H \to G$ of algebraic groups is said to be a monomorphism if $\mathrm{Ker}(\varphi) = e$. A monomorphism $i \colon H \to G$ of algebraic groups defines an equivalence relation on G:

$$G \times H \; \underset{(g,h) \mapsto g}{\overset{(g,h) \mapsto gh}{\rightrightarrows}} \; G.$$

The quotient of G by this relation (if it exists) is denoted G/H.

THEOREM B.37. *Let $i: H \to G$ be a monomorphism of algebraic groups over k. Then G admits a quotient G/H for the equivalence relation defined by (H, i); in particular, the sheaf $G\tilde{/}H$ is represented by an algebraic scheme G/H over k. The quotient map $u: G \to G/H$ is faithfully flat.*

In the proof, we assume that G is quasi-projective.

STEP 1. *The theorem becomes true after a finite extension of the base field.*

PROOF. For a finite extension k' of k, we let $U[k']$ denote the union of the open subsets $W \subset G_{k'}$ stable under the right action of $H_{k'}$ and such that the quotient $W/H_{k'}$ exists. Then $U[k']$ is the largest open subset of $G_{k'}$ with these properties. The left translate of $U[k']$ by an element of $G(k')$ also has these properties, and so equals $U[k']$; thus $U[k']$ is stable under the left action of $G(k')$. Theorem B.35 implies that $U[k]$ is dense in G, and, in particular, contains a closed point. After possibly replacing k by a finite extension, we may suppose that $U[k]$ contains a k-point. Then, for every finite extension k'/k, the set $U[k']$ contains $G(k')$. Now Lemma B.36 shows that $U[k'] = X_{k'}$ for some k'. □

STEP 2. *Suppose that G admits a quotient $u: G \to X$ for the equivalence relation defined by H. Then every finite set of closed points of X is contained in an open affine subset.*

PROOF. Let $x_1, \ldots, x_n$ be closed points of X and U a dense open affine subset of X.

Suppose initially that each x_i equals $u(g_i)$ for some $g_i \in G(k)$, and that the open subset

$$\bigcap_{i=1}^{n} g_i (u^{-1}(U))^{-1}$$

of G, which is automatically dense, contains a k-rational point g. Then $g \in g_i \cdot (u^{-1}(U))^{-1}$ for all i, and so $g_i \in g \cdot u^{-1}(U)$ and $x_i \in g \cdot U$. Therefore the open affine subset $g \cdot U$ has the required properties.

We know that $x_i = u(g_i)$ for some closed point g_i of G. Let K be a finite extension of k such that all the points g'_j of G_K mapping to some g_i are K-rational (take K to be any normal extension of k such that every field $\kappa(g_i)$ embeds into it). Then

$$\bigcap_j g'_j (u^{-1}(U_K))^{-1}$$

is a dense open subset of G_K, and therefore contains a closed point g. After possibly extending K, we may suppose that g is K-rational. The previous case now shows that there exists an open affine subset U' of X_K containing the images x'_j of the g'_j. As the x'_j are *all* the points of X_K mapping to an x_i, they form a union of orbits for the finite locally free equivalence relation on X_K defined by the projection $X_K \to X$. By arguing as in (B.18), we obtain a saturated open affine subset $W' \subset U'$ containing all the x'_j. Its image W in X contains all the x_i, and it is open and affine because it is the quotient of the affine W' by a finite locally free equivalence relation (see the affine case B.18). □

STEP 3. *Conclusion (descent)*

PROOF. Let K be a finite extension of k such that the quotient $G_K \to G_K/H_K$ exists. The inverse image of the equivalence relation

$$\operatorname{Spec}(K \otimes_k K) \underset{p_2}{\overset{p_1}{\rightrightarrows}} \operatorname{Spec}(K)$$

(see B.3) with respect to $G_K/H_K \to \operatorname{Spec}(K)$ is an equivalence relation on G_K/H_K satisfying the conditions of Theorem B.26. Its quotient is the required quotient of G by H.   □

As shown earlier (5.14, 5.34), Theorem B.37 can be used to prove that every normal algebraic subgroup N of an algebraic group G arises as the kernel of a quotient map $G \to G/N$, and that every monomorphism of algebraic groups is a closed immersion.

REMARK B.38. The quasi-projectivity hypothesis can be removed from the proof of (B.37) by first removing it from the proof of (B.35) – see SGA 3, V, 8.1. Once this has been done, it is possible to deduce that all algebraic groups G over a field are, in fact, quasi-projective. We may suppose that G is connected. It then contains a connected affine normal algebraic subgroup N such that G/N is an abelian variety (Barsotti, Chevalley, Raynaud; 8.28). The morphism $G \to G/N$ is affine and hence quasi-projective. Now G is quasi-projective because abelian varieties are projective (Barsotti, Matsusaka) and a composite of quasi-projective maps is quasi-projective. Alternatively, it is possible to prove directly that all algebraic groups are quasi-projective (see 8.43 for more general result).

NOTES. The elementary proof of (B.18) follows lectures of Tate from 1967. For the rest, we have followed Brochard 2014 and the original source, SGA 3, V.

Root Data

In the main body of the work, we classify split reductive groups in terms of certain combinatorial objects called root data. Here we review the theory of root data. Proofs of some of the more standard statements are omitted. The standard reference for root systems is Bourbaki 1968.

Throughout, F is a field of characteristic zero, for example, $\mathbb{Q}$ or $\mathbb{R}$. Vector spaces V over F are finite-dimensional. The subspace spanned by a subset S of V is denoted by $\langle S \rangle$. We let $V^\vee$ denote the dual vector space of V, and we write $\langle \ , \ \rangle$ for the pairing $(x, f) \mapsto f(x): V \times V^\vee \to F$. When F is a subfield of $\mathbb{R}$, an inner product on V is a positive definite bilinear form $(\ , \ )$. A linear map $\alpha: V \to V$ is orthogonal for $(\ , \ )$ if $(\alpha x, \alpha y) = (x, y)$ for all $x, y \in V$.

After C.18, all root systems are reduced.

a. Preliminaries

A ***reflection*** of a vector space V over F is an endomorphism s of V that fixes the elements of some hyperplane H and acts as -1 on a complementary line. If α is a nonzero element of V such that $s(\alpha) = -\alpha$, then s is said to be a ***reflection with vector*** α. Then $V = H \oplus \langle \alpha \rangle$ with s acting as $1 \oplus -1$. In particular, s is determined by H and α, and $s^2 = 1$.

LEMMA C.1. *If $\alpha^\vee$ is an element of $V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, then*

$$s_\alpha: x \mapsto x - \langle x, \alpha^\vee \rangle \alpha \tag{173}$$

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, let s be a reflection with vector α, and let H be its fixed hyperplane. We seek a map $\alpha^\vee: V \to F$ such that $\alpha^\vee(H) = 0$ and $\langle \alpha, \alpha^\vee \rangle = 2$. 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 such map. □

REMARK C.2. There is a canonical isomorphism $V \otimes V^{\vee} \simeq \operatorname{End}(V)$ under which $v \otimes f$ corresponds to the map $x \mapsto \langle x, f \rangle v$. Under this isomorphism, s_{α} corresponds to $\operatorname{id}_V - \alpha \otimes \alpha^{\vee}$.

LEMMA C.3. *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 $t = 1$. □

Let V be a vector space over F.

DEFINITION C.4. A subgroup X of V is a ***lattice*** in V if it is generated as a $\mathbb{Z}$-module by a basis of V. This means that the natural map $X \otimes_{\mathbb{Z}} F \to V$ is an isomorphism.

REMARK C.5. When $F = \mathbb{Q}$, every finitely generated subgroup of V spanning V is a lattice, but this is not true when $F = \mathbb{R}$ or $\mathbb{C}$. For example, $\mathbb{Z}1 + \mathbb{Z}\sqrt{2}$ is not a lattice in $\mathbb{R}$. When $F = \mathbb{R}$, the lattices in V are exactly the discrete subgroups X such that V/X is compact.

DEFINITION C.6. Let X and Y be free $\mathbb{Z}$-modules of finite rank. A bi-additive pairing $X \times Y \to \mathbb{Z}$ is said to be ***perfect*** if it has discriminant ± 1. This means that it realizes each of X and Y as the dual of the other.

REMARK C.7. Let $\langle \, , \, \rangle : V \times W \to F$ be a nondegenerate bilinear pairing of F-vector spaces, and let Y be a lattice in W. Then

$$X = \{v \in V \mid \langle v, Y \rangle \subset \mathbb{Z}\}$$

is the unique lattice in V such that $\langle \, , \, \rangle$ restricts to a perfect pairing $X \times Y \to \mathbb{Z}$.

b. Reflection groups

Let V be a vector space over $\mathbb{R}$ equipped with an inner product $(\, , \,)$. A ***reflection group*** on V is a discrete subgroup of the group of linear automorphisms of V generated by orthogonal reflections.

LEMMA C.8. *For each nonzero vector α in V, there is a unique orthogonal reflection with vector α, namely,*

$$s_\alpha(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha. \tag{174}$$

PROOF. Certainly, s_α is an orthogonal reflection with vector α. Let s' be a second such reflection, and let $H = \langle\alpha\rangle^\perp$. Then H is stable under s', and projects 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 coincides with s. □

Thus the reflection (173) defined by a vector $\alpha^\vee \in V^\vee$ is orthogonal if and only if $\alpha^\vee = 2(\ ,\alpha)/(\alpha,\alpha)$.

Now let R be a finite spanning subset, not containing 0, such that (a) $R \cap \mathbb{R}\alpha = \{\alpha, -\alpha\}$ and (b) $s_\alpha(R) \subset R$ for all $\alpha \in R$. We call the elements of R **roots**, and we let W denote the reflection group generated by the s_α for $\alpha \in R$. For each $\alpha \in R$, we have a hyperplane

$$H_\alpha = \{x \in V \mid s_\alpha(x) = x\} = \{x \in V \mid (x,\alpha) = 0\} = \langle\alpha\rangle^\perp.$$

The **chambers** for R are the connected components of $V \smallsetminus \bigcup_{\alpha\in R} H_\alpha$. The group W acts on the set of chambers.

A subset S of R is a **base** for R if it is a basis for V and 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 S are called the **simple roots** (for the base), and the roots $\sum_{\alpha\in S} m_\alpha\alpha$ with nonnegative coefficients m_α the **positive roots** (for the base).

Let t lie in a Weyl chamber. Thus, t is an element of V such that $(\alpha,t) \neq 0$ if $\alpha \in R$. Let $R_t^+ = \{\alpha \in R \mid (\alpha,t) > 0\}$. We say that $\alpha \in R_t^+$ is **indecomposable** if it cannot be written as a sum of two elements of R_t^+.

PROPOSITION C.9. *The indecomposable elements of R_t^+ form a base S_t, which depends only on the Weyl chamber of t, and R_t^+ is the system of positive roots for the base. Every base arises in this way from a unique Weyl chamber.*

PROOF. Suppose that S_t is not a base. Then there exists an element α of R_t^+ not a linear combination with nonnegative coefficients of the elements of S_t, and we may choose one with (α,t) minimal. As $\alpha \notin S_t$, it is decomposable, say, $\alpha = \beta + \gamma$ with $\beta, \gamma \in R_t^+$. Now

$$(\alpha,t) = (\beta,t) + (\gamma,t).$$

As $(\beta,t), (\gamma,t) > 0$, each is strictly less than (α,t), and so each is a linear combination with nonnegative coefficients of the elements of S_t, which is a contradiction. Thus no such element α exists. The rest of the proof is similarly straightforward (Humphreys 1990, 1.3, 1.12). □

The proposition shows that the base S and the set R^+ of positive roots determine each other.

PROPOSITION C.10. *The group W acts simply transitively on the set of bases, hence also on the set of chambers.*

PROOF. Humphreys 1990, 1.8. □

THEOREM C.11. *Let S be a base for R. Then W is generated by the reflections s_α with $\alpha \in S$, subject only to the relations*

$$(s_\alpha s_\beta)^{m(\alpha,\beta)} = 1,$$

where $m(\alpha, \beta)$ is the order of $s_\alpha s_\beta$ in W.

PROOF. For the first part of the statement, which is all we need, see Serre 1966, V, Théorème 2. For the complete statement, see Humphreys 1990, 1.9. □

A group G with a presentation $\langle S \mid (st)^{m(s,t)} = 1 \rangle$, where $m(s,s) = 1$ and $m(s,t) \geq 2$ for $s \neq t$, is called a ***Coxeter group***. Thus, the theorem says that W is a Coxeter group.

c. Root systems

Let V be a vector space over F.

DEFINITION C.12. A subset R of V 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 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.

We sometimes refer to the pair (V, R) as a root system over F. The elements of R are called the ***roots*** of the root system. If α is a root, then $s_\alpha(\alpha) = -\alpha$ is also a root. The dimension of V is called the ***rank*** of the root system.

