

Algebraic Groups

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



J.S. Milne

Version 2.00
December 20, 2015

An algebraic group is a matrix group defined by polynomial conditions. More abstractly, it is a group scheme of finite type over a field. These notes are a comprehensive modern introduction to the theory of algebraic groups assuming only the knowledge of algebraic geometry usually acquired in a first course.

This is still only a preliminary version, but is the last before the final version. It will be revised again before publication. In particular, repetitions, references to my website, and notational inconsistencies will be removed; exercises and examples will be added; errors will be corrected. The final version will be more tightly written, and will include 500 pages + front matter. I welcome suggestions for improvements to the final version, which can be sent to me at [jmilne at umich.edu](mailto:jmilne@umich.edu).

BibTeX information

```
@misc{milneiAG,  
  author={Milne, James S.},  
  title={Algebraic Groups (v2.00)},  
  year={2015},  
  note={Available at www.jmilne.org/math/},  
  pages={528}  
}
```

v1.00 (July 31, 2014). First published on the web, 331 pages.

v1.20 (January 29, 2015). Revised Parts A,B, 373 pages.

v2.00 (December 20, 2015). Significantly rewritten and completed.

Available at www.jmilne.org/math/

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

Copyright © 2014, 2015 J.S. Milne.

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

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 the points in some “universal” field, it is more natural to consider the functor of k -algebras defined by the algebraic group.

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 isomorphisms theorems hold for 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).³ 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 by passing to the algebraic closure where possible and by an occasional use of Hopf algebras. Unpleasantly technical arguments that I have not (so far) been able to avoid have been placed in separate sections where they can be ignored by all

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.” J. Tits, Lectures on Algebraic Groups, Fall 1966.

²To anyone who asked why we need to allow nilpotents, Grothendieck would say that they are already there in nature; neglecting them obscures our vision. And indeed they are there, for example, in the kernel of $SL_p \rightarrow PGL_p$.

³They also assumed the main classification results of the old theory.

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.

The exposition incorporates simplifications to the general theory from [Allcock 2009](#), [Doković 1988](#), [Iversen 1976](#), [Luna 1999](#), and [Steinberg 1998, 1999](#) and elsewhere.

The experienced reader is cautioned that, throughout the text, “algebraic group scheme” is shortened to “algebraic group”, nonclosed points are ignored, and a “group variety” is a smooth algebraic group.

Equivalently, a group variety is group in the category of algebraic varieties (geometrically reduced separated schemes of finite type over a field). However, it is important to note that varieties are always regarded as special algebraic schemes. For example, fibres of maps are to be taken in the sense of schemes, and the kernel of a homomorphism of group varieties is an algebraic group which is not necessarily a group variety (it need not be smooth). 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.⁴

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.

To repeat: all constructions are to be understood as being in the sense of schemes.

In writing this book, I have depended heavily on the expository efforts of earlier authors. The following works have been especially useful to me.

Demazure, Michel; Gabriel, Pierre. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. xxvi+700 pp.

Séminaire Heidelberg-Strasbourg 1965–66 (Groupes Algébriques), multigraphié par l’Institut de Mathématique de Strasbourg (Gabriel, Demazure, et al.). 407 pp.

The expository writings of Springer, especially: Springer, T. A., Linear algebraic groups. Second edition. Progress in Mathematics, 9. Birkhäuser Boston, Inc., Boston, MA, 1998. xiv+334 pp.

Waterhouse, William C., Introduction to affine group schemes. Graduate Texts in Mathematics, 66. Springer-Verlag, New York-Berlin, 1979. xi+164 pp.

Notes of Ngo, Perrin, and Pink have also been useful.

Finally, I note that the new edition of SGA 3 is a magnificent resource.

⁴An example is Chevalley’s theorem on representations; see [4.21](#).

Contents

Preface	3
Contents	6
Notations and conventions	14
Foundations	14
Prerequisites	15
References	15
Introduction	15
1 Basic definitions and properties	17
a Definition	17
b Basic properties of algebraic groups	21
c Algebraic subgroups	24
d Examples	27
e Kernels	28
f Group actions	30
g Closed subfunctors: definitions and statements	31
h Transporters	32
i Normalizers	33
j Centralizers	34
k Closed subfunctors: proofs	36
2 Examples; some basic constructions	39
a Affine algebraic groups	39
b Anti-affine algebraic groups	42
c Homomorphisms of algebraic groups	43
d Products	44
e Semidirect products	45
f The algebraic subgroup generated by a map	46
g Forms of algebraic groups	49
h Restriction of scalars	50
Exercises	52
3 Affine algebraic groups and Hopf algebras	55
a The comultiplication map	55
b Hopf algebras	56
c Hopf algebras and algebraic groups	57
d Hopf subalgebras	58
e Hopf subalgebras of $\mathcal{O}(G)$ versus algebraic subgroups of G	59
f Subgroups of $G(k)$ versus algebraic subgroups of G	59

g	Affine algebraic groups G such that $G(k)$ is dense in G : a survey	60
h	Affine algebraic groups in characteristic zero are smooth	62
i	Smoothness in characteristic $p \neq 0$	64
j	Faithful flatness for Hopf algebras	65
	Exercises	67
4	Linear representations of algebraic groups	69
a	Representations and comodules	69
b	Stabilizers	70
c	Every representation is a union of finite-dimensional representations	71
d	Affine algebraic groups are linear	72
e	Constructing all finite-dimensional representations	72
f	Semisimple representations	74
g	Characters and eigenspaces	75
h	Chevalley's theorem	77
i	The subspace fixed by a group	78
5	Group theory; the isomorphism theorems	81
a	Terminology on functors	81
b	Definitions	82
c	The homomorphism theorem	84
d	Existence of quotients by normal subgroups	85
e	Properties of quotients	88
f	The isomorphism theorem	89
g	The correspondence theorem	90
h	The category of commutative algebraic groups	91
i	The group of connected components of an algebraic group	91
j	Torsors and extensions	96
	Exercises	96
6	The isomorphism theorems using sheaves.	97
a	Some sheaf theory	97
b	The isomorphism theorems for abstract groups	99
c	The isomorphism theorems for group functors	99
d	The isomorphism theorems for sheaves of groups	100
e	The isomorphism theorems for affine algebraic groups	101
f	The isomorphism theorems for algebraic groups	101
g	Some category theory	104
	Exercises	105
7	Existence of quotients of algebraic groups	107
a	Equivalence relations	107
b	Existence of quotients in the finite affine case	111
c	Existence of quotients in the finite case	116
d	Existence of quotients in the presence of quasi-sections	118
e	Existence generically of a quotient	121
f	Existence of quotients of algebraic groups	122
g	Complements	124
8	Subnormal series; solvable and nilpotent algebraic groups	125

a	Subnormal series	125
b	Isogenies	127
c	Composition series for algebraic groups	127
d	Solvable and nilpotent algebraic groups	129
e	The derived group of an algebraic group	130
f	Nilpotent algebraic groups	133
g	Existence of a greatest algebraic subgroup with a given property	134
h	Semisimple and reductive groups	135
i	A standard example	137
9	Algebraic groups acting on schemes	139
a	Group actions	139
b	The fixed subscheme	140
c	Orbits and isotropy groups	141
d	The functor defined by projective space	143
e	Quotients: definition and properties	144
f	Quotients: construction in the affine case	146
g	Linear actions	148
h	Complements	148
i	Flag varieties	149
j	Exercises	149
	Exercises	149
10	The structure of general algebraic groups	151
a	Summary	151
b	Generalities	152
c	Local actions	153
d	Anti-affine algebraic groups and abelian varieties	154
e	Rosenlicht's decomposition theorem.	154
f	Rosenlicht's dichotomy	156
g	The Barsotti-Chevalley theorem	156
h	Anti-affine groups	158
i	Extensions of abelian varieties by affine algebraic groups (survey)	160
	Exercises	161
11	Tannaka duality; Jordan decompositions	163
a	Recovering a group from its representations	163
b	Application to Jordan decompositions	166
c	Characterizations of categories of representations	171
d	Tannakian categories	173
e	Proof of Theorem 11.25	174
f	Properties of G versus those of $\text{Rep}_k(G)$: a summary	182
12	The Lie algebra of an algebraic group	183
a	Definition	183
b	The Lie algebra of an algebraic group	184
c	Basic properties of the Lie algebra	186
d	The adjoint representation; definition of the bracket	187
e	Description of the Lie algebra in terms of derivations	189

f	Stabilizers	190
g	Centres	192
h	Normalizers and centralizers	193
i	An example of Chevalley	194
j	The universal enveloping algebra	194
k	The universal enveloping p -algebra	199
	Exercises	202
13	Finite group schemes	203
a	Generalities	203
b	Etale group schemes	205
c	Finite group schemes of order n are killed by n	207
d	Cartier duality	209
e	Finite group schemes of order p	211
f	Derivations of Hopf algebras	211
g	Structure of the underlying scheme of a finite group scheme	214
h	Finite group schemes of height at most one	216
i	The Frobenius and Verschiebung morphisms	217
j	The Witt schemes W_n	220
k	Commutative group schemes over a perfect field	221
14	Tori; groups of multiplicative type; linearly reductive groups	225
a	The characters of an algebraic group	225
b	The algebraic group $D(M)$	225
c	Diagonalizable groups	227
d	Diagonalizable representations	229
e	Tori	230
f	Groups of multiplicative type	230
g	Representations of a group of multiplicative type	232
h	Criteria for an algebraic group to be of multiplicative type	233
i	Rigidity	235
j	Unirationality	237
k	Actions of \mathbb{G}_m on affine and projective space	239
l	Linearly reductive groups	241
m	The smoothness of fixed subschemes	242
n	Maps to tori	245
o	Central tori as almost-factors	246
p	Etale slices; Luna's theorem	247
	Exercises	249
15	Unipotent algebraic groups	251
a	Preliminaries from linear algebra	251
b	Unipotent algebraic groups	252
c	Unipotent algebraic groups in characteristic zero	258
d	Unipotent algebraic groups in nonzero characteristic	261
e	Split and wound unipotent groups: a survey	266
	Exercises	267
16	Cohomology and extensions	269

a	Crossed homomorphisms	269
b	Hochschild cohomology	270
c	Hochschild extensions	273
d	The cohomology of linear representations	275
e	Linearly reductive groups	277
f	Applications to homomorphisms	278
g	Applications to centralizers	278
h	Calculation of some extensions	281
17	The structure of solvable algebraic groups	291
a	Trigonalizable algebraic groups	291
b	Commutative algebraic groups	294
c	Structure of trigonalizable algebraic groups	297
d	Solvable algebraic groups	300
e	Solvable algebraic groups (variant)	303
f	Nilpotent algebraic groups	306
g	Split solvable groups	308
h	Complements on unipotent algebraic groups	309
i	The canonical filtration on an algebraic group	309
j	Summary	310
	Exercises	310
18	Borel subgroups; Cartan subgroups	313
a	Borel fixed point theorem	313
b	Borel subgroups	315
c	The density theorem	321
d	Centralizers of tori are connected	322
e	The normalizer of a Borel subgroup	326
f	Borel and parabolic subgroups over an arbitrary base field	329
g	Maximal tori and Cartan subgroups over an arbitrary base field	329
	Exercises	331
19	The variety of Borel subgroups	333
a	The variety of Borel subgroups	333
b	Decomposition of a projective variety under the action of a torus (Białynicki-Birula)	335
c	Chevalley's theorem on the Borel subgroups containing a maximal torus	340
d	Proof of Chevalley's theorem (Luna)	342
e	Proof of Chevalley's theorem (following SHS)	344
f	Summary	346
20	The geometry of reductive algebraic groups	349
a	Definitions	349
b	The universal covering	350
c	Line bundles and characters	351
d	Existence of a universal covering	353
e	Applications	354
f	Proof of theorem 20.13	355
21	Algebraic groups of semisimple rank at most one	357

a	Brief review of reductive groups	357
b	Group varieties of semisimple rank 0	358
c	Limits in algebraic varieties	358
d	Limits in algebraic groups	360
e	Actions of tori on a projective space	365
f	Homogeneous curves	366
g	The automorphism group of the projective line	367
h	Review of Borel subgroups	368
i	Criteria for a group variety to have semisimple rank 1.	369
j	Split reductive groups of semisimple rank 1.	371
k	Properties of SL_2	373
l	Classification of the split reductive groups of semisimple rank 1	374
m	Roots	377
n	Forms of GL_2	379
22 Reductive groups		381
a	Semisimple groups	381
b	Reductive groups	382
c	The roots of a split reductive group	385
d	The centre of a reductive group	388
e	Root data and root systems	389
f	The root datum of a split reductive group	391
g	The root data of the classical semisimple groups	394
h	The Weyl groups and Borel subgroups	397
i	Subgroups normalized by T	400
j	Big cells and the Bruhat decomposition	401
k	The parabolic subgroups	407
l	The isogeny theorem: statements	408
m	The isogeny theorem: proofs	412
n	The structure of semisimple groups	417
o	Reductive groups in characteristic zero	422
p	Roots of nonsplit reductive groups: a survey	424
q	Pseudo-reductive groups: a survey	426
r	Levi subgroups: a survey	428
s	Exercises	429
23 Root data and their classification		431
a	Equivalent definitions of a root datum	431
b	Deconstructing root data	433
c	Semisimple root data and root systems	433
d	Root systems	434
24 Representations of reductive groups		443
25 The existence theorem		447
a	Characteristic zero: classical approach	447
b	Characteristic zero: Tannakian approach.	448
c	All characteristics: Chevalley's approach	450
d	All characteristics: explicit construction	450

e	Spin groups	451
f	Groups of types A, B, C, D	463
g	Groups of type E_6	463
h	Groups of type E_7	464
i	Groups of type E_8	464
j	Groups of type F_4	464
k	Groups of type G_2	464
26	Nonsplit algebraic groups: a survey.	465
a	General classification (Satake-Tits)	465
b	Relative root systems and the anisotropic kernel.	465
27	Cohomology: a survey	469
a	Definition of nonabelian cohomology; examples	469
b	Generalities on forms	475
c	Forms of semisimple algebraic groups	478
d	Classical groups	480
e	The Galois cohomology of algebraic groups; applications	486
A	Review of algebraic geometry	491
a	Affine algebraic schemes	491
b	Algebraic schemes	493
c	Subschemes	494
d	Algebraic schemes as functors	495
e	Fibred products of algebraic schemes	498
f	Algebraic varieties	499
g	The dimension of an algebraic scheme	499
h	Tangent spaces; smooth points; regular points	500
i	Galois descent for closed subschemes	502
j	On the density of points	503
k	Schematically dominant maps	504
l	Separated maps; affine maps	505
m	Finite schemes	505
n	Finite algebraic varieties (étale schemes)	506
o	The algebraic variety of connected components of an algebraic scheme	506
p	Flat maps	506
q	Flat descent	507
r	Finite maps and quasi-finite maps	508
s	The fibres of regular maps	509
t	Étale maps	510
u	Smooth maps	510
v	Complete algebraic schemes	511
w	Proper maps	511
x	Algebraic schemes as flat sheaves (will be moved to Chapter V)	512
y	Restriction of the base field (Weil restriction of scalars)	512
B	Dictionary	515
a	Demazure and Gabriel 1970	515
b	Borel 1969/1991; Springer 1981/1998	515

c	Waterhouse 1979	516
C	Solutions to the exercises	517
	Bibliography	519
	Index	525

Notations and conventions

Throughout, k is a field and R is a k -algebra. All algebras over a field or ring are required to be commutative and finitely generated unless it is specified otherwise. Unadorned tensor products are over k . An extension of k is a field containing k . When V is a vector space over k , we often write V_R or $V(R)$ for $R \otimes V$. The symbol k^{al} denotes an algebraic closure of k , and k^{sep} denotes the separable closure of k in k^{al} .

An algebraic scheme over k (or algebraic k -scheme) is a scheme of finite type over k (EGA I, 6.5.1). An algebraic variety is a geometrically-reduced separated algebraic scheme. A “point” of an algebraic scheme or variety means “closed point”.⁵ 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. When the base field k is understood, we write “algebraic scheme” for “algebraic scheme over k ”.

Let R be a finitely generated k -algebra. We let Alg_R denote the category of finitely generated R -algebras.

All categories are locally small (i.e., the objects may form a proper class, but 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 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 loosely refer to a natural transformation of functors as a map of functors.

An element g of a partially ordered set P is a **greatest** element if, for every element a in P , $a \leq g$. An element m in P is **maximal** if, for a in P , $m \leq a$ implies $a = m$. If a partially ordered set has a greatest element, it must be the unique maximal element, but otherwise there can be more than one maximal element (or none). **Least** and **minimal** elements are defined similarly. When the partial order is inclusion, we often say **smallest** for least.

A diagram $A \rightarrow B \rightrightarrows C$ is said to be **exact** if the first arrow is the equalizer of the pair of arrows.

After p.161, all algebraic groups are affine. (The reader may wish to assume this throughout, and skip Chapters 7 and 10.)

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 doesn’t quantify over proper classes 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 functors from one of these categories to another (Ernst 2015). 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} , and let Alg_k^0 denote the category of k -algebras of the form $k[T_0, \dots, T_n]/\mathfrak{a}$

⁵Let X be an algebraic scheme over a field, and let X_0 be the set of closed points in X with the induced topology. Then the map $U \mapsto U \cap X_0$ is a bijection from the set of open subsets of X onto the set of open 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 proper irreducible closed subset Z of X_0 ; the point z lies in an open subset U if and only if $U \cap Z$ is nonempty.

for some $n \in \mathbb{N}$ and ideal \mathfrak{a} in $k[T_0, \dots, T_n]$. Thus the objects of Alg_k^0 are indexed by the ideals in some subring $k[T_0, \dots, T_n]$ of $k[T_0, \dots]$ — 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 $R \rightarrow A$ 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 $\text{Alg}_k^0 \hookrightarrow \text{Alg}_k$ is an equivalence of categories because every finitely generated k -algebra is isomorphic to a small k -algebra. 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 (DG, p.xxv), and take a small k -algebra to be one that is small relative to the chosen universe.⁶

Prerequisites

A first course in algebraic geometry. Since these vary greatly, we review the definitions and statements that we need from algebraic geometry in Appendix A. In a few places, which can usually be skipped, we assume more algebraic geometry.

References

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

AG Algebraic Geometry (v6.00, 2014).

CA A Primer of Commutative Algebra (v4.01, 2014).

LAG Lie Algebras, Algebraic Groups, and Lie Groups (v2.00, 2013).

I also refer to:

DG Demazure, Michel; Gabriel, Pierre. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. xxvi+700 pp.

SHS Séminaire Heidelberg-Strasbourg 1965–66 (Groupes Algébriques), multigraphié par l’Institut de Mathématique de Strasbourg (Gabriel, Demazure, et al.). 407 pp.

SGA 3 Schémas en Groupes, Séminaire de Géométrie Algébriques du Bois Marie 1962–64, dirigé par M. Demazure et A. Grothendieck. Revised edition (P. Gille and P. Polo editors), Documents Mathématiques, SMF, 2011.

EGA Eléments de Géométrie Algébrique, A. Grothendieck; J. A. Dieudonné; I, Le langage des schémas (Springer Verlag 1971); II, III, IV Inst. Hautes Etudes Sci. Publ. Math. 8, 11, 17, 20, 24, 28, 32, 1961–1967.

A reference monnnn is to question nnnn on mathoverflow.net.

Introduction

The work can be divided roughly into six parts.

⁶Or they may simply ignore the problem, which is what most of the literature does.

A. BASIC THEORY (CHAPTERS 1–10)

)

The first ten chapters cover the general theory of algebraic groups (not necessarily affine). After defining algebraic groups 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 groups to Hopf algebras, and we prove that all affine algebraic groups in characteristic zero are smooth. We study the linear representations of algebraic groups and the actions of algebraic groups on algebraic schemes. We show that every algebraic group is an extension of a finite étale algebraic group by a connected algebraic group, and that every connected group variety over a perfect field is an extension of an abelian variety by an affine group variety (Barsotti-Chevalley theorem).

B. PRELIMINARIES ON AFFINE ALGEBRAIC GROUPS (CHAPTERS 11-13)

The next three chapters are preliminary to the more detailed study of affine algebraic groups in the later chapters. They cover Tannakian duality, in which the category of representations of an algebraic group plays the role of the topological dual of a locally compact abelian group; Jordan decompositions; the Lie algebra of an algebraic group; the structure of finite algebraic groups.

C. SOLVABLE ALGEBRAIC GROUPS (CHAPTERS 14-17)

The next four chapters study solvable algebraic groups. Among these are the diagonalizable groups and the unipotent groups.

An algebraic group G is diagonalizable if every linear representation $r: G \rightarrow \mathrm{GL}_V$ of G is a direct sum of one-dimensional representations. In other words if, relative to some basis for V , $r(G)$ lies in the algebraic subgroup \mathbb{D}_n 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 V of G contains a nonzero fixed vector. This implies that, relative to some basis for V , $r(G)$ lies in the algebraic subgroup \mathbb{U}_n of strictly upper triangular matrices in GL_n .

Every smooth connected solvable algebraic group over a perfect field is an extension of a group of multiplicative type by a unipotent group.

D. REDUCTIVE GROUPS (CHAPTERS 18-25)

This is the heart of the book.

E. SURVEY CHAPTERS (CHAPTERS 26-27)

These describe the classification theorems of Satake-Selbach-Tits (the anisotropic kernel etc.) and the Galois cohomology of algebraic groups (classification of the forms of an algebraic group; description of the classical algebraic groups in terms of algebras with involution; etc.).

APPENDICES

In an appendix, we review the algebraic geometry needed.

Basic definitions and properties

Recall that k is a field, and that an algebraic k -scheme is a scheme of finite type over k . We often omit the k . Morphisms of k -schemes are required to be k -morphisms.

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 $m: G \times G \rightarrow G$ be a regular map. The pair (G, m) is an **algebraic group over k** if there exist regular maps

$$e: * \rightarrow G, \quad \text{inv}: G \rightarrow G \tag{1}$$

such that the following diagrams commute:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\text{id} \times m} & G \times G \\ \downarrow m \times \text{id} & & \downarrow m \\ G \times G & \xrightarrow{m} & G \end{array} \quad \begin{array}{ccc} * \times G & \xrightarrow{e \times \text{id}} & G \times G \xleftarrow{\text{id} \times e} G \times * \\ & \searrow \cong & \downarrow m \\ & & G \end{array} \tag{2}$$

$$\begin{array}{ccccc} G & \xrightarrow{(\text{inv}, \text{id})} & G \times G & \xleftarrow{(\text{id}, \text{inv})} & G \\ \downarrow & & \downarrow m & & \downarrow \\ * & \xrightarrow{e} & G & \xleftarrow{e} & * \end{array} \tag{3}$$

Here $*$ is the one-point variety $\text{Spm}(k)$. 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**.¹ A **homomorphism** $\varphi: (G, m) \rightarrow (G', m')$ of algebraic groups is a regular map $\varphi: G \rightarrow G'$ such that $\varphi \circ m = m' \circ (\varphi \times \varphi)$.

Similarly, an **algebraic monoid** over k is an algebraic scheme M over k together with regular maps $m: M \times M \rightarrow M$ and $e: * \rightarrow M$ such that the diagrams (2) commute. An algebraic group G is **trivial** if $e: * \rightarrow G$ is an isomorphism, and a homomorphism $\varphi: (G, m) \rightarrow (G', m')$ is **trivial** if it factors through $e': * \rightarrow G'$.

¹As we note elsewhere (p.3, p.5, 1.50, 5.40, p.515) in most of the current 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. In particular, nilpotents are not allowed.

For example,

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

becomes a group variety with the usual matrix multiplication,

$$(a_{ij}), (b_{ij}) \mapsto (c_{ij}), \quad c_{ij} = \sum_l a_{il} b_{lj}.$$

For many more examples, see Chapter 2.

DEFINITION 1.2. 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 that is a variety is called a **subgroup variety**.

HOMOGENEITY

1.3. 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 identify $X(k)$ with the set of points x of $|X|$ such that $\kappa(x) = k$. Let (G, m) be an algebraic group over k . The map $m(k): G(k) \times G(k) \rightarrow G(k)$ 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 $m: G \times G \rightarrow G$ 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*.²

1.4. 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 homogeneous³ when k is algebraically closed (but not in general otherwise; see 1.7).

ALGEBRAIC GROUPS AS FUNCTORS

Since we allow nilpotents in the structure sheaf, the points of an algebraic group with coordinates in a field, even algebraically closed, do not convey much information about the group. Thus, it is natural to consider its points in a k -algebra. Once we do that, the points capture *all* information about the algebraic group.

²Assume k is algebraically closed. The map $|m|: |G \times G| \rightarrow |G|$ is continuous, and $|G \times G| = |G| \times |G|$ as a set, but *not* as a topological space. The multiplication map $|G| \times |G| \rightarrow |G|$, i.e., $G(k) \times G(k) \rightarrow G(k)$, need not be continuous for the product topology.

³An algebraic scheme X over k is said to be homogeneous if the group of automorphisms of X (as a k -scheme) acts transitively on $|X|$.

1.5. An algebraic scheme X over k defines a functor

$$\tilde{X}: \text{Alg}_k^0 \rightarrow \text{Set}, \quad R \mapsto X(R),$$

and the functor $X \mapsto \tilde{X}$ is fully faithful (Yoneda lemma, A.28); in particular, \tilde{X} determines X uniquely up to a unique isomorphism. We say that a functor from k -algebras to sets is **representable** if it is of the form \tilde{X} .

Let (G, m) be an algebraic group over k . Then $R \mapsto (G(R), m(R))$ is a functor from k -algebras to groups whose underlying functor to sets is representable, and every such functor arises from an essentially unique algebraic group. Thus, to give an algebraic group over k amounts to giving a functor $\text{Alg}_k^0 \rightarrow \text{Grp}$ whose underlying functor to sets is representable by an algebraic scheme. We sometimes write \tilde{G} for G regarded as a functor.

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

From this perspective, SL_n is the algebraic group over k whose R -points are the $n \times n$ matrices with entries in R and determinant 1.

1.6. An algebraic subscheme H of an algebraic group G is an algebraic subgroup of G if and only if $H(R)$ is a subgroup of $G(R)$ for all k -algebras R . In more detail, assume that $H(R)$ is a subgroup of $G(R)$ for all (small) R ; then the Yoneda lemma (A.28) shows that the maps

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

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

1.7. Consider the functor of k -algebras

$$\mu_3: R \mapsto \{a \in R \mid a^3 = 1\}.$$

This is represented by $\text{Spm}(k[T]/(T^3 - 1))$, 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 $\text{Spm}(k)$ 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 $\text{Spm}(k)$ and $\text{Spm}(k[\zeta])$ where ζ is a primitive cube root of 1. In particular, $|\mu_3|$ is not homogeneous.

(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.

DENSITY OF POINTS

In general, the k -points of an algebraic group tell us little about the group, but sometimes they do. For example, a smooth algebraic group G over a separably closed field k is commutative if $G(k)$ is commutative (1.21).

1.8. Let X be an algebraic scheme over k , and let S be a subset of $X(k) \subset |X|$. We say that S is **schematically dense** in X if the family of homomorphisms

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

is injective. Let $S \subset X(k)$ be schematically dense in X :

- (a) if Z is a closed algebraic subscheme of X such that $Z(k)$ contains S , then $Z = X$;
- (b) if $u, v: X \rightarrow Y$ are regular maps from X to a separated algebraic scheme Y such that $u(s) = v(s)$ for all $s \in S$, then $u = v$.

If $S \subset X(k)$ is schematically dense in X , then S is dense in $|X|$, and the converse is true if X is reduced. A schematically dense subset remains schematically dense under extension of the base field. If an algebraic scheme X admits a schematically dense subset $S \subset X(k)$, then it is geometrically reduced. For a geometrically reduced scheme X , a subset of $X(k)$ is schematically dense in X if and only if it is dense in $|X|$. See (A.62) et seq.

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

- (a) If $G(k')$ is dense in G , then G is reduced. Conversely, if G is geometrically reduced, then $G(k')$ is dense in G if and only if it is dense in the topological space $|G_{k'}|$. (A.59, A.60).
- (b) If G is smooth, then $G(k')$ is dense in G whenever k' contains the separable closure of k (A.44).
- (c) $G(k)$ is dense in G if and only if G is reduced and $G(k)$ is dense $|G|$.

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.

1.10. Let R be a (finitely generated) k -algebra. Formally, an algebraic scheme over R is a scheme X equipped with a morphism $X \rightarrow \text{Spm } R$ of finite type. Less formally, we can think of X as 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 spectra finitely generated R -algebras A . A morphism of algebraic R -schemes $\varphi: X \rightarrow Y$ is a morphism of schemes compatible with the R -algebra structures, i.e., such that $\varphi_* \mathcal{O}_X \rightarrow \mathcal{O}_Y$ is a homomorphism of sheaves of R -algebras. Let G be an algebraic scheme over R and let $m: G \times G \rightarrow G$ be a morphism of R -schemes. The pair (G, m) is an **algebraic group over** R if there exist R -morphisms $e: \text{Spm}(R) \rightarrow G$ and $\text{inv}: G \rightarrow G$ such that the diagrams (2) and (3) 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.

b. Basic properties of algebraic groups

PROPOSITION 1.11. *The maps e and inv in (1.1) are uniquely determined by (G, m) . If $\varphi: (G, m_G) \rightarrow (H, m_H)$ is a homomorphism of algebraic groups, then $\varphi \circ e_G = e_H$ and $\varphi \circ \text{inv}_G = \text{inv}_H \circ \varphi$.*

PROOF. It suffices to prove the second statement. For a k -algebra R , the map $\varphi(R)$ is a homomorphism of abstract groups $(G(R), m_G(R)) \rightarrow (H(R), m_H(R))$, 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.28) now shows that the same is true for φ . \square

PROPOSITION 1.12. *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 $m \circ (\text{id} \times \text{inv}): G \times G \rightarrow G$ sending (g_1, g_2) to $g_1 g_2^{-1}$, and so it is closed. \square

Therefore “group variety” = “geometrically reduced algebraic group”.

COROLLARY 1.13. *Let G be an algebraic group over k , and let k' be a field containing k . If $G(k')$ is dense in G , then a homomorphism $G \rightarrow H$ of algebraic groups is determined by its action on $G(k')$.*

PROOF. Let φ, φ' be homomorphisms $G \rightarrow H$. Because H is separated, the subscheme Z of G on which they agree is closed (see A.37). If $\varphi(x) = \varphi'(x)$ for all $x \in G(k')$, then $Z(k') = G(k')$, and so $Z = G$. \square

Recall that an algebraic scheme over a field is a finite disjoint union of its (closed-open) connected components (A.14). For an algebraic group G , we let G° denote the connected component of G containing e , and we call it the **identity** (or **neutral**) **component** of G .

PROPOSITION 1.14. *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: for every field k' containing k ,*

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

In particular, G is connected if and only if $G_{k'}$ is connected; the algebraic group G° is geometrically connected; every connected algebraic group is geometrically connected.

For the proof, we shall need the following elementary lemma. Recall (A.84) that the set of connected components of an algebraic scheme X can be given the structure of a zero-dimensional algebraic variety $\pi_0(X)$. Moreover, $X \rightarrow \pi_0(X)$ is a regular map whose fibres are the connected components of X .

LEMMA 1.15. *Let X be a connected algebraic scheme over k such that $X(k) \neq \emptyset$. Then X is geometrically connected; moreover, for any algebraic scheme Y over k ,*

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

In particular, $X \times Y$ is connected if Y is connected.

PROOF. Because $\pi_0(X)$ is a zero-dimensional algebraic variety, it equals $\text{Spm}(A)$ for some étale k -algebra A (A.82). If A had more than one factor, $\mathcal{O}(X)$ would contain nontrivial idempotents, and X would not be connected. Therefore, A is a field containing k , and, because $X(k)$ is nonempty, it equals k . Now

$$\pi_0(X_{k^{\text{al}}}) \stackrel{\text{A.84}}{=} \pi_0(X)_{k^{\text{al}}} = \text{Spm}(k^{\text{al}}),$$

which shows that $X_{k^{\text{al}}}$ is connected, and

$$\pi_0(X \times Y) \stackrel{\text{A.84}}{\simeq} \pi_0(X) \times \pi_0(Y) \simeq \pi_0(Y),$$

as required. □

PROOF (OF 1.14). The identity component G° of G has a k -point, namely, e , and so $G^\circ \times G^\circ$ is a connected component of $G \times G$ (1.15). As m maps (e, e) to e , it maps $G^\circ \times G^\circ$ into G° . Similarly, inv maps G° into G° . Therefore G° is an algebraic subgroup of G . For any extension k' of k ,

$$(G \rightarrow \pi_0(G))_{k'} \simeq G_{k'} \rightarrow \pi_0(G_{k'})$$

(see A.84). As G° is the fibre over e , this implies that $(G^\circ)_{k'} \simeq (G_{k'})^\circ$. In particular, $(G^\circ)_{k^{\text{al}}} \simeq (G_{k^{\text{al}}})^\circ$, and so G° is geometrically connected. □

COROLLARY 1.16. *A connected algebraic group is irreducible.*

PROOF. It suffices to show that G is *geometrically* irreducible. Thus, we may suppose that k is algebraically closed, and hence that G is homogeneous (1.4). By definition, no irreducible component is contained in the union of the remainder. Therefore, there exists a point that lies on exactly one irreducible component. By homogeneity, all points have this property, and so the irreducible components are disjoint. As $|G|$ is connected, there must be only one, and so G is irreducible. □

SUMMARY 1.17. 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 example, the subscheme of \mathbb{A}^2 defined by the equation $XY = 0$ is connected but not irreducible (and hence is not the underlying scheme of an algebraic group).

PROPOSITION 1.18. *Let G be an algebraic group over k .*

- (a) *If G is reduced and k is perfect, then G is geometrically reduced (hence a group variety).*
- (b) *If G is geometrically reduced, then it is smooth (and conversely).*

PROOF. (a) This is true for every algebraic scheme (A.39).

(b) It suffices to show that $G_{k^{\text{al}}}$ is smooth, but some point of $G_{k^{\text{al}}}$ is smooth (A.52), and so every point is smooth because $G_{k^{\text{al}}}$ is homogeneous (1.4). □

Therefore

“group variety” = “smooth algebraic group”.

In characteristic zero, all algebraic groups are smooth (see 3.38 below for a proof in the affine case and 10.36 for the general case).

EXAMPLE 1.19. Let k be a nonperfect field of characteristic p , and let $a \in k \setminus k^p$. Let G be the algebraic subgroup of \mathbb{A}^1 defined by the equation

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

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

DEFINITION 1.20. An algebraic group (G, m) is **commutative** if $m \circ t = m$, where t is the transposition map $(x, y) \mapsto (y, x): G \times G \rightarrow G \times G$.

PROPOSITION 1.21. *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 $G(k^{\text{sep}})$ is commutative.*

PROOF. According to the Yoneda lemma (A.28), $m \circ t = m$ 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 $G(k^{\text{sep}})$ is commutative, then $m \circ t$ and m agree on $(G \times G)(k^{\text{sep}})$, which is dense in $G \times G$ (1.9). \square

PROPOSITION 1.22. *The following conditions on an algebraic group G are equivalent:*

- (a) G is smooth;
- (b) G° is smooth;
- (c) the local ring $\mathcal{O}_{G,e}$ is regular;
- (d) the tangent space $T_e(G)$ to G at e has dimension $\dim G$;
- (e) G is geometrically reduced;
- (f) for all k -algebras R and all ideals I in R such that $I^2 = 0$, the map $G(R) \rightarrow G(R/I)$ is surjective.

PROOF. (a) \implies (b) \implies (c) \implies (d): These implications are obvious (see A.48, A.51).

(d) \implies (a). The condition implies that the point e is smooth on G (A.51), and hence on $G_{k^{\text{al}}}$. By homogeneity (1.4), all points on $G_{k^{\text{al}}}$ are smooth, which means that G is smooth.

(a) \iff (e). This was proved in (1.18).

(a) \iff (f). This is a standard criterion for an algebraic scheme to be smooth (A.53). \square

COROLLARY 1.23. *For an algebraic group G ,*

$$\dim T_e(G) \geq \dim G,$$

with equality if and only if G is smooth.

PROOF. In general, for a point e on an algebraic k -scheme G with $\kappa(e) = k$, $\dim T_e(G) \geq \dim G$ with equality if and only if $\mathcal{O}_{G,e}$ is regular (A.48). But we know (1.22), that $\mathcal{O}_{G,e}$ is regular if and only if G is smooth. \square

c. Algebraic subgroups

For a closed subset S of an algebraic scheme X , we let S_{red} denote the reduced closed subscheme of X with $|S_{\text{red}}| = S$. A morphism $\phi: Y \rightarrow X$ factors through S_{red} if $|\phi|$ factors through S and Y is reduced. See A.25.

PROPOSITION 1.24. *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 $G_{\text{red}} \times G_{\text{red}}$ is reduced (A.39), and so the restriction of m to $G_{\text{red}} \times G_{\text{red}}$ factors through $G_{\text{red}} \hookrightarrow G$:

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

Similarly, e and inv induce maps $*$ $\rightarrow G_{\text{red}}$ and $G_{\text{red}} \rightarrow G_{\text{red}}$, and these make the diagrams (2, 3), p.17, commute for $(G_{\text{red}}, m_{\text{red}})$. \square

COROLLARY 1.25. *Let G be an algebraic group over k . If k is perfect, then G_{red} is a smooth algebraic subgroup of G .*

PROOF. Over a perfect field, reduced algebraic schemes are geometrically reduced (1.46), and so G_{red} is geometrically reduced, hence an algebraic subgroup of G , and hence smooth (1.22). \square

LEMMA 1.26. *Let G be an algebraic group over k . The Zariski closure \bar{S} of a (not abstract) subgroup S of $G(k)$ is a subgroup of $G(k)$.*

PROOF. For $a \in G(k)$, the map $x \mapsto ax: G(k) \rightarrow G(k)$ is a homeomorphism because its inverse is of the same form. For $a \in S$, we have $aS \subset S \subset \bar{S}$, and so $a\bar{S} = (aS)^- \subset \bar{S}$. Thus, for $a \in \bar{S}$, we have $Sa \subset \bar{S}$, and so $\bar{S}a = (Sa)^- \subset \bar{S}$. Hence $\bar{S}\bar{S} \subset \bar{S}$. The map $x \mapsto x^{-1}: G(k) \rightarrow G(k)$ is a homeomorphism, and so $(\bar{S})^{-1} = (S^{-1})^- = \bar{S}$. \square

PROPOSITION 1.27. *Every algebraic subgroup of an algebraic group is closed (in the Zariski topology).*

PROOF. Let H be an algebraic subgroup of an algebraic group G . If $H_{k^{\text{al}}}$ is closed in $G_{k^{\text{al}}}$ then H is closed in G (see A.10) and so we may suppose that k is algebraically closed. We may also suppose that H and G are reduced, because passing to the reduced algebraic subgroup doesn't change the underlying topological space. By definition, $|H|$ is locally closed, i.e., open in its closure S . Now S is a subgroup of $|G|$ (1.26), and it is a finite disjoint union of cosets of $|H|$. As each coset is open, it is also closed. Therefore H is closed in S , and so equals it. \square

COROLLARY 1.28. *The algebraic subgroups of an algebraic group satisfy the descending chain condition.*

PROOF. In fact, the closed subschemes of an algebraic scheme satisfy the descending chain condition (A.19). \square

COROLLARY 1.29. *Every algebraic subgroup of an affine algebraic group is affine.*

PROOF. Closed subschemes of affine algebraic schemes are affine (A.19). \square

COROLLARY 1.30. *Let H and H' be subgroup varieties of an algebraic group G over k . Then $H = H'$ if $H(k') = H'(k')$ for some field k' containing the separable closure of k .*

PROOF. The condition implies that

$$H(k') = (H \cap H')(k') = H'(k'). \quad (4)$$

But $H \cap H'$ is closed in H (1.27). As H is a variety, $H(k')$ is dense in H (A.61), and so (4) implies that $H \cap H' = H$. Similarly, $H \cap H' = H'$. \square

PROPOSITION 1.31. *Let G be an algebraic group over k , and let S be 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 (i.e., such that H is reduced and $H(k)$ is dense in $|H|$).*

PROOF. Let H denote the reduced closed subscheme of G such that $|H|$ is the closure of S in $|G|$. Then $S = G(k) \cap |H| = H(k)$. As H is reduced and $H(k)$ is dense in $|H|$, it is geometrically reduced (1.8). Therefore $H \times H$ is reduced, and so the map $m_G: H \times H \rightarrow G$ factors through H . Similarly, inv_G restricts to a regular map $H \rightarrow H$ and $*$ factors through H . Thus H is an algebraic subgroup of G . Also $H(k)$ is schematically dense in H because it is dense and H is reduced. Conversely, if H is a reduced algebraic subgroup of G such that $H(k)$ is dense in $|H|$, then the above construction starting with $S = H(k)$ gives back H . \square

COROLLARY 1.32. *Let G be an algebraic group over k , and let S be a closed subgroup of $G(k)$. There is a unique subgroup variety H of G such that $S = H(k)$. 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 proposition. \square

COROLLARY 1.33. *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 (abstract) subgroups of $G(k)$.*

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

DEFINITION 1.34. Let G be an algebraic group over k , and let S be 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 .

ASIDE 1.35. Let k be an infinite perfect field. Then $H(k)$ is dense in $|H|$ for any connected group variety H over k (cf. 3.26 below). Let G be an algebraic group over k ; then the map $H \mapsto H(k)$ is a bijection from the set of connected subgroup varieties of G to the set of closed subgroups of $G(k)$ whose closures in $|G|$ are connected.

PROPOSITION 1.36. *Let $(H_j)_{j \in J}$ be a family of algebraic subgroups of G . Then $H \stackrel{\text{def}}{=} \bigcap_{j \in J} H_j$ 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 (A.19). Moreover, for all k -algebras R ,

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

which is a subgroup of $G(R)$, and so H is an algebraic subgroup of G (1.6). 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,

$$\begin{aligned} H(R) &= \{g \in G(R) \mid f_R(g) = 0 \text{ for all } f \in \bigcup I(H_j)\} \\ &= \text{Hom}(\mathcal{O}(G)/I, R). \end{aligned} \quad \square$$

In fact, because of (1.28), every infinite intersection is equal to a finite intersection.

EXAMPLE 1.37. (a) Let $G = \text{GL}_p$ over a field of characteristic p . Then SL_p and the group H of scalar matrices in G are smooth subgroups of G , but $\text{SL}_p \cap H = \mu_p$ is not reduced.

(b) Let $G = \mathbb{G}_a^2$. Then $H_1 = \mathbb{G}_a \times \{0\}$ and $H_2 = \{(x, x^2 + ax^4)\}$ are smooth algebraic subgroups of G , but their intersection is not reduced.

NORMAL AND CHARACTERISTIC SUBGROUPS

DEFINITION 1.38. 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 k -algebras R .
- (b) An algebraic subgroup H of G is **characteristic** if $\alpha(H_R) = H_R$ for all 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 (i.e., as algebraic k -schemes equipped with a morphism to $\text{Spm}(R)$ (1.10)). Because of the Yoneda lemma (loc. cit.), the two interpretations give the same condition.

PROPOSITION 1.39. *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 $(G^\circ)_{k'} = (G_{k'})^\circ$, every automorphism of $G_{k'}$ fixing e maps $(G^\circ)_{k'}$ 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 $\alpha(G_R^\circ) \subset G_R^\circ$, and, because G_R° is an open subscheme of G_R , for this it suffices to show that $\alpha(|G_R^\circ|) \subset |G_R^\circ|$. Let $x \in |G_R^\circ|$, and let s be the image of x in $\text{Spm}(R)$. Then x lies in the fibre $G_{\kappa(s)}$ of G_R over s :

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

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

REMARK 1.40. 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 $H_R \subset \alpha(H_R) \subset H_R$.

NOTES. The definition of characteristic subgroup agrees with DG II, §1, 3.9, p.166. The proof that G° is characteristic is from DG II, §5, 1.1, p.234.

DESCENT OF SUBGROUPS

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

- (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 $\Gamma = \text{Gal}(k'/k)$. 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 $\mathcal{O}_{G'}$.
- (c) Let $k' = k^{\text{sep}}$. A subgroup variety H' is stable under the action of Γ on G' (hence defined over k) if and only if $H'(k')$ is stable under the action of Γ on $G(k')$.

Apply (A.55, A.56).

d. Examples

We give some examples to illustrate what can go wrong.

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

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

This is a connected group variety over k that becomes isomorphic to \mathbb{A}^1 over k^{al} , but $G(k)$ is finite (and so not dense in G). If $k = k_0(t)$, then $G(k) = \{e\}$ (Rosenlicht 1957, p.46).

1.43. Let k be nonperfect of characteristic p , and let $t \in k \setminus k^p$. Let G be the algebraic subgroup of \mathbb{A}^1 defined by the equation

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

Then G_{red} is not an algebraic group for any map $m: G_{\text{red}} \times G_{\text{red}} \rightarrow G_{\text{red}}$ (Exercise 2-5; SGA 3, VI_A, 1.3.2a).

1.44. Let k be nonperfect of characteristic $p \geq 3$, and let $t \in k \setminus k^p$. Let G be the algebraic subgroup of \mathbb{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).

1.45. We saw in (1.25) that G_{red} is an algebraic subgroup of G when k is perfect. However, it need not be normal even when G is connected. For examples, see (2.23) below.

1.46. The formation of G_{red} doesn't commute with change of the base field. For example, G may be reduced without $G_{k^{\text{al}}}$ being reduced (1.19). The best one can say is that the algebraic subgroup $(G_{k^{\text{al}}})_{\text{red}}$ of $G_{k^{\text{al}}}$ 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

$$k' = k^{p^{-\infty}} \stackrel{\text{def}}{=} \{x \in k^{\text{al}} \mid \exists m \geq 1 \text{ such that } x^{p^m} \in k\}.$$

Then k' is the smallest perfect subfield of k^{al} containing k , and $(G_{k'})_{\text{red}}$ is a smooth algebraic subgroup of $G_{k'}$ (1.25). The algebraic variety $(G_{k'})_{\text{red}}$ and its multiplication map are defined over a finite subextension of k' .

e. Kernels

Let $\varphi: G \rightarrow H$ be a homomorphism of algebraic groups, and let

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

Then $\text{Ker}(\varphi)$ is a closed subscheme of G such that

$$\text{Ker}(\varphi)(R) = \text{Ker}(\varphi(R))$$

for all k -algebras R . Therefore $\text{Ker}(\varphi)$ is an algebraic subgroup of G (see 1.6). It is called the **kernel** of φ . When G and H are affine, so also is $N = \text{Ker}(\varphi)$, and

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

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

EXAMPLE 1.47. Let \mathbb{G}_a be the algebraic group $(\mathbb{A}^1, +)$. The algebraic group G in (1.19) is the kernel of the homomorphism

$$\phi: \mathbb{G}_a \times \mathbb{G}_a \rightarrow \mathbb{G}_a, \quad (x, y) \mapsto y^p - ax^p.$$

It is not geometrically reduced, and so $\text{Ker}(\phi)$ is not a group variety even though ϕ is a homomorphism of group varieties. In the old terminology, one defined the kernel of ϕ to be the subgroup variety $G': Y = a^{\frac{1}{p}} X$ of $(\mathbb{G}_a \times \mathbb{G}_a)_{k^{\text{al}}}$, and observed that it is not defined over k (cf. Springer 1998, 12.1.6).

DEFINITION 1.48. A sequence of algebraic groups

$$e \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \rightarrow e \tag{5}$$

is **exact** if π is faithfully flat and i is an isomorphism of N onto the kernel of π . When (5) is exact, G is called an **extension** of Q by N .

We shall see (5.17) that, for group varieties (but not algebraic groups in general), a homomorphism $\pi: G \rightarrow Q$ is faithfully flat if it is surjective as a map of schemes, i.e., $|\pi|: |G| \rightarrow |Q|$ is surjective.

PROPOSITION 1.49. *A surjective homomorphism $\varphi: G \rightarrow H$ of group varieties is smooth if and only if $\text{Ker}(\varphi)$ is smooth.*

PROOF. We may suppose that k is algebraically closed. Recall (A.107), that a dominant map $\varphi: Y \rightarrow X$ of smooth algebraic varieties is smooth if and only if the maps $(d\varphi)_y: T_y(Y) \rightarrow T_{\varphi(y)}(X)$ on the tangent spaces are surjective for all $y \in Y$.

Let $N = \text{Ker}(\varphi)$. 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

$$0 \rightarrow T_e(N) \rightarrow T_e(G) \rightarrow T_e(H).$$

The fibres of φ are the cosets of N in G , which all have the same dimension, and so

$$\dim N = \dim G - \dim H$$

(A.99). On the other hand (1.23),

$$\begin{aligned} \dim G &= \dim T_e(G) \\ \dim H &= \dim T_e(H) \\ \dim T_e(N) &\geq \dim N, \text{ with equality if and only if } N \text{ is smooth.} \end{aligned}$$

Thus, we see that $\dim T_e(N) = \dim N$ (and N is smooth) if and only if $(d\varphi)_e: T_e(G) \rightarrow T_e(H)$ is surjective. It remains to note that, by homogeneity (1.4), if $(d\varphi)_e$ is surjective, then $(d\varphi)_g$ is surjective for all $g \in G$. \square

NOTES. There is the more precise statement. Let $\varphi: G \rightarrow H$ be a homomorphism of algebraic groups over k . Suppose that G is smooth. The following conditions are equivalent:

- (a) $\text{Lie}(\varphi): \mathfrak{g} \rightarrow \mathfrak{h}$ is surjective;
- (b) $\text{Ker}(\varphi)$ is smooth and $\varphi(G)_{\text{red}}$ is open in H ;
- (c) H is smooth and φ is smooth.

Proof to be added (DG II, §5, 5.3, p.250).

ASIDE 1.50. Let $\varphi: G \rightarrow H$ be a homomorphism of group varieties over k . Borel 1991 et al. define the kernel of φ to be the subgroup variety $\text{Ker}(\varphi_{k^{\text{al}}})_{\text{red}}$ of $G_{k^{\text{al}}}$, which “need not be defined over k ” (see 1.47). Springer 1998, 12.1.3 writes:

Let $\phi: G \rightarrow G'$ be a k -homomorphism of group varieties over k . If k is perfect or the tangent map $(d\phi)_e$ is surjective, then the “kernel” is defined over k .

In the first case, $\text{Ker}(\phi)_{\text{red}}$ is geometrically reduced (A.39), and so $\text{Ker}(\phi_{k^{\text{al}}})_{\text{red}} = (\text{Ker}(\phi)_{\text{red}})_{k^{\text{al}}}$; in the second case, $\text{Ker}(\phi)$ is smooth, and so $\text{Ker}(\phi_{k^{\text{al}}})_{\text{red}} = \text{Ker}(\phi)_{k^{\text{al}}}$.

ASIDE 1.51. In the language of EGA/SGA, our algebraic groups over k are algebraic group schemes over k , i.e., group schemes over k whose underlying scheme is of finite type over k (SGA 3, VI_A, p.295). Some of the above results hold without finiteness conditions. For example, group schemes over a field are always separated (ibid. 0.3, p.296). For a quasicompact morphism $u: G \rightarrow H$ of group schemes locally of finite type over k , the following conditions are equivalent:

- (a) u is a closed immersion;
- (b) u is a monomorphism;
- (c) $\text{Ker}(u)$ is trivial;

in particular, every subgroup scheme of H is closed (SGA 3, VI_B, 1.4.2, p.341). However, let $(\mathbb{Z})_k$ denote the constant group scheme over a field k of characteristic zero (cf. 2.3 below). The obvious homomorphism of $(\mathbb{Z})_k \rightarrow \mathbb{G}_{a,k}$ of group schemes over k has trivial kernel but is not a closed immersion (ibid. 1.4.3, p.341). As another example, over an algebraically closed field k there is a zero-dimensional (nonaffine) reduced group scheme G with $G(k) = k$; the obvious homomorphism $k \rightarrow \mathbb{G}_a$ of group schemes is both mono and epi, but it is not an isomorphism.

f. Group actions

By a functor (resp. group functor) 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 $\mu: G \times X \rightarrow X$ 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

$$\mu: G \times X \rightarrow X$$

such that the following diagrams commute:

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{\text{id} \times \mu} & G \times X \\ \downarrow m \times \text{id} & & \downarrow \mu \\ G \times X & \xrightarrow{\mu} & X \end{array} \quad \begin{array}{ccc} * \times X & \longrightarrow & G \times X \\ & \searrow \simeq & \downarrow \mu \\ & & X. \end{array}$$

Because of the Yoneda lemma (A.28), 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 $\mu(g, x)$.

Let $\mu: G \times X \rightarrow X$ be an action of an algebraic group G on an algebraic scheme X . The following diagram commutes

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

and both horizontal maps are isomorphisms. It suffices to check this on the R -points (R a k -algebra), where it is obvious (the inverse of the top map is $(g, x) \mapsto (g, g^{-1}x)$). Therefore, the map $\mu: G \times X \rightarrow X$ is isomorphic to the projection map p_2 . It follows that μ is faithfully flat, and that it is smooth (resp. finite) if G is smooth (resp. finite).

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

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

is defined to be the restriction of μ to $G \times \{x\} \simeq G$. We say that G acts **transitively** on X if $G(k^{\text{al}})$ acts transitively on $X(k^{\text{al}})$, in which case the orbit map μ_x is surjective for all $x \in X(k)$ (because it is on k^{al} -points).

PROPOSITION 1.52. *Let G be an algebraic group. Let X and Y be nonempty algebraic schemes on which G acts, and let $f: X \rightarrow Y$ be an equivariant map.*

- (a) If Y is reduced and G acts transitively on Y , then f is faithfully flat.
 (b) If G acts transitively on X , then the set $f(X)$ is locally closed in Y .
 (c) If X is reduced and G acts transitively on X , 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 .

Because the set $f(X)$ is locally closed in Y , there exists a unique reduced subscheme $f(X)_{\text{red}}$ of Y having it as its underlying set.

PROOF. (a) As G acts transitively on Y and X is nonempty, the map $f(k^{\text{al}})$ 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.88), 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. As it is also surjective, it is faithfully flat.

(b) Because $f(X)$ is the image of a regular map, it contains a dense open subset U of its closure $\overline{f(X)}$ (A.59). We shall show that $f(X)$ is open in $\overline{f(X)}$ (hence locally closed). Regard $\overline{f(X)}$ as a reduced algebraic subscheme of Y , and let $y \in f(X)$. If $y = gu$ for some $(g, u) \in G(k) \times U(k)$, then $y \in gU \subset f(X)$, and so y is an interior point of $\overline{f(X)}$. In general, there exists a finite field extension K of k , a point y' of $f(X)(K)$ lying over y , and a $(g, u) \in G(K) \times U(K)$ such that $gu = y'$. Now $y' \in gU_K \subset f(X_K)$, and so y lies in the image of gU_K in $f(X)$, which is open,⁴ and so again y is an interior point of $\overline{f(X)}$.

(c) Because X is reduced, f factors through $f(X)_{\text{red}}$, and so the first part of the statement follows from (a) and (b). For the second part, let $Z = f(X)_{\text{red}}$. As Z is reduced, it suffices to show that $Z(R)$ is stable under the action of $G(R)$ when R is a field containing k , but this is obvious. \square

g. 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 $\text{Alg}_k^0 \rightarrow \text{Set}$.

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

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

A homomorphism of k -algebras $R \rightarrow R'$ defines a map $Z(R) \rightarrow Z(R')$, 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 $A = k[T_1, \dots, T_n]$, then $h^A = \mathbb{A}^n$, and the set of zeros of $\mathfrak{a} = (f_1, \dots, f_m)$ in $h^A(R)$ is the set of zeros in R^n of the polynomials $f_i \in k[T_1, \dots, T_n]$

1.54. Let Z be a subfunctor of a functor X . From a map of functors $f: h^A \rightarrow X$, we obtain a subfunctor $h^{-1}(Z) \stackrel{\text{def}}{=} Z \times_X h^A$ 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 $f: h^A \rightarrow X$, the subfunctor $f^{-1}(Z)$ of h^A is the functor of zeros of some ideal \mathfrak{a} in A .

⁴The map $X_K \rightarrow X$, being flat, is open (A.87).

Later in this chapter (§1k), we shall prove the following statements.

1.55. Let X be an algebraic scheme over k . The closed subfunctors of h_X are exactly those of the form h_Z with Z a closed subscheme of X (1.77). Recall that h_X denotes the functor $R \rightsquigarrow X(R)$.

1.56. Let Z be a closed subfunctor of a functor X . For every map $Y \rightarrow X$ of functors, $Z \times_X Y$ is a closed subfunctor of Y (1.78).

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 $\text{Alg}_R^0 \rightarrow \text{Alg}_k^0$. For functors Y and X , we let $\underline{\text{Mor}}(Y, X)$ denote the functor

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

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

1.57. Let Z be a subfunctor of a functor X , and let Y be an algebraic scheme. If Z is closed in X , then $\underline{\text{Mor}}(Y, Z)$ is closed in $\underline{\text{Mor}}(Y, X)$ (1.82).

h. Transporters

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

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

Here Y_R and Z_R can be interpreted as algebraic R -schemes (A.32) or as functors on the category of small R -algebras. Because of the Yoneda lemma (A.32), the different interpretations give the same condition. Explicitly,

$$gY_R \subset Z_R \iff gY(R') \subset Z(R') \text{ for all (small) } R\text{-algebras } R'.$$

Note that, because $G(R)$ is a group,

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

PROPOSITION 1.58. If Z is closed in X , then $T_G(Y, Z)$ is represented by a closed subscheme of G .

PROOF. Consider the diagram:

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

The map b is defined by the action of G on X , and c is defined by the inclusion of Z into X . According to (1.57), $\underline{\text{Mor}}(Y, Z)$ is a closed subfunctor of $\underline{\text{Mor}}(Y, X)$, and so $T_G(Y, Z)$ is a closed subfunctor of X (1.56). Therefore it is represented by a closed subscheme of G (1.55). \square

i. Normalizers

Let G be an algebraic group over k .

PROPOSITION 1.59. *Let H be an algebraic subgroup of G . There is a unique algebraic subgroup $N_G(H)$ of G such that*

$$N_G(H)(R) = \{g \in G(R) \mid gH_Rg^{-1} = H_R\}$$

for all k -algebras R .

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

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

PROOF. The uniqueness follows from the Yoneda lemma (A.28). 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 (1.6). But, when we let G act on itself by inner automorphisms,

$$N = T_G(H, H),$$

and so this follows from (1.58). □

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 1.60. *Let H be a subgroup variety of G , and let k' be a field containing k . If $H(k')$ 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 $x \mapsto gxg^{-1}: G \rightarrow G$. Then ${}^g H \cap H$ is an algebraic subgroup of H such that

$$({}^g H \cap H)(k') = {}^g H(k') \cap H(k') = H(k').$$

As $H(k')$ is dense in H , this implies that ${}^g H \cap H = H$, and so ${}^g H = H$. In particular, $gH(R)g^{-1} = H(R)$ for all k -algebras R , and so $g \in N_G(H)(k)$. The converse is obvious. □

COROLLARY 1.61. *Let H be an algebraic subgroup of a smooth algebraic group G . If for some separably closed field k' containing k , $H_{k'}$ is stable under all inner automorphisms $\text{inn}(g)$ with $g \in G(k')$, then H is normal in G .*

PROOF. Let $N = N_G(H)$. Then N is an algebraic subgroup of G , and the condition implies that $N(k') = G(k')$. As G is smooth, this implies that $N = G$ (1.9b). □

COROLLARY 1.62. *Let H be a subgroup variety of a group variety G . If $H(k^{\text{sep}})$ is normal in $G(k^{\text{sep}})$, then H is normal in G .*

PROOF. Because H is a variety, $H(k^{\text{sep}})$ is dense in H , and so (1.60) shows that $N_G(H)(k^{\text{sep}}) = G(k^{\text{sep}})$. Because G is a variety, this implies that $N_G(H) = G$. □

COROLLARY 1.63. *Let H be a normal algebraic subgroup of a group variety G . If H_{red} is a subgroup variety of G , then it is normal in G .*

PROOF. As H is normal, $H(k^{\text{sep}})$ is normal in $G(k^{\text{sep}})$, but $H(k^{\text{sep}}) = H_{\text{red}}(k^{\text{sep}})$ and so we can apply (1.62). \square

The examples in (1.45) show that it is necessary to take G to be a group variety in (1.62) and (1.63). Specifically, when k is perfect, G_{red} is a subgroup variety of G and $G_{\text{red}}(k) = G(k)$, but G_{red} need not be normal.

DEFINITION 1.64. 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 $G_{k'}$.

COROLLARY 1.65. Let N be a normal subgroup variety of a group variety G , and let H be a subgroup variety of N . If H is weakly characteristic in N , then it is normal in G .

PROOF. By hypothesis, $H_{k^{\text{sep}}}$ is stable under all automorphisms of $N_{k^{\text{sep}}}$, in particular, by those induced by an inner automorphism of $G_{k^{\text{sep}}}$. Therefore $H(k^{\text{sep}})$ is normal in $G(k^{\text{sep}})$, and so we can apply (1.62). \square

EXAMPLE 1.66. A weakly characteristic algebraic subgroup need not be characteristic. For example, every commutative algebraic group G over a perfect field contains a greatest unipotent subgroup U (17.17 below). Clearly $\alpha U = U$ for all automorphisms α of G . The formation of U commutes with extensions of the base field, and so U is even weakly characteristic. However, it need not be characteristic (17.22 below).

j. Centralizers

Let G be an algebraic group over k .

PROPOSITION 1.67. Let H be an algebraic subgroup of G . There is a unique algebraic subgroup $C_G(H)$ of G such that, for all k -algebras R ,

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

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

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

Recall (1.12) that the diagonal Δ_H is closed in $H \times H$, and hence in $G \times G$. Now

$$C = T_G(H, \Delta_H),$$

which is represented by a closed subscheme G (by 1.58). \square

The algebraic subgroup $C_G(H)$ is called the **centralizer** of H in G . 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 $C_G(G)$.

EXAMPLE 1.68. Let k be a field of characteristic $2 \neq 0$, and let $a \in k \setminus k^2$. Let $G = \text{SL}_4$, and let

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

Then $C_G(h)$ 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.

PROPOSITION 1.69. *Let H be a subgroup variety of G , and let k' be a field containing k . If $H(k')$ is dense in H , then $C_G(H)(k)$ consists of the elements of $G(k')$ centralizing $H(k')$ in $G(k')$.*

PROOF. Let n be an element of $G(k)$ centralizing $H(k')$. Then $n \in N_G(H)(k)$ (1.60), and the homomorphism $x \mapsto nxn^{-1}: H \rightarrow H$ 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 n centralizes H . \square

COROLLARY 1.70. *Let H be a subgroup variety of a group variety G . If $H(k^{\text{sep}})$ is contained in the centre of $G(k^{\text{sep}})$, then H is contained in the centre of G .*

PROOF. We have to show that $C_G(H) = G$. For this, we may replace k with k^{sep} (1.41a), and so assume that k is separably closed. Because H is a variety, $H(k)$ is dense in H , and so (1.69) shows that $C_G(H)(k) = G(k)$. Because G is a group variety, this implies that $C_G(H) = G$ (1.9d). \square

COMPLEMENTS

1.71. 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 .⁵ Similarly, $C_G(H)$ and $N_G(H)$ need not be smooth, even when H and G are. For some situations where they are smooth, see 16.23 and 14.66 below.

1.72. Assume that k is perfect, and let H be a subgroup variety of a group variety G . Then

$$C_G(H)_{\text{red}}(k^{\text{al}}) = C_G(H)(k^{\text{al}}) \stackrel{(1.69)}{=} C_{G(k^{\text{al}})}(H(k^{\text{al}})),$$

and so $C_G(H)_{\text{red}}$ is the unique subgroup variety C of G such that $C(k^{\text{al}})$ is the centralizer of $H(k^{\text{al}})$ in $G(k^{\text{al}})$. Similarly, $N_G(H)_{\text{red}}$ is the unique subgroup variety N of G such that $N(k^{\text{al}})$ is the normalizer of $H(k^{\text{al}})$ in $G(k^{\text{al}})$.

1.73. When k has characteristic zero, all algebraic groups over k are smooth (3.38, 10.36 below). It follows from (1.72) that, over a field of characteristic zero, $C_G(H)$ is the unique algebraic subgroup C of G such that $C(k^{\text{al}})$ is the centralizer of $H(k^{\text{al}})$ in $G(k^{\text{al}})$, and $N_G(H)$ is the unique algebraic subgroup N of G such that $N(k^{\text{al}})$ is the normalizer of $H(k^{\text{al}})$ in $G(k^{\text{al}})$.

1.74. Let H be a subgroup variety of a group variety G . In Borel 1991, p.52, the normalizer N of H in G is defined to be the subgroup variety $N_{G_{k^{\text{al}}}}(H_{k^{\text{al}}})_{\text{red}}$ of $G_{k^{\text{al}}}$, which “need not be defined over k ”. The centralizer is similarly defined to be a subgroup variety of $G_{k^{\text{al}}}$.

⁵For another example, let G , φ , and N be as in (8.43) below, and let $H = \mathbb{G}_a \rtimes_{\varphi} G$. Then $Z(H) = N$, which is not reduced.

k. Closed subfunctors: proofs

In this section, “functor” means “functor $\text{Alg}_k^0 \rightarrow \text{Set}$ ” unless indicated otherwise.

CLOSED SUBFUNCTORS

LEMMA 1.75. *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 $f: h^A \rightarrow Y$, the subfunctor $f^{-1}(Z)$ of h^A is represented by a quotient of A .*

PROOF. This is a restatement of the definition. \square

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

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

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

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

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 1.76. Let B be a k -algebra, and let Z be a subfunctor of $X = h^B$. For the identity map $f: h^B \rightarrow X$, $f^{-1}(Z) = Z$. 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

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

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

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

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 1.77. 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 1.76). 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 affines U in X . Now $Z = h_{Z'}$ where Z' is the closed subscheme of X defined by \mathcal{I} (A.19).

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

PROPOSITION 1.78. *Let Z be a closed subfunctor of a functor X . For every map $Y \rightarrow X$ of functors, $Z \times_X Y$ is a closed subfunctor of Y .*

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

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

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

RESTRICTION OF SCALARS

LEMMA 1.79. *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

$$b = \sum e_i \otimes a_i, \quad a_i \in A,$$

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 $\mathfrak{a} \supset \mathfrak{a}_0$. \square

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

$$R \mapsto X(B \otimes R): \text{Alg}_k^0 \rightarrow \text{Set}.$$

PROPOSITION 1.80. *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 all homomorphisms $\varphi: A \rightarrow R$,

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

i.e.,

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

We can 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 $\varphi': B \otimes A \rightarrow R'$,

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

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

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

According to (1.79), there exists an ideal \mathfrak{a} in A such that an ideal \mathfrak{a}' of A contains \mathfrak{a} if and only if $\mathfrak{b} \subset B \otimes \mathfrak{a}'$. On taking $\mathfrak{a}' = \text{Ker } \varphi$, we find that

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

Now

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

as required. \square

APPLICATION TO $\underline{\text{Mor}}$

LEMMA 1.81. *An intersection of closed subfunctors of a functor is closed.*

PROOF. Let $Z_i, i \in I$, be closed subfunctors of X , and let $f: h^A \rightarrow X$ be 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 $\mathfrak{a} = \sum_{i \in I} \mathfrak{a}_i$. \square

THEOREM 1.82. *Let Z be a subfunctor of a functor X , and let Y be an algebraic scheme. If Z is closed in X , then $\underline{\text{Mor}}(Y, Z)$ is closed in $\underline{\text{Mor}}(Y, X)$.*

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 ,

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

and so $\underline{\text{Mor}}(Y, X) = X_*$. In this case, the theorem is proved in (1.80).

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

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

in which ρ_i is the restriction map. We know that $\underline{\text{Mor}}(Y_i, Z)$ is closed in $\underline{\text{Mor}}(Y_i, X)$, hence $\rho_i^{-1}(\underline{\text{Mor}}(Y_i, Z))$ is closed in $\underline{\text{Mor}}(Y, X)$ (1.78), and so (see 1.81) it remains to show that

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

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

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

defined by the evaluation map

$$\mu: \underline{\text{Mor}}(Y, X) \times Y \rightarrow X$$

factors through Z . For each i , we know that $H_i \times Y_i \rightarrow X$ 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 $h^A \rightarrow X$. Then $\mu^{-1}(Z)$ is a closed subscheme of $\underline{\text{Mor}}(Y, X) \times Y$ containing $(\bigcap_i H_i) \times Y_i$ for all i , and hence containing $(\bigcap_i H_i) \times Y$. Since this holds for all maps $h^A \rightarrow X$, it follows that $\mu^{-1}(Z) \supset (\bigcap_i H_i) \times Y$. \square

ASIDE 1.83. In this section, we used that k is a field only to deduce in the proof of (1.79) that B is free as a k -module. Thus, 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 let Z be a closed subfunctor of X ; let Y be a locally free scheme over k , i.e., such that Y admits a covering by open affines Y_i for which $\mathcal{O}(Y_i)$ is a free k -module; then $\underline{\text{Mor}}(Y, Z)$ is a closed subfunctor of $\underline{\text{Mor}}(Y, X)$. See DG I, §2, 7.5, p. 64; also Jantzen 1987, 1.15.

Examples; some basic constructions

Let G be an algebraic group over k . Then $\mathcal{O}(G)$ is a k -algebra. When G is affine, $G = \text{Spec}(\mathcal{O}(G))$, and we call $\mathcal{O}(G)$ the *coordinate ring* of G . When G is embedded as a closed subvariety of some affine space \mathbb{A}^n , $\mathcal{O}(G)$ 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

$$\Delta: \mathcal{O}(G) \rightarrow \mathcal{O}(G) \otimes \mathcal{O}(G)$$

corresponding to $m: G \times G \rightarrow G$ is called the *comultiplication map*.

At the opposite extreme, when $\mathcal{O}(G) = k$, the algebraic group G is said to be *anti-affine*. For example, if G is complete as an algebraic scheme, then it is anti-affine.

Later (10.33), 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 algebraic groups and anti-affine algebraic groups, and we describe some methods of constructing algebraic groups.

Recall (1.5) 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. 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 $x \in F(R)$, there is a unique homomorphism $A \rightarrow R$ such that $F(A) \rightarrow F(R)$ sends a to x .

a. Affine algebraic groups

2.1. The *additive group* \mathbb{G}_a is the functor $R \mapsto (R, +)$. 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 $r \in \mathbb{G}_a(R)$, there is a unique homomorphism $k[T] \rightarrow R$ such that the map $\mathbb{G}_a(k[T]) \rightarrow \mathbb{G}_a(R)$ sends T to r .

The comultiplication map is the k -algebra homomorphism $\Delta: k[T] \rightarrow k[T] \otimes k[T]$ such that

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

2.2. The *multiplicative group* \mathbb{G}_m is the functor $R \mapsto (R^\times, \cdot)$. 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 $\Delta: k[T, T^{-1}] \rightarrow k[T, T^{-1}] \otimes k[T, T^{-1}]$ 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.,

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

Then

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

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

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

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 ,

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

and the comultiplication map sends $k_a \otimes k_b$ to k_{ab} .

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 $k \rightarrow k \otimes k$. We often write e for the trivial algebraic group.

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. When k has characteristic $p \neq 0$, α_{p^m} is the functor $R \rightsquigarrow \{r \in R \mid r^{p^m} = 0\}$. To show that this set is a subgroup of $(R, +)$, use that $(x + y)^p = x^p + y^p$ 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 , V_a denotes the functor $R \rightsquigarrow R \otimes V$.¹ Assume now that V is finite dimensional, and let V^\vee be the dual vector space. Then²

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

Therefore V_a is an algebraic group. The choice of a basis for V determines an isomorphism $V_a \rightarrow \mathbb{G}_a^{\dim V}$.

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

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

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

¹Our notation V_a is that of DG, II, §1, 2.1, p.147. Many other notations are used, for example, $\mathbf{W}(V)$ (SGA 3, I, 4.6.1, p. 24), or V_a (Jantzen 1987, 2.2.)

²Recall that, for a finite-dimensional k -vector space V , the symmetric algebra $\mathrm{Sym}(V)$ on V has the following universal property: every k -linear map $V \rightarrow A$ from V to a k -algebra A extends uniquely to a k -algebra homomorphism $\mathrm{Sym}(V) \rightarrow A$.

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

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

and the universal element in $\mathrm{GL}_n(k[T_{11}, \dots])$ is the matrix $(T_{ij})_{1 \leq i, j \leq n}$:

for every $(a_{ij})_{1 \leq i, j \leq n} \in \mathrm{GL}_n(R)$, there is a unique homomorphism $k[T_{11}, \dots] \rightarrow R$ such that the map $\mathrm{GL}_n(k[T_{11}, \dots]) \rightarrow \mathrm{GL}_n(R)$ sends (T_{ij}) to (a_{ij}) .

The comultiplication map is the k -algebra homomorphism

$$\Delta: k[T_{11}, \dots] \rightarrow k[T_{11}, \dots] \otimes k[T_{11}, \dots]$$

such that

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

Symbolically,

$$(\Delta T_{ij})_{i,j} = (T_{il})_{i,l} \otimes (T_{lj})_{l,j}.$$

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

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

When V has finite dimension n , the choice of a basis for V determines an isomorphism $\mathrm{GL}_V \approx \mathrm{GL}_n$, and so GL_V is an algebraic group in this case.

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),

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

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

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

2.10. 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 . See Chapter 14.

2.11. An algebraic group G 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. In characteristic zero, a vector group U is canonically isomorphic to $\mathrm{Lie}(U)_a$; in particular, it has an action of k . See Chapter 15.

2.12. A k -algebra A is **finite** if it is finitely generated as a k -vector space. An algebraic k -scheme X is **finite** over k if $\mathcal{O}_X(U)$ is a finite k -algebra for every open affine U in X . An algebraic group G over k is **finite** if it is finite as a scheme over k .

The following conditions on an algebraic scheme over k are equivalent: (a) X is finite over k ; (b) X is affine and $\mathcal{O}_X(X)$ is a finite k -algebra; (c) $|X|$ is finite and discrete. In particular, we see that every finite algebraic group is affine. The dimension of $\mathcal{O}(G)$ as a k -vector space is called the **order** $o(G)$ of G . See Chapter 13.

2.13. A k -algebra A is **étale** if it is a finite product of separable field extensions of k . A finite algebraic scheme X over k is **étale** if $\mathcal{O}(X)$ is an étale k -algebra. An algebraic group G over k is **étale** if it is étale as a scheme over k .

The following conditions on a scheme X finite over k are equivalent: (a) X is étale over k ; (b) X is smooth over k ; (c) X is geometrically reduced; (d) X is an algebraic variety. Thus, the étale algebraic groups over k are exactly the finite group varieties over k .

Let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. The functor $X \mapsto X(k^{\text{sep}})$ is an equivalence from the category of étale algebraic schemes over k to the category of finite sets endowed with a continuous action of Γ (discrete topology on $X(k^{\text{sep}})$; Krull topology on Γ) (see my Field Theory notes, Chapter 8). Correspondingly, the functor $G \mapsto G(k^{\text{sep}})$ is an equivalence from the category of étale algebraic groups over k to the category of finite groups endowed with a continuous action of Γ by group homomorphisms. See Chapter 13.

b. Anti-affine algebraic groups

Later (10.34) we shall show that every anti-affine algebraic group is both connected and smooth. In particular, we need only consider anti-affine group varieties.

Clearly, a complete connected group variety G has $\mathcal{O}(G) = k$. Such a group variety is called an **abelian variety**. Abelian varieties are commutative and projective. The abelian varieties of dimension 1 are exactly the elliptic curves, i.e., curves of genus 1 equipped k -point. 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 largely ignore here. See, for example, Milne 1986 and Mumford 2008.

In the remainder of this section, we describe the classification of anti-affine algebraic groups in terms of abelian varieties — it can be skipped.

Consider an extension

$$e \rightarrow T \rightarrow G \rightarrow A \rightarrow e \tag{9}$$

of an abelian variety A by a torus T . The group of characters $X^*(T)$ of T is defined to be $\text{Hom}(T_{k^{\text{sep}}}, \mathbb{G}_m)$. By definition, the torus T becomes isomorphic to \mathbb{G}_m^r ($r = \dim T$) over k^{sep} , and so

$$X^*(T) \approx \text{End}(\mathbb{G}_m)^r \simeq \mathbb{Z}^r.$$

From a character χ of T , we obtain by extension of scalars and pushout from (9), an extension

$$e \rightarrow \mathbb{G}_m \rightarrow G_\chi \rightarrow A_{k^{\text{sep}}} \rightarrow e$$

over k^{sep} , and hence an element

$$c(\lambda) \in \text{Ext}^1(A_{k^{\text{sep}}}, \mathbb{G}_m).$$

Let $A^\vee = \text{PicVar}(A)$ be the dual abelian variety to A . Then

$$\text{Ext}^1(A_{k^{\text{sep}}}, \mathbb{G}_m) \simeq A^\vee(k^{\text{sep}})$$

(e.g., [Milne 1986](#), 11.3), and so the extension (9) gives rise to a homomorphism $c: X^*(T) \rightarrow A^\vee(k^{\text{sep}})$.

PROPOSITION 2.14. *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

$$\begin{array}{ccccccc} e & \longrightarrow & H^1(A, \mathcal{O}_A)_a^\vee & \longrightarrow & E(A) & \longrightarrow & A \longrightarrow e \\ & & \downarrow \gamma & & \downarrow & & \parallel \\ e & \longrightarrow & U & \longrightarrow & G & \longrightarrow & A \longrightarrow e \end{array}$$

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

$$e \rightarrow U \times T \rightarrow G \rightarrow A \rightarrow e$$

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 2.15. *Let A be an abelian variety over a field k .*

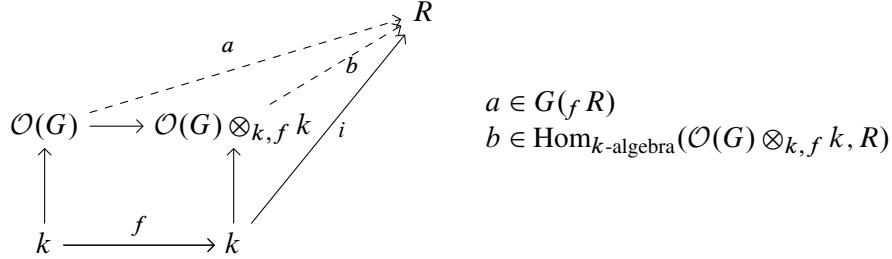
- (a) *If k has nonzero characteristic, then the isomorphism classes of anti-affine groups over A are in one-to-one correspondence with the free abelian subgroups Λ of $A^\vee(k^{\text{sep}})$ of finite rank stable under the action of $\text{Gal}(k^{\text{sep}}/k)$.*
- (b) *If k has characteristic zero, 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](#). □

c. Homomorphisms of algebraic groups

2.16. Let k be a field of characteristic $p \neq 0$. For a k -algebra R , we let f_R denote the homomorphism $a \mapsto a^p: R \rightarrow R$. When $R = k$, we omit the subscript on f . For a k -algebra $k \xrightarrow{i} R$, we let f_R denote the ring R regarded as a k -algebra by means of the map

$k \xrightarrow{f} k \xrightarrow{i} R$. Let G be an algebraic group over k (not necessarily affine), and let $G^{(p)}$ denote the functor $R \mapsto G({}_f R)$. When G is affine, this is represented by $\mathcal{O}(G) \otimes_{k, f} k$ (tensor product of $\mathcal{O}(G)$ with k relative to the map $f: k \rightarrow k$),



and so it is again an affine algebraic group. In the general case, we can cover G with open affines, and again deduce that $G^{(p)}$ is an algebraic group. The k -algebra homomorphism $f_R: R \rightarrow {}_f R$ defines a homomorphism $G(R) \rightarrow G^{(p)}(R)$, which is natural in R , and so arises from a homomorphism $F: G \rightarrow G^{(p)}$ of algebraic groups, called the **Frobenius map**. When G is affine, it corresponds to the homomorphism of Hopf algebras

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

Similarly we define $F^n: G \rightarrow G^{(p^n)}$ by replacing p with p^n . Then F^n is the composite

$$G \xrightarrow{F} G^{(p)} \xrightarrow{F} \dots \xrightarrow{F} G^{(p^n)}.$$

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

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

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

2.17. A homomorphism $\alpha: G \rightarrow H$ of connected group varieties is an **isogeny** if it is surjective and its kernel is finite. An isogeny is **separable** if its kernel is étale (equivalently, $(d\alpha)_e: T_e G \rightarrow T_e H$ is an isomorphism). An isogeny is **central** if its kernel is contained in the centre of G .

d. Products

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

$$R \mapsto G_1(R) \times \dots \times G_n(R).$$

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

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

2.19. Let $G_1 \rightarrow H \leftarrow G_2$ be homomorphisms 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:

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

For example, 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 .

e. Semidirect products

DEFINITION 2.20. 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 $(n, q) \mapsto nq: N(R) \times Q(R) \rightarrow G(R)$ is a bijection of sets for all k -algebras R .

In other words, G is a semidirect product of 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 (normal) subgroup \mathbb{U}_n (defined by $a_{ii} = 1$) and its subgroup \mathbb{D}_n (defined by $a_{ij} = 0$ for $i < j$) (see 2.9).

PROPOSITION 2.21. Let N and Q be algebraic subgroups of an algebraic group G . Then G is the semidirect product of N and Q if and only if there exists a homomorphism $G \rightarrow Q'$ whose restriction to Q is an isomorphism and whose kernel is N .

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

\Leftarrow : Let $\varphi: G \rightarrow Q'$ be the given homomorphism. 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 $Q(R)$. \square

Recall that an action of an algebraic group G on a functor X from k -algebras to sets is a natural transformation $\theta: G \times X \rightarrow X$ such that each map $G(R) \times X(R) \rightarrow X(R)$ is an action of the group $G(R)$ on the set $X(R)$. Now let N and Q be algebraic groups, and suppose that there is given an action of Q on N

$$(q, n) \mapsto \theta_R(q, n): Q(R) \times N(R) \rightarrow N(R)$$

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

$$R \rightsquigarrow N(R) \rtimes_{\theta_R} Q(R): \text{Alg}_k^0 \rightarrow \text{Grp}$$

is an algebraic group because its underlying functor to sets is $N \times Q$, which is represented by $\mathcal{O}(N) \otimes \mathcal{O}(G)$. 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

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

EXAMPLE 2.22. In contrast to abstract groups, a finite algebraic group of order p may act nontrivially on another such group, and so there are noncommutative finite algebraic groups of order p^2 . For example, there is an action of μ_p on α_p ,

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

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 $s = 0$.

EXAMPLE 2.23. As promised (1.45), here are two examples of algebraic groups G over a perfect field such that G_{red} is not normal.

- (a) Let $G = \mu_3 \rtimes (\mathbb{Z}/2\mathbb{Z})_k$ with the obvious action of $(\mathbb{Z}/2\mathbb{Z})_k$ on μ_3 and k perfect of characteristic 3. Then $G_{\text{red}} = (\mathbb{Z}/2\mathbb{Z})_k$ is not normal.
- (b) Let $G = \alpha_p \rtimes \mathbb{G}_m$ with the obvious action of \mathbb{G}_m on α_p and k perfect of characteristic p . Then $G_{\text{red}} = \mathbb{G}_m$ is not normal. See Exercise 2-6 (or SGA 3, VI_A, 0.2, p.296).

f. The algebraic subgroup generated by a map

Let $f: X \rightarrow G$ be a regular map from an algebraic scheme X over k to an algebraic group G . We shall show that there exists a smallest algebraic subgroup H of G such that f factors through H in the following two cases: X is geometrically reduced (2.25); X and G are affine (2.27).

GEOMETRICALLY REDUCED CASE

Recall that $\text{inv}: G \rightarrow G$ is the map $g \mapsto g^{-1}$.

PROPOSITION 2.24. Let $f: X \rightarrow G$ be a regular map from a geometrically reduced algebraic scheme X over k to an algebraic group G . Assume that $\text{inv}(f(X)) \subset f(X)$, and let f^n denote the map

$$(x_1, \dots, x_n) \mapsto f(x_1) \cdots f(x_n): X^n \rightarrow G.$$

The reduced algebraic subscheme of G with underlying set the closure of $\bigcup_n \text{Im}(f^n)$ is a smooth algebraic subgroup of G .

PROOF. Because X is geometrically reduced, so also is X^n (A.39). The map $f^n: X^n \rightarrow H$ is schematically dominant for n large because it is dominant and H is reduced (A.70). 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

$m^{-1}(Z \setminus H)$ 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 $x_1, \dots, x_n, y_1, \dots, y_n \in X(k)$ such that

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

(because $\text{Im}(f^n) \times \text{Im}(f^n)$ is constructible, and therefore contains an open subset of its closure; A.68). But this is absurd, because

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

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

PROPOSITION 2.25. *Let $(f_i: X_i \rightarrow G)_{i \in I}$ be a finite family of regular maps from geometrically reduced algebraic schemes X_i over k to an algebraic group G . There exists a smallest algebraic subgroup H of G such that all f_i factor through H . Moreover, H is smooth.*

PROOF. Let $X = \bigsqcup_{i \in I} X_i \sqcup X_i$, and let $f: X \rightarrow G$ be the map whose restriction to $X_i \sqcup X_i$ is f_i on the first component and $\text{inv} \circ f_i$ on the second component. Then $\text{inv}(f(X)) \subset f(X)$, and the algebraic subgroup H attached to f in (2.24) has the required properties. \square

We call H the **algebraic subgroup of G generated by the f_i** (or X_i). Its formation commutes with extension of the base field (A.70).

PROPOSITION 2.26. *Let $f: X \rightarrow G$ be a regular map from a geometrically reduced scheme X over k to an algebraic group G . If X is geometrically connected and $f(X)$ contains e , then the algebraic subgroup of G generated by f is connected.*

PROOF. Let f' be the map $X' \stackrel{\text{def}}{=} X \sqcup X \rightarrow G$ acting as f on the first component and $\text{inv} \circ f$ on the second. The hypotheses imply that $\bigcup \text{Im}(f'^m)$ is connected, and so its closure H is connected. \square

AFFINE CASE

Let $f: X \rightarrow G$ be a regular map from an affine algebraic scheme X to an affine algebraic group G . Assume that the image of f contains e , say $f(o) = e$. Let I_n be the kernel of the homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(X^n)$ of k -algebras defined by the regular map

$$(x_1, \dots, x_n) \mapsto f(x_1) \cdots f(x_n): X^n \rightarrow G.$$

From the regular maps

$$\begin{aligned} X &\rightarrow X^2 \rightarrow \cdots \rightarrow X^n \rightarrow \cdots \rightarrow G, \\ (x) &\mapsto (x, o) \mapsto \cdots \end{aligned}$$

we get inclusions

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

and we let $I = \bigcap I_n$.

PROPOSITION 2.27. *Assume that $\text{inv}(f(X(R))) \subset f(X(R))$ for all R . Then the subscheme H of G defined by I is an algebraic subgroup of G . It is the smallest algebraic subgroup H of G such that $H(R)$ contains $f(X(R))$ for all k -algebras R . In other words, it is the smallest algebraic subgroup such that $f: X \rightarrow G$ factors through H .*

PROOF. From the diagram of algebraic schemes

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

we get a diagram of k -algebras

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

The image of $\mathcal{O}(G)$ in $\mathcal{O}(X^n)$ is $\mathcal{O}(G)/I_n$ and its image in $\mathcal{O}(X^{2n})$ is $\mathcal{O}(G)/I_{2n}$, and so the diagram shows that

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

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

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

factors through $\mathcal{O}(G) \rightarrow \mathcal{O}(G)/I$, and defines a multiplication map $m_H: H \times H \rightarrow H$. The triple (H, m_H, e) is the smallest algebraic submonoid of G such that $H(R)$ contains $f(X(R))$ for all k -algebras R .

The hypothesis $\text{inv}(f(X(R))) \subset f(X(R))$ implies that $\text{inv}(H)$ has the same property, and so equals H . Therefore (H, m_H) is an algebraic subgroup of G . It clearly has the required properties. \square

We write $\langle X, f \rangle$ for the algebraic subgroup H in the proposition, and call it the **algebraic subgroup generated by f** (or X). If $f(X)$ is not stable under inv , we define $\langle X, f \rangle$ to be the algebraic subgroup generated by $f \sqcup \text{inv} \circ f: X \sqcup X \rightarrow G$.

PROPOSITION 2.28. *Let K be a field containing k . Then $\langle X, f \rangle_K = \langle X_K, f_K \rangle$.*

PROOF. The definition of I commutes with extension of the base field. \square

PROPOSITION 2.29. *If X is geometrically connected (resp. geometrically reduced), then $\langle X, f \rangle$ is connected (resp. geometrically reduced).*

PROOF. We may suppose that k is algebraically closed. An affine scheme Y is connected if and only if $\mathcal{O}(Y)$ has no nontrivial idempotent (CA 14.2). 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 $\mathcal{O}(G)/I_n \rightarrow \mathcal{O}(X^n)$ is injective. As X is connected and k is algebraically closed, X^n is connected, and so this is a contradiction. The proof of the remaining statement is similar. \square

NOTES. The first approach follows that in SGA 3, VI_B, §7, p.384. The second approach is based on the construction of the derived group in Waterhouse 1979.

g. Forms of algebraic groups

Details to be added (see Chapter 25).

2.30. Let G be an algebraic group over k . A **form** of G over k is an algebraic group G' over k that becomes isomorphic to G over k^{al} . When G is smooth, G' then becomes isomorphic to G over k^{sep} .

2.31. Let G be a smooth quasi-projective algebraic group³ over a field k , and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. Let G' be a form of G over k , and choose an isomorphism $a: G_{k^{\text{sep}}} \rightarrow G'_{k^{\text{sep}}}$. Then $\tau \mapsto c_\tau = a^{-1} \circ \tau a$ is a continuous 1-cocycle for Γ with values in $\text{Aut}(G_{k^{\text{sep}}})$ whose cohomology class does not depend on the choice of a . In this way, the isomorphism classes of forms of G over k are classified by $H^1(\Gamma, \text{Aut}(G_{k^{\text{sep}}}))$. When G is not smooth, the k -forms are classified by the flat cohomology group $H^1(k, \underline{\text{Aut}}(G))$.

2.32. Let G be an algebraic group over a field k . There exists an exact sequence

$$e \rightarrow Z(G) \rightarrow G \rightarrow G^{\text{ad}} \rightarrow e$$

(see later). The algebraic group G^{ad} is called the **adjoint group** of G . The action of G on itself by inner automorphisms defines an action of G^{ad} on G . An **inner automorphism** of G is an automorphism defined by an element of $G^{\text{ad}}(k)$. Such an automorphism need not be of the form $\text{inn}(g)$ with $g \in G(k)$, but it becomes of this form over k^{al} .

2.33. Let G be a smooth quasi-projective algebraic group over a field k . An **inner form** of G is a pair (G_0, α) consisting of an algebraic group G_0 over k and a $G(k^{\text{sep}})$ -conjugacy class of isomorphisms $a: G_{k^{\text{sep}}} \rightarrow G_{0k^{\text{sep}}}$ such that $a^{-1} \circ \tau a$ is an inner automorphism of $G_{k^{\text{sep}}}$ for all $\tau \in \Gamma$. An isomorphism $(G_0, \alpha) \rightarrow (G'_0, \alpha')$ of inner forms is an isomorphism of algebraic groups $\varphi: G_0 \rightarrow G'_0$ (over k) such that

$$a \in \alpha \implies \varphi \circ a \in \alpha'.$$

Any two isomorphisms $(G_0, \alpha) \rightarrow (G'_0, \alpha')$ differ by an inner automorphism of G_0 (or G'_0). If (G_0, α) is an inner form of G , and $a \in \alpha$, then $\tau \mapsto c_\tau \stackrel{\text{def}}{=} a^{-1} \circ \tau a$ is a 1-cocycle for Γ with values in $G^{\text{ad}}(k^{\text{sep}})$ whose cohomology class does not depend on the choice of a in α . In this way, we obtain a one-to-one correspondence between the isomorphism classes of inner forms of G and the elements of $H^1(k, G^{\text{ad}})$.

2.34. Let G be a smooth algebraic group over a field k . Corresponding to the exact sequence

$$e \rightarrow G^{\text{ad}} \rightarrow \underline{\text{Aut}}(G) \rightarrow U \rightarrow e$$

we obtain maps

$$H^1(k, G^{\text{ad}}) \xrightarrow{a} H^1(k, \underline{\text{Aut}}(G)) \rightarrow H^1(k, U).$$

Sometimes (e.g., Voskresenskii 1998, 3.10), a form of G is said to be inner or outer according as its class in $H^1(k, \underline{\text{Aut}}(G))$ lies in the image of a or not. It is important to note that, with this definition, the inner forms are classified by the image of a , not $H^1(k, G^{\text{ad}})$.

³In fact, all algebraic groups over a field are quasi-projective.



h. Restriction of scalars

Throughout this section, A is a finite k -algebra.

2.35. 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

$$(F)_{A/k}: \text{Alg}_k \rightarrow \text{Set}, \quad R \mapsto X(A \otimes R).$$

For a closed subscheme X of \mathbb{A}^n or \mathbb{P}^n , the existence of $X_{A/k}$ follows from (1.80). See A.125 and A.126 in general.

2.36. For a quasi-projective algebraic group G over A , the functor $(G)_{A/k}$,

$$R \mapsto G(A \otimes R): \text{Alg}_k \rightarrow \text{Set}$$

takes values in the category of groups and is representable (2.35), and so it is an algebraic group. The algebraic group $(G)_{A/k}$ is said to have been obtained from G by (**Weil**) **restriction of scalars** (or by **restriction of the base ring**), and $(G)_{A/k}$ is called the **Weil restriction** of G . Thus

$$(G)_{A/k}(R) \simeq G(R)$$

all k -algebras R . The functor $G \mapsto (G)_{A/k}$ from quasi-projective algebraic A -groups to algebraic k -groups is denoted by $\text{Res}_{A/k}$ or $\Pi_{A/k}$.

From now on, all algebraic groups are quasi-projective.

2.37. Let G be an algebraic group over k . For a k -algebra R , the map $r \mapsto 1 \otimes r: R \rightarrow A \otimes R$ is a homomorphism of k -algebras, and so it induces a homomorphism

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

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

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

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

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

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

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

$$\begin{array}{ccccc} & & \beta(R) & & \\ & \swarrow & \text{---} & \searrow & \\ G_A(R) \stackrel{\text{def}}{=} G(R_0) & \xrightarrow{\alpha(R_0)} & H(k' \otimes_k R_0) & \xrightarrow{\gamma} & H(R) \end{array}$$

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

2.38. According to (2.37), for every algebraic k -group G and algebraic A -group H ,

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

In other words, $\Pi_{A/k}$ is right adjoint to the functor “change of base ring $k \rightarrow A$ ”. Being a right adjoint, $\Pi_{A/k}$ preserves inverse limits (MacLane 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 checked directly from the definition of $\Pi_{A/k}$.

2.39. For any sequence of finite homomorphisms $k \rightarrow k' \rightarrow A$ 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 ,

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

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 $H \rightsquigarrow H_A$.

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

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

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

$$\begin{aligned} (\Pi_{A/k}G)_K(R) &= (\Pi_{A/k}G)(R) \\ &= G(A \otimes_k R) \\ &\simeq G(A \otimes_k K \otimes_K R) \\ &= \Pi_{A \otimes_k K/K}(G_K)(R) \end{aligned}$$

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

2.41. 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,

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

Indeed, for any k -algebra R ,

$$\begin{aligned} (G)_{A/k}(R) &= G(A \otimes_k R) \\ &= G_1(k_1 \otimes_k R) \times \cdots \times G_n(k_n \otimes_k R) \\ &= (G_1)_{k_1/k}(R) \times \cdots \times (G_n)_{k_n/k}(R) \\ &= ((G_1)_{k_1/k} \times \cdots \times (G_n)_{k_n/k})(R). \end{aligned}$$

2.42. Let A be an étale k -algebra, and let K be a field containing all k -conjugates of A . Then

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

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

$$(\Pi_{A/k}G)_K \stackrel{(10)}{\simeq} \Pi_{A \otimes K/K} G_K \stackrel{(11)}{\simeq} \prod_{\alpha:A \rightarrow K} G_\alpha$$

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

2.43. 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 $G(k[\varepsilon]) \rightarrow G(k)$ over P is the tangent space to G at P (A.47). There is an exact sequence

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

where V is the tangent space to G at e . For a more general statement, see 12.29.

2.44. We saw in (2.42) that, when A is étale, $(G)_{A/k}$ becomes isomorphic to a product of copies of G over some field containing A . This is far from being true when A/k is an inseparable field extension. For example, let k be a nonperfect field of characteristic 2, and let $A = k[\sqrt{a}]$ where $a \in k \setminus k^2$. Then

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

For an algebraic group G over k ,

$$(\Pi_{A/k}G_A)_A \stackrel{2.40}{\simeq} \Pi_{A \otimes A/A} G_{A \otimes A} \simeq \Pi_{A[\varepsilon]/A} G_{A[\varepsilon]},$$

which is an extension of G_A by a vector group (2.43). However, $(G)_{A/k}$ is smooth if G is smooth — this follows from the criterion (A.53).

ASIDE 2.45. When F is represented by an algebraic scheme X , it is not always true that $(F)_{A/k}$ is represented by a scheme. Let $X = \bigcup_i U_i$ be an open affine covering of X . Then $X' = \bigcup_i (U_i)_{A/k}$ is a scheme, and \tilde{X}' is a subfunctor of $(F)_{A/k}$, but it need not equal $(F)_{A/k}$. If $[A:k] = d$ and every d -tuple of points of X lies in some U_i , then $\tilde{X}' = (F)_{A/k}$, and so $(F)_{A/k}$ is representable. See the proof of Theorem 4, p.194, of Bosch et al. 1990.

ASIDE 2.46. Let F be a functor from k -algebras (not necessarily finitely generated) to sets and let $A = \text{Nat}(F, \mathbb{A}^1)$. Then $F(R) \simeq \text{Hom}_{k\text{-algebra}}(A, R)$ for all k -algebras R . It is tempting to conclude that F is representable, but, in general, A will not be a set, and hence not a k -algebra.

Exercises

EXERCISE 2-1. For a homomorphism $G \rightarrow H$ of abstract groups with kernel N , show that the map

$$(g, n) \mapsto (g, gn): G \times N \rightarrow G \times_H G \tag{12}$$

is a bijection. Deduce that, for every homomorphism $G \rightarrow H$ of algebraic k -groups with kernel N , there is a unique isomorphism of algebraic k -schemes

$$G \times N \rightarrow G \times_H G \tag{13}$$

that becomes the map (12) when we take points with coordinates in a k -algebra R .

EXERCISE 2-2. Show that for any diagram of abstract groups

$$\begin{array}{ccccc} & & H & & \\ & & \downarrow \beta & & \\ N & \longrightarrow & G & \longrightarrow & G', \end{array} \quad (14)$$

with N the kernel of $G \rightarrow G'$, the map

$$(n, h) \mapsto (n \cdot \beta(h), h): N \times H \rightarrow G \times_{G'} H \quad (15)$$

is an isomorphism. Deduce that, for every diagram (14) of algebraic groups, there is a unique isomorphism

$$M \times H \simeq G \times_{G'} H$$

that becomes (15) when we take points with coordinates in a k -algebra R .

EXERCISE 2-3. Let G be an algebraic over a field k , and let $k' = k[\varepsilon]$ where $\varepsilon^m = 0$. Show that $(G)_{k'/k}$ has a filtration whose quotients are G or vector groups.

EXERCISE 2-4. Let G be a finite (hence affine) algebraic group. Show that the following conditions are equivalent:

- (a) the k -algebra $\mathcal{O}(G_{\text{red}})$ is étale;
- (b) $\mathcal{O}(G_{\text{red}}) \otimes \mathcal{O}(G_{\text{red}})$ 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 2-5. Let k be a nonperfect field of characteristic p , and let $a \in k \setminus k^p$. Show that the functor

$$R \rightsquigarrow G(R) \stackrel{\text{def}}{=} \{x \in R \mid x^{p^2} = ax^p\}$$

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 2-4 shows that $\mathcal{O}(G)/\mathfrak{N}$ is not a Hopf algebra.)

EXERCISE 2-6. Let k be a field of characteristic p . Show that the extensions

$$0 \rightarrow \mu_p \rightarrow G \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$$

with G a finite commutative algebraic group are classified by the elements of $k^\times/k^{\times p}$ (the split extension $G = \mu_p \times \mathbb{Z}/p\mathbb{Z}$ corresponds to the trivial element in $k^\times/k^{\times p}$). Show that G_{red} is not a subgroup of G unless the extension splits.

EXERCISE 2-7. Over a field k of characteristic 3, let $G = \mu_3 \rtimes (\mathbb{Z}/2\mathbb{Z})_k$ for the (unique) nontrivial action of $(\mathbb{Z}/2\mathbb{Z})_k$ on μ_3 ; then $G_{\text{red}} = (\mathbb{Z}/2\mathbb{Z})_k$, which is not normal in G .⁴ Similarly, over a field of characteristic p , let $G = \alpha_p \rtimes \mathbb{G}_m$ for the obvious nontrivial action of \mathbb{G}_m on α_p ; then G is a connected algebraic group such that $G_{\text{red}} = \mathbb{G}_m$ is an algebraic subgroup of G which is not normal.

⁴Let R be a k -algebra with no nontrivial idempotents but containing a primitive cube root ζ of 1. Let σ denote the nonneutral element of $(\mathbb{Z}/2\mathbb{Z})_k(R) = \mathbb{Z}/2\mathbb{Z}$. By definition $\sigma\zeta\sigma = \zeta^{-1} = \zeta^2$. Therefore $\zeta\sigma = \sigma\zeta^2$, and $\zeta\sigma\zeta^{-1} = \zeta\sigma\zeta^2 = \sigma\zeta^4 = \sigma\zeta \notin (\mathbb{Z}/2\mathbb{Z})_k(R)$.

EXERCISE 2-8. Let $\alpha: G \rightarrow H$ be an isogeny of affine group varieties over k , and let k' be a finite field extension of k . Prove the following (Pink 2004, 1.6):

- (a) if k'/k is separable, then $(\alpha)_{k'/k}: (G)_{k'/k} \rightarrow (H)_{k'/k}$ is an isogeny if and only if α is an isogeny;
- (b) if k'/k is inseparable, then $(\alpha)_{k'/k}: (G)_{k'/k} \rightarrow (H)_{k'/k}$ is an isogeny if and only if α is a separable isogeny.

Affine algebraic groups and Hopf algebras

We explain the relation between affine algebraic groups and Hopf algebras.

a. *The comultiplication map*

Let A be a k -algebra, and let $\Delta: A \rightarrow A \otimes A$ be a homomorphism. Because

$$\mathrm{Spm}(A \otimes A) \simeq \mathrm{Spm}(A) \times \mathrm{Spm}(A)$$

(A.34), we can regard $\mathrm{Spm}(\Delta)$ as a map $\mathrm{Spm}(A) \times \mathrm{Spm}(A) \rightarrow \mathrm{Spm}(A)$.

From a pair of homomorphisms of k -algebras $f_1, f_2: A \rightarrow R$ we get a homomorphism

$$(f_1, f_2): A \otimes A \rightarrow R, \quad (a_1, a_2) \mapsto f_1(a_1)f_2(a_2),$$

and we set

$$f_1 \cdot f_2 = (f_1, f_2) \circ \Delta. \tag{16}$$

This defines a binary operation on $h^A(R) = \mathrm{Hom}(A, R)$.

PROPOSITION 3.1. *The pair $(\mathrm{Spm}(A), \mathrm{Spm}(\Delta))$ is an algebraic group over k if and only if (16) makes $\mathrm{Hom}(A, R)$ into a group for all k -algebras R .*

PROOF. Let $(G, m) = (\mathrm{Spm} A, \mathrm{Spm} \Delta)$. From (A, Δ) we get a functor $h^A: R \rightsquigarrow \mathrm{Hom}(A, R)$ from k -algebras to the category of sets equipped with a binary operation (i.e., to magmas).

If h^A takes values in the subcategory of groups, then there are natural transformations $e: * \rightarrow h^A$, and $\mathrm{inv}: h^A \rightarrow h^A$ making the diagrams (2, 3), p.17, commute. According to the Yoneda lemma (A.27), these natural transformations arise from regular maps $e: * \rightarrow G$, $\mathrm{inv}: G \rightarrow G$ making the same diagrams commute, and so (G, m) is an algebraic group.

Conversely, the existence of the regular maps e and inv implies that (h^A, h^Δ) takes values in the subcategory of groups. □

REMARK 3.2. Let G be an affine algebraic group, and let $\mathcal{O}(G)$ be its coordinate ring. Then

$$G(R) \simeq \mathrm{Hom}_{k\text{-algebra}}(\mathcal{O}(G), R),$$

and so an $f \in \mathcal{O}(G)$ defines an evaluation map

$$f_R: G(R) \rightarrow R, \quad g \mapsto g(f); \tag{17}$$

i.e.,

$$f_R(g) = g(f), \quad f \in \mathcal{O}(G), \quad g \in G(R).$$

In this way, we get an isomorphism

$$\mathcal{O}(G) \simeq \text{Nat}(G, \mathbb{A}^1) \quad (18)$$

where \mathbb{A}^1 is the functor sending a k -algebra R to its underlying set. Similarly,

$$\mathcal{O}(G \times G) \simeq \text{Nat}(G \times G, \mathbb{A}^1)$$

With this interpretation

$$(\Delta f)_R(g_1, g_2) = f_R(g_1 \cdot g_2), \quad f \in \mathcal{O}(G), \quad g_1, g_2 \in G(R). \quad (19)$$

b. Hopf algebras

Let (G, m) be an affine algebraic group over k , and let $A = \mathcal{O}(G)$. We saw in the preceding chapter that m corresponds to a homomorphism $\Delta: A \rightarrow A \otimes A$. The maps e and inv correspond to homomorphisms of k -algebras $\epsilon: A \rightarrow k$ and $S: A \rightarrow A$, and the diagrams (2) and (3), p.17, correspond to diagrams

$$\begin{array}{ccc} A \otimes A \otimes A & \xleftarrow{\text{id} \otimes \Delta} & A \otimes A \\ \uparrow \Delta \otimes \text{id} & & \uparrow \Delta \\ A \otimes A & \xleftarrow{\Delta} & A \end{array} \quad \begin{array}{ccc} k \otimes A & \xleftarrow{\epsilon \otimes \text{id}} & A \otimes A & \xrightarrow{\text{id} \otimes \epsilon} & A \otimes k \\ & \swarrow \simeq & \uparrow \Delta & \searrow \simeq & \\ & & A & & \end{array} \quad (20)$$

$$\begin{array}{ccccc} A & \xleftarrow{(S, \text{id})} & A \otimes A & \xrightarrow{(\text{id}, S)} & A \\ \uparrow & & \uparrow \Delta & & \uparrow \\ k & \xleftarrow{\epsilon} & A & \xrightarrow{\epsilon} & k \end{array} \quad (21)$$

DEFINITION 3.3. A pair (A, Δ) consisting of a k -algebra A and a k -algebra homomorphism $\Delta: A \rightarrow A \otimes A$ is a **Hopf algebra**¹ if there exist k -algebra homomorphisms

$$\epsilon: A \rightarrow k, \quad S: A \rightarrow A$$

such that the diagrams (20), (21) commute:

$$\begin{aligned} (\text{id} \otimes \Delta) \circ \Delta &= (\Delta \otimes \text{id}) \circ \Delta \\ (\text{id}, \epsilon) \circ \Delta &= \text{id} = (\epsilon, \text{id}) \circ \Delta \\ (\text{id}, S) \circ \Delta &= \epsilon = (S, \text{id}) \circ \Delta. \end{aligned}$$

The maps Δ, ϵ, S are called respectively the **comultiplication** map, the **co-identity** map, and the **inversion** or **antipode**. A **homomorphism** of Hopf algebras $f: (A, \Delta_A) \rightarrow (B, \Delta_B)$ is a homomorphism $f: A \rightarrow B$ of k -algebras such that $(f \otimes f) \circ \Delta_A = \Delta_B \circ f$.

¹Recall that we require k -algebras to be commutative and finitely generated. The general definition of a Hopf algebra allows A to be an arbitrary ring. Thus, we are considering only a special class of Hopf algebras, and not all statements for our Hopf algebras generalize.

3.4. The pair (ϵ, S) in the definition of a Hopf algebra is uniquely determined by (A, Δ) . Moreover, for every homomorphism $f: (A, \Delta_A) \rightarrow (B, \Delta_B)$ of Hopf algebras,

$$\begin{cases} \epsilon_B \circ f = \epsilon_A \\ f \circ S_A = S_B \circ f. \end{cases} \quad (22)$$

These statements can be proved in the same way as the similar statements for algebraic groups using the Yoneda lemma (see 1.11), or deduced from them. 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 $G \rightarrow \mathbb{A}^1$ (3.2). Then

$$\begin{aligned} (\Delta f)_R(g_1, g_2) &= f_R(g_1 \cdot g_2), \\ (\epsilon f)_R(g) &= f(e) \\ (Sf)_R(g) &= f(g^{-1}) \end{aligned}$$

for $g, g_1, g_2 \in G(R)$.

EXERCISE 3.6. For a set X , let $R(X)$ denote the k -algebra of maps $X \rightarrow k$. For a second set Y , let $R(X) \otimes R(Y)$ act on $X \times Y$ according to the rule $(f \otimes g)(x, y) = f(x)g(y)$.

- Show that the map $R(X) \otimes R(Y) \rightarrow R(X \times Y)$ just defined is injective. (Hint: choose a basis f_i for $R(X)$ as a k -vector space, and consider an element $\sum f_i \otimes g_i$.)
- Let Γ be a group and define maps

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

Show that if Δ maps $R(\Gamma)$ into the subring $R(\Gamma) \otimes R(\Gamma)$ of $R(\Gamma \times \Gamma)$, then Δ, ϵ , and S define on $R(\Gamma)$ the structure of a Hopf algebra.

- If Γ is finite, show that Δ always maps $R(\Gamma)$ into $R(\Gamma) \otimes R(\Gamma)$.

c. Hopf algebras and algebraic groups

The next proposition shows that to give a structure Δ of a Hopf algebra on A is the same as giving a structure m of an algebraic group on $\text{Spm } A$.

PROPOSITION 3.7. *Let A be a k -algebra, and let $\Delta: A \rightarrow A \otimes A$ be 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 (20, 21) are the same as the diagrams (2, 3) 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. \square

COROLLARY 3.8. *The functor Spm is an equivalence from the category of Hopf algebras over k to the category of affine algebraic groups, with quasi-inverse $(G, m) \rightsquigarrow (\mathcal{O}(G), \mathcal{O}(m))$.*

ASIDE 3.9. For an algebraic scheme X , the k -algebra $\mathcal{O}(X)$ need not be finitely generated, even for quasi-affine varieties. However, it is when X is an algebraic group (10.33 below). Therefore, we get a functor $G \rightsquigarrow (\mathcal{O}(G), \mathcal{O}(m))$ from algebraic groups over k (not necessarily affine) to Hopf algebras over k (in our sense). Let $G^{\text{aff}} = \text{Spm}(\mathcal{O}(G), \mathcal{O}(m))$. The canonical homomorphism $G \rightarrow G^{\text{aff}}$ is universal among the homomorphisms from G to an affine algebraic group (ibid.).

d. Hopf subalgebras

DEFINITION 3.10. 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 3.11. *The image of a homomorphism $f: A \rightarrow B$ of Hopf algebras is a Hopf subalgebra of B .*

PROOF. Immediate from (3.4). □

DEFINITION 3.12. A **Hopf ideal** in a Hopf algebra (A, Δ) 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 3.13. *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 $f: V \rightarrow V'$ 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 $f: A \rightarrow B$ of Hopf algebras. Then

$$\begin{cases} \Delta_A(\mathfrak{a}) \subset \text{Ker}(f \otimes f) = A \otimes \mathfrak{a} + \mathfrak{a} \otimes A \\ \epsilon_A(\mathfrak{a}) = 0 \quad \text{by (22)} \\ S_A(\mathfrak{a}) \subset \mathfrak{a} \quad \text{by (22)} \end{cases}$$

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 3.14. *Let \mathfrak{a} be a Hopf ideal in a Hopf k -algebra A . The quotient vector space A/\mathfrak{a} has a unique Hopf k -algebra structure for which $A \rightarrow A/\mathfrak{a}$ is a homomorphism. Every homomorphism of Hopf k -algebras $A \rightarrow B$ whose kernel contains \mathfrak{a} factors uniquely through $A \rightarrow A/\mathfrak{a}$.*

PROOF. Routine verification. □

PROPOSITION 3.15. *A homomorphism $f: A \rightarrow B$ of Hopf k -algebras induces an isomorphism of Hopf k -algebras*

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

PROOF. Routine verification. □

PROPOSITION 3.16. *Every homomorphism $f: A \rightarrow B$ 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 from (3.15). □

e. Hopf subalgebras of $\mathcal{O}(G)$ versus algebraic subgroups of G

PROPOSITION 3.17. *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 $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$, and so is a Hopf ideal (3.13). Conversely, if \mathfrak{a} is a Hopf ideal, then $\mathcal{O}(H) = \mathcal{O}(G)/\mathfrak{a}$ has a unique Hopf algebra structure for which $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is a homomorphism of Hopf algebras (3.14). This means that there is a unique algebraic group structure on H for which the inclusion $H \hookrightarrow G$ is a homomorphism of algebraic groups (3.8). \square

f. Subgroups of $G(k)$ versus algebraic subgroups of G

In this section, we reprove (1.31) for affine algebraic groups.

Recall 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 (1.27). We prove a converse.

PROPOSITION 3.18. *Let G be an affine algebraic group. Let S be a closed subgroup of $G(k)$. Then $S = H(k)$ for a unique reduced algebraic subgroup H of G . The algebraic subgroups H of G that arise in this way are exactly those for which $H(k)$ is dense in H (i.e., H is reduced and $H(k)$ is dense in $|H|$; 1.9c).*

PROOF. Each $f \in \mathcal{O}(G)$ defines a function $h(f): S \rightarrow k$, and, for $x, y \in S$, $(\Delta_G f)(x, y) = f(x \cdot y)$ (see (19), p. 56). Therefore, when we let $R(S)$ denote the k -algebra of maps $S \rightarrow k$ and define $\Delta_S: R(S) \rightarrow R(S \times S)$ as in Exercise 3.6, we obtain a commutative diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{\Delta_G} & \mathcal{O}(G \times G) \\ \downarrow h & & \downarrow \\ R(S) & \xrightarrow{\Delta_S} & R(S \times S). \end{array}$$

The vertical map at right factors into

$$\mathcal{O}(G \times G) \simeq \mathcal{O}(G) \otimes \mathcal{O}(G) \xrightarrow{h \otimes h} R(S) \otimes R(S) \rightarrow R(S \times S).$$

Therefore the kernel \mathfrak{a} of h satisfies

$$\Delta_G(\mathfrak{a}) \subset \text{Ker}(h \otimes h) = \mathcal{O}(G) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathcal{O}(G)$$

(cf. the proof of 3.13). 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. \square

ASIDE 3.19. 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

$$t \mapsto x^t = \exp(t \log x): \mathbb{A}^1 \rightarrow \mathrm{GL}_n,$$

where

$$\exp(z) = \sum_{i=0}^{p-1} \frac{z^i}{i!} \text{ and } \log(z) = - \sum_{i=1}^{p-1} \frac{(1-z)^i}{i}.$$

Let G be the smallest subgroup variety of GL_n containing these subgroups for $x \in X$. 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 $y^p = 0$.

ASIDE 3.20. We have seen that the study of affine algebraic groups is equivalent to the study of Hopf algebras. Of course, the “affine” is essential. However, for a general algebraic group G , the local ring \mathcal{O}_e at e equipped with the structure provided by m captures some of the structure of G . For example, the connected algebraic subgroups of G are in one-to-one correspondence with the ideals \mathfrak{a} in \mathcal{O}_e such that $\Delta(\mathfrak{a}) \subset A \otimes \mathfrak{a} + \mathfrak{a} \otimes A$ and $S(\mathfrak{a}) = \mathfrak{a}$. [Add discussion of hyperalgebras; references.]

g. Affine algebraic groups G such that $G(k)$ is dense in G : a survey

Clearly, the algebraic groups G over k such that $G(k)$ is dense in G are of particular interest. In this subsection, we list the known results concerning them. Many of these results will be proved later in the book. [Citations, both internal and external, will be added.]

Recall the equivalent conditions:

- (a) $G(k)$ is dense in G (see 1.9);
- (b) $G(k)$ is schematically dense in G (see 1.8);
- (c) G is reduced and $G(k)$ is dense in $|G|$.

For a group variety, the conditions are equivalent to:

- (d) $G(k)$ is dense in $G(k^{\mathrm{al}})$ (for the Zariski topology).

As $G(k)$ can only be dense in G if G is a group variety, from now on G is an *group variety* over k .

3.21. $G(k)$ is dense in G if k is separably closed.

3.22. If G is finite, then $G(k)$ is dense in G if and only if G is constant. For example, $\mu_n(k)$ is dense in μ_n if and only if k contains n distinct n th roots of 1.

3.23. In general, there is an exact sequence

$$e \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow e$$

with $\pi_0(G)$ a finite group variety (5.48). The group $G(k)$ is dense in G if and only if $\pi_0(G)$ is constant and $G^\circ(k)$ is dense in G° .

3.24. Let k be finite. Then $G(k)$ is dense in G if and only if G is a finite constant group.

From now on, G is a *connected affine group variety* over k .

3.25. Let k be infinite. Then $G(k)$ is dense in G when $G = \mathbb{G}_a, \mathbb{G}_m, \mathrm{GL}_n$, or SL_n . For a direct proof, see [Waterhouse 1979](#), 4.5.

3.26. Let k be infinite. If k is perfect, then G is unirational over k and so $G(k)$ is dense in G . See [Borel 1991](#), 18.2, or [Springer 1998](#), 13.3.9.

3.27. There exist forms G of \mathbb{G}_a over infinite fields such that $G(k)$ is finite, and hence not dense in G ([1.42](#)).

3.28. A group variety G is said to be unipotent if it is isomorphic to a subgroup variety of \mathbb{U}_n for some n (see [Chapter 15](#)). A unipotent group variety G is said to be *split* if it admits a subnormal series whose quotients are all isomorphic to \mathbb{G}_a ([8.17](#)). Let G be a unipotent group variety. If G is split, then it is isomorphic as a variety to \mathbb{A}^n , and so $G(k)$ is dense in G when k is infinite. Otherwise, the examples of Rosenlicht ([1.42](#), [3.27](#)) show that $G(k)$ need not be dense in G .

3.29. A connected group variety G is said to be reductive if $G_{k^{\mathrm{al}}}$ contains no connected normal unipotent subgroup variety except e . For example, tori are reductive. A reductive group variety G is unirational, and so $G(k)$ is dense in G if k is infinite. See ([19.21](#)); also [Borel 1991](#), 18.2, or [Springer 1998](#), 13.3.10.

3.30. If G contains a connected normal split-unipotent subgroup U such that G/U is reductive, then $G \approx U \times G/U$ as an algebraic variety (Rosenlicht), and so $G(k)$ is dense in G when k is infinite.

3.31. Suppose that G is the Weil restriction $(G)_{k'/k}$ of a group variety G' over a finite extension k' of k . If G' is reductive and k is infinite, then $G(k)$ is dense in G ([Pink 2004](#), 1.7).

3.32. If a connected group variety G is unirational, then $G(k)$ is dense in G when k is infinite. So which group varieties are unirational? A connected group variety G over a field k is unirational if k is perfect or G is reductive ([3.26](#), [3.29](#)). On the other hand, Rosenlicht's forms of \mathbb{G}_a ([3.27](#)) are not unirational, and many tori, even in characteristic zero, are not rational. Every connected group variety over an algebraically closed field is unirational ([3.30](#)).

3.33. One can ask when $G(k)$ is dense in G also for nonaffine algebraic groups, but there doesn't seem to be much that one can say. They are never unirational and for an elliptic curve E over \mathbb{Q} , the group $E(\mathbb{Q})$ may be infinite (hence dense in E) or finite (hence not dense).

3.34. A *matrix group* is an affine algebraic group G such that $G(k)$ is schematically dense in G . Every matrix group is isomorphic to a subgroup of GL_n for some n (see [Section 6.d](#)), and the matrix subgroups H of GL_n are exactly the subgroup varieties such that $H(k)$ is dense in $|H|$. Every affine algebraic group G has an associated matrix group G' such that $G'(k) = G(k)$. In good cases, $G' = G_{\mathrm{red}}$. In bad cases, $\dim G' < \dim G$.

h. 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 3.35. *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. Let $T_e(G)$ denote the tangent space at the neutral element of G . Recall (1.23) that $\dim G \leq \dim T_e(G)$, with equality if and only if G is smooth. As $T_e(G) \simeq \text{Hom}(\mathfrak{m}_e/\mathfrak{m}_e^2, k)$, (A.47), the hypothesis implies that $T_e(G) \simeq T_e(G_{\text{red}})$. Hence

$$\dim G \leq \dim T_e(G) = \dim T_e(G_{\text{red}}) \stackrel{1.22}{=} \dim G_{\text{red}}.$$

As $\dim G = \dim G_{\text{red}}$, this shows that $\dim G = \dim T_e(G)$ and G is smooth. \square

LEMMA 3.36. *Let V and V' be vector spaces over a field. Let W be a subspace of V , and let y be a nonzero element of V' . Then 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 $V \otimes V' \simeq (W \otimes V') \oplus (W' \otimes V')$. \square

LEMMA 3.37. *Let (A, Δ) be a Hopf algebra over k , and let I denote the kernel of the co-identity map ϵ .*

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

(b) *For all $a \in I$,*

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

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

(b) Let $a \in I$. Using the second diagram in (20), p.56, we find that

$$(\text{id} \otimes \epsilon)(\Delta(a) - a \otimes 1 - 1 \otimes a) = a \otimes 1 - a \otimes 1 - 1 \otimes 0 = 0$$

$$(\epsilon \otimes \text{id})(\Delta(a) - a \otimes 1 - 1 \otimes a) = 1 \otimes a - 0 \otimes 1 - 1 \otimes a = 0.$$

Hence

$$\begin{aligned} \Delta(a) - a \otimes 1 - 1 \otimes a &\in \text{Ker}(\text{id} \otimes \epsilon) \cap \text{Ker}(\epsilon \otimes \text{id}) \\ &= (A \otimes I) \cap (I \otimes A). \end{aligned}$$

That

$$(A \otimes I) \cap (I \otimes A) = I \otimes I$$

follows from comparing

$$A \otimes A = (k \otimes k) \oplus (k \otimes I) \oplus (I \otimes k) \oplus (I \otimes I)$$

$$A \otimes I = (k \otimes I) \oplus (I \otimes I)$$

$$I \otimes A = (I \otimes k) \oplus (I \otimes I). \quad \square$$

THEOREM 3.38 (CARTIER 1962). *Every affine algebraic group over a field of characteristic zero is smooth.*

PROOF. We may replace k with its algebraic closure. Thus, let G be an algebraic group over an algebraically closed field k of characteristic zero, and let $A = \mathcal{O}(G)$. Let $\mathfrak{m} = \mathfrak{m}_e = \text{Ker}(\epsilon)$. Let a be a nilpotent element of A ; according to (3.35), it suffices to show that a lies in \mathfrak{m}^2 .

If a maps to zero in $A_{\mathfrak{m}}$, then it maps to zero in $A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2$, and therefore in A/\mathfrak{m}^2 by (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 3.37)

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

Because Δ is a homomorphism of k -algebras,

$$0 = \Delta(a^n) = (\Delta a)^n = (a \otimes 1 + 1 \otimes a + y)^n. \quad (23)$$

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

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

As $a^n = 0$ and the terms with $i+j \geq 2$ lie in $A \otimes \mathfrak{m}^2$, equation (23) shows that

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

and so

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

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

$$na^{n-1} \otimes \bar{a} \in a^{n-1}\mathfrak{m} \otimes A/\mathfrak{m}^2 \quad (\text{inside } A \otimes (A/\mathfrak{m}^2)). \quad (24)$$

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 (see 3.36) $\bar{a} = 0$. In other words, $a \in \mathfrak{m}^2$, as required. \square

COROLLARY 3.39. *In characteristic zero, all finite algebraic groups are étale.*

PROOF. They are finite and smooth, and hence étale. \square

COROLLARY 3.40. *All surjective homomorphisms of affine algebraic groups in characteristic zero are smooth.*

PROOF. Apply (1.49). \square

COROLLARY 3.41. *Let H and H' be affine algebraic subgroups of an algebraic group G over a field k of characteristic zero. If $H(k^{\text{al}}) = H'(k^{\text{al}})$, then $H = H'$.*

PROOF. The condition implies that $H(k^{\text{al}}) = (H \cap H')(k^{\text{al}}) = H'(k^{\text{al}})$, and so $H = H \cap H' = H'$ (1.9). \square

COROLLARY 3.42. *Let G be an affine algebraic group over an algebraically closed field k of characteristic zero. Every closed subgroup S of $G(k)$ is of the form $H(k)$ for a unique algebraic subgroup H of G .*

PROOF. This follows from (3.18) and the theorem. \square

ASIDE 3.43. Theorem 3.38 fails for algebraic monoids. The algebraic scheme $M = \text{Spm}(k[T]/(T^n))$ admits a trivial monoid structure (e is the unique map $* \rightarrow M$ and m factors through $*$), but it is not reduced if $n > 1$.

ASIDE 3.44. We sketch a second proof of the theorem. Let \mathfrak{m} be the maximal ideal at e in $A = \mathcal{O}(G)$. It suffices to show that the graded ring $B = \bigoplus_n \mathfrak{m}^n / \mathfrak{m}^{n+1}$ has no nonzero nilpotents.² This ring inherits a Hopf algebra structure from A , and $\Delta(a) = a \otimes 1 + 1 \otimes a$ for $a \in \mathfrak{m}$ (by 3.37). Let x_1, \dots, x_m be a basis for $\mathfrak{m}/\mathfrak{m}^2$. We shall show that the x_i are algebraically independent in B (and so B is a polynomial ring over k). Suppose not, and let f be a nonzero homogeneous polynomial of least degree h such that $f(x_1, \dots, x_m) = 0$ (in B). Then

$$0 = \Delta(f(x_1, \dots, x_m)) = f(\Delta x_1, \dots, \Delta x_m) = f(x_1 \otimes 1 + 1 \otimes x_1, \dots, x_m \otimes 1 + 1 \otimes x_m).$$

On expanding the last expression as an element of $\sum_{i=0}^h B_{h-i} \otimes B_i$, we find that the term of bidegree $(h-1, 1)$ is

$$T_{h-1,1} = \sum_{j=1}^m \frac{\partial f}{\partial X_j}(x_1, \dots, x_m) \otimes x_j.$$

As the x_j are linearly independent, the condition $T_{h-1,1} = 0$ implies that $\frac{\partial f}{\partial X_j}(x_1, \dots, x_m) = 0$ for $j = 1, \dots, m$. Because we are in characteristic zero, at least one of these equations gives a nontrivial dependence relation (of degree $h-1$) between x_i , which contradicts the minimality of f .

For more details, see [Procesi 2007](#), Chapter 8, 7.3, p.235 or [Waterhouse 1979](#), 11.4.

ASIDE 3.45. Cartier announced his theorem in footnote 14 of [Cartier 1962](#):

Un raisonnement tout semblable prouve qu'un schéma en groupes de type fini sur un corps de caractéristique nulle est *réduit*.

The proof hinted at by Cartier is sketched in (3.44). The above proof follows [Oort 1966](#). Theorem 3.38 is true for all algebraic groups, not necessarily affine (see 10.36 below). See also DG II, §6, 1.1, p.255; [Mumford 2008](#), §11; SGA 3, VI_A, 6.9, p.332, and VI_B, 1.6.1, p.342.

i. Smoothness in characteristic $p \neq 0$

Let G be an affine algebraic group over a field k of characteristic $p \neq 0$.

PROPOSITION 3.46. *Assume that k is perfect. For all $r \geq 1$, the image of the homomorphism of k -algebras*

$$a \mapsto a^{p^r} : \mathcal{O}(G) \rightarrow \mathcal{O}(G)$$

is a Hopf subalgebra of $\mathcal{O}(G)$. For all sufficiently large r , it is geometrically reduced.

PROOF. Recall (2.16) that there is a homomorphism $F^r : G \rightarrow G^{(p^r)}$, which corresponds to the homomorphism of Hopf k -algebras

$$c \otimes a \mapsto ca^{p^r} : k \otimes_{f^r, k} \mathcal{O}(G) \rightarrow \mathcal{O}(G).$$

When k is perfect, this has image $\mathcal{O}(G)^{p^r}$, which is therefore a Hopf subalgebra of $\mathcal{O}(G)$ (3.11).

In proving the second part, we may assume 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 $a \in \mathfrak{N}$. Let r be such that $p^r \geq n$; then $a^{p^r} = 0$ for all $a \in \mathfrak{N}$. With this r , $\mathcal{O}(G)^{p^r}$ is reduced. \square

²In fact, $\text{Spm}(B)$ is the tangent cone at e .

j. Faithful flatness for Hopf algebras

In this section, we prove an important technical result.

THEOREM 3.47. *Let $A \subset B$ be finitely generated Hopf algebras over a field k . Then B is faithfully flat over A .*

STEP 0. *Assume that A is reduced.*

The homomorphism $A \rightarrow B$ of Hopf algebras corresponds to a homomorphism of affine algebraic groups $H \rightarrow G$. Because $A \rightarrow B$ is injective, the map $H(k^{\text{al}}) \rightarrow G(k^{\text{al}})$ is surjective. Therefore (1.52a) implies that the map $H \rightarrow G$ is faithfully flat if G is reduced. This proves the theorem when A is reduced.

STEP 1. *Assume that the augmentation ideal of A is nilpotent*

Recall (Exercise 2-1) that, for any homomorphism $H \rightarrow G$ of algebraic groups with kernel N , there is a canonical isomorphism $(h, n) \mapsto (hn, h): H \times N \rightarrow H \times_G H$. Because of the correspondence between algebraic groups and Hopf algebras, this implies that, for every homomorphism $A \rightarrow B$ of Hopf algebras, the map

$$b_1 \otimes b_2 \mapsto b_1 \otimes \bar{b}_2: B \otimes_A B \rightarrow B \otimes_k (B/I_A B) \quad (25)$$

is an isomorphism of left B -modules. Here I_A is the augmentation ideal $\text{Ker}(A \xrightarrow{\epsilon} k)$ of A .

Let $I = I_A$, and assume that I is nilpotent, say $I^n = 0$. Choose a family $(e_j)_{j \in J}$ of elements in B whose image in B/IB is a k -basis and consider the map

$$(a_j)_{j \in J} \mapsto \sum_j a_j e_j: A^{(J)} \rightarrow B \quad (26)$$

where $A^{(J)}$ is a direct sum of copies of A indexed by J . We shall show that (26) is an isomorphism (hence B is even free as an A -module).

Let C be the cokernel of (26). A diagram chase in

$$\begin{array}{ccccccc} A^{(J)} & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ \downarrow & & \downarrow & & & & \\ (A/I)^{(J)} & \xrightarrow{\text{onto}} & B/IB & & & & \end{array}$$

shows that every element of C is the image of an element of B mapping to zero in B/IB , i.e., lying in IB . Hence $C = IC$, and so $C = IC = I^2C = \dots = I^n C = 0$. Hence $A^{(J)} \rightarrow B$ is surjective.

For the injectivity, consider the diagrams

$$\begin{array}{ccc} A^{(J)} \xrightarrow{\text{onto}} B & & k^{(J)} \xrightarrow{\cong} B/IB \\ \downarrow & & \downarrow \\ M \longrightarrow B^{(J)} \xrightarrow{\text{onto}} B \otimes_A B & & (B/IB)^{(J)} \xrightarrow{\cong} (B/IB) \otimes_k (B/IB) \end{array}$$

in which the lower arrows are obtained from the upper arrows by tensoring on the left with B and B/IB respectively, and M is the kernel. If $b \in B^{(J)}$ maps to zero in $B \otimes_A B$,

then it maps to zero in $B/IB \otimes_k B/IB$, which implies that it maps to zero in $(B/IB)^{(J)}$. Therefore M is contained in $(IB)^{(J)} = I \cdot B^{(J)}$.

Recall (25) that

$$B \otimes_A B \simeq B \otimes_k B/IB$$

as left B -modules. As B/IB is free as a k -module (k is a field), $B \otimes_k B/IB$ is free as a left B -module, and so $B \otimes_A B$ is free (hence projective) as a left B -module. Therefore $B^{(J)}$ is a direct sum of B -submodules,

$$B^{(J)} = M \oplus N.$$

We know that

$$M \subset I \cdot B^{(J)} = IM \oplus IN,$$

and so $M \subset IM$. Hence $M \subset IM \subset I^2M = \dots = 0$. We have shown that $B^{(J)} \rightarrow B \otimes_A B$ is injective, and this implies that $A^{(J)} \rightarrow B$ is injective because $A^{(J)} \subset B^{(J)}$.

STEP 2. *General case*

Recall (Exercise 2-2) that for any diagram of algebraic groups

$$\begin{array}{ccccc} & & H & & \\ & & \downarrow \beta & & \\ M & \longrightarrow & G & \longrightarrow & G', \end{array}$$

with M the kernel of $G \rightarrow G'$, there is a canonical isomorphism

$$(m, h) \mapsto (mh, h): M \times H \simeq G \times_{G'} H. \quad (27)$$

After Theorem 3.38, we may suppose that k has characteristic $p \neq 0$. According to (3.46), there exists an n such that $\mathcal{O}(G)^{p^n}$ is a reduced Hopf subalgebra of $\mathcal{O}(G)$. Let G' be the algebraic group such that $\mathcal{O}(G') = \mathcal{O}(G)^{p^n}$, and consider the diagrams

$$\begin{array}{ccccc} N & \longrightarrow & H & \longrightarrow & G' \\ \downarrow & & \downarrow & & \parallel \\ M & \longrightarrow & G & \longrightarrow & G' \end{array} \quad \begin{array}{ccccc} \mathcal{O}(N) & \longleftarrow & \mathcal{O}(H) & \xleftarrow[\text{flat}]{\text{faithfully}} & \mathcal{O}(G') \\ \uparrow & & \uparrow \text{injective} & & \parallel \\ \mathcal{O}(M) & \longleftarrow & \mathcal{O}(G) & \longleftarrow & \mathcal{O}(G') \end{array}$$

where N and M are the kernels of the homomorphisms $H \rightarrow G'$ and $G \rightarrow G'$ respectively. Because $\mathcal{O}(G')$ is reduced, the homomorphism $\mathcal{O}(G') \rightarrow \mathcal{O}(H)$ is faithfully flat, and so $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ remains injective after it has been tensored with $\mathcal{O}(H)$:

$$\begin{array}{ccc} \mathcal{O}(G) \otimes_{\mathcal{O}(G')} \mathcal{O}(H) & \xrightarrow{\text{injective}} & \mathcal{O}(H) \otimes_{\mathcal{O}(G')} \mathcal{O}(H) \\ \downarrow \simeq (27) & & \downarrow \simeq (25) \\ \mathcal{O}(M) \otimes \mathcal{O}(H) & \dashrightarrow & \mathcal{O}(N) \otimes \mathcal{O}(H). \end{array}$$

Because $k \rightarrow \mathcal{O}(H)$ is faithfully flat (k is a field), the injectivity of the dashed arrow implies that $\mathcal{O}(M) \rightarrow \mathcal{O}(N)$ is injective, and hence it is faithfully flat (because the augmentation ideal of $\mathcal{O}(M)$ is nilpotent). Now the dashed arrow's being faithfully flat, implies that the top arrow is faithfully flat, which, because $\mathcal{O}(G') \rightarrow \mathcal{O}(H)$ is faithfully flat, implies that $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is faithfully flat (CA 11.7).

CONSEQUENCES

- 3.48. Theorem 3.47 holds for all Hopf algebras (not necessarily finitely generated).
- 3.49. Let $A \subset B$ be Hopf algebras. If A and B are integral domains with fields of fractions K and L , then $B \cap K = A$.
- 3.50. Let $A \subset B$ be Hopf algebras. If A and B are integral domains with the same field of fractions, then $A = B$.
- 3.51. A Hopf algebra A is finitely generated if it is an integral domain and its field of fractions is a finitely generated field extension.
- 3.52. Let G be a smooth affine algebraic group. Every Hopf subalgebra of $\mathcal{O}(G)$ is finitely generated (and so corresponds to a quotient of G).

ASIDE 3.53. See Waterhouse 1979, Chapter 14, and Takeuchi, Mitsuhiro. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.* 7 (1972), 251–270.

Exercises

EXERCISE 3-1. We use the notations of Exercise 3.6, p.57. Let Γ be an arbitrary group. From a homomorphism $\rho: \Gamma \rightarrow \mathrm{GL}_n(k)$, we obtain a family of functions $g \mapsto \rho(g)_{i,j}$, $1 \leq i, j \leq n$, on G . Let $R'(\Gamma)$ be the k -subspace of $R(\Gamma)$ spanned by the functions arising in this way for varying n . (The elements of $R'(\Gamma)$ are called the **representative functions** on Γ .)

- Show that $R'(\Gamma)$ is a k -subalgebra of $R(\Gamma)$.
- Show that Δ maps $R'(\Gamma)$ into $R'(\Gamma) \otimes R'(\Gamma)$.
- Deduce that Δ , ϵ , and S define on $R'(\Gamma)$ the structure of a Hopf algebra.

EXERCISE 3-2. Let A be a Hopf algebra. Prove the following statements by interpreting them as statements about algebraic groups.

- $S \circ S = \mathrm{id}_A$.
- $\Delta \circ S = t \circ (S \otimes S) \circ \Delta$ where $t(a \otimes b) = b \otimes a$.
- $\epsilon \circ S = \epsilon$.
- The map $a \otimes b \mapsto (a \otimes 1)\Delta(b): A \otimes A \rightarrow A \otimes A$ is a homomorphism of k -algebras.

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

EXERCISE 3-3. Verify directly that $\mathcal{O}(\mathbb{G}_a)$ and $\mathcal{O}(\mathrm{GL}_n)$ satisfy the axioms to be a Hopf algebra.

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 .

Linear representations of algebraic groups

Throughout this chapter, G is an affine algebraic group over k . We shall see later (10.33) that every algebraic group G over k has a greatest 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

Let V be a vector space over k . We let GL_V denote the functor of k -algebras,

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

When V is finite dimensional, GL_V is an algebraic group.

A **linear representation** of G is a homomorphism $r: G \rightarrow \text{GL}_V$ of group-valued functors. When V is finite dimensional, r is a homomorphism of algebraic groups. A linear representation ρ is **faithful** if $\rho(R)$ is injective for all k -algebras R . For finite-dimensional linear representations, this is equivalent to ρ being a closed immersion (see 5.18 below). From now on we write “representation” for “linear representation”.

To give a representation (V, r) of G on V is the same as giving an action

$$G \times V_{\mathfrak{a}} \rightarrow V_{\mathfrak{a}}$$

of G on the functor $V_{\mathfrak{a}}$ such that, for all small k -algebras R , $G(R)$ acts on $V_{\mathfrak{a}}(R) \stackrel{\text{def}}{=} R \otimes V$ through R -linear maps. When viewed in this way, we call (V, r) a **G -module**.

A (right) **$\mathcal{O}(G)$ -comodule** is a k -linear map $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ such that

$$\begin{cases} (\text{id}_V \otimes \Delta) \circ \rho &= (\rho \otimes \text{id}_{\mathcal{O}(G)}) \circ \rho \\ (\text{id}_V \otimes \epsilon) \circ \rho &= \text{id}_V. \end{cases} \quad (28)$$

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.

4.1. Let $r: G \rightarrow \text{GL}_V \subset \text{End}_V$ be a representation. Then r maps the universal element a in $G(\mathcal{O}(G))$ to an $\mathcal{O}(G)$ -linear endomorphism $r(a)$ of $\text{End}(V \otimes \mathcal{O}(G))$, which is uniquely determined by its restriction to a k -linear homomorphism $\rho: V \rightarrow V \otimes \mathcal{O}(G)$. The map ρ

is an $\mathcal{O}(G)$ -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 $\mathcal{O}(G)$ -comodule structures on V . The map ρ is called the **co-action** corresponding to r .

More explicitly, let $(e_i)_{i \in I}$ be a basis for V and let $(r_{ij})_{i,j \in I}$ be a family of elements of $\mathcal{O}(G)$. The map

$$\rho: V \rightarrow V \otimes \mathcal{O}(G), \quad e_j \mapsto \sum_{i \in I} e_i \otimes r_{ij} \quad (\text{finite sum}),$$

is a comodule structure on V if and only if

$$\left. \begin{aligned} \Delta(r_{ij}) &= \sum_{l \in I} r_{il} \otimes r_{lj} \\ \epsilon(r_{ij}) &= \delta_{ij} \end{aligned} \right\} \quad \text{all } i, j \in I. \quad (29)$$

A family (r_{ij}) satisfying these conditions¹ defines a representation r of G on V , namely, that sending $g \in G(R)$ to the automorphism of V_R with matrix $(r_{ij}(g))_{i,j \in I}$. Assume 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 $\mathcal{O}(\text{End}_V)$ is a polynomial ring in the symbols T_{ij} , and the homomorphism $\mathcal{O}(\text{End}_V) \rightarrow \mathcal{O}(G)$ defined by r sends T_{ij} to r_{ij} .

EXAMPLE 4.2. Let $G = \text{GL}_n$ and let r be the standard representation of G on $V = k^n$. Then $\mathcal{O}(G) = k[T_{11}, T_{12}, \dots, T_{nn}, 1/\det]$ and, relative to the standard basis $(e_i)_{1 \leq i \leq n}$ for V , the map $r: G(R) \rightarrow \text{GL}_n(R)$ is (tautologically) $g \mapsto (T_{ij}(g))_{1 \leq i, j \leq n}$. Correspondingly, the co-action is

$$\rho: V \rightarrow V \otimes \mathcal{O}(G), \quad e_j \mapsto \sum_{1 \leq i \leq n} e_i \otimes T_{ij}.$$

Since $\Delta(T_{ij}) = \sum_{1 \leq l \leq n} T_{il} \otimes T_{lj}$ and $\epsilon(T_{ij}) = \delta_{ij}$, this does define a comodule structure on V .

b. Stabilizers

PROPOSITION 4.3. *Let $r: G \rightarrow \text{GL}_V$ be a finite-dimensional representation of G , and let W be a subspace of V . The functor*

$$R \mapsto G_W(R) = \{\alpha \in G(R) \mid \alpha(W_R) = W_R\}$$

is represented by an algebraic subgroup G_W of G .

PROOF. Let $\rho: \mathcal{O}(G) \rightarrow V \otimes \mathcal{O}(G)$ be the corresponding co-action. Let $(e_i)_{i \in J}$ be a basis for W , and extend it to a basis $(e_i)_{i \in J \sqcup I}$ for V . Write

$$\rho(e_j) = \sum_{i \in J \sqcup I} e_i \otimes a_{ij}, \quad a_{ij} \in \mathcal{O}(G).$$

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

$$ge_j = \sum_{i \in J \sqcup I} e_i \otimes g(a_{ij}).$$

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 $\mathcal{O}(G)$ by the ideal generated by $\{a_{ij} \mid j \in J, i \in I\}$. \square

¹When I is infinite, it is necessary to require that, for all j , the element $r_{ij} = 0$ for almost all i .

The subgroup G_W of G is called the *stabilizer* of W in V , and is sometimes denoted $\text{Stab}_G(W)$. We say that an algebraic subgroup H of G *stabilizes* a subspace W of V if $H \subset G_W$.

COROLLARY 4.4. *Let H be an algebraic subgroup of G such that $H(k)$ is dense in H . If $hW = W$ for all $h \in H(k)$, then H stabilizes W .*

PROOF. The condition implies that $(H \cap G_W)(k) = H(k)$, and so $H \cap G_W = H$. \square

PROPOSITION 4.5. *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 (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 $\mathcal{O}(G_{W \otimes W'})$, from which one can deduce that

$$\mathfrak{a}(W \otimes W') = \mathfrak{a}(W) + \mathfrak{a}(W'). \quad \square$$

c. Every representation is a union of finite-dimensional representations

PROPOSITION 4.6. *Every $\mathcal{O}(G)$ -comodule (V, ρ) is a filtered union of its finite-dimensional sub-comodules.*

PROOF. As a finite sum of finite-dimensional sub-comodules is a finite-dimensional sub-comodule, it suffices to show that each element v of V is contained in a finite-dimensional sub-comodule. Let $(e_i)_{i \in I}$ be a basis for $\mathcal{O}(G)$ as a k -vector space, and let

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

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

$$\Delta(e_i) = \sum_{j,k} r_{ijk} (e_j \otimes e_k), \quad r_{ijk} \in k.$$

We shall show that

$$\rho(v_k) = \sum_{i,j} r_{ijk} (v_i \otimes e_j) \quad (30)$$

from which it follows that the k -subspace of V spanned by v and the v_i is a subcomodule containing v . Recall from (28) that

$$(\text{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \text{id}_{\mathcal{O}(G)}) \circ \rho.$$

On applying each side of this equation to v , we find that

$$\sum_{i,j,k} r_{ijk} (v_i \otimes e_j \otimes e_k) = \sum_k \rho(v_k) \otimes e_k \quad (\text{inside } V \otimes \mathcal{O}(G) \otimes \mathcal{O}(G)).$$

On comparing the coefficients of $1 \otimes 1 \otimes e_k$ in these two expressions, we obtain (30). \square

COROLLARY 4.7. *Every representation of G is a filtered union of its finite-dimensional subrepresentations.*

PROOF. Let $r: G \rightarrow \text{GL}_V$ be representation of G , and let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be 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. \square

d. Affine algebraic groups are linear

A right action of an algebraic group G on an algebraic scheme X is a regular map $X \times G \rightarrow X$ such that, for all k -algebras R , the map $X(R) \times G(R) \rightarrow X(R)$ is a right action of the group $G(R)$ on the set $X(R)$. Such an action defines a map

$$\mathcal{O}(X) \rightarrow \mathcal{O}(X) \otimes \mathcal{O}(G),$$

which makes $\mathcal{O}(X)$ into an $\mathcal{O}(G)$ -comodule. In this way, we get a 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 $m: G \times G \rightarrow G$ is called the **regular representation**. The corresponding co-action is $\Delta: \mathcal{O}(G) \rightarrow \mathcal{O}(G) \otimes \mathcal{O}(G)$.

THEOREM 4.8. *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 $(e_i)_{1 \leq i \leq n}$ be a basis for V , and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. According to (4.1), the image of $\mathcal{O}(\mathrm{GL}_V) \rightarrow A$ contains the a_{ij} . But, because $\epsilon: A \rightarrow k$ is a co-identity (21),

$$e_j = (\epsilon \otimes \mathrm{id}_A)\Delta(e_j) = \sum_i \epsilon(e_i)a_{ij},$$

and so the image contains V ; it therefore equals A . We have shown that $\mathcal{O}(\mathrm{GL}_V) \rightarrow A$ is surjective, which means that $G \rightarrow \mathrm{GL}_V$ is a closed immersion. \square

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 , 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 (1.29), and the theorem shows that the converse is true. Therefore, the linear algebraic groups over k are exactly the affine algebraic groups.

e. Constructing all finite-dimensional representations

Let G be an algebraic group over k , and let V be a finite-dimensional k -vector space. The k -vector space $V \otimes \mathcal{O}(G)$ equipped with the k -linear map

$$\mathrm{id}_V \otimes \Delta: V \otimes \mathcal{O}(G) \rightarrow V \otimes \mathcal{O}(G) \otimes \mathcal{O}(G)$$

is an $\mathcal{O}(G)$ -comodule, called the **free comodule on V** (compare the definitions). 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 $(\mathcal{O}(G), \Delta)$:

$$\begin{array}{ccc} V \otimes \mathcal{O}(G) & \xrightarrow{V \otimes \Delta} & V \otimes \mathcal{O}(G) \otimes \mathcal{O}(G) \\ \downarrow \approx & & \downarrow \approx \\ \mathcal{O}(G)^n & \xrightarrow{\Delta^n} & (\mathcal{O}(G) \otimes \mathcal{O}(G))^n. \end{array}$$

PROPOSITION 4.9. *Let (V, ρ) be an $\mathcal{O}(G)$ -comodule. Let V_0 denote V regarded as a k -vector space, and let $(V_0 \otimes \mathcal{O}(G), \text{id}_{V_0} \otimes \Delta)$ be the free comodule on V_0 . Then*

$$\rho: V \rightarrow V_0 \otimes \mathcal{O}(G)$$

is an injective homomorphism of $\mathcal{O}(G)$ -comodules.

PROOF. The commutative diagram (see (28), p.69)

$$\begin{array}{ccc} V & \xrightarrow{\rho} & V_0 \otimes \mathcal{O}(G) \\ \downarrow \rho & & \downarrow \text{id}_{V_0} \otimes \Delta \\ V \otimes \mathcal{O}(G) & \xrightarrow{\rho \otimes \text{id}_{\mathcal{O}(G)}} & V_0 \otimes \mathcal{O}(G) \otimes \mathcal{O}(G) \end{array}$$

says exactly that the map $\rho: V \rightarrow V_0 \otimes \mathcal{O}(G)$ is a homomorphism of $\mathcal{O}(G)$ -comodules. It is injective because its composite with $\text{id}_V \otimes \epsilon$ is id_V (ibid.). \square

COROLLARY 4.10. *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

COROLLARY 4.11. *Every finite-dimensional representation of G arises as a subrepresentation of a direct sum of copies of the regular representation.*

PROOF. Restatement of (4.10). \square

THEOREM 4.12. *Let (V, r) be a faithful finite-dimensional representation of G . Then every finite-dimensional representation W of G is isomorphic to a subquotient of a direct sum of representations $\bigotimes^m (V \oplus V^\vee)$.*

PROOF. After (4.9), we may assume that $W \subset \mathcal{O}(G)^n$ for some n . Let W_i be the image of W under the i th projection $\mathcal{O}(G)^n \rightarrow \mathcal{O}(G)$; then $W \hookrightarrow \bigoplus_i W_i$, and so we may even assume that $W \subset \mathcal{O}(G)$.

We choose a basis for V , and use it to identify G with a subgroup of GL_n . Then there is a surjective homomorphism

$$\mathcal{O}(\text{GL}_n) = k[T_{11}, T_{12}, \dots, T_{nn}, 1/\det] \twoheadrightarrow \mathcal{O}(G) = k[t_{11}, t_{12}, \dots, t_{nn}, 1/\det].$$

As W is finite dimensional, it is contained in a subspace

$$\{f(t_{ij}) \mid \deg f \leq s\} \cdot \det^{-s'}$$

of $\mathcal{O}(G)$ for some $s, s' \in \mathbb{N}$.