C.13. It follows from C.3 that the reflection s_α in (RS2) is uniquely determined by α, and so the condition (RS3) does make sense.

C.14. Using C.1, we can be more explicit: a finite spanning subset R of V not containing 0 is a root system if there exists a map $\alpha \mapsto \alpha^\vee : R \to V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \subset \mathbb{Z}$, and the reflection $s_\alpha : x \mapsto \langle x, \alpha^\vee \rangle \alpha$ maps R into R. Remarks C.1 and C.13 show that there is at most one map $\alpha \mapsto \alpha^\vee$ satisfying these conditions. The element $\alpha^\vee \in V^\vee$ is called the ***coroot*** of α.

C.15. The **Weyl group** $W = W(R)$ of a root system (V, R) is the group of automorphisms of V generated by the reflections s_α for $\alpha \in R$. The group $W(R)$ acts on R, and as R spans V, this action is faithful. Therefore $W(R)$ is finite. For $\alpha \in R$, let H'_α denote the hyperplane in $V^\vee$ orthogonal to α:

$$H'_\alpha = \{t \in V^\vee \mid \langle \alpha, t \rangle = 0\}.$$

When $F \subset \mathbb{R}$, the **Weyl chambers** are the connected components of $V \smallsetminus \bigcup_{\alpha \in R} H'_\alpha$. The group $W(R)$ acts on the set of Weyl chambers.

EXAMPLE C.16. Let V be the hyperplane in F^{n+1} consisting of $(n+1)$-tuples $(x_1, \ldots, x_{n+1})$ such that $\sum x_i = 0$, and let

$$R = \{\alpha_{ij} \stackrel{\text{def}}{=} e_i - e_j \mid i \neq j, \quad 1 \leq i, j \leq n+1\},$$

where $(e_i)_{1 \leq i \leq n+1}$ is the standard basis for F^{n+1}. For each $i \neq j$, let $s_{\alpha_{ij}}$ be the linear map $V \to V$ that interchanges 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.

C.17. Let (V, R) be a root system over F, and let V_0 be the $\mathbb{Q}$-vector space generated by R. Then $c \otimes v \mapsto cv \colon V_0 \otimes_{\mathbb{Q}} F \to V$ is an isomorphism, and R is a root system in V_0. Thus, to give a root system over F is the same as giving a root system over $\mathbb{Q}$ (or $\mathbb{R}$). The proof is straightforward.

C.18. Let α be a root. If $\beta = c\alpha$ ($c \in \mathbb{Q}$) is also a root, then $2c = \langle c\alpha, \alpha^\vee \rangle \in \mathbb{Z}$. Using this one finds that $\mathbb{Q}\alpha \cap R$ equals $\{-\alpha, \alpha\}$, $\{-2\alpha, -\alpha, \alpha, 2\alpha\}$, or $\{-\alpha, -\alpha/2, \alpha/2, \alpha\}$. When only the first case occurs, the root system is said to be **reduced**. In other words, R is reduced if, for every $\alpha \in R$, the only multiples of α in R are $\pm\alpha$.

From now on "root system" will mean "reduced root system".

An invariant inner product

C.19. Let (V, R) be a root system over $F \subset \mathbb{R}$. There exists an inner product $(\ ,\ )$ on V for which the elements of W act as orthogonal maps. For example, we can choose any inner product $(\ ,\ )'$ and define $(x, y) = \sum_{w \in W}(wx, wy)'$.

C.20. Once an invariant inner product has been chosen, the above theory takes on a more familiar form. For example, s_α is given by the formula (174). The hyperplane H_α of vectors in V fixed by s_α is orthogonal to α, and the ratio $(x, \alpha)/(\alpha, \alpha)$ is independent of the choice of the inner form:

$$\langle x, \alpha^\vee \rangle = 2\frac{(x, \alpha)}{(\alpha, \alpha)} = (x, \alpha'), \quad \text{where } \alpha' = \frac{2\alpha}{(\alpha, \alpha)}.$$

Note that the map $\alpha \mapsto (\ , \alpha)$ is an isomorphism $V \to V^\vee$ that sends H_α onto H'_α. Thus it maps $V \smallsetminus \bigcup_{\alpha \in R} H_\alpha$ isomorphically onto $V^\vee \smallsetminus \bigcup_{\alpha \in R} H'_\alpha$.

Bases

Let (V, R) be a (reduced) root system over $F \subset \mathbb{R}$.

C.21. As before, a **base** for R is a subset S of R that is a basis for V and such that each root can be written as a linear combination of elements of S with coefficients integers all of the same sign. A **system of positive roots** for R is a subset R^+ such that (a) for each root α, exactly one of $\pm\alpha$ lies in R^+, and (b) if α and β are distinct elements of R^+ and $\alpha + \beta \in R$, then $\alpha + \beta \in R^+$. If S is a base for R, then $\mathbb{N}S \cap \Phi$ is a system of positive roots. Conversely, if R^+ is a system of positive roots, then the **simple roots**, i.e., those that cannot be written as the sum of two elements of R^+, form a base.

C.22. On applying the results of the previous section to $V \otimes_F \mathbb{R}$ and the choice of an invariant inner form, we find that bases exist and are in one-to-one correspondence with the Weyl chambers. The Weyl group acts simply transitively on the set of Weyl chambers, and hence on the set of bases for R. The Weyl group is a Coxeter group with generators s_α, $\alpha \in S$. Moreover, $W \cdot S = R$ (Humphreys 1990, 1.5).

C.23. If $(V_i, R_i)_{i \in I}$ is a finite family of root systems, then

$$\bigoplus_{i \in I}(V_i, R_i) \stackrel{\text{def}}{=} (\bigoplus_{i \in I} V_i, \bigsqcup R_i)$$

is a root system, called the **direct sum** of the (V_i, R_i). A root system is **indecomposable** (or **irreducible**) if it cannot be written as a direct sum of nonempty root systems. Clearly, every root system is a direct sum of indecomposable root systems (and the decomposition is unique).

C.24. Let S be a base for R. If (V, R) is indecomposable, then 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. 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 C.25. Let (V, R) be the root system in C.16, and endow V with the usual inner product. If we choose

$$t = ne_1 + \cdots + e_n - \frac{n}{2}(e_1 + \cdots + e_{n+1}),$$

then

$$R_t^+ \stackrel{\text{def}}{=} \{\alpha \mid (t, \alpha) > 0\} = \{e_i - e_j \mid i > j\}.$$

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

$$\tilde{\alpha} = e_1 - e_{n+1} = \alpha_1 + \cdots + \alpha_n.$$

For a detailed study of root systems of rank 2, see Section g below.

Diagrams

C.26. Let (V, R) be a root system over $\mathbb{Q}$. The ***root lattice*** $Q(R)$ is the $\mathbb{Z}$-submodule of V spanned by R, i.e., $Q(R) = \mathbb{Z}R$. The ***weight lattice*** is

$$P(R) = \{v \in V \mid \langle v, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}.$$

Let $R^\vee = \{\alpha^\vee \mid \alpha \in R\}$ and $Q(R^\vee) = \mathbb{Z}R^\vee$. Then $P(R)$ is the unique lattice in V such that $\langle\,,\,\rangle$ restricts to a perfect pairing $P(R) \times Q(R^\vee) \to \mathbb{Z}$ (see C.7). The condition (RS3) says that $Q(R) \subset P(R)$. Because $P(R)$ and $Q(R)$ are lattices in the same $\mathbb{Q}$-vector space, the quotient $P(R)/Q(R)$ is finite.

C.27. A ***diagram*** is a root system (V, R) together with a lattice X in V such that

$$Q(R) \subset X \subset P(R).$$

To give X amounts to giving a subgroup of the finite group $P(R)/Q(R)$.

d. Root data

When X is a free $\mathbb{Z}$-module of finite rank, we let $X^\vee$ denote the linear dual $\mathrm{Hom}(X, \mathbb{Z})$ of X, and we write $\langle\,,\,\rangle$ for the perfect pairing

$$\langle x, f \rangle \mapsto f(x) \colon X \times X^\vee \to \mathbb{Z}.$$

DEFINITION C.28. A ***root datum***[1] is a triple $\mathcal{R} = (X, R, \alpha \mapsto \alpha^\vee)$ in which X is a free $\mathbb{Z}$-module of finite rank, R is a finite subset of X, and $\alpha \mapsto \alpha^\vee$ is a map 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 $s_\alpha \colon X \to X$ is the reflection $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$;

(rd3) the group generated by the automorphisms s_α of X is finite (it is denoted $W(\mathcal{R})$ and called the ***Weyl group*** of $\mathcal{R}$).

Note that s_α is a reflection of $X_\mathbb{Q}$ with vector α and fixed hyperplane $\{x \in X_\mathbb{Q} \mid \langle x, \alpha^\vee \rangle = 0\}$. We let $R^\vee = \{\alpha^\vee \mid \alpha \in R\}$. 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).

---

[1] The original French term is "donnée radicielle" (SGA 3, XXI).

The condition (rd1) implies that $s_\alpha(\alpha) = -\alpha$, and that the converse holds if $\alpha \neq 0$. If, for every $\alpha \in R$, the only multiples of α in R are $\pm\alpha$, then the root datum is said to be **reduced**. *From now on, "root datum" will mean "reduced root datum".*

PROPOSITION C.29. *Let $(X, R, \alpha \mapsto \alpha^\vee)$ be a triple satisfying (rd1) and (rd2), and let V be the $\mathbb{Q}$-subspace of $X_\mathbb{Q}$ spanned by R. Then (V, R) is a root system (not necessarily reduced) and the image of $\alpha^\vee$ in $V^\vee$ is the coroot of α in the sense of root systems.*

PROOF. We check (C.14). The inclusion $V \hookrightarrow X_\mathbb{Q}$ defines a surjection $f \mapsto \bar{f} \colon X_\mathbb{Q}^\vee \twoheadrightarrow V^\vee$. Let $\alpha \in R$. Then $\alpha \neq 0$ because $\langle \alpha, \bar{\alpha}^\vee \rangle = 2$. Moreover, $s_\alpha(R) \subset R$ by hypothesis, and $\langle R, \bar{\alpha}^\vee \rangle = \langle R, \alpha^\vee \rangle \subset \mathbb{Z}$ because $\alpha^\vee \in X^\vee$. $\qquad\square$

C.30. By a **base** S for a root datum $(X, R, \alpha \mapsto \alpha^\vee)$, we mean a base of the associated root system (V, R). There is a natural identification of the Weyl group W of $(X, R, \alpha \mapsto \alpha^\vee)$ with that of (V, R), and so $WS = R$ (see C.22).

PROPOSITION C.31. *Let $(X, R, \alpha \mapsto \alpha^\vee)$ be a triple satisfying (rd1) and (rd2), and let $\alpha, \beta \in R$. If $\langle x, \alpha^\vee \rangle = \langle x, \beta^\vee \rangle$ for all $x \in R$, then $\alpha = \beta$. Hence the map $\alpha \mapsto \alpha^\vee \colon R \to R^\vee$ is a bijection.*

PROOF. As $\langle \beta, \alpha^\vee \rangle = \langle \beta, \beta^\vee \rangle = 2$, we have $s_\alpha(\beta) = \beta - 2\alpha$, and similarly, $s_\beta(\alpha) = \alpha - 2\beta$. Now

$$\begin{cases} s_\beta s_\alpha(\alpha) = s_\beta(-\alpha) = 2\beta - \alpha = \alpha + 2(\beta - \alpha) \\ s_\beta s_\alpha(\beta - \alpha) = s_\beta(\beta - \alpha) = \beta - \alpha, \end{cases}$$

and inductively $(s_\beta s_\alpha)^n(\alpha) = \alpha + 2n(\beta - \alpha)$. But $(s_\beta s_\alpha)^n(\alpha)$ lies in the finite set R by (rd2), and so $\alpha = \beta$. $\qquad\square$

COROLLARY C.32. *Let $r, s \in R^\vee$. If $\langle x, r \rangle = \langle x, s \rangle$ for all $x \in R$, then $r = s$.*

PROOF. Write $r = \alpha^\vee$ and $s = \beta^\vee$. Then the proposition shows that $a = \beta$ and so $\alpha^\vee = \beta^\vee$. $\qquad\square$

PROPOSITION C.33. *Let X be a free $\mathbb{Z}$-module of finite rank, and let R and $R^\vee$ be finite subsets of X and $X^\vee$. There exists at most one map $\alpha \mapsto \alpha^\vee \colon R \to R^\vee \subset X^\vee$ satisfying (rd1) and (rd2).*

PROOF. Let $\alpha \mapsto \alpha^\vee \colon R \to R^\vee$ be a map satisfying (rd1) and (rd2). Let V be the $\mathbb{Q}$-subspace of $X_\mathbb{Q}$ generated by R. Then $V^\vee$ is a quotient of $(X_\mathbb{Q})^\vee$ and $\alpha^\vee$ is determined as an element of $R^\vee$ by its image $\bar{\alpha}^\vee$ in $V^\vee$ (see C.32). But $\bar{\alpha}^\vee$ is the coroot of α in the sense of root systems (C.29), and so $\alpha \mapsto \bar{\alpha}^\vee$ is uniquely determined by (V, R) and α (see C.14). $\qquad\square$

Thus, we could define a root system to be a triple $(X, R, R^\vee)$ such that there exists a map $\alpha \mapsto \alpha^\vee \colon R \to R^\vee \subset X^\vee$ satisfying (rd1), (rd2), and (rd3).