Let $(e_i)_{1 \leq i \leq n}$ denote the standard basis for k^n . 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

$$e_j \mapsto T_{ij}: (V, \rho) \rightarrow (\mathcal{O}(\text{GL}_n), \Delta)$$

is a homomorphism of $\mathcal{O}(\text{GL}_n)$ -comodules (see (8), p.41). Thus the homogeneous polynomials of degree 1 in the T_{ij} form an $\mathcal{O}(\text{GL}_n)$ -comodule isomorphic to the direct sum of n copies of (V, r) . We can construct the $\mathcal{O}(\text{GL}_n)$ -comodule

$$\{f \in k[T_{11}, T_{12}, \dots] \mid f \text{ homogeneous of degree } s\}$$

as a quotient of the s -fold tensor product of

$$\{f \in k[T_{11}, T_{12}, \dots] \mid f \text{ homogeneous of degree } 1\}.$$

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 $\{f \mid \deg f \leq s\}$, and by tensoring this r -times with $1/\det$ we get $\{f(T_{ij}) \mid \deg f \leq s\} \cdot \det^{-s}$. Now W is a subrepresentation of a quotient of this representation. \square

The dual was only used to construct the representation $1/\det$, and so it is not needed for subgroups of SL_n .

4.13. Here is a more abstract statement of the proof. Let (V, r) be a faithful representation of G of dimension n , and let W be 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 $\mathcal{O}(\mathrm{GL}_V) \rightarrow \mathcal{O}(G)$. 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

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.²

PROPOSITION 4.14. *Let G be an algebraic group over k , and let (V, r) be a representation of G . If V is a sum of simple subrepresentations, say $V = \sum_{i \in I} S_i$ (the sum need not be direct), then for 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 the sum $S_J \stackrel{\mathrm{def}}{=} \sum_{j \in J} S_j$ is direct and $W \cap S_J = 0$. I claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). For this, it suffices to show that each S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals S_i or 0. In the first case, $S_i \subset W + S_J$, and in the second $S_J \cap S_i = 0$ and $W \cap (S_J + S_i) = 0$, contradicting the definition of I . \square

²Traditionally, simple (resp. semisimple) representations of G are said to 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” in both situations.

We have seen that if V is semisimple, then every subrepresentation W is a direct summand. The converse of this is also true. Let V be a representation such that every subrepresentation has a complement. Let v be a nonzero element of V , and let W be maximal among the subrepresentations not containing v (exists by Zorn's lemma). Then V/W is simple, and so $V = W \oplus S$ with S simple. Using this, one shows that V is a sum of simple modules (Jacobson, Basic Algebra II, p.120).

g. Characters and eigenspaces

A **character** of an algebraic group G is a homomorphism $G \rightarrow \mathbb{G}_m$. As $\mathcal{O}(\mathbb{G}_m) = k[X, X^{-1}]$ and $\Delta(X) = X \otimes X$, 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

$$G \xrightarrow{\chi} \mathbb{G}_m \hookrightarrow \mathrm{GL}_V. \quad (31)$$

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 $r: G \rightarrow \mathrm{GL}_V$ be a representation of G , and let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be the corresponding co-action. Let χ be a character of G , and let $a(\chi)$ be the corresponding group-like element of $\mathcal{O}(G)$. Then (see (31)), G acts on V through χ if and only if ρ factors as

$$V \xrightarrow{v \mapsto v \otimes X} V \otimes \mathcal{O}(\mathbb{G}_m) \xrightarrow{v \otimes X \mapsto v \otimes a(\chi)} V \otimes \mathcal{O}(G),$$

i.e., if and only if

$$\rho(v) = v \otimes a(\chi), \quad \text{all } v \in V. \quad (32)$$

More generally, we say that G acts on a subspace W of V **through a character** χ if W is stable under G and G acts on W through χ . Note that this means, in particular, that the elements of W are common eigenvectors for the $g \in G(k)$: if $w \in W$, then for every $g \in G(k)$, $r(g)w$ is a scalar multiple of w . If G acts on subspaces W and W' through a character χ , then it acts on $W + W'$ through χ . Therefore, there is a greatest subspace V_χ of V on which G acts through χ , called the **eigenspace for G with character χ** .

PROPOSITION 4.15. *Let (V, r) be a representation of G , and let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be 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 (32)), and it clearly contains every such subspace. \square

Let A be a Hopf algebra, and let a be a group-like element of A . Then, from the second diagram in (20), p.56, we see that

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

and so $\epsilon(a) = 1$.

LEMMA 4.16. *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 $e_i \neq e$:

$$e = \sum_i c_i e_i, \quad c_i \in k. \quad (33)$$

We may even suppose that the e_i occurring in the sum are linearly independent. Now

$$\begin{aligned} \Delta(e) &= e \otimes e = \sum_{i,j} c_i c_j e_i \otimes e_j \\ \Delta(e) &= \sum_i c_i \Delta(e_i) = \sum_i c_i e_i \otimes e_i. \end{aligned}$$

The $e_i \otimes e_j$ are also linearly independent, and so this implies that

$$\begin{cases} c_i c_i = c_i & \text{all } i \\ c_i c_j = 0 & \text{if } i \neq j. \end{cases}$$

We also know that

$$1 = \epsilon(e) = \sum c_i \epsilon(e_i) = \sum c_i.$$

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

THEOREM 4.17. *Let $\rho: G \rightarrow \text{GL}(V)$ be a representation of an algebraic group on a vector space V . If V is a sum of eigenspaces, say $V = \sum_{\chi \in \mathcal{E}} V_\chi$ with \mathcal{E} a set of characters of G , then it is a direct sum of the eigenspaces*

$$V = \bigoplus_{\chi \in \mathcal{E}} V_\chi.$$

PROOF. We shall make use of Lemma 4.16. If the sum is not direct, then there exists a finite set $\{\chi_1, \dots, \chi_m\}$, $m \geq 2$, and a relation

$$v_1 + \dots + v_m = 0, \quad v_i \in V_{\chi_i}, \quad v_i \neq 0.$$

On applying ρ to this relation, we find that

$$0 = \rho(v_1) + \dots + \rho(v_m) = v_1 \otimes a(\chi_1) + \dots + v_m \otimes a(\chi_m).$$

For every linear map $f: V \rightarrow k$,

$$0 = f(v_1) \cdot a(\chi_1) + \dots + f(v_m) \cdot a(\chi_m),$$

which contradicts the linear independence of the $a(\chi_i)$. \square

As one-dimensional representations are simple, (4.14) shows that V in (4.17) is a direct sum of one-dimensional eigenspaces, but this is a weaker statement than the theorem.

Later (14.12) 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 let χ be 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 4.18. *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 (4.11), χ occurs in $\mathcal{O}(G)^n$ for some n , i.e., there exists a nonzero subspace W of $\mathcal{O}(G)^n$ such that H acts on W through χ . Under some projection $\mathcal{O}(G)^n \rightarrow \mathcal{O}(G)$, W maps to a nonzero subspace of $\mathcal{O}(G)$, which shows that χ occurs in $\mathcal{O}(G)$. \square

h. Chevalley's theorem

THEOREM 4.19 (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 $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$. According to (4.6), 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 $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is a homomorphism of Hopf algebras

$$\begin{aligned} \Delta(\mathfrak{a}) &\subset \mathcal{O}(G) \otimes \mathfrak{a} + \mathfrak{a} \otimes \mathcal{O}(G), \\ \epsilon(\mathfrak{a}) &= 0 \end{aligned}$$

(see 3.13). The first of these applied to e_j , $j \in J$, shows that $\mathfrak{a}' \subset \mathfrak{a}$, and the second shows that

$$e_j = (\epsilon, \text{id})\Delta(e_j) = \sum_{i \in I} \epsilon(e_i)a_{ij}.$$

As the e_j , $j \in J$, generate \mathfrak{a} (as an ideal), so do the a_{ij} , $j \in J$, and so $\mathfrak{a}' = \mathfrak{a}$. Thus $H = G_W$. The next (elementary) lemma allows us to replace W with the one-dimensional subspace $\bigwedge^d W$ of $\bigwedge^d V$. \square

LEMMA 4.20. *Let W be a subspace of dimension d in a vector space V , and let D denote the one-dimensional subspace $\bigwedge^d W$ of $\bigwedge^d V$. Let α be an automorphism of V_R for some k -algebra R . Then $\alpha W_R = W_R$ if and only if $(\bigwedge^d \alpha)D_R = D_R$.*

PROOF. Let $(e_j)_{1 \leq j \leq d}$ be a basis for W , and extend it to a basis $(e_i)_{1 \leq i \leq n}$ of V . Let $w = e_1 \wedge \dots \wedge e_d$. For all k -algebras R ,

$$W_R = \{v \in V_R \mid w \wedge v = 0 \text{ (in } \bigwedge^{d+1} V_R)\}.$$

To see this, let $v \in V_R$ and write $v = \sum_{i=1}^n a_i e_i$, $a_i \in R$. Then

$$w \wedge v = \sum_{d+1 \leq i \leq n} a_i e_1 \wedge \cdots \wedge e_d \wedge e_i.$$

As the elements $e_1 \wedge \cdots \wedge e_d \wedge e_i$, $d+1 \leq i \leq n$, are linearly independent in $\wedge^{d+1} V$, we see that

$$w \wedge v = 0 \iff a_i = 0 \text{ for all } d+1 \leq i \leq n.$$

Let $\alpha \in \text{GL}(V_R)$. If $\alpha W_R = W_R$, then obviously $(\wedge^d \alpha)(D_R) = D_R$. Conversely, suppose that $(\wedge^d \alpha)(D_R) = D_R$, so that $(\wedge^d \alpha)w = cw$ for some $c \in R^\times$. If $v \in W_R$, then $w \wedge v = 0$, and so

$$0 = (\wedge^{d+1} \alpha)(w \wedge v) = (\wedge^d \alpha)w \wedge \alpha v = c(w \wedge (\alpha v)),$$

which implies that $\alpha v \in W_R$. □

REMARK 4.21. Theorem 4.19 is stronger than the usual form of the theorem (Borel 1991, Springer 1998) 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.70). On applying this with $R = k[\varepsilon]$, $\varepsilon^2 = 0$, we find that the Lie algebra of H is the stabilizer of L in $\text{Lie}(G)$ — see (12.26) below.

i. The subspace fixed by a group

Let G be an algebraic group (not necessarily affine), and let (V, r) be a representation of G . We let V^G denote the subspace of V fixed by G :

$$V^G \stackrel{\text{def}}{=} \{v \in V \mid g \cdot v_R = v_R \text{ (in } V_R) \text{ for all } k\text{-algebras } R \text{ and all } g \in G(R)\}.$$

PROPOSITION 4.22. 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 $s \mapsto s \otimes 1_R: S \rightarrow S \otimes R$. By hypothesis, $\sum v_i \otimes 1_S \otimes e_i$ is fixed by g' :

$$g' \cdot (\sum v_i \otimes 1_S \otimes e_i) = \sum v_i \otimes 1_S \otimes e_i.$$

But,

$$g' \cdot (\sum v_i \otimes 1_S \otimes e_i) = \sum g(v_i \otimes 1_S) \otimes e_i$$

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 . □

COMPLEMENTS

4.23. If $G(k')$ is dense in G , then

$$V^G = V \cap V(k')^{G(k')}$$

(because the stabilizer G_W of $W \stackrel{\text{def}}{=} V \cap V(k')^{G(k')}$ has the property that $G_W(k') = G(k')$). For example, if G is a connected group variety over a perfect infinite field (3.26), or a group variety over a separably closed field (1.9d), then

$$V^G = V(k)^{G(k)}.$$

4.24. Let ρ be the co-action of (V, r) . The subspace V^G of V is the kernel of the linear map

$$v \mapsto \rho(v) - v \otimes 1: V \rightarrow V \otimes \mathcal{O}(G)$$

(because this is the subspace fixed by the universal element $\text{id} \in G(\mathcal{O}(G))$). It follows that

$$(V \otimes k')^{G_{k'}} \simeq V^G \otimes k',$$

for every field k' containing k .

4.25. 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 (4.22) shows that

$$(V^G)_{\mathfrak{a}} = (V_{\mathfrak{a}})^G.$$

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 affine algebraic groups over a field k .

a. Terminology on functors

All functors are from Alg_k^0 to Set .

DEFINITION 5.1. A **flat sheaf** (better, **sheaf for the flat (fpqc) topology**) is a functor $F: \text{Alg}_k^0 \rightarrow \text{Set}$ such that

- (a) (local) for all small k -algebras R_1, \dots, R_m

$$F(R_1 \times \dots \times R_m) \simeq F(R_1) \times \dots \times F(R_m);$$

- (b) (descent) for all faithfully flat maps $R \rightarrow R'$ of small k -algebras, the sequence

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

is exact, i.e., the first arrow is the equalizer of the pair of arrows. The maps in the pair are defined by the homomorphisms $R' \rightarrow R' \otimes_R R'$ sending r to $r \otimes 1$ or $1 \otimes r$.

A **morphism** of flat sheaves is a natural transformation (map of functors).

EXAMPLE 5.2. Let $F = h^A \stackrel{\text{def}}{=} \text{Hom}(A, -)$ for some k -algebra A . Then F is a sheaf. Condition (a) is obvious, and condition (b) follows from the exactness of

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

for any faithfully flat homomorphism $R \rightarrow R'$ (CA 11.9). Similarly, for every algebraic scheme X , the functor h_X is a flat sheaf.

DEFINITION 5.3. A subfunctor D of a functor F is **fat**¹ if, for every small R and $x \in F(R)$, there exists a finite faithfully flat family² 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 .

¹In DG III, §1, 1.4, p.285, a fat subfunctor is said to be “dodu” (Larousse: dodu adj. Se dit d’un animal gras, bien en chair).

²This means that the map $R \rightarrow \prod R_i$ is faithfully flat.

LEMMA 5.4. Let D be a fat subfunctor of a sheaf S . Every morphism $D \rightarrow S'$ from D to a sheaf S' extends uniquely to S .

PROOF. Obvious. \square

REMARK 5.5. A subfunctor D of a functor F is fat if it satisfies the following condition:

(*) for every small k -algebra R and $x \in F(R)$, there exists a faithfully flat R -algebra R' such that the image of x in $F(R')$ belongs to $D(R')$.

Conversely, if F is a sheaf and D is a fat subfunctor such that $D(\prod R_i) \rightarrow \prod D(R_i)$ is surjective for all finite families (R_i) of k -algebras, then D satisfies (*).

In fact, our fat subsheaves will usually satisfy (*).

LEMMA 5.6. Let $\varphi: Y \rightarrow X$ be a faithfully flat morphism of algebraic schemes over k . The functor $R \mapsto \varphi(Y(R))$ is a fat subfunctor of \tilde{X} .

PROOF. We check the condition (5.5(*)). Let R be a k -algebra, and let $x \in X(R)$. Write $Y \times_X \text{Spm}(R)$ as a finite union of open affines U_i . Let $R_i = \mathcal{O}(U_i)$, and let $R' = \prod_i R_i$:

$$\begin{array}{ccccc} Y & \longleftarrow & Y \times_X \text{Spm}(R) & \longleftarrow & \bigsqcup_i U_i = \text{Spm}(R') \\ \downarrow \varphi & & \downarrow \text{faithfully flat} & & \\ X & \xleftarrow{x} & \text{Spm}(R), & & \end{array}$$

Then R' is a faithfully flat R -algebra, and the image of x in $X(R')$ lifts to Y (i.e., the map $\text{Spm}(R') \rightarrow \text{Spm}(R) \xrightarrow{x} X$ factors through $Y \xrightarrow{\varphi} X$). \square

b. Definitions

DEFINITION 5.7. A homomorphism $G \rightarrow Q$ of algebraic groups is a **quotient map** if it is faithfully flat.

In other words, “quotient map” of algebraic groups means “faithfully flat homomorphism”. For affine algebraic groups, the condition means that the map of k -algebras $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is faithfully flat. A quotient map remains a quotient map after extension of the base field.

PROPOSITION 5.8. *Quotients of smooth algebraic groups are smooth.*

PROOF. Let $q: G \rightarrow Q$ be a quotient map. Then $\mathcal{O}_Q \rightarrow q_*\mathcal{O}_G$ is injective, and remains injective after extension of the base field. Therefore \mathcal{O}_Q is geometrically reduced (hence smooth 1.22), if G is. \square

A quotient map $\varphi: G \rightarrow Q$ is surjective as a map of schemes (i.e., $|\varphi|$ is surjective), but a surjective homomorphism need not be flat. For example, let G be a nonreduced algebraic group over a perfect field; then G_{red} is an algebraic subgroup of G and the inclusion map $G_{\text{red}} \rightarrow G$ is surjective without being a quotient map. As another example, the trivial homomorphism $\mathbb{G}_m \rightarrow \alpha_p$ is surjective without being a quotient map.

DEFINITION 5.9. A homomorphism $G \rightarrow H$ of algebraic groups is an **embedding** if it is a closed immersion.

In other words, “embedding” of algebraic groups means “morphism that is both a homomorphism and a closed immersion”. For affine algebraic groups, the condition means that the map $\mathcal{O}(H) \rightarrow \mathcal{O}(G)$ is surjective. An embedding remains an embedding after extension of the base field.

An embedding $\varphi: G \rightarrow H$ 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 $\alpha_p \rightarrow e$ is injective but not an embedding.

PROPOSITION 5.10. *The following conditions on a homomorphism $\varphi: G \rightarrow H$ of algebraic groups over k are equivalent:*

- (a) $\varphi(R): G(R) \rightarrow H(R)$ is injective for all (small) k -algebras R ;
- (b) $\text{Ker}(\varphi) = e$;
- (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. (b) \Leftrightarrow (a): The sequence

$$e \rightarrow \text{Ker}(\varphi)(R) \rightarrow G(R) \rightarrow H(R)$$

is exact for all R .

(c) \Rightarrow (b): There are two homomorphisms $\text{Ker}(\varphi) \rightarrow G$ whose composite with φ is the trivial homomorphism, namely, the given inclusion and the trivial homomorphism. The two must be equal, and so $\text{Ker}(\varphi)$ is trivial.

(d) \Rightarrow (c): This is obvious.

(a) \Rightarrow (d): Let $\varphi_1, \varphi_2: X \rightarrow G$ 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 , which implies that $\varphi_1(R) = \varphi_2(R)$ for all R . This implies that $\varphi_1 = \varphi_2$ (Yoneda lemma). \square

DEFINITION 5.11. A homomorphism $\varphi: G \rightarrow H$ of algebraic groups is a **monomorphism** if it satisfies the equivalent conditions of the proposition.

PROPOSITION 5.12. *If a homomorphism of algebraic groups is both a monomorphism and a quotient map, then it is an isomorphism.*

PROOF. Let $\varphi: G \rightarrow H$ 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 $H(R')$ (5.6). In the commutative diagram below, the rows are exact and the vertical maps are injective.

$$\begin{array}{ccccc} G(R) & \longrightarrow & G(R') & \rightrightarrows & G(R' \otimes_R R') \\ \downarrow \varphi(R) & & \downarrow \varphi(R') & & \downarrow \varphi(R' \otimes_R R') \\ H(R) & \longrightarrow & H(R') & \rightrightarrows & H(R' \otimes_R R') \end{array}$$

A diagram chase shows that $g \in G(R)$, and maps to h in $H(R)$. \square

COROLLARY 5.13. *If a homomorphism of algebraic groups is both an embedding and a quotient map, then it is an isomorphism.*

PROOF. A closed immersion is certainly a monomorphism. \square

c. The homomorphism theorem

The next theorem is of fundamental importance.

THEOREM 5.14 (HOMOMORPHISM THEOREM). *Every homomorphism of affine algebraic groups $\varphi: G \rightarrow H$ factors as*

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

with q a quotient map and i an embedding.

PROOF. As G and H are affine, the factorizations $G \xrightarrow{q} I \xrightarrow{i} H$ of φ with i an embedding correspond to the factorizations

$$\mathcal{O}(H) \xrightarrow{a} \mathcal{O}(I) \xrightarrow{b} \mathcal{O}(G)$$

of the homomorphism $\mathcal{O}(\varphi)$ of Hopf algebras (see 3.9) with a surjective. According to (3.16), there exists such a factorization with b injective. Now (3.47) shows that b is faithfully flat, which proves the theorem. \square

PROPOSITION 5.15. *The following conditions on a homomorphism $\varphi: G \rightarrow Q$ of affine algebraic groups are equivalent:*

- (a) φ is faithfully flat;
- (b) $R \mapsto \varphi(G(R))$ is a fat subfunctor of \tilde{Q} ;
- (c) the homomorphism of k -algebras $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is injective.

PROOF. (a) \Rightarrow (b): Special case of (5.6).

(b) \Rightarrow (c): Consider the universal element $a = \text{id}_{\mathcal{O}(Q)} \in G(\mathcal{O}(Q))$. By assumption, there exists a $g \in G(R')$ with R' faithfully flat over $\mathcal{O}(Q)$ such that a and g map to the same element of $Q(R')$, i.e., such that the diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{g} & R' \\ \uparrow & & \uparrow \text{faithfully flat} \\ \mathcal{O}(Q) & \xrightarrow{a=\text{id}} & \mathcal{O}(Q) \end{array}$$

commutes. Being faithfully flat, the map $\mathcal{O}(Q) \rightarrow R$ is injective (A.85d), and so $\mathcal{O}(Q) \rightarrow \mathcal{O}(G)$ is injective.

(c) \Rightarrow (a): Factor φ as in Theorem 5.14, $\varphi = i \circ q$. The composite of the maps

$$\mathcal{O}(Q) \rightarrow \mathcal{O}(I) \rightarrow \mathcal{O}(G),$$

is injective, and so $\mathcal{O}(Q) \rightarrow \mathcal{O}(I)$ is injective, but it is also surjective because i is a closed immersion. Therefore, i is an isomorphism, and φ is a quotient map. \square

COROLLARY 5.16. *Let G and Q be reduced connected affine algebraic groups, and let $G \rightarrow Q$ be a quotient map. Then*

$$\mathcal{O}(Q) = \mathcal{O}(G) \cap k(Q)$$

where $k(Q)$ is the field of fractions of $\mathcal{O}(Q)$. In particular, $G \rightarrow Q$ is an isomorphism if $k(Q) = k(G)$.

PROOF. Let $\mathcal{O}(Q) = A$ and $\mathcal{O}(G) = B$, so that $A \subset B$ and B is faithfully flat over A . Because B is faithfully flat over A , $cB \cap A = cA$ 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 $a/c \in A$. \square

COROLLARY 5.17. *Let $\varphi: G \rightarrow H$ be a homomorphism of affine algebraic groups with H reduced. The following are equivalent:*

- (a) φ is surjective (i.e., $|\varphi|$ is surjective);
- (b) φ is dominant;
- (c) φ is faithfully flat.

PROOF. A surjective map is certainly dominant. If φ is dominant, then, because H is reduced, the map $\mathcal{O}(H) \rightarrow \mathcal{O}(G)$ is injective, and so φ is faithfully flat by (5.15). Finally, if φ is faithfully flat, then it is surjective (by definition A.86). \square

The statement fails for nonreduced H — see the discussion following (5.8).

PROPOSITION 5.18. *A homomorphism of affine algebraic groups is a monomorphism if and only if it is a closed immersion.*

PROOF. Obviously, a closed immersion is a monomorphism. Conversely, if φ is a monomorphism, then in the factorization $\varphi = i \circ q$ of (5.14), the map q is an isomorphism (5.12). \square

5.19. We define the **image** of a homomorphism $\varphi: G \rightarrow H$ of algebraic groups to be the algebraic group I in (5.14) regarded as a subgroup of H , and we denote it by $\varphi(G)$. Note that $\varphi(G)$ is the smallest algebraic subgroup of H through which φ factors. Moreover $\varphi: G \rightarrow \varphi(G)$ is surjective, and its fibres are cosets of $\text{Ker}(\varphi)$ in G , and so

$$\dim(G) = \dim(\varphi(G)) + \dim(\text{Ker}(\varphi)).$$

The theorem shows that an embedding $\varphi: G \rightarrow H$ is an isomorphism of G onto an algebraic subgroup of H (because the map q in the factorization of φ is an isomorphism).

ASIDE 5.20. An epimorphism of algebraic groups need not be faithfully flat — consider

$$\mathbb{T}_2 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \hookrightarrow \text{SL}_2.$$

However, a homomorphism $\varphi: G \rightarrow H$ of algebraic groups is faithfully flat if it is an epimorphism in the category of algebraic schemes. To see this, factor φ as in (5.14), and use that the quotient H/I exists (see Chapter 7).

d. Existence of quotients by normal subgroups

THEOREM 5.21. *Let N be a normal algebraic subgroup of an affine algebraic group G . There exists a quotient map $q: G \rightarrow Q$ with kernel N . Moreover, q is universal among homomorphisms containing N in their kernel: for every homomorphism $\varphi: G \rightarrow H$ such that $\varphi(N) = e$, there exists a unique homomorphism $Q \rightarrow H$ making*

$$\begin{array}{ccc} G & \xrightarrow{q} & Q \\ & \searrow \varphi & \downarrow \\ & & H \end{array}$$

commute. The algebraic group Q is affine.

We write G/N for the algebraic group Q in the theorem. More precisely, the quotient of G by N is any quotient map $q: G \rightarrow G/N$ with kernel N .

Let $\varphi: G \rightarrow H$ be a homomorphism, and let $\varphi = i \circ q$ be the factorization in (5.14). By the universality, q factors through $G \rightarrow G/N$, and one sees immediately that the resulting homomorphism $G/N \rightarrow I$ is an isomorphism. Therefore, we obtain the homomorphism theorem in its usual form.

COROLLARY 5.22 (HOMOMORPHISM THEOREM). *The image of a homomorphism $\varphi: G \rightarrow G'$ of affine algebraic groups is an algebraic subgroup $\varphi(G)$ of G' , and φ defines an isomorphism of G/N onto $\varphi(G)$ where $N = \text{Ker}(\varphi)$; in particular, every homomorphism of algebraic groups factors as follows:*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \text{quotient map} \downarrow & & \uparrow \text{embedding} \\ G/N & \xrightarrow{\text{isomorphism}} & \varphi(G). \end{array}$$

(quotient map=faithfully flat homomorphism; embedding=homomorphism that is a closed immersion).

The following is a preliminary to proving Theorem 5.21.

PROPOSITION 5.23. *Let G be an affine algebraic group over a field k , and let H be an algebraic subgroup of G . Among the quotient maps $G \rightarrow Q$ trivial on H , there is a universal one.*

PROOF. Given a finite family $(G \xrightarrow{q_i} Q_i)_{i \in I}$ of quotient maps of algebraic groups trivial on H , we let $H_I = \bigcap_{i \in I} \text{Ker}(q_i)$. According to (1.28), there exists a family for which H_I is minimal. For such a family, I claim that the map from G to the image of $(q_i): G \rightarrow \prod_{i \in I} Q_i$ is universal. If it isn't, then there exists a homomorphism $q: G \rightarrow Q$ containing H in its kernel but not H_I . But then $H_{I \cup \{q\}} = H_I \cap \text{Ker}(q)$ is properly contained in H_I . \square

In order to prove Theorem 5.21, it remains to show that, when H is normal, it equals the kernel of the universal map in (5.23). For this, it suffices to show that it arises as the kernel of some homomorphism.

PROOF OF THEOREM 5.21.

LEMMA 5.24. *Let (V, r) be a representation of an affine algebraic group G . If N is a normal algebraic subgroup of G , then V^N is stable under G .*

PROOF. Let $w \in V^N(R)$ and let $g \in G(R)$ for some k -algebra R . For an R -algebra R' and $n \in N(R')$

$$r(n)(r(g)w) = r(ng)w = r(gn')w = r(g)r(n')w = r(g)w,$$

because $n' \stackrel{\text{def}}{=} g^{-1}ng \in N(R')$. Therefore, $r(g)w \in V^N(R)$ (see 4.22), as required. \square

LEMMA 5.25. *Let k be algebraically closed. When H is normal in G , it is possible to choose the pair (V, L) in (4.19) so that H acts on L through the trivial character.*

PROOF. Let (V, L) be as in (4.19), and let χ be the character of G on L . It suffices to show that there exists a representation (W, r) of G and a one-dimensional subspace L_1 in W such that (a) H acts on L_1 through χ and (b) L_1 is a direct summand of W as an H -module, because then H is the stabilizer of $L \otimes L_1^\vee$ in $V \otimes W^\vee$ (see 4.5) and H acts trivially on $L \otimes L_1^\vee$.

Suppose first that $G(k)$ is dense in G . Let W be the sum of the one-dimensional subspaces in V stable under H . If a one-dimensional subspace D is stable under H , 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 (4.4). As W is a sum of simple representations of H , (4.14) shows that L is a direct summand of W as an H -module.

In the general case, we choose n so large that $G^{(p^n)}$ is smooth (see 3.46). Because H is the stabilizer of L in V , it is the stabilizer of $L^{\otimes p^n}$ in $V^{\otimes p^n}$ (by 4.5), and so we can replace (V, L) with $(V^{\otimes p^n}, L^{\otimes p^n})$. Consider the exact sequence (2.16)

$$e \rightarrow N \rightarrow G \xrightarrow{F^n} G^{(p^n)} \rightarrow e.$$

Clearly $L^{\otimes p^n} \subset (V^{\otimes p^n})^N$, which is stable under G (5.24). The action of G on $(V^{\otimes p^n})^N$ factors through $G^{(p^n)}$, and the argument in the last paragraph completes the proof. \square

LEMMA 5.26. *Let G be an affine algebraic group over an algebraically closed field k . Every normal algebraic subgroup N of G arises as the kernel of a representation of G .*

PROOF. According to (5.25), there exists a representation (V, r) of G and a one-dimensional subspace L of V such that N is the stabilizer of L and $L \subset V^N$. Because N is normal, G stabilizes V^N , and the kernel N' of the representation of G on V^N obviously contains N . As N' stabilizes L , it is contained in N , and so equals it. \square

THEOREM 5.27. *Every normal algebraic subgroup N of an affine algebraic group G arises as the kernel of a homomorphism $G \rightarrow H$ with H affine.*

PROOF. Proposition 5.26 shows that $N_{k'}$ is the kernel of a homomorphism $\alpha: G_{k'} \rightarrow H_{k'}$ for some extension k' of k , which we may take to be finite. Let β be the composite of the homomorphisms

$$G \xrightarrow{i_G} (G)_{k'/k} \xrightarrow{(\alpha)_{k'/k}} (H)_{k'/k}$$

(see 2.37). 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 $R \rightarrow R'$. Therefore

$$\text{Ker}(\beta(R)) = G(R) \cap N(R') = N(R),$$

and so $N = \text{Ker}(\beta)$. \square

COROLLARY 5.28. *Every normal algebraic subgroup N of an affine algebraic group G arises as the kernel of a representation of G .*

PROOF. Let N be the kernel of $G \rightarrow H$, and choose a faithful representation of H (which exists by 4.8). \square

e. Properties of quotients

LEMMA 5.29. Let X and Y be algebraic schemes over k , and let D be a fat subfunctor of \tilde{X} . Every map of functors $D \rightarrow \tilde{Y}$ extends uniquely to a map of functors $\tilde{X} \rightarrow \tilde{Y}$ (hence to a map of schemes $X \rightarrow Y$ by the Yoneda lemma).

PROOF. As \tilde{X} and \tilde{Y} are flat sheaves, we can apply (5.4). \square

PROPOSITION 5.30. Let $\varphi: G \rightarrow Q$ be a homomorphism of affine 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 $G \rightarrow Q$, the sequence

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

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 (5.15). \square

PROPOSITION 5.31. Let I be the image of a homomorphism $\varphi: G \rightarrow H$ of affine algebraic groups. Then $G \rightarrow I$ 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. Immediate from the above. \square

PROPOSITION 5.32. Let $\varphi: G \rightarrow H$ be a homomorphism of affine algebraic groups. If φ is a quotient map, then $G(K) \rightarrow H(K)$ is surjective for every algebraically closed field K containing k . Conversely, if $G(K) \rightarrow H(K)$ is surjective for some separably closed field K containing k and H is smooth, then φ is a quotient map.

PROOF. If φ is a quotient map, then so also is φ_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) applied to R modulo a maximal ideal shows that there exists a K -algebra homomorphism $R \rightarrow K$. Under the map $H(R) \rightarrow H(K)$, h' maps to h , and under the map $G(R) \rightarrow G(K)$, g maps to an element lifting h .

For the converse statement, let I be the image of φ . Then $I(K) \subset H(K)$, and so $I = H$ (A.61). \square

COROLLARY 5.33. If the sequence of affine algebraic groups

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

is exact and K is an algebraically closed field containing k , then

$$e \rightarrow N(K) \rightarrow G(K) \rightarrow Q(K) \rightarrow e$$

is exact.

PROOF. The sequence $e \rightarrow N(R) \rightarrow G(R) \rightarrow Q(R)$ is always exact, and (5.32) shows that $G(K) \rightarrow Q(K)$ is surjective. \square

f. The isomorphism theorem

Let H and N be subgroups of an abstract group G . Recall that H is said to normalize N if $hNh^{-1} = N$ for all $h \in H$, and then the isomorphism theorem says that HN is a subgroup of G , and that

$$h \cdot H \cap N \rightarrow h \cdot N : H/H \cap N \rightarrow HN/N$$

is an isomorphism.

5.34. Let H and N be algebraic subgroups of an affine 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

$$N \rtimes_{\theta} H \rightarrow G.$$

We define $NH = HN$ to be the image of this homomorphism. Then

$$N \rtimes_{\theta} H \rightarrow NH$$

is a quotient map (see 5.31), and so 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' . It follows that HN is the unique algebraic subgroup of G containing $R \rightsquigarrow H(R)N(R)$ as a fat subfunctor (5.29). If H and N are smooth, then HN is smooth (see 5.8); if $H \cap N$ is also smooth, then

$$(HN)(k^{\text{sep}}) = H(k^{\text{sep}}) \cdot N(k^{\text{sep}})$$

and HN is the unique smooth algebraic subgroup of G with this property.

PROPOSITION 5.35. *Let H and N be algebraic subgroups of an affine algebraic group G with N normal. The canonical map*

$$N \rtimes_{\theta} H \rightarrow G \tag{34}$$

is an isomorphism if and only if $N \cap H = \{e\}$ and $NH = G$.

PROOF. There is an exact sequence

$$e \rightarrow N \cap H \rightarrow N \rtimes_{\theta} H \rightarrow NH \rightarrow e.$$

Therefore (34) is an embedding if and only if $N \cap H = \{e\}$, and it is surjective if and only if $NH = G$. \square

EXAMPLE 5.36. Consider the algebraic subgroups SL_n and \mathbb{G}_m (nonzero scalar matrices) of GL_n . Then $\mathbb{G}_m \cdot \text{SL}_n = \text{GL}_n$, but $\mathbb{G}_m(k) \cdot \text{SL}_n(k) \neq \text{GL}_n(k)$ in general (an invertible matrix A is the product of a scalar matrix with a matrix of determinant 1 if and only if $\det(A)$ is an n th power in k). The functor $R \rightsquigarrow \mathbb{G}_m(R) \cdot \text{SL}_n(R)$ is fat in GL_n .

THEOREM 5.37. *Let H and N be algebraic subgroups of an affine algebraic group G such that H normalizes N . Then $H \cap N$ is a normal algebraic subgroup of H , and the natural map*

$$H/H \cap N \rightarrow HN/N$$

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

$$H(R)/(H \cap N)(R) \simeq H(R) \cdot N(R)/N(R), \quad (35)$$

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 fat subfunctor of HN/N , and so the isomorphism (35) extends uniquely to an isomorphism $H/H \cap N \rightarrow HN/N$ (see 5.29). \square

In other words, there is a diagram

$$\begin{array}{ccccccc} e & \longrightarrow & N & \longrightarrow & HN & \longrightarrow & HN/N & \longrightarrow & e \\ & & & & & & \uparrow \simeq & & \\ & & & & & & H/H \cap N & & \end{array} \quad (36)$$

in which the row is exact.

g. The correspondence theorem

PROPOSITION 5.38. *Let H and N be algebraic subgroups of an affine 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 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

$$(G \times_{G/N} \bar{H})(R) = G(R) \times_{(G/N)(R)} \bar{H}(R).$$

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, $H' = HN$ (5.34). \square

THEOREM 5.39. *Let N be a normal algebraic subgroup of an affine algebraic group G . The map $H \mapsto H/N$ defines a one-to-one correspondence between the set of algebraic subgroups of G containing N and the set of algebraic subgroups of G/N . An algebraic subgroup H of G containing N is normal if and only if H/N is normal in G/N , in which case the map*

$$G/H \rightarrow (G/N)/(H/N) \quad (37)$$

defined by the quotient map $G \rightarrow G/N$ is an isomorphism.

PROOF. The first statement follows from Proposition 5.38. For the second statement, note that the map

$$G(R)/H(R) \rightarrow (G(R)/N(R))/(H(R)/N(R))$$

defined by the quotient map $G(R) \rightarrow G(R)/N(R)$ is an isomorphism, 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 (5.29). \square



ASIDE 5.40. The Noether isomorphism theorems fail for group varieties. Consider, for example, the algebraic group GL_p and its normal subgroups SL_p and D (group of scalar matrices), where p is the characteristic of ground field. Then $\mathrm{SL}_p \cap D = \{1\}$ in the category of group varieties, but

$$\mathrm{SL}_p / (\mathrm{SL}_p \cap D) \rightarrow \mathrm{SL}_p \cdot D / D$$

is the quotient map $\mathrm{SL}_p \rightarrow \mathrm{PGL}_p$, which is not an isomorphism of group varieties (it is purely inseparable of degree 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 that period, which didn't allow nilpotents, and almost all authors have followed them. My own expository work in this field is predicated on the believe that, in order to learn the modern theory of algebraic groups, one should not have to learn it first in the language of 1950s algebraic geometry, nor should one have to first read EGA.³

h. The category of commutative algebraic groups

THEOREM 5.41. *The commutative algebraic groups over a field 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, 5.14). Therefore the category is abelian. \square

COROLLARY 5.42. *The finitely generated commutative co-commutative Hopf algebras over a field form an abelian category.*

PROOF. This category is contravariantly equivalent to that in the theorem. \square

ASIDE 5.43. Theorem 5.41 is generally credited to Grothendieck. As we have seen, it is a fairly direct consequence of allowing the coordinate rings to have nilpotent elements. See SGA 3, VI_A, 5.4.3, p.327; DG III §3, 7.4, p. 355.

Corollary 5.42 is proved purely in the context of Hopf algebras in Sweedler 1969, Chapter XVI, for finite-dimensional commutative co-commutative Hopf algebras, and in Takeuchi 1972, 4.16, for finitely generated commutative co-commutative Hopf algebras.

i. The group of connected components of an algebraic group

Recall that an étale k -algebra is a finite product of 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, \dots, 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 $A_1 \times \cdots \times A_m$).

Let X be an algebraic scheme over k . Then $\mathcal{O}(X)$ is a k -algebra (not necessarily finitely generated).

PROPOSITION 5.44. *There exists a greatest étale k -subalgebra $\pi(X)$ in $\mathcal{O}(X)$.*

³SGA 3 and Conrad et al. 2010 require both.

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

$$1 = e_1 + \cdots + e_n$$

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

Define

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

Recall that

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

for all k -algebras R (A.13). It follows that the morphism $X \rightarrow \pi_0(X)$ corresponding to the inclusion $\pi(X) \hookrightarrow \mathcal{O}(X)$ is universal among morphisms from X to étale k -schemes.

PROPOSITION 5.45. *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. For affine schemes, these statements are proved in Waterhouse 1979, but the proofs their extend without difficulty to all algebraic schemes (AG, Chap. 10). \square

For example, if k is algebraically closed in $\mathcal{O}(X)$, then $\pi(X) = k$ and $\pi(X_{k^{\text{sep}}}) = k^{\text{sep}}$. It follows that there are no nontrivial idempotents in $\mathcal{O}(X_{k^{\text{sep}}})$, and so $X_{k^{\text{sep}}}$ is connected. Using this, we obtain (b) of the following proposition.

PROPOSITION 5.46. *Let X be an algebraic scheme over k .*

(a) *The fibres of the morphism $\varphi: X \rightarrow \pi_0(X)$ are the connected components X .*

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

PROOF. Statement (a) is obvious, and (b) was noted above. \square

REMARK 5.47. Let X be an algebraic scheme over k .

(a) The connected components of $X_{k^{\text{sep}}}$ form a finite set on which $\text{Gal}(k^{\text{sep}}/k)$ acts continuously, and $\pi_0(X)$ is the étale scheme over k corresponding to this set under the equivalence $Z \rightsquigarrow Z(k^{\text{sep}})$ (see 2.13).

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

Let G be an algebraic group (not necessarily affine) over k . In this case, the k -algebra $\mathcal{O}(G)$ is finitely generated (see 10.33 below), but we don't need that here.

Because G° is a normal subgroup of G , the set $\pi_0(X_{k^{\text{sep}}})$ of connected components of $X_{k^{\text{sep}}}$ has a (unique) group structure for which

$$G(k^{\text{sep}}) \rightarrow \pi_0(X_{k^{\text{sep}}}) \quad (38)$$

is a homomorphism. This group structure is respected by the action of $\text{Gal}(k^{\text{sep}}/k)$, and so it arises from an étale group $\pi_0(X)$ over k . In this way, we get a homomorphism

$$G \rightarrow \pi_0(G)$$

of algebraic groups over k which, on k^{sep} -points, becomes (38).⁴

PROPOSITION 5.48. *Let G be an algebraic group (not necessarily affine) over a field k .*

- (a) *The homomorphism $G \rightarrow \pi_0(G)$ 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*

$$e \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow e.$$

- (c) *The formation of the exact sequence in (b) commutes with extension of the base field. For every field extension $k' \supset k$,*

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

- (d) *The fibres of $|G| \rightarrow |\pi_0(G)|$ are the connected components of $|G|$. The order of the finite algebraic group $\pi_0(G)$ is the number of connected components of $G_{k^{\text{al}}}$.*
- (e) *For algebraic groups G and G' ,*

$$\begin{aligned} (G \times G')^\circ &\simeq G^\circ \times G'^\circ \\ \pi_0(G \times G') &\simeq \pi_0(G) \times \pi_0(G'). \end{aligned}$$

PROOF. Immediate from the above. □

DEFINITION 5.49. Let G be an algebraic group over a field k . The quotient $G \rightarrow \pi_0(G)$ of G is the **component group** or **group of connected components** of G .

REMARK 5.50. (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 $G^\circ \rightarrow G$ (because its composite with $G \rightarrow \pi_0(G)$ is trivial).

(c) The set $|\pi_0(G)|$ can be identified with the set of $\text{Gal}(k^{\text{sep}}/k)$ -orbits in the group $\pi_0(G)(k^{\text{sep}})$, and need not itself be a group. For example, $\pi_0(\mu_n) = \mu_{n_0}$ where n_0 is the largest factor of n not divisible by the characteristic exponent of k , and $|\mu_{n_0}|$ need not be a group.

⁴Alternatively, we can argue as follows. Let $A = \mathcal{O}(G)$. The multiplication map $m: G \times G \rightarrow G$ defines a comultiplication map $\Delta: A \rightarrow A \otimes A$, which makes A into a Hopf algebra. As Δ is a k -algebra homomorphism, it sends $\pi(A)$ into

$$\pi(A \otimes A) \simeq \pi(A) \otimes \pi(A).$$

Similarly, $S: A \rightarrow A$ sends $\pi(A)$ into $\pi(A)$, and we can define ϵ on $\pi(A)$ to be the restriction of ϵ on A . Therefore $\pi(A)$ is a Hopf subalgebra of A . Hence $\pi_0(G) \stackrel{\text{def}}{=} \text{Spm}(\pi(A))$ is an étale algebraic group over k , and $G \rightarrow \pi_0(G)$ is a homomorphism of algebraic groups.

PROPOSITION 5.51. *Let G be an affine algebraic group over k . Then G° is the unique connected normal algebraic subgroup of G admitting an étale quotient G/G° .*

PROOF. Let N be a normal algebraic subgroup of G such that G/N exists and is étale. According to (5.48a), the homomorphism $G \rightarrow G/N$ factors through $G \rightarrow \pi_0(G)$, and so we get a commutative diagram

$$\begin{array}{ccccccc} e & \longrightarrow & G^\circ & \longrightarrow & G & \longrightarrow & \pi_0 G & \longrightarrow & e \\ & & \downarrow & & \parallel & & \downarrow & & \\ e & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & e \end{array}$$

with exact rows. On applying the snake lemma (Exercise 6-4) to the diagram, we obtain an exact sequence of algebraic groups:

$$1 \rightarrow G^\circ \rightarrow N \rightarrow \pi_0 G.$$

If N is connected, then the homomorphism $N \rightarrow \pi_0 G$ is trivial, and so $G^\circ \simeq N$. \square

Let G be an affine algebraic group. Proposition 5.51 says that there is a unique exact sequence

$$e \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow e$$

with G° connected and $\pi_0(G)$ étale. This is sometimes called the *connected-étale exact sequence*.

PROPOSITION 5.52. *Let*

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

be an exact sequence of algebraic groups. If N and Q are connected, then so is G ; conversely, if G is connected, then so is Q (but not necessarily N).

PROOF. If N is connected, then it maps to e in $\pi_0(G)$, and so $G \rightarrow \pi_0(G)$ factors through Q , and hence through $\pi_0(Q)$, which is trivial if Q is connected.

The surjective homomorphism $G \rightarrow Q \rightarrow \pi_0(Q)$ factors through $\pi_0(G)$, and so $\pi_0(Q)$ is trivial if $\pi_0(G)$ is. \square

For the parenthetical statement, note that \mathbb{G}_m is connected, but $\mu_n = \text{Ker}(\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m)$ is not connected unless n is a power of the characteristic exponent of k .

EXAMPLES

5.53. 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

$$e \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow e.$$

When k is perfect, the homomorphism $G \rightarrow \pi_0(G)$ has a section, and so G is a semidirect product

$$G = G^\circ \rtimes \pi_0(G).$$

To see this, note that the homomorphism $G_{\text{red}} \rightarrow \pi_0(G)$ is an isomorphism because both groups are étale and the homomorphism becomes an isomorphism on k^{al} -points:

$$G_{\text{red}}(k^{\text{al}}) = G(k^{\text{al}}) \xrightarrow{\cong} \pi_0(G)(k^{\text{al}}).$$

Now we can apply (2.21).

5.54. The groups \mathbb{G}_a , GL_n , \mathbb{T}_n , \mathbb{U}_n , \mathbb{D}_n (see 2.1, 2.8, 2.9) are connected because in each case $\mathcal{O}(G)$ is an integral domain. For example,

$$k[\mathbb{T}_n] = k[\mathrm{GL}_n]/(T_{ij} \mid i > j),$$

which is isomorphic to the polynomial ring in the symbols T_{ij} , $1 \leq i \leq j \leq n$, with the product $T_{11}T_{22} \cdots T_{nn}$ inverted.

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

$$I(\sigma) \cdot \mathrm{diag}(a_1, \dots, a_n) \cdot I(\sigma)^{-1} = \mathrm{diag}(a_{\sigma(1)}, \dots, a_{\sigma(n)}). \quad (39)$$

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

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

where $\theta: S_n \rightarrow \mathrm{Aut}(\mathbb{D}_n)$ sends σ to the automorphism in (39). In this case, $\pi_0 G = (S_n)_k$ and $G^\circ = \mathbb{D}_n$.

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

$$A, r \mapsto A \cdot \mathrm{diag}(r, 1, \dots, 1): \mathrm{SL}_n(R) \times \mathbb{G}_m(R) \rightarrow \mathrm{GL}_n(R)$$

defines an isomorphism of k -algebras

$$\mathcal{O}(\mathrm{GL}_n) \simeq \mathcal{O}(\mathrm{SL}_n) \otimes \mathcal{O}(\mathbb{G}_m),$$

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

5.57. Assume $\mathrm{char}(k) \neq 2$. For every nondegenerate quadratic space (V, q) , the algebraic group $\mathrm{SO}(q)$ is connected. It suffices to prove this after replacing k with k^{al} , and so we may suppose that q is the standard quadratic form $X_1^2 + \cdots + X_n^2$, in which case we write $\mathrm{SO}(q) = \mathrm{SO}_n$. The latter is shown to be connected in Exercise 5-5 below.

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

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

ASIDE 5.59. (a) An algebraic variety over \mathbb{C} is connected for the Zariski topology if and only if it is connected for the complex topology. Therefore an algebraic group G over \mathbb{C} is connected if and only if $G(\mathbb{C})$ is connected for the complex topology. We could for example deduce that GL_n over \mathbb{C} is a connected algebraic group from knowing that $\mathrm{GL}_n(\mathbb{C})$ is connected for the complex topology. However, it is easier to deduce that $\mathrm{GL}_n(\mathbb{C})$ is connected from knowing that GL_n is connected.

(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 $\mathrm{GL}_2(\mathbb{R})$ is not connected, whereas μ_3 is not connected as an algebraic group, but $\mu_3(\mathbb{R}) = \{1\}$ is connected.

j. Torsors and extensions

This section will be expanded. In particular, we shall define $H^1(R_0, G)$ and $\text{Ext}^1(G, H)$ etc.

5.60. Let R_0 be a k -algebra, and let G be an algebraic group over R_0 . A right G -torsor over R_0 is a scheme X faithfully flat over R_0 together with an action $X \times G \rightarrow X$ of G on X such that the map

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

is an isomorphism of R_0 -schemes. If G is affine (resp. finite, smooth) over k , then the morphism $X \rightarrow \text{Spm}(R_0)$ is affine (resp. finite, smooth) (because it becomes so after the faithfully flat base extension $X \rightarrow \text{Spm}(R_0)$, and we can apply (A.90)).

5.61. Let

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e,$$

be an exact sequence of algebraic groups over k with Q affine. Then G is an N -torsor over Q (Exercise 2-1). Therefore, if N and Q are affine (resp. finite, smooth) then G is affine (resp. finite, smooth).

Exercises

EXERCISE 5-1. Let A and B be algebraic subgroups of an affine algebraic group G , and let AB be the sheaf associated with the subfunctor $R \mapsto A(R) \cdot B(R)$ of G .

- Show that AB is representable by $\mathcal{O}(G)/\mathfrak{a}$ where \mathfrak{a} is the kernel of homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(A) \otimes \mathcal{O}(B)$ defined by the map $a, b \mapsto ab: A \times B \rightarrow G$ (of set-valued functors).
- Show that, for any k -algebra R , an element $G(R)$ lies in $(AB)(R)$ if and only if its image in $G(R')$ lies in $A(R') \cdot B(R')$ for some faithfully flat R -algebra R' , i.e.,

$$(AB)(R) = \bigcap_{R'} G(R) \cap (A(R') \cdot B(R')).$$

EXERCISE 5-2. Show that if $e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$ is exact, so also is $\pi_0(N) \rightarrow \pi_0(G) \rightarrow \pi_0(Q) \rightarrow e$. Give an example to show that $\pi_0(N) \rightarrow \pi_0(G)$ need not be a closed immersion.

EXERCISE 5-3. What is the map $\mathcal{O}(\text{SL}_n) \rightarrow \mathcal{O}(\text{GL}_n)$ defined in example 5.56?

EXERCISE 5-4. Prove directly that $\pi(\mathcal{O}(\text{O}_n)) = k \times k$.

EXERCISE 5-5. (Springer 1998, 2.2.2). Let k be a field 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 $A^t = -A$.

- Show that the functor $R \mapsto V(R)$ is represented by a finitely generated k -algebra A , and that A is an integral domain.
- Show that $A \mapsto (I_n + A)^{-1}(I_n - A)$ defines a bijection from a nonempty open subset of $\text{SO}_n(k^{\text{al}})$ onto an open subset of $V(k^{\text{al}})$.
- Deduce that SO_n is connected.
- Deduce that SO_n is rational.

The isomorphism theorems using sheaves.

In this chapter, we use sheaves to express some of the material in the previous chapter more efficiently, and we explain how to extend the results to general algebraic groups (not necessarily affine).

a. *Some sheaf theory*

All functors are from Alg_k^0 to Set .

PROPOSITION 6.1. *Let F be a functor. Among the morphisms from F to a flat sheaf there exists a universal one $\alpha: F \rightarrow aF$.*

The universal property means that, for every homomorphism $\beta: F \rightarrow S$ from F to a sheaf S , there is a unique morphism $\gamma: aF \rightarrow S$ rendering

$$\begin{array}{ccc}
 F & \xrightarrow{\alpha} & aF \\
 & \searrow \beta & \downarrow \gamma \\
 & & S
 \end{array}$$

commutative. 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 functor is *separated* if $F(R) \rightarrow \prod F(R_i)$ is injective whenever $(R_i)_{i \in I}$ is a finite family of small R -algebras such that $R \rightarrow \prod_{i \in I} R_i$ is faithfully flat.

LEMMA 6.2. *Let F be a functor. Among the morphisms from F to a separated functor, there exists a universal one $\alpha: F \rightarrow F'$.*

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 faithfully flat family $(R_i)_{i \in I}$ of R -algebras. Define

$$F'(R) = F(R)/\sim .$$

One checks easily that this is a separated functor, and that the morphism $F \rightarrow F'$ is universal. □

LEMMA 6.3. *Let F be a separated functor. Among the morphisms from F to a flat sheaf there exists a universal one $\alpha: F \rightarrow aF$.*

PROOF. Let

$$(aF)(R) = \lim_{\rightarrow} \text{Eq}(\prod_{i \in I} F(R_i) \rightrightarrows \prod_{(i,j) \in I \times I} F(R_i \otimes_R R_j))$$

where the limit is over finite families $(R_i)_{i \in I}$ of small R -algebras such that the homomorphism $R \rightarrow \prod_{i \in I} R_i$ is faithfully flat. One checks easily that this is a sheaf, and that the morphism $F \rightarrow aF$ is universal. \square

If F is local (i.e., satisfies (a) of 5.1), then

$$(aF)(R) = \lim_{\rightarrow} \text{Eq}(F(R') \rightrightarrows F(R' \otimes_R R'))$$

where the limit is over the small faithfully flat R -algebras R' .

Now, for a functor F , the composite of the morphisms

$$F \rightarrow F' \rightarrow aF'$$

is the required universal morphism from F to a sheaf.

Proposition says that, for a functor F and a sheaf S , Let \mathcal{P} denote the category of functors and \mathcal{S} the category of sheaves. Then \mathcal{S} is a full subcategory of \mathcal{P} , and (6.1) says that the functor $a: \mathcal{P} \rightarrow \mathcal{S}$ is left adjoint to the inclusion functor $i: \mathcal{S} \rightarrow \mathcal{P}$:

$$\text{Hom}_{\mathcal{P}}(F, iS) \simeq \text{Hom}_{\mathcal{S}}(aF, S). \quad (40)$$

Therefore a is left adjoint to i , and so it preserves direct limits.

6.4. Let S be a sheaf. For any fat subfunctor D of S , $(S, D \hookrightarrow S)$ is the sheaf associated with D .

6.5. Let F be a flat sheaf. We say that F is **representable** if there exists an algebraic k -scheme X such that $\tilde{X} \approx F$. If there exists a nonzero k -algebra R , an algebraic R -scheme X , and bijections $X(R') \rightarrow F(R')$, natural in R' , for every R -algebra R' , then F is representable (descent).

6.6. Let F be a separated functor $\text{Alg}_k^0 \rightarrow \text{Set}$. We say that an algebraic scheme X over k together with a natural transformation

$$\alpha(R): F(R) \rightarrow X(R)$$

represents the sheaf associated with F if

- (a) for all small k -algebras R , $\alpha(R): F(R) \rightarrow X(R)$ is injective, and
- (b) for all $x \in V(R)$, there exists a faithfully flat R -algebra R' and a $y \in F(R')$ such that $\alpha(R')(y) = x$.

Of course, this just means that (\tilde{X}, α) is the sheaf associated with F . If (X, α) and (X', α') both represent the sheaf associated with F , then there exists a unique isomorphism $\varphi: X \rightarrow X'$ such that $h_\varphi \circ \alpha = \alpha'$.

b. The isomorphism theorems for abstract groups

First we recall the statements for abstract groups.

6.7. (Existence of quotients). The kernel of a homomorphism $G \rightarrow G'$ of groups is a normal subgroup, and every normal subgroup N of G arises as the kernel of a quotient map $G \rightarrow G/N$.

6.8. (Homomorphism theorem). The image of a homomorphism $\varphi: G \rightarrow G'$ of groups is a subgroup $\varphi(G)$ of G' , and φ defines an isomorphism of $G/\text{Ker}(\varphi)$ onto $\varphi(G)$; in particular, every homomorphism of groups is the composite of a quotient map with an embedding:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \text{quotient map} \downarrow & & \uparrow \text{embedding} \\ G/N & \xrightarrow{\text{isomorphism}} & I \end{array}$$

6.9. (Isomorphism theorem). Let H and N be subgroups of G with N normal in G . Then HN is a subgroup of G , $H \cap N$ is a normal subgroup of H , and the map

$$xH \cap N \mapsto xN: H/H \cap N \rightarrow (HN)/N$$

is an isomorphism.

6.10. (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 if and only if H/N is normal in G/N , in which case the natural map

$$G/H \rightarrow (G/N)/(H/N)$$

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, (6.10) is often called the lattice theorem.

c. The isomorphism theorems for group functors

By a **group functor** we mean a functor $G: \text{Alg}_k^0 \rightarrow \text{Grp}$. A **homomorphism** $\varphi: G \rightarrow G'$ of group functors is a natural transformation. A subgroup functor of a group functor G is a subfunctor G' such that $G'(R)$ is a subgroup of $G(R)$ for all k -algebras R ; it is normal if $G'(R)$ 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 $R \mapsto G(R)/N(R)$. For subgroup functors H and N of G , we define HN to be the subfunctor $R \mapsto H(R)N(R)$ of G .

Let $\varphi: G \rightarrow G'$ be a homomorphism of group functors. The kernel of φ is the group functor $R \mapsto \text{Ker}(\varphi(R))$, and the image φG of φ is the subfunctor $R \mapsto \varphi(G(R))$ of G . We say that φ is a quotient map if $\varphi(R)$ is surjective for all R .

With these definitions, the isomorphism theorems 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.

d. The isomorphism theorems for sheaves of groups

The sheaves of groups form a full subcategory \mathbf{S} of the category \mathbf{P} of group functors. The sheaf associated with a group functor is again a group functor, and so the inclusion functor $i: \mathbf{S} \rightarrow \mathbf{P}$ has a left adjoint a ,

$$\mathrm{Hom}_{\mathbf{P}}(F, iG) \simeq \mathrm{Hom}_{\mathbf{S}}(aF, G).$$

As i and a are adjoint functors, the first preserves finite direct limits and the second finite inverse limits. Using this, one can show that the isomorphism theorems hold for sheaves of groups, as we now explain.

6.11. (Existence of quotients). Let $\varphi: G \rightarrow G'$ be a homomorphism of sheaves of groups. The kernel of φ is automatically a sheaf (hence a sheaf of normal subgroups of G). We say that φ is a quotient map if the image φG of φ is fat in G' , i.e., if G' is the sheaf associated with the functor $R \mapsto \varphi(G(R))$. Let N be a sheaf of normal subgroups of G . We define G/\tilde{N} to be $a(G/N)$. Then $G \rightarrow G/\tilde{N}$ 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 $G \rightarrow G/N$ (obviously), and then $G/N \rightarrow G/\tilde{N}$ factors uniquely through $G/N \rightarrow G/\tilde{N}$ because H is a sheaf.

6.12. (Homomorphism theorem). Let $\varphi: G \rightarrow G'$ be a homomorphism 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 G' through which φ factors, and $\varphi(G)$ is a fat subfunctor of $\mathrm{Im}(\varphi)$. The map φ defines an isomorphism of functors of groups

$$G/\mathrm{Ker}(\varphi) \rightarrow \varphi(G)$$

(see Section d). On passing to the associated sheaves, we obtain an isomorphism of sheaves

$$G/\tilde{\mathrm{Ker}}(\varphi) \rightarrow \mathrm{Im}(\varphi),$$

and hence a factorization

$$G \twoheadrightarrow G/\tilde{\mathrm{Ker}}(\varphi) \xrightarrow{\cong} \mathrm{Im}(\varphi) \hookrightarrow G'$$

of φ .

Let G be a sheaf of groups.

6.13. (Isomorphism theorem). Let H and N be sheaves of subgroups of G with N normal in G . We define HN to be the sheaf associated with the group functor $R \mapsto H(R)N(R)$. Then HN is a sheaf of subgroups of G , $H \cap N$ is a normal subgroup of H , and the map

$$xH \cap N \mapsto xN: H/\tilde{H \cap N} \rightarrow (HN)/\tilde{N}$$

is an isomorphism (because it is obtained from an isomorphism of group functors by passing to the associated sheaves).

6.14. (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

$$G/\tilde{H} \rightarrow (G/\tilde{N})/(H/\tilde{N})$$

is an isomorphism. Again, all these statements can be derived easily from the corresponding statements for group functors.

e. *The isomorphism theorems for affine algebraic groups*

Let G be an affine algebraic group. Then $\tilde{G}: R \rightsquigarrow G(R)$ is a sheaf of groups, and the functor $G \rightsquigarrow \tilde{G}$ is fully faithful. Therefore, we may identify category of affine algebraic groups over k with the category of sheaves of groups whose underlying sheaf of sets is representable by an object of Alg_k^0 . In order to prove (6.11, 6.12, 6.13, 6.14) for affine algebraic groups, it suffices to show that each of the constructions in these statements takes affine algebraic groups to affine algebraic groups. This is straightforward, and accomplished in a more general setting in the next section.

f. *The isomorphism theorems for algebraic groups*

We write \tilde{G} , or just G , for the flat sheaf defined by an algebraic group G . Recall that 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.

We shall need to use two consequences of the general existence theorem on quotients proved in the next chapter.

6.15. *Every monomorphism of algebraic groups is a closed immersion (7.37).*

6.16. *Let N be a normal algebraic subgroup of an algebraic group G . The homomorphism of sheaves $G \rightarrow \tilde{G}/N$ is represented by a faithfully flat homomorphism $G \rightarrow G/N$ of algebraic groups (7.38).*

THEOREM 6.17 (EXISTENCE OF QUOTIENTS). *The kernel of a homomorphism $G \rightarrow G'$ of algebraic groups is a normal algebraic subgroup, and every normal algebraic subgroup N of G arises as the kernel of a quotient map $G \rightarrow G/N$.*

PROOF. Restatement of previous results (Section 1.e, 6.16). □

We define the image of a homomorphism $\varphi: G \rightarrow G'$ to be the smallest algebraic subgroup $\varphi(G)$ of G' through which φ factors (cf. 1.36).

THEOREM 6.18 (HOMOMORPHISM THEOREM). *The image of a homomorphism $\varphi: G \rightarrow G'$ of algebraic groups is an algebraic subgroup $\varphi(G)$ of G' , and φ defines an isomorphism of $G/\text{Ker}(\varphi)$ onto $\varphi(G)$; in particular, every homomorphism of groups is the composite of a quotient map with an embedding:*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \text{quotient map} \downarrow & & \uparrow \text{embedding} \\ G/N & \xrightarrow{\text{isomorphism}} & I \end{array} \quad (N = \text{Ker}(\varphi)).$$

PROOF. First consider the diagram of functors:

$$\begin{array}{ccc} \tilde{G} & \xrightarrow{\varphi} & \tilde{G}' \\ \downarrow & & \uparrow \\ \tilde{G}/\tilde{N} & \xrightarrow{\text{isomorphism}} & I \end{array}$$

as in Section c. Now pass to the associated sheaves:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow & & \uparrow \\ \tilde{G}/N & \xrightarrow{\text{isomorphism}} & aI \end{array}$$

The arrow $G \rightarrow \tilde{G}/N$ is the quotient map $G \rightarrow G/N$ in (6.16) regarded as a map of sheaves. The arrow $\tilde{G}/N \rightarrow aI$ is an isomorphism of sheaves. Therefore aI is representable by an algebraic group J . The homomorphism of sheaves $aI \rightarrow G'$ is injective, which means that the homomorphism $J \rightarrow G'$ of algebraic groups is a monomorphism. According to (6.15), it is a closed immersion. \square

THEOREM 6.19 (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*

$$xH \cap N \mapsto xN: H/H \cap N \rightarrow (HN)/N$$

is an isomorphism.

PROOF. As before, we define HN to be the image of the homomorphism $H \times_{\theta} N \rightarrow G$ of algebraic groups. It is the sheaf associated with the subfunctor $R \mapsto H(R)N(R)$ of \tilde{G} . Clearly, $H \cap N$ is a normal algebraic subgroup of H . The map of functors

$$xH \cap N \mapsto xN: \tilde{H}/\widetilde{H \cap N} \rightarrow \tilde{H}\tilde{N}/\tilde{N}$$

is an isomorphism (Section c). On passing to the associated sheaves, we obtain the required isomorphism. \square

THEOREM 6.20 (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 if and only if H/N is normal in G/N , in which case the natural map*

$$G/H \rightarrow (G/N)/(H/N)$$

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 .

PROOF. The same as that of (5.39). \square

PROPOSITION 6.21. *The following conditions on a homomorphism $\varphi: G \rightarrow Q$ of affine algebraic groups are equivalent:*

- (a) φ is faithfully flat;
- (b) $R \mapsto \varphi(G(R))$ is a fat subfunctor of \tilde{Q} ;
- (c) the map $\mathcal{O}_Q \rightarrow \varphi_* \mathcal{O}_G$ of sheaves on Q is injective.

PROOF. (a) \Rightarrow (b): Special case of (5.6).

(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 $\text{Spm}(R) = U \hookrightarrow G$ of $G(R)$, we see that there exists a faithfully flat map $R \rightarrow R'$ and a commutative diagram

$$\begin{array}{ccc} G & \longleftarrow & \text{Spm}(R') \\ \downarrow \varphi & & \downarrow \\ Q & \longleftarrow & \text{Spm}(R). \end{array}$$

From this, we get a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_G(\varphi^{-1}U) & \longrightarrow & R' \\ \uparrow & & \uparrow \\ \mathcal{O}_Q(U) & \xlongequal{\quad} & R. \end{array}$$

As $R \rightarrow R'$ is injective (A.85d), so also is $\mathcal{O}_Q(U) \rightarrow \mathcal{O}_G(\varphi^{-1}U)$.

(c) \Rightarrow (a): Factor φ as in Theorem 5.14, $\varphi = i \circ q$. The composite of the maps

$$\mathcal{O}_Q \rightarrow i_*\mathcal{O}_I \rightarrow \varphi_*G,$$

is injective, and so $\mathcal{O}_Q \rightarrow i_*\mathcal{O}_I$ is injective, but it is also surjective because i is a closed immersion. Therefore, i is an isomorphism, and φ is faithfully flat. \square

PROPOSITION 6.22. Let

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

be an exact sequence of algebraic groups. If G is affine, then so also are N and Q ; if N and Q are affine, so also is G .

PROOF. Every algebraic subgroup H of an algebraic group G is closed (1.27), and hence affine if G is affine.

By definition, G/N represents the functor G/\tilde{N} , and we know that G/\tilde{N} is representable by an affine algebraic group when G is affine (5.21).

If N and Q are affine, then so also is G because it is a torsor under N over Q (see 5.61). \square

All the results proved in Chapter 5 for affine algebraic groups now hold mutatis mutandis for general algebraic groups. For reference, we state some of these.

6.23. Let $\varphi: G \rightarrow H$ be a homomorphism of algebraic groups with H reduced. The following are equivalent:

- (a) φ is surjective (i.e., $|\varphi|$ is surjective);
- (b) φ is dominant;
- (c) φ is faithfully flat.

6.24. Every normal algebraic subgroup N of an algebraic group G such that G/N is affine arises as the kernel of a linear representation of G .

6.25. Let $\varphi: G \rightarrow H$ be a homomorphism of algebraic groups. If φ is a quotient map, then $G(K) \rightarrow H(K)$ is surjective for every algebraically closed field K containing k . Conversely, if $G(K) \rightarrow H(K)$ is surjective for some separably closed field K containing k and H is smooth, then φ is a quotient map.

6.26. If the sequence of algebraic groups

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

is exact and K is an algebraically closed field containing k , then

$$e \rightarrow N(K) \rightarrow G(K) \rightarrow Q(K) \rightarrow e$$

is exact.

6.27. The category of commutative algebraic group schemes over a field is abelian, and the subcategory of affine commutative algebraic group schemes is thick (6.22).

NOTES. That the Noether isomorphism theorems hold for algebraic groups over a field is implicit in DG and SGA 3, and explicit in SHS Exposé 7, §3, p.242.

g. Some category theory

Let \mathcal{A} be a category. A morphism $\alpha: A \rightarrow B$ in \mathcal{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 $\alpha: A \rightarrow B$ is a monomorphism (resp. epimorphism) then we call A a subobject of B (resp. we call B a quotient object of A).

Let $\alpha: A \rightarrow B$ a morphism. The subobjects of B through which α factors form 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 \mathcal{A} is an object e such that, for all objects A of \mathcal{A} , each set $\text{Hom}(A, e)$ and $\text{Hom}(e, A)$ have exactly one element. A morphism is trivial if it factors through e .

Assume that \mathcal{A} has a null object. Let $\alpha: A \rightarrow B$ be a morphism. We call a morphism $u: K \rightarrow A$ 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 $u: A' \rightarrow A$ is normal if it is the kernel of some morphism $A \rightarrow B$. 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 $\alpha: A \rightarrow B$ can be written as a composite $A \xrightarrow{q} I \xrightarrow{v} B$ with q an epimorphism and v a monomorphism.

Now let \mathcal{A} denote the category of algebraic groups over a field k . A morphism in \mathcal{A} is a monomorphism if and only if it is a closed immersion. 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. The image of a homomorphism $\alpha: G \rightarrow H$ as we defined it is an image in the sense of categories.

The trivial group e is a null object in \mathcal{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 $\alpha: A \rightarrow B$ can be written as a composite of an epimorphism and a monomorphism.

Clearly, \mathcal{A} is not an exact category, but some of the results for exact categories hold for \mathcal{A} . It is not possible to make \mathcal{A} into an exact category by restricting the homomorphisms to

be normal, because a composite of normal homomorphisms need not be normal (a normal subgroup of a normal group need not be normal). However, when we replace \mathcal{A} with the category of commutative algebraic groups, then we do get an exact category (even an abelian category).

Exercises

EXERCISE 6-1. 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 .

EXERCISE 6-2. (Dedekind's modular laws). Let A, B, C be algebraic subgroups of an algebraic group G such that A is a subgroup of B . Show:

- (a) $B \cap AC = A(B \cap C)$;
- (b) if $G = AC$, then $B = A(B \cap C)$.

EXERCISE 6-3. 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) $N \cap Q = 1$, and (c) the restriction to Q of the canonical map $G \rightarrow G/N$ is an isomorphism.

EXERCISE 6-4. A homomorphism $u: G \rightarrow G'$ of algebraic groups is said to be **normal** if its image is a normal subgroup of G' . For a normal homomorphism $u: G \rightarrow G'$, the quotient map $G' \rightarrow G'/u(G)$ 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 following commutative diagram, the blue sequences are exact and the homomorphisms a, b, c are normal, then the red sequence exists and is exact:

$$\begin{array}{ccccccc}
 e & \longrightarrow & \text{Ker } f & \longrightarrow & \text{Ker } a & \longrightarrow & \text{Ker } b & \longrightarrow & \text{Ker } c & \longrightarrow & e \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & e & & \\
 & & \downarrow a & & \downarrow b & & \downarrow c & & & & \\
 e & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & e & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \text{Coker } a & \longrightarrow & \text{Coker } b & \longrightarrow & \text{Coker } c & \longrightarrow & \text{Coker } g' & \longrightarrow & e.
 \end{array}$$

EXERCISE 6-5. 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

$$0 \rightarrow \text{Ker } f \rightarrow \text{Ker } g \circ f \xrightarrow{f} \text{Ker } g \rightarrow \text{Coker } f \xrightarrow{g} \text{Coker } g \circ f \rightarrow \text{Coker } g \rightarrow 0.$$

Hint: use the extended snake lemma.

EXERCISE 6-6. Let G and H be algebraic groups over k , and let \tilde{G} and \tilde{H} denote the sheaves they define. Show that the canonical map

$$\mathrm{Ext}^1(G, H) \rightarrow \mathrm{Ext}^1(\tilde{G}, \tilde{H})$$

is a bijection. Here $\mathrm{Ext}^1(G, H)$ (resp. $\mathrm{Ext}^1(\tilde{G}, \tilde{H})$) denotes the set of equivalence classes of extensions of G by H in the category of algebraic groups over k (resp. of \tilde{G} by \tilde{H} in the category of sheaves of groups over k). Same statement for affine algebraic groups.

Existence of quotients of algebraic groups

Let H be an algebraic subgroup of an algebraic group G over a field k . In this section, we prove that G/H exists as a separated algebraic scheme over k .¹

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 (7.18, 7.24). This implies the existence of a quotient whenever there exists a “quasi-section” (i.e., a one-to-finite section) (see 7.29). In general, there will exist a quasi-section for an equivalence relation over a dense open subset (7.33). Using this, we deduce the existence of G/H (7.35).

In this section, we work over a noetherian base ring R_0 , and we ignore set-theoretic questions. All R_0 -algebras are finitely generated. An algebraic scheme over R_0 is a scheme of finite type over $\text{Spec}(R_0)$. 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, $R \mapsto X(R)$, which we denote by \tilde{X} or h_X . The functor $X \mapsto \tilde{X}$ is an equivalence of categories.

a. Equivalence relations

DEFINITION 7.1. A pair of morphisms $u_0, u_1: F_1 \rightrightarrows F_0$ 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 the 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' of F_0 is **saturated** with respect to an equivalence relation if $F'(R)$ is a union of equivalence classes for all R (i.e., $u_1(u_0^{-1}(F')) \subset F'$).

¹This result is not proved in DG; it was planned for “Tome II” — see DG, Tome I, p.342.

EXAMPLE 7.2. 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 $G \times F \rightarrow F$ be a free action. Then

$$G \times F \begin{array}{c} \xrightarrow{(g,x) \mapsto gx} \\ \xrightarrow{(g,x) \mapsto x} \end{array} F$$

is an equivalence relation. The graph of the equivalence relation on $F(R)$ is

$$\{(gx, x) \mid g \in G(R), x \in F(R)\}.$$

The action being free means that the map

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

is injective: $(gx, x) = (g'x', x') \iff x = x'$ and $g^{-1}g'x = x \iff x = x'$ and $g = g'$.

EXAMPLE 7.3. For any map of functors $u: F_0 \rightarrow F$, the pair

$$F_1 = F_0 \times_{u, F, u} F_0 \begin{array}{c} \xrightarrow{p_1} \\ \xrightarrow{p_2} \end{array} F_0$$

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 7.4. Let $u_0, u_1: F_1 \rightrightarrows F_0$ be an equivalence relation on F_0 , and let $f: F'_0 \rightarrow F_0$ be a morphism. Form the fibred product

$$\begin{array}{ccc} F'_1 & \xrightarrow{(u'_0, u'_1)} & F'_0 \times F'_0 \\ \downarrow & & \downarrow f \times f \\ F_1 \times F_1 & \xrightarrow{u_0 \times u_1} & F_0 \times F_0. \end{array}$$

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 7.5. 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 7.6. Suppose given a diagram

$$F_1 \begin{array}{c} \xrightarrow{u_0} \\ \xrightarrow{u_1} \end{array} F_0 \xrightarrow{u} F$$

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

- (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

$$\text{Hom}(F, T) \longrightarrow \text{Hom}(F_0, T) \begin{array}{c} \xrightarrow{\circ u_0} \\ \xrightarrow{\circ u_1} \end{array} \text{Hom}(F_1, T)$$

is exact.