DEFINITION C.34. A root datum $(X, R, \alpha \mapsto \alpha^\vee)$ is **semisimple** if R spans the $\mathbb{Q}$-vector space $X_\mathbb{Q}$.

In this case, $\alpha^\vee$ is the unique element of $(X_\mathbb{Q})^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ and the reflection $x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ maps R into R (C.13). In particular, the map $\alpha \mapsto \alpha^\vee$ (hence $R^\vee$) is uniquely determined by (X, R). We often regard a semisimple root datum as a pair (X, R) such that R spans $X_\mathbb{Q}$ and there exists a map $\alpha \mapsto \alpha^\vee$ satisfying (rd1), (rd2), and (rd3).

PROPOSITION C.35. *If (X, R) is a semisimple root datum, then $(X_\mathbb{Q}, R)$ is a root system with the same map $\alpha \mapsto \alpha^\vee$, and*

$$Q(R) \subset X \subset P(R). \tag{175}$$

Conversely, if (V, R) is a root system, then, for any choice of a lattice X in V satisfying (175), the pair (X, R) is a semisimple root datum.

PROOF. We showed that $(X_\mathbb{Q}, R)$ is a root system in C.29. Also $Q(R) \subset X$ because $R \subset X$, and $X \subset P(R)$ because $R^\vee \subset X^\vee$. Conversely, let (V, R) be a root system, and let X be a lattice between Q and P. If $\alpha \in R$, then $\langle R, \alpha^\vee \rangle \subset \mathbb{Z}$, and so $\alpha^\vee \in X^\vee$. Therefore, we have a well-defined map $\alpha \mapsto \alpha^\vee$ satisfying (rd1) and (rd2). The group of automorphisms of V (hence of X) generated by the s_α acts faithfully on R, and so it is finite. Therefore $(X, R, \alpha \mapsto \alpha^\vee)$ is a root datum (obviously semisimple). □

Thus, to give a semisimple root datum amounts to giving a diagram in the sense of C.27.

DEFINITION C.36. The **rank** (resp. **semisimple rank**) of a root datum $(X, R, R^\vee)$ is the dimension of $X \otimes_\mathbb{Z} \mathbb{Q}$ (resp. $(\mathbb{Z}R) \otimes_\mathbb{Z} \mathbb{Q}$).

e. Duals of root data

Let $(X, R, \alpha \mapsto \alpha^\vee)$ be a root datum. We want to show that $(X^\vee, R^\vee, \alpha^\vee \mapsto \alpha)$ is also a root datum. The most elegant way of doing this is to give a definition that is intrinsically self-dual. The following is the definition of a root datum in SGA 3, XXI, 1.1.1.

DEFINITION C.37. A **root datum (in the sense of SGA 3)** is an ordered quadruple $\mathcal{R} = (X, R, X^\vee, R^\vee)$, where

◇ $X, X^\vee$ are free $\mathbb{Z}$-modules of finite rank in duality by a pairing $\langle\ ,\ \rangle : X \times X^\vee \to \mathbb{Z}$,

◇ $R, R^\vee$ are finite subsets of X and $X^\vee$ in bijection by a correspondence $\alpha \leftrightarrow \alpha^\vee$,

satisfying the following conditions:

RD1 $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in R$;

RD2 $s_\alpha(R) \subset R$ and $s_{\alpha^\vee}(R^\vee) \subset R^\vee$ for all $\alpha \in R$.

Here s_α and $s_{\alpha^\vee}$ are given by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad \text{i.e.,} \quad s_\alpha = \mathrm{id}_X - \alpha \otimes \alpha^\vee$$
$$s_{\alpha^\vee}(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

Thus, in C.37, the condition $s_{\alpha^\vee}(R^\vee) \subset R^\vee$ replaces the condition that $W(\mathcal{R})$ is finite in C.28. Definition C.37 has the merit of being obviously self-dual: $(X, R, X^\vee, R^\vee)$ is a root datum if and only if $(X^\vee, R^\vee, X, R)$ is a root datum.

Recall that the condition $\langle \alpha, \alpha^\vee \rangle = 2$ implies that $s_\alpha(\alpha) = -\alpha$ and $s_\alpha^2 = 1$.

Set

$$\begin{aligned} Q &= Q(R) = \mathbb{Z}R \subset X & Q^\vee &= Q(R^\vee) = \mathbb{Z}R^\vee \subset X^\vee \\ V &= \mathbb{Q} \otimes_\mathbb{Z} Q & V^\vee &= \mathbb{Q} \otimes_\mathbb{Z} Q^\vee \\ X_0 &= \{x \in X \mid \langle x, R^\vee \rangle = 0\}. \end{aligned}$$

By $\mathbb{Z}R$ we mean the $\mathbb{Z}$-submodule of X generated by the $\alpha \in R$.

LEMMA C.38. *For $\alpha \in R$, $x \in X$, and $y \in X^\vee$,*

$$\langle s_\alpha(x), y \rangle = \langle x, s_{\alpha^\vee}(y) \rangle, \tag{176}$$

and so

$$\langle s_\alpha(x), s_{\alpha^\vee}(y) \rangle = \langle x, y \rangle. \tag{177}$$

PROOF. We have

$$\langle s_\alpha(x), y \rangle = \langle x - \langle x, \alpha^\vee \rangle \alpha, y \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle$$
$$\langle x, s_{\alpha^\vee}(y) \rangle = \langle x, y - \langle \alpha, y \rangle \alpha^\vee \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle,$$

which gives the first formula, and the second is obtained from the first by replacing y with $s_{\alpha^\vee}(y)$.   □

The second equality says that $s_{\alpha^\vee}$ is the transpose of s_α – it is often denoted $s_\alpha^\vee$.

Let $(X, R, X^\vee, R^\vee)$ be a root datum in the sense of SGA 3. We define a homomorphism $p \colon X \to X^\vee$,

$$p(x) = \sum_{\alpha \in R} \langle x, \alpha^\vee \rangle \alpha^\vee.$$

LEMMA C.39. *(a) For all $x \in X$,*

$$\langle x, p(x) \rangle = \sum_{\alpha \in R} \langle x, \alpha^\vee \rangle^2 \geq 0, \tag{178}$$

with strict inequality holding if $x \in R$.
   (b) For all $x \in X$ and $w \in W$, $\langle wx, p(wx) \rangle = \langle x, p(x) \rangle$.
   (c) For all $\alpha \in R$,

$$\langle \alpha, p(\alpha) \rangle \alpha^\vee = 2p(\alpha), \quad \text{all } \alpha \in R. \tag{179}$$

PROOF. (a) Certainly, $\langle x, p(x) \rangle = \langle x, \sum \langle x, \alpha^\vee \rangle \alpha^\vee \rangle = \sum \langle x, \alpha^\vee \rangle^2$, which is a sum of squares of integers. If $x \in R$, then at least one term is nonzero.

(b) It suffices to check this for $w = s_\alpha$, but

$$\langle s_\alpha x, \alpha^\vee \rangle = \langle x, \alpha^\vee \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, \alpha^\vee \rangle = -\langle x, \alpha^\vee \rangle$$

and so each term on the right of (178) is unchanged if x is replaced with $s_\alpha x$.

(c) Recall that, for $y \in X^\vee$,

$$s_{\alpha^\vee}(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

On multiplying this by $\langle \alpha, y \rangle$ and re-arranging, we find that

$$\langle \alpha, y \rangle^2 \alpha^\vee = \langle \alpha, y \rangle y - \langle \alpha, y \rangle s_{\alpha^\vee}(y).$$

But

$$-\langle \alpha, y \rangle = \langle s_\alpha(\alpha), y \rangle \overset{(176)}{=} \langle \alpha, s_{\alpha^\vee}(y) \rangle$$

and so

$$\langle \alpha, y \rangle^2 \alpha^\vee = \langle \alpha, y \rangle y + \langle \alpha, s_{\alpha^\vee}(y) \rangle s_{\alpha^\vee}(y),$$

which we rewrite as

$$\langle \alpha, \beta^\vee \rangle^2 \alpha^\vee = \langle \alpha, \beta^\vee \rangle \beta^\vee + \langle \alpha, s_{\alpha^\vee}(\beta^\vee) \rangle s_{\alpha^\vee}(\beta^\vee).$$

As β runs over R, both $\beta^\vee$ and $s_{\alpha^\vee}(\beta^\vee)$ run over $R^\vee$, and so when we sum we obtain (179). □

REMARK C.40. Suppose $m\alpha$ is also a root. On replacing α with $m\alpha$ in (179) and using that p is a homomorphism of $\mathbb{Z}$-modules, we find that

$$m \langle \alpha, p(\alpha) \rangle (m\alpha)^\vee = 2p(\alpha), \quad \text{all } \alpha \in R.$$

Therefore,

$$(m\alpha)^\vee = m^{-1} \alpha^\vee.$$

In particular,

$$(-\alpha)^\vee = -(\alpha^\vee).$$

LEMMA C.41. *The map* $p \colon X \to X^\vee$ *defines an isomorphism*

$$1 \otimes p \colon V \to V^\vee.$$

In particular, $\dim V = \dim V^\vee$.

PROOF. When $\alpha \in R$, (178) shows that $\langle \alpha, p(\alpha) \rangle \neq 0$, and now (179) shows that $p(Q)$ has finite index in $Q^\vee$. Therefore, when we tensor $p \colon Q \to Q^\vee$ with $\mathbb{Q}$, we get a surjective map $1 \otimes p \colon V \to V^\vee$; in particular, $\dim V \geq \dim V^\vee$. From the symmetry between (X, R) and $(X^\vee, R^\vee)$, we deduce that $\dim V^\vee \leq \dim V$, and hence that $\dim V = \dim V^\vee$. Therefore $1 \otimes p \colon V \to V^\vee$ is an isomorphism. □

LEMMA C.42. *The kernel of $p: X \to X^\vee$ is X_0.*

PROOF. Clearly, $X_0 \subset \mathrm{Ker}(p)$, but if $x \notin X_0$, then (178) shows that $p(x) \neq 0$. $\square$

PROPOSITION C.43. *The intersection $Q \cap X_0$ is zero and the sum $Q + X_0$ has finite index in X. Therefore, there is an exact sequence*

$$0 \to Q \oplus X_0 \xrightarrow{(q,x) \mapsto q+x} X \to \text{finite group} \to 0.$$

PROOF. The map

$$1 \otimes p: \mathbb{Q} \otimes X \to V^\vee$$

has kernel $\mathbb{Q} \otimes X_0$ by (C.42), and it sends the subspace V of $\mathbb{Q} \otimes X$ isomorphically onto $V^\vee$ by (C.41). Therefore

$$(\mathbb{Q} \otimes X_0) \oplus V \simeq \mathbb{Q} \otimes X,$$

from which the proposition follows. $\square$

A root datum $(X, R, \alpha \mapsto \alpha^\vee)$ is ***toral*** if $R = \emptyset$. The proposition shows that every root datum is "isogenous" to a direct sum of a toral root datum and a semisimple root datum.

LEMMA C.44. *The form $\langle \, , \, \rangle$ defines a nondegenerate pairing $V \times V^\vee \to \mathbb{Q}$.*

PROOF. Let $x \in X$. If $\langle x, \alpha^\vee \rangle = 0$ for all $a^\vee \in R^\vee$, then $x \in \mathrm{Ker}(p) = X_0$. As its left kernel is zero and the spaces have the same dimension, the pairing is nondegenerate. $\square$

The ***Weyl group*** $W = W(R)$ of $\mathcal{R} = (X, R, X^\vee, R^\vee)$ is defined to be the subgroup of $\mathrm{Aut}(X)$ generated by the s_α for $\alpha \in R$.

LEMMA C.45. *For every $x \in X$ and $w \in W$, $w(x) - x \in Q$.*

PROOF. For $\alpha \in R$,

$$s_\alpha(x) - x = -\langle x, \alpha^\vee \rangle \alpha \in Q.$$

Now, for $\alpha_1, \alpha_2 \in R$,

$$(s_{\alpha_1} \circ s_{\alpha_2})(x) - x = s_{\alpha_1}(s_{\alpha_2}(x) - x) + s_{\alpha_1}(x) - x \in Q.$$

Continue in this fashion. $\square$

We let $w \in W$ act on $X^\vee$ as $(w^\vee)^{-1}$, i.e., so that

$$\langle wx, wy \rangle = \langle x, y \rangle, \quad \text{all } w \in W, x \in X, y \in X^\vee.$$

Note that this makes s_α act on $X^\vee$ as $(s_{\alpha^\vee})^{-1} = s_{\alpha^\vee}$ (see 176).

PROPOSITION C.46. *The Weyl group W acts faithfully on R (and so is finite).*

PROOF. By symmetry, it is equivalent to show that W acts faithfully on $R^\vee$. Let w be an element of W such that $w(\alpha) = \alpha$ for all $\alpha \in R^\vee$. For $x \in X$,

$$\langle w(x) - x, \alpha^\vee \rangle = \langle w(x), \alpha^\vee \rangle - \langle x, \alpha^\vee \rangle = \langle x, w^{-1}(\alpha^\vee) \rangle - \langle x, \alpha^\vee \rangle = 0.$$

Thus $w(x) - x$ is orthogonal to $R^\vee$. As it lies in Q (see C.45), this implies that it is zero (C.44), and so $w = 1$.   □

Thus, if $(X, R, X^\vee, R^\vee)$ is a root datum in the sense of SGA 3, then the triple $(X, R, \alpha \mapsto \alpha^\vee)$ is a root datum in the sense of C.28. The next proposition proves the converse.

PROPOSITION C.47. *Let $(X, R, f : \alpha \mapsto \alpha^\vee)$ be a triple satisfying the conditions (rd1), (rd2), and (rd3) of C.28; let $X^\vee = \mathrm{Hom}(X, \mathbb{Z})$, and let $R^\vee = f(R)$; then the quadruple $(X, R, X^\vee, R^\vee)$ equipped with the natural pairing $X \times X^\vee \to \mathbb{Z}$ and the bijection $\alpha \leftrightarrow f(\alpha)$ is a root system in the sense of SGA 3 (C.37).*

PROOF. We have to show that $s_{\alpha^\vee}(R^\vee) \subset R^\vee$. Because $s_{\alpha^\vee}$ is the transpose s_α^t of s_α (see C.38), it suffices to show that $s_\alpha^t(R^\vee) \subset R^\vee$.

Let $\alpha, \beta \in R$. Then $s_\alpha s_\beta s_\alpha$ and $s_{s_\alpha(\beta)}$ are involutions in the group generated by s_α; let t be their composite $t = s_{s_\alpha(\beta)} \circ s_\alpha s_\beta s_\alpha$. A direct calculation (cf. Springer 1979, 1.4) shows that

$$t(x) = x + (\langle x, s_\alpha^t(\beta^\vee) \rangle - \langle x, s_\alpha(\beta)^\vee \rangle) s_\alpha(\beta), \quad \text{all } x \in X.$$

As

$$\langle s_\alpha(\beta), s_\alpha^t(\beta^\vee) \rangle - \langle s_\alpha(\beta), s_\alpha(\beta)^\vee \rangle = \langle \beta, \beta^\vee \rangle - \langle s_\alpha(\beta), s_\alpha(\beta)^\vee \rangle = 2 - 2 = 0,$$

we see that t is unipotent. On the other hand, as t lies in a finite group, it has finite order, say $t^m = 1$, and it follows that t is the identity map (see the proof of C.3). Hence

$$\langle x, s_\alpha^t(\beta^\vee) \rangle - \langle x, s_\alpha(\beta)^\vee \rangle = 0 \text{ for all } x \in X,$$

and so

$$s_\alpha^t(\beta^\vee) = s_\alpha(\beta)^\vee \in R^\vee.$$ □

We conclude that to give a root system in the sense of SGA 3 (C.37) amounts to giving a root system in the sense of C.28.

COROLLARY C.48. *If $(X, R, \alpha \mapsto \alpha^\vee)$ satisfies the axioms (rd1), (rd2), and (rd3) for a root system, then so does $(X^\vee, R^\vee, \alpha^\vee \mapsto \alpha)$.*

PROOF. If $(X, R, \alpha \mapsto \alpha^\vee)$ satisfies (rd1), (rd2), and (rd3), then $(X, R, X^\vee, R^\vee)$ satisfies (RD1) and (RD2). As these axioms are self-dual, $(X^\vee, R^\vee, X, R)$ satisfies (RD1) and (RD2), and so $(X^\vee, R^\vee, \alpha^\vee \mapsto \alpha)$ satisfies (rd1), (rd2), and (rd3).   □

COROLLARY C.49. *Let* $(X, R, \alpha \mapsto \alpha^\vee)$ *be a root system, and let* $\alpha, \beta \in R$. *Then*

$$s_\alpha(\beta)^\vee = s_{\alpha^\vee}(\beta^\vee).$$

PROOF. As s_α and $s_{\alpha^\vee}$ are adjoint (C.38) and preserve R and $R^\vee$, by the uniqueness (C.33), they must intertwine the bijection $\beta \mapsto \beta^\vee$ with itself.   □

EXERCISE C.50. Let X be a free $\mathbb{Z}$-module of finite rank, and let R and $R^\vee$ be finite subsets of X and $X^\vee$. Show that $(X, R, X^\vee, R^\vee)$ is a root datum if and only if it satisfies the following conditions:

(a) R and $R^\vee$ are root systems in $\mathbb{Q}R \overset{\text{def}}{=} (\mathbb{Z}R) \otimes \mathbb{Q}$ and $\mathbb{Q}R^\vee \overset{\text{def}}{=} (\mathbb{Z}R^\vee) \otimes \mathbb{Q}$.

(b) there exists a one-to-one correspondence $\alpha \leftrightarrow \alpha^\vee \colon R \leftrightarrow R^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ and the reflections s_α and $s_{\alpha^\vee}$ of the root systems $(\mathbb{Q}R, R)$ and $(\mathbb{Q}R^\vee, R^\vee)$ are

$$x \mapsto x - \langle x, \alpha^\vee \rangle \alpha, \quad x \in \mathbb{Q}R$$
$$y \mapsto y - \langle \alpha, y \rangle \alpha^\vee, \quad y \in \mathbb{Q}R^\vee.$$

(This is essentially the definition in Malle and Testerman 2011, 9.10.)

NOTES. The original source for root data is SGA 3, XXI. The observation that the axiom (RD2) can be replaced by the axioms (rd2) and (rd3) is from Springer 1979, §1. Proposition C.33 is due to Gabber (Conrad et al. 2015, 3.2.4).

f. Deconstructing root data

C.51. Let $(X, R, R^\vee)$ be a root datum. Let $X_0 = \{x \in X \mid \langle x, R^\vee \rangle = 0\}$ as before, and let $X' = X/X_0$. The quotient map $X \to X'$ is injective on Q (see C.43), and we let R' denote the image of R in X'. Then (X', R') is a semisimple root datum, and $(X'_\mathbb{Q}, R')$ is a root system (C.35). We now explain how to construct a root datum from a root system and a homomorphism of $\mathbb{Z}$-modules. Every root datum arises in this way, and so this essentially reduces the problem of classifying the root data to that of classifying root systems.

Let (V, R) be a root system, let Y be a finitely generated $\mathbb{Z}$-module, and let $\varphi \colon Y \to P(R)/Q(R)$ be a homomorphism whose kernel X is torsion-free. Define $X(\varphi)$ to be the kernel of the map

$$(p, y) \mapsto \bar{p} - \varphi(y) \colon P(R) \oplus Y \to P(R)/Q(R).$$

Then $X(\varphi)$ is a free $\mathbb{Z}$-module of finite rank, and it contains the submodule $Q(R) \oplus 0$ of $P(R) \oplus Y$. Let $R(\varphi)$ denote R regarded as a subset of $X(\varphi)$. Then $(X(\varphi), R(\varphi))$ is a root datum with associated root system (V, R); moreover, $X(\varphi)/Q(R(\varphi)) \simeq Y$.

g.   Classification of reduced root systems

As every root system is uniquely a direct sum of indecomposable systems (C.23), we need only classify the latter. We choose an invariant inner product (C.19). For an indecomposable root system, this is uniquely determined up to scalar multiplication, and so the ratio of the lengths of two vectors is independent of the choice of the inner product.

The (reduced) 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.

Root systems of rank 2

Assume $F = \mathbb{R}$. 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 assume that β is not a multiple of α, there are only the following possibilities (in the table, we have chosen β to be the longer root):

$n(\beta,\alpha)\cdot n(\alpha,\beta)$	$n(\alpha,\beta)$	$n(\beta,\alpha)$	ϕ	$\|\beta\|/\|\alpha\|$
0	0	0	$\pi/2$	
1	1	1	$\pi/3$	1
	-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	$5\pi/6$	

(180)

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 a glance at the table shows that one of the numbers, say, $n(\alpha, \beta)$, equals 1. Then

$$s_\beta(\alpha) = \alpha - n(\alpha, \beta)\beta = \alpha - \beta,$$

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 from the table 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.
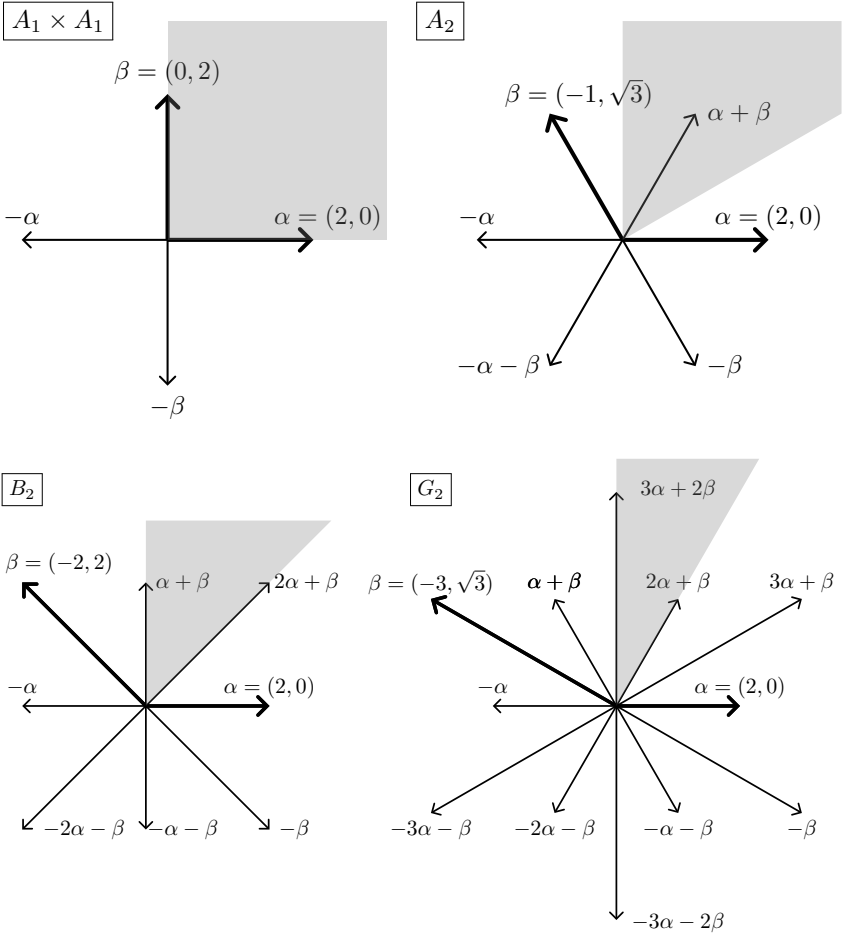
Note that each set of vectors does satisfy (RS1), (RS2), and (RS3). The root system $A_1 \times A_1$ is decomposable and the remainder are indecomposable. We have

	$A_1 \times A_1$	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 product as in (C.19). From the second expression, we see that $n(w\alpha, w\beta) = n(\alpha, \beta)$ for all $w \in W$.

Let S be a base for R. The **Cartan matrix** of R (relative to S) is the matrix $(n(\alpha, \beta))_{\alpha, \beta \in S}$. Its diagonal entries $n(\alpha, \alpha)$ equal 2, and the remaining entries are negative or zero.