REMARK 7.7. 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 7.8. 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:

$$\begin{array}{ccc} X_1 & \begin{array}{c} \xrightarrow{u_0} \\ \xrightarrow{u_1} \end{array} & X_0 & \xrightarrow{u} & X \\ & & & \searrow v & \downarrow \text{---} \\ & & & & T \end{array} \quad v \circ u_0 = v \circ u_1$$

In other words, u is the cokernel of (u_0, u_1) if

$$\text{Hom}(X, T) \rightarrow \text{Hom}(X_0, T) \rightrightarrows \text{Hom}(X_1, T)$$

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 $X_0 \times_X X_0 \rightrightarrows X_0$. Conditions (a) and (c) in (7.6) 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 7.9. A pair $u_0, u_1: F_1 \rightrightarrows F_0$ is an equivalence relation if and only if

- (a) $F_1(R) \xrightarrow{(u_0, u_1)} (F_0 \times F_0)(R)$ is a injective for all R ;
- (b) there exists a map $s: F_0 \rightarrow F_1$ such that $u_0 \circ s = \text{id}_{F_0} = u_1 \circ s$ (i.e., there exists a common section to u_0 and u_1);
- (c) there exist maps $v_0, v_1, v_2: F_2 \rightarrow F_1$ (of functors) such that

$$\begin{array}{ccccc} F_2 & \begin{array}{c} \xrightarrow{v_0} \\ \xrightarrow{v_1} \end{array} & F_1 & \xrightarrow{u_0} & F_0 \\ & & \downarrow v_2 & & \downarrow u_1 \\ & & F_1 & \begin{array}{c} \xrightarrow{u_0} \\ \xrightarrow{u_1} \end{array} & F_0 \end{array}$$

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

$$\begin{array}{ccc} F_2 & \xrightarrow{v_0} & F_1 \\ \downarrow v_2 & & \downarrow u_1 \\ F_1 & \xrightarrow{u_0} & F_0 \end{array} \quad \begin{array}{ccc} F_2 & \xrightarrow{v_1} & F_1 \\ \downarrow v_2 & & \downarrow u_1 \\ F_1 & \xrightarrow{u_1} & F_0 \end{array}$$

are cartesian.

PROOF. \implies :

(a) is part of the definition of 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

$$F_0 \xrightarrow{(\text{id}, \text{id})} S \xrightarrow{(u_0, u_1)^{-1}} F_1.$$

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

$$\left. \begin{array}{l} v_0 : (x, y, z) \mapsto (y, z) \\ v_1 : (x, y, z) \mapsto (x, z) \\ v_2 : (x, y, z) \mapsto (x, y) \end{array} \right\} \in F_1(R) = \{(z, w) \in (F_0 \times F_0)(R) \mid z \sim w\}.$$

With the last identification,

$$\begin{aligned} u_0(z, w) &= w \\ u_1(z, w) &= z. \end{aligned}$$

Now

$$\begin{aligned} u_0 \circ v_0 \text{ and } u_0 \circ v_1 &\text{ both map } (x, y, z) \text{ to } z \\ u_1 \circ v_0 \text{ and } u_1 \circ v_2 &\text{ both map } (x, y, z) \text{ to } y \\ u_1 \circ v_1 \text{ and } u_1 \circ v_2 &\text{ both map } (x, y, z) \text{ to } x. \end{aligned}$$

This proves the commutativity, and the first square is cartesian because

$$\begin{aligned} F_1 \times_{F_0} F_1 &= \{(x, y), (x', y') \mid x \sim y, x' \sim y', y = x'\} \\ &= \{(x, y, y') \mid x \sim y, y \sim y'\}. \end{aligned}$$

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

$$\left\{ \begin{array}{l} x = u_1(x') \\ y = u_0(x') \end{array} \right. \text{ some } x' \in F_1(R) \quad \left\{ \begin{array}{l} x = u_1(x'') \\ z = u_0(x'') \end{array} \right. \text{ some } x'' \in F_1(R).$$

Now $u_1(x') = u_1(x'')$, and so there exists an $x''' \in F_2(R)$ such that

$$v_1(x''') = x' \text{ and } v_2(x''') = x''$$

(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 $x \sim x$). \square

REMARK 7.10. Let $u_0, u_1: F_1 \rightrightarrows F_0$ be an equivalence relation. From the symmetry of the equivalence relation, we obtain an automorphism $s': F_0 \rightarrow F_0$ 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

7.11. Let M be 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. Recall that this is equivalent to M being finitely generated and projective (CA 12.5). We say that an A -algebra $u: A \rightarrow B$ is **locally free of finite rank** if it is so as an A -module.

7.12. 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 as in the last paragraph 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 sequence²

$$A \longrightarrow \prod_{i \in I} A_{f_i} \rightrightarrows \prod_{(i,j) \in I \times I} A_{f_i f_j}$$

we obtain a well-defined characteristic polynomial of b in $A[T]$.

7.13. Let A be a subring of B such that B is a faithfully flat A -module. 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 (Bourbaki AC I, 3.6, Pptn 12).

7.14. Let A be a ring and $u: M \rightarrow N$ a homomorphism of A -modules. Then u is injective (resp. surjective, bijective, zero) if and only if $u_{\mathfrak{m}}: M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$ is injective (resp. surjective, bijective, zero) for all maximal ideals \mathfrak{m} in A (Bourbaki AC, II, 3.3, Thm 1).

7.15. 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 (Bourbaki AC, II, 3.4, Cor. to Pptn 15).

²Because there exists a sheaf \mathcal{O} on $\text{spec}(A)$ with $\mathcal{O}(D(f)) = A_f$ for all $f \in A$, or use that $A \rightarrow \prod_i A_{f_i}$ is faithfully flat.

7.16. A locally free module of constant rank over a semilocal ring is free (Bourbaki, AC II, 5.3, Pptn 5).

7.17. If B faithfully flat over A and $M \otimes_A B$ faithfully flat over B , then M faithfully flat over A ,

$$\begin{array}{ccc} B & \xrightarrow{\text{faithfully flat}} & M \otimes_A B \\ \uparrow \text{faithfully flat} & & \uparrow \\ A & \xrightarrow{\quad\quad\quad} & M. \end{array}$$

To prove this statement, test with

$$(N): \quad N' \rightarrow N \rightarrow N''.$$

Then

$$(N) \text{ exact} \iff (N) \otimes_A B \text{ exact} \iff ((N) \otimes_A B) \otimes_B (M \otimes_A B) \text{ exact}.$$

But this last is isomorphic to $((N) \otimes_A M) \otimes_A B$, which is exact if and only if $(N) \otimes_A M$ is exact.

THE THEOREM

Let A_0 and A_1 be R_0 -algebras. We say that the pair of maps $u_0, u_1: A_0 \rightrightarrows A_1$ is an equivalence relation if $\circ u_0, \circ u_1: h^{A_1} \rightrightarrows h^{A_0}$ is an equivalence relation.

THEOREM 7.18. *Given an equivalence relation $u_0, u_1: A_0 \rightrightarrows A_1$ with u_0 locally free of constant rank r , then a quotient $u: A \rightarrow A_0$ exists; moreover, A_0 is locally free of rank r as an A -module.*

The proof will occupy the remainder of this subsection. Consider the diagram

$$\begin{array}{ccccc} A_2 & \xleftarrow{v_0} & A_1 & \xleftarrow{u_0} & A_0 \\ \uparrow v_2 & & \uparrow u_1 & & \uparrow u \\ A_1 & \xleftarrow{u_0} & A_0 & \xleftarrow{u} & A. \end{array}$$

Condition (c) for a quotient says that, for all R_0 -algebras R ,

$$\text{Hom}(R, A) \longrightarrow \text{Hom}(R, A_0) \begin{array}{c} \xrightarrow{u_0} \\ \xrightarrow{u_1} \end{array} \text{Hom}(R, A_1)$$

is exact. With $R = R_0$, this says that $A = \text{Ker}(u_0, u_1)$ and u equals the inclusion map — define them so. Then we know,

- (a) $h^{A_1}(R) \rightarrow (h^{A_0} \times h^{A_0})(R) = h^{A_0 \otimes_R A_0}(R)$ 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 the remark);
- (c) the undashed part of the diagram is commutative, and the two left hand squares are cocartesian (see the proposition);

- (d) u_1 is locally free of rank r (hypothesis and remark);
- (e) $u = \text{Ker}(u_0, u_1)$ (construction);
and we have to show
- (f) the right hand square is cocartesian ($\implies u$ is a quotient)
- (g) u is locally free of rank r .

STEP 0. Statement (a) is equivalent to (a'): $A_0 \otimes_A A_0 \rightarrow A_1$ is surjective.

PROOF. First note that we have a factorization

$$\begin{array}{ccccc} A_0 \otimes_{R_0} A_0 & \longrightarrow & A_0 \otimes_A A_0 & \longrightarrow & A_1 \\ h^{A_0} \times h^{A_0} & \longleftarrow & h^{A_0} \times_{h^A} h^{A_0} & \longleftarrow & h^{A_1} \end{array}$$

So (a) is equivalent to: (a*) $h^{A_1} \rightarrow h^{A_0 \otimes_A A_0}$ is injective. Certainly, (a') implies (a*). The converse follows from the general statement:

$$\left\{ \begin{array}{l} R \text{ a finite } C\text{-algebra} \\ h^R \rightarrow h^C \text{ injective} \end{array} \right\} \implies R \text{ is a quotient of } C, \text{ i.e., } C \xrightarrow{\text{onto}} R.$$

Note that $h^R \rightarrow h^C$ is injective if and only if $h^R \times_{h^C} h^R \simeq h^R$, i.e., the map $b \mapsto b \otimes 1 - 1 \otimes b: R \rightarrow R \otimes_C R$ is an isomorphism.

To show that $C \rightarrow R$ is surjective, it suffices to show that $C_{\mathfrak{m}} \rightarrow R_{\mathfrak{m}}$ is surjective for all maximal ideals \mathfrak{m} of C . Note that we still have

$$\left\{ \begin{array}{l} R_{\mathfrak{m}} \text{ a finite } C_{\mathfrak{m}}\text{-algebra} \\ R_{\mathfrak{m}} \simeq R_{\mathfrak{m}} \otimes_{C_{\mathfrak{m}}} R_{\mathfrak{m}}. \end{array} \right.$$

Thus, we may assume that C is local (with maximal ideal \mathfrak{m}). Then, by Nakayama's lemma, it suffices to prove that

$$C/\mathfrak{m}C \rightarrow R/\mathfrak{m}R$$

is surjective. Let $k = C/\mathfrak{m}C$ (a field) and $K = R/\mathfrak{m}R$. The hypotheses implies that $K \simeq K \otimes_k K$, but this implies that $\dim_k(K) = 1$, and so $k \simeq K$. \square

Note now that R_0 has dropped out of all the hypotheses, and so 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 (7.13). \square

STEP 2. We may assume 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 $A_{\mathfrak{p}}$ (arbitrary \mathfrak{p}). Then (f) follows from (7.14) and (g') follows from (7.15). \square

STEP 3. We may assume 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, $A \rightarrow (A[T])_{\mathfrak{p}}$ is flat (because $A \rightarrow A[T]$ 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 (7.17). □

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

$$F(T) = T^r - \sigma_1 T^{r-1} + \dots + (-)^r \sigma_r$$

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).

$$\begin{array}{ccc}
 A_2 \xleftarrow{v_0} A_1 \xleftarrow{u_0} A_0 & & z \xleftarrow{v_0} y \xleftarrow{u} x \\
 \uparrow v_2 & & \uparrow v_2 & & \uparrow F & & \uparrow u_1 \\
 A_1 \xleftarrow{u_0} A_0 \xleftarrow{u} A & & * \xleftarrow{u_0} * & & & & * \\
 \uparrow v_1 & & \uparrow u_1 & & & & \\
 A_1 \xleftarrow{u_0} A_0 & & & & & &
 \end{array}$$

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 $F_0(x) = 0$. □

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 $\mathfrak{m}_1, \dots, \mathfrak{m}_N$ be distinct maximal ideals of A_0 , and let $a_1, \dots, a_N \in A$ be distinct modulo \mathfrak{m} (recall that the residue field is infinite). Take $x \in A_0$ such that $x \equiv a_i \pmod{\mathfrak{m}_i}$ (exists by the Chinese remainder theorem). Then the characteristic polynomial of x , modulo \mathfrak{m} , has N distinct roots, namely, a_1, \dots, a_N , and so $N \leq r$. □

STEP 6. *Completion of the proof.*

Now apply (7.16):

$$\left. \begin{array}{l} A_1 \text{ locally free of rank } r \text{ over } A_0 \text{ (via } u_1) \\ A_0 \text{ semilocal} \end{array} \right\} \implies A_1 \text{ free over } A_0 \text{ (via } u_1)$$

Note that the set $u_0(A_0)$ generates A_1 as a (u_1, A_0) -module (because $A_0 \otimes_A A_0 \rightarrow A_1$ is surjective). Therefore Lemma 7.19 below shows that there $x_1, \dots, x_r \in A_0$, such that $u_0(x_1), \dots, u_0(x_r)$ 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 $\{x_1, \dots, x_r\}$ 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

$$\begin{aligned} z &= v_0(y) = v_1(y) \\ z_i &= v_0(y_i) = v_1(y_i). \end{aligned}$$

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 7.19. *Let $u: A \rightarrow B$ be a homomorphism with A local and B semilocal. Assume that u maps the maximal ideal \mathfrak{m} of A into the radical \mathfrak{r} 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. 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 $B = \prod_j k_j$ of k . Correspondingly, $N = \prod_j N_j$ 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.

I 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

$$m = \sum c_j m_j, \quad c_j \in k.$$

The set of families (c_j) such that $m = 0$ in N_j is a proper subspace of k^r , and a finite union of proper subspaces of a finite dimensional vector space over an infinite field cannot equal the whole space³ — hence we can find 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 induction, 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}, m form a B -basis for N . \square

REMARK 7.20. Let $u: A \rightarrow A_0$ be faithfully flat. Then $u = \text{Ker}(u_0, u_1)$, 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 $u: A \rightarrow A_0$. The theorem says that every equivalence relation with A_1 locally free of constant rank over A_0 is of this form.

REMARK 7.21. (a) The situation

$$A \xrightarrow{u} A_0 \begin{array}{c} \xrightarrow{u_0} \\ \xrightarrow{u_1} \end{array} A_0 \otimes_A A_0 \quad \left\{ \begin{array}{l} u \text{ faithfully flat} \\ u = \text{Ker}(u_0, u_1) \end{array} \right.$$

³Suppose $V = \bigcup_{i=1}^n V_i$ with $V_i \neq V$. Let $f_i: V \rightarrow k$ 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.

is stable under base change (because u stays faithfully flat).

(b) The above situation is stable under products, i.e.,

$$\begin{array}{ccccc} A & \longrightarrow & A_0 & \rightrightarrows & A_0 \otimes_A A_0 \\ \otimes_{R_0} & & \otimes_{R_0} & & \otimes_{R_0} \\ B & \longrightarrow & B_0 & \rightrightarrows & B_0 \otimes_B B_0 \end{array}$$

is of the same form.

(c) A map $\varphi: A_0 \rightarrow B_0$ defines a map $A \rightarrow B$ if $\varphi \otimes \varphi$ satisfies the obvious commutativity condition:

$$\begin{array}{ccccc} A & \xrightarrow{u} & A_0 & \rightrightarrows & A_1 \\ \downarrow & & \downarrow \varphi & & \\ B & \longrightarrow & B & \rightrightarrows & B_1. \end{array}$$

In other words, we have a map

$$\text{Hom}((A_0, A_1), (B_0, B_1)) \rightarrow \text{Hom}(A, B).$$

c. Existence of quotients in the finite case

PRELIMINARIES

7.22. Let Z be a closed subset of $X = \text{Spec}(A)$ and let S be a finite set of points of $X \setminus Z$; then there exists an $f \in A$ such that f is zero on Z but is not zero at any point in S .

PROOF. This is the prime avoidance lemma (CA 2.8) □

7.23. Let $A \rightarrow B$ be a locally free A -algebra of rank r . Let \mathfrak{p} be a prime ideal in A , and let $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ be the prime ideals of B lying over it. An element b of B lies in $\mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_n$ if and only if its norm $\text{Nm}(b) \in \mathfrak{p}$.

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 $\mathfrak{q}_1, \dots, \mathfrak{q}_n$. Then B is free of rank r (7.16), and $\text{Nm}(b)$ is the determinant of A -linear map $\ell_b: B \rightarrow B, x \mapsto bx$. Now

$$\begin{aligned} \text{Nm}(b) \notin \mathfrak{p} &\iff \text{Nm}(b) \text{ invertible} \quad (\mathfrak{p} \text{ is the only maximal ideal of } A) \\ &\iff \ell_b \text{ invertible} \quad (\text{linear algebra}) \\ &\iff b \text{ is invertible in } B \\ &\iff b \notin \mathfrak{q}_1 \cup \dots \cup \mathfrak{q}_n. \quad (\mathfrak{q}_1, \dots, \mathfrak{q}_n \text{ are the only maximal ideals of } B). \quad \square \end{aligned}$$

THE THEOREM

Let X be an algebraic scheme over R_0 , i.e., a scheme of finite type over $\text{Spec}(R_0)$. Then X defines a functor \tilde{X} , and $X \rightsquigarrow \tilde{X}$ is an equivalence of categories. By an equivalence relation on X , we mean an equivalence relation on \tilde{X} .

THEOREM 7.24. Let $(u_0, u_1): X_1 \rightrightarrows X_0$ be an equivalence relation on the algebraic scheme X_0 over R_0 . Assume

- (a) $u_0: X_1 \rightarrow X_0$ 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 of X_0 .

Then a quotient $u: X_0 \rightarrow X$ exists; moreover, u is locally free of rank r .

The proof will occupy the rest of this subsection.

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 $u_1u_0^{-1}(x)$. Let U' denote the union of the equivalence classes contained in U , i.e., U' is the complement in U of $u_1u_0^{-1}(X_0 \setminus U)$. 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 , but it need not be affine.

As U is affine and the set $u_1u_0^{-1}(x)$ is finite and contained in U' , there exists an $f \in \mathcal{O}_{X_0}(U)$ that is zero on $U \setminus U'$ but is not zero at any of the points of $u_1u_0^{-1}(x)$ (7.22). In other words, the principal open subset $D(f)$ of U is contained in U' and contains $u_1u_0^{-1}(x)$. Let U'' be the union of the equivalence classes contained in $D(f)$, i.e.,

$$U'' = D(f) \setminus u_1u_0^{-1}(U' \setminus D(f)).$$

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 $Z(f) = U' \setminus D(f)$. It is the zero set of f in U' , and so $u_0^{-1}(Z(f))$ is the zero set of $u_0^*(f)$ in $u_0^{-1}(U')$. Therefore $u_1u_0^{-1}(Z(f))$ is the zero set of $\text{Nm}(u_0^*(f))$ in U' (7.23). By construction, its complement in $D(f)$ is exactly U'' , and so U'' is the set of points of $D(f)$ where $\text{Nm}(u_0^*(f))$ is not zero, which is an open affine subset of $D(f)$. \square

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 $u: X_0 \rightarrow X$ in the category of R_0 -ringed spaces.
- (b) If u_0, u_1 , and u are morphisms of schemes, and then $u: X_0 \rightarrow X$ 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

$$\mathcal{O}_X(U) \rightarrow \mathcal{O}_{X_0}(u^{-1}(U)) \rightrightarrows \mathcal{O}_{X_1}((u_0 \circ u)^{-1}U)$$

is exact. Then \mathcal{O}_X is a sheaf of R_0 -algebras on X , and $u: X_0 \rightarrow X$ is a cokernel of (u_0, u_1) in the category of ringed spaces.

(b) Let $v: X_0 \rightarrow T$ be a morphism of schemes such that $v \circ u_0 = v \circ u_1$. By hypothesis, there exists a unique morphism of ringed spaces $r: X \rightarrow T$ such that $r \circ u = v$. It remains to show that, for all $x \in X$, the homomorphism $\mathcal{O}_{r(x)} \rightarrow \mathcal{O}_x$ induced by r is local. But $x = u(x_0)$ for some $x_0 \in X_0$, and $\mathcal{O}_x \rightarrow \mathcal{O}_{x_0}$ and the composite

$$\mathcal{O}_{r(x)} \rightarrow \mathcal{O}_x \rightarrow \mathcal{O}_{x_0}$$

are local, which implies the statement. \square

STEP 3. Completion of the proof

PROOF. Let (u_0, u_1) be as in the statement of the theorem. As in the affine case, we first construct the cokernel $u: X_0 \rightarrow X$ of (u_0, u_1) in the category of 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 ringed spaces. From the affine case (7.18), we see that V is an affine scheme. As finitely many V cover X (Step 1), we deduce that X is an algebraic scheme over R_0 and that u is a morphism of R_0 -schemes. It follows that u is the cokernel of (u_0, u_1) in the category of schemes over R_0 (Step 2); moreover, $X_1 \simeq X_0 \times_X X_0$ because this condition is local on X . \square

REMARK 7.25. It is possible to weaken the hypothesis (a) to

$$u_0: X_1 \rightarrow X_0 \text{ is locally free of finite rank,}$$

because such an equivalence relation decomposes into a finite disjoint union of equivalence relations of constant rank.

APPLICATION

PROPOSITION 7.26. *Let G be an algebraic group over R_0 , and let H be an algebraic subgroup of G . Assume that H is locally free of rank r over R_0 . Then the quotient sheaf G/H is representable by an algebraic scheme G/H over R_0 , and the morphism $G \rightarrow G/H$ is locally free of rank r ; moreover, $G \times H \simeq G \times_{G/H} G$.*

PROOF. Apply the theorem to the equivalence relation

$$G \times H \begin{array}{c} \xrightarrow{(g, h) \mapsto gh} \\ \xrightarrow{(g, h) \mapsto g} \end{array} G.$$

on G . \square

d. Existence of quotients in the presence of quasi-sections

PRELIMINARIES

We shall need the following technical lemma.

LEMMA 7.27. *Let*

$$\begin{array}{ccc} Y_1 & \begin{array}{c} \xrightarrow{v_0} \\ \xrightarrow{v_1} \end{array} & Y_0 \\ \downarrow f_1 & & \downarrow f_0 \\ X_1 & \begin{array}{c} \xrightarrow{u_0} \\ \xrightarrow{u_1} \end{array} & X_0 \end{array}$$

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 $\Delta: Y_0 \times_{X_0} Y_0 \rightarrow Y_1$ 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

$$\text{Coker}(v_0, v_1) \rightarrow \text{Coker}(u_0, u_1)$$

PROOF. Let T be an object of \mathcal{C} , and consider the diagram

$$\begin{array}{ccccc} C(u_0, u_1)(T) & \xrightarrow{u} & \text{Hom}(X_0, T) & \rightrightarrows & \text{Hom}(X_1, T) \\ \downarrow f(T) & & \downarrow T(f_0) & & \downarrow T(f_1) \\ C(v_0, v_1)(T) & \xrightarrow{v} & \text{Hom}(Y_0, T) & \rightrightarrows & \text{Hom}(Y_1, T). \end{array}$$

in which the left hand terms are defined to make the rows exact. Here $T(f_i)$ is the map defined by $f_i: Y_i \rightarrow X_i$. The cokernel of (u_0, u_1) exists if and only if the functor $T \rightsquigarrow C(u_0, u_1)(T): \mathcal{C} \rightarrow \text{Set}$ 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 the $C(u_0, u_1)$ 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 the second part of the statement is obvious.

Let $g \in C(v_0, v_1)(T)$. Thus g is a map $Y_0 \rightarrow T$ such that $g \circ v_0 = g \circ v_1$:

$$\begin{array}{ccccc} & & Y_0 \times_{X_0} Y_0 & & \\ & \swarrow \Delta & \downarrow p_1 \downarrow p_2 & & \\ Y_1 & \xrightarrow{v_0} & Y_0 & \xrightarrow{g} & T \\ \downarrow f_1 & \xrightarrow{v_1} & \downarrow f_0 & & \\ X_1 & \xrightarrow{u_0} & X_0 & \xrightarrow{h} & T \\ & \xrightarrow{u_1} & & & \end{array}$$

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 $h: X_0 \rightarrow T$, 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 an epimorphism. \square

Recall that “functor” means “set-valued functor on finitely generated R_0 -algebras representable by a scheme of finite type over $\text{Spec}(R_0)$ ”. Thus it makes sense to say that a map of functors is faithfully flat. Moreover, a faithfully flat morphism is an effective epimorphism. The pull-back of a faithfully flat morphism is faithfully flat, and so is also an effective epimorphism.

We shall apply the lemma in the following situation: (u_0, u_1) is an equivalence relation, and (v_0, v_1) is the inverse image of (u_0, u_1) with respect to a faithfully flat map $f_0: Y_0 \rightarrow X_0$. Then f_1 is a pull-back of f_0 , and so f_0 and f_1 are both faithfully flat, and hence effective epimorphisms. There exists a morphism $s: X_0 \rightarrow X_1$ such that $u_0 \circ s = \text{id}_{X_0} = u_1 \circ s$ (7.9) and we can take Δ to be the section of $Y_1 \rightarrow Y_0 \times_{X_0} Y_0$ defined by the morphism

$$Y_0 \times_{X_0} Y_0 \xrightarrow{p_1} Y_0 \xrightarrow{f_0} X_0 \xrightarrow{s} X_1.$$

It is possible to replace the condition “ f_0 is faithfully flat” with the condition “ f_0 admits a section”.

THE THEOREM

DEFINITION 7.28. 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 a finite locally free surjective morphism $f: u_0^{-1}(Y_0) \rightarrow X_0$;
- (b) every subset of Y_0 consisting of points that are equivalent in pairs is contained in an open affine of Y_0 .

Condition (a) says, in particular, that Y_0 meets every equivalence class in a finite nonempty set. Therefore, the subsets in (b) are finite. Condition (b) says that, for all $x \in Y_0$, the finite set $u_1 u_0^{-1}(x) \cap Y_0$ is contained in an open affine of Y_0 .

THEOREM 7.29. 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 $u: X_0 \rightarrow X$ exists; moreover, u is surjective, and if u_0 is open (resp. universally closed, flat) then u is also.

PROOF. Let Y_0 be a quasi-section. Let $i: Y_0 \hookrightarrow X_0$ be 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 . By definition (7.4), Y_1 is the intersection $u_0^{-1}(Y_0) \cap u_1^{-1}(Y_0)$, and so we have a cartesian square:

$$\begin{array}{ccc} Y_1 & \longrightarrow & u_0^{-1}(Y_0) \\ \downarrow v_1 & & \downarrow f = u_1|_{u_0^{-1}(Y_0)} \\ Y_0 & \xrightarrow{i} & X_0. \end{array} \quad \begin{array}{l} f = u_1|_{u_0^{-1}(Y_0)} \\ v_1 = u_1|_{Y_1} \end{array}$$

It follows that v_1 is finite locally free and surjective. Therefore, the equivalence relation $Y_1 \rightrightarrows Y_0$ on Y_0 satisfies the hypotheses of Theorem 7.24, and so it admits a quotient $v: Y_1 \rightarrow Y$.

Let $Z_0 = u_0^{-1}(Y_0)$. Let $u'_0: Z_0 \rightarrow Y_0$ be the restriction of u_0 to Z_0 , and let $(w_0, w_1): Z_1 \rightrightarrows Z_0$ be the inverse image of (v_0, v_1) with respect to u'_0 . The morphism $u'_0: Z_0 \rightarrow Y_0$ admits a section (because u_0 does 7.9b), and so Lemma 7.27 et seq. shows that the pair of maps $(w_0, w_1): Z_1 \rightrightarrows Z_0$ admits a cokernel $w: Z_0 \rightarrow Z$ (equal to $v \circ u'_0: Z_0 \rightarrow Y$). Moreover, $Z_1 \rightarrow Z_0 \times_Z Z_0$ is an isomorphism because it is a pull-back of the isomorphism $Y_1 \rightarrow Y_0 \times_Y Y_0$. Thus w is a quotient of (w_0, w_1) .

We now have a diagram

$$\begin{array}{ccccc} Y_1 & \xrightarrow{v_0} & Y_0 & & \\ \uparrow & v_1 & \uparrow & \searrow v & \\ Z_1 & \xrightarrow{w_0} & Z_0 & \xrightarrow{w} & Z \\ \downarrow & w_1 & \downarrow f & \nearrow u & \\ X_1 & \xrightarrow{u_0} & X_0 & & \\ & & u_1 & & \end{array}$$

Here v and w are the cokernels of (v_0, v_1) and (w_0, w_1) respectively. Note that (w_0, w_1) is the inverse image of (u_0, u_1) with respect to $i \circ u'_0$, which equals the map $Z_0 \hookrightarrow X_1 \xrightarrow{u_0} X_0$. Therefore, according to Example 7.5, 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 equals f , which is finite and locally free, and so it is faithfully flat. Lemma 7.27 et seq. now shows that there exists a morphism $u: X_0 \rightarrow Z$ such that $u \circ f = w$ and u is the cokernel of (u_0, u_1) .

The morphism $X_1 \rightarrow X_0 \times_Y X_0$ is an isomorphism because the morphism $Z_1 \rightarrow Z_0 \times_Z Z_0$ obtained from it by a faithfully flat base change $f \times f$ is an isomorphism. We have shown that $u: X_0 \rightarrow Z$ is a quotient of (u_0, u_1) .

Finally, u is obviously surjective. The morphism v is finite and locally free (7.24), and it now follows easily from the above diagram that u is open (resp. universally closed, flat) if u_0 is. \square

REMARK 7.30. The map $u: X_0 \rightarrow Z$ is the cokernel of (u_0, u_1) in the category of ringed spaces.

e. Existence generically of a quotient

We now work over a base field k .

PRELIMINARIES

7.31. Let X and Y be algebraic schemes over field 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 .

PROOF. The fibre of $X \times Y$ over $\{x, y\}$ is equal to the fibre of $\text{Spec}(\kappa(x)) \times Y \rightarrow Y$ over y . But, because x is closed, $\kappa(x)$ is a finite extension of k , and so this fibre is obviously finite. \square

7.32. Let $A \rightarrow B$ be a local homomorphism of local noetherian rings, and let $u: M' \rightarrow M$ 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 $\text{Coker}(u)$ is flat over A . (SGA 1, IV, 5.7).

THE THEOREM

THEOREM 7.33. Let $u_0, u_1: X_1 \rightrightarrows X_0$ be an equivalence relation on an algebraic scheme X 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 (7.29) 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) $Z \cap u_1 u_0^{-1}(z)$ is finite and nonempty; (b) $u_0^{-1}(Z) \xrightarrow{u_1} X$ is flat at the points of $u_1^{-1}(z)$.

PROOF. We construct a Z satisfying (a), and then show that the Z we have constructed also satisfies (b).

To obtain Z , we construct a strictly decreasing sequence $Z_0 \supset Z_1 \supset \dots$ of closed subsets of X_0 such that $Z \cap u_1 u_0^{-1}(z)$ 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 (a). 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, \dots, 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 $u_0(y_1), \dots, u_0(y_r)$. 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 $f \in k[X_0, \dots, X_m]$ which is zero at x but not at any point $u_0(y_i)$ (homogeneous avoidance lemma; cf. 7.22). 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 (7.32) implies that \mathcal{O}'_y is flat over \mathcal{O}_z . \square

STEP 2. *Let z be a closed point of X_0 . There exists a saturated open subset W_z of X_0 admitting a quasi-section and meeting all the irreducible components of X passing through z .*

PROOF. Let Z be as in Step 1, and let $u'_1: u_0^{-1}(Z) \rightarrow X_0$ be the restriction of u_1 . The fibre $u'^{-1}_1(z)$ is finite (7.31). 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 greatest 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). \square

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 $u_0^{-1}(X_0 \setminus \bar{W}_z)$ is then saturated (because $u_1(u_0^{-1}(X_0 \setminus \bar{W}_z))$ 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 $X_0 \setminus \bar{W}_z$. Then W_z and $W_{z'}$ are disjoint, and the equivalence relation induced on $W_z \cup W_{z'}$ 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. \square

As noted earlier, this completes the proof of the theorem.

f. Existence of quotients of algebraic groups

PRELIMINARIES

LEMMA 7.34. *Let X be an algebraic scheme over a field k . Suppose that, for every finite extension k' of k , we have an open subscheme $U[k']$ of $X_{k'}$ containing $X(k')$, and that $U[k']_{k''} \subset U[k'']$ if $k' \subset k''$. Then $U[k'] = X_{k'}$ for some finite extension k' of k .*

PROOF. Let $Z[k']$ denote the complement of $U[k']$ in $X_{k'}$. Choose a closed point x_i in each irreducible component of $Z[k]$, and let K/k be a finite normal extension of k such that the residue field $\kappa(x_i)$ embeds into K for all i . Every point of X_K above an x_i is K -rational and so lies in $U[K]$, and so $\dim Z[K] < \dim Z[k]$. On repeating the argument with K for k , we obtain a finite extension L/K such that

$$\dim Z[L] < \dim Z[K] < \dim Z[k].$$

Eventually this process stops with $Z[k']$ empty. \square

THE THEOREM

THEOREM 7.35. *Let H be an algebraic subgroup of a quasi-projective algebraic group G over k . Then G admits a quotient G/H for the equivalence relation defined by H (7.2); in particular, the sheaf $G\tilde{/}H$ is represented by an algebraic scheme G/H over k . The quotient map $u: G \rightarrow G/H$ is faithfully flat.*

The proof will occupy the remainder of this subsection.

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 greatest 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 7.33 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 7.34 shows that $U[k'] = X_{k'}$ for some k' . \square

STEP 2. *Suppose that the quotient sheaf $G\tilde{/}H$ is representable by an algebraic scheme X over k . Then every finite set of closed points of X is contained in an open affine.*

PROOF. Let $u: G \rightarrow X$ denote the quotient map. Let U be a dense open affine subset of X , and let x_1, \dots, x_n be closed points 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, for all i ,

$$g \in g_i \cdot (u^{-1}(U))^{-1}$$

and so $g_i \in g \cdot u^{-1}(U)$ and $x_i \in g \cdot U$. Therefore the open affine $g \cdot U$ 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 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 $X_K \rightarrow X$. By arguing as in (7.18), we obtain a saturated open affine $W' \subset U'$ 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 7.18). \square

STEP 3. *Conclusion (descent)*

PROOF. Let K be a finite extension of k such that the quotient $G_K \rightarrow G_K/H_K$ exists. The inverse image of the equivalence relation

$$\mathrm{Spec}(K \otimes_k K) \begin{array}{c} \xrightarrow{p_1} \\ \xrightarrow{p_2} \end{array} \mathrm{Spec}(K)$$

(see 7.3) with respect to $G_K/H_K \rightarrow \mathrm{Spec}(K)$ is an equivalence relation on G_K/H_K satisfying the conditions of Theorem 7.24. Its quotient is the required quotient of G by H . \square

REMARK 7.36. The hypothesis that G be quasi-projective in (7.35) can be removed in two different ways: (a) by removing the hypothesis from (7.33); (b) by using that every algebraic group over a field is quasi-projective.

APPLICATIONS

PROPOSITION 7.37. *Every monomorphism of algebraic groups is a closed immersion.*

PROOF. Let $H \rightarrow G$ be a monomorphism of algebraic groups. Then H is isomorphic (as a sheaf, and hence as a scheme) to the fibre of the map $G \rightarrow G/H$ over the distinguished point of G/H . Therefore $H \rightarrow G$ is a closed immersion. \square

PROPOSITION 7.38. *Let N be a normal algebraic subgroup of an algebraic group G . The homomorphism of sheaves $G \rightarrow G/\tilde{N}$ is represented by an faithfully flat homomorphism $G \rightarrow G/N$ of algebraic groups*

PROOF. We know G/\tilde{N} is a functor to groups whose underlying functor to sets is representable by an algebraic scheme G/N . Therefore G/N is an algebraic group. \square

NOTES. The elementary proof of (7.18) follows lectures of Tate from 1967. For the rest, we have followed the original source, SGA 3, V, and Brochard 2014.

g. Complements

Groupoids. List the known results (and explain how the above proofs generalize)..

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 . A **subnormal series**¹ of G is a finite sequence $(G_i)_{i=0,\dots,s}$ 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 $i = 1, \dots, s$:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = e. \quad (41)$$

A subnormal series $(G_i)_i$ is a **normal series** (resp. **characteristic series**) if each G_i is normal (resp. characteristic) in G . A subnormal series is **central** if it is a normal series such that G_i/G_{i+1} is contained in the centre of G/G_{i+1} for all i .

PROPOSITION 8.1. *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

$$H \cap G_i / H \cap G_{i+1} \hookrightarrow G_i / G_{i+1}.$$

PROOF. Consider the algebraic subgroup $H \cap G_i$ of G_i . According to the isomorphism theorem (5.37, 6.19), the algebraic subgroup $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}$ of G_i is normal, and

$$H \cap G_i / H \cap G_{i+1} \simeq (H \cap G_i) \cdot G_i / G_{i+1} \hookrightarrow G_i / G_{i+1}. \quad \square$$

¹Demazure and Gabriel (1970, IV, p.471) and some other authors call this a composition series (suite de composition), but this conflicts with the usual terminology in English and German, which requires that the quotients in a composition series (Compositionsreihe) be simple, i.e., a composition series is a maximal subnormal series (Albert, Modern Higher Algebra; Burnside, Theory of Groups of Finite Order; Dummit and Foote, Abstract Algebra; Hungerford, Algebra; Jacobson, Basic Algebra; van der Waerden, Modern Algebra; Weber, Lehrbuch der Algebra (1899, II, p.23); Wikipedia; Zariski and Samuel, Commutative Algebra).

Two subnormal sequences

$$\begin{aligned} G &= G_0 \supset G_1 \supset \cdots \supset G_s = e \\ G &= H_0 \supset H_1 \supset \cdots \supset H_t = e \end{aligned} \quad (42)$$

are said to be **equivalent** if $s = t$ and there is a permutation π of $\{1, 2, \dots, s\}$ such that $G_i/G_{i+1} \approx H_{\pi(i)}/H_{\pi(i)+1}$.

THEOREM 8.2. *Any two subnormal series (42) in an algebraic group have equivalent refinements.*

PROOF. Let $G_{i,j} = G_{i+1}(H_j \cap G_i)$ and $H_{j,i} = H_{j+1}(G_i \cap H_j)$, and consider the refinements

$$\begin{aligned} \cdots \supset G_i &= G_{i,0} \supset G_{i,1} \supset \cdots \supset G_{i,t} = G_{i+1} \supset \cdots \\ \cdots \supset H_j &= H_{j,0} \supset H_{j,1} \supset \cdots \supset H_{j,s} = H_{j+1} \supset \cdots \end{aligned}$$

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) . \square

LEMMA 8.3 (BUTTERFLY LEMMA). *Let $H_1 \supset N_1$ and $H_2 \supset N_2$ be algebraic subgroups of an algebraic group G with N_1 and N_2 normal in H_1 and H_2 . Then $N_1(H_1 \cap H_2)$ and $N_2(N_1 \cap H_2)$ are normal algebraic subgroups of the algebraic groups $N_1(H_1 \cap H_2)$ and $N_2(H_2 \cap H_1)$ respectively, and there is a canonical isomorphism of algebraic groups*

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}$$

PROOF. The algebraic group $H_1 \cap H_2$ is normal in $H_1 \cap H_2$ and so $N_1(H_1 \cap H_2)$ is normal in $N_1(H_1 \cap H_2)$ (see Exercise 6-1). Similarly, $N_2(H_2 \cap N_1)$ is normal in $N_2(H_2 \cap H_1)$.

The subgroup $H_1 \cap H_2$ of G normalizes $N_1(H_1 \cap H_2)$, and so the isomorphism Theorem 5.37 shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap H_2)} \simeq \frac{(H_1 \cap H_2) \cdot N_1(H_1 \cap H_2)}{N_1(H_1 \cap H_2)}. \quad (43)$$

As $H_1 \cap N_2 \subset H_1 \cap H_2$, we have that $H_1 \cap H_2 = (H_1 \cap H_2)(H_1 \cap N_2)$, and so

$$N_1 \cdot (H_1 \cap H_2) = N_1 \cdot (H_1 \cap H_2) \cdot (H_1 \cap N_2).$$

The first of Dedekind's modular laws (Exercise 6-2a) with $A = H_1 \cap N_2$, $B = H_1 \cap H_2$, and $C = N_1$ becomes

$$\begin{aligned} (H_1 \cap H_2) \cap N_1(H_1 \cap H_2) &= (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) \\ &= (H_1 \cap N_2)(N_1 \cap H_2). \end{aligned}$$

Therefore (43) is an isomorphism

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)}.$$

A symmetric argument shows that

$$\frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)},$$

and so

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(H_2 \cap N_1)}. \quad \square$$

b. Isogenies

DEFINITION 8.4. An *isogeny* of algebraic groups is a normal homomorphism whose kernel and cokernel are both finite.²

For connected group varieties, this agrees with the definition in (2.17). For commutative algebraic groups, it agrees with the definition in DG V, §3, 1.6, p.577; specifically, they define an isogeny of commutative affine group schemes (not necessarily of finite type) over a field k to be a morphism with profinite kernel and cokernel.

It follows from Exercise 6-5 that a composite of isogenies is an isogeny if it is normal.

DEFINITION 8.5. Two algebraic groups G and H are *isogenous*, denoted $G \sim H$, if there exist algebraic groups G_1, \dots, G_n such that $G = G_1$, $H = G_n$, and, for each $i = 1, \dots, n-1$, either there exists an isogeny $G_i \rightarrow G_{i+1}$ or there exists an isogeny $G_{i+1} \rightarrow G_i$.

In other words, “isogeny” is the equivalence relation generated by the binary relation “there exists an isogeny from G to H ”.

c. Composition series for algebraic groups

Let G be an algebraic group over k . A subnormal series

$$G = G_0 \supset G_1 \supset \dots \supset G_s = e$$

is a *composition series* if

$$\dim G_0 > \dim G_1 > \dots > \dim G_s$$

and the series can not 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

²Is this the correct definition for nonconnected algebraic groups? I can't find a definition in the literature. For example, CGP don't define it, and SGA 3 only defines an isogeny of reductive (hence connected) groups (XXII, 4.2.9). An isogeny is defined to be a surjective homomorphism with finite kernel by authors who (implicitly) assume that all algebraic groups are smooth and connected. Do they mean $G_{\text{red}} \rightarrow G$ to be an isogeny? (over a perfect field say). It is always surjective with trivial kernel. The Encyclopedia of Math defines an isogeny of group schemes to be an epimorphism with finite flat kernel (epimorphism in what category? not group schemes).

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

$$\mu_1 \subset \mu_{1^2} \subset \mu_{1^3} \subset \cdots \subset \mathbb{G}_m$$

shows that \mathbb{G}_m does not.

LEMMA 8.6. *Let*

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

be a subnormal series 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 8.7. *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 is a permutation π of $\{1, 2, \dots, s\}$ such that G_i/G_{i+1} is isogenous to $H_{\pi(i)}/H_{\pi(i)+1}$ for all i .

PROOF. The existence of a composition series is obvious. For the proof of the second statement, we use the notations of the proof of (8.2):

$$G_{i,j} \stackrel{\text{def}}{=} G_{i+1}(H_j \cap G_i)$$

$$H_{j,i} \stackrel{\text{def}}{=} H_{j+1}(G_i \cap H_j).$$

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

$$\begin{aligned} G_i/G_{i+1} &\sim G_{i,\pi(i)}/G_{i,\pi(i)+1} && (8.6) \\ &\approx H_{\pi(i),i}/H_{\pi(i),i+1} && \text{(butterfly lemma)} \\ &\sim H_{\pi(i)}/H_{\pi(i)+1} && (8.6). \end{aligned}$$

As $i \mapsto \pi(i)$ is a bijection, this completes the proof. □

EXAMPLE 8.8. 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.

REMARKS

8.9. 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 (1.39). Therefore $(G_i^\circ)_i$ is still a composition series.

8.10. An algebraic group is connected if and only if it has no nontrivial finite étale quotient (see Chapter 7). An algebraic group is said to be **strongly connected** if it has no nontrivial finite quotient (étale or not). A strongly connected algebraic group is connected, and a smooth connected algebraic group is strongly connected (because all of its quotients are smooth 5.8).

We define the **strong identity component** G^{so} of G to be the intersection of the kernels of the homomorphisms from G to a finite algebraic group. It is the smallest normal algebraic subgroup having the same dimension as G . If G is smooth, then $G^{so} = G^\circ$. If k is perfect and G_{red} is normal in G , then $G^{so} = (G_{\text{red}})^\circ$ (because G_{red} is smooth, and the $(G_{\text{red}})^\circ$ is a characteristic subgroup of G_{red}).

One may hope that every algebraic group has a composition series whose terms are strongly connected, but this seems unlikely — the argument in (8.9) fails because we do not know that N^{so} is characteristic in N .³

d. Solvable and nilpotent algebraic groups

An algebraic group is solvable if it can be constructed from commutative algebraic groups by successive extensions, and it is nilpotent if it can be constructed from commutative algebraic groups by successive *central* extensions. More formally:

DEFINITION 8.11. An algebraic group G is **solvable** if it admits 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**).

DEFINITION 8.12. An algebraic group G is **nilpotent** if it admits a central subnormal series (see p.125), 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** or **central series**).

PROPOSITION 8.13. *Algebraic subgroups, quotients, and extensions of solvable algebraic groups are solvable.*

PROOF. An intersection of a solvable series in G with an algebraic subgroup H is a solvable series in H (apply 8.1); the image in a quotient Q of a solvable series in G is a solvable series in Q (correspondence theorem 5.39); and a solvable series in a normal algebraic subgroup N of G can be combined with a solvable series in G/N to give a solvable series in G . □

³I thank Michael Wibmer for pointing this out to me.

EXAMPLE 8.14. The group \mathbb{T}_n of upper triangular matrices is solvable, and the group \mathbb{U}_n is nilpotent (see 8.46).

EXAMPLE 8.15. 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 that 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).

PROPOSITION 8.16. *Algebraic subgroups and quotients (but not necessarily extensions) of nilpotent algebraic groups are nilpotent.*

PROOF. An intersection of a nilpotent series in G with an algebraic subgroup H is a nilpotent series in H (apply 8.1). The image in a quotient Q of a nilpotent series in G is a nilpotent series in Q . \square

DEFINITION 8.17. 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 \mathbb{G}_m .

Every term G_i in such a subnormal series is smooth, connected, and affine (10.1 below); in particular, every split solvable algebraic group G is smooth, connected, and affine.

NOTES. In the literature, a split solvable algebraic group over k is usually called a k -solvable algebraic group or a k -split solvable algebraic group. We can omit the “ k ” because of our convention that statements concerning an algebraic group G over k are intrinsic to G over k . Here are a few of the definitions in the literature.

DG IV, §4, 3.1, p.530: The k -group G is said to be k -résoluble [k -solvable] if it is affine and admits a subnormal series whose quotients are isomorphic to \mathbb{G}_a or \mathbb{G}_m [note that the “affine” is automatic].

SGA3, XVII, 5.1.0: Let k be a field and G an algebraic k -group. Following the terminology introduced by Rosenlicht (*Questions of rationality for solvable algebraic groups over nonperfect fields*. Ann. Mat. Pura Appl. (4) 61 1963 97–120), we say that G is “ k -résoluble” if it has a composition series [i.e., subnormal series] whose successive quotients are isomorphic to \mathbb{G}_a .

Conrad et al. 2010, A.1, p.392: A smooth connected solvable group G over a field k is k -split if it admits a composition series [presumably meaning subnormal series] over k whose successive quotients are k -isomorphic to \mathbb{G}_m or \mathbb{G}_a [note that the “smooth” and “connected” are automatic; in the modern world, the “ k ” seems superfluous].

Borel 1991, 15.1: Let G be connected solvable [it is affine group variety over k]. G splits over k , or is k -split, if it has a composition series [presumably meaning subnormal series] $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ consisting of connected k -subgroups such that G_i/G_{i+1} is k -isomorphic to \mathbb{G}_a or \mathbb{G}_m ($0 \leq i < n$).

Springer 1998, 12.3.5, p.218: A connected solvable k -group [meaning affine group variety] is called k -split if there exists a sequence $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ of closed, connected, normal k -subgroups such that the quotients G_i/G_{i+1} are k -isomorphic to either \mathbb{G}_a or \mathbb{G}_m .

e. The derived group of an algebraic group

Let G be an algebraic group over a field k .

DEFINITION 8.18. The *derived group* of G is the intersection of the normal algebraic subgroups N of G such that G/N is commutative. The derived group of G is denoted $\mathcal{D}G$ (or G' or G^{der} or $[G, G]$).

PROPOSITION 8.19. *The quotient $G/\mathcal{D}G$ is commutative (hence $\mathcal{D}G$ is the smallest normal subgroup with this property).*

PROOF. Because the affine subgroups of G satisfy the descending chain condition (1.28), $\mathcal{D}G = N_1 \cap \dots \cap N_r$ for certain normal affine subgroups N_1, \dots, N_r such that G/N_i is commutative. The canonical homomorphism

$$G \rightarrow G/N_1 \times \dots \times G/N_r$$

has kernel $N_1 \cap \dots \cap N_r$, and so realizes $G/\mathcal{D}G$ as an algebraic subgroup of a commutative algebraic group. \square

We shall need another description of $\mathcal{D}G$, which is analogous to the description of the derived group as the subgroup generated by commutators.

PROPOSITION 8.20. *The derived group $\mathcal{D}G$ is the algebraic subgroup of G generated by the commutator map*

$$(g_1, g_2) \mapsto [g_1, g_2] \stackrel{\text{def}}{=} g_1 g_2 g_1^{-1} g_2^{-1}: G \times G \rightarrow G$$

in each of the two cases (a) G is affine; (b) G is smooth.

PROOF. Let H be the algebraic subgroup of G generated by G^2 and the map $(g_1, g_2) \mapsto [g_1, g_2]$ (2.24, 2.27 et seq.). This means that H is the smallest algebraic subgroup of G containing the image of the commutator map. It follows from this description that it is normal. As $H(R)$ contains all commutators in $G(R)$ (see 2.27), the group $G(R)/H(R)$ is commutative; but the functor $R \mapsto G(R)/H(R)$ is fat in G/H , and so this implies that the algebraic group G/H is commutative. On the other hand, if N is a 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 $H = \mathcal{D}G$. \square

COROLLARY 8.21. *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 each k -algebra R , the group $(\mathcal{D}G)(R)$ consists of the elements of $G(R)$ that lie in $\mathcal{D}(G(R'))$ for some faithfully flat R -algebra R' .*
- (d) *$\mathcal{D}G$ is a characteristic subgroup of G .*

PROOF. (a) Immediate consequence of the proposition.

(b) Apply (2.25; 2.26; 2.29).

(c) Immediate consequence of the proposition.

(d) Clearly $(\mathcal{D}G)(R)$ is preserved by the automorphisms of G . \square

When G is affine, we can make this explicit. Let I_n be the kernel of the homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(G^{2n})$ of k -algebras defined by the regular map (not a homomorphism)

$$(g_1, g_2, \dots, g_{2n}) \mapsto [g_1, g_2] \cdot [g_3, g_4] \cdots: G^{2n} \rightarrow G$$

where $[g_i, g_j] = g_i g_j g_i^{-1} g_j^{-1}$. From the regular maps

$$\begin{aligned} G^2 &\rightarrow G^4 \rightarrow \dots \rightarrow G^{2n} \rightarrow \dots, \\ (g_1, g_2) &\mapsto (g_1, g_2, 1, 1) \mapsto \dots \end{aligned}$$

we get inclusions

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

and we let $I = \bigcap I_n$. Then the coordinate ring of $\mathcal{D}G$ is $\mathcal{O}(G)/I$ (this is a restatement of (8.20) in the affine case).

PROPOSITION 8.22. *Let G be an affine group variety. Then $\mathcal{O}(\mathcal{D}G) = \mathcal{O}(G)/I_n$ for some n , and $(\mathcal{D}G)(k') = \mathcal{D}(G(k'))$ for every separably closed field k' containing k .*

PROOF. We may suppose that G is connected. As G is smooth and connected, so also is G^{2n} (3.13). Therefore, each ideal I_n is prime, and a descending sequence of prime ideals in a noetherian ring terminates (CA 21.6). This proves the first part of the statement.

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 (CA 15.8). 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 $U \cdot U^{-1}$. \square

COROLLARY 8.23. *The derived group $\mathcal{D}G$ of a connected affine group variety G is the unique connected subgroup variety such that $(\mathcal{D}G)(k^{\text{sep}}) = \mathcal{D}(G(k^{\text{sep}}))$.*

PROOF. The derived group has these properties by (8.21) and (8.22), and it is the only algebraic subgroup with these properties because $(\mathcal{D}G)(k^{\text{sep}})$ is dense in $\mathcal{D}G$. \square

EXAMPLE 8.24. Let $G = \text{GL}_n$. Then $\mathcal{D}G = \text{SL}_n$. Certainly, $\mathcal{D}G \subset \text{SL}_n$. Conversely, every element of $\text{SL}_n(k)$ is a commutator ($\text{SL}_n(k)$ is generated by elementary matrices, and every elementary matrix is a commutator if $|k| > 3$).

ASIDE 8.25. For an algebraic group G , the 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 $G = \text{PGL}_n$ over nonperfect separably closed field of characteristic p dividing n .

COMMUTATOR GROUPS

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 $h_2 \in H_2$.

PROPOSITION 8.26. *Let H_1 and H_2 be connected group subvarieties of a connected affine group variety G . Then there is a (unique) connected subgroup variety (H_1, H_2) of G such that $(H_1, H_2)(k^{\text{al}}) = (H_1(k^{\text{al}}), H_2(k^{\text{al}}))$.*

PROOF. Consider the regular map

$$(h_1, h_2, \dots; h'_1, h'_2, \dots) \mapsto [h_1, h'_1][h_2, h'_2] \cdots: H_1^n \times H_2^n \rightarrow G.$$

Let I_n be the kernel of the homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(H_1^n \times H_2^n)$ of k -algebras defined by the map, and let $I = \bigcap I_n$. As before, the subscheme H of G defined by I is a smooth connected algebraic subgroup of G , and $H(k^{\text{al}}) = (H_1(k^{\text{al}}), H_2(k^{\text{al}}))$. \square

REMARK 8.27. Let G be an algebraic group over k which is either affine or smooth.

(a) For each 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) A central series in G (see 8.12) is a chain of algebraic subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

such that $(G, G_i) \subset G_{i+1}$.

SOLVABLE ALGEBRAIC GROUPS

Let G be an algebraic group. Write \mathcal{D}^2G for the second derived group $\mathcal{D}(\mathcal{D}G)$, \mathcal{D}^3G for the third derived group $\mathcal{D}(\mathcal{D}^2G)$ and so on. The *derived series* for G is the normal series

$$G \supset \mathcal{D}G \supset \mathcal{D}^2G \supset \cdots.$$

If G is smooth, then each group \mathcal{D}^nG is smooth and characteristic in G , connected if G is connected, and $\mathcal{D}^nG/\mathcal{D}^{n+1}G$ is commutative.

PROPOSITION 8.28. *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 $G_1 \supset \mathcal{D}G$, $G_2 \supset \mathcal{D}^2G$, and so on. \square

COROLLARY 8.29. *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 (8.21a). Hence one series terminates with e if and only if the other does. \square

COROLLARY 8.30. *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 this property (8.21). \square

In particular, a group variety is solvable if and only if it admits a solvable series of group subvarieties.

f. Nilpotent algebraic groups

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 8.31. *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. \square

COROLLARY 8.32. *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 (8.21). \square

In particular, a group variety is nilpotent if and only if it admits a nilpotent series of group subvarieties.

COROLLARY 8.33. *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. \square

g. Existence of a greatest algebraic subgroup with a given property

Let P be a property of algebraic groups. We assume the following:

- (a) every quotient of a group with property P has property P ;
- (b) every extension of groups with property P has property P .

For example, the property of being connected satisfies (a) and (b) (see 5.52).

LEMMA 8.34. *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 (5.37)

$$\begin{array}{ccccccc} e & \longrightarrow & N & \longrightarrow & HN & \longrightarrow & HN/N & \longrightarrow & e \\ & & & & & & \uparrow \simeq & & \\ & & & & & & H/H \cap N & & \end{array}$$

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 . \square

LEMMA 8.35. *An algebraic group G has at most one maximal normal algebraic subgroup with property P .*

PROOF. Suppose that H and N are both maximal among the normal algebraic subgroups of G with property P . Then HN is also a normal algebraic subgroup with property P (8.34), and so $H = HN = N$. \square

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 the infinite chain of algebraic subgroups

$$e \subset \mu_\ell \subset \mu_{\ell^2} \subset \cdots \subset \mathbb{G}_m$$

shows that \mathbb{G}_m has no greatest finite algebraic subgroup (note that the algebraic groups μ_{ℓ^n} are connected if $\ell = \text{char}(k)$ and smooth if $\ell \neq \text{char}(k)$).

Recall (8.9) that an algebraic group G is strongly connected if it has no nontrivial finite quotient. Clearly quotients and extensions of strongly connected algebraic groups are strongly connected (same argument as in 5.52). Moreover, if H is a normal algebraic subgroup of a strongly connected algebraic group G and $H \neq G$, then $\dim H < \dim G$.

PROPOSITION 8.36. *Every algebraic group G contains a greatest strongly connected normal algebraic subgroup H with property P . The quotient G/H contains no strongly connected normal algebraic subgroup with property P except e .*

PROOF. The trivial algebraic subgroup e is strongly connected, normal, and has property P . Any strongly connected normal algebraic subgroup H of greatest dimension among those with property P is maximal. According to (8.35) H contains all other strongly connected algebraic subgroups with property P . If G/H contained strongly connected normal algebraic subgroup $H' \neq e$ with property P , then the inverse image of H' in G would properly contain H and would violate the maximality of H . \square

For example, every algebraic group contains a greatest strongly connected finite algebraic subgroup, namely e .

Caution: it is not clear that being strongly connected is preserved by extension of the base field.

COROLLARY 8.37. *Every algebraic group G contains a greatest smooth connected normal algebraic subgroup H with property P . The quotient G/H contains no connected normal group subvariety with property P except e .*

PROOF. Apply (8.36) with “ P ” replaced by “ P and smooth”, and note that connected smooth algebraic groups are strongly connected. Alternatively, prove it by the same argument as (8.36). \square

SUMMARY 8.38. Let P be a property of algebraic groups over k such that quotients and extensions of algebraic groups with property P have property P . Let G be an algebraic group over k . Among the smooth connected normal algebraic subgroups of G with property P there is a greatest one H ; the quotient G/H contains no smooth connected normal algebraic subgroups with property P except e .

Let P be a property of group varieties over k such that quotients and extensions of algebraic groups with property P have property P . Let G be a group variety over k . Among the connected normal subgroup varieties of G with property P , there is a greatest one H ; the quotient G/H contains no connected normal subgroup variety with property P except e .

h. Semisimple and reductive groups

8.39. Let G be a connected group variety over k . Extensions and quotients of solvable algebraic groups are solvable (8.13), and so G contains a greatest connected solvable normal subgroup variety. 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 $G_{k^{\text{al}}}$ is semisimple, i.e., if its **geometric radical** $R(G_{k^{\text{al}}})$ is trivial. If k is algebraically closed, then $G/R(G)$ is semisimple. If G over k is semisimple, then $G_{k'}$ over k' is reductive for k' a field containing k .

8.40. An algebraic group G is said to be **unipotent** if every nonzero representation of G has a nonzero fixed vector. Let Q be a quotient of unipotent group G . A nonzero representation of Q can be regarded a representation of G , and so has a nonzero fixed vector. Therefore Q is unipotent. Let G be an extension of unipotent groups Q and N ,

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e,$$

and let V be a representation of G . The subspace V^N of V is stable under G because N is normal (5.24), and G acts on it through the quotient Q . Now

$$V \neq 0 \implies V^N \neq 0 \implies V^G = (V^N)^Q \neq 0.$$

This shows that G is unipotent. Thus “unipotent” satisfies the conditions (a) and (b) of the preceding section.

8.41. It follows from (8.40) that every connected group variety contains a greatest connected unipotent normal subgroup variety. 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 $G_{k^{\text{al}}}$ is reductive, i.e., if its **geometric unipotent radical** $R_u(G_{k^{\text{al}}})$ is trivial. If k is algebraically closed, then $G/R_u(G)$ is reductive. If G over k is reductive, then $G_{k'}$ over k' is reductive for all fields k' containing k .

8.42. A connected group variety G is **k -reductive** (or **pseudo-reductive**) if $R_u(G) = e$. Every reductive group is k -reductive, but a k -reductive group need not be reductive (see the next example). In particular, a group variety G over k may be k -reductive without $G_{k'}$ being k' -reductive for k' a field containing k .

EXAMPLE 8.43. Let k be a field of characteristic p , and let $a \in k \setminus k^p$. Let G be the algebraic group over k

$$R \rightsquigarrow \{(x, y) \in R^2 \mid x^p - ay^p \in R^\times\}$$

with the multiplication

$$(x, y)(x', y') = (xx' + ay'y', xy' + x'y).$$

Then $\mathcal{O}(G) = k[X, Y, Z]/((X^p - aY^p)Z - 1)$, and G is a connected group variety (the polynomial $(X^p - aY^p)Z - 1$ is irreducible). Let $\varphi: G \rightarrow \mathbb{G}_m$ be the homomorphism

$$(x, y) \mapsto x^p - ay^p.$$

The kernel N of φ is the algebraic group defined by $X^p - aY^p = 0$, which is not reduced. We have $R_u(G) = e$, but $R_u(G_{k^{\text{al}}}) = N_{\text{red}} \simeq \mathbb{G}_a$. Thus G is not reductive.

ASIDE 8.44. According to our principle that everything concerning an algebraic group G over a field k should be intrinsic to G over k , “ k -reductive” and “reductive” should be “reductive” and “geometrically reductive”, but we have chosen to follow tradition. Reductive groups form a very important class over any field. However, questions concerning general algebraic groups over nonperfect fields, often can be reduced only to questions concerning pseudo-reductive (not reductive) groups, because in general $G/R_u(G)$ is only pseudo-reductive. Therefore pseudo-reductive groups also form an important class. Their study leads to significant problems that have only recently been resolved (Conrad et al. 2010). Happily, over perfect fields, the two notions coincide.

ASIDE 8.45. For (8.43), see Springer 1998, 12.1.6. Springer defines the unipotent radical of G to be that of $G_{k^{\text{al}}}$, and notes that in this example it is “not defined over the ground field” (ibid. p.222). 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 ours (ibid. p.251).

i. A standard example

The next example will play a fundamental role in the rest of the text.

8.46. Fix an $n \in \mathbb{N}$. We number the pairs (i, j) , $1 \leq i < j \leq n$, as follows:

$$\begin{array}{cccccccc} (1, 2) & (2, 3) & \cdots & (n-1, n) & (1, 3) & \cdots & (n-2, n) & \cdots & (1, n) \\ C_1 & C_2 & & C_{n-1} & C_n & & C_{2n-3} & & C_{\frac{n(n-1)}{2}}. \end{array}$$

For $r = 0, \dots, m = \frac{n(n-1)}{2}$, let $U_n^{(r)}$ and $P_n^{(r)}$ denote the algebraic subgroups of \mathbb{U}_n such that

$$\begin{aligned} U_n^{(r)}(R) &= \{(a_{ij}) \in \mathbb{U}_n(R) \mid a_{ij} = 0 \text{ for } (i, j) = C_l, l \leq r\} \\ P_n^{(r)}(R) &= \{(a_{ij}) \in \mathbb{U}_n(R) \mid a_{ij} = 0 \text{ for } (i, j) = C_l, l \neq r\} \end{aligned}$$

for all k -algebras R . In particular, $U_n^{(0)} = \mathbb{U}_n$. For example, when $n = 3$,

$$\begin{aligned} C_1 = (1, 2), \quad U_3^{(1)} &= \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad P_3^{(1)} = \left\{ \begin{pmatrix} 1 & * & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \simeq U_3^{(0)} / U_3^{(1)} \\ C_2 = (2, 3), \quad U_3^{(2)} &= \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad P_3^{(2)} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \simeq U_3^{(1)} / U_3^{(2)} \\ C_3 = (1, 3), \quad U_3^{(3)} &= \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad P_3^{(3)} = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \simeq U_3^{(2)} / U_3^{(3)}. \end{aligned}$$

Then:

(a) Each $U_n^{(r)}$ is a normal algebraic subgroup of \mathbb{T}_n , and

$$\mathbb{U}_n = U_n^{(0)} \supset \cdots \supset U_n^{(r)} \supset U_n^{(r+1)} \supset \cdots \supset U_n^{(m)} = e. \quad (44)$$

(b) For $r > 0$, the maps

$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{p_r} & P_n^{(r)} & \longrightarrow & U_n^{(r-1)} / U_n^{(r)} \\ c & \mapsto & 1 + cE_{i_0 j_0} & \mapsto & (1 + cE_{i_0, j_0}) \cdot U_n^{(r)}, \end{array}$$

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 $r > 0$,

$$A \cdot (1 + cE_{i_0 j_0}) \cdot A^{-1} \equiv 1 + \begin{pmatrix} a_{ii} \\ a_{jj} \end{pmatrix} c E_{i_0 j_0} \pmod{U_n^r(R)}$$

where $A = (a_{ij}) \in \mathbb{T}_n(R)$, $c \in \mathbb{G}_a(R) = R$, and $(i_0, j_0) = C_r$.

Therefore

$$\mathbb{T}_n \supset U_n^{(0)} \supset \cdots \supset U_n^{(r)} \supset U_n^{(r+1)} \supset \cdots \supset U_n^{(m)} = e \quad (45)$$

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, (45) is a solvable series for \mathbb{T}_n and (44) 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.

Algebraic groups acting on schemes

All schemes are algebraic over k . Algebraic groups are not required to be affine. By a functor (resp. group functor) we mean a functor from Alg_k^0 to Set (resp. Grp). The Yoneda lemma (A.28) allows us to identify an algebraic scheme X with the functor \tilde{X} it defines. For a functor X and k -algebra R , we let X_R denote the functor of small R -algebras defined by X . For functors X, Y , we let $\underline{\text{Hom}}(X, Y)$ denote the functor $R \mapsto \text{Hom}(X_R, Y_R)$. For a closed subset Z of an algebraic scheme X , we let Z_{red} denote the reduced subscheme of X with $|Z_{\text{red}}| = Z$; for a locally closed subset Z , we let Z_{red} denote the open subscheme of $(\bar{Z})_{\text{red}}$ with $|Z_{\text{red}}| = Z$.

a. Group actions

Recall (§1f) that an action of a group functor G on a functor X is a natural transformation $\mu: G \times X \rightarrow X$ such that $\mu(R)$ is an action of $G(R)$ on $X(R)$ for all k -algebras R , and that an action of an algebraic group G on an algebraic scheme X is a regular map

$$\mu: G \times X \rightarrow X$$

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 $\mu(g, x)$.

Let $\mu: G \times X \rightarrow X$ be an action of an algebraic group G on an algebraic scheme X . The following diagram commutes

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

and both horizontal maps are isomorphisms. It suffices to check this on the R -points (R a small k -algebra), where it is obvious (the inverse of the top map is $(g, x) \mapsto (g, g^{-1}x)$). Therefore, the map $\mu: G \times X \rightarrow X$ is isomorphic to the projection map p_2 . It follows that μ is faithfully flat, and that it is smooth (resp. finite) if G is smooth (resp. finite).

b. The fixed subscheme

THEOREM 9.1. *Let $\mu: G \times X \rightarrow X$ be an action of a group functor G on an algebraic scheme X . If X is separated, then the functor 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 of X .

PROOF. We regard G and X as functors. An $x \in X(R)$ defines maps

$$\begin{aligned} g &\mapsto gx_{R'}: G(R') \rightarrow X(R') \\ g &\mapsto x_{R'}: G(R') \rightarrow X(R'), \end{aligned}$$

natural in the R -algebra R' . Thus, we get two maps

$$X(R) \rightarrow \underline{\mathrm{Hom}}(G_R, X_R),$$

natural in R . These are the components of the map γ in the following diagram:

$$\begin{array}{ccccc} X & \xrightarrow{\gamma} & \underline{\mathrm{Hom}}(G, X) \times \underline{\mathrm{Hom}}(G, X) & \xrightarrow{\simeq} & \underline{\mathrm{Hom}}(G, X \times X) \\ \uparrow & & \uparrow \alpha \mapsto (\alpha, \alpha) & & \uparrow \alpha \mapsto \Delta_X \circ \alpha \\ X^G & \longrightarrow & \underline{\mathrm{Hom}}(G, X) & \xrightarrow[\simeq]{\mathrm{id}} & \underline{\mathrm{Hom}}(G, X). \end{array}$$

The remaining maps are obvious. The diagram is commutative, and each square is cartesian, because it becomes so when each functor is evaluated at a k -algebra R . As X is separated, Δ_X is a closed immersion, and so $\underline{\mathrm{Hom}}(G, X)$ is a closed subfunctor of $\underline{\mathrm{Hom}}(G, X \times X)$ (1.82). Therefore X^G is a closed subfunctor of X (1.78), which implies that the functor X^G is represented by a closed subscheme of X (1.77). \square

It is obvious from its definition that the formation of X^G commutes with extension of the base field.

9.2. Let $\mu: G \times X \rightarrow X$ be an action of a group variety G on an algebraic variety X over a field k . When k is algebraically closed,

$$(X^G)_{\mathrm{red}} = \bigcap_{g \in G(k)} X^g,$$

where X^g is the closed subvariety of X on which the regular map $x \mapsto \mu(g, x)$ agrees with the identity map. When k is perfect, $(X^G)_{\mathrm{red}}$ is the unique closed subvariety of X such that

$$(X^G)_{\mathrm{red}}(k^{\mathrm{al}}) = \{x \in X(k^{\mathrm{al}}) \mid gx = x \text{ for all } g \in G(k^{\mathrm{al}})\}.$$

PROPOSITION 9.3. *Let $\mu: G \times X \rightarrow X$ be an action of an algebraic group G on a separated scheme X . For every k -algebra R , $X^G(R)$ consists of the elements x of $X(R)$ such that*

$$\mu(g_{S \otimes R}, x_{S \otimes R}) = x_{S \otimes R} \tag{46}$$

for all k -algebras S and $g \in G(S)$.

In other words, it is not necessary to require that $\mu(g, x_{R'}) = x_{R'}$ hold for all R -algebras R' and $g \in G(R')$, but only that it hold for R -algebras of the form $S \otimes R$ and g of the form $g_{S \otimes R}$, $g \in G(S)$.

PROOF. Let $x \in X(R)$ satisfy the condition in the proposition, and let $g \in G(R')$ for some R -algebra R' . Let S be the k -algebra underlying R' . We have a commutative diagram

$$\begin{array}{ccccc} S & \xrightarrow{\varphi} & R \otimes S & \xleftarrow{\lambda} & R \\ & \searrow \text{id} & \downarrow \psi & \swarrow & \\ & & R' & & \end{array}$$

where

$$\varphi(s) = 1 \otimes s \quad \lambda(r) = r \otimes 1 \quad \psi(r \otimes s) = rs.$$

Therefore,

$$\begin{aligned} g &= G(\psi)G(\varphi)(g) = G(\psi)(g_{R \otimes S}) \\ x_{R'} &= X(\psi)X(\lambda)(x) = X(\psi)(x_{R \otimes S}) \end{aligned}$$

and so

$$\mu(g, x_{R'}) = X(\psi)(\mu(g_{S \otimes R}, x_{S \otimes R})).$$

But

$$X(\psi)(\mu(g_{S \otimes R}, x_{S \otimes R})) \stackrel{(46)}{=} X(\psi)(x_{R \otimes S}) = x_{R'},$$

and so $g \cdot x_{R'} = x_{R'}$, as required. □

c. Orbits and isotropy groups

Let k be algebraically closed. In the action,

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

there are two orbits, namely, $\{(0, 0)\}$ and its complement. The smaller of these is closed, but the larger isn't even affine. Now consider a group variety G acting on a variety X . The orbit O of $x \in X$ is the image of the regular map $g \mapsto gx: G \rightarrow X$, and so it contains a dense open subset U of its closure \bar{O} (A.59). But O is a union of the sets gU , $g \in G$, and so is itself open in \bar{O} . Therefore $\bar{O} \setminus O$ is closed of dimension $< \dim \bar{O}$, and so it is a union of orbits of dimension $< \dim O$. It follows that every orbit of lowest dimension in X is closed.

We extend this discussion to algebraic groups acting on schemes.

Let $\mu: G \times X \rightarrow X$ be an action of an algebraic group G on an algebraic scheme X , and let $x \in X(k)$. The **orbit map**

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

is defined to be the restriction of μ to $G \times \{x\} \simeq G$. We say that G acts **transitively** on X if $G(k^{\mathrm{al}})$ acts transitively on $X(k^{\mathrm{al}})$. Then the orbit map μ_x is surjective for all $x \in X(k)$ (because it is on k^{al} -points).

We repeat Proposition 1.52 for reference.

PROPOSITION 9.4. *Let G be an algebraic group. Let X and Y be nonempty algebraic schemes on which G acts, and let $f: X \rightarrow Y$ be an equivariant map.*

- (a) *If Y is reduced and $G(k^{\mathrm{al}})$ acts transitively on $Y(k^{\mathrm{al}})$, then f is faithfully flat.*
- (b) *If $G(k^{\mathrm{al}})$ acts transitively on $X(k^{\mathrm{al}})$, then $f(X)$ is a locally closed subset of Y .*

(c) If X is reduced and $G(k^{\text{al}})$ acts transitively on $X(k^{\text{al}})$, 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 .

DEFINITION 9.5. Let $\mu: G \times X \rightarrow X$ be an action of an algebraic group on a nonempty algebraic scheme X over k , and let $x \in X(k)$. Then (9.4b) applied to the orbit map $\mu_x: G \rightarrow X$ shows that the set $\mu_x(G)$ is locally closed in X . The **orbit** O_x of x is defined to be $\mu_x(G)_{\text{red}}$.

EXAMPLE 9.6. 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 9.7. Let $\mu: G \times X \rightarrow X$ be an action of a algebraic group G on an algebraic scheme X , and let $x \in X(k)$. If G is reduced, then O_x is stable under G and the orbit map $\mu_x: G \rightarrow O_x$ is faithfully flat; hence O_x is smooth if G is smooth.

PROOF. The first statement follows from (9.4c) applied to $f = \mu_x$. As μ_k is faithfully flat, the map $\mathcal{O}_{O_x} \rightarrow \mu_{x*}(\mathcal{O}_G)$ is injective, and remains so after extension of the base field. Therefore O_x is geometrically reduced, and so it has nonempty smooth locus (A.52). By homogeneity (over k^{al}), it equals O_x . \square

PROPOSITION 9.8. Let $\mu: G \times X \rightarrow X$ 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 $Y(k^{\text{al}})$ is stable under $G(k^{\text{al}})$.
- (b) Let Y be a subscheme of X . If Y is stable under G , then $|\bar{Y}|_{\text{red}}$ and $(|\bar{Y}| \setminus |Y|)_{\text{red}}$ are stable under G .

PROOF. (a) As G is geometrically reduced and Y is reduced, $G \times Y$ is reduced (A.39). It follows that $\mu: G \times Y \rightarrow X$ factors through Y if and only if $\mu(k^{\text{al}})$ factors through $Y(k^{\text{al}})$.

(b) When we identify $X(k^{\text{al}})$ with $|X_{k^{\text{al}}}|$, the set $|\bar{Y}|_{\text{red}}(k^{\text{al}})$ becomes identified with the closure of $Y(k^{\text{al}})$ in $X(k^{\text{al}})$. As $G(k^{\text{al}})$ acts continuously on $X(k^{\text{al}})$ and stabilizes $Y(k^{\text{al}})$, it stabilizes the closure of $Y(k^{\text{al}})$. Now (a) shows that $|\bar{Y}|_{\text{red}}$ is stable under the action of G . A similar argument applies to $(|\bar{Y}| \setminus |Y|)_{\text{red}}$. \square

Now assume that X is separated. For $x \in X(k)$, we define G_x to be the fibred product:

$$\begin{array}{ccc} G_x & \longrightarrow & X \\ \downarrow & & \downarrow \Delta_X \\ G & \xrightarrow{g \mapsto (x, gx)} & X \times X \end{array}$$

It is a closed subscheme of G , and, for all k -algebras R ,

$$G_x(R) = \{g \in G(R) \mid gx_R = x_R\},$$

which is a subgroup of $G(R)$. Therefore G_x is an algebraic subgroup of G — it is called the **isotropy group** at x .