For example, the Cartan matrices of the root systems of rank 2 are

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \quad \begin{pmatrix} 2 & -1 \\ -2 & 2 \end{pmatrix} \quad \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$
$$A_1 \times A_1 \qquad\quad A_2 \qquad\qquad B_2 \qquad\qquad G_2$$

and the Cartan matrix for the root system in (C.16, C.25) 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 C.52. *The Cartan matrix of (V, R) is independent of S, and determines (V, R) up to isomorphism.*

PROOF. If S' is a second base for R, then we know that $S' = wS$ for a *unique* $w \in W$ (see C.22) and that $n(w\alpha, w\beta) = n(\alpha, \beta)$. Thus S and S' give the same Cartan matrices up to the naming of the index sets. Let (V', R') be a second root system with the same Cartan matrix. This means that there exists a base S' for R' and a bijection $\alpha \mapsto \alpha' : S \to S'$ such that

$$n(\alpha, \beta) = n(\alpha', \beta') \text{ for all } \alpha, \beta \in S. \tag{181}$$

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 (181). But by definition the s_α generate the Weyl groups, and so the isomorphism maps W onto W', and hence it maps $R = W \cdot S$ onto $R' = W' \cdot S'$ (see C.22). We have shown that the bijection $S \to S'$ extends uniquely to an isomorphism $(V, R) \to (V', R')$ of root systems.□

The automorphisms of R

Let $A(R)$ denote the group of linear automorphisms of V leaving R stable. It is a finite group containing the Weyl group $W(R)$ as a normal subgroup (because $t s_\alpha t^{-1} = s_{t(\alpha)}$ if $t \in A(R)$ and $\alpha \in R$).

PROPOSITION C.53. *Let S be a base for R, and let D be the group of elements of $A(R)$ leaving S stable. Then $A(R) = W(R) \rtimes D$.*

PROOF. If $a \in A(R)$, then $a(S)$ is a base for R, and so $a(S) = w(S)$ for a unique $w \in W(R)$ (see C.22). Now $a = wd$ with $d \in D$, and this expression for a is unique.   □

Let S be a base for R. The last sentence in the proof of (C.52) allows us to identify D with the set of permutations of S leaving the Cartan matrix invariant.

In the next section we attach a (Dynkin) diagram to (V, R, S) whose nodes correspond to the elements of S and whose automorphisms correspond to the elements of D. For this reason, the elements of D are called the **graph automorphisms** of R. From the Dynkin diagrams displayed below, we see that D is trivial when (V, R) is indecomposable of type A_1, B_n, C_n, G_2, F_4, E_7, or E_8. It has order 2 for types A_n ($n \geq 2$), D_n ($n \geq 5$), and E_6, and it is a permutation group on three symbols for type D_4.

Classification of root systems by Dynkin diagrams

Let (V, R) be a root system, and let S be a base for R.

PROPOSITION C.54. *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

PROOF. 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 this can be read off from the table (180), p. 621.□

Choose a base S for R. Then the **Coxeter graph** of (V, R) is the graph whose nodes are indexed by the elements of S; two distinct nodes are joined by $n(\alpha, \beta) \cdot n(\beta, \alpha)$ edges. Up to the indexing of the nodes, it is independent of the choice of S.

PROPOSITION C.55. *The Coxeter graph is connected if and only if the root system is indecomposable.*

In other words, the decomposition of the Coxeter graph of (V, R) into its connected components corresponds to the decomposition of (V, R) into a direct sum of its indecomposable summands.

PROOF. A root system is decomposable if and only if R can be written as a disjoint union $R = R_1 \sqcup R_2$ with each root in R_1 orthogonal to each root in R_2. Since roots α, β are orthogonal if and only if $n(\alpha, \beta) \cdot n(\beta, \alpha) = 4\cos^2 \phi = 0$, this is equivalent to the Coxeter graph being disconnected. □

The Coxeter graph does not determine the Cartan matrix because it just 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 inequality sign $<$ on the lines joining the nodes indexed by α and β pointing towards the shorter root. The resulting diagram is called the **Dynkin diagram** of the root system. It determines the Cartan matrix and hence the root system.

For example, the Dynkin diagrams of the root systems of rank 2 are
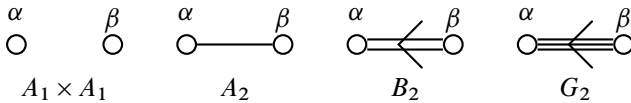
THEOREM C.56. *The Dynkin diagrams arising from indecomposable root systems are exactly the diagrams A_n $(n \geq 1)$, B_n $(n \geq 2)$, C_n $(n \geq 3)$, D_n $(n \geq 4)$, E_6, E_7, E_8, F_4, G_2 displayed below (p. 626).*

For example, the Dynkin diagram of the root system in (C.16) is A_n. Note that Coxeter graphs do not distinguish B_n from C_n. We have used the conventional (Bourbaki) numbering for the simple roots.

A Dynkin diagram is **simply laced** if it has no multiple edges. This means that the simple roots in the corresponding indecomposable root system all have the same length (see table (180), p. 621). The simply laced Dynkin diagrams are A_n $(n \geq 1)$, D_n $(n \geq 4)$, and E_n $(6 \leq n \leq 8)$.

Indecomposable Dynkin diagrams

A_n

$$\underset{\alpha_1}{\circ}\!\!-\!\!\underset{\alpha_2}{\circ}\!\!-\!\!\underset{\alpha_3}{\circ}\ \text{-----}\ \underset{\alpha_{n-2}}{\circ}\!\!-\!\!\underset{\alpha_{n-1}}{\circ}\!\!-\!\!\underset{\alpha_n}{\circ}$$

$(n \geq 1)$

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
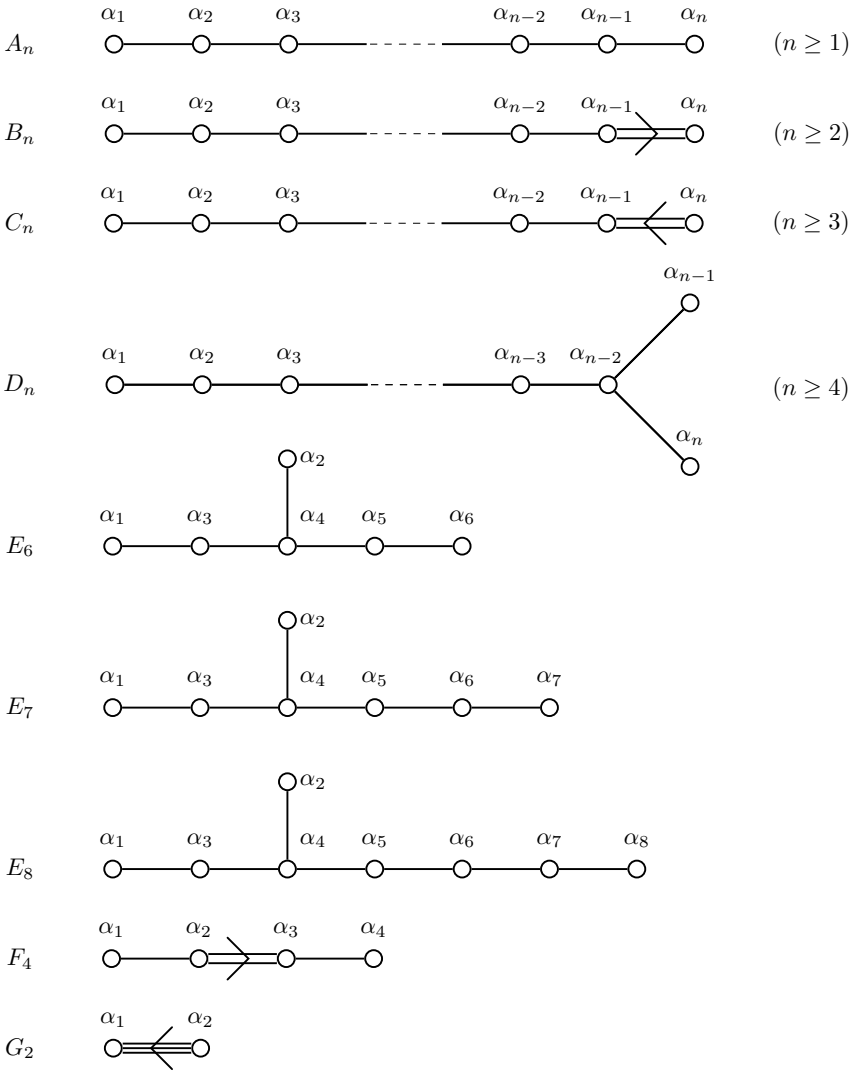
References

ADAMS, J. 2013. Galois cohomology of real groups. arXiv:1310.7917.

ADAMS, J. F. 1969. *Lectures on Lie groups*. W. A. Benjamin, Inc., New York and Amsterdam.

ALLCOCK, D. 2009. A new approach to rank one linear algebraic groups. *J. Algebra* 321:2540–2544.

BALAJI, V., DELIGNE, P., AND PARAMESWARAN, A. J. 2016. On complete reducibility in characteristic p. arXiv:1607.08564.

BARSOTTI, I. 1953. A note on abelian varieties. *Rend. Circ. Mat. Palermo (2)* 2:236–257.

BARSOTTI, I. 1955. Un teorema di struttura per le varietà gruppali. *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat. (8)* 18:43–50.

BATE, M., MARTIN, B., RÖHRLE, G., AND TANGE, R. 2010. Complete reducibility and separability. *Trans. Amer. Math. Soc.* 362:4283–4311.

BERGMAN, G. M. 1978. The diamond lemma for ring theory. *Adv. in Math.* 29:178–218.

BERRICK, A. J. AND KEATING, M. E. 2000. *An introduction to rings and modules with K-theory in view*. Cambridge Studies in Advanced Mathematics, Vol. 65. Cambridge University Press, Cambridge.

BIAŁYNICKI-BIRULA, A. 1973. Some theorems on actions of algebraic groups. *Ann. of Math. (2)* 98:480–497.

BIAŁYNICKI-BIRULA, A. 1976. Some properties of the decompositions of algebraic varieties determined by actions of a torus. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* 24:667–674.

BIRKHOFF, G. 1937. Representability of Lie algebras and Lie groups by matrices. *Ann. of Math. (2)* 38:526–532.

BOREL, A. 1956. Groupes linéaires algébriques. *Ann. of Math. (2)* 64:20–82.

BOREL, A. 1970. Properties and linear representations of Chevalley groups, pp. 1–55. In *Seminar on Algebraic Groups and Related Finite Groups* (The Institute for Advanced Study, Princeton, NJ, 1968/69), Lecture Notes in Mathematics, Vol. 131. Springer-Verlag, Berlin.

BOREL, A. 1975. Linear representations of semi-simple algebraic groups, pp. 421–440. In *Algebraic geometry* (Proceedings of Symposia in Pure Mathematics, Vol. 29, Humboldt State University, Arcata, Calif., 1974). American Mathematical Society, Providence, RI.

BOREL, A. 1985. On affine algebraic homogeneous spaces. *Arch. Math. (Basel)* 45:74–78.

BOREL, A. 1991. *Linear algebraic groups*. Graduate Texts in Mathematics, Vol. 126. Springer-Verlag, Berlin.

BOREL, A. AND HARDER, G. 1978. Existence of discrete cocompact subgroups of reductive groups over local fields. *J. Reine Angew. Math.* 298:53–64.

BOREL, A. AND SPRINGER, T. A. 1966. Rationality properties of linear algebraic groups, pp. 26–32. In *Algebraic Groups and Discontinuous Subgroups* (Proceedings of Symposia in Pure Mathematics, Boulder, CO, 1965). American Mathematical Society, Providence, RI.

BOREL, A. AND SPRINGER, T. A. 1968. Rationality properties of linear algebraic groups. II. *Tôhoku Math. J. (2)* 20:443–497.

BOREL, A. AND TITS, J. 1965. Groupes réductifs. Inst. Hautes Études Sci. Publ. Math. 27:55–150.

BOREL, A. AND TITS, J. 1972. Compléments à l'article: "Groupes réductifs". Inst. Hautes Études Sci. Publ. Math. 41:253–276.

BOREL, A. AND TITS, J. 1978. Théorèmes de structure et de conjugaison pour les groupes algébriques linéaires. *C. R. Acad. Sci. Paris Sér. A-B* 287:A55–A57.

BOROVOI, M. 2014. Galois cohomology of reductive algebraic groups over the field of real numbers. arXiv:1401.5913.

BOROVOI, M. AND TIMASHEV, D. A. 2015. Galois cohomology of real semisimple groups. arXiv:1506.06252.

BOSCH, S., LÜTKEBOHMERT, W., AND RAYNAUD, M. 1990. *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Vol. 21. Springer-Verlag, Berlin.

BOURBAKI, N. 1958. *Algèbre. Chapitre 8: Modules et anneaux semi-simples*. Hermann, Paris.

BOURBAKI, N. 1968. *Groupes et algèbres de Lie. Chapitres 4, 5 et 6*. Hermann, Paris.

BOURBAKI, N. 1972. *Groupes et algèbres de Lie. Chapitres 2 et 3*. Hermann, Paris.

BOURBAKI, N. 1975. *Groupes et algèbres de Lie. Chapitres 7 et 8*. Hermann, Paris.

BRION, M. 2009. Anti-affine algebraic groups. *J. Algebra* 321:934–952.

BRION, M. 2015a. On extensions of algebraic groups with finite quotient. *Pacific J. Math.* 279:135–153.

BRION, M. 2015b. Some structure theorems for algebraic groups. arXiv:1509.03059.

BRION, M. 2016. Epimorphic subgroups of algebraic groups. arXiv:1605.07769.

BRION, M., SAMUEL, P., AND UMA, V. 2013. *Lectures on the structure of algebraic groups and geometric applications*. CMI Lecture Series in Mathematics, Vol 1. Hindustan Book Agency, New Delhi.

BROCHARD, S. 2014. Topologies de Grothendieck, descente, quotients, pp. 1–62. In *Autour des schémas en groupes Vol. I*, Panoramas et Synthèses, Vol. 42/43. Société Mathématique de France, Paris.

BROSNAN, P. 2005. On motivic decompositions arising from the method of Białynicki-Birula. Invent. Math. 161:91–111.

BRUHAT, F. AND TITS, J. 1987. Groupes algébriques sur un corps local. Chapitre III. Compléments et applications à la cohomologie galoisienne. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 34:671–698.

CARTIER, P. 1962. Groupes algébriques et groupes formels, pp. 87–111. In *Colloque sur la Théorie des Groupes Algébriques* (Bruxelles, 1962). Librairie Universitaire, Louvain.

CARTIER, P. 2005. Sur les problèmes de classification des groups, pp. 266–274. In *Classification des groupes algébriques semi-simples* (Collected works, Vol. 3). Springer-Verlag, Berlin.

CASSELMAN, B. 2015. On Chevalley's formula for structure constants. *J. Lie Theory* 25:431–441.

CAYLEY, A. 1846. Sur quelques propriétés des déterminants gauches. *J. Reine Angew. Math.* 32:119–123.

CHERNOUSOV, V. I. 1989. The Hasse principle for groups of type E_8. *Dokl. Akad. Nauk SSSR* 306:1059–1063.

CHEVALLEY, C. C. 1955a. Sur certains groupes simples. *Tôhoku Math. J. (2)* 7:14–66.

CHEVALLEY, C. C. 1955b. *Théorie des groupes de Lie. Tome III. Théorèmes généraux sur les algèbres de Lie.* Actualités Scientifiques et Industrielles no. 1226. Hermann, Paris.

CHEVALLEY, C. C. 1956–58. *Classification des groupes de Lie algébriques, Seminaire ENS, Paris.* mimeographed. Reprinted by Springer-Verlag, Berlin, 2005.

CHEVALLEY, C. C. 1960. Une démonstration d'un théorème sur les groupes algébriques. *J. Math. Pures Appl. (9)* 39:307–317.

CHEVALLEY, C. C. 1961. Certains schémas de groupes semi-simples, pp. 219–234. In *Séminaire Bourbaki, Vol. 6* Exp. No. 219. Société Mathématique de France, Paris.

CONRAD, B. 2014. Reductive group schemes, pp. 93–444. In *Autour des schémas en groupes. Vol. I*, Panoramas et Synthèses, Vol. 42/43. Société Mathématique de France, Paris.

CONRAD, B., GABBER, O., AND PRASAD, G. 2015. *Pseudo-reductive groups*. New Mathematical Monographs, Vol. 26. Cambridge University Press, Cambridge, second edition.

DE GRAAF, W. A. 2007. Classification of 6-dimensional nilpotent Lie algebras over fields of characteristic not 2. *J. Algebra* 309:640–653.

DELIGNE, P. 1990. Catégories tannakiennes, pp. 111–195. In *The Grothendieck Festschrift, Vol. II*, Progress in Mathematics. Birkhäuser Boston, Boston, MA.

DELIGNE, P. 2014. Semi-simplicité de produits tensoriels en caractéristique p. *Invent. Math.* 197:587–611.

DELIGNE, P. AND LUSZTIG, G. 1976. Representations of reductive groups over finite fields. *Ann. of Math. (2)* 103:103–161.

DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. In *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, Vol. 900. Springer-Verlag, Berlin.

DEMAZURE, M. 1965. Schémas en groupes réductifs. *Bull. Soc. Math. France* 93:369–413.

DEMAZURE, M. 1972. *Lectures on p-divisible groups*. Lecture Notes in Mathematics, Vol. 302. Springer-Verlag, Berlin.

DEMAZURE, M. AND GABRIEL, P. 1966. *Séminaire Heidelberg–Strasbourg 1965–66 (Groupes Algébriques)*. Multigraphié par l'Institut de Mathématique de Strasbourg, 406 pages. Cited as SHS.

DEMAZURE, M. AND GABRIEL, P. 1970. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson, Paris. Cited as DG.

DEMAZURE, M. AND GROTHENDIECK, A. 1964. *Schémas en groupes (SGA 3). Séminaire de Géométrie Algébrique du Bois Marie 1962–64*. Dirigé par M. Demazure et A. Grothendieck. Multigraphié par I.H.E.S; reprinted by Springer-Verlag, Berlin: Lecture Notes in Mathematics, Vols 151, 152, 153 (1970).

DEMAZURE, M. AND GROTHENDIECK, A. 2011. *Schémas en groupes (SGA 3). Séminaire de Géométrie Algébrique du Bois Marie 1962–64*. Dirigé par M. Demazure et A. Grothendieck. Documents Mathématiques, Vol. 7,8. Société Mathématique de France, Paris. Revised edition of Demazure and Grothendieck 1964. Annotated and edited by Gille, P., and Polo, P.. Cited as SGA 3.

DOKOVIĆ, D. Ž. 1988. An elementary proof of the structure theorem for connected solvable affine algebraic groups. *Enseign. Math. (2)* 34:269–273.

FOGARTY, J. 1973. Fixed point schemes. *Amer. J. Math.* 95:35–51.

FOGARTY, J. AND NORMAN, P. 1977. A fixed-point characterization of linearly reductive groups, pp. 151–155. In *Contributions to algebra* (collection of papers dedicated to Ellis Kolchin). Academic Press, New York.

FOSSUM, R. AND IVERSEN, B. 1973. On Picard groups of algebraic fibre spaces. *J. Pure Appl. Algebra* 3:269–280.

GARIBALDI, R. S. 1998. Isotropic trialitarian algebraic groups. *J. Algebra* 210:385–418.

GARIBALDI, R. S. 2001. Groups of type E_7 over arbitrary fields. *Comm. Algebra* 29:2689–2710.

GARIBALDI, S. 2016. E_8, the most exceptional group. *Bull. Amer. Math. Soc. (N.S.)* 53:643–671.

GECK, M. 2016. On the construction of semisimple Lie algebras and Chevalley groups. arXiv:1602.04583.

GROTHENDIECK, A. 1967. Eléments de géométrie algébrique. *Publ. Math. IHES* 4, 8, 11, 17, 20, 24, 28, 32. (1960–67) En collaboration avec J. Dieudonné. Cited as EGA.

GROTHENDIECK, A. 1972. *Groupes de monodromie en géométrie algébrique. I*. Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I).

HARDER, G. 1965. Über einen Satz von E. Cartan. *Abh. Math. Sem. Univ. Hamburg* 28:208–214.

HARDER, G. 1966. Über die Galoiskohomologie halbeinfacher Matrizengruppen. II. *Math. Z.* 92:396–415.

HARDER, G. 1975. Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. III. *J. Reine Angew. Math.* 274/275:125–138.

HAREBOV, A. AND VAVILOV, N. 1996. On the lattice of subgroups of Chevalley groups containing a split maximal torus. *Comm. Algebra* 24:109–133.

HARTSHORNE, R. 1977. *Algebraic geometry*. Graduate Texts in Mathematics, Vol. 52. Springer-Verlag, Berlin.

HERPEL, S. 2013. On the smoothness of centralizers in reductive groups. *Trans. Amer. Math. Soc.* 365:3753–3774.

HESSELINK, W. H. 1981. Concentration under actions of algebraic groups, pp. 55–89. In *Paul Dubreil and Marie-Paule Malliavin Algebra Seminar, 33rd Year* (Paris, 1980), Lecture Notes in Mathematics, Vol. 867. Springer-Verlag, Berlin.

HOCHSCHILD, G. P. 1981. *Basic theory of algebraic groups and Lie algebras*. Graduate Texts in Mathematics, Vol. 75. Springer-Verlag, Berlin.

HUMPHREYS, J. E. 1972. *Introduction to Lie algebras and representation theory*. Graduate Texts in Mathematics, Vol. 9. Springer-Verlag, Berlin.

HUMPHREYS, J. E. 1975. *Linear algebraic groups*. Graduate Texts in Mathematics, No. 21. Springer-Verlag, Berlin.

HUMPHREYS, J. E. 1990. *Reflection groups and Coxeter groups*. Cambridge Studies in Advanced Mathematics, Vol. 29. Cambridge University Press, Cambridge.

HUMPHREYS, J. E. 1995. *Conjugacy classes in semisimple algebraic groups*. Mathematical Surveys and Monographs, Vol. 43. American Mathematical Society, Providence, RI.

IVERSEN, B. 1972. A fixed point formula for action of tori on algebraic varieties. Invent. Math. 16:229–236.

IVERSEN, B. 1976. The geometry of algebraic groups. *Advances in Math.* 20:57–85.

JACOBSON, N. 1962. *Lie algebras*. Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers, Inc., New York and London. Reprinted by Dover, New York, 1979.

JACOBSON, N. 1985. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition.

JACOBSON, N. 1989. *Basic algebra. II*. W. H. Freeman and Company, New York, second edition.

JANTZEN, J. C. 1997. Low-dimensional representations of reductive groups are semisimple, pp. 255–266. In *Algebraic groups and Lie groups*, Australian Mathematical Society Lecture Series., Vol. 9. Cambridge University Press, Cambridge.

JANTZEN, J. C. 2003. *Representations of algebraic groups*. Mathematical Surveys and Monographs, Vol. 107. American Mathematical Society, Providence, RI, second edition.

KAMBAYASHI, T., MIYANISHI, M., AND TAKEUCHI, M. 1974. *Unipotent algebraic groups*. Lecture Notes in Mathematics, Vol. 414. Springer-Verlag, Berlin.

KAMBAYASHI, T. AND RUSSELL, P. 1982. On linearizing algebraic torus actions. *J. Pure Appl. Algebra* 23:243–250.

KEMPF, G. R. 1976. Linear systems on homogeneous spaces. *Ann. of Math. (2)* 103:557–591.

KNESER, M. 1969. *Lectures on Galois cohomology of classical groups*. Tata Institute of Fundamental Research, Bombay.

KNUS, M.-A., MERKURJEV, A., ROST, M., AND TIGNOL, J.-P. 1998. *The book of involutions*. American Mathematical Society Colloquium Publications, Vol. 44. American Mathematical Society, Providence, RI.

KOHLS, M. 2011. A user friendly proof of Nagata's characterization of linearly reductive groups in positive characteristics. *Linear Multilinear Algebra* 59:271–278.

KOLCHIN, E. R. 1948. Algebraic matric groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations. *Ann. of Math. (2)* 49:1–42.

KOSTANT, B. 1966. Groups over *Z*, pp. 90–98. In *Algebraic Groups and Discontinuous Subgroups* (Proceedings of Symposia in Pure Mathematics, Vol. 9, Boulder, CO, 1965). American Mathematical Society, Providence, RI.

LANG, S. 1956. Algebraic groups over finite fields. *Amer. J. Math.* 78:555–563.

LANG, S. 2002. *Algebra.* Graduate Texts in Mathematics, Vol. 211. Springer-Verlag, Berlin.

LAZARD, M. 1955. Sur les groupes de Lie formels à un paramètre. *Bull. Soc. Math. France* 83:251–274.

LEMIRE, N., POPOV, V. L., AND REICHSTEIN, Z. 2006. Cayley groups. *J. Amer. Math. Soc.* 19:921–967.

LUNA, D. 1999. Retour sur un théorème de Chevalley. *Enseign. Math. (2)* 45:317–320.

LUSZTIG, G. 2009. Study of a **Z**-form of the coordinate ring of a reductive group. *J. Amer. Math. Soc.* 22:739–769.

MAC LANE, S. 1969. One universe as a foundation for category theory, pp. 192–200. In *Reports of the Midwest Category Seminar. III*, Lecture Notes in Mathematics, Vol. 195. Springer-Verlag, Berlin.

MAC LANE, S. 1971. *Categories for the working mathematician.* Graduate Texts in Mathematics, Vol. 5. Springer-Verlag, Berlin.

MAGID, A. 2011. The Hochschild–Mostow group. *Notices Amer. Math. Soc.* 58:1089–1090.

MALLE, G. AND TESTERMAN, D. 2011. *Linear algebraic groups and finite groups of Lie type.* Cambridge Studies in Advanced Mathematics, Vol. 133. Cambridge University Press, Cambridge.

MATSUMURA, H. 1986. *Commutative ring theory.* Cambridge Studies in Advanced Mathematics, Vol. 8. Cambridge University Press, Cambridge.