PROPOSITION 9.9. *Let G be a smooth algebraic group acting on an algebraic scheme X , and let Y have the smallest dimension among the nonempty subschemes of X stable under G . Then Y is closed.*

PROOF. Let Y be a nonempty stable subscheme of X . Then $(|\bar{Y}| \setminus |Y|)_{\text{red}}$ is stable under G (9.8), and

$$\dim(Y) > \dim(|\bar{Y}| \setminus |Y|)_{\text{red}}.$$

If Y has smallest possible dimension, then $|\bar{Y}| = |Y|$. □

COROLLARY 9.10. *Let G be a smooth algebraic group acting on a nonempty algebraic scheme X over an algebraically closed field k . Then there exists an $x \in X$ such that O_x is closed.*

PROOF. Let Y be a nonempty stable subscheme of X of smallest dimension. Let $x \in Y$. Then O_x is a stable subscheme of Y , and so $O_x = Y_{\text{red}}$. □

ASIDE 9.11. The algebraicity in (9.10) is essential: a complex Lie group acting on a complex variety need not have closed orbits (Springer 1998, p.41).

DEFINITION 9.12. A nonempty algebraic scheme X with an action of G is a **homogeneous scheme** for G if $G(k^{\text{al}})$ acts transitively on $X(k^{\text{al}})$ and the orbit map $\mu_x: G_{k^{\text{al}}} \rightarrow X_{k^{\text{al}}}$ for some $x \in X(k^{\text{al}})$. (The orbit map μ_x is then faithfully flat for all $x \in X(k^{\text{al}})$.)

One can ask whether every algebraic G -scheme X over k is a union of homogeneous subschemes. A necessary condition for this is that the k^{al} -points of X over a single point of X lie in a single orbit of $G_{k^{\text{al}}}$. 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 9-1.

NOTES. This section follows DG, II, §5, no. 3, p.242.

d. The functor defined by projective space

9.13. 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 N (a complement of M) such that $N = M \oplus M'$. Let M be 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 12.5). 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 (ibid.), and so M is (globally) a direct summand of R^{n+1} .

9.14. Let

$$P^n(R) = \{\text{direct summands of rank 1 of } R^{n+1}\}.$$

Then P^n is a functor $\text{Alg}_k \rightarrow \text{Set}$. One can show that the functor P^n is local in the sense of (A.29).

9.15. Let H_i be the hyperplane $T_i = 0$ in k^{n+1} , and let

$$P_i^n(R) = \{L \in P^n(R) \mid L \oplus H_i R = R^{n+1}\}.$$

The P_i^n form an open affine cover of P^n , and so P^n is an algebraic scheme over k (A.29). We denote it by \mathbb{P}^n .

9.16. When K is a field, every K -subspace of K^{n+1} is a direct summand, and so $\mathbb{P}^n(K)$ consists of the lines through the origin in K^{n+1} .

e. Quotients: definition and properties

DEFINITION 9.17. Let G be an algebraic group (not necessarily affine) over k , and let H be an algebraic subgroup of G . A separated algebraic scheme X equipped with an action $\mu: G \times X \rightarrow X$ of G and a point $o \in X(k)$ is called the **quotient** of G by H if the map $g \mapsto go: G(R) \rightarrow X(R)$ realizes \tilde{G}/\tilde{H} as a fat subfunctor of \tilde{X} , i.e., if $\tilde{X} = \tilde{G}/\tilde{H}$. Explicitly, this means that, for every (small) k -algebra R ,

- (a) the nonempty fibres of the map $g \mapsto go: G(R) \rightarrow X(R)$ are 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 Chapter 7 we proved that quotients always exist, but we won't assume that here.

PROPOSITION 9.18. *Let (X, o) be a quotient of G by H (assumed to exist). For every G -scheme X' and point $o' \in X'(k)$ fixed by H , there is a unique G -equivariant map $X \rightarrow X'$ sending o to o' .*

PROOF. There is a unique G -equivariant map of functors $\tilde{G}/\tilde{H} \rightarrow \tilde{X}'$ sending the coset of H to o' . Because \tilde{X}' is a sheaf, this extends uniquely to a map of sheaves $\tilde{X} \rightarrow \tilde{X}'$ (5.4). According to the Yoneda lemma, this map arises from a unique map $X \rightarrow X'$ having the required properties. \square

Thus, a quotient of G by H (if it exists) is uniquely determined up to a unique isomorphism. We write G/H for the quotient of G by H (if it exists). Note that $(G/H)(k^{\text{al}}) = G(k^{\text{al}})/H(k^{\text{al}})$.

LEMMA 9.19. *Let H be an algebraic subgroup of an algebraic group G , and assume that G/H exists. Then*

$$(g, h) \mapsto (g, gh): G \times H \rightarrow G \times_{G/H} G$$

is an isomorphism.

PROOF. For all k -algebras R , the map

$$(g, h) \mapsto (g, gh): G(R) \times H(R) \rightarrow G(R) \times_{G(R)/H(R)} G(R)$$

is a bijection. As $G(R)/H(R)$ injects into $(G/H)(R)$, this remains true with the first set replaced by the second; hence $G \times H \simeq G \times_{G/H} G$. \square

PROPOSITION 9.20. *Let H be an algebraic subgroup of an algebraic group G , and assume that the quotient G/H exists. Then the canonical map $q: G \rightarrow G/H$ is faithfully flat (hence open). It follows that G/H is smooth if G is.*

PROOF. According to (9.19), the projection map $p_1: G \times_{G/H} G \rightarrow G$ differs by an isomorphism from the projection map $G \times H \rightarrow G$, and so is faithfully flat. This implies that the map $G \rightarrow G/H$ is faithfully flat (A.89), and hence open (A.87).

Because q is faithfully flat, the map $\mathcal{O}_{G/H} \rightarrow q_*\mathcal{O}_G$ is injective, and remains injective 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^{al}). \square

REMARK 9.21. Let G be an algebraic group over k . A (right) G -torsor over k is a nonempty algebraic scheme X over k together with an action $X \times G \rightarrow X$ of G on X such that the map $(x, g) \mapsto (x, xg): X \times G \rightarrow X \times X$ is an isomorphism. Then, for each k -algebra R , the set $X(R)$ is either empty or a principal homogeneous space for $G(R)$. More generally, a G -torsor over an algebraic k -scheme S is a faithfully flat map $X \rightarrow S$ together with an action¹ $X \times G \rightarrow X$ of G on X over S such that the map $(x, g) \mapsto (x, xg): X \times G \rightarrow X \times_S X$ is an isomorphism. Lemma 9.19 and Proposition 9.20 show that G is an H -torsor over G/H .

PROPOSITION 9.22. *Let $G \times X \rightarrow X$ 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 $\mu_o: G \rightarrow X$ is faithfully flat.*

PROOF. If (X, o) is the quotient of G by G_o , then μ_o is faithfully flat by (9.20). 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 (9.17a) is satisfied. If μ_o is faithfully flat, then (5.6) shows that the condition (9.17b) is satisfied. \square

PROPOSITION 9.23. *Let $G \times X \rightarrow X$ 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 $G/G_o \rightarrow O_o$.*

PROOF. Because G is reduced, the orbit map μ_o is faithfully flat (9.7). Hence we can apply (9.22). \square

COROLLARY 9.24. *Let $G \times X \rightarrow X$ 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 $G/G_o \rightarrow O_o$.*

PROOF. Special case of the proposition. \square

REMARK 9.25. The algebraic subgroup G_o in (9.24) need not be smooth — consider, for example, the action in characteristic p of SL_p on PGL_p by left translation. If k is perfect, then $(G_o)_{\mathrm{red}}$ is an group subvariety of G , and $G/(G_o)_{\mathrm{red}} \rightarrow O_o$ is a finite purely inseparable map. This is the best that one can do in the world of algebraic varieties.

PROPOSITION 9.26. *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 $\bar{q}: G/H \rightarrow G/H'$ is faithfully flat. If the scheme H'/H is smooth (resp. finite) over k , then the morphism $G/H' \rightarrow G/H$ is smooth (resp. finite and flat). In particular, the map $G \rightarrow G/H$ is smooth (resp. finite and flat) if H is smooth (resp. finite).

PROOF. We have a cartesian square of functors

$$\begin{array}{ccc} \tilde{G} \times (\tilde{H}'/\tilde{H}) & \xrightarrow{(g,x) \mapsto gx} & \tilde{G}/\tilde{H} \\ \downarrow (g,x) \mapsto g & & \downarrow \\ \tilde{G} & \xrightarrow{q'} & \tilde{G}/\tilde{H}'. \end{array}$$

¹By this we mean an action $X \times G \simeq X \times_S G_S \rightarrow X$ of G_S on X over S .

On passing to the associated sheaves and applying the Yoneda lemma, we get a cartesian square of algebraic schemes

$$\begin{array}{ccc} G \times (H'/H) & \xrightarrow{\mu} & G/H \\ \downarrow p_1 & & \downarrow \bar{q} \\ G & \xrightarrow{q'} & G/H'. \end{array}$$

Because q' is faithfully flat, whatever properties p_1 has, so will \bar{q} (see A.90). \square

f. Quotients: construction in the affine case

In Chapter 7 we proved the existence of G/H in the general case. Here we give a direct explicit construction of G/H when G is affine (and smooth).

LEMMA 9.27. *Let $G \times X \rightarrow X$ 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 $G/G_o \rightarrow X$ is an immersion.*

PROOF. As G is smooth, the map $\mu_o: G \rightarrow O_o$ is faithfully flat and O_o is stable under G (9.7, 9.5), and so the pair (O_o, o) is a quotient of G by G_o by (9.22).

That $G/G_o \rightarrow X$ is an immersion follows from (9.4c). \square

THEOREM 9.28. *The quotient G/H exists as a separated algebraic scheme for every smooth affine algebraic group G and algebraic subgroup H .*

PROOF. According to Chevalley's theorem (4.19), 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 , $H = G_L$ where L is considered as a point of $\mathbb{P}^n(k)$. Now Lemma 9.27 completes the proof. \square

EXAMPLE 9.29. The proof of Theorem 9.28 shows that, for every representation (V, r) of G and line L in $\mathbb{P}(V)$ is a quotient of G by the stabilizer of L in G . For example, let $G = \text{GL}_2$ and let $H = \mathbb{T}_2 = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$. Then H is the subgroup fixing the line $L = \left\{ \begin{pmatrix} * \\ 0 \end{pmatrix} \right\}$ 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.²

PROOF IN THE NONSMOOTH CASE

[This is not of much interest — the important case for the rest of the book is the smooth affine case, and the general case is proved in Chapter 7. However, it may be possible to give an easy deduction of the general affine case from the smooth affine case using only the elementary result (7.18).]

To remove the “smooth” from Theorem 9.28, it suffices to remove the “smooth” from Lemma 9.27.

²In Chapter 18, we shall study the subgroups H such that G/H is complete (they are the parabolic subgroups).

LEMMA 9.30. *Let $G \times X \rightarrow X$ 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 $G/G_o \rightarrow X$ is an immersion.*

PROOF. When G is smooth, this was proved above. Otherwise, there exists a finite purely inseparable extension k' of k and a smooth algebraic subgroup G' of $G_{k'}$ such that $G'_{k^{\text{al}}} = (G_{k^{\text{al}}})_{\text{red}}$ (see 1.46). 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 (9.34) below. Therefore G/H exists because $(G/H)_{k'} \simeq G_{k'}/H_{k'}$ exists and we can apply (9.31) below.

In proving that $i: G/G_o \rightarrow X$ 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 $U \rightarrow X$ is an immersion (A.31). Now the open sets $i^{-1}(gU) = gi^{-1}(U)$, $g \in G(k)$, cover G/G_o . \square

Proofs of the following results will (probably not) be added.

LEMMA 9.31. *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. DG III, 2, 7.4, p321. In the affine case, which is all we need, this follows from the elementary result (7.18). \square

LEMMA 9.32. *Let S be an algebraic scheme and let $R \rightrightarrows S$ be an equivalence relation on S such that the first projection $R \rightarrow S$ 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. DG III, 2, 7.1, 7.2, p.318. \square

LEMMA 9.33. *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 $R_0 \rightarrow S$ and $R \rightarrow S$ are flat. If S/R_0 is an algebraic scheme over k , then so also is G/R .*

PROOF. DG III, 2, 7.3, p320. \square

LEMMA 9.34. *Let G be an algebraic group, and let G_0 , H , and H_0 be 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 9.32). Hence G/H exists by (9.33) 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 with only a singly point, which is therefore affine. \square

g. Linear actions

DEFINITION 9.35. An action $G \times X \rightarrow X$ of an algebraic group G on an algebraic variety X is said to be **linear** if there exists a representation $r: G \rightarrow \mathrm{GL}_V$ of G on a finite-dimensional vector space V and a G -equivariant immersion $X \hookrightarrow \mathbb{P}(V)$.

PROPOSITION 9.36. *If G is affine, X is an algebraic variety, and the action is transitive, then the action is linear.*

PROOF. Let $o \in X$. Then the orbit map $\mu_o: G/G_o \rightarrow X$ is an immersion (9.27). As X is reduced and the action is transitive, the orbit map is an isomorphism. The proof of (9.28) shows that the action of G on G/G_o is linear. \square

REMARK 9.37. In the situation of (9.36), 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**.

ASIDE 9.38. There is the following theorem of Sumihiro (1974, 1975): Let $G \times X \rightarrow X$ be an action of a connected affine group variety G on a normal algebraic variety X an algebraically closed field, and let O be an orbit of G in X . Then there exists an open neighbourhood U of O on which G acts linearly. The hypothesis of normality is essential. (See also Slodowy, LNM 815, I, 1.3.)

h. Complements

In this section, G is an algebraic group and H is an algebraic group. We assume that G/H exists.

9.39. When G is affine, the algebraic scheme G/H is quasiprojective. This follows from its construction. (In fact, homogeneous spaces of group varieties are always quasi-projective; Chow 1957. More generally, let G a group scheme smooth over a normal scheme S with connected fibres. Then every homogeneous space under G is locally quasi-projective on S . (Raynaud 1970, LNM 119).)

9.40. We have,

$$\dim G = \dim H + \dim G/H.$$

It suffices to prove this with k algebraically closed. Then we may pass to the associated reduced algebraic varieties, and apply a little algebraic geometry (specifically A.99).

9.41. 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 .

9.42. Let H' be an algebraic subgroup of G containing H and such that $\dim H' = \dim H$. Then $\dim(H'/H) = 0$ (9.40), and so H'/H is finite (2.12). Therefore the canonical map $G/H \rightarrow G/H'$ is finite and flat (9.26). In particular, it is proper.

9.43. Consider an algebraic group G acting on an algebraic variety X . Assume that $G(k^{\mathrm{al}})$ acts transitively on $X(k^{\mathrm{al}})$. By homogeneity, X is smooth, and, for any $o \in X(k)$, the map $g \mapsto go: G \rightarrow X$ defines an isomorphism $G/G_o \rightarrow X$. When k is perfect, $(G_o)_{\mathrm{red}}$ is a smooth algebraic subgroup of G (1.25), and $G/(G_o)_{\mathrm{red}} \rightarrow X$ is finite and purely inseparable (9.42).

9.44. Let $G \supset H$ be group varieties, and let o be the canonical point in $(G/H)(k)$. Then G/H is an algebraic variety (9.20), and the map $G \rightarrow G/H$ has the following universal property: for any algebraic variety X with an action of G and point o' of $X(k)$ fixed by H , there is a unique regular map $G/H \rightarrow X$, $go \mapsto go'$ making the following diagram commute:

$$\begin{array}{ccc} G & \xrightarrow{g \mapsto go} & G/H \\ & \searrow^{g \mapsto go'} & \downarrow \text{---} \\ & & X'. \end{array}$$

9.45. When G is affine and H is normal, the quotient G/H constructed in (5.21) satisfies the definition (9.17) — see (5.30). Therefore G/H is affine in this case.

ASIDE 9.46. The quotient G/H may be affine without H being normal. When G is reductive, Matsushima’s criterion says that G/H is affine if and only if H° is reductive (Matsushima 1960 in characteristic zero; Richardson 1977, Borel 1985 in all characteristics). For more general G , see Cline et al. 1977, Koitabashi 1989, etc.

ASIDE 9.47. For a discussion of what happens to the orbits when you change the algebraically closed base field and the group is semisimple, see mo49885.

i. Flag varieties

A **flag** F in finite-dimensional vector space V is a sequence of distinct subspaces $0 = V_0 \subset V_1 \subset \dots \subset V_r = V$ 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

$$0 = F_0 \subset F_1 \subset \dots \subset F_r = R \otimes V$$

with F_i a direct factor of $R \otimes V$ of rank $\dim(V_i)$.

PROPOSITION 9.48. 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 $GL_V / B(F)$ represents the functor $\mathcal{B}(F)$.

PROOF. The functor $R \mapsto GL_V(R) / B(F)(R)$ is a fat subfunctor of both $\mathcal{B}(F)$ and $R \mapsto (GL_V / B(F))(R)$. □

A variety of the form $GL_V / B(F)$ is called a **flag variety**. They are complete varieties (see 18.21 below, or prove directly).

j. Exercises

EXERCISE 9-1. Let G be a smooth connected algebraic group acting on algebraic variety X .

(a) Show that a point x of X lies in a homogeneous subscheme of X if $\kappa(x)$ is separable over k and the k^{al} -points of X over x lie in a single $G_{k^{\text{al}}}$ -orbit.

(b) Show that (a) fails if the k^{al} -points of X over x don’t lie in a single orbit (e.g., if G is the trivial group).

(c) Show that (a) fails 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) fails without the separability condition. (Let $G = \{(u, v) \mid v^p = u - tu^p\}$, $t \in k \setminus k^p$. 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 $X \setminus \{x\} = G$ with G acting by translation, and so it is a homogeneous space for G , but the complement $\{x\}$ of $X \setminus \{x\}$ in X is not a homogeneous space — it is not even smooth.)

See [mo150207 \(user76758\)](#).

EXERCISE 9-2. Let G be a group variety acting transitively on irreducible varieties X and Y , and let $f: X \rightarrow Y$ be an equivariant quasi-finite regular dominant map. Then f is finite (hence proper). (AG, Exercise 9-4.)

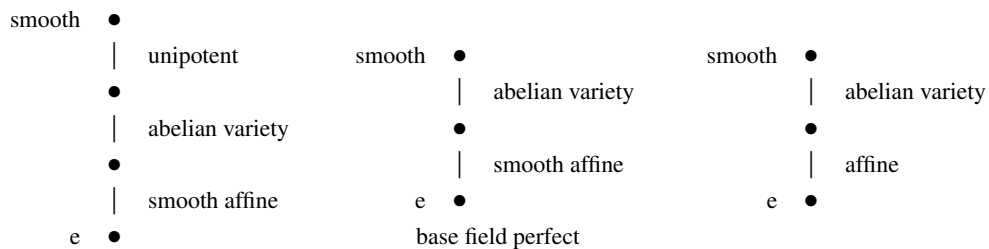
The structure of general algebraic groups

In this chapter, we explain the position that affine algebraic groups occupy within the category of all algebraic groups.

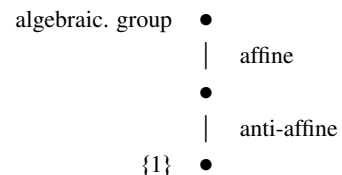
a. Summary

Every smooth connected algebraic group G over a field k contains a greatest smooth connected *affine* normal algebraic subgroup N (10.3). When k is perfect, the quotient G/N is an abelian variety (Barsotti-Chevalley theorem 10.25); otherwise G/N may be an extension of a unipotent algebraic group by an abelian variety (10.29).

On the other hand, every smooth connected algebraic group G contains a smallest connected affine normal algebraic subgroup N (not necessarily smooth) such that G/N is an abelian variety (10.26). When k is perfect, N is smooth, and it agrees with the group in the preceding paragraph.



Finally, every algebraic group G has a greatest affine algebraic quotient $G \rightarrow G^{\text{aff}}$ (10.33). The algebraic groups arising as the kernel N of such a quotient map are characterized by the condition $\mathcal{O}(N) = k$, and are said to be “anti-affine”. They are smooth, connected, and commutative. In nonzero characteristic, they are all semi-abelian varieties, i.e., extensions of abelian varieties by tori, but in characteristic zero they may also be an extension of a semi-abelian variety by a vector group (§2b).



b. Generalities

Let N and H be algebraic subgroups of an algebraic group G , and suppose that N is normal. There is an action θ of H on N by conjugation, and so we can form the semidirect product $N \rtimes_{\theta} H$ (§2e). The homomorphism

$$(n, h) \mapsto nh: N \rtimes_{\theta} H \rightarrow G$$

has kernel $N \cap H$ and image the algebraic subgroup NH of G whose R -points are the elements of $G(R)$ that lie in $N(R)H(R)$ for some faithfully flat R -algebra R' . The natural map of functors $H \rightarrow NH/N$ determines an isomorphism

$$H/N \cap H \rightarrow NH/N$$

of algebraic groups (5.37, 6.19).

LEMMA 10.1. *Let*

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

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 so also is Q .*

PROOF. (a) Assume that N and Q are affine. The morphism $G \rightarrow Q$ is faithfully flat with affine fibres. Now $G \times_Q G \simeq G \times N$ (9.19), and so the morphism $G \times_Q G \rightarrow G$ is affine. By faithfully flat descent, the morphism $G \rightarrow Q$ is affine. As Q is affine, so also is G .

Assume that N and Q are smooth. The morphism $G \rightarrow Q$ has smooth fibres of constant dimension, and so it is smooth. As Q is smooth, this implies that G .

Let $\pi_0(G)$ be the group of connected components of G ; it is an étale algebraic group, and the natural map $G \rightarrow \pi_0(G)$ is universal among homomorphisms from G to étale algebraic groups (5.48). If N is connected, then $G \twoheadrightarrow \pi_0(G)$ factors through Q , and hence through $\pi_0(Q)$, which is trivial if Q is also connected.

(b) We have $Q \simeq G/N$, which is affine if G is (9.45).

Because $G \rightarrow Q$ is faithfully flat, the map $\mathcal{O}_Q \rightarrow q_*\mathcal{O}_G$ is injective. Hence Q is reduced if G is reduced. The map $G \rightarrow Q$ stays faithfully flat under extension of the base field, and so Q is geometrically reduced (hence smooth) if G is geometrically reduced.

The faithfully flat homomorphism $G \rightarrow Q \rightarrow \pi_0(Q)$ factors through $\pi_0(G)$, and so $\pi_0(Q)$ is trivial if $\pi_0(G)$ is. □

In particular, an extension of connected affine group varieties is again a connected affine group variety, and a quotient of a connected group variety by a normal algebraic subgroup is a connected group variety.

LEMMA 10.2. *Let H and N be algebraic subgroups of an algebraic group G with N normal. If H and N are affine (resp. connected, resp. smooth), then HN is affine (resp. connected, resp. smooth).*

PROOF. Apply (10.1) and (8.34). □

PROPOSITION 10.3. *Every algebraic group contains a greatest smooth connected affine normal algebraic subgroup (i.e., a greatest connected affine normal subgroup variety).*

PROOF. Let G be an algebraic group over k . Certainly, G contains maximal connected affine normal subgroup varieties (e.g., any such variety of greatest dimension). Let H and N be two such maximal subgroup varieties. Then HN has the same properties by (10.2), and so $H = HN = N$. \square

DEFINITION 10.4. A **pseudo-abelian** variety is a connected group variety such that every connected affine normal subgroup variety is trivial.

PROPOSITION 10.5. *Every connected group variety G can be written as an extension*

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

of a pseudo-abelian variety Q by a connected affine normal subgroup variety N in exactly one way.

PROOF. Let N be the greatest connected affine normal subgroup variety of G (see 10.3), and let $Q = G/N$. If Q is not pseudo-abelian, then it contains a nontrivial connected affine normal subgroup variety H . Let H' be the inverse image of H in G . From the exact sequence

$$e \rightarrow N \rightarrow H' \rightarrow H \rightarrow e$$

and (10.1) we see that H' is an affine subgroup variety of G . Because H is normal in Q , H' is normal in G (cf. 5.39), and so this contradicts the definition of N . Hence Q is a pseudo-abelian variety.

In order for G/N to be pseudo-abelian, N must be maximal among the normal affine subgroup varieties of G ; therefore it is unique (10.3). \square

c. Local actions

PROPOSITION 10.6. *Let $G \times X \rightarrow X$ be an algebraic group acting faithfully on a connected separable algebraic scheme X over k . If there is a fixed point P , 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 a homomorphism $G(R) \rightarrow \text{Aut}(R \otimes_k (\mathcal{O}_P/\mathfrak{m}_P^{n+1}))$ for all k -algebras R . These are natural in R , and so arise from a homomorphism $\rho_n: G \rightarrow \text{GL}_{\mathcal{O}_P/\mathfrak{m}_P^{n+1}}$ of algebraic groups. Let $H_n = \text{Ker}(\rho_n)$, 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 $\mathcal{I}\mathcal{O}_P \subset \bigcap_n \mathfrak{m}_P^n = 0$ (Krull intersection theorem, CA 3.15). It follows that X^H contains an open neighbourhood of P . As X^H is closed and X is connected, 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 $\rho_n: G \rightarrow \text{GL}_{\mathcal{O}_P/\mathfrak{m}_P^{n+1}}$ is a monomorphism, hence a closed immersion (5.18, 7.37), and so G is affine. \square

COROLLARY 10.7. *Let G be a connected algebraic group, and let \mathcal{O}_e be 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 $G/Z \times G \rightarrow G$. \square

COROLLARY 10.8. *Let G be an algebraic group. If G is connected, then $G/Z(G)$ is affine.*

PROOF. The action of G/Z on G by conjugation is faithful and has a fixed point, namely, e . \square

d. *Anti-affine algebraic groups and abelian varieties*

DEFINITION 10.9. An algebraic group G over k is *anti-affine* if $\mathcal{O}(G) = k$.

For example, a complete connected algebraic group is anti-affine. Every homomorphism from an anti-affine algebraic group to an affine algebraic group is trivial. In particular, an algebraic group that is both affine and anti-affine is trivial.

PROPOSITION 10.10. *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 $G \rightarrow H$ 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 $G \rightarrow H$ factors through $Z(H) \hookrightarrow H$ (10.7). \square

COROLLARY 10.11. *Let G be a connected algebraic group. Every anti-affine algebraic subgroup H of G is contained in the centre of G .*

PROOF. Apply (10.10) to the inclusion map. \square

COROLLARY 10.12. *Every anti-affine algebraic G is commutative and connected.*

PROOF. The last corollary shows that it is commutative, and $\pi_0(G)$ is affine, and so $G \rightarrow \pi_0(G)$ is both trivial and surjective. \square

DEFINITION 10.13. An *abelian variety* is a complete connected group variety. An *abelian subvariety* of an algebraic group is a complete connected subgroup variety.

e. *Rosenlicht's decomposition theorem.*

Recall that a *rational map* $\phi: X \dashrightarrow Y$ 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 $U \rightarrow Y$; in the equivalence class, there is a pair with U greatest (and U is called “the open subvariety on which ϕ is defined.”) We shall need to use the following results, which can be found, for example, in [Milne 1986](#).

10.14. 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).

10.15. A 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).

10.16. Every rational map from a smooth variety V to an abelian variety A is defined on the whole of V (combine 10.14 and 10.15).

10.17. Every regular map from a connected group variety to an abelian variety is the composite of a homomorphism with a translation (ibid. 3.6).

10.18. Every abelian variety is commutative (10.12, or apply (10.17) to the map $x \mapsto x^{-1}$).

10.19. Multiplication by a nonzero integer on an abelian variety is faithfully flat with finite kernel (ibid. 8.2).

LEMMA 10.20. *Let G be a commutative connected group variety over k , and let*

$$(v, g) \mapsto v + g: V \times G \rightarrow V$$

be a G -torsor. There exists a morphism $\phi: V \rightarrow G$ 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

$$g \mapsto g + P: G \rightarrow V$$

is an isomorphism. Its inverse

$$\phi: V \rightarrow G$$

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 $K \stackrel{\text{def}}{=} \kappa(P)$ is a finite *separable* extension of k (of degree n , say). Let P_1, \dots, P_n be the k^{al} -points of V lying over P , and let \tilde{K} denote the Galois closure (over k) of K in k^{al} . Then the P_i lie in $V(\tilde{K})$. Let $\Gamma = \text{Gal}(\tilde{K}/k)$.

For each i , we have a morphism

$$\phi_i: V_{\tilde{K}} \rightarrow G_{\tilde{K}} \quad v \mapsto (v - P_i)$$

defined over \tilde{K} . The sum $\sum \phi_i$ is Γ -equivariant, and so arises from a morphism $\phi: V \rightarrow G$ over k . For $g \in G$,

$$\phi(v + g) = \sum_{i=1}^n \phi_i(v + g) = \sum_{i=1}^n (\phi_i(v) + g) = \phi(v) + ng. \quad \square$$

PROPOSITION 10.21. *Let A be an abelian subvariety of a connected group variety G . There exists a regular map $\phi: G \rightarrow A$ 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 10.11), there exists a faithfully flat homomorphism $\pi: G \rightarrow Q$ with kernel A . Because A is smooth, the map π has smooth fibres of constant dimension and so is smooth. Let K be the field of rational functions on Q , and let $V \rightarrow \text{Spm}(K)$ be the map obtained by pullback with respect to $\text{Spm}(K) \rightarrow Q$. Then V is an A_K -torsor over K (see 9.21). The morphism $\phi: V \rightarrow A_K$ 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 (see 10.16)

$$\phi: G \rightarrow A$$

satisfying

$$\phi(g + a) = \phi(g) + na$$

on a dense open subset of G , and hence on the whole of G . □

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 10.22 (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*

$$(a, n) \mapsto an: A \times N \rightarrow G \quad (47)$$

is a faithfully flat homomorphism with finite kernel. When k is perfect, N can be chosen to be smooth.

PROOF. Let $\phi: G \rightarrow A$ be the map given by (10.21). After we apply a translation, this will be a homomorphism (10.17) 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 10.11), the map (47) is a homomorphism. It is surjective (hence faithfully flat 5.17) because the homomorphism $A \rightarrow G/N \simeq A$ is multiplication by n , and its kernel is $N \cap A$, which is the finite group scheme A_n (apply 10.19).

When k is perfect, we can replace N with N_{red} , which is a smooth algebraic subgroup of N . □

f. Rosenlicht's dichotomy

The next result is the second key ingredient in Rosenlicht's proof of the Barsotti-Chevalley theorem.

PROPOSITION 10.23. *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 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 $E \stackrel{\text{def}}{=} \bar{X} \setminus X$. Let $P \in E$, and let H be the isotropy group at P . Then H is an algebraic subgroup of G and

$$\dim(G) - \dim(H) = \dim(G/H) \leq \dim E \leq \dim G - 1,$$

and so $\dim(H) \geq 1$. As it fixes P and acts faithfully on \bar{X} , it is affine (10.6).

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 to Milne 2013, 4.1, for the details; see also Brion et al. 2013, 2.3.

g. The Barsotti-Chevalley theorem

THEOREM 10.24. *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 . Let N be the greatest connected affine normal subgroup variety of $G_{k^{\text{al}}}$ (10.3). Because N is unique, it is stable under $\text{Gal}(k^{\text{al}}/k)$, and hence defined over k (1.41). It is therefore trivial. We have shown

that $G_{k^{\text{al}}}$ is pseudo-abelian. It suffices to show that it is complete, and so we may assume that k is algebraically closed. We use induction on the dimension of G .

Let Z be the centre of G . If $\dim(Z) = 0$, then the representation of G on the k -vector space $\mathcal{O}_e/\mathfrak{m}_e^{n+1}$ has finite (hence affine) kernel for n sufficiently large (see 10.7), which implies that G itself is affine (10.1a), and hence trivial. Therefore, we may assume that $\dim(Z) > 0$.

If Z_{red} is complete, then there exists an almost-complement N to Z_{red} (10.22), which we may assume to be smooth. A connected affine normal subgroup variety of N is normal in G , and hence trivial. Therefore N is pseudo-abelian, and so, by induction, it is complete. As G is a quotient of $Z_{\text{red}} \times N$, it also is complete (A.114d).

If Z_{red} is not complete, then it contains a connected affine subgroup variety N of dimension > 0 (see 10.23). Because it is contained in the centre, N is normal in G , which is a contradiction, and so this case doesn't occur. \square

THEOREM 10.25 (BARSOTTI 1955; CHEVALLEY 1960). *Every connected group variety G over a perfect field can be written as an extension*

$$e \rightarrow N \rightarrow G \rightarrow A \rightarrow e$$

of an abelian variety A by a connected affine normal subgroup variety N in exactly one way. The formation of the extension commutes with extension of the base field.

PROOF. According to (10.5), G is (uniquely) an extension of pseudo-abelian variety by a connected affine normal subgroup variety, but, because the base field is perfect, the pseudo-abelian variety is abelian (10.24). This proves the first statement. As abelian varieties remain abelian varieties under extension of the base field and connected affine normal subgroup varieties remain connected affine normal subgroup varieties, the second statement follows from the uniqueness. \square

THEOREM 10.26. *Let G be a connected group variety over a field k . There exists a smallest connected affine normal algebraic subgroup N of G such that G/N is an abelian variety.*

PROOF. Let N_1 and N_2 be connected affine normal algebraic subgroups of G such that G/N_1 and G/N_2 are abelian varieties. There is a closed immersion $G/N_1 \cap N_2 \hookrightarrow G/N_1 \times G/N_2$, and so $G/N_1 \cap N_2$ is also complete (hence an abelian variety). This shows that, if there exists a connected affine normal algebraic subgroup N of G such that G/N is an abelian variety, then there exists a smallest such subgroup.

We know that for some finite purely inseparable extension k' of k , $G' \stackrel{\text{def}}{=} G_{k'}$ contains a connected affine normal algebraic subgroup N' such that G'/N' is an abelian variety. By induction on the degree of k' over k , we may suppose that $k'^p \subset k$. Consider the Frobenius map

$$F: G' \rightarrow G'^{(p)} \stackrel{\text{def}}{=} G' \otimes_{k'} k'^{(1/p)}.$$

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 p th 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, hence, that N is defined over k . Now N is connected, normal, and affine, and G/N is an abelian variety (because $N_{k'} \supset N'$ and so $(G/N)_{k'}$ is a quotient of $G_{k'}/N'$). \square

COROLLARY 10.27. *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 G' (8.21). Let N be as in Theorem 10.26. As G/N is commutative (10.16), $G' \subset N$. Therefore G' is affine. As it is smooth, connected, and normal, it is trivial. \square

EXAMPLE 10.28. Let R be a complete discrete valuation ring with field of fractions K and perfect residue field k . Let A be an abelian variety over K . According to an important theorem of Néron, there exists smooth group scheme \mathcal{A} over R with generic fibre A such that the canonical map $\mathcal{A}(S) \rightarrow A(S_K)$ is an isomorphism for all smooth R -schemes S . Let A_0 denote the special fibre of \mathcal{A}/R — it is an algebraic group over k . If A_0 is an abelian variety over k , then A is said to have good reduction. Otherwise there is a filtration $A_0 \supset A_0^\circ \supset N \supset e$ with A_0/A_0° finite, A_0°/N an abelian variety, and N a commutative affine algebraic group. It is an important theorem that, after K has been replaced by a suitable finite extension, A_0° will be a semi-abelian variety.

ASIDE 10.29. 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 ,

$$e \rightarrow A \rightarrow G \rightarrow U \rightarrow e,$$

in a unique way.

ASIDE 10.30. The map $G \rightarrow A$ in (10.25) is universal among maps from G to an abelian variety sending e to e . Therefore A is the Albanese variety of G and $G \rightarrow A$ is the Albanese map. In his proof of (10.25), Chevalley (1960) begins with the Albanese map $G \rightarrow A$ of G , and proves that its kernel is affine. The above proof follows Rosenlicht 1956. The first published proof of the theorem is in Barsotti 1955.

ASIDE 10.31. Over a base ring other than a field, the Barsotti-Chevalley theorem (and much else in this chapter) becomes false. For example, the Néron model over a discrete valuation ring of an elliptic curve with bad reduction cannot be written as an extension of a proper group scheme by an affine group scheme. As another example, consider the constant group scheme $(\mathbb{Z}/2\mathbb{Z})_S$ over a scheme S . As a scheme $(\mathbb{Z}/2\mathbb{Z})_S = S \sqcup S$, and for any open subscheme U of S , it has $G = S \sqcup U$ as a subgroup scheme. If $S = \mathbb{A}^2$ and $U = \mathbb{A}^2 \setminus \{(0,0)\}$, then G is neither affine nor proper over S , and it cannot be written as an extension of such group schemes.

h. Anti-affine groups

Let G be an algebraic scheme over k , and let A be a k -algebra. To give a regular map $\text{Spm } A \rightarrow G$ of k -schemes is the same as giving a homomorphism of k -algebras $\mathcal{O}(G) \rightarrow A$:

$$\text{Hom}(\text{Spm } A, G) \simeq \text{Hom}(\mathcal{O}(G), A) \quad (48)$$

(A.13). Now assume that G has the structure $m: G \times G \rightarrow G$ of an algebraic group, and that A has the structure $\Delta: A \rightarrow A \otimes A$ of a Hopf algebra. Then $\mathcal{O}(m): \mathcal{O}(G) \rightarrow \mathcal{O}(G) \otimes \mathcal{O}(G)$ defines a Hopf algebra structure on $\mathcal{O}(G)$, and, under (48), homomorphisms of algebraic groups correspond to homomorphisms of Hopf algebras. Once we have proved that $\mathcal{O}(G)$ is finitely generated as a k -algebra, this will show that the $G \rightarrow G^{\text{aff}} \stackrel{\text{def}}{=} \text{Spm}(\mathcal{O}(G), \mathcal{O}(m))$ is universal among homomorphisms from G to an affine algebraic group.

PROPOSITION 10.32. *Every Hopf algebra over field k is a directed union of finitely generated sub-Hopf subalgebras over k .*

PROOF. Let A be a k -algebra (not necessarily finitely generated) and $\Delta: A \rightarrow A \otimes A$ a k -algebra homomorphism such that there exist k -algebra homomorphisms

$$\epsilon: A \rightarrow k, \quad S: A \rightarrow A,$$

for which the diagrams (20), (21) commute. By (4.6), every finite subset of A is contained in a finite-dimensional k -subspace V such that $\Delta(V) \subset V \otimes A$. Let (e_i) be a basis for V , and write $\Delta(e_j) = \sum_i e_i \otimes a_{ij}$. Then $\Delta(a_{ij}) = \sum_k a_{ik} \otimes a_{kj}$ (see (29), p.70), 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 $\Delta(Sa) = \sum S c_i \otimes S b_i$ (Exercise 3-2b). 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. \square

PROPOSITION 10.33. *Let G be an algebraic group over k .*

- (a) *The k -algebra $\mathcal{O}(G)$ is finitely generated; therefore $G^{\text{aff}} \stackrel{\text{def}}{=} \text{Spm}(\mathcal{O}(G), \mathcal{O}(m))$ is an algebraic group over k .*
- (b) *The natural map $\phi: G \rightarrow G^{\text{aff}}$ is universal for homomorphisms from G to affine algebraic groups; it is faithfully flat.*
- (c) *The kernel N of ϕ is anti-affine.*

PROOF. (a) We saw in (10.32), that $\mathcal{O}(G)$ 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 $f_i: G \rightarrow G_i$ of algebraic groups over k with $G_i = \text{Spm}(\mathcal{O}_i)$. Let $N = \bigcap_i \text{Ker}(f_i)$. Then $N = \text{Ker}(f_{i_0})$ for some i_0 (1.28), and $G/N \rightarrow G_{i_0}$ is a closed immersion (7.37). Therefore G/N is affine. Let i_1 be such that $\mathcal{O}_{i_0} \subset \mathcal{O}_{i_1}$. The homomorphism $G \rightarrow G_{i_0}$ factors through G_{i_1} . Thus, we have morphisms

$$G_{i_1} \xrightarrow{a} G/N \xrightarrow{b} G_{i_0}$$

with $b \circ a$ faithfully flat (3.47) and b a closed immersion. Correspondingly, we have homomorphisms

$$\mathcal{O}(G_{i_1}) \xleftarrow{a'} \mathcal{O}(G/N) \xleftarrow{b'} \mathcal{O}(G_{i_0})$$

with a' surjective $a' \circ b'$ faithfully flat (hence injective). Therefore $\mathcal{O}(G_{i_0}) \simeq \mathcal{O}(G/N)$. Similarly, $\mathcal{O}(G_{i_1}) \simeq \mathcal{O}(G/N)$, and so $\mathcal{O}(G_{i_0}) = \mathcal{O}(G_{i_1})$ as a subalgebra of $\mathcal{O}(G)$. As this is true for all i_1 with $\mathcal{O}_{i_0} \subset \mathcal{O}_{i_1}$ we see that $\mathcal{O}(G) = \mathcal{O}(G_{i_0})$, which is therefore finitely generated.

(b) We proved this above.

(c) This follows from the definition of N . \square

Thus every algebraic group is an extension of an affine algebraic group by an anti-affine algebraic group

$$1 \rightarrow G_{\text{ant}} \rightarrow G \rightarrow G^{\text{aff}} \rightarrow 1,$$

in a unique way; in fact, it is a *central* extension (10.11).

PROPOSITION 10.34. *Every anti-affine algebraic group is smooth and connected.*

PROOF. Let G be an anti-affine algebraic group over a field k . Then $G_{k^{\text{al}}}$ is anti-affine, and so we may suppose that k is algebraically closed. The G_{red}° is an algebraic subgroup of G (1.25). As $G \rightarrow G/G_{\text{red}}^{\circ}$ is faithfully flat, the homomorphism $\mathcal{O}(G/G_{\text{red}}^{\circ}) \rightarrow \mathcal{O}(G)$ is injective. Therefore $\mathcal{O}(G/G_{\text{red}}^{\circ}) = k$. As G/G_{red}° is finite, it is trivial, and so $G = G_{\text{red}}^{\circ}$. \square

COROLLARY 10.35. *An algebraic group G is affine if $Z(G^{\circ})$ is affine.*

PROOF. Let $N = \text{Ker}(G \rightarrow G^{\text{aff}})$. Because N is anti-affine, it is contained in G° , and hence in $Z(G^{\circ})$ (10.11). In particular, it is affine. The square

$$\begin{array}{ccc} G \times N & \longrightarrow & G \\ \text{affine} \downarrow & & \downarrow \\ G & \xrightarrow{\text{faithfully flat}} & G/N \end{array}$$

is cartesian (9.19), and so the morphism $G \rightarrow G/N$ is affine (A.90). As $G/N \simeq G^{\text{aff}}$ is affine, this implies that G is affine. \square

COROLLARY 10.36. *Every algebraic group over a field of characteristic zero is smooth.*

PROOF. As extensions of smooth algebraic groups are smooth (10.1), this follows from (10.33, 10.34). \square

NOTES. The proof of 10.33 (resp. 10.34; 10.35) follows DG III, §3, 8.1, 8.2, p.357 (resp. DG, III, §3, 8.3, p.358; DG, III, §3, 8.4, p.359).

i. Extensions of abelian varieties by affine algebraic groups (survey)

After the Barsotti-Chevalley theorem, the study of algebraic groups 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

$$e \longrightarrow H \xrightarrow{i} G \xrightarrow{p} A \longrightarrow e \quad (49)$$

of algebraic groups. Two extensions (G, i, p) and (G', i', p') of A by H are equivalent if there exists an isomorphism $f: G \rightarrow G'$ such that the following diagram commutes

$$\begin{array}{ccccccccc} e & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & A & \longrightarrow & e \\ & & \parallel & & \downarrow f & & \parallel & & \\ e & \longrightarrow & H & \xrightarrow{i'} & G' & \xrightarrow{p'} & A & \longrightarrow & e. \end{array}$$

We let $\text{Ext}(A, H)$ denote the set of equivalence classes of extensions of A by H .

For an exact sequence (49), the sequence

$$e \longrightarrow Z(H) \xrightarrow{Z(i)} Z(G) \xrightarrow{f} A \longrightarrow e \quad (50)$$

is exact, and the map (49) \mapsto (50) defines a bijection

$$\text{Ext}(A, H) \rightarrow \text{Ext}(A, Z(H))$$

where $\text{Ext}(A, Z(H))$ denotes the set of equivalence classes of extensions of A by $Z(H)$ in the (abelian) category of commutative algebraic groups. Hence $\text{Ext}(A, H)$ 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 $\text{Ext}(A, Z)$ 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_n (product of copies of \mathbb{G}_a) (see 17.19 below). There are the following results:

- (a) $\text{Ext}(A, \mathbb{G}_m) \simeq H^1(A, \mathcal{O}_A^\times)$, 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 $\text{Ext}(A, U)$ where U is unipotent. In characteristic 0, we have

$$\text{Ext}^1(A, V_n) \simeq H^1(A, \mathcal{O}_A \otimes V) \simeq V^{\dim(A)}$$

(Barsotti; Serre 1959, VII.18). In characteristic p , the computation is more complicated, and involves $\text{Ext}(N, Z^\circ)$, 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 $\text{Ext}(A, U) \simeq U(k)^{\dim A}$. See Wu 1986.

Exercises

EXERCISE 10-1. Let G be an algebraic group (not necessarily connected). Show that $G/Z(G)$ is affine if $\mathcal{D}G$ is affine.

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”. Also, we shall write $\mathcal{O}(G)$ for the coordinate ring of G .

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 $G \rightarrow G^{\vee\vee}$ is an isomorphism of topological groups (Pontryagin duality). Moreover, the dual of a compact commutative group is a discrete commutative group, and so, the study of compact commutative topological groups is equivalent to that of discrete commutative groups.

Clearly, “commutative” is required in the above statements, because 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 the analogue of this for algebraic groups. Recall that all algebraic groups are affine.

The tannakian perspective is that an algebraic group G and its category $\text{Rep}(G)$ of finite-dimensional representations should be considered equal partners.

a. Recovering a group from its representations

Let k be a ring (for the moment) and let A be an k -algebra (not necessarily finitely generated) equipped with k -homomorphisms $\Delta: A \rightarrow A \otimes A$ and $\epsilon: A \rightarrow k$ for which the diagrams (20), p.20, commute. Then the functor

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

is an affine monoid over k . 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:

$$(r_A(g)f_R)(x) = f_R(x \cdot g) \text{ all } x \in G(R). \tag{51}$$

LEMMA 11.1. *With the above notations, let u be a k -algebra endomorphism of A . If the diagram*

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ \downarrow u & & \downarrow 1 \otimes u \\ A & \xrightarrow{\Delta} & A \otimes A \end{array} \tag{52}$$

commutes, then there exists a $g \in G(k)$ such that $u = r_A(g)$.

PROOF. Let $\phi: G \rightarrow G$ be the morphism corresponding to u , so that

$$(uf)_R(x) = f_R(\phi_R x) \text{ all } f \in A, x \in G(R). \quad (53)$$

We shall prove that the lemma holds with $g = \phi(e)$.

From (52), we obtain a commutative diagram

$$\begin{array}{ccc} G & \xleftarrow{m} & G \times G \\ \downarrow \phi & & \downarrow 1 \times \phi \\ G & \xleftarrow{m} & G \times G. \end{array}$$

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 $x \in G(R)$,

$$(uf)_R(x) \stackrel{(53)}{=} f_R(x \cdot g_R) \stackrel{(51)}{=} (r_A(g)f)_R(x),$$

and so $u = r_A(g)$. □

Let G be an algebraic monoid 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 $\lambda_V \stackrel{\text{def}}{=} r_V(g): V_R \rightarrow V_R$. These maps satisfy the following conditions:

(a) for all representations V, W ,

$$\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W,$$

(b) $\lambda_{\mathbf{1}}$ is the identity map (here $\mathbf{1} = k$ with the trivial action)

(c) for all G -equivariant maps $u: V \rightarrow W$,

$$\lambda_W \circ u_R = u_R \circ \lambda_V,$$

THEOREM 11.2. *Let G be an algebraic monoid over k , and let R be a k -algebra. Suppose that, for every finite-dimensional representation (V, r_V) of G , we are given an R -linear map $\lambda_V: V_R \rightarrow V_R$. 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 (4.6) 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 $\lambda_A: A \rightarrow A$, $A = \mathcal{O}(G)_R$, corresponding to the regular representation r_A of G on A . The map $m: A \otimes A \rightarrow A$ is equivariant¹ for

¹Here are the details. For $x \in G(R)$,

$$\begin{aligned} (r(g) \circ m)(f \otimes f')(x) &= (r(g)(ff'))(x) = (ff')(xg) = f(xg) \cdot f'(xg) \\ (m \circ r(g) \otimes r(g))(f \otimes f')(x) &= ((r(g)f) \cdot (r(g)f'))(x) = f(xg) \cdot f'(xg). \end{aligned}$$

the representations $r_A \otimes r_A$ and r_A , which means that λ_A is a k -algebra homomorphism. Similarly, the map $\Delta: A \rightarrow A \otimes A$ is equivariant for the representations r_A on A and $1 \otimes r_A$ on $A \otimes A$, and so the diagram in (11.1) commutes with u replaced by λ_A . Now Lemma 11.1, 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 -module. There is an injective homomorphism of representations

$$\rho: V \rightarrow V_0 \otimes \mathcal{O}(G)$$

(4.9). 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) . \square

COMPLEMENTS

Let V be a finitely generated module over a k -algebra R . By a representation of G on V , we mean a homomorphism $r: G_R \rightarrow \mathrm{GL}_V$ of group-valued functors. To give such a homomorphism is the same as giving an R -linear map $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ satisfying the conditions (28), p.69. We let $\mathrm{Rep}_R(G)$ denote the category of representations of G on finitely generated R -modules. We omit the subscript when $R = k$.

11.3. Each $g \in G(R)$ defines a family as in the theorem. Thus, from the category $\mathrm{Rep}(G)$, 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 11.2 is often called the *reconstruction theorem*.

11.4. Let (λ_V) be a family as in Theorem 11.2. If G is an algebraic group, then each λ_V is an isomorphism and $\lambda_{V^\vee} = (\lambda_V)^\vee$, because this true of the maps $r_V(g)$.

11.5. For a k -algebra R , let ω_R be the forgetful functor $\mathrm{Rep}_R(G) \rightarrow \mathrm{Mod}_R$, and let $\mathrm{End}^\otimes(\omega_R)$ denote the set of natural transformations $\lambda: \omega_R \rightarrow \omega_R$ commuting with tensor products — the last condition means that λ satisfies conditions (a) and (b) of the theorem. The theorem says that the canonical map $G(R) \rightarrow \mathrm{End}^\otimes(\omega_R)$ 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 (11.4), this can be written $G \simeq \underline{\mathrm{Aut}}^\otimes(\omega)$.

11.6. 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 (cf. Springer 1998, p.39, and Exercise 3-1). In this way, we can recover $\mathcal{O}(G)$ directly as the ring of “representative functions” on G .

11.7. In (11.2), 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 $\otimes^n(V \oplus V^\vee)$ or $V^{\otimes n} \otimes \det^{-s}$ (apply 4.12). Here \det^{-1} is the dual of the representation of G on $\bigwedge^{\dim V} V$. Then (11.2) can be interpreted as saying that G is the subgroup of GL_V fixing all tensors in subquotients of representations $V^{\otimes n} \otimes \det^{-s}$ fixed by G .

11.8. In general, we can't omit "quotients of" from (11.7).² However, we can omit it if V is semisimple or if some nonzero multiple of every character $H \rightarrow \mathbb{G}_m$ extends to a character $G \rightarrow \mathbb{G}_m$ of G .

b. Application to Jordan decompositions

THE JORDAN DECOMPOSITION OF A LINEAR MAP

In this subsection, we review some linear algebra.

Recall that an endomorphism α of a vector space V is **diagonalizable** if V has a basis of eigenvectors for α , and that it is **semisimple** if it becomes diagonalizable after an extension of the base field k . For example, the linear map $x \mapsto Ax: k^n \rightarrow k^n$ defined by an $n \times n$ matrix A is diagonalizable if and only if there exists an invertible matrix P with entries in k such that PAP^{-1} is diagonal, and it is semisimple if and only if there exists such a matrix P with entries in some field containing k .

From linear algebra, we know that α is semisimple if and only if its minimum polynomial $m_\alpha(T)$ has distinct roots; in other words, if and only if the subring $k[\alpha] \simeq k[T]/(m_\alpha(T))$ of $\text{End}_k(V)$ generated by α is 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 $\text{id}_V - \alpha$ is nilpotent. Clearly, if α is nilpotent, then its minimum polynomial divides T^m for some m , and so the eigenvalues³ of α are all zero, even in k^{al} . From linear algebra, we know that the converse is also true, and so α is unipotent if and only if its eigenvalues in k^{al} all equal 1.

Let α be an endomorphism of a finite-dimensional vector space V over k . We say that α **has all of its eigenvalues** in k if the characteristic polynomial $P_\alpha(T)$ of α splits in $k[X]$:

$$P_\alpha(T) = (T - a_1)^{n_1} \cdots (T - a_r)^{n_r}, \quad a_i \in k.$$

For each eigenvalue a of α in k , the **primary space**⁴ is defined to be:

$$V^a = \{v \in V \mid (\alpha - a)^N v = 0, \quad N \text{ sufficiently divisible}\}^5.$$

PROPOSITION 11.9. *If α has all of its eigenvalues 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

$$a(T)Q(T) + b(T)R(T) = 1.$$

²Consider for example, the subgroup $B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ of GL_2 acting on $V = k \times k$ and suppose that a vector $v \in (V \oplus V^\vee)^{\otimes n}$ is fixed by B . Then $g \mapsto gv$ is a regular map $\text{GL}_2/B \rightarrow (V \oplus V^\vee)^{\otimes n}$ of algebraic varieties. But $\text{GL}_2/B \simeq \mathbb{P}^1$ and $(V \oplus V^\vee)^{\otimes n}$ is affine, and so the map is trivial. Therefore, v is fixed by GL_2 , and so $B' = B$.

³We define the **eigenvalues** of an endomorphism of a vector space to be the *family* of roots of its characteristic polynomial in some algebraically closed field.

⁴This is Bourbaki's terminology (LIE VII, §1); "generalized eigenspace" is also used.

⁵By this I mean that there exists an N_0 such that the statement holds for all positive integers divisible by N_0 , i.e., that N is sufficiently large for the partial ordering

$$M \leq N \iff M \text{ divides } N.$$

For any $v \in V$,

$$a(\alpha)Q(\alpha)v + b(\alpha)R(\alpha)v = v, \quad (54)$$

which implies immediately that $\text{Ker}(Q(\alpha)) \cap \text{Ker}(R(\alpha)) = 0$. Moreover, because

$$Q(\alpha)R(\alpha) = 0 = R(\alpha)Q(\alpha),$$

(54) expresses v as the sum of an element of $\text{Ker}(R(\alpha))$ and an element of $\text{Ker}(Q(\alpha))$. Thus, V is the direct sum of $\text{Ker}(Q(\alpha))$ and $\text{Ker}(P(\alpha))$.

On applying this remark repeatedly to the characteristic polynomial

$$(T - a_1)^{n_1} \dots (T - a_r)^{n_r}$$

of α and its factors, we find that

$$V = \bigoplus_i \text{Ker}(\alpha - a_i)^{n_i},$$

as claimed. □

COROLLARY 11.10. *An endomorphism α of a finite-dimensional k -vector space V has all of its eigenvalues in k if and only if, for some choice of basis for V , the matrix of α is upper triangular.*

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**.

THEOREM 11.11. *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 .

For example,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

PROOF. Assume first that α has all of its eigenvalues in k , so that V is a direct sum of the primary spaces of α , say, $V = \bigoplus_{1 \leq i \leq m} V^{a_i}$ where the a_i are the distinct roots of P_α . Define α_s to be the automorphism of V that acts as a_i on V^{a_i} for each i . Then α_s is a semisimple automorphism of V , and $\alpha_u \stackrel{\text{def}}{=} \alpha \circ \alpha_s^{-1}$ commutes with α_s (because it does on each V^{a_i}) and is unipotent (because its eigenvalues are 1). Thus α_s and α_u satisfy (a) and (b).

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

$$Q(T) \equiv a_i \pmod{(T - a_i)^{n_i}}, \quad i = 1, \dots, m.$$

Then $Q(\alpha)$ acts as a_i on V^{a_i} for each i , and so $\alpha_s = Q(\alpha)$, which is a polynomial in α . Similarly, $\alpha_s^{-1} \in k[\alpha]$, and so $\alpha_u \stackrel{\text{def}}{=} \alpha \circ \alpha_s^{-1} \in k[\alpha]$.

It remains to prove the uniqueness of α_s and α_u . Let $\alpha = \beta_s \circ \beta_u$ be a second decomposition satisfying (a) and (b). Then β_s and β_u commute with α , and therefore also with α_s and α_u (because they are polynomials in α). It follows that $\beta_s^{-1}\alpha_s$ is semisimple and that $\alpha_u\beta_u^{-1}$ is unipotent. Since they are equal, both must equal 1. This completes the proof in this case.

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

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

$$A = (\sigma A_s)(\sigma A_u)$$

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

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

$$A_s = c_0 + c_1 A + \cdots + c_{n-1} A^{n-1} \quad (n = \dim V).$$

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

$$\alpha_s = c_0 + c_1 \alpha + \cdots + c_{n-1} \alpha^{n-1} \in k[\alpha].$$

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 .

PROPOSITION 11.12. *Let V and W be vector spaces over a perfect field k . Let α and β be automorphisms of V and W respectively, and let $\varphi: V \rightarrow W$ be a linear map. If $\varphi \circ \alpha = \beta \circ \varphi$, then $\varphi \circ \alpha_s = \beta_s \circ \varphi$ and $\varphi \circ \alpha_u = \beta_u \circ \varphi$.*

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that both α and β have all of their eigenvalues in k . Recall that α_s acts on each 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 11.13. *Let V be a vector space over a perfect field. Every subspace W of V stable under α is stable under α_s and α_u , and $\alpha|_W = \alpha_s|_W \circ \alpha_u|_W$ is the Jordan decomposition of $\alpha|_W$.*

PROOF. The subspace W is stable under α_s and α_u because each is a polynomial in α . Clearly the decomposition $\alpha|_W = \alpha_s|_W \circ \alpha_u|_W$ has the properties (a) and (b) of (11.11), and so is the Jordan decomposition $\alpha|_W$. □

PROPOSITION 11.14. *For any automorphisms α and β of vector spaces V and W over a perfect field,*

$$\begin{aligned}(\alpha \otimes \beta)_s &= \alpha_s \otimes \beta_s \\ (\alpha \otimes \beta)_u &= \alpha_u \otimes \beta_u.\end{aligned}$$

PROOF. It suffices to prove this after an extension of scalars, and so we may suppose that both α and β have all of their eigenvalues in k . For any $a, b \in k$, $V^a \otimes W^b \subset (V \otimes W)^{ab}$, 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 $(\alpha \otimes \beta)_u = \alpha_u \otimes \beta_u$. \square

EXAMPLE 11.15. Let k be a nonperfect field of characteristic 2, so that there exists an $a \in k \setminus k^2$, 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 has eigenvalues 1, -1 , and $-1 = 1$). These matrices do not have coefficients in k , and so, if M had a Jordan decomposition in $M_2(k)$, it would have two distinct Jordan decompositions in $M_2(k^{\text{al}})$, contradicting the uniqueness of the decomposition.

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 (11.11), 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 11.16. *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

Finally, we are able to prove the following important theorem.

THEOREM 11.17. *Let G be an algebraic group over a perfect field k . For every $g \in G(k)$, there exist unique elements $g_s, g_u \in G(k)$ such that, for all representations (V, r_V) of G , $r_V(g_s) = r_V(g)_s$ and $r_V(g_u) = r_V(g)_u$. Furthermore,*

$$g = g_s g_u = g_u g_s. \tag{55}$$

PROOF. In view of (11.12) and (11.14), the first assertion follows immediately from (11.2) applied to the families $(r_V(g)_s)_V$ and $(r_V(g)_u)_V$. Now choose a faithful representation r_V . Because

$$r_V(g) = \begin{cases} r_V(g)_s r_V(g)_u = r_V(g_s) r_V(g_u) = r_V(g_s g_u) \\ r_V(g)_u r_V(g)_s = r_V(g_u) r_V(g_s) = r_V(g_u g_s) \end{cases}$$

(55) follows. □

The elements g_s and g_u are called the *semisimple* and *unipotent parts* of g , and $g = g_s g_u$ is the *Jordan decomposition* (or *Jordan-Chevalley decomposition*) of g .

11.18. 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 .

11.19. To check that a decomposition $g = g_s g_u$ is the Jordan decomposition, it suffices to check that $r(g) = r(g_s) r(g_u)$ is the Jordan decomposition of $r(g)$ for a single faithful representation of G .

11.20. Homomorphisms of algebraic groups preserve Jordan decompositions. To see this, let $u: G \rightarrow G'$ be a homomorphism and let $g = g_s g_u$ be a Jordan decomposition in $G(k)$. If $\varphi: G' \rightarrow \mathrm{GL}_V$ is a representation of G' , then $\varphi \circ u$ is a representation of G , and so

$$(\varphi \circ u)(g) = ((\varphi \circ u)(g_s)) \cdot ((\varphi \circ u)(g_u))$$

is the Jordan decomposition in $\mathrm{GL}(V)$. When we choose φ to be faithful, this implies that $u(g) = u(g_s) \cdot u(g_u)$ is the Jordan decomposition of $u(g)$.

11.21. Let G be a group variety over an algebraically closed field. In general, the set $G(k)_s$ of semisimple elements in $G(k)$ will not be closed for the Zariski topology. However, the set $G(k)_u$ of unipotent elements is closed. To see this, embed G in GL_n for some n . A matrix A is unipotent if and only if its characteristic polynomial is $(T - 1)^n$. But the coefficients of the characteristic polynomial of A are polynomials in the entries of A , and so this is a polynomial condition on A .

ASIDE 11.22. We have defined Jordan decompositions for algebraic groups G which are not necessarily smooth. However, as we require the base field to be perfect, G_{red} is a smooth algebraic subgroup of G such that $G_{\mathrm{red}}(k) = G(k)$. Therefore everything comes down to smooth groups.

ASIDE 11.23. Our proof of the existence of Jordan decompositions (Theorem 11.17) is the standard one, except that we have made Lemma 11.1 explicit. As Borel has noted (1991, p. 88; 2001, VIII 4.2, p. 169), the result essentially goes back to [Kolchin 1948b](#), 4.7.

ASIDE 11.24. “. . . there is a largely separate line of work on linear algebraic groups, which owes even more to Chevalley and certainly merits the label ‘Jordan-Chevalley decomposition’. Actually, a couple of papers by Kolchin in 1948 started in this direction, but Chevalley’s 1951 book and his famous 1956-58 classification seminar made the results basic to all further work. The striking fact is that the semisimple and unipotent parts in the multiplicative Jordan decomposition are intrinsically defined in any connected linear algebraic group (over any algebraically closed field, though Chevalley’s early work started out over arbitrary fields). Adaptations to fields of definition then follow.” ([Humphreys mo152239](#).)

c. Characterizations of categories of representations

Pontryagin duality identifies the topological groups that arise as the dual of a locally compact commutative group — they are exactly the locally compact commutative groups.

Similarly, Tannakian theory identifies the tensor categories that arise as the category of representations of an algebraic group. We briefly explain the answer.

In this section, k -algebras are not required to be finitely generated, and we ignore set-theoretic questions. An abelian category together with a k -vector space structure on every Hom group said to be k -linear if the composition maps are k -bilinear.

By an **affine group** over k we mean a functor G from k -algebras to groups whose underlying functor to sets is representable by a k -algebra $\mathcal{O}(G)$:

$$G(R) = \text{Hom}_{k\text{-algebra}}(\mathcal{O}(G), R).$$

When $\mathcal{O}(G)$ is finitely generated, G is an affine algebraic group.

Let $\omega: \mathbf{A} \rightarrow \mathbf{B}$ be a faithful functor of categories. We say that a morphism $\omega X \rightarrow \omega Y$ **lives in** \mathbf{A} if it lies in $\text{Hom}(X, Y) \subset \text{Hom}(\omega X, \omega Y)$.

For k -vector spaces U, V, W , there are canonical isomorphisms

$$\begin{aligned} \phi_{U,V,W}: U \otimes (V \otimes W) &\rightarrow (U \otimes V) \otimes W, & u \otimes (v \otimes w) &\mapsto (u \otimes v) \otimes w \\ \psi_{U,V}: U \otimes V &\rightarrow V \otimes U, & u \otimes v &\mapsto v \otimes u. \end{aligned} \quad (56)$$

THEOREM 11.25. *Let \mathbf{C} be a k -linear abelian category and let $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ be a k -bilinear functor. The pair (\mathbf{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 $\omega: \mathbf{C} \rightarrow \text{Vec}_k$ 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 \mathbf{C} for all X, Y, Z ;
- (c) there exists an (identity) object $\mathbf{1}$ in \mathbf{C} such that $\omega(\mathbf{1}) = k$ and the canonical isomorphisms

$$\omega(\mathbf{1}) \otimes \omega(X) \simeq \omega(X) \simeq \omega(X) \otimes \omega(\mathbf{1})$$

live in \mathbf{C} ;

- (d) for every object X such that $\omega(X)$ has dimension 1, there exists an object X^{-1} in \mathbf{C} such that $X \otimes X^{-1} \approx \mathbf{1}$.

PROOF. If $(\mathbf{C}, \otimes) = (\text{Rep}(G), \otimes)$ for some affine group scheme G over k , then the forgetful functor has the required properties, which proves the necessity of the condition. We defer the proof of the sufficiency to the final section of this chapter (Section e). \square

NOTES

11.26. The group scheme G depends on the choice of ω . Once ω has been chosen, G has the same description as in (11.2), namely, for a k -algebra R , the group $G(R)$ consists of families $(\lambda_X)_{X \in \text{ob}(\mathbf{C})}$, $\lambda_X \in \text{End}(X) \otimes R$, such that

- (a) for all X, Y in \mathbf{C} ,

$$\lambda_{X \otimes Y} = \lambda_X \otimes \lambda_Y;$$

- (b) $\lambda_{\mathbf{1}}$ is the identity map;
- (c) for all morphisms $u: X \rightarrow Y$,

$$\lambda_Y \circ u_R = u_R \circ \lambda_X.$$

In other words, $G = \underline{\text{Aut}}^{\otimes}(\omega)$. Therefore (11.2) shows that, when we start with $(\mathbf{C}, \otimes) = (\text{Rep}(G), \otimes)$, we get back the group G .

11.27. Let \mathbf{C} be a k -linear abelian category equipped with a k -bilinear functor $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$. The *dual* of an object X of \mathbf{C} is an object X^{\vee} equipped with an “evaluation map” $\text{ev}: X^{\vee} \otimes X \rightarrow \mathbf{1}$ having the property that the map

$$\alpha \mapsto \text{ev} \circ (\alpha \otimes \text{id}_X): \text{Hom}(T, X^{\vee}) \rightarrow \text{Hom}(T \otimes X, \mathbf{1})$$

is an isomorphism for all objects T of \mathbf{C} . If there exists a functor ω as in (11.25), then duals always exist, and the affine group G attached to ω is algebraic if and only if there exists an X such that every object of \mathbf{C} is isomorphic to a subquotient of a direct sum of objects $\otimes^m(X \oplus X^{\vee})$. The necessity of this condition follows from (4.12).

EXAMPLES

11.28. Let M be a commutative group. An M -*gradation* on a finite-dimensional k -vector space V 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 (11.25), 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 (14.3) below.

11.29. Let K be a topological group. The category $\text{Rep}_{\mathbb{R}}(K)$ of continuous representations of K on finite-dimensional real vector spaces has a natural tensor product. The forgetful functor satisfies the conditions of (11.25), and so there is an affine algebraic group \tilde{K} over \mathbb{R} , called the *real algebraic envelope* of K , for which there exists a natural equivalence

$$\text{Rep}_{\mathbb{R}}(K) \rightarrow \text{Rep}_{\mathbb{R}}(\tilde{K}).$$

This equivalence is induced by a homomorphism $K \rightarrow \tilde{K}(\mathbb{R})$, which is an isomorphism when K is compact (Serre 1993, 5.2).

11.30. Let G be a connected complex Lie group, and let \mathbf{C} be the category of complex-analytic representations of G on finite-dimensional complex vector spaces. With the obvious functors $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ and $\omega: \mathbf{C} \rightarrow \text{Vec}_{\mathbb{C}}$, this satisfies the hypotheses of Theorem 11.25, and so it is the category of representations of an affine group $A(G)$. Almost by definition, there exists a homomorphism $P: G \rightarrow A(G)(\mathbb{C})$ with the property that, for each complex-analytic representation (V, ρ) of G , there exists a unique representation $(V, \hat{\rho})$ of $A(G)$ such that $\hat{\rho} = \rho \circ P$.

The group $A(G)$ is sometimes called the *Hochschild-Mostow group* (for a brief exposition of this work of Hochschild and Mostow (1957–69), see Magid, Andy, Notices AMS, Sept. 2011, p.1089). Hochschild and Mostow also studied $A(G)$ for G a finitely generated (abstract) group.

d. Tannakian categories

In this subsection, we review a little of the abstract theory of Tannakian categories. See [Saavedra Rivano 1972](#) or [Deligne and Milne 1982](#) for the details.

A k -linear **tensor category** is a system $(\mathbf{C}, \otimes, \phi, \psi)$ in which \mathbf{C} is a k -linear category, $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ is a k -bilinear functor, and ϕ and ψ are functorial isomorphisms

$$\begin{aligned}\phi_{X,Y,Z}: X \otimes (Y \otimes Z) &\rightarrow (X \otimes Y) \otimes Z \\ \psi_{X,Y}: X \otimes Y &\rightarrow Y \otimes X\end{aligned}$$

satisfying certain natural conditions which ensure that the tensor product of every (unordered) finite family of objects of \mathbf{C} is well-defined up to a well-defined isomorphism. In particular, there is an identity object $\mathbf{1}$ (tensor product of the empty family) such that $X \rightsquigarrow \mathbf{1} \otimes X: \mathbf{C} \rightarrow \mathbf{C}$ 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 (56).

A k -linear tensor category is **rigid** if every object has a dual (in the sense of 11.27). For example, category is rigid if G is an affine group. A rigid abelian k -linear tensor category (\mathbf{C}, \otimes) is a **Tannakian category** over k if $\text{End}(\mathbf{1}) = k$ and there exists a k -algebra R and an exact faithful k -linear functor $\omega: (\mathbf{C}, \otimes) \rightarrow (\text{Vec}_R, \otimes)$ preserving the tensor structure. Such a functor is said to be a **R -valued fibre functor** for \mathbf{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 11.31. *Let (\mathbf{C}, \otimes) be a neutral Tannakian category over k , and let ω be a k -valued fibre functor. Then,*

- (a) *the functor $\underline{\text{Aut}}^\otimes(\omega)$ (see 11.5) of k -algebras is represented by an affine group scheme G ;*
- (b) *the functor $\mathbf{C} \rightarrow \text{Rep}(G)$ defined by ω is an equivalence of tensor categories.*
- (c) *For an affine group scheme G over k , the obvious morphism of functors $G \rightarrow \underline{\text{Aut}}^\otimes(\omega_{\text{forget}})$ is an isomorphism.*

PROOF. The functor ω satisfies the conditions of Theorem 11.25. For (a), (b), and (c), this is obvious; for (d) one has to note that if $\omega(X)$ has dimension 1, then the map $\text{ev}: X^\vee \otimes X \rightarrow \mathbf{1}$ is an isomorphism. \square

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 \mathbf{C} with values in a k -algebra R .

THEOREM 11.32. *Let $\mathbf{C}, \otimes, \omega, G$ be as in Theorem 11.31, and let R be a k -algebra.*

- (a) *For every R -valued fibre functor ν on \mathbf{C} , the functor*

$$R \rightsquigarrow \text{Isom}^\otimes(\omega \otimes R, \nu)$$

is represented by an affine scheme $\underline{\text{Isom}}^\otimes(\omega_R, \nu)$ 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 $v \mapsto \underline{\text{Isom}}^{\otimes}(\omega_R, v)$ establishes an equivalence between the category of R -valued fibre functors on \mathbf{C} and the category of right G_R -torsors on $\text{Spec}(R)$ for the flat (fpqc) topology.

PROOF. The proof is an extension of that of Theorems 11.25 and 11.31 — see Deligne and Milne 1982, Theorem 3.2. \square

e. Proof of Theorem 11.25

CATEGORIES OF COMODULES OVER A COALGEBRA

A *coalgebra*⁶ over k is a k -vector space C equipped with a pair of k -linear maps

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

such that the diagrams (20), p.56, commute. The linear dual C^\vee of C becomes an associative algebra over k with the multiplication

$$C^\vee \otimes C^\vee \xrightarrow{\text{can.}} (C \otimes C)^\vee \xrightarrow{\Delta^\vee} C^\vee, \quad (57)$$

and the structure map

$$k \simeq k^\vee \xrightarrow{\epsilon^\vee} C^\vee. \quad (58)$$

We say that C is *cocommutative* if C^\vee is commutative (resp. étale).

Let (C, Δ, ϵ) be a coalgebra over k . A C -comodule is a k -linear map $\rho: V \rightarrow V \otimes C$ satisfying the conditions (28), p.69. In terms of a basis $(e_i)_{i \in I}$ for V , these conditions become

$$\left. \begin{aligned} \Delta(c_{ij}) &= \sum_{k \in I} c_{ik} \otimes c_{kj} \\ \epsilon(c_{ij}) &= \delta_{ij} \end{aligned} \right\} \quad \text{all } i, j \in I. \quad (59)$$

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. When V is finite dimensional over k , so also is C_V . If (V, ρ) is a sub-comodule of the C -comodule (C, Δ) , then $V \subset C_V$.

An additive category \mathbf{C} is said to be *k -linear* if the Hom sets are k -vector spaces and composition is k -bilinear. Functors of k -linear categories are required to be k -linear, i.e., the maps $\text{Hom}(a, b) \rightarrow \text{Hom}(Fa, Fb)$ defined by F are required to be k -linear.

For example, if C is k -coalgebra, then $\text{Comod}(C)$ is a k -linear category. In fact, $\text{Comod}(C)$ is a k -linear abelian category, and the forgetful functor $\omega: \text{Comod}(C) \rightarrow \text{Vec}_k$ is exact, faithful, and k -linear. The next theorem provides a converse to this statement.

THEOREM 11.33. *Let \mathbf{C} be an essentially small⁷ k -linear abelian category, and let $\omega: \mathbf{C} \rightarrow \text{Vec}_k$ be an exact faithful k -linear functor. Then there exists a coalgebra C such that \mathbf{C} is equivalent to the category of C -comodules of finite dimension.*

⁶Sometimes this is called a *co-associative* coalgebra over k with *co-identity*.

⁷This hypothesis is essential. Let S be a proper class, and let \mathbf{C} be the category of finite-dimensional vector spaces over k equipped with an S -gradation. The coalgebra C has an idempotent for each element of S , and so its underlying “set” is a proper class.

The proof will occupy the rest of this subsection.

Because ω is faithful, $\omega(\text{id}_X) = \omega(0)$ if and only if $\text{id}_X = 0$, 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 \mathbf{C} , $\text{Hom}(X, Y)$ is a subspace of $\text{Hom}(\omega X, \omega Y)$, and hence has finite dimension over k .