MATSUSAKA, T. 1953. Some theorems on Abelian varieties. *Nat. Sci. Rep. Ochanomizu Univ.* 4:22–35.

MCNINCH, G. 2013. On the descent of Levi factors. *Arch. Math. (Basel)* 100:7–24.

MCNINCH, G. J. 1998. Dimensional criteria for semisimplicity of representations. *Proc. London Math. Soc. (3)* 76:95–149.

MCNINCH, G. J. 2005. Optimal SL(2)-homomorphisms. *Comment. Math. Helv.* 80:391–426.

MCNINCH, G. J. 2010. Levi decompositions of a linear algebraic group. *Transform. Groups* 15:937–964.

MCNINCH, G. J. 2014a. Levi factors of the special fiber of a parahoric group scheme and tame ramification. *Algebr. Represent. Theory* 17:469–479.

MCNINCH, G. J. 2014b. Linearity for actions on vector groups. *J. Algebra* 397:666–688.

MILNE, J. S. 1986. Abelian varieties, pp. 103–150. In *Arithmetic geometry* (Storrs, Conn., 1984). Springer-Verlag, Berlin.

MILNE, J. S. 2007. Semisimple algebraic groups in characteristic zero. arXiv:0705.1348.

MILNE, J. S. 2013. A proof of the Barsotti–Chevalley theorem on algebraic groups. arXiv:1311.6060.

MILNE, J. S. 2017. A primer of commutative algebra, v4.02. Available at www.jmilne.org/math and http://hdl.handle.net/2027.42/136228. Cited as CA.

MILNE, J. S. AND SHIH, K.-Y. 1982. Conjugates of Shimura varieties, pp. 280–356. In *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, Vol. 900. Springer-Verlag, Berlin.

MIRKOVIĆ, I. AND VILONEN, K. 2007. Geometric Langlands duality and representations of algebraic groups over commutative rings. *Ann. of Math. (2)* 166:95–143.

MÜLLER, P. 2003. Algebraic groups over finite fields, a quick proof of Lang's theorem. *Proc. Amer. Math. Soc.* 131:369–370.

MUMFORD, D. 1970. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, Vol. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London.

MUMFORD, D., FOGARTY, J., AND KIRWAN, F. 1994. *Geometric invariant theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete (2), Vol. 34. Springer-Verlag, Berlin, third edition.

NAGATA, M. 1960. On the fourteenth problem of Hilbert, pp. 459–462. In *Proceedings International Congress of Mathematics 1958*. Cambridge University Press, Cambridge.

NAGATA, M. 1961/1962. Complete reducibility of rational representations of a matric group. *J. Math. Kyoto Univ.* 1:87–99.

NIELSEN, H. A. 1974. Diagonalizably linearized coherent sheaves. *Bull. Soc. Math. France* 102:85–97.

NORI, M. V. 1987. On subgroups of $GL_n(\mathbb{F}_p)$. Invent. Math. 88:257–275.

OESTERLÉ, J. 1984. Nombres de Tamagawa et groupes unipotents en caractéristique p. Invent. Math. 78:13–88.

OORT, F. 1966. Algebraic group schemes in characteristic zero are reduced. Invent. Math. 2:79–80.

PINK, R. 2004. On Weil restriction of reductive groups and a theorem of Prasad. *Math. Z.* 248:449–457.

PLATONOV, V. AND RAPINCHUK, A. 1994. *Algebraic groups and number theory*. Pure and Applied Mathematics, Vol. 139. Academic Press Inc., Boston, MA.

POPOV, V. L. 2015. On the equations defining affine algebraic groups. *Pacific J. Math.* 279:423–446.

PRASAD, G. AND RAPINCHUK, A. S. 2006. On the existence of isotropic forms of semi-simple algebraic groups over number fields with prescribed local behavior. *Adv. Math.* 207:646–660.

PRASAD, G. AND YU, J.-K. 2006. On quasi-reductive group schemes. *J. Algebraic Geom.* 15:507–549. With an appendix by Brian Conrad.

RAGHUNATHAN, M. S. 2015. On Chevalley's $\mathbb{Z}$-form. Indian J. Pure Appl. Math. 46:695–700.

RAYNAUD, M. 1970. *Faisceaux amples sur les schémas en groupes et les espaces homogènes*. Lecture Notes in Mathematics, Vol. 119. Springer-Verlag, Berlin.

REE, R. 1964. Commutators in semi-simple algebraic groups. *Proc. Amer. Math. Soc.* 15:457–460.

RICHARDSON, R. W. 1977. Affine coset spaces of reductive algebraic groups. *Bull. London Math. Soc.* 9:38–41.

ROSENLICHT, M. 1956. Some basic theorems on algebraic groups. *Amer. J. Math.* 78:401–443.

ROSENLICHT, M. 1957. Some rationality questions on algebraic groups. *Ann. Mat. Pura Appl. (4)* 43:25–50.

ROSENLICHT, M. 1961. Toroidal algebraic groups. *Proc. Amer. Math. Soc.* 12:984–988.

ROSENLICHT, M. 1963. Questions of rationality for solvable algebraic groups over nonperfect fields. *Ann. Mat. Pura Appl. (4)* 61:97–120.

RUSSELL, P. 1970. Forms of the affine line and its additive group. *Pacific J. Math.* 32:527–539.

SAAVEDRA RIVANO, N. 1972. *Catégories Tannakiennes*. Lecture Notes in Mathematics, Vol. 265. Springer-Verlag, Berlin.

SANCHO DE SALAS, C. 2001. *Grupos algebraicos y teoría de invariantes*. Aportaciones Matemáticas: Textos, Vol. 16. Sociedad Matemática Mexicana, México.

SANCHO DE SALAS, C. AND SANCHO DE SALAS, F. 2009. Principal bundles, quasi-abelian varieties and structure of algebraic groups. *J. Algebra* 322:2751–2772.

SATAKE, I. 1963. On the theory of reductive algebraic groups over a perfect field. *J. Math. Soc. Japan* 15:210–235.

SATAKE, I. 1967. Symplectic representations of algebraic groups satisfying a certain analyticity condition. *Acta Math.* 117:215–279.

SATAKE, I. 1971. *Classification theory of semi-simple algebraic groups*. Lecture Notes in Pure and Applied Mathematics, Vol. 3. Marcel Dekker, Inc., New York. With an appendix by M. Sugiura.

SCHARLAU, W. 1985. *Quadratic and Hermitian forms*. Grundlehren der Mathematischen Wissenschaften, Vol. 270. Springer-Verlag, Berlin.

SELBACH, M. 1976. *Klassifikationstheorie halbeinfacher algebraischer Gruppen*. Mathematisches Institut der Universität Bonn, Bonn. Diplomarbeit, Universität Bonn, Bonn, 1973, Bonner Mathematische Schriften, Nr. 83.

SERRE, J.-P. 1959. *Groupes algébriques et corps de classes*. Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris. Translated as *Algebraic groups and class fields*, Springer-Verlag, Berlin, 1988.

SERRE, J.-P. 1962. *Corps locaux*. Publications de l'institut de mathématique de l'université de Nancago, VIII. Hermann, Paris. Translated as *Local fields*, Springer-Verlag, Berlin, 1979.

SERRE, J.-P. 1966. *Algèbres de Lie semi-simples complexes*. W. A. Benjamin, Inc., New York and Amsterdam. Translated as *Complex semisimple Lie algebras*, Springer-Verlag, Berlin, 1987.

SERRE, J.-P. 1970. *Cours d'arithmétique*. Collection SUP: "Le Mathématicien", Vol. 2. Presses Universitaires de France, Paris. Translated as *A Course in Arithmetic*, Springer-Verlag, Berlin, 1973.

SERRE, J.-P. 1993. Gèbres. *Enseign. Math. (2)* 39:33–85.

SERRE, J.-P. 1994. Sur la semi-simplicité des produits tensoriels de représentations de groupes. Invent. Math. 116:513–530.

SERRE, J.-P. 1997. *Galois cohomology*. Springer-Verlag, Berlin. Translation of *Cohomologie Galoisienne*; revised by the author.

SOPKINA, E. 2009. Classification of all connected subgroup schemes of a reductive group containing a split maximal torus. *J. K-Theory* 3:103–122.

SPRINGER, T. A. 1977. *Invariant theory*. Lecture Notes in Mathematics, Vol. 585. Springer-Verlag, Berlin.

SPRINGER, T. A. 1979. Reductive groups, pp. 3–27. In *Automorphic forms, representations and L-functions* (Proceedings of Symposia in Pure Mathematics, Vol. 33, Part 1, Oregon State University, Corvallis, OR, 1977). American Mathematical Society, Providence, RI.

SPRINGER, T. A. 1994. Linear algebraic groups, pp. 1–121. In *Algebraic geometry. IV*, Encyclopaedia of Mathematical Sciences, Vol. 55. Springer-Verlag, Berlin. (Translation of *Algebraicheskaya geometriya 4*, VNINITI, Moscow, 1989).

SPRINGER, T. A. 1998. *Linear algebraic groups*. Progress in Mathematics, Vol. 9. Birkhäuser Boston, Boston, MA.

SPRINGER, T. A. AND VELDKAMP, F. D. 2000. *Octonions, Jordan algebras and exceptional groups*. Springer Monographs in Mathematics. Springer-Verlag, Berlin.

STEINBERG, R. 1965. Regular elements of semisimple algebraic groups. Inst. Hautes Études Sci. Publ. Math. pp. 49–80. Reprinted in Serre 1997.

STEINBERG, R. 1967. *Lectures on Chevalley groups*. Department of Mathematics, Yale University. mimeographed notes (reprinted by the American Mathematical Society, 2016).

STEINBERG, R. 1968. *Endomorphisms of linear algebraic groups*. Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, RI.

STEINBERG, R. 1999. The isomorphism and isogeny theorems for reductive algebraic groups. *J. Algebra* 216:366–383.

SUZUKI, K. 1971. A note on a theorem of E. Cartan. *Tôhoku Math. J. (2)* 23:17–20.

SWEEDLER, M. E. 1967. Hopf algebras with one grouplike element. *Trans. Amer. Math. Soc.* 127:515–526.

SWEEDLER, M. E. 1969. *Hopf algebras*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York and Amsterdam.

TAKEUCHI, M. 1972. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.* 7:251–270.

TAKEUCHI, M. 1983. A hyperalgebraic proof of the isomorphism and isogeny theorems for reductive groups. *J. Algebra* 85:179–196.

TATE, J. 1997. Finite flat group schemes, pp. 121–154. In *Modular forms and Fermat's last theorem* (Boston, MA, 1995). Springer-Verlag, Berlin.

TATE, J. AND OORT, F. 1970. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)* 3:1–21.

THĂŃG, N. 2008. On Galois cohomology of semisimple groups over local and global fields of positive characteristic. *Math. Z.* 259:457–467.

THĂŃG, N. 2012. On Galois cohomology of semisimple groups over local and global fields of positive characteristic, II. *Math. Z.* 270:1057–1065.

TITS, J. 1966. Classification of algebraic semisimple groups, pp. 33–62. In *Algebraic Groups and Discontinuous Subgroups* (Proceedings of Symposia in Pure Mathematics, Boulder, CO, 1965). American Mathematical Society, Providence, RI.

TITS, J. 1968. Lectures on Algebraic Groups, notes by P. André and D. Winter, fall term 1966–1967, Yale University.

TITS, J. 1971. Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque. *J. Reine Angew. Math.* 247:196–220.

TITS, J. 1992. Théorie des groupes, Annuaire du Collège de France 1991-92. Reprinted in Tits 2013.

TITS, J. 1993. Théorie des groupes, Annuaire du Collège de France 1992-93. Reprinted in Tits 2013.

TITS, J. 2013. *Résumés des cours au Collège de France 1973–2000.* Documents Mathématiques (Paris), Vol. 12. Société Mathématique de France, Paris.

TOTARO, B. 2008. Hilbert's 14th problem over finite fields and a conjecture on the cone of curves. *Compos. Math.* 144:1176–1198.

TOTARO, B. 2013. Pseudo-abelian varieties. *Ann. Sci. École Norm. Sup. (4)* 46:693–721.

VOSKRESENSKIĬ, V. E. 1998. *Algebraic groups and their birational invariants.* Translations of Mathematical Monographs, Vol. 179. American Mathematical Society, Providence, RI.

WATERHOUSE, W. C. 1979. *Introduction to affine group schemes.* Graduate Texts in Mathematics, Vol. 66. Springer-Verlag, Berlin.

WEIL, A. 1946. *Foundations of Algebraic Geometry.* American Mathematical Society Colloquium Publications, Vol. 29. American Mathematical Society, New York.

WEIL, A. 1957. On the projective embedding of Abelian varieties, pp. 177–181. In *Algebraic geometry and topology.* A symposium in honor of S. Lefschetz. Princeton University Press, Princeton, NJ.

WEIL, A. 1982. *Adeles and algebraic groups.* Progress in Mathematics, Vol. 23. Birkhäuser Boston. Based on lectures at IAS, 1959–1960.

WU, X. L. 1986. On the extensions of abelian varieties by affine group schemes, pp. 361–387. In *Group theory, Beijing 1984*, Lecture Notes in Mathematics, Vol. 1185. Springer-Verlag, Berlin.

ZIBROWIUS, M. 2015. Symmetric representation rings are λ-rings. *New York J. Math.* 21:1055–1092.

Index

Errata for Algebraic Groups (2017)

Starred items have been corrected in the paperback edition.

DG=Demazure and Gabriel 1970; CGP=Conrad, Gabber, and Prasad 2015.

Contributors include: Jarod Alper; Michel Brion; Magnus Carlson; Dylon Chow; Brian Conrad; Rostislav Devyatov; Ofer Gabber; Cédric Pépin; Bjorn Poonen; Matthieu Romagny; Zev Rosengarten; Thierry Stulemeijer; Vladimir Sotirov; Yugo Takanashi; Christian Voigt; Qijun Yan.

Chapter 1

The Notation 3.2 should be placed earlier in the book. For example, it is implicitly used in the proof of 1.49.

*p.18. Proof of 1.40. Multiplication on $G(k)$ is continuous for the Zariski topology, but not necessarily for the product topology, and so we don't know that there exist A and B as claimed. A correct proof is not difficult.

*p.20. Corrected statement of 1.45: Let G be an algebraic group over k and S a closed subgroup of $G(k)$. There is a unique reduced algebraic subgroup H of G such that $|H|$ is the closure $\bar{S}$ of S in $|G|$; it is geometrically reduced and $H(k) = S$. The algebraic subgroups H of G that arise in this way are exactly those for which $H(k)$ is schematically dense in H.

*p.21 Definition 1.48. Let G be an algebraic group over k and S a subgroup of $G(k)$. The unique algebraic subgroup H of G such S is schematically dense in H is called the Zariski closure of S in G.

*p.26. Proposition 1.65. In the proof of (a), one should choose U before passing to the algebraic closure.

Chapter 2

*p.48 The group G has height $\leq n$ if $Ker(F_G^n) = G$, i.e., F_G^n is trivial (rather than 0).

*p.51. Replace X with G thrice in the first paragraph of Section 2g.

*p.60. Section 2j: Define torsors over nonaffine bases, because such torsors occur later in the book.

Chapter 3

*p.80, 3.52. Two inner forms (G, f) and (G', f') are said to be equivalent if there exists an isomorphism $\varphi: G \to G'$ such that $f' = \varphi_K \circ f$ up to an inner automorphism of G_{0K}, i.e., such that $f'^{-1} \circ \varphi_K \circ f$ is inner.

*p.85. G_W is the stabilizer of W in G (not V).

Chapter 4

*p.95. In the proof of 4.29, $V^{\otimes m} \otimes W$ should be $V^{\otimes m} \otimes V'$ (twice).

Chapter 5

*p.123. Delete $\mathrm{Coker}(g')$ from the diagram and sequence in Exercise 5-7 (the homomorphism g' need not be normal).

Chapter 6

*p.129, 6.19. In (c,d,e), G should be assumed to be smooth (to be safe). See DG, II, Sect. 5, 4.8, p.247, for a proof of (c) in the smooth case.

*p.136. In the example 6.48, take $p = 2$, otherwise the multiplication doesn't preserve the defining relation. Also, the kernel N of φ is $X^p - tY^p = 1$ (not 0).

Chapter 8

*p.150. The proof of Proposition 8.9 requires X to be reduced. Corollary 8.10 is correct, but the proof requires an addition step. This suffices for the applications.

*p.157. The line before Proposition 8.37 should read: central extension if G is connected.

Chapter 9

*p.173, 9.25. λ_X should lie in $\mathrm{End}(\omega(X))$..., not $\mathrm{End}(X)$...

*p.181. In the proof of 9.44 requires correction.

Chapter 11

*p.223. Proposition 11.36 should read $\ldots\alpha = \mathrm{Lie}(\varphi)$ not $\ldots\alpha = \mathrm{Lie}(\varphi) \circ \mathrm{Lie}(\varphi)$.

*p.224. Throughout the section on the Verschiebung morphism, G is commutative (as in the first paragraph). In definition 11.39 the second arrow is reversed.

Chapter 12

*p.244. In 12.41, N should be a central subgroup of H. This suffices for the applications.

*p.249. The proof of 12.57 is missing a step: first show that the Reynolds operator is A^G-linear. Also a_i should be r_i.

Chapter 13

*p.255. In the proof of 13.4, replace $=\subset$ with $\simeq$.

*p.262. In (86), set $Z = X$.

Chapter 14

*p.273. In Theorem 13.47(c) (and corollaries), it is necessary to require X to be proper, otherwise there may be no fixed points.

Chapter 15

*p.317. Delete 15.29 and 15.30. The proofs in Section 15h have been rewritten.

Chapter 16

*p.324. In the last sentence of first paragraph, replace "diagonalizable" with "trigonalizable".

*p.330. Near the end of 16.20, the field k' is $k[c^{1/p}]$.

*p.349. In 16.65, the subgroup H should be connected (obviously).

Chapter 17

*p.360. The statement before 17.28 should say that SL_2 (not SL_3) has dimension 3 (obviously).

*p.364. In 17.42, take $I = \{1, 2, \ldots, n\}$ (or rewrite the last sentence).

*p.386. Delete Exercise 17-7. It is true that Steinberg 1968, 7.2, proves that every surjective endomorphism of an algebraic group over an algebraically closed field fixes a Borel subgroup, but you should read Steinberg's proof rather than trying to prove it yourself.

Chapter 18

*p.388 and p.396 In the last sentence of 18.4 and in 18-1, G should be reductive.

*p.389. In the statement of 18.8, the target of α is G', not G. This is correct in the diagram.

Chapter 19

*p.399 Definition 19.7 should read: An algebraic group G over k is almost-simple if it is semisimple and non-commutative and its only smooth connected normal subgroups are G and e. It is simple if in addition its centre is trivial. Similarly change in 19.8.

Chapter 20

*p.417. In the proof of 20.27, interchange second and third.

*p.419. In the statement of 20.33, add "G of semisimple rank 1" after "reductive group". In the final sentence of the proof, (first,second,third) should be (second,third,first).

*p.420. The reference to "Section 2k" should be to "Section 3k".

Chapter 21

*p.440 The proof of Theorem 21.51 has been rewritten.

*p.445. The necessity in Theorem 21.68(d) fails in characteristics $2, 3$ (and is not "obvious" in characteristics $\neq 2, 3$).

*p.447. The proof of Proposition 21.71 only shows that $B_u e_w \subset Y(w)$. To prove equality, show as in the proof of 21.75 that (T3) holds, and deduce that $G = \bigcup_w B_u w B$.

*p.449. In the proof of Proposition 21.11, replace the appeal to 21.67 with a direct argument.

*p.456–60. In several places in Example (A_n), I write n instead of $n + 1$. In 21.96, replace SL_n with SL_{n+1} and $\mathbb{Z}/n\mathbb{Z}$ with $\mathbb{Z}/(n+1)\mathbb{Z}$.

Set braces are missing in the lines displaying Φ and Δ in 21.97, 21.98, 21.99, and an equality symbol is missing for Δ in 21.98.

In Example C_n there is an errant SO_{2n+1}. In Example (D_n), SO_n should be SO_{2n} and, two lines later, SO_{2n+1} should be SO_{2n}.

*p.460 middle, definition of ϕ, the last y_{2n} should be y_n.

*p.460 last paragraph, $2n + 1 \times 2n + 1$ should be $2n \times 2n$.

*p.461. In Exercise 21-2 one needs to assume that the unipotent group is smooth, otherwise there are the infamous unipotent isogenies in characteristic 2, as in 18.3 and as discussed in Section 2 of Prasad and Yu 2006.

Chapter 22

*p.468. Redefined $E(\lambda)$ to be induced from the opposite Borel subgroup B' so as to agree with the literature. Now it is nonzero if and only if λ is dominant etc.

*p.469. Expanded the proof of the crucial Lemma 22.24.

*p.473. Example 22.35 mysteriously repeats example 22.34 instead of giving the fundamental weights of PGL_n.

*p.480. In Theorem 22.52, either assume k has characteristic zero or replace V with $H^0(G/B', L(\chi))$.

Chapter 23

*p.488. End of second sentence of last paragraph of the proof of 23.11, change U_{α_2} to $U_{\alpha_2}(k)$.

*p.494. In the statement of Corollary, 23.32, change "an algebraic group" to "a reductive algebraic group" (so (G', T) is a split reductive group, and having a root datum makes sense).

*p.497 23.42. Any inner automorphism of a pinned reductive group is trivial.

*p.498. Replace (X, Φ, Δ) with $(X, \Phi, \Phi^\vee, \Delta)$ thrice. ¬¿

*p.498.The statement of Corollary 23.48 is incorrect. When G is split, the map $H^1(k, \text{Inn}(G)) \to H^1(k, \text{Aut}(G))$ is injective as a map of pointed sets, but not necessarily as a map of sets. See p.523 below. This is not used, but it means that it is necessary to distinguish the two notions of inner form, even for split groups.

*p.498. In the proof of Corollary 23.47, the first G should be $\text{Aut}(G)$.

*p.498. Corollary 23.48 should only say that an inner form (G, f) is trivial if and only if the inner form G is trivial.

4

p.499. In 23.50, $\mathrm{Hom}(G,H)$ is not affine unless $\mathrm{Out}(G)$ is finite (because $(\mathbb{Z})_k$ is not affine).

*p.500 In 23.52, G is a reductive group.

*p.500. Here is a more precise statement of Corollary 23.54: Let G be a reductive group over k. There exists an inner form (H,f) of G such that H is quasi-split, and any two such inner forms are equivalent. In particular, the class of (H,f) in $H^1(k,G^{\mathrm{ad}})$ is uniquely determined.

*p.501. In the statement of Corollary 23.56, the objects of the second category are reduced root data.

*p.504. Line 4, should read $[X_i,Y_i]=H_i\ldots$, not $[X_i,X_i]\ldots$.

*p.504. In the last displayed equation of the "First proof", J_j should be Y_j.

*p.504. Proposition 23.64 has been deleted and a remark added.

*p.505. The last displayed equation before Lemma 23.65 should read $h_i(v_\alpha)=\langle\alpha,\alpha_i^\vee\rangle v_\alpha$ (subscript i is missing).

*p.506. In the condition (c), replace β_R with β. In the next line, replace $\mathfrak{g}_R$ with $\mathfrak{g}_\mathcal{R}$.

*p.506. In the proof of Lemma 23.68, p.475 should be p.476.

*p.507. In Theorem 23.70, (d) and (e), G should be $G(\mathfrak{g})$.

Chapter 24

*p.513 In line 3, replace "isogeny" with "central isogeny". In 24.3, "the field of definition of G_i as a subgroup of G" is the fixed field of the subgroup of $\mathrm{Gal}(k^s/k)$ fixing G_i.

*p.515, Caution: the second exact sequence in the displayed pair is only exact as a sequence of pointed sets. See p.498 above.

*p.516. Line 2: replace "subset" with "image of".

*p.516. Line 4: Homs modulo conjugation in the case D_4.

*p.518. Simple algebras over k are required to be nonzero.

*p.518. In fact, 24.20 is not proved in Jacobson 1989, Section 4.6, with the "separable" condition.

*p.524. Throughout this section, $n>2$.

*p.531. At the end of the first paragraph of Section 24i, replace $C(V,q)$ with $C_0(V,q)$.

*p.540. Near the bottom, F_2 should be F_4 — there is no F_2.

Chapter 25

*p.545 et seq. In 25.6(b), in the final sentence of 25.24, and in 25.27, the parabolic subgroup (P or Q) should be minimal, and in 25.27, S should be maximal split in P.

*p.546. The proof of 25.7 is only a brief sketch. The "nontrivial" on the first line of the proof of 25.10 should be "noncentral".

p.549. The statement in 25.16, that the relative root system is a root system, is certainly correct but (as explained to me by Brian Conrad) the proofs of this in

5

the classical literature (Borel and Tits 1965, Borel 1991, and Springer 1998) are incomplete. For a complete proof, see CGP, C.2.15.

*p.549. In line 1 of 25.19, add "torus" to "maximal split".

*p.563. In 25.66 and 25.68, the direct products should be direct sums. In 25.67 and 25.69, the $G^{(v)}$ should be required to be quasi-split for all but finitely many v.

Appendix A

*p.570. The proof in footnote 3 requires correction.

*p.582. In A.70, delete the word "faithfully".