For monomorphisms $X \xrightarrow{x} Y$ and $X' \xrightarrow{x'} Y$ with the same target, we write $x \leq x'$ if there exists a morphism $X \rightarrow X'$ (necessarily unique) giving a commutative triangle. The lattice of subobjects of Y is obtained from the collection of monomorphisms by identifying two monomorphisms x and x' if $x \leq x'$ and $x' \leq x$. The functor ω maps the lattice of subobjects of Y injectively⁸ to the lattice of subspaces of ωY . Hence X has finite length.

Similarly ω maps the lattice of quotient objects of Y injectively to the lattice of quotient spaces of ωY .

For X in \mathbf{C} , we let $\langle X \rangle$ denote the full subcategory of \mathbf{C} whose objects are the quotients of subobjects of direct sums of copies of X . For example, if \mathbf{C} is the category of finite-dimensional comodules over a coalgebra C , then $\langle X \rangle$ is the category of finite-dimensional comodules over C_X (see above).

Let X be an object of \mathbf{C} , and let S be 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 (11.33) IN THE CASE THAT \mathbf{C} IS GENERATED BY A SINGLE OBJECT

In the next three lemmas, we assume that $\mathbf{C} = \langle X \rangle$ for some X .

LEMMA 11.34. *For every monogenic object Y of \mathbf{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 $y = (y_1, \dots, y_m)$ 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 $X^m \rightarrow X$ whose kernel N is isomorphic to X^{m-1} .⁹ 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 $m' \leq \dim_k \omega(X)$. \square

⁸If $\omega(X) = \omega(X')$, then the kernel of

$$\begin{pmatrix} x \\ x' \end{pmatrix}: X \times X' \rightarrow Y$$

projects isomorphically onto each of X and X' (because it does after ω has been applied).

⁹Extend (a_1, \dots, a_m) to an invertible matrix $\begin{pmatrix} a_1, \dots, a_m \\ A \end{pmatrix}$; then $A: X^m \rightarrow X^{m-1}$ defines an isomorphism of N onto X^{m-1} , because $\omega(A)$ is an isomorphism $\omega(N) \rightarrow \omega(X)^{m-1}$.

As $\dim_k \omega(Y)$ can take only finitely many values when Y is monogenic, there exists a monogenic P for which $\dim_k \omega(P)$ has its largest possible value. Let $p \in \omega(P)$ generate P .

LEMMA 11.35. (a) *The pair (P, p) represents the functor ω .*

(b) *The object P is a projective generator for \mathbf{C} , i.e., the functor $\text{Hom}(P, -)$ is exact and faithful.*

PROOF. (a) Let X be an object of \mathbf{C} , and let $x \in \omega(X)$; we have to prove that there exists a unique morphism $f: P \rightarrow X$ such that $\omega(f)$ sends p to x . The uniqueness follows from the fact p generates P (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 $Q \rightarrow P$ defined by the projection map is surjective because P is generated by p . Therefore,

$$\dim_k \omega(Q) \geq \dim_k \omega(P),$$

but because $\dim_k(\omega(P))$ is maximal, equality must hold, and so $Q \rightarrow P$ is an isomorphism. The composite of its inverse with the second projection $Q \rightarrow X$ is a morphism $P \rightarrow X$ sending p to x .

(b) The object P is projective because ω is exact, and it is a generator because ω is faithful. \square

Let $A = \text{End}(P)$ — it is a k -algebra of finite dimension as a k -vector space (not necessarily commutative) — and let h^P be the functor $X \rightsquigarrow \text{Hom}(P, X)$.

LEMMA 11.36. *The functor h^P is an equivalence from \mathbf{C} to the category of right A -modules of finite dimension over k . Its composite with the forgetful functor is canonically isomorphic to ω .*

PROOF. Because P is a 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 ,

$$A^m \xrightarrow{u} A^n \rightarrow M \rightarrow 0$$

where u is an $m \times n$ matrix with coefficients in A . This matrix defines a morphism $P^m \rightarrow P^n$ whose cokernel X has the property that $h^P(X) \simeq M$. Therefore h^P is essentially surjective.

We have just shown that every object X in \mathbf{C} occurs in an exact sequence

$$P^m \xrightarrow{u} P^n \rightarrow X \rightarrow 0.$$

Let Y be a second object of \mathbf{C} . Then

$$\text{Hom}(P^m, Y) \simeq h^P(Y)^m \simeq \text{Hom}(A^m, h^P(Y)) \simeq \text{Hom}(h^P(P^m), h^P(Y)),$$

and the composite of these maps is that defined by h^P . From the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}(X, Y) & \longrightarrow & \text{Hom}(P^n, Y) & \longrightarrow & \text{Hom}(P^m, Y) \\ & & \downarrow & & \downarrow \simeq & & \downarrow \simeq \\ 0 & \longrightarrow & \text{Hom}(h^P(X), h^P(Y)) & \longrightarrow & \text{Hom}(A^n, h^P(Y)) & \longrightarrow & \text{Hom}(A^m, h^P(Y)) \end{array}$$

we see that $\text{Hom}(X, Y) \rightarrow \text{Hom}(h^P(X), h^P(Y))$ is an isomorphism, and so h^P is full.

For the second statement,

$$\omega(X) \simeq \text{Hom}(P, X) \simeq \text{Hom}(h^P(P), h^P(X)) = \text{Hom}(A, h^P(X)) \simeq h^P(X). \quad \square$$

As A is a finite k -algebra, its linear dual $C = A^\vee$ is a k -coalgebra, and to give a right A -module structure on a k -vector space is the same as giving a left C -comodule structure. Together with (11.36), this completes the proof in the case that $\mathbf{C} = \langle X \rangle$. Note that

$$A \stackrel{\text{def}}{=} \text{End}(P) \simeq \text{End}(h^P) \simeq \text{End}(\omega),$$

and so

$$C \simeq \text{End}(\omega)^\vee,$$

i.e., the coalgebra C is the k -linear dual of the algebra $\text{End}(\omega)$.

EXAMPLE 11.37. 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 \mathbf{C} to be $\text{Mod}(A)$, ω to the forgetful functor, and X to be A regarded as a left A -module, then

$$\text{End}(\omega|\langle X \rangle)^\vee \simeq A^\vee,$$

and the equivalence of categories $\mathbf{C} \rightarrow \text{Comod}(A^\vee)$ in (11.38 below) simply sends an A -module V to V with its canonical A^\vee -comodule structure. This is explained in detail in (11.42) and (11.43).

PROOF OF (11.33) IN THE GENERAL CASE

We now consider the general case. For an object X of \mathbf{C} , let $A_X = \text{End}(\omega|\langle X \rangle)$, 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

$$\langle X \rangle \rightarrow \text{Comod}(C_X).$$

Define a partial ordering on the set of isomorphism classes of objects in \mathbf{C} by the rule:

$$[X] \leq [Y] \text{ if } \langle X \rangle \subset \langle Y \rangle.$$

Note that $[X], [Y] \leq [X \oplus Y]$, so that we get a directed set, and that if $[X] \leq [Y]$, then restriction defines a homomorphism $A_Y \rightarrow A_X$. When we pass to the limit over the isomorphism classes, we obtain the following more precise form of the theorem.

THEOREM 11.38. *Let \mathbf{C} be an essentially small k -linear abelian category and let $\omega: \mathbf{C} \rightarrow \text{Vec}_k$ be a k -linear exact faithful functor. Let $C(\omega)$ be the k -coalgebra $\lim_{\rightarrow [X]} \text{End}(\omega|\langle X \rangle)^\vee$. For each object Y in \mathbf{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 $\mathbf{C} \rightarrow \text{Comod}(C(\omega))$.*

ASIDE 11.39. It is essential in Theorems 11.25 and 11.38 that \mathbf{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 \mathbf{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.

BIALGEBRAS

DEFINITION 11.40. A **bi-algebra** over k is a k -module with compatible structures of an associative algebra with identity and of a co-associative coalgebra with co-identity. In detail, a bi-algebra over k is a quintuple $(A, m, e, \Delta, \epsilon)$ where

- (a) (A, m, e) is an associative algebra over k with identity e ;
- (b) (A, Δ, ϵ) is a co-associative coalgebra over k with co-identity ϵ ;
- (c) $\Delta: A \rightarrow A \otimes A$ is a homomorphism of algebras;
- (d) $\epsilon: A \rightarrow k$ is a homomorphism of algebras.

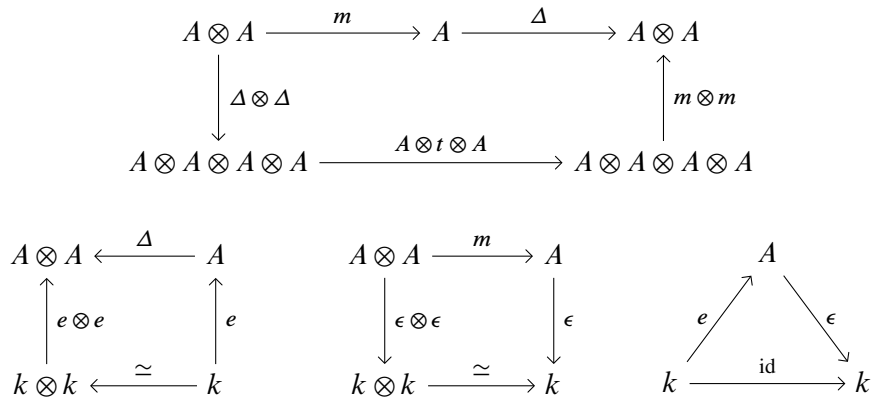
A **homomorphism** of bi-algebras $(A, m, \dots) \rightarrow (A', m', \dots)$ is a k -linear map $A \rightarrow A'$ that is both a homomorphism of k -algebras and a homomorphism of k -coalgebras.

The next proposition shows that the notion of a bi-algebra is self dual.

PROPOSITION 11.41. For a quintuple $(A, m, e, \Delta, \epsilon)$ satisfying (a) and (b) of (1.7), 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

11.42. Let A be a finite k -algebra (not necessarily commutative), and let R be a commutative k -algebra. Consider the functors

$$\text{Mod}(A) \xrightarrow[\text{forget}]{\omega} \text{Vec}(k) \xrightarrow[V \mapsto R \otimes_k V]{\phi_R} \text{Mod}(R).$$

For $M \in \text{ob}(\text{Mod}(A))$, let $M_0 = \omega(M)$. An element λ of $\text{End}(\phi_R \circ \omega)$ is a family of R -linear maps

$$\lambda_M: R \otimes_k M_0 \rightarrow R \otimes_k M_0,$$

functorial in M . An element of $R \otimes_k A$ defines such a family, and so we have a map

$$u: R \otimes_k A \rightarrow \text{End}(\phi_R \circ \omega),$$

which we shall show to be an isomorphism by defining an inverse β . Let $\beta(\lambda) = \lambda_A(1 \otimes 1)$. Clearly $\beta \circ u = \text{id}$, and so we only have to show $u \circ \beta = \text{id}$. The A -module $A \otimes_k M_0$ is a direct sum of copies of A , and the additivity of λ implies that $\lambda_{A \otimes_k M_0} = \lambda_A \otimes \text{id}_{M_0}$. The map $a \otimes m \mapsto am: A \otimes_k M_0 \rightarrow M$ is A -linear, and hence

$$\begin{array}{ccc} R \otimes_k A \otimes_k M_0 & \longrightarrow & R \otimes_k M \\ \downarrow \lambda_A \otimes \text{id}_{M_0} & & \downarrow \lambda_M \\ R \otimes_k A \otimes_k M_0 & \longrightarrow & R \otimes_k M \end{array}$$

commutes. Therefore

$$\lambda_M(1 \otimes m) = \lambda_A(1) \otimes m = (u \circ \beta(\lambda))_M(1 \otimes m) \text{ for } 1 \otimes m \in R \otimes M,$$

i.e., $u \circ \beta = \text{id}$.

11.43. Let C be a k -coalgebra, and let ω be the forgetful functor on $\text{Comod}(C)$. When C is finite over k , to give an object of $\text{Comod}(C)$ is essentially the same as giving a finitely generated module over the k -algebra $A = C^\vee$, and so (11.42) shows that

$$C \simeq \text{End}(\omega)^\vee.$$

In the general case,

$$C \simeq \varinjlim_{[X]} C_X \simeq \varinjlim_{[X]} \text{End}(\omega_C|_{\langle X \rangle})^\vee. \quad (60)$$

Let $u: C \rightarrow C'$ be a homomorphism of k -coalgebras. A coaction $V \rightarrow V \otimes C$ of C on V defines a coaction $V \rightarrow V \otimes C'$ of C' on V by composition with $\text{id}_V \otimes u$. Thus, u defines a functor $F: \text{Comod}(C) \rightarrow \text{Comod}(C')$ such that

$$\omega_{C'} \circ F = \omega_C. \quad (61)$$

LEMMA 11.44. *Every functor $F: \text{Comod}(C) \rightarrow \text{Comod}(C')$ satisfying (61) arises, as above, from a unique homomorphism of k -coalgebras $C \rightarrow C'$.*

PROOF. The functor F defines a homomorphism

$$\varinjlim_{[X]} \text{End}(\omega_{C'}|_{\langle FX \rangle}) \rightarrow \varinjlim_{[X]} \text{End}(\omega_C|_{\langle X \rangle}),$$

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

$$\varinjlim_{[X]} \text{End}(\omega_C|_{\langle X \rangle})^\vee \rightarrow \varinjlim_{[Y]} \text{End}(\omega_{C'}|_{\langle Y \rangle})^\vee$$

and hence a homomorphism $C \rightarrow C'$. This has the required property. \square

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 $m: C \otimes C \rightarrow C$ defines a functor

$$\phi^m: \text{Comod}(C) \times \text{Comod}(C) \rightarrow \text{Comod}(C)$$

sending (V, W) to $V \otimes W$ with the coaction

$$V \otimes W \xrightarrow{\rho_V \otimes \rho_W} V \otimes C \otimes W \otimes C \simeq V \otimes W \otimes C \otimes C \xrightarrow{V \otimes W \otimes m} V \otimes W \otimes C.$$

PROPOSITION 11.45. *The map $m \mapsto \phi^m$ defines a one-to-one correspondence between the set of k -coalgebra homomorphisms $m: C \otimes C \rightarrow C$ and the set of k -bilinear functors*

$$\phi: \text{Comod}(C) \times \text{Comod}(C) \rightarrow \text{Comod}(C)$$

such that $\phi(V, W) = V \otimes W$ as k -vector spaces.

- (a) *The homomorphism m is associative if and only if the canonical isomorphisms of vector spaces*

$$u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w: U \otimes (V \otimes W) \rightarrow (U \otimes V) \otimes W$$

are isomorphisms of C -comodules for all C -comodules U, V, W .

- (b) *The homomorphism m is commutative (i.e., $m(a, b) = m(b, a)$ for all $a, b \in C$) if and only if the canonical isomorphisms of vector spaces*

$$v \otimes w \mapsto w \otimes v: V \otimes W \rightarrow W \otimes V$$

are isomorphisms of C -comodules for all C -comodules W, V .

- (c) *There is an identity map $e: k \rightarrow C$ if and only if there exists a C -comodule U with underlying vector space k such that the canonical isomorphisms of vector spaces*

$$U \otimes V \simeq V \simeq V \otimes U$$

are isomorphisms of C -comodules for all C -comodules V .

PROOF. The pair $(\text{Comod}(C) \times \text{Comod}(C), \omega \otimes \omega)$, with $(\omega \otimes \omega)(X, Y) = \omega(X) \otimes \omega(Y)$ (as a k -vector space), satisfies the conditions of (11.38), 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 (11.44). The remaining statements involve only routine checking. \square

THEOREM 11.46. *Let \mathbf{C} be an essentially small k -linear abelian category, and let $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ be a k -bilinear functor. Let $\omega: \mathbf{C} \rightarrow \text{Vec}_k$ be a k -linear exact faithful functor such that*

- (a) $\omega(X \otimes Y) = \omega(X) \otimes \omega(Y)$ for all X, Y ;
 (b) the isomorphisms $\phi_{\omega X, \omega Y, \omega Z}$ and $\psi_{\omega X, \omega Y}$ live in \mathbf{C} for all X, Y, Z ;
 (c) there exists an (identity) object $\mathbf{1}$ in \mathbf{C} such that $\omega(\mathbf{1}) = k$ and the canonical isomorphisms

$$\omega(\mathbf{1}) \otimes \omega(X) \simeq \omega(X) \simeq \omega(X) \otimes \omega(\mathbf{1})$$

live in \mathbf{C} .

Let $C(\omega) = \varinjlim \text{End}(\omega|_{\langle X \rangle})^\vee$, so that ω defines an equivalence of categories $\mathbf{C} \rightarrow \text{Comod}(C(\omega))$ (Theorem 11.38). Then $C(\omega)$ has a unique structure (m, e) of a commutative k -bialgebra such that $\otimes = \phi^m$ and $\omega(\mathbf{1}) = (k \xrightarrow{e} C(\omega) \simeq k \otimes C(\omega))$.

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 11.45. \square

CATEGORIES OF REPRESENTATIONS OF AFFINE GROUPS

THEOREM 11.47. Let \mathbf{C} be an essentially small k -linear abelian category, let $\otimes: \mathbf{C} \times \mathbf{C} \rightarrow \mathbf{C}$ be a k -bilinear functor. Let ω be an exact faithful k -linear functor $\mathbf{C} \rightarrow \text{Vec}_k$ satisfying the conditions (a), (b), and (c) of (11.46). For each k -algebra R , let $G(R)$ be the set of families

$$(\lambda_V)_{V \in \text{ob}(\mathbf{C})}, \quad \lambda_V \in \text{End}_{R\text{-linear}}(\omega(V)_R),$$

such that

- ◇ $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$ for all $V, W \in \text{ob}(\mathbf{C})$,
- ◇ $\lambda_{\mathbf{1}} = \text{id}_{\omega(\mathbf{1})}$ for every identity object of $\mathbf{1}$ of \mathbf{C} , and
- ◇ $\lambda_W \circ \omega(u)_R = \omega(u)_R \circ \lambda_V$ for all arrows u in \mathbf{C} .

Then G is an affine monoid over k , and ω defines an equivalence of tensor categories,

$$\mathbf{C} \rightarrow \text{Rep}(G).$$

When ω satisfies the following condition, G is an affine group:

- (d) for any object X such that $\omega(X)$ has dimension 1, there exists an object X^{-1} in \mathbf{C} such that $X \otimes X^{-1} \approx \mathbf{1}$.

PROOF. Theorem 11.46 allows us to assume that $\mathbf{C} = \text{Comod}(C)$ 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 (11.42) we find that, for any k -algebra R ,

$$\underline{\text{End}}(\omega)(R) \stackrel{\text{def}}{=} \text{End}(\phi_R \circ \omega) = \varprojlim \text{Hom}_{k\text{-lin}}(C_X, R) = \text{Hom}_{k\text{-lin}}(C, R).$$

An element $\lambda \in \text{Hom}_{k\text{-lin}}(C_X, R)$ corresponds to an element of $\underline{\text{End}}(\omega)(R)$ commuting with the tensor structure if and only if λ is a k -algebra homomorphism; thus

$$\underline{\text{End}}^\otimes(\omega)(R) = \text{Hom}_{k\text{-alg}}(C, R) = G(R).$$

We have shown that $\underline{\text{End}}^\otimes(\omega)$ is representable by the affine monoid $G = \text{Spec } C$ and that ω defines an equivalence of tensor categories

$$\mathbf{C} \rightarrow \text{Comod}(C) \rightarrow \text{Rep}_k(G).$$

On applying (d) to the highest exterior power of an object of \mathbf{C} , we find that $\underline{\text{End}}^\otimes(\omega) = \underline{\text{Aut}}^\otimes(\omega)$, which completes the proof. \square

f. Properties of G versus those of $\text{Rep}_k(G)$: a summary

11.48. *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 $\text{Rep}_k(G) = \langle X \rangle$, then $G = \text{Spec}(B)$ where B is the linear dual of the finite k -algebra $A_X = \text{End}(\omega)$. See Section e.

11.49. *An algebraic group G is strongly connected if and only if, for every representation V on which G acts nontrivially, the full subcategory of $\text{Rep}(G)$ of subquotients of V^n , $n \geq 0$, is not stable under \otimes . In characteristic zero, a group is strongly connected if and only if it is connected.*

This follows from (11.48).

11.50. *An algebraic group G is unipotent (i.e., isomorphic to an algebraic subgroup of \mathbb{U}_n for some n) if and only if every simple representation is trivial (15.5).*

11.51. *An algebraic group G is trigonalizable (i.e., isomorphic to an algebraic subgroup of \mathbb{T}_n for some n) if and only if every simple representation has dimension 1 (17.2).*

This is the definition (17.1).

11.52. *A connected group variety G over an algebraically closed field is solvable if and only if it is trigonalizable (Lie-Kolchin theorem (17.33)).*

11.53. *Let G be a connected group variety. If $\text{Rep}(G)$ is semisimple, then G is pseudoreductive (22.19). In characteristic zero, $\text{Rep}(G)$ is semisimple if and only if G is reductive (22.138).*

The Lie algebra of an algebraic group

Recall that all algebraic groups are affine. In this chapter, a k -algebra is (as in Bourbaki) a k -vector space A equipped with a bilinear map $A \times A \rightarrow A$ (not necessarily associative, commutative, or finitely generated unless it is denoted by R).

a. Definition

DEFINITION 12.1. A **Lie algebra** over a field k is a vector space \mathfrak{g} over k together with a k -bilinear map

$$[\cdot, \cdot]: \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$$

(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 $u: \mathfrak{g} \rightarrow \mathfrak{g}'$ 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 (a) applied to $[x + y, x + y]$ shows that the Lie bracket is skew-symmetric,

$$[x, y] = -[y, x], \text{ for all } x, y \in \mathfrak{g}, \tag{62}$$

and that (62) allows us to rewrite the Jacobi identity as

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]] \tag{63}$$

or

$$[[x, y], z] = [x, [y, z]] - [y, [x, z]] \tag{64}$$

We shall be mainly concerned with finite-dimensional Lie algebras.

EXAMPLE 12.2. Let A be an associative k -algebra. 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 ij th position and 0 elsewhere. These matrices form a basis for \mathfrak{gl}_n , and

$$[e_{ij}, e_{i'j'}] = \delta_{j'i}e_{ij'} - \delta_{j'i}e_{i'j} \quad (\delta_{ij} = \text{Kronecker delta}).$$

EXAMPLE 12.3. Let A be a k -algebra (not necessarily associative or commutative). A **derivation** of A is a k -linear map $D: A \rightarrow A$ such that

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

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 $A \rightarrow A$ is a Lie subalgebra $\text{Der}_k(A)$ of \mathfrak{gl}_A .

DEFINITION 12.4. Let \mathfrak{g} be a Lie algebra. For a fixed x in \mathfrak{g} , the linear map

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

is called the **adjoint map** of x , and is denoted $\text{ad}_{\mathfrak{g}}(x)$ or $\text{ad}(x)$. The Jacobi identity (specifically (63)) implies 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

$$\text{ad}_{\mathfrak{g}}: \mathfrak{g} \rightarrow \text{Der}_k(\mathfrak{g})$$

is a homomorphism of Lie algebras. It is called the **adjoint representation**.

b. The Lie algebra of an algebraic group

12.5. The Lie algebra of an algebraic group G can be defined to be the tangent space of G at the neutral element e (A.47):

$$L(G) = \text{Ker}(G(k[\varepsilon]) \rightarrow G(k)), \quad \varepsilon^2 = 0. \quad (65)$$

Thus, an element of $L(G)$ is a homomorphism $\varphi: \mathcal{O}(G) \rightarrow k[\varepsilon]$ whose composite with $\varepsilon \mapsto 0: k[\varepsilon] \rightarrow k$ is the co-identity map $\epsilon: \mathcal{O}(G) \rightarrow k$. In particular, φ maps the augmentation ideal $I \stackrel{\text{def}}{=} \text{Ker}(\epsilon)$ into (ε) . As $\varepsilon^2 = 0$, φ factors through $\mathcal{O}(G)/I^2$. Now $\mathcal{O}(G)/I^2 \simeq k \oplus (I/I^2)$

(3.37), and φ sends $(a, b) \in k \oplus I/I^2$ to $a + D(b)\varepsilon$ with $D(b) \in k$. The map $\varphi \mapsto D$ is a bijection, and so

$$L(G) \simeq \text{Hom}(I/I^2, k) \quad (k\text{-linear maps}). \quad (66)$$

For definiteness, we *define* the Lie algebra of G to be

$$\text{Lie}(G) = \text{Hom}_{k\text{-linear}}(I/I^2, k). \quad (67)$$

Note that $\text{Lie}(G)$ is a k -vector space.

Following a standard convention, we write \mathfrak{g} for $\text{Lie}(G)$, \mathfrak{h} for $\text{Lie}(H)$, and so on.

12.6. For example,

$$L(\text{GL}_n) = \{I + A\varepsilon \mid A \in M_n(k)\}.$$

On the other hand, $\mathcal{O}(G)$ is the k -algebra of polynomials in the symbols $X_{11}, X_{12}, \dots, X_{nn}$ with $\det(X_{ij})$ inverted, and the ideal I consists of the polynomials without constant term; it follows that the k -vector space I/I^2 has basis

$$X_{11} + I^2, X_{12} + I^2, \dots, X_{nn} + I^2.$$

Therefore

$$\text{Hom}_{k\text{-linear}}(I/I^2, k) \simeq M_n(k).$$

The isomorphism $\text{Lie}(\text{GL}_n) \rightarrow L(\text{GL}_n)$ is $A \mapsto I + A\varepsilon$.

We define the bracket on $\text{Lie}(\text{GL}_n)$ to be

$$[A, B] = AB - BA. \quad (68)$$

Thus $\text{Lie}(\text{GL}_n) \simeq \mathfrak{gl}_n$. Regard $I + A\varepsilon$ and $I + B\varepsilon$ as elements of $G(k[\varepsilon])$ where now $k[\varepsilon] = k[X]/(X^3)$; then the commutator of $I + A\varepsilon$ and $I + B\varepsilon$ in $G(k[\varepsilon])$ is

$$\begin{aligned} & (I + A\varepsilon)(I + B\varepsilon)(I + A\varepsilon)^{-1}(I + B\varepsilon)^{-1} \\ &= (I + A\varepsilon)(I + B\varepsilon)(I - A\varepsilon + A^2\varepsilon^2)(I - B\varepsilon + B^2\varepsilon^2) \\ &= I + (AB - BA)\varepsilon^2 \end{aligned}$$

and so the bracket measures the failure of commutativity in $\text{GL}_n(k[\varepsilon])$ 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 (68) in the case of GL_n .

12.7. For example,

$$L(\mathbb{U}_n) = \left\{ \begin{pmatrix} 1 & \varepsilon c_{12} & \cdots & \varepsilon c_{1n-1} & \varepsilon c_{1n} \\ 0 & 1 & \cdots & \varepsilon c_{2n-1} & \varepsilon c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \varepsilon c_{n-1n} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \right\},$$

and

$$\text{Lie}(\mathbb{U}_n) \simeq \mathfrak{n}_n \stackrel{\text{def}}{=} \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \geq j\} \quad (\text{strictly upper triangular matrices}).$$

12.8. Let V be a finite-dimensional k -vector space. The Lie algebra of the algebraic group $V_{\mathfrak{a}}$ is V itself:

$$\text{Lie}(V_{\mathfrak{a}}) = V.$$

12.9. We write $e^{\varepsilon X}$ for the element of $L(G) \subset G(k[\varepsilon])$ corresponding to an element X of $\text{Lie}(G)$ under the isomorphism (66):

$$L(G) \simeq \text{Lie}(G).$$

For example, if $G = \text{GL}_n$, so $\text{Lie}(G) = \mathfrak{gl}_n$, then

$$e^{\varepsilon X} = I + \varepsilon X \quad (X \in M_n(k), e^{\varepsilon X} \in \text{GL}_n(k[\varepsilon])).$$

We have

$$\begin{aligned} e^{\varepsilon(X+X')} &= e^{\varepsilon X} \cdot e^{\varepsilon X'}, \quad X, X' \in \text{Lie}(G), \\ e^{\varepsilon(cX)} &= e^{(c\varepsilon)X}, \quad c \in k, \quad X \in \text{Lie}(G). \end{aligned}$$

The first equality expresses that $X \mapsto e^{\varepsilon X} : \text{Lie}(G) \rightarrow L(G)$ is a homomorphism of abelian groups, and the second that multiplication by c on $\text{Lie}(G)$ 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 12-1).

DEFINITION 12.10. Let G be an algebraic group over k , and let U be a vector group over k (2.11). An action of G on U defines an action of G on $\text{Lie}(U)$. The action is said to be **linear** if there exists a G -equivariant isomorphism of algebraic groups $U \simeq \text{Lie}(U)$.

Let V be a finite-dimensional vector space. An action of G on $V_{\mathfrak{a}}$ is linear if and only if it arises from a linear representation of G on V .

ASIDE 12.11. In characteristic zero, all actions are linear. Let G be a smooth algebraic group over a field k of characteristic $p \neq 0$, and let U be a vector group on which G acts. If the unipotent radical k is defined over k and the representation of G° on $\text{Lie}(U)$ is simple, then the action of G on U is linear. Without these conditions, there may be nonlinear representations [McNinch 2014](#).

c. Basic properties of the Lie algebra

12.12. The functor Lie maps finite inverse limits to finite inverse limits. For example, if

$$e \rightarrow G' \rightarrow G \rightarrow G''$$

is exact, then so also is

$$0 \rightarrow \text{Lie}(G') \rightarrow \text{Lie}(G) \rightarrow \text{Lie}(G'').$$

Indeed, with Lie replaced by L , the required sequence is the sequence of kernels in the exact commutative diagram

$$\begin{array}{ccccccc} e & \longrightarrow & G'(k[\varepsilon]) & \longrightarrow & G(k[\varepsilon]) & \longrightarrow & G''(k[\varepsilon]) \\ & & \downarrow & & \downarrow & & \downarrow \\ e & \longrightarrow & G'(k) & \longrightarrow & G(k) & \longrightarrow & G''(k). \end{array}$$

Similarly, if $G' \hookrightarrow G$, then $\text{Lie}(G') \hookrightarrow \text{Lie}(G)$. Moreover, Lie commutes with fibred products:

$$\text{Lie}(H_1 \times_G H_2) \simeq \text{Lie}(H_1) \times_{\text{Lie}(G)} \text{Lie}(H_2).$$

For example, if H_1 and H_2 are algebraic subgroups of an algebraic group G , then $\text{Lie}(H_1)$ and $\text{Lie}(H_2)$ are subspaces of $\text{Lie}(G)$ and

$$\text{Lie}(H_1 \cap H_2) = \text{Lie}(H_1) \cap \text{Lie}(H_2).$$

PROPOSITION 12.13. *Let $H \subset G$ be algebraic groups such that $\text{Lie}(H) = \text{Lie}(G)$. 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 (1.23). We have

$$\dim(H) = \dim(\mathfrak{h}) = \dim(\mathfrak{g}) \geq \dim(G) \geq \dim(H).$$

Because H is smooth, there is equality throughout. Now G is smooth because $\dim(\mathfrak{g}) = \dim(G)$, and it equals H because $\dim(G) = \dim(H)$ and G is smooth and connected. \square

12.14. As $\text{Lie}(G) = \text{Lie}(G^\circ)$, we need G to be connected in (12.13). In characteristic p , $\text{Lie}(\alpha_p) = \text{Lie}(\mathbb{G}_a)$, and so we need H to be smooth in (12.13).

12.15. Let H_1 and H_2 be algebraic subgroups of an algebraic group G . We say that H_1 and H_2 **cross transversally** in G if their Lie algebras cross transversally in the Lie algebra of G , i.e., if

$$\dim(\text{Lie}(H_1) \cap \text{Lie}(H_2)) = \dim(\text{Lie}(H_1)) + \dim(\text{Lie}(H_2)) - \dim(\text{Lie}(G)).$$

PROPOSITION 12.16. *Let H_1 and H_2 be smooth algebraic subgroups of an algebraic group G . If H_1 and H_2 cross transversally in G , then $H_1 \cap H_2$ is smooth.*

PROOF. We have

$$\begin{aligned} \dim(H_1) + \dim(H_2) - \dim(G) &\leq \dim(H_1 \cap H_2) && \text{(AG 5.36)} \\ &\leq \dim \text{Lie}(H_1 \cap H_2) && \text{(1.23)} \\ &= \dim \text{Lie}(H_1) \cap \text{Lie}(H_2) && \text{(12.12)} \\ &= \dim \text{Lie}(H_1) + \dim \text{Lie}(H_2) - \dim \text{Lie}(G) && \text{(hypothesis)}. \end{aligned}$$

As H_1 and H_2 are smooth,

$$\dim(H_1) + \dim(H_2) - \dim(G) \geq \dim \text{Lie}(H_1) + \dim \text{Lie}(H_2) - \dim \text{Lie}(G),$$

and so equality holds throughout. In particular, $\dim(H_1 \cap H_2) = \dim \text{Lie}(H_1 \cap H_2)$, and so $H_1 \cap H_2$ is smooth. \square

d. The adjoint representation; definition of the bracket

12.17. Let G be an algebraic group over k , and let R be a k -algebra. Define $\mathfrak{g}(R)$ by the exact sequence

$$1 \rightarrow \mathfrak{g}(R) \rightarrow G(R[\varepsilon]) \xrightarrow{\varepsilon \mapsto 0} G(R) \rightarrow 1. \quad (69)$$

Thus $\mathfrak{g}(k) = L(G)$. For example, let V be a k -vector space, and let $G = \text{GL}_V$. Let $V(\varepsilon) = R[\varepsilon] \otimes V$. Then $V(\varepsilon) = V_R \oplus \varepsilon V_R$ as an R -module, and

$$\mathfrak{g}(R) = \{\text{id} + \varepsilon\alpha \mid \alpha \in \text{End}(V_R)\}$$

where $\text{id} + \varepsilon\alpha$ acts on $V(\varepsilon)$ by

$$(\text{id} + \varepsilon\alpha)(x + \varepsilon y) = x + \varepsilon y + \varepsilon\alpha(x). \quad (70)$$

12.18. Recall (3.37) that we have a split-exact sequence of k -vector spaces

$$0 \rightarrow I \rightarrow \mathcal{O}(G) \xrightarrow{\epsilon} k \rightarrow 0$$

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

$$0 \rightarrow I_R \rightarrow \mathcal{O}(G)_R \xrightarrow{\epsilon_R} R \rightarrow 0.$$

By definition, an element of $\mathfrak{g}(R)$ is a homomorphism $\varphi: \mathcal{O}(G)_R \rightarrow R[\epsilon]$ whose composite with $R[\epsilon] \xrightarrow{\epsilon \mapsto 0} R$ is ϵ_R . As in (12.5), 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 . Hence

$$\mathfrak{g}(R) \simeq \text{Hom}_{R\text{-linear}}(I_R/I_R^2, R) \simeq \text{Hom}_{k\text{-linear}}(I/I^2, k) \otimes R \simeq \mathfrak{g}(k) \otimes R.$$

As in (12.9), we write $X \mapsto e^{\epsilon X}$ for the isomorphism $\mathfrak{g} \otimes R \rightarrow \mathfrak{g}(R)$. For a homomorphism $f: G \rightarrow H$,

$$f(e^{\epsilon X}) = e^{\epsilon \text{Lie}(f)(X)}, \quad \text{for } X \in \mathfrak{g} \otimes R. \quad (71)$$

This expresses that the isomorphism $\mathfrak{g} \otimes R \simeq \mathfrak{g}(R)$ is functorial in \mathfrak{g} .

12.19. The group $G(R[\epsilon])$ acts on $\mathfrak{g}(R)$ by inner automorphisms. As $G(R)$ is a subgroup of $G(R[\epsilon])$, it also acts. In this way, we get a homomorphism

$$G(R) \rightarrow \text{Aut}_{k\text{-linear}}(\mathfrak{g}(R)),$$

which is natural in R , and so defines a representation

$$\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}. \quad (72)$$

This is called the **adjoint representation** (or **action**) of G .

By definition,

$$x \cdot e^{\epsilon X} \cdot x^{-1} = e^{\epsilon \text{Ad}(x)X} \quad \text{for } x \in G(R), X \in \mathfrak{g} \otimes R. \quad (73)$$

For a homomorphism $f: G \rightarrow H$,

$$\begin{array}{ccc} G \times \mathfrak{g} & \xrightarrow{(x,X) \mapsto \text{Ad}(x)X} & \mathfrak{g} \\ f \times \text{Lie}(f) \downarrow & & \downarrow \text{Lie}(f) \\ H \times \mathfrak{h} & \xrightarrow{(y,Y) \mapsto \text{Ad}(y)Y} & \mathfrak{h} \end{array} \quad (74)$$

commutes, i.e.,

$$\text{Lie}(f)(\text{Ad}(x)X) = \text{Ad}(f(x))\text{Lie}(f)(X) \quad \text{for } x \in G(R), X \in \mathfrak{g} \otimes R.$$

Indeed,

$$e^{\epsilon \text{LHS}} \stackrel{(71)}{=} f(e^{\epsilon \text{Ad}(x)X}) \stackrel{(73)}{=} f(x \cdot e^{\epsilon X} \cdot x^{-1})$$

and

$$e^{\epsilon \text{RHS}} \stackrel{(73)}{=} f(x) \cdot e^{\epsilon \text{Lie}(f)(X)} \cdot f(x)^{-1},$$

which agree because of (71).

12.20. On applying the functor Lie to Ad, we get a homomorphism of k -vector spaces

$$\text{ad}: \mathfrak{g} \rightarrow \text{End}(\mathfrak{g}).$$

For $x, y \in \mathfrak{g}$, define

$$[x, y] = \text{ad}(x)(y). \quad (75)$$

This is the promised bracket.

THEOREM 12.21. *There is a unique functor Lie from the category of algebraic groups over k to the category of Lie algebras such that:*

- (a) $\text{Lie}(G) = \text{Hom}_{k\text{-linear}}(I_G/I_G^2, k)$ as a k -vector space;
- (b) the bracket on $\text{Lie}(\text{GL}_n) = \mathfrak{gl}_n$ is $[X, Y] = XY - YX$.

The action of G on itself by conjugation defines a representation $\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$ of G on \mathfrak{g} (as a k -vector space), whose differential is the adjoint representation $\text{ad}_{\mathfrak{g}}: \mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$ of \mathfrak{g} .

PROOF. The uniqueness follows from the fact that every algebraic group admits a faithful representation $G \rightarrow \text{GL}_n$ (4.8), which induces an injection $\mathfrak{g} \rightarrow \mathfrak{gl}_n$ (12.12). We have to show that the bracket (75) has the property (b). An element $I + \varepsilon A \in \text{Lie}(\text{GL}_n)$ acts on $M_n(k[\varepsilon])$ as

$$X + \varepsilon Y \mapsto (I + \varepsilon A)(X + \varepsilon Y)(I - \varepsilon A) = X + \varepsilon Y + \varepsilon(AX - XA). \quad (76)$$

On taking V to be $M_n(k)$ in (12.17), and comparing (76) with (70), we see that $\text{ad}(A)$ acts as $\text{id} + \varepsilon u$ with $u(X) = AX - XA$, as required. That Lie is a functor follows from the commutativity of (74). This completes the proof of the first statement.

The second statement is immediate from our definition of the bracket. \square

e. Description of the Lie algebra in terms of derivations

DEFINITION 12.22. Let A be a k -algebra and M an A -module. A k -linear map $D: A \rightarrow M$ is a k -derivation of A into M if

$$D(fg) = f \cdot D(g) + g \cdot D(f) \quad (\text{Leibniz rule}).$$

For example, $D(1) = D(1 \times 1) = D(1) + D(1)$, and so $D(1) = 0$. By linearity, this implies that

$$D(c) = 0 \text{ for all } c \in k.$$

Conversely, every additive map $A \rightarrow M$ satisfying the Leibniz rule and zero on k is a k -derivation.

Let $u: A \rightarrow k[\varepsilon]$ 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 $A \rightarrow k$ and, when we use u_0 to make k into an A -module, the second condition says that u_1 is a k -derivation $A \rightarrow k$.

Recall that $\mathcal{O}(G)$ has a co-algebra structure (Δ, ϵ) . By definition, the elements of $L(G)$ are the k -algebra homomorphisms $u: \mathcal{O}(G) \rightarrow k[\varepsilon]$ such that the composite of u with $\varepsilon \mapsto 0: k[\varepsilon] \rightarrow 0$ is ϵ , i.e., such that $u_0 = \epsilon$. Thus, we have proved the following statement.

PROPOSITION 12.23. *There is a natural one-to-one correspondence between the elements of $L(G)$ and k -derivations $\mathcal{O}(G) \rightarrow k$ (where $\mathcal{O}(G)$ acts on k through ϵ), i.e.,*

$$L(G) \simeq \text{Der}_{k,\epsilon}(\mathcal{O}(G), k).$$

The correspondence is $\epsilon + \epsilon D \leftrightarrow D$, 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 $\text{Der}_k(A, A)$ of k -derivations of A into A . The bracket

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

of two derivations is again a derivation. In this way, $\text{Der}_k(A, A)$ becomes a Lie algebra.

A derivation $D: A \rightarrow A$ is **left invariant** if

$$\Delta \circ D = (\text{id} \otimes D) \circ \Delta.$$

If D and D' are left invariant, then

$$\begin{aligned} \Delta \circ [D, D'] &= \Delta \circ (D \circ D' - D' \circ D) \\ &= (\text{id} \otimes D) \circ \Delta \circ D' - (\text{id} \otimes D') \circ \Delta \circ D \\ &= (\text{id} \otimes (D \circ D')) \circ \Delta - (\text{id} \otimes (D' \circ D)) \circ \Delta \\ &= (\text{id} \otimes [D, D']) \circ \Delta \end{aligned}$$

and so $[D, D']$ is left invariant.

PROPOSITION 12.24. *The map*

$$D \mapsto \epsilon \circ D: \text{Der}_k(A, A) \rightarrow \text{Der}_{k,\epsilon}(A, k)$$

defines an isomorphism from the subspace of left invariant derivations onto $\text{Der}_{k,\epsilon}(A, k)$.

PROOF. If D is a left invariant derivation $A \rightarrow A$, then

$$D = (\text{id} \otimes \epsilon) \circ \Delta \circ D = (\text{id} \otimes \epsilon) \circ (\text{id} \otimes D) \circ \Delta = (\text{id} \otimes (\epsilon \circ D)) \circ \Delta,$$

and so D is determined by $\epsilon \circ D$. Conversely, if $d: A \rightarrow k$ is a derivation, the $D = (\text{id} \otimes d) \circ \Delta$ is a left invariant derivation $A \rightarrow A$. \square

Thus $L(G)$ is isomorphic (as a k -vector space) to the space of left invariant derivations $A \rightarrow A$, which is a Lie subalgebra of $\text{Der}_k(A, A)$. 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 $G = \text{GL}_n$, and hence for all G .

f. Stabilizers

Let (V, r) be a representation of an algebraic group G , and let W be a subspace of V . Recall (4.3) that there exists an (unique) algebraic subgroup G_W of G such that

$$G_W(R) = \{\alpha \in G(R) \mid \alpha(W_R) = W_R\}$$

for all k -algebras R .

PROPOSITION 12.25. *With the above notations,*

$$\mathrm{Lie}(G_W) = \{x \in \mathrm{Lie}(G) \mid \mathrm{Lie}(r)(x)W \subset W\}.$$

PROOF. It suffices to prove this with $G = \mathrm{GL}_V$. Let $\mathrm{id} + \alpha\varepsilon \in \mathfrak{gl}_V$. Then $\mathrm{id} + \alpha\varepsilon \in \mathrm{Lie}(G_W)$ if and only if $\mathrm{id} + \alpha\varepsilon \in G_W(k[\varepsilon])$, i.e.,

$$(\mathrm{id} + \alpha\varepsilon)W[\varepsilon] \subset W[\varepsilon].$$

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 $\alpha w_0 \in W$. \square

REMARK 12.26. Let $\mathfrak{g} \rightarrow \mathfrak{gl}(V)$ be a representation of the Lie algebra \mathfrak{g} , and let W be a subspace of V . Define

$$\mathrm{Stab}_{\mathfrak{g}}(W) = \{x \in \mathfrak{g} \mid xW \subset W\}.$$

A representation $r: G \rightarrow \mathrm{GL}_V$ defines a representation $dr: \mathfrak{g} \rightarrow \mathfrak{gl}(V)$, and (12.25) says that

$$\mathrm{Lie}(\mathrm{Stab}_G(W)) = \mathrm{Stab}_{\mathfrak{g}}(W).$$

For example, in the situation of Chevalley's Theorem 4.19, on applying Lie to

$$H = \mathrm{Stab}_G(L)$$

we find that

$$\mathfrak{h} = \mathrm{Stab}_{\mathfrak{g}}(L).$$

PROPOSITION 12.27. *Let G be an algebraic group over k , let S be a k -algebra, and let J be an ideal in S such that $J^2 = 0$. The kernel of*

$$G(S) \rightarrow G(S/J)$$

is canonically isomorphic to $\mathfrak{g} \otimes J$.

PROOF. When $S = k[\varepsilon]$ and $J = (\varepsilon)$, this is the isomorphism (66)

$$\mathrm{Ker}(G(k[\varepsilon]) \rightarrow G(k)) \simeq \mathrm{Hom}(I/I^2, k).$$

In the general case, an element of the kernel is a homomorphism $\varphi: \mathcal{O}(G) \rightarrow S$ making the diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{\varphi} & S \\ \downarrow \epsilon & & \downarrow \\ k & \longrightarrow & S/J \end{array}$$

commute. Because $J^2 = 0$, such a homomorphism factors uniquely through $\mathcal{O}(G)/I^2 \simeq k \oplus I/I^2$. Thus, to give an element of the kernel is the same as giving a homomorphism $\varphi': k \oplus I/I^2 \rightarrow S$ making the diagram

$$\begin{array}{ccc} k \oplus I/I^2 & \xrightarrow{\varphi'} & S \\ \downarrow \epsilon & & \downarrow \\ k & \longrightarrow & S/J \end{array}$$

commute. This condition means that $\varphi'(c, x) = c + D(x)$ with $D \in \text{Hom}_{k\text{-linear}}(I/I^2, J)$. The map $\varphi \mapsto D$ is an isomorphism of the kernel onto

$$\text{Hom}(I/I^2, J) \simeq \text{Hom}(I/I^2, k) \otimes J = \mathfrak{g} \otimes J. \quad \square$$

COROLLARY 12.28. *Let G be an algebraic group over k , let S be a k -algebra, and let J be an ideal in S with $J^2 = 0$. There is an exact sequence*

$$0 \rightarrow J \otimes \mathfrak{g} \otimes R \rightarrow G(S \otimes R) \xrightarrow{\text{can.}} G(S \otimes R/J \otimes R)$$

natural in the k -algebra R .

PROOF. Apply (12.27) to the ideal $J \otimes R$ in $S \otimes R$. \square

COROLLARY 12.29. *Let G/k , S , and J be as in the statement of the proposition. If G is smooth or there exists a section to $S \rightarrow S/J$, then there is a canonical exact sequence*

$$0 \rightarrow (\mathfrak{g} \otimes J)_{\mathfrak{a}} \rightarrow \Pi_{S/k} G_S \rightarrow \Pi_{(S/J)/k} G_{S/J} \rightarrow 0.$$

PROOF. Let R be a k -algebra. If G is smooth or there exists a section to $S \rightarrow S/J$, then the canonical map $G(S \otimes R) \rightarrow G(S \otimes R/J \otimes R)$ is surjective. Thus the statement follows from (12.28). \square

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 12.30. *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 $\text{Lie}(Z(G)) = z(\mathfrak{g})$.

PROOF. There are maps

$$\text{Ad}: G \rightarrow \text{Aut}(\mathfrak{g}), \quad \text{Ker}(\text{Ad}) \supset Z(G) \tag{77}$$

$$\text{ad}: \mathfrak{g} \rightarrow \text{Der}(\mathfrak{g}), \quad \text{Ker}(\text{ad}) = z(\mathfrak{g}). \tag{78}$$

The second map is obtained by applying Lie to the first (see 12.21), and so (see 12.12)

$$\text{Ker}(\text{ad}) = \text{Lie}(\text{Ker}(\text{Ad})).$$

Therefore

$$\dim z(\mathfrak{g}) = \dim \text{Ker}(\text{ad}) = \dim \text{Lie}(\text{Ker}(\text{Ad})) \stackrel{(1.23)}{\geq} \dim \text{Ker}(\text{Ad}) \stackrel{(77)}{\geq} \dim Z(G), \tag{79}$$

which proves the first part of the statement.

If $\dim z(\mathfrak{g}) = \dim Z(G)$, then

$$\dim \text{Ker}(\text{ad}) = \dim \text{Ker}(\text{Ad}) = \dim Z(G).$$

The first equality implies that Ker Ad is smooth (1.23), and the second equality implies that $Z(G)^{\circ} = (\text{Ker Ad})^{\circ}$. Hence $Z(G)^{\circ}$ is smooth, which implies that $Z(G)$ is smooth. Finally, $\text{Lie}(Z(G)) \subset z(\mathfrak{g})$, and so they are equal if they have the same dimension. \square

h. Normalizers and centralizers

PROPOSITION 12.31. *Let G be an algebraic group, and let H be an algebraic subgroup of G . The action of H on G by conjugation defines an action of H on $\mathrm{Lie}(G)$, and*

$$\begin{aligned}\mathrm{Lie}(C_G(H)) &= \mathrm{Lie}(G)^H \\ \mathrm{Lie}(N_G(H))/\mathrm{Lie}(H) &= (\mathrm{Lie}(G)/\mathrm{Lie}(H))^H.\end{aligned}$$

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

$$x \cdot (e^{\varepsilon X})_S \cdot x^{-1} = (e^{\varepsilon X})_S \text{ for all } k[\varepsilon]\text{-algebras } S \text{ and } x \in H(S), \quad (80)$$

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

$$y \cdot e^{\varepsilon' X_R} \cdot y^{-1} = e^{\varepsilon' X_R} \text{ for all } k\text{-algebras } R \text{ and } y \in H(R), \quad (81)$$

where X_R is the image of X in $\mathfrak{g} \otimes R$.

We show that (80) \implies (81). Let $y \in H(R)$ for some k -algebra R . Take $S = R[\varepsilon]$. Then $y \in H(R) \subset H(S)$, and (80) for $y \in H(S)$ implies (81) for $y \in H(R)$.

We show that (81) \implies (80). Let $x \in H(S)$ for some $k[\varepsilon]$ -algebra S ; there is a $k[\varepsilon]$ -homomorphism $\varphi: S[\varepsilon'] \rightarrow S$ acting as the identity on S and sending ε' to $\varepsilon 1_S$. On taking $R = S$ in (81), and applying φ , we obtain (80).

The proof of the second statement uses similar arguments (SHS, Exposé 4, 3.4, p.185). \square

COROLLARY 12.32. *If H is commutative and $\mathfrak{g}^H \rightarrow (\mathfrak{g}/\mathfrak{h})^H$ is surjective, then $\mathrm{Lie}(C_G(H)) = \mathrm{Lie}(N_G(H))$.*

PROOF. Because H is commutative, (81) holds for all $X \in \mathfrak{h}$, and so $\mathfrak{h} = \mathfrak{h}^H \subset \mathfrak{g}^H$. From the exact sequence

$$0 \rightarrow \mathfrak{h} \rightarrow \mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h} \rightarrow 0,$$

we get an exact sequence

$$0 \rightarrow \mathfrak{h}^H \rightarrow \mathfrak{g}^H \rightarrow (\mathfrak{g}/\mathfrak{h})^H.$$

Using (12.31), we can rewrite this as

$$0 \rightarrow \mathfrak{h} \rightarrow \mathrm{Lie}(C_G(H)) \rightarrow \mathrm{Lie}(N_G(H))/\mathfrak{h}.$$

Therefore the surjectivity of $\mathfrak{g}^H \rightarrow (\mathfrak{g}/\mathfrak{h})^H$ implies that of $\mathrm{Lie}(C_G(H)) \rightarrow \mathrm{Lie}(N_G(H))$. \square

COROLLARY 12.33. *Let H be a commutative algebraic subgroup of an algebraic group G . If $\mathfrak{g}^H \rightarrow (\mathfrak{g}/\mathfrak{h})^H$ is surjective and $C_G(H)$ is smooth, then $C_G(H)$ is open in $N_G(H)$.*

PROOF. The hypothesis implies that $\mathrm{Lie}(C_G(H)) = \mathrm{Lie}(N_G(H))$ (12.32), and therefore $C_G(H)^\circ = N_G(H)^\circ$ (12.13). \square

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 that $\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$ need not be smooth.

12.34. 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

$$\begin{aligned} X: A(a, b) &\mapsto a - 1 \\ Y: A(a, b) &\mapsto b. \end{aligned}$$

Then $\mathcal{O}(G) = k[X, Y, (X + 1)^{-1}]$, which is an integral domain, and so G is connected and smooth. Note that

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a' & 0 & 0 \\ 0 & a'^p & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a' & 0 & 0 \\ 0 & a'^p & b - a'^p b + a^p b' \\ 0 & 0 & 1 \end{pmatrix},$$

and so the centre of G consists of the elements $A(a, b)$ with $a^p = 1$ and $b = 0$. Therefore

$$\mathcal{O}(Z(G)) = \mathcal{O}(G)/(X^p - 1, Y) \simeq k[X]/(X^p - 1),$$

which is not reduced (it equals μ_p). In particular, G is not commutative. However $\text{Lie}(G)$ is commutative. The kernel of $\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$ consists of the elements $A(a, b)$ with $a^p = 1$, and so equals $\text{Spm}(k[G]/(X^p - 1))$, which is not reduced; therefore Ad is not smooth. In this case,

$$\dim z(\mathfrak{g}) = 2 > \dim(\text{Ker}(\text{Ad})) = 1 > \dim(Z(G)) = 0$$

— all of the inequalities in (79) are strict.

j. The universal enveloping algebra

Recall (12.2) that an associative k -algebra A becomes a Lie algebra $[A]$ with the bracket $[a, b] = ab - ba$. Let \mathfrak{g} be a Lie algebra. Among the pairs consisting of an associative k -algebra A and a Lie algebra homomorphism $\mathfrak{g} \rightarrow [A]$, there is one, $(U(\mathfrak{g}), \mathfrak{g} \xrightarrow{\rho} [U(\mathfrak{g})])$, that is universal:

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{\rho} & U(\mathfrak{g}) \\ \text{Lie} \searrow & & \downarrow \exists! \text{ associative} \\ & & A \end{array} \quad \left\{ \begin{array}{l} \text{Hom}(\mathfrak{g}, [A]) \simeq \text{Hom}(U(\mathfrak{g}), A). \\ \alpha \circ \rho \leftrightarrow \alpha \end{array} \right.$$

In other words, every Lie algebra homomorphism $\mathfrak{g} \rightarrow [A]$ extends uniquely to a homomorphism of associative algebras $U(\mathfrak{g}) \rightarrow A$. 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 k -algebra structure defined by

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

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

$$x \otimes y - y \otimes x - [x, y], \quad x, y \in \mathfrak{g}. \quad (82)$$

The extension of a k -linear map $\alpha: \mathfrak{g} \rightarrow A$ to a k -algebra homomorphism $T(\mathfrak{g}) \rightarrow A$ factors through $U(\mathfrak{g})$ if and only if α is a Lie algebra homomorphism $\mathfrak{g} \rightarrow [A]$. Therefore $U(\mathfrak{g})$ and the map $\mathfrak{g} \rightarrow [U(\mathfrak{g})]$ have the required universal property.

When \mathfrak{g} is commutative, (82) 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 k -algebra $U(\mathfrak{g})$ is generated by the image of any k -vector space basis for \mathfrak{g} (because this is true for $T(\mathfrak{g})$). In particular, $U(\mathfrak{g})$ is finitely generated if \mathfrak{g} is finite-dimensional.

THEOREM 12.35 (POINCARÉ, BIRKHOFF, WITT). *Let $(e_i)_{i \in I}$ be an ordered basis for \mathfrak{g} as a k -vector space, and let $\varepsilon_i = \rho(e_i)$. Then the ordered monomials*

$$\varepsilon_{i_1} \varepsilon_{i_2} \cdots \varepsilon_{i_n}, \quad i_1 \leq i_2 \leq \cdots \leq i_n, \quad (83)$$

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

For example, if \mathfrak{g} is finite-dimensional with basis $\{e_1, \dots, e_r\}$ as a k -vector space, then the monomials

$$\varepsilon_1^{m_1} \varepsilon_2^{m_2} \cdots \varepsilon_r^{m_r}, \quad m_1, \dots, m_r \in \mathbb{N},$$

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 $\varepsilon_1, \dots, \varepsilon_r$.

As $U(\mathfrak{g})$ is generated as a k -algebra by (ε_i) , it is generated as a k -vector space by the monomials $\varepsilon_{i_1} \varepsilon_{i_2} \cdots \varepsilon_{i_m}$, $m \in \mathbb{N}$. The relations implied by (82),

$$xy = yx + [x, y]$$

allow one to “reorder” the factors in such a term, and deduce that the ordered monomials (83) span $U(\mathfrak{g})$; the import of the theorem is that the set is linearly independent. The proof of this can’t be too easy — for example, it must use the Jacobi identity.

PROOF OF THE PBW THEOREM

Choose a basis \mathcal{B} for \mathfrak{g} and a total ordering of \mathcal{B} . The monomials

$$x_1 \otimes x_2 \otimes \cdots \otimes x_m, \quad x_i \in \mathcal{B}, \quad m \in \mathbb{N}, \quad (84)$$

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 the elements (82). 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 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 $\sigma_{r,s}: T(\mathfrak{g}) \rightarrow T(\mathfrak{g})$ 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 $T \rightarrow T'$ 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 let S be 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 $\sigma_{r,s}(T) < T$. \square

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 $T \rightarrow T_1 \rightarrow T_2 \rightarrow \cdots$ 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 $U(\mathfrak{g})$. \square

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

$$A \otimes x \otimes y \otimes B - A \otimes y \otimes x \otimes B - A \otimes [x, y] \otimes B, \quad x, y \in \mathcal{B}, \quad x > y, \quad A, B \text{ monomials.}$$

By considering the terms with $\deg(A)$ a maximum, one sees that T cannot be reduced. \square

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 $A \rightarrow B_1$ and $A \rightarrow B_2$ have the form

$$\begin{aligned} \underline{x \otimes y} \otimes z &\rightarrow y \otimes x \otimes z + [x, y] \otimes z \\ x \otimes \underline{y \otimes z} &\rightarrow x \otimes z \otimes y + x \otimes [y, z]. \end{aligned}$$

But,

$$\begin{aligned} y \otimes \underline{x \otimes z} + [x, y] \otimes z &\rightarrow \underline{y \otimes z} \otimes x + y \otimes [x, z] + [x, y] \otimes z \\ &\rightarrow z \otimes y \otimes x + [y, z] \otimes x + y \otimes [x, z] + [x, y] \otimes z \end{aligned}$$

and

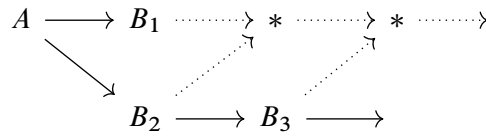
$$\begin{aligned} \underline{x \otimes z} \otimes y + x \otimes [y, z] &\rightarrow z \otimes \underline{x \otimes y} + [x, z] \otimes y + x \otimes [y, z] \\ &\rightarrow z \otimes y \otimes x + z \otimes [x, y] + [x, z] \otimes y + x \otimes [y, z]. \end{aligned}$$

The terms on the right differ by

$$[[y, z], x] + [y, [x, z]] + [[x, y], z],$$

which, because of the Jacobi identity (12.1b), 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 $\text{red}(T) = T'$.

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 $\text{red}(S + T) = \text{red}(S) + \text{red}(T)$.*

PROOF. Let $W = \sigma(S + T)$ be a reduced reduction of $S + T$. It suffices to show that

$$W = \text{red}(S) + \text{red}(T).$$

There exists a reduction σ' such that $\sigma'(\sigma(S)) = \text{red}(S)$. Now

$$\sigma'(\sigma(S + T)) = \sigma'(W) = W$$

because W is reduced, and

$$\sigma'(\sigma(S + T)) = \sigma'(\sigma(S)) + \sigma'(\sigma(T)) = \text{red}(S) + (\sigma'\sigma)(T).$$

Let σ'' be such that $\sigma''(\sigma'\sigma)(T) = \text{red}(T)$. Then

$$W = \sigma''(W) = \sigma''(\text{red}(S)) + \sigma''(\sigma'\sigma(T)) = \text{red}(S) + \text{red}(T). \quad \square$$

An induction argument now shows that every T in $T(\mathfrak{g})$ is uniquely reducible.

STEP 7. *The map $T \mapsto \text{red}(T): T(\mathfrak{g}) \rightarrow T(\mathfrak{g})$ is k -linear and has the following properties:*

- (a) $T - \text{red}(T) \in I(\mathfrak{g})$;
- (b) $\text{red}(T) = T$ if T is reduced;
- (c) $\text{red}(T) = 0$ 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 $\text{red}(T)$ is a reduction of T (see Step 1). For (c), if $T \in I(\mathfrak{g})$ then $\text{red}(T)$ is reduced and lies in $I(\mathfrak{g})$, and so is zero (Step 3). □

STEP 8. *Completion of the proof.*

PROOF. Let $T(\mathfrak{g})_{\text{red}}$ denote the k -subspace of $T(\mathfrak{g})$ consisting of reduced tensors. The map red is a k -linear projection onto $T(\mathfrak{g})_{\text{red}}$ with kernel $I(\mathfrak{g})$:

$$T(\mathfrak{g}) \simeq I(\mathfrak{g}) \oplus T(\mathfrak{g})_{\text{red}} \quad (\text{as } k\text{-vector spaces}). \quad \square$$

REMARK 12.36. The proof shows that the universal enveloping algebra $U(\mathfrak{g})$ of \mathfrak{g} can be identified with the k -vector subspace $T(\mathfrak{g})_{\text{red}}$ equipped with the multiplication

$$T \cdot T' = \text{red}(T \otimes T').$$

ASIDE 12.37. From [Bergman 1978](#):

[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.

ASIDE 12.38. It is an open question whether $U(\mathfrak{g}) \approx U(\mathfrak{g}')$ implies $\mathfrak{g} \approx \mathfrak{g}'$ ([Bergman 1978](#)).

NOTES. The above proof of the PBW theorem follows notes of Casselman (Introduction to Lie Algebras, www.math.ubc.ca/~cass/) and [Bergman 1978](#).

k. The universal enveloping p -algebra

Throughout this section, $\text{char}(k) = p \neq 0$. Let x_0 and x_1 be elements of a Lie algebra \mathfrak{g} . For $0 < r < p$, let

$$s_r(x_0, x_1) = -\frac{1}{r} \sum_u \text{ad}_{x_{u(1)}} \text{ad}_{x_{u(2)}} \cdots \text{ad}_{x_{u(p-1)}}(x_1)$$

where u runs over the maps $\{1, 2, \dots, p-1\} \rightarrow \{0, 1\}$ taking the value 0 exactly r times. For example, $s_1(x_0, x_1)$ equals $[x_0, x_1]$ for $p = 2$ and $[x_1, [x_1, x_0]]$ for $p = 3$.

PROPOSITION 12.39. Let A be an associative k -algebra (not necessarily commutative). For $a, b \in A$, write

$$\text{ad}(a)b = [a, b] = ab - ba.$$

Then the Jacobson formulas hold for $a, b \in A$:

- (a) $\text{ad}(a)^p = \text{ad}(a^p)$
- (b) $(a+b)^p = a^p + b^p + \sum_{0 < r < p} s_r(a, b)$.

PROOF. When we put

$$L_a(b) = ab = R_b(a),$$

we find that

$$\text{ad}(a^p)(b) = (L_a^p - R_a^p)(b) = (L_a - R_a)^p(b) = \text{ad}(a)^p(b),$$

which proves (a).

We claim that, for $a_1, \dots, a_p \in A$,

$$\sum_{s \in S_p} a_{s(1)} \cdots a_{s(p)} = \sum_{t \in S_{p-1}} \text{ad}(a_{t(1)}) \cdots \text{ad}(a_{t(p-1)})(a_p). \quad (85)$$

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_1, \dots, i_r) runs over the strictly increasing sequences of integers in the interval $[1, p-1]$, and where (j_1, \dots, j_{p-1-r}) denotes the strictly increasing sequence whose values are integers in $[1, p-1]$ distinct from i_1, \dots, 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 (85).

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 $[1, p]$ into $\{0, 1\}$ taking the value 0 exactly r times. For $s \in S_p$, let $w_s \in F(r)$ denote the map such that $w_s^{-1}(0) = \{s^{-1}(1), \dots, s^{-1}(r)\}$. Then $s \mapsto w_s$ is a surjective map such that the inverse image of each $w \in F(r)$ contains of $r!(p-r)!$ elements. Putting

$$\begin{aligned} a_1 &= \cdots = a_r = x_0 \\ a_{r+1} &= \cdots = a_p = x_1 \end{aligned}$$

we therefore have

$$x_{w_s(1)} \cdots x_{w_s(p)} = a_{s(1)} \cdots a_{s(p)}$$

and

$$\sum_{w \in F(r)} x_{w(1)} \cdots x_{w(p)} = \frac{1}{r!(p-r)!} \sum_{s \in S_p} a_{s(1)} \cdots a_{s(p)}.$$

By the same method, we obtain

$$s_r(x_0, x_1) = \left(-\frac{1}{r}\right) \frac{1}{r!(p-r-1)!} \sum_{t \in S_{p-1}} \text{ad}(a_{t(1)}) \cdots \text{ad}(a_{t(p-1)})(a_p).$$

The required formula now follows from (85). \square

DEFINITION 12.40. A p -Lie algebra is a Lie algebra \mathfrak{g} equipped with a map

$$x \mapsto x^{[p]}: \mathfrak{g} \rightarrow \mathfrak{g}$$

such that

- (a) $(cx)^{[p]} = c^p x^{[p]}$, all $c \in k$, $x \in \mathfrak{g}$;
- (b) $\text{ad}(x^{[p]}) = (\text{ad}(x))^p$, all $x \in \mathfrak{g}$;
- (c) $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{r=1}^{p-1} s_r(x, y)$.

The term $r \cdot s_r(x, y)$ is the coefficient of c^r in $\text{ad}(cx + y)^{p-1}(y)$. Note that (12.39) says that $[A]$ becomes a p -Lie algebra with $a^{[p]} = a^p$.

Let \mathfrak{g} be a p -Lie algebra, and let $\varphi: \mathfrak{g} \rightarrow U(\mathfrak{g})$ be the universal map. The elements $\varphi(x)^{[p]} - \varphi(x^{[p]})$ 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 $\mathfrak{g} \rightarrow U(\mathfrak{g}) \rightarrow U^{[p]}(\mathfrak{g})$. Then j is a homomorphism of p -Lie algebras, and the pair $(U^{[p]}(\mathfrak{g}), j)$ is universal: every k -linear map $\alpha: \mathfrak{g} \rightarrow A$ with A associative extends uniquely to a k -algebra homomorphism $T(\mathfrak{g}) \rightarrow A$, which factors through $U^{[p]}(\mathfrak{g})$ if and only if it is a p -Lie algebra homomorphism,

$$\begin{array}{ccc}
 \mathfrak{g} & \xrightarrow{\text{p-Lie}} & U^{[p]}(\mathfrak{g}) \\
 & \searrow j & \downarrow \text{\textcircled{!} associative} \\
 & & A \\
 & \swarrow \text{p-Lie} & \\
 & &
 \end{array}
 \quad \left\{ \begin{array}{l} \text{Hom}(\mathfrak{g}, [A]) \simeq \text{Hom}(U^{[p]}(\mathfrak{g}), A) \\ \alpha \circ j \leftrightarrow \alpha \end{array} \right.$$

The functor $\mathfrak{g} \mapsto U^{[p]}(\mathfrak{g})$ is left adjoint to the functor sending an associative k -algebra to its associated p -Lie algebra.

THEOREM 12.41. 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 $U(\mathfrak{g}) \rightarrow U^{[p]}(\mathfrak{g})$. Let U_{p-1} denote the subspace of $U(\mathfrak{g})$ generated by the monomials $\prod e_i^{m_i}$ with $\sum m_i \leq p-1$. As $c_i \equiv e_i^p$ modulo U_{p-1} , the PBW theorem (12.35) implies that the monomials

$$\prod e_i^{n_i} \prod c_i^{m_i}, \quad 0 \leq n_i < p, \quad m_i \geq 0$$

form a basis for $U(\mathfrak{g})$, from which the statement follows. □

COROLLARY 12.42. If \mathfrak{g} is finite-dimensional as a k -vector space, so also if $U^{[p]}(\mathfrak{g})$, and the map $j: \mathfrak{g} \rightarrow U^{[p]}(\mathfrak{g})$ is injective.

PROOF. Obvious from the theorem. □

NOTES. The exposition in this section follows that in DG II, §7, especially 3.2, p.275; 3.5, p.277.

Exercises

EXERCISE 12-1. A nonzero element c of k defines an endomorphism of $k[\varepsilon]$ sending 1 to 1 and 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 $\mathrm{Lie}(G) \stackrel{\mathrm{def}}{=} \mathrm{Hom}(I/I^2, k) \simeq L(G)$.

EXERCISE 12-2. Let G be the orthogonal group, so that

$$G(R) = \{X \in M_n(R) \mid X^t \cdot X = I\}.$$

Show that the Lie algebra of G is

$$\mathfrak{g} = \{I + \varepsilon Y \in M_n(k) \mid Y^t + Y = 0\}$$

and that the adjoint representation is given by

$$\mathrm{Ad}(g)(Y) = gYg^{-1}.$$

Show that

$$X \mapsto (I - X)(I + X)^{-1}$$

defines a birational isomorphism $\lambda: G \dashrightarrow \mathfrak{g}$ and that it 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. (Assume k has characteristic zero. The partial inverse is $Y \mapsto (I - Y)(I + Y)^{-1}$.)

ASIDE 12.43. 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 equivariant for the action of G on G by conjugation and the adjoint action of G on \mathfrak{g} . The Cayley map for the orthogonal group (12-2) was found by Cayley (J. Reine. Angew. Math. 32 (1846), 119-123). 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, Popov, Reichstein, J. Amer. Math. Soc. 19 (2006), no. 4, 921–967 (also [mo101322](#)). The Cayley map, when it exists, gives an explicit realization of the group as a rational variety. See also: Borovoi, Mikhail; Kunyavskii, Boris; Lemire, Nicole; Reichstein, Zinovy Stably Cayley groups in characteristic zero. Int. Math. Res. Not. IMRN 2014, no. 19, 5340–5397.

Finite group schemes

In this chapter we study finite algebraic groups. As a finite algebraic group is étale unless the base field has characteristic $p \neq 0$ and p divides the order of the group, this is largely a study of p -phenomena in characteristic p . Those not interested in such things can skip the chapter.

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 prefer to write this as “finite group scheme”.

a. Generalities

PROPOSITION 13.1. *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 finite; (d) $\text{spm}(A)$ 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) \Leftrightarrow (c). According to the Noether normalization theorem, there exist algebraically independent elements x_1, \dots, x_r in A such that A is finite over $k[x_1, \dots, x_r]$. Clearly

$$A \text{ is finite over } k \iff r = 0 \iff A \text{ has Krull dimension } 0.$$

(d) \Rightarrow (b). Let \mathfrak{m} be such that $\{\mathfrak{m}\}$ is open in $\text{spm}(A)$. There exists an $f \in A$ such that $\text{spm}(A_f) = \{\mathfrak{m}\}$. 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 13.10). 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} . Since this is true of all maximal ideals in A , it follows that A has dimension zero.

(a) \Rightarrow (d). Because A is artinian, it has only finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_r$, and some product $\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r} = 0$ (CA §16). Now the Chinese remainder theorem shows that

$$A \simeq A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_r^{n_r}$$

and so

$$\text{spm}(A) = \bigsqcup \text{spm}(A/\mathfrak{m}_i^{n_i}) = \bigsqcup \{\mathfrak{m}_i\} \quad (\text{disjoint union of open one-point sets}).$$

Therefore, $\text{spm}(A)$ is discrete. □

PROPOSITION 13.2. *The following conditions on an algebraic group G over k are equivalent: (a) G is affine and $\mathcal{O}(G)$ is artinian; (b) G has dimension zero; (c) the morphism $G \rightarrow \mathrm{Spm} k$ is finite; (d) $|G|$ is discrete (in which case it is finite).*

PROOF. The implications (a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) follow immediately from (13.1). It remains to prove (d) \Rightarrow (a). Assume that $|G|$ is discrete, and write G as a finite union of open affines, $G = \bigcup_i U_i$. Then U_i is discrete, and so $U_i = \mathrm{Spm}(A_i)$ with A_i artinian. It follows that $|G|$ is a finite set of open-closed one-point subsets u_i , and that $\mathcal{O}_G(u_i)$ is a local artinian ring A_i . Now $G = \mathrm{Spm}(\prod A_i)$, which is affine with coordinate ring the artinian ring $\prod A_i$. \square

DEFINITION 13.3. An algebraic group G over k is finite if G is finite as a scheme over k . This means that G is affine and $\mathcal{O}(G)$ is a finite k -algebra. The dimension of $\mathcal{O}(G)$ as a k -vector space is called the order $o(G)$ of G .

PROPOSITION 13.4. *Let G be a finite group scheme over k . There is a unique exact sequence*

$$e \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow e$$

with G° connected and $\pi_0(G)$ étale. If k is perfect, then this sequence splits, and realizes G as a semidirect product $G^\circ \rtimes \pi_0(G)$.

PROOF. For the connected-étale exact sequence, see Proposition 5.51. If k is perfect, then G_{red} is a subgroup scheme of G (1.25), and the map $G \rightarrow \pi_0(G)$ induces an isomorphism $G_{\mathrm{red}} \rightarrow \pi_0(G)$ (5.53). \square

EXAMPLE 13.5. Let k be a nonperfect field of characteristic p , and let $c \in k \setminus k^p$. Let

$$G = \bigsqcup_{i=0}^{p-1} G_i, \quad G_i = \mathrm{Spm}(k[T]/(T^p - c^i)).$$

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

$$0 \rightarrow \mu_p \rightarrow G \rightarrow (\mathbb{Z}/p\mathbb{Z})_k \rightarrow 0.$$

This is nonsplit, because $G_i \simeq \mathrm{Spm}(k[c^{1/p}])$ if $i \neq 0$ and $G_0 \simeq \mathrm{Spm}(k)$.

EXAMPLE 13.6. Let k and c be as in (13.5). 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

$$ab = \begin{cases} a+b \in G_{i+j}(R) & \text{if } i+j < p \\ a+b-c \in G_{i+j-p}(R) & \text{if } i+j \geq p. \end{cases}$$

This makes $G(R)$ into a group, and G into a finite algebraic group. Its identity component is $G_0 = \alpha_p$, and there is a nonsplit exact sequence

$$0 \rightarrow \alpha_p \rightarrow G \rightarrow (\mathbb{Z}/p\mathbb{Z})_k \rightarrow 0.$$

PROPOSITION 13.7. *A finite group scheme G over k is étale if k has characteristic zero, or if it has characteristic $p \neq 0$ and p does not divide $o(G)$.*

PROOF. When k has characteristic zero, Cartier's theorem (3.38) shows that G is smooth, and hence étale. Let k have characteristic $p \neq 0$. If p does not divide $o(G)$, then the Frobenius map $F_G^r: G \rightarrow G^{(p^r)}$ is injective, and its image $G^{(p^r)}$ is smooth for r large (3.46). \square

In other words, a finite group scheme G over k is étale if $o(G)$ is invertible in k .

LOCALLY FREE FINITE GROUP SCHEMES OVER A BASE SCHEME

The most important finite group schemes over a ring (or base scheme) are those that are locally free, whose definition we now review.

13.8. Let R_0 be a commutative ring, and let M be an R_0 -module. Recall (7.12) that we say that M is 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 12.5). Therefore, when R_0 is noetherian, an R_0 -module is locally free of finite rank if and only if it is finite and flat.

We say that an R_0 -algebra is locally free of finite rank if it is so an R_0 -module. A finite R_0 -algebra A is locally free of finite rank if and only if it is locally free (equivalently, flat when R_0 is noetherian).

13.9. Let S be a scheme. Recall that a morphism of schemes $\varphi: X \rightarrow S$ is finite if, for all open affines U of S , $\varphi^{-1}(U)$ is an open affine of X and $\mathcal{O}_X(\varphi^{-1}(U))$ is a finite $\mathcal{O}_S(U)$ -algebra. It suffices to check the condition for enough U to cover S . A group scheme G over S is finite (resp. locally free and finite) if it is finite (resp. locally free and finite) as a scheme over S .

13.10. Let G be a finite group scheme over S . If S is locally noetherian, then G is locally free if and only if it is flat. We say that G is locally free of finite order r over S if G is of the form $\text{Spec}(A)$ where A is a sheaf of \mathcal{O}_S -algebras that is locally free of constant rank r . If S is locally noetherian and connected, then G is of finite order over S (for some r) if and only if it is finite and flat.

13.11. 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 $\Delta: A \rightarrow A \otimes_{R_0} A$ such that (A, Δ) is a Hopf algebra over R_0 .

b. Etale group schemes

13.12. Recall that a k -algebra A is **diagonalizable** if it is isomorphic to the product algebra k^n for some $n \in \mathbb{N}$, and it is **étale** if $k' \otimes A$ is diagonalizable for some field k' containing k . In particular, an étale k -algebra is finite.

13.13. 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) $k' \otimes A$ is reduced for all fields k' containing k ; (d) $k^{\text{sep}} \otimes A$ is diagonalizable. See Chapter 8 of my notes *Fields and Galois Theory*.

13.14. The quotient $k[T]/(f(T))$ of $k[T]$ by the ideal generated by a polynomial f is étale if and only if f is separable, i.e., has only simple roots in k^{al} . Every étale k -algebra is a finite product of such quotients.

13.15. The following conditions on a scheme X finite over $\text{Spm}(k)$ are equivalent: (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. This is an immediate consequence of (13.13).

13.16. A scheme finite over $\text{Spm}(k)$ satisfying the equivalent conditions of (13.15) is said to be *étale*.

13.17. Choose a separable closure k^{sep} of k , and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. The functor $X \rightsquigarrow X(k^{\text{sep}})$ is an equivalence from the category of étale schemes over k to the category of finite discrete Γ -sets. By a discrete Γ -set we mean a set X equipped with an action $\Gamma \times X \rightarrow X$ of Γ that is continuous relative to the Krull topology on Γ and the discrete topology on X . An action of Γ on a finite discrete set is continuous if and only if it factors through $\text{Gal}(K/k)$ for some finite Galois extension K of k contained in k^{sep} . See Chapter 8 of my notes *Fields and Galois Theory*.

13.18. A group scheme (G, m) over k is said to be *étale* if the scheme G is étale over k . Thus, an étale group scheme over k is just a group variety of dimension zero.

13.19. 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). Thus (13.17) implies the following statement.

The functor $G \rightsquigarrow G(k^{\text{sep}})$ 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.

EXAMPLES

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

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

$$\sigma \mapsto \sigma|_K: \Gamma \rightarrow \text{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$$

and all nontrivial such homomorphisms arise in this way. Thus, up to isomorphism, there is exactly one étale group scheme G^K of order 3 over k for each separable quadratic extension K of k , plus the constant group G_0 . For G_0 , $G_0(k)$ has order 3. For G^K , $G^K(k)$ has order 1 but $G^K(K)$ has order 3. There are infinitely many distinct quadratic extensions of \mathbb{Q} , for example, $\mathbb{Q}[\sqrt{-1}]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, ..., $\mathbb{Q}[\sqrt{p}]$, As $\mu_3(\mathbb{Q}) = 1$ but $\mu_3(\mathbb{Q}[\sqrt[3]{1}]) = 3$, μ_3 must be the group corresponding to $\mathbb{Q}[\sqrt[3]{1}]$.

REMARKS

13.22. For an étale group scheme G , the order of G is the order of the (abstract) group $G(k^{\text{sep}})$.

13.23. Let K be a subfield of k^{sep} containing k . Then $K = (k^{\text{sep}})^{\text{Gal}(K/k)}$, and it follows that

$$G(K) = G(k^{\text{sep}})^{\text{Gal}(K/k)}.$$

13.24. Not every zero-dimensional algebraic variety X over a field k can be made into a group scheme. For example, it must have a k -point. Beyond that, it must be possible to endow the set $X(k^{\text{sep}})$ with a group structure for which $\text{Gal}(k^{\text{sep}}/k)$ acts by group homomorphisms. In such an action, an orbit consists of elements of the same order.

Consider the scheme $X = \text{Spm}(k \times k')$ with k'/k a field extension of degree 5. The action of $\text{Gal}(k'/k)$ on $X(k^{\text{sep}})$ has only two orbits, but a group of order 6 has elements of order 1, 2, and 3, and so there must be at least three orbits for in any group action by group homomorphisms.

c. Finite group schemes of order n are killed by n

Let G be a finite (abstract) group of order n . Lagrange's theorem says that every subgroup of G has order dividing n . When applied to the subgroup generated by an element x of G , it implies that $x^n = e$. Both statements extend to finite group schemes.

PROPOSITION 13.25. Let G be a locally free finite group scheme of rank $o(G)$ over a ring R_0 , and let H be a locally free finite subgroup scheme of G of rank $o(H)$. Then

$$o(G) = o(H) \cdot \text{rank}(G/H).$$

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 $G \rightarrow G/H$ is locally free of rank $o(H)$ (7.26), and the ranks in $G \rightarrow G/H \rightarrow \text{Spm}(R_0)$ multiply. \square

Consider the algebraic group $G = \text{GL}_n$ over a field k , and let

$$\mathcal{O}(\text{GL}_n) = k[T_{11}, \dots, T_{nn}, 1/\det].$$

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 $[p]: \mathcal{O}(G) \rightarrow \mathcal{O}(G)$ denote the homomorphism corresponding to the p th power map $x \mapsto x^p: G \rightarrow G$. 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

$$[p]I_{\text{GL}_n} \subset I_{\text{GL}_n}^p. \quad (86)$$

PROPOSITION 13.26. *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 n th power map $n_G: G \rightarrow G$ is trivial: $n_G = 1_G$.*

PROOF. If G is étale, the statement is obvious (13.22). Also, if the statement is true for N and Q , then it is true for any every extension G of Q by N , because $o(G) = o(N) \cdot o(Q)$ and the sequence

$$0 \rightarrow N(R) \rightarrow G(R) \rightarrow Q(R)$$

is exact. Thus, we may suppose that G is connected, and hence that $n = p^m$ for some m (13.4, 13.25).

The regular representation realizes G as a closed subgroup scheme of GL_n (4.8). Therefore we have a surjective homomorphism of Hopf algebras, $\mathcal{O}(GL_n) \rightarrow \mathcal{O}(G)$. This maps the augmentation ideal of GL_n onto that of $\mathcal{O}(G)$, and we can deduce from (86) that

$$[p]I_G \subset I_G^p$$

where $[p]$ now denotes the homomorphism $\mathcal{O}(G) \rightarrow \mathcal{O}(G)$ corresponding to $p_G: G \rightarrow G$. 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. \square

COROLLARY 13.27. *Let G be a locally free finite group scheme of order n over a reduced ring R_0 . Then $n_G = 1_G$.*

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 $R_0 \rightarrow \prod_{\mathfrak{p} \text{ minimal}} R_{0\mathfrak{p}}$ is injective (because $R_0 \rightarrow \prod_{\mathfrak{p} \text{ minimal}} R_0/\mathfrak{p}$ is injective). Consider the diagram

$$\begin{array}{ccc} \mathcal{O}(G) & \xrightarrow{a} & \prod_{\mathfrak{p}} \mathcal{O}(G)_{\mathfrak{p}} \\ \downarrow & & \downarrow b \\ \mathcal{O}(Z) & \longrightarrow & \prod_{\mathfrak{p}} \mathcal{O}(Z)_{\mathfrak{p}} \end{array} \quad (\mathfrak{p} \text{ runs over the minimal primes of } R_0).$$

The map a is injective because $\mathcal{O}(G)$ is flat over R_0 , and Proposition 13.26 applied to $G_{R_{0\mathfrak{p}}}$ shows that b is an isomorphism. It follows that $\mathcal{O}(G) \rightarrow \mathcal{O}(Z)$ is injective, hence an isomorphism. \square

ASIDE 13.28. Proposition 13.26 holds for locally free finite group schemes over *reduced* schemes S (13.27), and for *commutative* locally free finite group schemes over arbitrary base schemes (Tate and Oort 1970, p.4).

NOTES. The proof of (13.26) follows that in Tate 1997, p.142. See also SGA 3, VII_A, 8.5.1, p.503; 8.5.2, p.505.

d. Cartier duality

For a k -vector space V , we let V' denote the dual vector space. If V and W are finite-dimensional, then the natural homomorphisms $V \rightarrow V''$ and $V' \otimes W' \rightarrow (V \otimes W)'$ are isomorphisms. Moreover, $k' = k$.

Let G be a finite algebraic group, and let $A = \mathcal{O}(G)$. We have k -linear maps

$$\left\{ \begin{array}{l} m: A \otimes A \rightarrow A \\ e: k \rightarrow A \end{array} \right. \quad \left\{ \begin{array}{l} \Delta: A \rightarrow A \otimes A \\ \epsilon: A \rightarrow k \end{array} \right.$$

defining the algebra and co-algebra structures respectively. On passing to the linear duals, we obtain k -linear maps

$$\left\{ \begin{array}{l} m': A' \rightarrow A' \otimes A' \\ e': A' \rightarrow k \end{array} \right. \quad \left\{ \begin{array}{l} \Delta': A' \otimes A' \rightarrow A' \\ \epsilon': k \rightarrow A' \end{array} \right.$$

The duals of the diagrams (20) show that (Δ', ϵ') defines an algebra structure on A' (not necessarily commutative), and one sees that (dually) (m', e') defines a co-algebra structure on A' . The algebra (A', Δ', ϵ') is commutative if and only if G is commutative.

LEMMA 13.29. *If G is commutative, then the system $(A', \Delta', \epsilon', m', e')$ is a Hopf algebra.*

PROOF. More precisely, we show that if S is an inversion for $\mathcal{O}(G)$, then S' is an inversion for $\mathcal{O}(G)$. We have 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):

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

□

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 algebraic group G' is called the **Cartier dual** of G . The functor $G \rightsquigarrow G'$ is a contravariant equivalence from the category of commutative algebraic groups over k to itself, and $(G')' \simeq G$.

We now describe the functor $R \rightsquigarrow G'(R)$. For a k -algebra R , let G_R denote the functor of R -algebras $R' \rightsquigarrow G(R')$, and let $\underline{\text{Hom}}(G, \mathbb{G}_m)(R)$ denote the set of natural transformations $u: G_R \rightarrow \mathbb{G}_{mR}$ 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,

$$R \rightsquigarrow \underline{\text{Hom}}(G, \mathbb{G}_m)(R)$$

becomes a functor from k -algebras to groups.

THEOREM 13.30. *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

$$G(R) = \mathrm{Hom}_{R\text{-algebra}}(\mathcal{O}(G), R) \hookrightarrow \mathrm{Hom}_{R\text{-linear}}(\mathcal{O}(G), R) = \mathcal{O}(G')_R. \quad (87)$$

The multiplication in $\mathcal{O}(G)$ corresponds to comultiplication in $\mathcal{O}(G')$, from which it follows that the image of (87) 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.75). Thus,

$$G(R) \simeq \underline{\mathrm{Hom}}(G', \mathbb{G}_m)(R).$$

This isomorphism is natural in R , and so we have shown that $G \simeq \underline{\mathrm{Hom}}(G', \mathbb{G}_m)$. To obtain the required isomorphism, replace G with G' and use that $(G')' \simeq G$. \square

From Theorem 13.30 we obtain a natural bimultiplicative morphism of schemes

$$G \times G' \rightarrow \mathbb{G}_m$$

that induces isomorphisms

$$\begin{cases} G \rightarrow \underline{\mathrm{Hom}}(G', \mathbb{G}_m) \\ G' \rightarrow \underline{\mathrm{Hom}}(G, \mathbb{G}_m). \end{cases}$$

This is called the *Cartier pairing*.

EXAMPLE 13.31. The action

$$(i, \zeta) \mapsto \zeta^i: \mathbb{Z}/n\mathbb{Z} \times \mu_n \rightarrow \mathbb{G}_m$$

defines a isomorphisms of algebraic groups .

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} \rightarrow \underline{\mathrm{Hom}}(\mu_n, \mathbb{G}_m) \\ \mu_n \rightarrow \underline{\mathrm{Hom}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m). \end{cases}$$

EXAMPLE 13.32. Let $G = \alpha_p$, so that $\mathcal{O}(G) = k[X]/(X^p) = k[x]$. Let $1, y, y_2, \dots, y_{p-1}$ be the basis of $\mathcal{O}(G)' = \mathcal{O}(G)'$ dual to $1, x, \dots, x^{p-1}$. Then $y^i = i!y_i$; in particular, $y^p = 0$. In fact, $G' \simeq \alpha_p$, and the pairing $\alpha_p \times \alpha_p \rightarrow \mathbb{G}_m$ is

$$a, b \mapsto \exp(ab): \alpha_p(R) \times \alpha_p(R) \rightarrow R^\times$$

where

$$\exp(ab) = 1 + \frac{ab}{1!} + \frac{(ab)^2}{2!} + \dots + \frac{(ab)^{p-1}}{(p-1)!}.$$

ASIDE 13.33. Let G commutative algebraic group that is either finite or of multiplicative type. Then

$$H^1(k, G) \simeq \mathrm{Ext}^1(G', \mathbb{G}_m)$$

where G' is the Cartier dual of G if G is finite and $(\Gamma)_k$ if $G = D(\Gamma)$. (Waterhouse 1971).

ASIDE 13.34. Everything in this section holds without change for locally free finite group schemes over a ring (or scheme).

e. Finite group schemes of order p

LEMMA 13.35. Let (A, Δ) be a finite cocommutative Hopf algebra over k , and let (A', Δ') be its Cartier dual. Let $d: A \rightarrow k$ be a derivation, and regard d 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 $x, y \in A$,

$$\Delta'(d)(x \otimes y) = d(xy) = xd(y) + yd(x) = (d \otimes 1 + 1 \otimes d)(x \otimes y). \quad \square$$

PROPOSITION 13.36. Let G be a finite group scheme of order p over an algebraically closed field k . Either G is the constant group scheme $(\mathbb{Z}/p\mathbb{Z})_k$, or k has characteristic p and $G = \mu_p$ or α_p . In particular, G is commutative and the k -algebra $\mathcal{O}(G)$ is generated by a single element.

PROOF. Recall (13.4, 13.25) that we have an exact sequence

$$e \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow e$$

with G° connected and $\pi_0(G)$ étale, and that $o(G) = o(G^\circ) \cdot o(\pi_0(G))$. As $o(G)$ is prime, G° is either e or all of G and, accordingly, G is either étale or connected. If G is étale, then it is constant because k is algebraically closed, hence it is isomorphic to $(\mathbb{Z}/p\mathbb{Z})_k$, and $\mathcal{O}(G)$, the k -algebra consisting of all k -valued functions on $\mathbb{Z}/p\mathbb{Z}$, is generated by any function that takes distinct values at the points of $\mathbb{Z}/p\mathbb{Z}$.

Suppose that $G = \text{Spm}(A)$ is connected, i.e., the k -algebra A is a local artin ring. Its augmentation ideal $I \subset A$ is nilpotent. By Nakayama's lemma $I \neq I^2$, hence there exists a non-zero k -derivation $d: A \rightarrow k$. This means that the element $d \in I' \subset A'$ has the property $\Delta_{A'}(d) = d \otimes 1 + 1 \otimes d$ (13.35). Thus $k[d] \subset A'$ is a k -subbialgebra of A' , and as $k[d]$ is a commutative ring, we obtain a surjective k -bialgebra homomorphism $A'' \simeq A \twoheadrightarrow (k[d])'$; as the order p of G is prime, this implies that the rank of $k[d]$ equals p , and hence $k[d] = A'$. As before we conclude that $G' = \text{Spm}(A')$ is either étale or connected. If G' is étale this means that $G' \approx (\mathbb{Z}/p\mathbb{Z})_k$, and thus $G \approx \mu_p$. As G was supposed to be connected this implies $\text{char}(k) = p$. If G' is connected, d is nilpotent, and, as $k[d]$ is of rank p , we must have $d^{p-1} \neq 0$ and $d^p = 0$; as $\Delta_{A'}$ is a ring homomorphism this implies that $p = 0$ in k , hence $\text{char}(k) = p$; moreover we already know that $\Delta_{A'}(d) = d \otimes 1 + 1 \otimes d$, hence $G' \approx \alpha_p$, and thus $G \approx \alpha_p$, which proves the result. Note that the last part of the proof could have been given using p -Lie algebras (cf. SGA 3, VII_A, 7). \square

REMARK 13.37. There exist noncommutative finite algebraic group of order p^2 (see 2.22, 13.5, 13.6).

NOTES. The proposition and proof are copied almost verbatim from Tate and Oort 1970.

f. Derivations of Hopf algebras

Let R_0 be a commutative ring.

13.38. Let A be an R_0 -algebra, and let M be an A -module. Recall (12.22) that an R_0 -derivation $D: A \rightarrow M$ is an R_0 -linear map such that

$$D(ab) = aD(b) + bD(a).$$

We say that an R_0 -derivation $d: A \rightarrow \Omega$ is **universal** if every R_0 -derivation $D: A \rightarrow M$ is of the form $\lambda \circ d$ for a unique A -linear map $\lambda: \Omega \rightarrow M$:

$$\lambda \leftrightarrow \lambda \circ d: \text{Hom}_{A\text{-linear}}(\Omega, M) \simeq \text{Der}_{R_0}(A, M).$$

Such a pair (Ω, d) is uniquely determined up to a unique isomorphism.

13.39. Let B be an R_0 -algebra, and let N be 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 $A \rightarrow B \oplus N$ is a pair (φ, D) with φ a homomorphism $A \rightarrow B$ and D an R_0 -derivation for the A -module structure on N defined by φ .

13.40. 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 $\gamma_0: A \rightarrow C$ making the diagram commute. Let γ be another R_0 -linear map $A \rightarrow C$ lifting φ . Then $\gamma = \gamma_0 + D$ with D an R_0 -linear map $A \rightarrow J$, and γ is an R_0 -algebra homomorphism if and only if D is an R_0 -derivation $A \rightarrow J_\varphi$. Thus, the set of liftings of φ is either empty or a principal homogeneous space under $\text{Der}_{R_0}(A, J_\varphi)$.

13.41. Let A be an R_0 -algebra and let $\epsilon: A \rightarrow R_0$ be an R_0 -algebra homomorphism 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 $D: A \rightarrow M_\epsilon$ is zero on R_0 and I^2 , and hence defines an R_0 -linear map $I/I^2 \rightarrow M$. Every R_0 -linear map $I/I^2 \rightarrow M$ arises from a unique derivation, and so

$$\text{Der}_{R_0}(A, M_\epsilon) \simeq \text{Hom}_{R_0\text{-linear}}(I/I^2, M).$$

Let (A, Δ) be a Hopf algebra over R_0 . Thus, $A \simeq R_0 \oplus I$, and we let $\pi: A \rightarrow I/I^2$ denote the map $a = (a_0, b) \mapsto b \bmod I^2$.

THEOREM 13.42. *Let (A, Δ) be a Hopf algebra over R_0 . Then*

$$(1 \otimes \pi) \circ \Delta: A \rightarrow A \otimes I/I^2$$

is the universal derivation for A/R_0 .

We shall deduce this from a more explicit statement. Let M be an A -module. For an R_0 -linear map $\lambda: I/I^2 \rightarrow M$, we define $D_\lambda = (\text{id}, \lambda \circ \pi) \circ \Delta$:

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\text{id} \otimes \pi} A \otimes I/I^2 \xrightarrow{\text{id} \otimes \lambda} A \otimes M \xrightarrow{a \otimes m \mapsto am} M.$$

Explicitly, if $\Delta(a) = \sum a_i \otimes a'_i$, then $D_\lambda(a) = \sum a_i \cdot \lambda \pi(a'_i)$.

PROPOSITION 13.43. *The map $\lambda \mapsto D_\lambda$ is an R_0 -linear isomorphism*

$$\mathrm{Hom}_{R_0\text{-linear}}(A, M) \rightarrow \mathrm{Der}_{R_0}(A, M).$$

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 13.39). Then $G(B \oplus N) \stackrel{\mathrm{def}}{=} \mathrm{Hom}(A, B \oplus N)$ 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

$$\begin{cases} \varphi \cdot \varphi' = (\varphi, \varphi') \circ \Delta & (\text{product in } G(B) = \mathrm{Hom}(A, B)) \\ \varphi \cdot D' = (\varphi, D') \circ \Delta = \left(A \xrightarrow{\Delta} A \otimes A \xrightarrow{a \otimes a' \mapsto \varphi(a) \cdot D'(a')} N \right) \\ \varphi' \cdot D = (\varphi', D) \circ \Delta. \end{cases}$$

Let $j: B \oplus N \rightarrow B$ be the projection map. Then $j_*: G(B \oplus N) \rightarrow G(B)$ 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 $\varphi: A \rightarrow B$ be an element of $G(B)$, and write N_φ for N regarded as an A -module by means of φ . According to (13.39), the fibre $j_*^{-1}(\varphi)$ over φ consists of the pairs (φ, D) with D an R_0 -derivation $A \rightarrow N_\varphi$:

$$j_*^{-1}(\varphi) = \{(\varphi, D) \in G(B \oplus N)\} \simeq \mathrm{Der}_{R_0}(A, N_\varphi).$$

Let $\epsilon_B: A \xrightarrow{\epsilon} R_0 \rightarrow B$ be the neutral element in $G(B)$. Then

$$x \mapsto (\varphi, 0) \cdot x: j_*^{-1}(\epsilon_B) \rightarrow j_*^{-1}(\varphi)$$

is a bijection. Explicitly, this is the map $(\epsilon_B, D) \mapsto (\varphi, \varphi \cdot D)$, and so we have a bijection

$$D \mapsto (\varphi, D) \circ \Delta: \mathrm{Der}_{R_0}(A, N_{\epsilon_B}) \rightarrow \mathrm{Der}_\varphi(A, N_\varphi).$$

On the other hand (13.41), we have a bijection

$$\lambda \mapsto \lambda \circ \pi: \mathrm{Hom}_{R\text{-linear}}(I/I^2, N) \rightarrow \mathrm{Der}_{R_0}(A, N_{\epsilon_B}).$$

On composing these maps, and taking $B = A$, $N = M$, and $\varphi = \mathrm{id}_A$, we obtain the required isomorphism. \square

For an A -module M ,

$$\mathrm{Der}_{R_0}(A, M) \simeq \mathrm{Hom}_{R_0\text{-linear}}(I/I^2, M) \simeq \mathrm{Hom}_{A\text{-linear}}(A \otimes I/I^2, M),$$

which implies (13.42).

g. Structure of the underlying scheme of a finite group scheme

LEMMA 13.44. Let (A, Δ) be a finitely generated Hopf algebra over k , and let I be its augmentation ideal. Let $n \geq 0$ be an integer which is less than the characteristic of k if this is nonzero. Let x_1, \dots, 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} .

The assumption on n is that $n! \neq 0$ in k .

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 $A = k \oplus I \rightarrow I/I^2$ killing k . Let $d_i: I/I^2 \rightarrow k$ be the k -linear map such that $d_i(x_j) = \delta_{ij}$ (Kronecker delta). According to (13.42), there exists a (unique) derivation $D_i: A \rightarrow k$ such that

$$D_i(a) = \sum_j a_j \cdot d_i(\pi(b_j))$$

if $\Delta(a) = \sum a_j \otimes b_j$. Then $D_i(x_i) = \delta_{ij}$. More generally,

$$D_r^{m_r} D_{r-1}^{m_{r-1}} \cdots D_1^{m_1} (x_1^{m_1} \cdots x_r^{m_r}) = m_1! m_2! \cdots m_r!,$$

while $D_r^{m_r} D_{r-1}^{m_{r-1}} \cdots D_1^{m_1}$ applied to any other monomial of total degree $m_1 + \cdots + m_r = n$ is zero. According to the assumption 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. \square

Recall (2.16) that an algebraic group G is said to have height ≤ 1 if the Frobenius map $F_G: G \rightarrow G^{(p)}$ is trivial. This means that $a^p = 0$ for all $a \in I$.

PROPOSITION 13.45. Let G be a connected finite group scheme of height 1 over a field k of characteristic p . Then

$$\mathcal{O}(G) \approx k[T_1, \dots, T_n]/(T_1^p, \dots, T_n^p) \quad (88)$$

for some $n \geq 1$.

PROOF. Immediate consequence of the lemma. \square

THEOREM 13.46. Let G be a connected finite group scheme over a perfect field k of characteristic p . Then

$$\mathcal{O}(G) \approx k[T_1, \dots, T_n]/(T_1^{p^{e_1}}, \dots, T_n^{p^{e_n}}) \quad (89)$$

for some integers $e_1, \dots, e_n \geq 1$.

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 we just proved the statement (13.45). In the general case, we argue by induction. Because k is perfect,

$$B \stackrel{\text{def}}{=} A^p = \{a^p \mid a \in A\}$$

is a Hopf subalgebra of A (see 3.46). By induction,

$$B = k[t_1, \dots, t_n] \simeq k[T_1, \dots, T_n]/(T_1^{q_1}, \dots, T_n^{q_n}), \quad q_i = \text{power of } p.$$

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 $z_j^p = 0$ and that the z_j be linearly independent in I/I^2 . We shall complete the proof by showing that the homomorphism

$$\begin{cases} Y_i \mapsto y_i \\ Z_j \mapsto z_j \end{cases} : C \stackrel{\text{def}}{=} k[Y_1, \dots, Z_1, \dots]/(Y_1^{p^{q_1}}, \dots, Z_1^p, \dots) \rightarrow A$$

is an isomorphism.

Embed B in C by $t_i \mapsto Y_i^p$. Then C is a free B -module. By Theorem 3.47, A is faithfully flat (hence free) over the local ring B . As in (3.47, Step 2), it suffices to show that the map $C/I_B C \rightarrow A/I_B A$ is an isomorphism. Clearly,

$$C/I_B C \simeq k[Y_1, \dots, Z_1, \dots]/(Y_1^p, \dots, Z_1^p, \dots).$$

The quotient $A/I_B A$ is the Hopf algebra representing the kernel of $\text{Spm}(A, \Delta) \rightarrow \text{Spm}(A^p, \Delta)$ (Section 1.e), which has height 1, and so it also is of the form (88). If a homomorphism between two algebras of this form is an isomorphism modulo the squares of the maximal ideals, then it is surjective (Nakayama), and then, by counting dimensions, an isomorphism. As $I_B A \subset I_A^2$, it remains to show that the elements y_j and z_j form a basis for I_A/I_A^2 .

Let a be any element of I_A , and write a^p in I_B as a polynomial in the t_i . As k is perfect, we can take the p th root of this to get a polynomial u in the y_i with $u^p = a^p$. Then $(a - u)^p = 0$, and by maximality of the $\{z_j\}$, we can express $a - u$ modulo I_A^2 in terms of the z_j . We have shown that the elements y_j and z_j span I_A/I_A^2 . Suppose that $\sum \alpha_i y_i + \sum \beta_j z_j$ lies in I_A^2 . On raising this to the p th power, we find that the element $\sum \alpha_i^p y_i^p = \sum \alpha_i^p t_i$ is in I_B^2 . But the t_i form a basis for I_B/I_B^2 , and so this implies that all α_i are zero. Now $\sum \beta_j z_j$ is in I_A^2 , which by definition of the z_j implies that all $\beta_j = 0$. This completes the proof that the elements y_j and z_j form a basis for I_A/I_A^2 . \square

These results allow us to reprove Cartier's theorem (3.38) and (13.7).

COROLLARY 13.47. *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} (13.44). Hence x is not nilpotent. Therefore $x \in I^2$. Now Lemma 3.35 shows that G is smooth (3.35).

Alternatively, Lemma 13.44 shows that the graded ring $\text{gr}_I(A)$ is isomorphic to $k[T_1, \dots, T_r]$ for $r = \dim_k(I/I^2)$. Recall that I is the maximal ideal in A at the neutral element e . When we localize we get

$$\text{gr}_I(A) \simeq \text{gr}_{\mathfrak{m}_e}(A_e) \approx k[T_1, \dots, T_r].$$

This implies that A_e is a regular local ring (Atiyah and Macdonald 1969, 11.22).

(b) If G is connected and finite, then (13.46) shows that its order is a power of p . The statement now follows from connected-étale exact sequence (13.4). \square

EXAMPLE 13.48. Let k be a nonperfect field of characteristic p , and let $c \in k \setminus k^p$. The finite subgroup scheme G of $\mathbb{G}_a \times \mathbb{G}_a$ with

$$G(R) = \{(x, y) \mid x^{p^2} = 0, y^p = cx^p\}$$

is connected, but $\mathcal{O}(G)$ is not of the form (89) (Waterhouse 1979, p.113).



h. Finite group schemes of height at most one

Let \mathfrak{g} be a p -Lie algebra over k . Recall that the universal enveloping p -Lie algebra $j: \mathfrak{g} \rightarrow U^{[p]}(\mathfrak{g})$ has the following property: every p -Lie algebra homomorphism $\mathfrak{g} \rightarrow [A]$ with A an associative k -algebra extends uniquely to a k -algebra homomorphism $U^{[p]}(\mathfrak{g}) \rightarrow A$. From this universality we deduce that there is:

- (a) a unique homomorphism of k -algebras

$$\Delta: U^{[p]}(\mathfrak{g}) \rightarrow U^{[p]}(\mathfrak{g}) \times U^{[p]}(\mathfrak{g})$$

such that $\Delta(j(x)) = 1 \otimes j(x) + j(x) \otimes 1$ for $x \in \mathfrak{g}$;

- (b) a unique homomorphism of k -algebras $\epsilon: U^{[p]}(\mathfrak{g}) \rightarrow k$ such that $\epsilon \circ j = 0$;
(c) a unique homomorphism $S: U^{[p]}(\mathfrak{g}) \rightarrow U^{[p]}(\mathfrak{g})$ 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

$$\begin{aligned} \sum u_i \otimes v_i &= \sum v_i \otimes u_i, & \sum u_i \otimes \Delta v_i &= \sum \Delta u_i \otimes v_i, \\ \sum \epsilon(u_i) v_i &= u, & \sum S(u_i) v_i &= \epsilon(u). \end{aligned}$$

It suffices indeed to check these equalities when $u = 1$ or $j(x)$, $x \in \mathfrak{g}$, in which case they are obvious.

PROPOSITION 13.49. *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 denote the maps

$$\begin{aligned} U \otimes R &\xrightarrow{\Delta \otimes R} U \otimes U \otimes R \xrightarrow{\simeq} (U \otimes R) \otimes_R (U \otimes R) \\ U \otimes R &\xrightarrow{\epsilon \otimes R} k \otimes R \simeq R. \end{aligned}$$

PROPOSITION 13.50. *Let \mathfrak{g} be a p -Lie algebra. The functor*

$$R \rightsquigarrow G(\mathfrak{g})(R) \stackrel{\text{def}}{=} \left\{ x \in (U^{[p]}(\mathfrak{g}) \otimes R)^{\times} \mid \Delta_R x = x \otimes x, \quad \epsilon_R x = 1 \right\}$$

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 (12.41), 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 $G(\mathfrak{g}) \rightarrow \text{Spm}(A)$, and so $G(\mathfrak{g})$ is a finite scheme over k . Finally, the coproduct $\Delta_A: A \rightarrow A \otimes A$ defined by the group structure on $G(\mathfrak{g})$ is the dual of the multiplication map $U \otimes U \rightarrow U$ (apply (19), p.56). See DG II, §7, 3.8, p.279, for more details. \square

PROPOSITION 13.51. *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. Omitted for the moment (DG II, §7, 4.2, p.282). \square

In particular, every algebraic group G of height ≤ 1 is isomorphic to $G(\mathfrak{g})$ for some p -Lie algebra \mathfrak{g} .

i. The Frobenius and Verschiebung morphisms

Let X be a scheme over \mathbb{F}_p . The absolute Frobenius morphism $\sigma_X: X \rightarrow X$ acts as the identity map on $|X|$ and as the map $f \mapsto f^p: \mathcal{O}_X(U) \rightarrow \mathcal{O}_X(U)$ on the sections over every open subset U of X . For all morphisms $\varphi: X \rightarrow Y$ of schemes over \mathbb{F}_p ,

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

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

Now let k be a field of characteristic p . The morphism $\sigma_{\text{Spm}(k)}: \text{Spm}(k) \rightarrow \text{Spm}(k)$ corresponds to the homomorphism $a \mapsto a^p: k \rightarrow k$. We write $X \rightsquigarrow X^{(p)}$, $\varphi \rightsquigarrow \varphi^{(p)}$ for base change with respect to $\sigma_{\text{Spm}(k)}$. If (G, m) is an algebraic group over k , then so also is $(G^{(p)}, m^{(p)})$.

For a scheme X over k , the relative Frobenius morphism $F_X: X \rightarrow X^{(p)}$ is defined by the diagram

$$\begin{array}{ccc}
 & & X \\
 & \swarrow \sigma_X & \nearrow F_X \\
 X & \xleftarrow{\quad} & X^{(p)} \\
 \downarrow & & \downarrow \\
 \text{Spm}(k) & \xleftarrow{\sigma_{\text{Spm}(k)}} & \text{Spm}(k)
 \end{array}$$

in which the square is cartesian (cf. 2.16). The assignment $X \mapsto F_X$ has the following properties.

(a) Functoriality: for all morphisms $\varphi: X \rightarrow Y$ of schemes over k ,

$$F_Y \circ \varphi = \varphi^{(p)} \circ F_X.$$

(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.

In particular, if (G, m) is an algebraic group over k , then

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

commutes, and so $F_G: G \rightarrow G^{(p)}$ is a homomorphism.

For example, if X is a closed subvariety of \mathbb{A}^n defined by polynomials $f_i(T_1, \dots, T_n) = \sum a_{(i)} T^{(i)}$, then $X^{(p)}$ is the closed subvariety of \mathbb{A}^n defined by the polynomials $f_i^{(p)} = \sum a_{(i)}^p T^{(i)}$ and $\sigma_X: X \rightarrow X^{(p)}$ sends a point (c_1, \dots, c_n) to (c_1^p, \dots, c_n^p) .

PROPOSITION 13.52. *An algebraic group G is smooth if and only if the Frobenius map $F_G: G \rightarrow G^{(p)}$ is faithfully flat.*

PROOF. In general, a reduced finitely generated k -algebra A is geometrically reduced if and only if $A \otimes k^{1/p}$ is reduced. On the other hand, F_G is faithfully flat if and only if the corresponding map $A^{(p)} \rightarrow A$ is injective. To complete the proof, compare $A \otimes k^{1/p}$ with $A^{(p)}$. □

Let G be a commutative finite group scheme over k . Then $F_G: G \rightarrow G^{(p)}$ induces a homomorphism $V_G: (G^{(p)})' \simeq (G')^{(p)} \rightarrow G'$ on the Cartier dual. This is the Verschiebung (shift) 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 $\otimes^p V$ by

$$\tau(v_1 \otimes \dots \otimes v_p) = v_{\tau(1)} \otimes \dots \otimes v_{\tau(p)},$$

and the $\text{Sym}^p V$ is the greatest quotient of $\otimes^p V$ on which S_p acts trivially: $\text{Sym}^p V = (V^{\otimes p})_{S_p}$. Now let G be an algebraic group over k , 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:

$$\begin{array}{ccccc} x \cdot a^p & \longleftarrow & [x(a \otimes \dots \otimes a)] & \longleftarrow & a \otimes x \\ & & & & \\ A & \longleftarrow & \text{Sym}^p(A) & \longleftarrow & A \otimes_{k,f} k & (f(a) = a^p) \\ & \swarrow \text{multiplication} & \uparrow \text{quotient} & & \\ & & A^{\otimes p} & & \end{array}$$

If A is finite, then we can form the above diagram for the dual A' of A , and take its dual, to get a diagram:

$$\begin{array}{ccc} A & \longrightarrow & (A^{\otimes p})^{S_p} \xrightarrow{\lambda_A} A \otimes_{k,f} k \\ & \searrow \text{comultiplication} & \downarrow \text{inclusion} \\ & & A^{\otimes p} \end{array}$$

Here λ_A is the unique k -linear map sending $x \cdot (a \otimes \cdots \otimes a)$ to $a \otimes x$. In fact, it is easy to see that this diagram exists for any A .

DEFINITION 13.53. For an algebraic group G over a field k , the **Verschiebung morphism**¹ is the morphism $V_G: G^{(p)} \rightarrow G$ corresponding to the homomorphism $A \otimes_{k, f} k \rightarrow A$ in the above diagram.

The assignment $G \mapsto V_G$ has the following properties.

- (a) Functoriality: for all homomorphisms $\varphi: G \rightarrow H$ of schemes over k ,

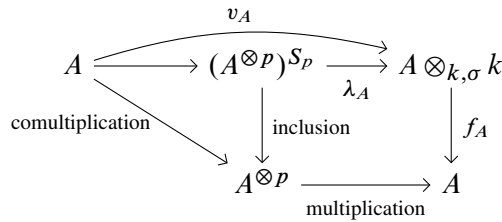
$$V_H \circ \varphi^{(p)} = \varphi \circ V_G.$$

- (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.

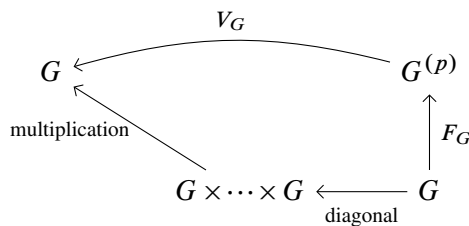
PROPOSITION 13.54. Let G be a commutative group scheme over k . Then:

- (a) $V_G \circ F_G = p \cdot \text{id}_G$,
- (b) $F_G \circ V_G = p \cdot \text{id}_{G^{(p)}}$.

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:



The square at right commutes. In terms of the group schemes, the diagram becomes



Hence

$$V_G \circ F_G = (\text{multiplication}) \circ (\text{diagonal}) = p \cdot \text{id}_G$$

- (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 be $p \cdot \text{id}_{G^{(p)}}$. □

¹“Verschiebung” means “shift”. Its name is perhaps explained by (90). The French usually translate it to “décalage”. The notation V_G is universal.

COROLLARY 13.55. *A smooth commutative group scheme G has exponent p if and only if $V_G = 0$.*

PROOF. If $V_G = 0$, then $p \cdot \text{id}_G = 0$ because $p \cdot \text{id}_G = V_G \circ F_G$. Conversely, if G is smooth and $p \cdot \text{id}_G = 0$, then $V_G = 0$ because F_G is faithfully flat (13.52). \square

j. The Witt schemes W_n

Fix a prime number p . Let T_0, T_1, \dots be a sequence of symbols, and define (Witt) polynomials

$$\begin{aligned} w_0 &= T_0 \\ w_1 &= T_0^p + pT_1 \\ &\dots \\ w_n &= T_0^{p^n} + pT_1^{p^{n-1}} + \dots + p^n T_n \\ &\dots \end{aligned}$$

These are polynomials with coefficients in \mathbb{Z} . If we invert p , then we can express that T_i as polynomials in the w_i ,

$$T_0 = w_0, \quad T_1 = p^{-1}(w_1 - w_0^p), \quad \dots$$

Let U_0, U_1, \dots be a second sequence of symbols.

PROPOSITION 13.56. *There exist unique polynomials $S_i, P_i \in \mathbb{Z}[T_0, T_1, \dots, U_0, U_1, \dots]$, $i = 0, 1, \dots$, such that*

$$\begin{aligned} w_n(S_0, \dots, S_n, \dots) &= w_n(T_0, \dots) + w_n(U_0, \dots) \\ w_n(P_0, \dots, P_n, \dots) &= w_n(T_0, \dots) \cdot w_n(U_0, \dots) \end{aligned}$$

for all $n \geq 0$.

PROOF. Serre 1962, II, §6, Thm 5. \square

For example,

$$\begin{aligned} S_0(a, b) &= a_0 + b_0 & S_1(a, b) &= a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} \\ P_0(a, b) &= a_0 \cdot b_0 & P_1(a, b) &= b_0^p a_1 + b_1 a_0^p + p a_1 b_1. \end{aligned}$$

PROPOSITION 13.57. *Let R be a commutative ring. For $n \geq 0$, the rules*

$$\begin{aligned} a + b &= (S_0(a, b), \dots, S_n(a, b)) \\ a \cdot b &= (P_0(a, b), \dots, P_n(a, b)). \end{aligned}$$

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

$$a \mapsto (w_0(a), \dots, w_n(a)): W_n(R) \rightarrow R^{n+1}$$

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 $R = \mathbb{Z}[T_0, \dots]$, and hence for any ring containing $\mathbb{Z}[T_0, \dots]$. But $\mathbb{Z}[T_0, \dots]$ can be embedded into \mathbb{C} , and we know the proposition for $R = \mathbb{C}$. \square

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 , and regard W_n as an algebraic group over k . The map

$$V: W_n(R) \rightarrow W_{n+1}(R), \quad (a_0, \dots, a_n) \mapsto (0, a_0, \dots, a_n) \quad (90)$$

is additive. This can be proved by the same argument as Proposition 13.57. Thus, we obtain a homomorphism of algebraic groups

$$V: W_n \rightarrow W_{n+1}.$$

PROPOSITION 13.58. *For all $n, r \geq 0$, the sequence*

$$0 \rightarrow W_n \xrightarrow{V^r} W_{n+r} \xrightarrow{\text{truncate}} W_r \rightarrow 0$$

is exact.

PROOF. In fact, for all k -algebras R , the sequence

$$0 \rightarrow W_n(R) \xrightarrow{V^r} W_{n+r}(R) \xrightarrow{\text{truncate}} W_r(R) \rightarrow 0$$

is obviously exact. \square

As W_n is defined over $\mathbb{F}_p \subset k$, we have $W_n^{(p)} \simeq W_n$. The Frobenius morphism $W_n \rightarrow W_n^{(p)} \simeq W_n$ acts on $W_n(R)$ as $(a_0, \dots, a_n) \mapsto (a_0^p, \dots, a_n^p)$ 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

Let k be a perfect field of characteristic p . Finite group schemes over k of order prime to p are étale (13.7), and so are classified in terms of the Galois group of k (13.19). 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 ,

$$W(k) \stackrel{\text{def}}{=} \varprojlim W_n(k).$$

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 relations ($c \in W$):

$$\begin{aligned} F \cdot c &= \sigma c \cdot F; \\ \sigma c \cdot V &= V \cdot c; \\ FV &= p = VF. \end{aligned}$$

Thus, to give a D -module amounts to giving a W -module M together with endomorphisms F and V of M satisfying the following conditions ($c \in W, m \in M$):

$$\begin{aligned} F(c \cdot m) &= \sigma c \cdot Fm \\ V(\sigma c \cdot m) &= c \cdot Vm \\ FV &= p \cdot \text{id}_M = VF. \end{aligned}$$

Such a module is called a **Dieudonné module**. We say that M is finitely generated (resp. finite) if it is finitely generated as a W -module.

For an algebraic group G over k , we define

$$M(G) = \varinjlim_n \text{Hom}(G, W_n).$$

THEOREM 13.59. *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 . Such an algebraic 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 $M(G)$.*

PROOF. For algebraic groups killed by V , this is a special case of (13.51). See DG V, §1, 4.3, p.552 for the proof. \square

THEOREM 13.60. *Let G be a commutative finite group scheme of p -power order over k . Then G has a unique decomposition*

$$G = G_{ec} \times G_{cc} \times G_{ce}$$

where G_{ec} (resp. $G_{cc}; G_{ce}$) is étale with connected dual (resp. connected with connected dual; connected with étale dual).

PROOF. We know (13.4) 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 $G_c = (G_c)'' = G_{cc} + G_{ce}$. On the other hand, $(G_e)'$ is connected, and so $(G_e)' = G_{ec}$. \square

We want to extend the functor M to all finite group schemes over k killed by a power of p . For $G = G_{ce}$, we define

$$M(G) = M(G)'$$

where the inner prime denotes the Cartier dual, and the outer $'$ denotes dual as a Dieudonné module (i.e., $(M, F, V)' = (M', F', V')$ with $M' = \text{Hom}_{W\text{-linear}}(M, W)$ and F' and V' the maps induced by V and F).

THEOREM 13.61. *There is a contravariant equivalence $G \rightsquigarrow M(G)$ from the category of commutative finite algebraic p -groups to the category of triples Dieudonné modules of finite length. The order of G is $p^{\text{length}(M(G))}$. For any perfect field k' containing k , there is functorial isomorphism*

$$M(G_{k'}) \simeq W(k') \otimes_{W(k)} M(G).$$

PROOF. Immediate consequence of the preceding two theorems. □

For example:

$$\begin{aligned} M(\mathbb{Z}/p\mathbb{Z}) &= W/pW, & F &= \sigma, & V &= 0; \\ M(\mu_p) &= W/pW, & F &= 0, & V &= \sigma^{-1}; \\ M(\alpha_p) &= W/pW, & F &= 0, & V &= 0. \end{aligned}$$

The theorem is very important since it reduces the study of commutative algebraic p -groups over perfect fields to semi-linear algebra. There are important generalizations of the theorem to Dedekind domains, and other rings.

ASIDE 13.62. For an extension of Theorem 13.59 (resp. Theorem 13.61) to nonperfect base fields, see [Schoeller 1972](#) (resp. [Takeuchi 1975](#)).

ASIDE 13.63. For more on finite group schemes, see [Demazure 1972](#) and [Tate 1997](#).

Tori; groups of multiplicative type; linearly reductive groups

Recall that algebraic groups are affine.

a. The characters of an algebraic group

Recall (p.75) that a character of an algebraic group G is a homomorphism $\chi: G \rightarrow \mathbb{G}_m$. Thus, to give a character χ of G is the same as giving a homomorphism of k -algebras $\mathcal{O}(\mathbb{G}_m) \rightarrow \mathcal{O}(G)$ respecting the comultiplications. 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 a unit $a = a(\chi)$ 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 $\mathcal{O}(G)$.

For characters χ, χ' , define

$$\chi + \chi': G(R) \rightarrow R^\times$$

by

$$(\chi + \chi')(g) = \chi(g) \cdot \chi'(g).$$

Then $\chi + \chi'$ is again a character, and the set of characters is a commutative group, denoted $X(G)$. The correspondence $\chi \leftrightarrow a(\chi)$ between characters and group-like elements has the property that

$$a(\chi + \chi') = a(\chi) \cdot a(\chi').$$

b. The algebraic group $D(M)$

Let M be a finitely generated commutative group (written multiplicatively), and let $k[M]$ be the k -vector space with basis M . Thus, the elements of $k[M]$ are finite sums

$$\sum_i a_i m_i, \quad a_i \in k, \quad m_i \in M.$$

When we endow $k[M]$ with the multiplication extending that on M ,

$$\left(\sum_i a_i m_i\right) \left(\sum_j b_j n_j\right) = \sum_{i,j} a_i b_j m_i n_j,$$

then $k[M]$ becomes a k -algebra, called the **group algebra** of M . It becomes a Hopf algebra when we set

$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad S(m) = m^{-1} \quad (m \in M)$$

because, for m an element of the basis M ,

$$\begin{aligned} (\text{id} \otimes \Delta)(\Delta(m)) &= m \otimes (m \otimes m) = (m \otimes m) \otimes m = (\Delta \otimes \text{id})(\Delta(m)), \\ (\epsilon \otimes \text{id})(\Delta(m)) &= 1 \otimes m, \quad (\text{id} \otimes \epsilon)(\Delta(m)) = m \otimes 1, \\ (S, \text{id})(m \otimes m) &= \epsilon(m) = (\text{id}, S)(m \otimes m), \end{aligned}$$

as required ((20), (21), p.56). 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 14.1. Let M be a cyclic group, generated by e .

- (a) Case e has infinite order. Then the elements of $k[M]$ are the finite sums $\sum_{i \in \mathbb{Z}} a_i e^i$ with the obvious addition and multiplication, and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, $S(e) = e^{-1}$. Therefore, $k[M] \simeq \mathcal{O}(\mathbb{G}_m)$ as a Hopf algebra.
- (b) Case e is of order n . Then the elements of $k[M]$ are sums $a_0 + a_1 e + \cdots + a_{n-1} e^{n-1}$ with the obvious addition and multiplication (using $e^n = 1$), and $\Delta(e) = e \otimes e$, $\epsilon(e) = 1$, and $S(e) = e^{n-1}$. Therefore, $k[M] \simeq \mathcal{O}(\mu_n)$ as a Hopf algebra.

EXAMPLE 14.2. Recall that if W and V are vector spaces with bases $(e_i)_{i \in I}$ and $(f_j)_{j \in J}$, then $W \otimes V$ has basis $(e_i \otimes f_j)_{(i,j) \in I \times J}$. It follows that, 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 14.3. For every finitely generated commutative group M , the functor $D(M)$

$$R \rightsquigarrow \text{Hom}(M, R^\times) \quad (\text{homomorphisms of groups})$$

is represented by the algebraic group $\text{Spm}(k[M])$. 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 $k[M] \rightarrow R$ is the same as giving a map of sets $M \rightarrow R$. The map $k[M] \rightarrow R$ is a k -algebra homomorphism if and only if $M \rightarrow R$ is a homomorphism from M into R^\times . This shows that $D(M)$ is represented by $k[M]$, and is therefore an algebraic group.

A decomposition of commutative groups

$$M \approx \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

defines a decomposition of k -bialgebras

$$k[M] \approx \mathcal{O}(\mathbb{G}_m) \otimes \cdots \otimes \mathcal{O}(\mathbb{G}_m) \otimes \mathcal{O}(\mu_{n_1}) \otimes \cdots \otimes \mathcal{O}(\mu_{n_r})$$

(14.1, 14.2). Since every finitely generated commutative group M has such a decomposition, this proves the second statement. \square

LEMMA 14.4. The group-like elements of $k[M]$ are exactly the elements of M .

PROOF. Let $e \in k[M]$ be group-like. Then

$$e = \sum c_i e_i \text{ for some } c_i \in k, e_i \in M.$$

The argument in the proof of Lemma 4.16 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 of them equals 1 and the remainder are zero. Therefore $e = e_i$ for some i . \square

Thus

$$X(D(M)) \simeq M.$$

The character of $D(M)$ corresponding to $m \in M$ is

$$D(M)(R) \stackrel{\text{def}}{=} \text{Hom}(M, R^\times) \xrightarrow{f \mapsto f(m)} R^\times \stackrel{\text{def}}{=} \mathbb{G}_m(R).$$

14.5. Let p be the characteristic exponent of k . Then:

$$\begin{aligned} D(M) \text{ is connected} & \iff \text{the only torsion in } M \text{ is } p\text{-torsion} \\ D(M) \text{ is smooth} & \iff M \text{ has no } p\text{-torsion} \\ D(M) \text{ is smooth and connected} & \iff M \text{ is free.} \end{aligned}$$

To see this, note that $D(\mathbb{Z}) = \mathbb{G}_m$, which is connected and smooth, and that $D(\mathbb{Z}/n\mathbb{Z}) = \mu_n$, which is connected and nonsmooth if n is a power of p , and is étale and nonconnected if $\gcd(n, p) = 1$ ($n > 1$).

Note that

$$\begin{aligned} D(M/\{\text{prime-to-}p \text{ torsion}\}) &= D(M)^\circ \quad (\text{identity component of } D(M)) \\ D(M/\{p\text{-torsion}\}) &= D(M)_{\text{red}} \quad (\text{reduced algebraic subgroup}) \\ D(M/\{\text{torsion}\}) &= D(M)_{\text{red}}^\circ \quad (\text{reduced connected algebraic subgroup}). \end{aligned}$$

ASIDE 14.6. When the binary operation on M is denoted by $+$, it is more natural to define $k[M]$ to be 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 14.7. An algebraic group G is **diagonalizable** if the group-like elements in $\mathcal{O}(G)$ span it as a k -vector space.

THEOREM 14.8. 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 4.16 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 $k[M] \xrightarrow{\sim} \mathcal{O}(G)$ of vector spaces. This isomorphism is compatible with the comultiplications, because it is on the basis elements $m \in M$ (obviously). \square

THEOREM 14.9. (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) The functor $M \rightsquigarrow D(M)$ is exact: if

$$1 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 1$$

is an exact sequence of commutative groups, then

$$1 \rightarrow D(M'') \rightarrow D(M) \rightarrow D(M') \rightarrow 1$$

is an exact sequence of algebraic groups.

(c) Algebraic subgroups and quotient groups (but not necessarily extensions) of diagonalizable algebraic groups are diagonalizable.

PROOF. (a) Certainly, we have a contravariant functor

$$D: \{\text{f.g. commutative groups}\} \rightsquigarrow \{\text{diagonalizable groups}\}.$$

We first show that D is fully faithful, i.e., that

$$\text{Hom}(M, M') \rightarrow \text{Hom}(D(M'), D(M)) \quad (91)$$

is an isomorphism for all M, M' . The functor sends finite direct limits to inverse limits and finite direct sums to products, and so it suffices to prove that (91) is an isomorphism when M and M' are cyclic. If, for example, M and M' are both infinite cyclic groups, then we may suppose that $M = \mathbb{Z} = M'$, and

$$\begin{aligned} \text{Hom}(M, M') &= \text{Hom}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}, \\ \text{Hom}(D(M'), D(M)) &= \text{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \{X^i \mid i \in \mathbb{Z}\} \simeq \mathbb{Z}; \end{aligned}$$

now (91) is $i \mapsto X^i$, which is an isomorphism. The remaining cases are similarly easy.

Theorem 14.8 shows that the functor is essentially surjective, and so it is an equivalence.

(b) The map $k[M'] \rightarrow k[M]$ is injective, and so $D(M) \rightarrow D(M')$ is a quotient map (5.15). 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 $M \rightarrow M''$ defines an isomorphism $k[M]/I_{k[M']} \rightarrow k[M'']$.

(c) If H is a subgroup of G , then the map $\mathcal{O}(G) \rightarrow \mathcal{O}(H)$ is surjective. Because it is a homomorphism of Hopf algebras, it maps group-like elements to group-like elements. Therefore, if the group-like elements of $\mathcal{O}(G)$ span it, then the same is true of $\mathcal{O}(H)$.

Let $D(M) \rightarrow Q$ be a quotient map, and let H be its kernel. Then $H = D(M'')$ for some quotient M'' of M . Let M' be the kernel of $M \rightarrow M''$. Then $D(M) \rightarrow D(M')$ and $D(M) \rightarrow Q$ are quotient maps with the same kernel, and so are isomorphic. \square

EXAMPLE 14.10. Let G be the algebraic group of monomial 2×2 matrices (5.54). Then G is an extension

$$e \rightarrow \mathbb{D}_2 \rightarrow G \rightarrow S_2 \rightarrow e$$

of diagonalizable groups, but it is not commutative, hence not diagonalizable. Later (14.27, 16.46) we shall see that an extension G of a diagonalizable group Q by a diagonalizable group is diagonalizable if G is commutative, which is always the case if Q is connected.

d. Diagonalizable representations

DEFINITION 14.11. A representation of an algebraic group is **diagonalizable** if it is a sum of one-dimensional representations (according to (4.17), 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 an invertible matrix P in $M_n(k)$ such that, for all k -algebras R and all $g \in G(R)$,

$$P g P^{-1} \in \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\}.$$

THEOREM 14.12. *The following conditions on an algebraic group G are equivalent:*

- (a) G is diagonalizable;
- (b) every finite-dimensional representation of G is diagonalizable;
- (c) every representation of G is diagonalizable;
- (d) for every representation (V, r) of G ,

$$V = \bigoplus_{\chi \in X(T)} V_\chi$$

(V_χ is the eigenspace with character χ , p.75).

PROOF. (a) \Rightarrow (c): Let $\rho: V \rightarrow V \otimes \mathcal{O}(G)$ be the comodule corresponding to a representation of G . 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 (28), p. 69,

$$\begin{cases} (\mathrm{id}_V \otimes \Delta) \circ \rho &= (\rho \otimes \mathrm{id}_{\mathcal{O}(G)}) \circ \rho \\ (\mathrm{id}_V \otimes \epsilon) \circ \rho &= \mathrm{id}_V. \end{cases}$$

to v , we find that

$$\begin{aligned} \sum_i u_i \otimes e_i \otimes e_i &= \sum_i \rho(u_i) \otimes e_i \\ v &= \sum u_i. \end{aligned}$$

The first equality shows that

$$\rho(u_i) = u_i \otimes e_i \in \langle u_i \rangle \otimes_k \mathcal{O}(G),$$

and the second shows that the set of u_i arising in this way span V .

(c) \Rightarrow (a): In particular, the regular representation of G is diagonalizable, and so $\mathcal{O}(G)$ is spanned by its eigenvectors. Let $f \in \mathcal{O}(G)$ be an eigenvector for the regular representation, and let χ be the corresponding character. Then

$$f(hg) = f(h)\chi(g) \quad \text{for } h, g \in G(R), R \text{ a } k\text{-algebra.}$$

In particular, $f(g) = f(e)\chi(g)$, and so f is a scalar multiple of χ . Hence $\mathcal{O}(G)$ is spanned by its characters.

(b) \Rightarrow (c): As every representation is a union of finite-dimensional subrepresentations (4.7), (b) implies that every representation is a sum (not necessarily direct) of one-dimensional subrepresentations.

(c) \Rightarrow (b): Trivial.

(c) \Rightarrow (d): Certainly, (c) implies that $V = \sum_{\chi \in X(G)} V_\chi$, and Theorem 4.17 implies that the sum is direct.

(d) \Rightarrow (c): Clearly each space V_χ is a sum of one-dimensional representations. \square

ASIDE 14.13. Let M be a finitely generated abelian group, and let V be a finite-dimensional k -vector space. An M -gradation of 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 . This follows from (d) of the theorem. See also (11.28).

e. Tori

DEFINITION 14.14. An algebraic group G is a **split torus** if it is isomorphic to a finite product of copies of \mathbb{G}_m , and it is a **torus** if $T_{k^{\text{sep}}}$ is a split torus.

Equivalently, a split torus is a connected diagonalizable algebraic group. Under the equivalence of categories $M \rightsquigarrow D(M)$ (see 14.9a), the split tori correspond to free commutative groups M of finite rank. A quotient of a split torus is again a split torus (because it corresponds to a subgroup of a free commutative group of finite rank), but an algebraic subgroup of a split torus need not be a split torus. For example, μ_n is a subgroup of \mathbb{G}_m (the map $\mu_n \rightarrow \mathbb{G}_m$ corresponds to $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$).

EXAMPLE 14.15. Let T be the split torus $\mathbb{G}_m \times \mathbb{G}_m$. Then $X(T) \simeq \mathbb{Z} \oplus \mathbb{Z}$, and the character corresponding to $(m_1, m_2) \in \mathbb{Z} \oplus \mathbb{Z}$ is

$$(t_1, t_2) \mapsto t_1^{m_1} t_2^{m_2}: T(R) \rightarrow \mathbb{G}_m(R).$$

Every representation V of T decomposes into a direct sum

$$V = \bigoplus_{(m_1, m_2) \in \mathbb{Z} \times \mathbb{Z}} V_{(m_1, m_2)},$$

where $V_{(m_1, m_2)}$ is the subspace of V on which $(t_1, t_2) \in T(k)$ acts on as $t_1^{m_1} t_2^{m_2}$ [not quite]. In this way, the category $\text{Rep}(T)$ acquires a gradation by the group $\mathbb{Z} \times \mathbb{Z}$.

f. Groups of multiplicative type

DEFINITION 14.16. An algebraic group G is of **multiplicative type** if $G_{k^{\text{sep}}}$ is diagonalizable.

A connected algebraic group of multiplicative type is a torus. Subgroups and quotient groups (but not necessarily extensions) of groups of multiplicative type are of multiplicative type because this is true of diagonalizable groups (14.9).

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).

Let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$ 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.,

$$M = \bigcup_K M^{\text{Gal}(k^{\text{sep}}/K)}$$

where K runs through the finite extensions of k contained in k^{sep} .

For an algebraic group G , we define $X^*(G) = X(G_{k^{\text{sep}}})$; in other words,

$$X^*(G) = \text{Hom}(G_{k^{\text{sep}}}, (\mathbb{G}_m)_{k^{\text{sep}}}).$$

The group Γ acts on $X^*(G)$, and because every homomorphism $G_{k^{\text{sep}}} \rightarrow \mathbb{G}_m$ 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

$$X^*(G_1 \times G_2) \simeq X^*(G_1) \oplus X^*(G_2).$$

The tori are the groups G of multiplicative type such that $X^*(G)$ is torsion free.

THEOREM 14.17. *The functor X^* is a contravariant equivalence from the category of algebraic groups of multiplicative type over k to the category of finitely generated commutative groups equipped with a continuous action of Γ . Under the equivalence, short exact sequences correspond to short exact sequences.*

PROOF. To give a continuous semilinear action of Γ on $k^{\text{sep}}[M]$ is the same as giving a continuous action of Γ on M by group homomorphisms: every action of G on $k^{\text{sep}}[M]$ preserves M because it is the set of group-like elements in $k^{\text{sep}}[M]$; conversely, an action of Γ on M extends semilinearly to an action of Γ on $k^{\text{sep}}[M]$. Thus, the theorem follows from Theorem 14.9 and Galois descent (A.55, A.56). \square

COROLLARY 14.18. *For every algebraic group D of multiplicative type, there is an exact sequence*

$$e \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow e$$

with G' a torus and G'' finite (of multiplicative type).

PROOF. Let $D = D(M)$; then the sequence corresponds to

$$0 \rightarrow M_{\text{tors}} \rightarrow M \rightarrow M/M_{\text{tors}} \rightarrow 0. \quad \square$$

Let G be a group of multiplicative type over k . For every $K \subset k^{\text{sep}}$,

$$G(K) = \text{Hom}(X^*(G), k^{\text{sep}\times})^{\Gamma_K}$$

where Γ_K is the subgroup of Γ of elements fixing K , and the notation means the $G(K)$ equals the group of homomorphisms $X^*(G) \rightarrow k^{\text{sep}\times}$ commuting with the actions of Γ_K .

EXAMPLE 14.19. Take $k = \mathbb{R}$, so that Γ is cyclic of order 2, and let $X^*(G) = \mathbb{Z}$. Then $\text{Aut}(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$, and so there are two possible actions of Γ on $X^*(G)$.

- (a) Trivial action. Then $G(\mathbb{R}) = \mathbb{R}^\times$, and $G \simeq \mathbb{G}_m$.
- (b) The generator ι of Γ acts on \mathbb{Z} as $m \mapsto -m$. Then $G(\mathbb{R}) = \text{Hom}(\mathbb{Z}, \mathbb{C}^\times)^\Gamma$ consists of the elements of \mathbb{C}^\times fixed under the following action of ι ,

$$\iota z = \bar{z}^{-1}.$$

Thus $G(\mathbb{R}) = \{z \in \mathbb{C}^\times \mid z\bar{z} = 1\}$, which is compact.

EXAMPLE 14.20. Let K be a finite separable extension of k , and let T be the functor $R \mapsto (R \otimes_k K)^\times$. Then T is the group of multiplicative type corresponding to the Γ -module $\mathbb{Z}^{\text{Hom}_k(K, k^{\text{sep}})}$ (families of elements of \mathbb{Z} indexed by the k -homomorphisms $K \rightarrow k^{\text{sep}}$). See 14.39 below.

EXAMPLE 14.21. The algebraic group μ_n is of multiplicative type for all n . The constant algebraic group $\mathbb{Z}/n\mathbb{Z}$ is of multiplicative type if n is not divisible by the characteristic (in nonzero characteristic p , the algebraic group $\mathbb{Z}/p\mathbb{Z}$ is unipotent and not of multiplicative type).

g. Representations of a group of multiplicative type

When G is a diagonalizable algebraic group, $\text{Rep}(G)$ is a semisimple abelian category¹ whose simple objects are in canonical one-to-one correspondence with the characters of G (14.12). When G is of multiplicative type, the description of $\text{Rep}(G)$ is only a little more complicated.

Let k^{sep} be a separable closure of k , and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$.

THEOREM 14.22. *Let G be an algebraic group of multiplicative type over k . Then $\text{Rep}(G)$ is a semisimple abelian category whose simple objects are in canonical one-to-one correspondence with the orbits of Γ acting on $X^*(G)$.*

PROOF. The group G is split by a finite Galois extension Ω of k — let $\bar{\Gamma} = \text{Gal}(\Omega/k)$. Then $\bar{\Gamma}$ act on $\mathcal{O}(G_\Omega) \simeq \Omega \otimes \mathcal{O}(G)$ through its action on Ω . Let (V, r) be a representation of G_Ω , 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.54, A.55, A.56) that the functor $V \mapsto V_\Omega$ from $\text{Rep}_k(G)$ to the category of objects of $\text{Rep}_\Omega(G_\Omega)$ equipped with a semilinear action of $\bar{\Gamma}$ is an equivalence of categories.

Let V be a finite-dimensional representation of G_Ω equipped with a semilinear action of $\bar{\Gamma}$. Then

$$V = \bigoplus_{\chi \in X(G_\Omega)} V_\chi.$$

An element γ of $\bar{\Gamma}$ acts on V by mapping V_χ isomorphically onto $V_{\gamma\chi}$. Therefore, as a representation of G_Ω equipped with a semilinear action of $\bar{\Gamma}$, V decomposes into a direct sum of simple objects corresponding to the orbits of $\bar{\Gamma}$ acting on $X(G_\Omega)$. As these are also the orbits of Γ acting on $X^*(G) \simeq X(G_\Omega)$, the statement follows. \square

ASIDE 14.23. Should add a description of the endomorphism algebra of each simple object, thereby completing the determination of the category up to equivalence.

¹An abelian category is semisimple if every object is semisimple, i.e., a finite direct sum of simple objects. To describe a semisimple abelian category up to equivalence, it suffices to list the isomorphism classes of simple objects and their endomorphism rings.

h. Criteria for an algebraic group to be of multiplicative type

Recall that a coalgebra over k to be a k -vector space C together with a pair of k -linear maps

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

such that the diagrams (20), p.56, commute. The linear dual C^\vee of C becomes an associative algebra over k with the multiplication

$$C^\vee \otimes C^\vee \xrightarrow{\text{can.}} (C \otimes C)^\vee \xrightarrow{\Delta^\vee} C^\vee, \tag{92}$$

and the structure map

$$k \simeq k^\vee \xrightarrow{\epsilon^\vee} C^\vee. \tag{93}$$

We say that C is *cocommutative* (resp. *coétale*) if C^\vee is commutative (resp. étale). More generally, we say that a cocommutative coalgebra over k is *coétale* if every finite-dimensional subcoalgebra is coétale.

Let (C, Δ, ϵ) be a coalgebra over k . A C -comodule is a k -linear map $\rho: V \rightarrow V \otimes C$ satisfying the conditions (28), p.69. In terms of a basis $(e_i)_{i \in I}$ for V , these conditions become

$$\left. \begin{aligned} \Delta(c_{ij}) &= \sum_{k \in I} c_{ik} \otimes c_{kj} \\ \epsilon(c_{ij}) &= \delta_{ij} \end{aligned} \right\} \quad \text{all } i, j \in I. \tag{94}$$

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. When V is finite dimensional over k , so also is C_V . If (V, ρ) is a sub-comodule of the C -comodule (C, Δ) , then $V \subset C_V$.

THEOREM 14.24. *The following conditions on an algebraic group G over k are equivalent:*

- (a) G is of multiplicative type (14.16);
- (b) G becomes diagonalizable over some field $K \supset k$;
- (c) G is commutative and $\text{Hom}(G, \mathbb{G}_a) = 0$;
- (d) G is commutative and $\mathcal{O}(G)$ is coétale.

PROOF. (a) \Rightarrow (b): Trivial — by definition, G becomes diagonalizable over k^{sep} .

(b) \Rightarrow (c): Clearly

$$\text{Hom}(G, \mathbb{G}_a) \simeq \{f \in \mathcal{O}(G) \mid \Delta(f) = f \otimes 1 + 1 \otimes f\}. \tag{95}$$

The condition on f is linear, and so, for any field $K \supset k$,

$$\text{Hom}(G_K, \mathbb{G}_{aK}) \simeq \text{Hom}(G, \mathbb{G}_a) \otimes K.$$

Thus, we may extend k and suppose that G is diagonalizable. If $u: G \rightarrow \mathbb{G}_a$ is a nontrivial homomorphism, then

$$g \mapsto \begin{pmatrix} 1 & u(g) \\ 0 & 1 \end{pmatrix}$$

is a nonsemisimple representation of G , which contradicts (14.12). (Alternatively, applying 14.22 avoids extending the base field.)

(c) \Rightarrow (d): We may assume that k is algebraically closed. Let C be finite-dimensional subcoalgebra of $\mathcal{O}(G)$, i.e., a finite-dimensional k -subspace such that $\Delta(C) \subset C \otimes C$. Let

$A = C^\vee$. Then A is a finite product of local Artin rings with residue field k (CA 16.7). If one of these local rings is not a field, then there exists a surjective homomorphism of k -algebras

$$A \rightarrow k[\varepsilon], \quad \varepsilon^2 = 0.$$

This can be written $x \mapsto \langle x, a \rangle + \langle x, b \rangle \varepsilon$ for some $a, b \in C$ with $b \neq 0$. For $x, y \in A$,

$$\langle xy, a \rangle + \langle xy, b \rangle \varepsilon = \langle x \otimes y, \Delta a \rangle + \langle x \otimes y, \Delta b \rangle \varepsilon$$

(definition (92) of the product in A) and

$$\begin{aligned} (\langle x, a \rangle + \langle x, b \rangle \varepsilon)(\langle y, a \rangle + \langle y, b \rangle \varepsilon) &= \langle x, a \rangle \langle y, a \rangle + (\langle x, a \rangle \langle y, b \rangle + \langle x, b \rangle \langle y, a \rangle) \varepsilon \\ &= \langle x \otimes y, a \otimes a \rangle + \langle x \otimes y, a \otimes b + b \otimes a \rangle \varepsilon. \end{aligned}$$

On equating these expressions, we find that

$$\begin{aligned} \Delta a &= a \otimes a \\ \Delta b &= a \otimes b + b \otimes a. \end{aligned}$$

On the other hand, the structure map $k \rightarrow A$ is $(\varepsilon|C)^\vee$, and so $\varepsilon(a) = 1$. Now

$$1 = (e \circ \varepsilon)(a) = ((S, \text{id}_A) \circ \Delta)(a) = S(a)a$$

and so a is a unit in A . Finally,

$$\begin{aligned} \Delta(ba^{-1}) &= \Delta b \cdot \Delta a^{-1} = (a \otimes b + b \otimes a)(a^{-1} \otimes a^{-1}) \\ &= 1 \otimes ba^{-1} + ba^{-1} \otimes 1, \end{aligned}$$

and so $\text{Hom}(G, \mathbb{G}_a) \neq 0$ (see (95)), which contradicts (c). Therefore A is a product of fields.

(d) \Rightarrow (a): We may suppose that k is separably closed. Let C be a finite-dimensional subcoalgebra of $\mathcal{O}(G)$, and let $A = C^\vee$. By assumption, A is a product of copies of k . Let a_1, \dots, a_n be elements of C such that

$$x \mapsto (\langle x, a_1 \rangle, \dots, \langle x, a_n \rangle): A \rightarrow k^n$$

is an isomorphism. Then 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 where V runs over the finite-dimensional subcomodules of $\mathcal{O}(G)$; see (4.6) and the discussion preceding the statement of the theorem). \square

In particular, if an algebraic group over k becomes diagonalizable over an algebraic closure of k , then it becomes diagonalizable over a finite separable extension of k .²

²Here is Tate's short direct proof of this (from Borel and Tits 1965, 1.5): Let k^{al} be an algebraic closure of k . As $X^*(T)$ is finitely generated, it suffices to show that every element $a \in X^*(T)$ is defined over k^{sep} . But T is diagonalizable over k^{al} , and so a is defined over k^{al} . Replacing k with k^{sep} , we see that it suffices to prove that, if a is defined over a purely inseparable extension of k , then it is defined over k .

There is nothing to prove if $p = 0$. Otherwise, let $q = p^s$ ($s \in \mathbb{Z}$, $s > 0$) be a power of p sufficiently large that a is defined over $k^{1/q}$. We have $a(t^q) = a^q(t) \in k(t)$ for $t \in T(K)$, and so

$$a(t^q) \in k(t) \cap k^{1/q}(t^q).$$

But if t is generic over k (i.e., $k(t) \simeq k(T)$), then the field $k(t)$ is linearly disjoint from k^{al} , and so $k(t) \cap k^{1/q}(t^q) = k(t^q)$ and $a(t^q) \in k(t^q)$. The element t^q is also generic over k as $x \mapsto x^q$ is a bijective morphism from T onto itself; the inclusion $a(t^q) \in k(t^q)$ shows that a is defined over k .

COROLLARY 14.25. *If a torus splits over a purely inseparable extension of k , then it is already split over k . In particular, every torus over a separably closed field is split.*

PROOF. The k -algebra $\mathcal{O}(G)$ is co-étale, and so $\mathcal{O}(G)^\vee$ is a union of étale subalgebras. An étale algebra over k is diagonalizable over k if it becomes diagonalizable over a purely inseparable extension of k . (In proving this, we may suppose that the étale algebra is a finite separable field extension K of k . If $K \otimes k'$ is diagonalizable for some purely inseparable extension k' of k , then there exists a k -algebra homomorphism $K \hookrightarrow k'$, and so the extension K/k is both separable and purely inseparable, hence trivial.) \square

COROLLARY 14.26. *A smooth commutative algebraic group G is of multiplicative type if and only if $G(k^{\text{al}})$ 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 $G \subset \mathbb{D}_n$. \square

Later (18.29), we shall show that “commutative” can be replaced by “connected”: every smooth connected algebraic group such that $G(k^{\text{al}})$ consists of semisimple elements is a torus.

COROLLARY 14.27. *An extension*

$$e \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow e \quad (96)$$

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, the exact sequence (96) gives rise to an exact sequence

$$0 \rightarrow \text{Hom}(G'', \mathbb{G}_a) \rightarrow \text{Hom}(G, \mathbb{G}_a) \rightarrow \text{Hom}(G', \mathbb{G}_a)$$

of abelian groups, and we can apply the criterion (14.24c). \square

i. Rigidity

For algebraic groups G, G' and a k -algebra R , we let $\underline{\text{Hom}}(G, G')(R)$ denote the set of homomorphisms of R -algebras $\mathcal{O}(G')_R \rightarrow \mathcal{O}(G)_R$ compatible with the comultiplications. Then $\underline{\text{Hom}}(G, G')$ is a functor from k -algebras to sets. Because of the Yoneda lemma, this agrees with the similar terminology for functors p.38, p.210, p.139. Note that

$$\underline{\text{Hom}}(G, G')(k) = \text{Hom}(G, G').$$

When G and G' are commutative, $\underline{\text{Hom}}(G, G')$ is a functor to commutative groups.

LEMMA 14.28. *Let V be a k -vector space, and let M be a finitely generated commutative group. Then the family of quotient maps*

$$V \otimes k[M] \rightarrow V \otimes k[M/nM], \quad n \geq 2,$$

is injective.

PROOF. An element f of $V \otimes k[M]$ can be written uniquely in the form

$$f = \sum_{x \in M} f_x \otimes x, \quad f_x \in V.$$

Assume $f \neq 0$, and let $I = \{x \in M \mid f_x \neq 0\}$. As I is finite, for some n , the elements of I will remain distinct in M/nM , and for this n , the image of f in $V \otimes_k k[M/nM]$ is nonzero. \square

THEOREM 14.29. *Every action of a connected algebraic group G on an algebraic group H of multiplicative type is trivial.*

PROOF. We may suppose that k is algebraically closed. We first prove the theorem in the case that H is finite. An action of G on $H = \mu_n$ is a homomorphism

$$G \rightarrow \underline{\text{Aut}}(\mu_n) \subset \underline{\text{Hom}}(\mu_n, \mu_n) \simeq \underline{\text{Hom}}(\mu_n, \mathbb{G}_m) \stackrel{(13.31)}{\simeq} \mathbb{Z}/n\mathbb{Z},$$

which is trivial because G is connected. Every finite algebraic group H of multiplicative type is a finite product of groups of the form μ_n (14.3). Therefore $\underline{\text{Hom}}(H, H)$ is an étale scheme, and $G \rightarrow \underline{\text{Aut}}(H) \subset \underline{\text{Hom}}(H, H)$ is trivial.

We now prove the general case. As k is algebraically closed, the group H is diagonalizable. We saw above, that G acts trivially on H_n for all n . Let $H = D(M)$ with M a finitely generated commutative group. Then $\mathcal{O}(H) = k[M]$ and $\mathcal{O}(H_n) = k[M/nM]$. Let

$$\rho: k[M] \rightarrow \mathcal{O}(G) \otimes k[M]$$

be the homomorphism of k -algebras corresponding to the action $G \times D(M) \rightarrow D(M)$. We have to show that $\rho(x) = 1 \otimes x$ for each $x \in k[M]$, but this follows from the fact that G acts trivially on H_n for all $n \geq 2$, and the family of maps

$$\mathcal{O}(G) \otimes_k k[M] \rightarrow \mathcal{O}(G) \otimes_k k[M/nM], \quad n \geq 2,$$

is injective (14.28). \square

COROLLARY 14.30. *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; hence $N \subset Z(G)$. \square

COROLLARY 14.31. *Let T be a subtorus of an algebraic group G . Then $N_G(T)^\circ = C_G(T)^\circ$.*

PROOF. Apply (14.30) to $T \subset N_G(T)^\circ$. \square

Hence, $N_G(T)/C_G(T)$ is finite.

COROLLARY 14.32. Let H be an extension of algebraic groups H' and H'' of multiplicative type:

$$e \rightarrow H' \rightarrow H \rightarrow H'' \rightarrow e.$$

Every action of a connected algebraic group G on H preserving H' is trivial.

PROOF. The action of G on H is given by a map $G \rightarrow \underline{\mathrm{Hom}}(H, H)$, which (14.29) shows takes values in the subfunctor $\underline{\mathrm{Hom}}(H'', H')$. It therefore defines an action of G on $H' \times H''$, which is trivial by (14.29) again. \square

When H is smooth, Lemma 14.28 can be replaced in the proof of Theorem 14.29 by the following result (which we shall use in the proof of 16.3).

PROPOSITION 14.33. Let H be a smooth algebraic group of multiplicative type. The family subschemes H_n is schematically dense in H . In particular, $\bigcup_n H_n(k)$ is dense in $|H|$. Here n runs over the integers $n \geq 1$ prime to the characteristic of k .

PROOF. Let X be a closed subvariety of H containing $\bigcup H_n(k)$. Then X contains every étale algebraic subgroup of H . Moreover, X contains an infinite subset of every copy of \mathbb{G}_m contained in H , and therefore contains \mathbb{G}_m . As H is a product of an étale algebraic group with some copies of \mathbb{G}_m (14.5), this proves the statement. \square

REMARK 14.34. In (16.46) below, we prove that extensions of connected multiplicative groups by multiplicative groups are multiplicative.

EXERCISE 14.35. Let R be a k -algebra with no idempotents except 0 and 1. Show that

$$\underline{\mathrm{Hom}}(\mathbb{G}_m, \mathbb{G}_m)(R) \simeq \mathbb{Z}.$$

(Hint: let $e_i = T^i$, and argue as in the proof of 4.16.) Deduce that, for all finitely generated \mathbb{Z} -modules Γ, Γ' ,

$$\underline{\mathrm{Hom}}(D(\Gamma), D(\Gamma')) \simeq \mathrm{Hom}(\Gamma', \Gamma)_k$$

(sheaf associated with the constant presheaf $R \rightsquigarrow \mathrm{Hom}(\Gamma', \Gamma)$).

ASIDE 14.36. Let M be a finitely generated \mathbb{Z} -module. Define M_k to be the affine group scheme (not necessarily algebraic) over k such that $M_k(T) = \mathrm{Hom}(\pi_0(T), M)$ for all algebraic schemes T . For finitely generated \mathbb{Z} -modules M, M'

$$\underline{\mathrm{Hom}}(D(M), D(M')) \simeq \mathrm{Hom}(M', M)_k.$$

See Exercise 14.35. Hence,

$$\mathrm{Hom}(T, \underline{\mathrm{Hom}}(D(M), D(M'))) \simeq \mathrm{Hom}(\pi_0(T), \mathrm{Hom}(M', M)).$$

Explanation to be added.

j. Unirationality

14.37. For an irreducible variety X over k , we let $k(X)$ denote the field of rational functions on X . Recall that an irreducible variety X is said to be **rational** (resp. **unirational**) if $k(X)$ 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).

LEMMA 14.38. *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, and let R be a k -algebra. Then

$$R' \stackrel{\text{def}}{=} k' \otimes R = Re_1 \oplus \cdots \oplus Re_n.$$

Let $\alpha \in R'$, and write $\alpha = a_1e_1 + \cdots + a_n e_n$. Then

$$\alpha \mapsto (a_1, \dots, a_n): (\mathbb{A}^1)_*(R) \rightarrow \mathbb{A}^n(R)$$

gives an isomorphism of functors $(\mathbb{A}^1)_* \rightarrow \mathbb{A}^n$, and hence of algebraic varieties. There exists a polynomial $P \in k[X_1, \dots, X_n]$ such that $\text{Nm}_{R'/R}(\alpha) = P(a_1, \dots, a_n)$. The isomorphism $(\mathbb{A}^1)_* \rightarrow \mathbb{A}^n$ of algebraic varieties identifies $(\mathbb{G}_m)_{k'/k}$ with the complement of the zero set of P in \mathbb{A}^n . \square

LEMMA 14.39. *Let k' be a finite separable extension of k . Then*

$$X^*((\mathbb{G}_m)_{k'/k}) \simeq \mathbb{Z}^{\text{Hom}_k(k', k^{\text{sep}})}$$

(as $\text{Gal}(k^{\text{sep}}/k)$ -modules).

PROOF. Here $\mathbb{Z}^{\text{Hom}_k(k', k^{\text{sep}})}$ is the free abelian group on the set of k -homomorphisms $k' \rightarrow k^{\text{sep}}$. Under the isomorphism, an element of the right hand side corresponds to the character χ of $((\mathbb{G}_m)_{k'/k})_{k^{\text{sep}}}$ such that, for each k^{sep} -algebra R , $\chi(R)$ is the map

$$c \otimes r \mapsto \left(\prod \sigma(c)^{n_\sigma} \right) r: (k' \otimes R)^\times \rightarrow R^\times. \quad \square$$

LEMMA 14.40. *Every torus T is a quotient of a product of tori of the form $(\mathbb{G}_m)_{k'/k}$ for varying k' .*

PROOF. Let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$, 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 $\mathbb{Z}[\Gamma/\Delta] \rightarrow M$ sending 1 to e . On applying this remark to the elements of a finite generating set for M , we get a surjective homomorphism $\prod_i \mathbb{Z}[\Gamma/\Delta_i] \rightarrow M$ 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

$$X^*(T) \rightarrow \bigoplus_i \mathbb{Z}[\Gamma/\Delta_i] \quad (97)$$

of Γ -modules. Let $k_i = (k^{\text{sep}})^{\Delta_i}$. Then $\mathbb{Z}[\Gamma/\Delta_i] \simeq X^*((\mathbb{G}_m)_{k_i/k})$ (14.39), and so the map (97) arises from a surjective homomorphism

$$\prod_i (\mathbb{G}_m)_{k_i/k} \rightarrow T$$

of tori (14.17). \square

PROPOSITION 14.41. *Every torus is unirational.*

PROOF. Combine (14.38) with (14.40). \square

COROLLARY 14.42. For every torus T over an infinite field k , $T(k)$ is dense in T .

PROOF. Combine (14.41) with (14.37). \square

ASIDE 14.43. Let G be a group variety over an infinite field k . Later (in the final version) we shall use (14.41) to show that G is unirational (hence $G(k)$ is dense in G) if either G is reductive or k is perfect.

ASIDE 14.44. A birational homomorphism of connected affine group varieties is an isomorphism (5.15).

k. Actions of \mathbb{G}_m on affine and projective space

Let \mathbb{R}^\times act continuously on \mathbb{R}^n , and let $a \in \mathbb{R}^n$. If $\lim_{t \rightarrow 0} ta$ exists, then it is a fixed point of the action because $t'(\lim_{t \rightarrow 0} ta) = \lim_{t \rightarrow 0} t'ta = \lim_{t \rightarrow 0} ta$. Similarly, if $\lim_{t \rightarrow \infty} ta$ exists, then it is fixed by the action. We prove similar statements in the algebraic setting.

Let $f: \mathbb{G}_m \rightarrow X$ be a regular map from \mathbb{G}_m to a variety X . If f extends to a regular map $\tilde{f}: \mathbb{A}^1 \rightarrow X$, then the extension is unique (because X is separated), and we let $\lim_{t \rightarrow 0} f(t) = \tilde{f}(0)$. Similarly, if f extends to $\tilde{f}: \mathbb{P}^1 \setminus \{0\} \rightarrow X$, we let $\lim_{t \rightarrow \infty} f(t) = \tilde{f}(\infty)$.

14.45. Let \mathbb{G}_m act on \mathbb{A}^n according to the rule

$$t(x_1, \dots, x_n) = (t^{m_1}x_1, \dots, t^{m_n}x_n), \quad t \in \mathbb{G}_m(k), \quad x_i \in k, \quad m_i \in \mathbb{Z}.$$

Assume that the m_i are not all 0. Let $v = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$, and let

$$b_i = \begin{cases} a_i & \text{if } m_i = 0 \\ 0 & \text{otherwise.} \end{cases}$$

The orbit map

$$\mu_v: \mathbb{G}_m \rightarrow \mathbb{A}^n, \quad t \mapsto (t^{m_1}a_1, \dots, t^{m_n}a_n)$$

corresponds to the homomorphism of k -algebras

$$k[T_1, \dots, T_n] \rightarrow k[T, T^{-1}], \quad T_i \mapsto a_i T^{m_i}. \quad (98)$$

Suppose first that $m_i \geq 0$ for all i . Because the m_i lie in \mathbb{N} , this homomorphism takes values in $k[T]$, and so μ_v extends uniquely to a regular map $\tilde{\mu}_v: \mathbb{A}^1 \rightarrow \mathbb{A}^n$, namely, to

$$t \mapsto (a_1 t^{m_1}, \dots, a_n t^{m_n}): \mathbb{A}^1 \rightarrow \mathbb{A}^n.$$

Note that

$$\lim_{t \rightarrow 0} \mu_v(t) \stackrel{\text{def}}{=} \tilde{\mu}_v(0) = (b_1, \dots, b_n),$$

which is 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 (98) maps into $k[T^{-1}]$, and so $\tilde{\mu}_v$ extends uniquely to a regular map $\tilde{\mu}_v: \mathbb{P}^1 \setminus \{0\} \rightarrow \mathbb{A}^n$; moreover

$$\lim_{t \rightarrow \infty} \mu_v(t) \stackrel{\text{def}}{=} \tilde{\mu}_v(\infty) = (b_1, \dots, b_n),$$

which is a fixed by the action of \mathbb{G}_m on \mathbb{A}^n .

Let (V, r) be a finite-dimensional representation of \mathbb{G}_m , and let $V = \bigoplus_{i \in \mathbb{Z}} V_i$ be the decomposition of V into its eigenspaces. Note that $V_0 = V^{\mathbb{G}_m}$, and that the vector (b_1, \dots, b_n) in the above example is the component of (a_1, \dots, a_n) in V_0 . The i for which $V_i \neq 0$ are called the **weights** of \mathbb{G}_m on V .

PROPOSITION 14.46. *Let $v \in V$, and let $v = \sum_i v_i$, $v_i \in V_i$. If the weights of \mathbb{G}_m on V are nonnegative, then the orbit map μ_v extends uniquely to a regular map $\tilde{\mu}_v: \mathbb{A}^1 \rightarrow V$, and*

$$\lim_{t \rightarrow 0} \mu_v(t) \stackrel{\text{def}}{=} \tilde{\mu}_v(0) = v_0.$$

If the weights of \mathbb{G}_m on V are nonpositive, then the orbit map μ_v extends uniquely to a regular map $\tilde{\mu}_v: \mathbb{P}^1 \setminus \{0\} \rightarrow V$, and

$$\lim_{t \rightarrow \infty} \mu_v(t) \stackrel{\text{def}}{=} \tilde{\mu}_v(\infty) = v_0.$$

PROOF. Choose a basis of eigenvectors for V , and apply (14.45). □

A finite-dimensional representation (V, r) of \mathbb{G}_m defines an action

$$\mathbb{G}_m \times \mathbb{P}(V) \rightarrow \mathbb{P}(V), \quad t, [v] \mapsto [r(t)(v)],$$

of \mathbb{G}_m on $\mathbb{P}(V)$. Here $[v]$ denotes the image in $\mathbb{P}(V)$ of an element v of V .

PROPOSITION 14.47. *Let (V, r) be a finite-dimensional representation of \mathbb{G}_m , and let $v \in V$.*

- (a) *The point $[v]$ is a fixed point for the action of \mathbb{G}_m on $\mathbb{P}(V)$ if and only if v is an eigenvector for \mathbb{G}_m in V .*
- (b) *The orbit map $\mu_{[v]}: t \mapsto t[v]: \mathbb{G}_m \rightarrow \mathbb{P}(V)$ extends to a regular map $\tilde{\mu}_{[v]}: \mathbb{P}^1 \rightarrow \mathbb{P}(V)$; either $[v]$ is a fixed point, or the closure of the orbit of $[v]$ in $\mathbb{P}(V)$ has exactly two fixed points, namely, $\lim_{t \rightarrow 0} \mu_{[v]}(t) \stackrel{\text{def}}{=} \tilde{\mu}_{[v]}(0)$ and $\lim_{t \rightarrow \infty} \mu_{[v]}(t) \stackrel{\text{def}}{=} \tilde{\mu}_{[v]}(\infty)$.*

PROOF. The statement (a) is obvious.

Write V as a sum of eigenspaces, $V = \bigoplus_{i \in \mathbb{Z}} V_i$. Let

$$v = v_r + v_{r+1} + \dots + v_s \quad v_i \in V_i.$$

The statement (b) is obvious if $[v]$ is fixed, and so we assume that it isn't. Then $r < s$.

Let e be an eigenvector in V_r . Extend e to a basis $\{e = e_0, \dots, e_n\}$ of eigenvectors for V , and let $\{e^\vee = e_0^\vee, \dots, e_n^\vee\}$ be the dual basis. Then \mathbb{G}_m acts on the affine space

$$D(e^\vee) \stackrel{\text{def}}{=} \{[v] \in \mathbb{P}(V) \mid e^\vee(v) \neq 0\} \approx \mathbb{A}^n$$

with nonnegative weights $0, \dots, s - r$. Therefore (14.46) the orbit map $\mu_{[v]}$ extends to a regular map $\tilde{\mu}: \mathbb{A}^1 \rightarrow \mathbb{A}_r$, and $\tilde{\mu}(0) = [v_r]$ is a fixed point of \mathbb{G}_m acting on \mathbb{A}_r .

Let e_s be an eigenvector in V_s . Then \mathbb{G}_m acts on the affine space $\mathbb{A}_s = \{[v] \in \mathbb{P}(V) \mid e_s^\vee(v) \neq 0\}$ with nonpositive weights, and so $\mu_{[v]}$ extends uniquely to a regular map $\tilde{\mu}: \mathbb{P}^1 \setminus \{0\} \rightarrow \mathbb{A}_s$, and $\tilde{\mu}(\infty) = [v_s]$ is a fixed point of \mathbb{G}_m acting on \mathbb{A}_s (14.46).

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. □

1. Linearly reductive groups

DEFINITION 14.48. An algebraic group is **linearly reductive** if every finite-dimensional representation is semisimple, i.e., a sum (hence a direct sum 4.14) of simple subrepresentations.

REMARK 14.49. If G is linearly reductive, then every representation of G (not necessarily finite-dimensional) is a direct sum of simple representations. To prove this, it suffices to show that the representation is a sum of simple representations (4.14), but as it is a union of its finite-dimensional subrepresentations (4.7), this is obvious.

PROPOSITION 14.50. *A commutative algebraic group is linearly reductive if and only if it is of multiplicative type.*

PROOF. We saw in (14.22) that $\text{Rep}(G)$ is semisimple if G is of multiplicative type. Conversely, if $\text{Rep}(G)$ is semisimple, then $\text{Hom}(G, \mathbb{U}_2) = 0$. But $\mathbb{U}_2 \simeq \mathbb{G}_a$, and so G is of multiplicative type by (14.24). □

EXAMPLE 14.51. Over a field of characteristic 2, the representation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} 1 & ac & bd \\ 0 & a^2 & b^2 \\ 0 & c^2 & d^2 \end{pmatrix} : \text{SL}_2 \rightarrow \text{GL}_3$$

is not semisimple because ac and bd are not linear polynomials in a^2, b^2, c^2, d^2 .

ASIDE 14.52. An algebraic group G over a field of characteristic zero is linearly reductive if and only if G° is reductive. We deduce this later from Weyl’s theorem on the semisimplicity of representations of semisimple Lie algebras. Alternatively, over \mathbb{C} , the reductive algebraic groups are precisely those of the form $G_{\mathbb{C}}$ with G a compact algebraic group over \mathbb{R} (i.e., $G(\mathbb{R})$ is compact and each connected component of G contains an \mathbb{R} -point); the representations of G are obviously semisimple, and they essentially coincide with those of $G_{\mathbb{C}}$.

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 (1962) for group varieties, and is often referred to as Nagata’s theorem. See DG IV, §3, 3.6, p.509, or Kohls 2011.

Let G be a linearly reductive group, and let (V, r) be 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 $\rho : V \rightarrow V^G$ with $\rho|_{V^G} = \text{id}$ and $\rho(V') = 0$.

The group $\text{GL}_n(k)$ acts linearly on $k[T_1, \dots, T_n]$ as follows: let $g = (a_{ij}) \in \text{GL}_n(k)$ and let $f \in k[T_1, \dots, T_n]$; then $(gf)(T_1, \dots, T_n) = f(T'_1, \dots, T'_n)$ with $T'_j = \sum_i a_{ij} T_i$.

THEOREM 14.53 (HILBERT 1890). *Let G be a linearly reductive subgroup of GL_n , and let $A = k[T_1, \dots, T_n]$. Then A^G is a finitely generated 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, the ideal $\mathfrak{a}A$ is finitely generated, say,

$$\mathfrak{a}A = (g_1, \dots, g_m),$$

and we may choose 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 $f \in k[g_1, \dots, g_m]$. Let

$$f = a_1 g_1 + \dots + a_m g_m, \quad a_i \in A.$$

On applying ρ , we find that

$$f = \rho(f) = \rho(r_1)g_1 + \cdots + \rho(r_m)g_m.$$

By induction, the $\rho(r_i)$ lie in $k[g_1, \dots, g_m]$, and so $f \in k[g_1, \dots, g_m]$. \square

ASIDE 14.54. Discuss the history of the finite generation of A^G , and the applications of these results to geometric quotients and geometric invariant theory.

m. The smoothness of fixed subschemes

THEOREM 14.55. *Let G be a linearly reductive group variety acting on a smooth variety X . Then the fixed-point scheme X^G is smooth.*

We shall need to use some basic results on regular local rings. This section can be skipped as we give a different proof of Theorem 14.55 later.

14.56. 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 .

(a) A local ring A is regular if and only if the canonical map

$$\mathrm{Sym}_{\kappa}(\mathfrak{m}/\mathfrak{m}^2) \rightarrow \mathrm{gr}(A) \stackrel{\mathrm{def}}{=} \bigoplus_{n \geq 0} \mathfrak{m}^n / \mathfrak{m}^{n+1}$$

is an isomorphism (Atiyah and Macdonald 1969, 11.22).

(b) Assume that A is regular. Let t_1, \dots, t_d be a regular system of parameters for A , and let $\mathfrak{a} = (t_1, \dots, t_s)$ for some $s \leq d$. Then A/\mathfrak{a} is local of dimension $d - s$, and its maximal ideal $\mathfrak{m}/\mathfrak{a}$ is generated by $\{t_{s+1} + \mathfrak{b}, \dots, t_d + \mathfrak{b}\}$, and so A/\mathfrak{b} is regular (CA 22.2). Every regular quotient of A is of this form.

We require several lemmas.

LEMMA 14.57. *Let A be a regular local ring of dimension d , and let \mathfrak{m} be 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, \dots, t_d for A such that*

$$\mathfrak{a} \equiv (t_1, \dots, t_s) \pmod{\mathfrak{m}^{n+1}}, \quad (99)$$

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 . In order to show that B is regular, we have to show that, for every $n \geq 1$, the canonical map

$$\mathrm{Sym}_{\kappa}^n(\mathfrak{n}/\mathfrak{n}^2) \rightarrow \mathfrak{n}^n / \mathfrak{n}^{n+1}$$

is an isomorphism (14.56a). Fix an n . Let t_1, \dots, t_d be a regular system of parameters for A such that (99) holds for n , and let $\mathfrak{b} = (t_1, \dots, t_s)$. Then

$$\mathfrak{a} + \mathfrak{m}^{i+1} = \mathfrak{b} + \mathfrak{m}^{i+1}$$

for all $i \leq n$, and so

$$\begin{aligned} (\mathfrak{b} + \mathfrak{m}^n) / (\mathfrak{b} + \mathfrak{m}^{n+1}) &\simeq (\mathfrak{a} + \mathfrak{m}^n) / (\mathfrak{a} + \mathfrak{m}^{n+1}) \simeq \mathfrak{n}^n / \mathfrak{n}^{n+1} \\ (\mathfrak{b} + \mathfrak{m}) / (\mathfrak{b} + \mathfrak{m}^2) &\simeq \mathfrak{n} / \mathfrak{n}^2. \end{aligned}$$

The quotient ring A/\mathfrak{b} is regular (14.56b), and so the canonical map

$$\text{Sym}_{B/\mathfrak{n}}^n((\mathfrak{b} + \mathfrak{m}) / (\mathfrak{b} + \mathfrak{m}^2)) \rightarrow (\mathfrak{b} + \mathfrak{m}^n) / (\mathfrak{b} + \mathfrak{m}^{n+1})$$

is an isomorphism (14.56a). The same is therefore true with \mathfrak{a} for \mathfrak{b} . As n was arbitrary, this completes the proof. \square

Let S be a set of automorphisms of a separated algebraic scheme X over k . The functor

$$R \rightsquigarrow \{x \in X(R) \mid sx = x \text{ for all } s \in S\}$$

is represented by the closed subscheme

$$X^S \stackrel{\text{def}}{=} \bigcap_{s \in S} \text{Equalizer}(s, \text{id}: X \rightrightarrows X)$$

of X . When S is a subgroup of $\text{Aut}(X)$, this is the fixed subscheme of the constant group functor $R \rightsquigarrow S$ (see 9.1).

LEMMA 14.58. *Let S be a set of automorphisms of a smooth variety X , and let $x \in X(k)$ be 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 $\mathcal{O}_{X, x} \rightarrow R$ is fixed by the automorphisms in S if and only if it factors through $\mathcal{O}_{X, x} / \mathfrak{a}$, i.e.,

$$\text{Hom}(\mathcal{O}_{X, x}, R)^S = \text{Hom}(\mathcal{O}_{X, x} / \mathfrak{a}, R) \subset \text{Hom}(\mathcal{O}_{X, x}, R).$$

From this the statement follows. \square

LEMMA 14.59. *Let G be a group variety acting on an algebraic variety X . Let $S \subset G(k)$ be dense in $|G|$. If X^S is smooth, then X^G is smooth, and equals X^S .*

PROOF. It suffices to prove that $X^S = X^G$. Clearly, $X^G \subset X^S$, and so it remains to show that G fixes X^S . Let $\mu: G \times X \rightarrow X$ denote the action of G on X . We have to show that μ and p_2 agree on $G \times X^S$. Certainly, they agree on the k^{al} -points of $G \times X^S$ because S is Zariski-dense in $G(k^{\text{al}})$, but this implies that they agree on $G \times X^S$ because $G \times X^S$ is reduced. \square

LEMMA 14.60. *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.*

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 $G(k)$ fixes x , 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 10.6).

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 $V_i, i \geq 1$, a nontrivial simple representation of G (here we use that

G is linearly reductive). Because V_i ($i \geq 1$) is simple, the subset $\{v - sv \mid v \in V_i, s \in S\}$ of V_i spans it, and so this subset contains a basis $(v_{ij})_j$ for V_i . Choose any basis $(v_{0j})_j$ for V_0 . We shall apply Lemma 14.57 to the ideal

$$\mathfrak{a} = \{f - f \circ s \mid f \in \mathfrak{m}, \quad s \in G(k)\}$$

in $\mathcal{O}_{X,x}$. Let $n > 0$. For $i = 0, 1, \dots, r$, choose a G -stable subspace $W_i \subset \mathfrak{m}/\mathfrak{m}^n$ mapping isomorphically onto V_i . Let $w_{ij} \in W_i$ map to v_{ij} , and choose $u_{ij} \in \mathfrak{m}$ such that $u_{ij} \equiv w_{ij} \pmod{\mathfrak{m}^{n+1}}$. Now $\{u_{ij} \mid i \geq 0, j \text{ arbitrary}\}$ is a regular system of parameters for A , and $\{u_{ij} \mid i > 0, j \text{ arbitrary}\}$ generates \mathfrak{a} modulo \mathfrak{m}^{n+1} . Therefore $\mathcal{O}_{X,x}/\mathfrak{a}$ is regular, and we know (14.58) that

$$\mathcal{O}_{X^S,x} = \mathcal{O}_{X,x}/\mathfrak{a}. \quad \square$$

On combining the last two lemmas, we obtain the following variant of (14.55).

THEOREM 14.61. *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 (14.55) because we can take k to be separably closed, and then $S = G(k)$ is dense in $|G|$.

THEOREM 14.62 (SMOOTHNESS OF CENTRALIZERS). *Let H be a linearly reductive group acting on a smooth algebraic group G . Then G^H is smooth.*

PROOF. Special case of Theorem 14.55. □

COROLLARY 14.63. *Let G be a smooth algebraic group, and let H be an algebraic subgroup of G of multiplicative type. Then $C_G(H)$ and $N_G(H)$ are smooth, and $C_G(H)$ is open in $N_G(H)$.*

PROOF. Recall (14.22) that an algebraic group of multiplicative type is linearly reductive. Let H act on G by inner automorphisms. Then $G^H = C_G(H)$, and so $C_G(H)$ is smooth. As an H -module, \mathfrak{h} is a direct factor of \mathfrak{g} , and so the quotient map $\mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h}$ induces a surjection $\mathfrak{g}^H \rightarrow (\mathfrak{g}/\mathfrak{h})^H$. Therefore $C_G(H)$ is open in $N_G(H)$ (12.33). Hence $N_G(H)$ is also smooth. □

COROLLARY 14.64. *Let G be a smooth algebraic group, and let H be a multiplicative algebraic subgroup of G .*

- (a) $N_G(H)$ is the unique smooth algebraic subgroup of G such $N_G(H)(k^{\text{sep}})$ is the normalizer of $H(k^{\text{sep}})$ in $G(k^{\text{sep}})$.
- (b) $C_G(H)$ is the unique smooth algebraic subgroup of G such $C_G(H)(k^{\text{sep}})$ is the centralizer of $H(k^{\text{sep}})$ in $G(k^{\text{sep}})$.

PROOF. As $N_G(H)$ is smooth, $N_G(H)(k^{\text{sep}})$ is dense in $N_G(H)$ and so (1.60) implies that

$$N_G(H)(k^{\text{sep}}) = N_{G(k^{\text{sep}})}(H(k^{\text{sep}}));$$

if N is a second smooth algebraic subgroup of G with this property, then

$$N(k^{\text{sep}}) = (N \cap N_G(H))(k^{\text{sep}}) = N_G(H)(k^{\text{sep}}),$$

and so

$$N = N \cap N_G(H) = N_G(H).$$

Similarly, $C_G(H)(k^{\text{sep}})$ is dense in $C_G(H)$ and we can apply (1.69). □

ASIDE 14.65. Let H be a subgroup variety of a group variety G over an algebraically closed field k . Then $C_G(H)$ is smooth if and only if \mathfrak{h} is *separable* in \mathfrak{g} , i.e., $\dim C_{G(k)}(\mathfrak{h}) = \dim \mathfrak{c}_{\mathfrak{g}}(\mathfrak{h})$ (Herpel 2013, Lemma 3.1).

ASIDE 14.66. Let G be a connected algebraic group over a field k . If k has characteristic zero, then every algebraic group is smooth (3.38); in particular, the centralizers of all algebraic subgroups of G are smooth. If k has characteristic $p \neq 0$ and G is reductive, then this is still true 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, it is true for GL_V and all p , and it is true for SL_V and all p not dividing the dimension of V .

NOTES. The proof of (14.55) follows Iversen 1972.

n. Maps to tori

LEMMA 14.67. Let X and Y be connected algebraic varieties over an algebraically closed field k . Every regular map $u: X \times Y \rightarrow \mathbb{G}_m$ is of the form $u = u_1 \cdot u_2$ with u_1 (resp. u_2) a regular map $X \rightarrow \mathbb{G}_m$ (resp. $Y \rightarrow \mathbb{G}_m$).

PROOF. Let x_0 and y_0 be smooth points on X and Y . We shall, in fact, show that

$$u(x, y) = u(x, y_0) \cdot u(x_0, y) \cdot u(x_0, y_0)^{-1}, \quad x, y \in X, Y. \quad (100)$$

It suffices to prove this on an open neighbourhood of (x_0, y_0) , and so we may assume that X is normal, and that Y is a dense open subset of a normal projective variety \tilde{Y} . We regard u as a rational function \tilde{u} on $X \times \tilde{Y}$, and let D denote its (Weil) divisor. Then $D = p_2^* E$ for some divisor E on \tilde{Y} (if Z is a prime divisor in $\mathrm{supp}(D)$, then $\overline{p_{2*} Z}$ is not equal to \tilde{Y} because $(Z \cap X) \cap Y$ is empty, and so it is a divisor on \tilde{Y}). Consider the rational function

$$y \mapsto \tilde{u}(x, y) \cdot \tilde{u}(x_0, y)^{-1}$$

on \tilde{Y} ; its divisor is $E - E = 0$. As \tilde{Y} is complete, this function is constant, and so

$$\tilde{u}(x, y) = \tilde{u}(x_0, y) \cdot v(x)$$

with v a nowhere vanishing function on X . On putting $y = y_0$, we see that $v(x) = u(x, y_0) \cdot u(x_0, y_0)^{-1}$. \square

PROPOSITION 14.68. Let G be a connected group variety, and let T be a torus. Every regular map $\varphi: G \rightarrow T$ such that $\varphi(e) = e$ is a homomorphism of algebraic groups.

PROOF. We may suppose, first that k is algebraically closed, and then that $T = \mathbb{G}_m$. According to the lemma, there exist regular maps $\varphi_1, \varphi_2: G \rightarrow \mathbb{G}_m$ such that $\varphi \circ m = \varphi_1 \cdot \varphi_2$, i.e.,

$$\varphi(g_1 g_2) = \varphi_1(g_1) \varphi_2(g_2), \text{ all } g_1, g_2 \in G.$$

Then $\varphi_1(e) \varphi_2(e) = e$, and so we can normalize the φ_i to have $\varphi_i(e) = e = \varphi_2(e)$. On taking g_1 (resp. g_2) to be e in the equation, we find that $\varphi = \varphi_2$ (resp. $\varphi = \varphi_1$), and so

$$\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2), \text{ all } g_1, g_2 \in G. \quad \square$$

NOTES. The above proof of (14.67) is due to Oort (see Fossum and Iversen 1973, 2.1).

ASIDE 14.69. For a variety X over a field k , let $U(X) = \Gamma(X, \mathcal{O}_X^\times)/k^\times$. Lemma 14.67 shows that

$$U(X) \oplus U(Y) \simeq U(X \times Y)$$

when k is algebraically closed. In fact, this is true over arbitrary fields (cf. SGA 7, VIII, 4.1): let $(x_0, y_0) \in X(k) \times Y(k)$; it suffices to prove that the identity (100) holds, and, for this, we may extend the base field and then normalize.

ASIDE 14.70. Note the similarity of (14.68) and (10.17). 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) the maximal connected affine group subvariety of G is a torus;
- (b) G contains no algebraic subgroup isomorphic to \mathbb{G}_a ;
- (c) for every connected group subvariety H of G , the torsion points of $H(k)$ of order prime to $\text{char}(k)$ 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. Rosenlicht (ibid. Thm 2, Thm 3) proves Lemma 14.67 for all toroidal algebraic groups, and deduces Proposition 14.68 for such groups.

o. Central tori as almost-factors

DEFINITION 14.71. An algebraic group G is *perfect* if it equals its derived group, i.e., has no nontrivial commutative quotient.

For example, a noncommutative algebraic group having no proper normal subgroup is perfect. A smooth connected algebraic group is perfect if it has no commutative quotient of dimension ≥ 1 .

PROPOSITION 14.72. Let T be a central torus in a connected group variety G .

- (a) The algebraic subgroup $T \cap \mathcal{D}(G)$ is finite.
- (b) If G/T is perfect, then there is an exact sequence

$$e \rightarrow T \cap \mathcal{D}(G) \rightarrow T \times \mathcal{D}(G) \rightarrow G \rightarrow e. \quad (101)$$

In particular, $G/\mathcal{D}(G)$ is a torus.

Note that T is central if it is normal (14.30).

PROOF. (a) To show that an algebraic group N is finite, it suffices to show that $N(k^{\text{al}})$ is finite. Note that

$$(T \cap \mathcal{D}G)(k^{\text{al}}) = T(k^{\text{al}}) \cap (\mathcal{D}G)(k^{\text{al}}).$$

Choose a faithful representation $G_{k^{\text{al}}} \rightarrow \text{GL}_V$ of $G_{k^{\text{al}}}$ (which exists by 4.8), and regard $G_{k^{\text{al}}}$ as an algebraic subgroup of GL_V . Because $T_{k^{\text{al}}}$ 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 14.12). When we choose bases for the V_{χ_i} , the group $T(k^{\text{al}})$ 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 $\text{diag}(\chi_i(t), \dots, \chi_i(t))$, $t \in k^{\text{al}}$. As $\chi_i \neq \chi_j$ for $i \neq j$, we see that the centralizer of $T(k^{\text{al}})$ in $\text{GL}(V)$ consists of the matrices of this shape but with the A_i arbitrary. Because $(\mathcal{D}G)(k^{\text{al}})$ is generated by commutators, its elements have determinant 1 on each summand V_{χ_i} . But $\text{SL}(V_{\chi_i})$ contains only finitely many scalar matrices $\text{diag}(a_i, \dots, a_i)$, and so $T(k^{\text{al}}) \cap (\mathcal{D}G)(k^{\text{al}})$ is finite.

(b) Note that $T \cdot \mathcal{D}G$ is a normal subgroup of G . 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,

$$G = T \cdot \mathcal{D}G,$$

and there exists an exact sequence

$$e \rightarrow T \cap \mathcal{D}(G) \rightarrow \mathcal{D}(G) \rtimes_{\theta} T \rightarrow G \rightarrow e$$

(5.34). Because T is central, θ is trivial, and $\mathcal{D}(G) \rtimes_{\theta} T = \mathcal{D}(G) \times T$. □

EXAMPLE 14.73. The centre of GL_n equals \mathbb{G}_m (nonzero scalar matrices). As $\text{GL}_n/\mathbb{G}_m = \text{PGL}_n$ is simple and noncommutative, it is perfect. The derived group of GL_n is SL_n , and the sequence (101) is

$$1 \rightarrow \mu_n \rightarrow \mathbb{G}_m \times \text{SL}_n \rightarrow \text{GL}_n \rightarrow 1.$$

ASIDE 14.74. We shall see in Chapter 22 that $G = \mathcal{D}G$ and $X(G) = 0$ if G is semisimple. If G is reductive, then its radical RG is a torus and G/RG is semisimple, and so $ZG \cap \mathcal{D}G$ is finite and there is an exact sequence

$$1 \rightarrow RG \cap \mathcal{D}G \rightarrow RG \times \mathcal{D}G \rightarrow G \rightarrow 1$$

Therefore the composite $\mathcal{D}G \rightarrow G \rightarrow G/RG$ is an isogeny of semisimple groups, and the composite $RG \rightarrow G \rightarrow G/\mathcal{D}G$ is an isogeny of tori.

p. Etale slices; Luna's theorem

Throughout this section, k is algebraically closed.

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 (see my notes *Algebraic Geometry*, Chapter 5).

Let Y and X be smooth varieties over k . A regular map $\varphi: Y \rightarrow X$ is *étale* at $P \in Y$ if the map $(d\varphi)_P: T_P(Y) \rightarrow T_{\varphi(P)}(X)$ on tangent spaces is an isomorphism. If φ is étale at P , then it is étale in an open neighbourhood of P .

LEMMA 14.75. *Let x be a smooth point of an affine algebraic variety X of dimension d . Then there exists a regular map $\varphi: X \rightarrow \mathbb{A}^d$ étale at x .*

PROOF. Let $\mathfrak{m} \subset \mathcal{O}(X)$ be the maximal ideal corresponding to x . Because x is smooth, there exist regular functions $f_1, \dots, f_d \in \mathfrak{m}$ whose images in $\mathfrak{m}/\mathfrak{m}^2 \stackrel{\text{def}}{=} T_x(V)^\vee$ span it as a k -vector space. This means that $(df_1)_x, \dots, (df_d)_x$ form a basis for $T_x(V)^\vee$. The map $(f_1, \dots, f_d): U \rightarrow \mathbb{A}^d$ is étale at x because $T_x(U) \rightarrow T_{(0, \dots, 0)}(\mathbb{A}^d)$ is dual to the map $(dT_i)_{(0, \dots, 0)} \mapsto (df_i)_x$. □

The proof of (14.75) can be stated more abstractly as follows: let W be a finite-dimensional k -subspace of \mathfrak{m} mapping isomorphically onto $\mathfrak{m}/\mathfrak{m}^2 = T_x(X)^\vee$, and let $\alpha: (T_x X)^\vee \rightarrow W$ be the inverse isomorphism; the inclusion of W into $\mathcal{O}(X)$ extends uniquely to a homomorphism of k -algebras $\text{Sym}(W) \rightarrow \mathcal{O}(X)$, and the composite of this with $\text{Sym}(\alpha)$ is a homomorphism of k -algebras

$$\text{Sym}((T_x X)^\vee) \rightarrow \mathcal{O}(X),$$

which defines a regular map $\varphi: X \rightarrow (T_x X)_\alpha$ (see 2.6). This is étale at x .

LEMMA 14.76 (LUNA 1972, LEMMA 1). *Let $G \times X \rightarrow X$ be an action of an algebraic group G on an affine algebraic scheme X over k . Let $x \in X(k)^G$ be a smooth point of X such that the isotropy group G_x is linearly reductive. Then there exists a regular map $\varphi: X \rightarrow (T_x X)_\alpha$ such that*

- (a) φ commutes with the actions of G_x ,
- (b) φ is étale at x , and
- (c) $\varphi(x) = 0$.

PROOF. Let $\mathfrak{m} \subset \mathcal{O}(X)$ be the maximal ideal corresponding to x . The quotient map $\mathfrak{m} \rightarrow \mathfrak{m}/\mathfrak{m}^2$ commutes with the action of G_x . Because 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 $\varphi: X \rightarrow (T_x X)_\alpha$ defined by W (as above) has the required properties. \square

An *étale slice at x* is a pair (N, φ) where φ is regular map as in the lemma and N is a complement to $T_x G_x$ in $T_x X$ stable under G_x . If G_x is linearly reductive, then there always exists an N , and hence an étale slice at x . The Luna slice theorem says that, under some hypotheses, it is possible to “integrate” an étale slice.

THE LUNA SLICE THEOREM

Let H be an algebraic subgroup of an algebraic group G . Let $H \times W \rightarrow W$ be an action of H on an algebraic variety W with fixed point o . Let H act on $G \times W$ by $h(g, w) = (gh^{-1}, hw)$, and let

$$G \wedge^H W = H \backslash G \times W.$$

Then G acts on $X = G \wedge^H W$ by $g \cdot [g', w] = [gg', w]$ and H is contained in the isotropy group of $[e, o]$. The Luna slice theorem says, that under some hypotheses on G and X , every algebraic G -scheme X is étale-locally of this form near a point x (and $H = G_x$).

LEMMA 14.77. *Let $G \times X \rightarrow X$ be an action of a reductive algebraic group G on an affine algebraic variety X over a field k of characteristic zero. Let x be a point of X whose orbit is closed. Then the isotropy group G_x at x is reductive.*

PROOF. Matsushima 1960; Luna 1973, p.84. \square

THEOREM 14.78 (LUNA SLICE THEOREM). *Let $G \times X \rightarrow X$ be an action of a reductive algebraic group G on an affine algebraic variety X over a field k of characteristic zero. Let $x \in X(k)$ be a smooth point of X whose orbit O_x is closed. Then there exists a G_x -stable smooth affine subvariety Y of X containing x such that*

- (a) $T_x(X) = T_x(Y) \oplus T_x(O_x)$;

(b) the G -equivariant map

$$[g, y] \mapsto \mu(g, y): G \wedge^{G_x} Y \xrightarrow{\psi} X,$$

is étale and its image U is open in X ;

(c) the map

$$G_x \backslash Y \simeq G \backslash (G \wedge^{G_x} Y) \xrightarrow{G \backslash \psi} G \backslash U$$

is étale at $[x]$;

(d) the maps ψ and $G \wedge^{G_x} Y \rightarrow G \backslash (G \wedge^{G_x} Y) \simeq G_x \backslash Y$ induce an isomorphism

$$G \wedge^{G_x} Y \simeq U \times_{G \backslash U} (G_x \backslash Y).$$

PROOF. The isotropy group G_x is reductive (14.77), hence linearly reductive (14.50), and so we can apply (14.76) to obtain a G_x -equivariant morphism $\varphi: X \rightarrow (T_x X)_\alpha$ étale at x and such that $\varphi(x) = 0$. Choose a G_x -stable subspace N of $T_x X$ such that $T_x(X) = T_x(O_x) \oplus N$. Let $Y = \varphi^{-1}(N)$: it is closed subvariety of X , containing x , smooth at x , and stable under G_x . Moreover, the map $\psi: G \wedge^{G_x} Y \rightarrow X$ is étale at $[e, x]$. On replacing Y with a suitable open neighbourhood of x we obtain a map with the required properties (see Luna 1973 for the details). \square

The subvariety Y of X is also called the *étale slice at x* .

COROLLARY 14.79. Let G be a group variety, and let H be an algebraic subgroup of multiplicative type. Then $C_G(H)$ is smooth.

PROOF. Let H act on G by conjugation, $H \times G \rightarrow G$. According to (14.78) there exists an H -equivariant map $f: G \rightarrow (T_e(G))_\alpha$ such that $f(e) = 0$ and f is étale at e . It follows that $\dim G^H = \dim \mathfrak{g}^H$. But $G^H = C_G(H)$ and $\mathfrak{g}^H = \text{Lie}(C_G(H))$ (12.31), and so $\dim C_G(H) = \dim \text{Lie}(C_G(H))$. Hence $C_G(H)$ is smooth. \square

ASIDE 14.80. The Luna slice theorem is the analogue in algebraic geometry of the slice theorem in differential geometry (Wikipedia ‘‘Slice theorem (differential geometry)’’). It is very important for understanding the local structure of quotients $G \backslash X$, especially moduli varieties. Theorem 14.78 is the original statement of the theorem, except that Luna doesn't assume x to be smooth. For extensions and applications of the theorem, see Bardsley and Richardson 1985; Mehta 2002; Alper 2010, Theorem 2. See also Aside 12.43.

Exercises

EXERCISE 14-1. Show that an extension of linearly reductive algebraic groups is linearly reductive.

EXERCISE 14-2. Verify that the map in (14.51) is a representation of SL_2 , and that the representation is not semisimple.

Unipotent algebraic groups

As always, we fix a field k , and all algebraic groups and homomorphisms are over k unless indicated otherwise.

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

$$\mathbb{U}_n(k) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}.$$

PROPOSITION 15.1. *Let V be a finite-dimensional vector space, and let G be a subgroup of $\text{GL}(V)$. If G consists of unipotent endomorphisms, then there exists a basis of V for which G is contained in \mathbb{U}_n .*

PROOF. We shall use the double centralizer theorem (see, for example, my notes *Class Field Theory*, IV, 1.13.):

Let M be a left module over a ring A (not necessarily commutative), and let $C = \text{End}_A(M)$. If M is semisimple as an A -module and finitely generated as a C -module, then the canonical map $A \rightarrow \text{End}_C(M)$ is surjective.

We now prove (15.1). It suffices to show that $V^G \neq 0$, because then we can apply induction on the dimension of V to obtain a basis of V with the required property (see the proof of 15.3 below). Being fixed by G is a linear condition, and so we may replace k by 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 . As V is simple as an A -module and k is algebraically closed, $\text{End}_A(V) = k \cdot \text{id}_V$ (Schur's lemma). Therefore, $A = \text{End}_k(V)$ (double centralizer theorem). The k -subspace J of A spanned by the elements $g - \text{id}_V$, $g \in G$, is a two-sided ideal in A . Because A is a simple k -algebra, either $J = 0$,

¹For any representation (V, r) of an abstract group G , the subspace V^G of V is the intersection of the kernels of the linear maps $v \mapsto gv - v: V \rightarrow V$ ($g \in G$). It follows that $(V \otimes \bar{k})^{G\bar{k}} \simeq V^G \otimes \bar{k}$, and so $(V \otimes \bar{k})^{G\bar{k}} \neq 0 \Rightarrow V^G \neq 0$.

and the proposition is proved, or $J = A$. But every element of J has trace zero (because the elements of G are unipotent), and so $J \neq A$. \square

b. Unipotent algebraic groups

DEFINITION 15.2. An algebraic group G is **unipotent** if every nonzero representation of G has a nonzero fixed vector, i.e.,

$$(V, r) \text{ a representation of } G, \quad V \neq 0 \implies V^G \neq 0.$$

Equivalently, G is unipotent if it has no nontrivial simple representations (i.e., the only simple representations are the one-dimensional spaces V with the trivial action $V = V^G$). 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 $\rho(v) = v \otimes 1$ (4.24).

Traditionally, a group variety G over an algebraically closed field k is said to be unipotent if every element of $G(k)$ is unipotent (Springer 1998, p.36). Our definition agrees with this (15.12).

As every representation is a union of finite-dimensional representations (4.7), it suffices to check the condition in (15.2) 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 it contains 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 15.3. *An algebraic group G is unipotent if and only if every finite-dimensional representation (V, r) of G is unipotent.*

PROOF. \implies : We use induction on the dimension of V . We may suppose that $V \neq 0$; then there exists a nonzero e_1 in V fixed by G . The induction hypothesis applied to the action of G on $V/\langle e_1 \rangle$ shows that there exist elements e_2, \dots, e_n of V forming a basis for $V/\langle e_1 \rangle$ and such that, relative to this basis, G acts on $V/\langle e_1 \rangle$ through \mathbb{U}_{n-1} . Now $\{e_1, e_2, \dots, e_n\}$ is a basis for V with the required property.

\impliedby : If e_1, \dots, e_n is such a basis, then the subspace spanned by e_1 is fixed by G . \square

We now 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 15.4. A Hopf algebra A is said to be **coconnected** if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \cdots$ of A by subspaces C_i such that²

$$\begin{cases} C_0 = k, \\ \bigcup_{r \geq 0} C_r = A, \\ \Delta(C_r) \subset \sum_{i=0}^r C_i \otimes C_{r-i}. \end{cases} \quad (102)$$

THEOREM 15.5. *The following conditions on an algebraic group G are equivalent:*

²This 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, Moss Eisenberg. Hopf algebras with one grouplike element. Trans. Amer. Math. Soc. 127 1967 515–526.

- (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. (following Waterhouse 1979, 8.3).

(a) \Rightarrow (b). Apply Proposition 15.3 to a faithful finite-dimensional representation of G (which exists by 4.8).

(b) \Rightarrow (c). Every quotient of a coconnected Hopf algebra is coconnected because the image of a filtration satisfying (102) will still satisfy (102), and so it suffices to show that $\mathcal{O}(\mathbb{U}_n)$ is coconnected. Recall that $\mathcal{O}(\mathbb{U}_n) \simeq k[X_{ij} \mid i < j]$, and that

$$\Delta(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \sum_{i < l < j} X_{il} \otimes X_{lj}. \tag{103}$$

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 (102), and it suffices to do this for the monomials in C_r . For the X_{ij} the condition can be read off from (103). 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

$$\begin{aligned} \left(\sum_i C_i \otimes C_{r-i}\right) \left(\sum_j C_j \otimes C_{s-j}\right) &\subset \sum_{i,j} (C_i C_j \otimes C_{r-i} C_{s-j}) \\ &\subset \sum_{i,j} C_{i+j} \otimes C_{r+s-i-j}, \end{aligned}$$

as required.

(c) \Rightarrow (a). Now assume that $A = \mathcal{O}(G)$ is a coconnected Hopf algebra, and let $\rho: V \rightarrow V \otimes A$ be an A -comodule. Then V is a union of the subspaces

$$V_r \stackrel{\text{def}}{=} \{v \in V \mid \rho(v) \in V \otimes C_r\}.$$

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

$$((\text{id} \otimes \Delta) \circ \rho)(V_{r+1}) \subset V \otimes \sum_i C_i \otimes C_{r-i}.$$

Hence $(\text{id} \otimes \Delta) \circ \rho$ maps V_{r+i} to zero in $V \otimes A/C_r \otimes A/C_r$. We now use that $(\text{id} \otimes \Delta) \circ \rho = (\rho \otimes \text{id}) \circ \rho$. If $V_r = 0$, then the map $V \rightarrow V \otimes A/C_r$ defined by ρ is injective, and also the map $V \rightarrow (V \otimes A/C_r) \otimes A/C_r$ defined by $(\rho \otimes \text{id}) \circ \rho$ is injective; hence $V_{r+1} = 0$. \square

COROLLARY 15.6. *An algebraic group is unipotent if and only if it admits a faithful unipotent representation.*

PROOF. Restatement of the equivalence of (a) and (b). \square

COROLLARY 15.7. *Subgroups, quotients, and extensions of unipotent algebraic groups are unipotent.*

PROOF. Let G be a unipotent algebraic group. Then G admits a faithful unipotent representation, and so every algebraic subgroup H of G does also; hence H is unipotent. Every nonzero representation of a quotient Q of G can be regarded as a representation of G , and so it has a nonzero fixed vector; hence Q is unipotent.

Suppose that G contains a normal subgroup N such that both N and G/N are unipotent. Let (V, r) be a nonzero representation of G . The subspace V^N is stable under G (5.24), and the representation of G on it factors through G/N . As V is nonzero, V^N is nonzero, and $V^G = (V^N)^{G/N}$ is nonzero. Hence G is unipotent. \square

COROLLARY 15.8. *Every algebraic group contains a greatest strongly connected unipotent normal algebraic subgroup and a greatest smooth connected unipotent normal algebraic subgroup.*

PROOF. After (15.7), we can apply (8.36) and (8.37). \square

COROLLARY 15.9. *Let k' be a field containing k . An algebraic group G over k is unipotent if and only if $G_{k'}$ is unipotent.*

PROOF. If G is unipotent, then $\mathcal{O}(G)$ is coconnected (15.9). But then $k' \otimes \mathcal{O}(G)$ is obviously coconnected, and so $G_{k'}$ unipotent. Conversely, suppose that $G_{k'}$ is unipotent, and let (V, r) be a representation of G . Then

$$(V \otimes k')^{G_{k'}} \simeq V^G \otimes k',$$

(4.24), and so

$$(V \otimes k')^{G_{k'}} \neq 0 \implies V^G \neq 0. \quad \square$$

COROLLARY 15.10. *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 .*

PROOF. Let (V, r) be a faithful finite-dimensional representation G (which exists by 4.8). If G is unipotent, then $r(G) \subset \mathbb{U}_n$ for some basis of V (15.3), and so $r(g)$ is unipotent for every $g \in G(k)$; this implies that g is unipotent (11.19). 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 $r(G(k)) \subset \mathbb{U}_n(k)$ (15.1). Because $G(k)$ is dense in G , this implies that $r(G) \subset \mathbb{U}_n$. \square

COROLLARY 15.11. *An algebraic subgroup $G(k)$ of GL_V over a perfect field is unipotent if $G(k)$ contains a dense (abstract) subgroup H consisting of unipotent endomorphisms.*

PROOF. There exists a basis of V for which $H \subset \mathbb{U}_n(k)$ (15.1). Because H is dense in G , this implies that $G \subset \mathbb{U}_n$. \square

COROLLARY 15.12. *A smooth algebraic group G is unipotent if and only if $G(k^{\mathrm{al}})$ consists of unipotent elements.*

PROOF. If $G(k^{\mathrm{al}})$ consists of unipotent elements, then $G_{k^{\mathrm{al}}}$ is unipotent (15.10), and so G is unipotent (15.9). Conversely, if G is unipotent, so is $G_{k^{\mathrm{al}}}$ (15.9), and so the elements of $G(k^{\mathrm{al}})$ are unipotent (15.10). \square

COROLLARY 15.13. *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 (15.9), 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 (GT 7.4), every nonzero finite-dimensional representation of H is semisimple, and so it contains a simple representation. Hence H is not unipotent, and it follows that G is not unipotent (15.7). Conversely, a finite p -group over a field of characteristic p has no simple representations,³ and so such a group is unipotent. \square

COROLLARY 15.14. *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 (15.13). \square

PROPOSITION 15.15. *An algebraic group that is both multiplicative and unipotent is trivial.*

PROOF. Let G be such an algebraic group, and let (V, r) be a nonzero finite-dimensional representation of G . Because G is multiplicative, V is semisimple, say, $V = \bigoplus_i V_i$ with V_i simple (14.22), which is impossible because G is unipotent. Therefore, there are no nonzero representations, and so $G = e$. \square

COROLLARY 15.16. *The intersection of a unipotent algebraic subgroup of an algebraic group with an algebraic subgroup of multiplicative type is trivial.*

PROOF. It is both unipotent and multiplicative, because these properties are inherited by subgroups (14.9, 15.7). \square


COROLLARY 15.17. *Every homomorphism from a unipotent algebraic group to an algebraic group of multiplicative type is trivial.*

PROOF. The image is both unipotent and multiplicative (14.9, 15.7). \square

COROLLARY 15.18. *Every homomorphism from an algebraic group of multiplicative type to a unipotent algebraic group is trivial.*

PROOF. The image is both multiplicative and unipotent. \square

In (16.18) below, we shall show that (15.18) remains true over a k -algebra R .

REMARK 15.19. For an algebraic group G , even over an algebraically closed field k , it is possible for all elements of $G(k)$ to be unipotent without G being unipotent. For example, the algebraic group μ_p is not unipotent (it is of multiplicative type), but $\mu_p(k) = 1$ if k has characteristic p . 

EXAMPLE 15.20. 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.

³Standard result — see, for example, Dummit and Foote, Exercise 23, p.820.

EXAMPLE 15.21. Let k be a nonperfect field of characteristic $p \neq 0$, and let $a \in k \setminus k^p$. The algebraic subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by the equation

$$Y^p = X - aX^p$$

becomes isomorphic to \mathbb{G}_a over $k[a^{\frac{1}{p}}]$, but it is not isomorphic to \mathbb{G}_a over k . To see this, we use that G is canonically an open subscheme of the complete regular curve C with function field the field of fractions of $\mathcal{O}(G)$. The complement of G in C consists of a single point with residue field $k[a^{\frac{1}{p}}]$. 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 .

ASIDE 15.22. An algebraic group G over k is a form of \mathbb{G}_a if and only if its underlying scheme is a form of \mathbb{A}^1 . Let U be a form of \mathbb{A}^1 and let C be a complete regular curve containing U as an open subscheme; then $C \setminus U$ consists of a single point P purely inseparable over k . See Russell 1970, 1.1, 1.2.

PROPOSITION 15.23. *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 (8.46) that \mathbb{U}_n has a central series

$$\mathbb{U}_n = U_n^{(0)} \supset \dots \supset U_n^{(r)} \supset U_n^{(r+1)} \supset \dots \supset U_n^{(m)} = e, \quad m = \frac{n(n-1)}{2},$$

whose quotients are canonically isomorphic to \mathbb{G}_a . The intersection of such a series with G has the required properties (cf. 8.1). \square

For example, every form of \mathbb{G}_a is an extension of \mathbb{G}_a by a finite subgroup of \mathbb{G}_a (15.54).

PROPOSITION 15.24. *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 H of G is unipotent (15.7), and (15.23) shows that every nontrivial unipotent algebraic group admits a nontrivial homomorphism to \mathbb{G}_a .

Conversely, suppose that the 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 1 because G is noetherian. Now (15.7) shows that G is unipotent. \square

PROPOSITION 15.25. *Let G be a connected algebraic group, and let N be the kernel of the adjoint representation $\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}$ (see 12.21). Then $N/Z(G)$ is unipotent.*

PROOF. It suffices to prove this with k algebraically closed (15.9). 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 (10.7). The representation on $\mathfrak{m}_e/\mathfrak{m}_e^2$ is the contragredient of the adjoint representation (12.19), 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 (10.7). As $N/Z(G)$ acts trivially on the quotients $\mathfrak{m}_e^i/\mathfrak{m}_e^{i+1}$ of the flag

$$\mathcal{O}_e/\mathfrak{m}^{n+1} \supset \mathfrak{m}_e/\mathfrak{m}^{n+1} \supset \mathfrak{m}_e^2/\mathfrak{m}^{n+1} \supset \dots,$$

it is unipotent (15.6). □

REMARK 15.26. (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 must have dimension 0; hence it is étale, and hence is trivial (15.13).

(b) We saw in (15.23) that every unipotent algebraic group is nilpotent. Conversely, every connected nilpotent algebraic group G contains a greatest subgroup G_s of multiplicative type; the group G_s is characteristic and central, and the quotient G/G_s is unipotent (17.55 below).

PROPOSITION 15.27. *Every connected group variety of dimension one is commutative.*

PROOF. We may assume 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 required. Otherwise, there exists a $g \in G(k) \setminus Z(G)(k)$, and we consider the homomorphism

$$\alpha: G \rightarrow G, \quad x \mapsto xgx^{-1}.$$

Because α is not constant, the closure of its image must be G . Therefore $\alpha(G)$ contains an open subset of G (A.68), and so the complement of $\alpha(G)(k)$ in $G(k)$ is finite. For a faithful representation (V, r) of G , the characteristic polynomial $\det(T - r(y))$ of $y \in G(k)$ is constant on the image of $\alpha(k)$, and so it takes only finitely many values as y runs over $G(k)$. The connectedness of G now implies that these characteristic polynomials are constant, and equal $\det(T - r(e)) = (T - 1)^{\dim V}$. Hence G is unipotent (15.12) and is therefore solvable (15.23). 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 (8.21), this implies that $\mathcal{D}G = e$. □

PROPOSITION 15.28. *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 scheme (i.e., it is quasi-affine).*

PROOF. According to Chevalley's theorem 4.19, 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_a , the isotropy group at any nonzero $x \in L$ is U , and so the map $g \mapsto gx$ is an immersion $G/U \rightarrow V_a$ (9.27). □

ASIDE 15.29. (a) Traditionally, a group variety G is said to be unipotent if its elements in some (large) algebraically closed field are unipotent (Borel 1991, 4.8, p.87; Springer 1998, p.36). For group varieties, this agrees with our definition (15.12).

(b) Demazure and Gabriel (IV, §2, 2.1, p.485) 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 nonzero homomorphism $H \rightarrow \mathbb{G}_a$. For affine algebraic group schemes, this agrees with our definition (15.24).

c. Unipotent algebraic groups in characteristic zero

We describe the structure of unipotent algebraic groups in characteristic zero. *Throughout this section, k is a field of characteristic zero.*

Recall (2.6) that, for a finite-dimensional vector space V , V_a denotes the algebraic group $R \rightsquigarrow R \otimes V$. Recall also that $\text{Lie}(\text{GL}_V) = \mathfrak{gl}_V$, that $\text{Lie}(\text{GL}_n) = \mathfrak{gl}_n$, and that $\text{Lie}(\mathbb{U}_n)$ is the Lie subalgebra

$$\mathfrak{n}_n \stackrel{\text{def}}{=} \{(c_{ij}) \mid c_{ij} = 0 \text{ if } i \geq j\}$$

of \mathfrak{gl}_n (Chapter 12).

LEMMA 15.30. *Let G be a unipotent algebraic subgroup of GL_V (V a finite-dimensional k -vector space V). For a suitable basis of V , $\text{Lie}(G) \subset \mathfrak{n}_n$. In particular, the elements of $\text{Lie}(G)$ are nilpotent endomorphisms of V .*

PROOF. Because, G is unipotent, there exists a basis of V for which $G \subset \mathbb{U}_n$ (15.3). Then

$$\text{Lie}(G) \subset \text{Lie}(\mathbb{U}_n) = \mathfrak{n}_n \subset \text{Lie}(\text{GL}_n) = M_n(k),$$

and the elements of \mathfrak{n}_n are nilpotent matrices. \square

Let V be a finite-dimensional vector space over k . For a nilpotent endomorphism u of the R -module V_R ,

$$\exp(u) \stackrel{\text{def}}{=} I + u + u^2/2! + u^3/3! + \dots$$

is a well defined automorphism of V_R (with inverse $\exp(-u)$).

Let G be a unipotent algebraic group, and let (V, r_V) be a finite-dimensional representation of G . Then r_V defines a representation $dr_V: \mathfrak{g} \rightarrow \mathfrak{gl}_V$ of \mathfrak{g} on V whose image, for a suitable choice of basis for V , is contained in \mathfrak{n}_n (15.30). Therefore, for all k -algebras R and $X \in \mathfrak{g}_R$, there is a well-defined endomorphism $\exp((dr_V)(X))$ of V_R . As (V, r_V) varies, these elements satisfy the conditions of (11.2), and so there exists a (unique) element $\exp(X) \in G(R)$ such that

$$r_V(\exp(X)) = \exp((dr_V)(X))$$

for all (V, r_V) . In this way, we get a homomorphism $\exp: \mathfrak{g}_R \rightarrow G(R)$, natural in R , and hence (by the Yoneda lemma) a morphism of schemes

$$\exp: \mathfrak{g}_a \rightarrow G.$$

One checks directly that, for $X \in \mathfrak{g}_R$ and $g \in G(R)$,

$$\begin{aligned} g \cdot \exp(X) \cdot g^{-1} &= \exp(\text{Ad}(g)(X)) \\ \text{Ad}(\exp(X)) &= 1 + \text{ad}(X) + \text{ad}(X)^2/2! + \text{ad}(X)^3/3! + \dots \end{aligned}$$

Moreover, if $X, Y \in \mathfrak{g}_R$ are such that $[X, Y] = 0$, then

$$\exp(X + Y) = \exp(X) \cdot \exp(Y). \quad (104)$$

PROPOSITION 15.31. *For all unipotent algebraic groups G , the exponential map*

$$\exp: \text{Lie}(G)_a \rightarrow G$$

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 (15.23), and hence equal \mathbb{G}_a (15.26). 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

$$\begin{array}{ccc} \mathrm{Lie}(G)_\mathfrak{a} & \xrightarrow{\exp} & G \\ \downarrow & & \downarrow \\ (\mathrm{Lie}(G)/\mathrm{Lie}(\mathbb{G}_a))_\mathfrak{a} & \xrightarrow{\exp} & G/\mathbb{G}_a. \end{array}$$

The vertical maps are faithfully flat. Moreover, $\mathrm{Lie}(G)_\mathfrak{a}$ is a $\mathrm{Lie}(\mathbb{G}_a)_\mathfrak{a}$ -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 $\exp: \mathrm{Lie}(\mathbb{G}_a)_\mathfrak{a} \rightarrow \mathbb{G}_a$, this shows that the top arrow is an isomorphism.

For the second statement, if G is commutative, then so also is \mathfrak{g} , and (104) shows that \exp is an isomorphism. □

COROLLARY 15.32. *The functor $G \rightsquigarrow \mathrm{Lie}(G)$ 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 , $\mathrm{Lie}(G)_\mathfrak{a} \simeq G$ (15.31), and for each finite-dimensional vector space V , $\mathrm{Lie}(V_\mathfrak{a}) \simeq V$ (12.8). □

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.

15.33. A finite-dimensional Lie algebra \mathfrak{g} is said to be **nilpotent** if it admits a filtration

$$\mathfrak{g} = \mathfrak{a}_r \supset \mathfrak{a}_{r-1} \supset \cdots \supset \mathfrak{a}_1 \supset \mathfrak{a}_0 = 0$$

by ideals such that $[\mathfrak{g}, \mathfrak{a}_i] \subset \mathfrak{a}_{i+1}$ for all i . Note that then

$$[x_1, [x_2, \dots [x_r, y] \dots]] = 0$$

for all $x_1, \dots, x_r, y \in \mathfrak{g}$; in other words,

$$\mathrm{ad}(x_1) \circ \cdots \circ \mathrm{ad}(x_r) = 0$$

for all $x_1, \dots, x_r \in \mathfrak{g}$. We shall need the following two statements:

- (a) a Lie subalgebra of \mathfrak{gl}_V (V a finite-dimensional vector space over k) is nilpotent if it consists of nilpotent endomorphisms (Engel's theorem, LAG I, 2.8);
- (b) every nilpotent Lie algebra \mathfrak{g} admits a faithful representation (V, ρ) such that $\rho(\mathfrak{g})$ consists of nilpotent endomorphisms (Ado's theorem, LAG I, 6.27).

15.34. Let

$$\exp(U) = 1 + U + U^2/2 + U^3/3! + \cdots \in \mathbb{Q}[[U]].$$

The *Campbell-Hausdorff series*⁴ is a formal power series $H(U, V)$ in the noncommuting 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

$$\log(T) = \log(1 - (1 - T)) = -\left(\frac{1-T}{1} + \frac{(1-T)^2}{2} + \frac{(1-T)^3}{3} + \dots\right).$$

Write

$$H(U, V) = \sum_{m \geq 0} H^m(U, V)$$

with $H^m(U, V)$ a homogeneous polynomial of degree m . Then

$$H^0(U, V) = 0$$

$$H^1(U, V) = U + V$$

$$H^2(U, V) = \frac{1}{2}[U, V] = \frac{1}{2}(\text{ad}U)(V)$$

and $H^m(U, V)$, $m \geq 3$, is a sum of terms each of which is a scalar multiple of

$$\text{ad}(U)^r \text{ad}(V)^s(V), \quad r + s = m,$$

or

$$\text{ad}(U)^r \text{ad}(V)^s(U), \quad r + s = m - 1,$$

(Bourbaki LIE, II, §6, no.4, Thm 2.).

For a nilpotent matrix X in $M_n(k)$,

$$\exp(X) \stackrel{\text{def}}{=} 1 + X + X^2/2 + X^3/3! + \dots$$

is a well-defined element of $\text{GL}_n(k)$. If $X, Y \in \mathfrak{n}_n$, then $\text{ad}(X)^n = 0 = \text{ad}(Y)^n$, 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 15.35. *Let G be a unipotent algebraic group. Then*

$$\exp(x) \cdot \exp(y) = \exp(H(x, y)) \tag{105}$$

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 for V (15.30), and so, for $x, y \in \mathfrak{g}_R$,

$$H(x, y) \stackrel{\text{def}}{=} \sum H^m(x, y)$$

is defined and nilpotent, and (105) holds because it holds in \mathfrak{n}_n . □

⁴Bourbaki writes ‘‘Hausdorff’’, Demazure and Gabriel write ‘‘Campbell-Hausdorff’’, and others write ‘‘Baker-Campbell-Hausdorff’’.

THEOREM 15.36. (a) Let \mathfrak{g} be a finite-dimensional nilpotent Lie algebra \mathfrak{g} over k . The maps

$$(x, y) \mapsto H(x, y): \mathfrak{g}(R) \times \mathfrak{g}(R) \rightarrow \mathfrak{g}(R) \quad (R \text{ a } k\text{-algebra})$$

make \mathfrak{g}_α into a unipotent algebraic group over k .

(b) The functor $\mathfrak{g} \rightsquigarrow \mathfrak{g}_\alpha$ 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 $G \rightsquigarrow \text{Lie}(G)$.

PROOF. (a) For the Lie algebra \mathfrak{n}_n , (15.35) shows that the maps make $(\mathfrak{n}_n)_\alpha$ into the algebraic group \mathbb{U}_n . Now we can apply Ado's theorem to deduce the statement for any nilpotent Lie algebra \mathfrak{g} .

(b) The two functors are inverse because $\text{Lie}(\mathfrak{g}_\alpha) \simeq \mathfrak{g}$ and $\text{Lie}(G)_\alpha \simeq G$. □

COROLLARY 15.37. Every Lie subalgebra \mathfrak{g} of \mathfrak{gl}_V formed of nilpotent endomorphisms is the Lie algebra of an algebraic group.

PROOF. According to Engel's theorem, \mathfrak{g} is nilpotent, and so $\mathfrak{g} = \text{Lie}(\mathfrak{g}_\alpha)$. □

ASIDE 15.38. Theorem 15.36 reduces the problem of classifying unipotent algebraic groups in characteristic zero to that of classifying nilpotent Lie algebras which, alas, is complicated. Except in low dimension, there are infinitely many isomorphism classes of a given dimension, and so the classification becomes a question of studying their moduli schemes. In low dimensions, there are complete lists. See [mo21114](#).

ASIDE 15.39. For more details on this section, see DG IV, §2, 4, p.497. See also [Hochschild 1971](#), Chapter 10.

d. Unipotent algebraic groups in nonzero characteristic

Throughout 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

$$Fc = c^\sigma F, \quad c \in k.$$

With $x^{[p]} = Fx$, a $k_\sigma[F]$ -module becomes a p -Lie algebra with trivial bracket (see 12.40).

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 $G \rightarrow \mathbb{G}_a$ amounts to giving an element $f \in \mathcal{O}(G)$ such that

$$\Delta_G(f) = f \otimes 1 + 1 \otimes f. \tag{106}$$

Such an f is said to be *primitive*, and we write $P(G)$ for the set of primitive elements in G ; thus

$$\text{Hom}(G, \mathbb{G}_a) \simeq P(G). \tag{107}$$

EXAMPLE 15.40. Let $f = \sum c_i T^i \in \mathcal{O}(\mathbb{G}_a)$. The condition (106) 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

$$k_\sigma[F] \rightarrow \text{End}(\mathbb{G}_a) \simeq P(\mathbb{G}_a).$$

This sends $\sum b_j F^j$ to the primitive element $\sum b_j T^{p^j}$, and so it is an isomorphism:

$$k_\sigma[F] \simeq \text{End}(\mathbb{G}_a) \simeq P(\mathbb{G}_a). \tag{108}$$

Note that $\sum b_j F^j$ acts on $\mathbb{G}_a(R) = R$ as $c \mapsto \sum b_j c^{p^j}$, and that this is an isomorphism $\mathbb{G}_a \rightarrow \mathbb{G}_a$ if and only if $b_0 \neq 0$ and $b_j = 0$ for $j \neq 0$.

Let G be an algebraic group. From the isomorphism $k_\sigma[F] \simeq \text{End}(\mathbb{G}_a)$, we get an action of $k_\sigma[F]$ on $P(G) \simeq \text{Hom}(G, \mathbb{G}_a)$. 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 15.41. *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 $u: M \rightarrow P(G)$ there is one $(U(M), u_M)$ that is universal: for each pair (G, u) , there exists a unique homomorphism $\alpha: G \rightarrow U(M)$ such that $P(\alpha) \circ u_M = u$:*

$$\begin{array}{ccc} U(M) & & M \xrightarrow{u_M} P(U(M)) \\ \uparrow \exists! \alpha & & \searrow u \quad \downarrow P(\alpha) \\ G & & P(G). \end{array}$$

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

$$U(M) = \text{Spm}(U^{[p]}(M), \Delta).$$

Let $u_M: M \rightarrow P(U(M))$ denote the map defined by $j: M \rightarrow U^{[p]}(M)$. The pair $(U(M), u_M)$ is universal, because

$$\begin{aligned} \text{Hom}(G, U(M)) &\simeq \text{Hom}((U^{[p]}(M), \Delta), (\mathcal{O}(G), \Delta_G)) \\ &\simeq \text{Hom}_{k_\sigma[F]}(M, P(G)). \end{aligned}$$

The second isomorphism states the universal property of $j: M \rightarrow U^{[p]}(M)$ (see p.201). \square

The proposition says that the functor P has an adjoint functor U :

$$\text{Hom}_{k_\sigma[F]}(M, P(G)) \simeq \text{Hom}(G, U(M)). \tag{109}$$

Hence P and U map direct limits to inverse limits (in particular, they map right exact sequences to left exact sequences).

REMARK 15.42. From the bijections

$$\begin{aligned} \operatorname{Hom}(G, U(k_\sigma[F])) &\simeq \operatorname{Hom}_{k_\sigma[F]}(k_\sigma[F], P(G)) && \text{(see (109))} \\ &\simeq P(G) && \text{(obvious)} \\ &\simeq \operatorname{Hom}(G, \mathbb{G}_a) && \text{(see (107))} \end{aligned}$$

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 15.43. *For a finitely generated $k_\sigma[F]$ -module M , the canonical map $u_M: M \rightarrow P(U(M))$ is bijective.*

PROOF. We have to show that the canonical map $j: M \rightarrow U^{[p]}(M)$ 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 12.35 shows that the elements

$$u_n = \prod_{i \in I} \frac{j(e_i)^{n_i}}{n_i!}, \quad n = (n_i)_{i \in I}, \quad 0 \leq n_i < p, \quad (\text{finite product}),$$

form a basis for $U^{[p]}(M)$ as a k -vector space (see 12.41). 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 $v_G: G \rightarrow U(P(G))$ 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 15.44. *For a commutative algebraic group G , the homomorphism $v_G: G \rightarrow U(P(G))$ is a quotient map.*

PROOF. On applying P to the right exact sequence

$$G \xrightarrow{v_G} U(P(G)) \rightarrow Q \rightarrow 0, \quad Q \stackrel{\text{def}}{=} \operatorname{Coker}(v_G),$$

we get a left exact sequence

$$0 \rightarrow P(Q) \rightarrow P(U(P(G))) \xrightarrow{P(v_G)} P(G).$$

As $P(v)$ is bijective, $P(Q) = 0$, and so Q is multiplicative (14.24). As it is also the quotient of a unipotent algebraic group, it is trivial (15.17). □

DEFINITION 15.45. An algebraic group is **elementary unipotent**⁵ if it is isomorphic to an algebraic subgroup of \mathbb{G}_a^r for some r .

With this definition, an algebraic group is unipotent if and only if it has a subnormal series whose quotients are elementary unipotent algebraic groups (15.23).

⁵Springer 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).

THEOREM 15.46. *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 (15.43), 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 (15.42) that every algebraic group in the essential image of U is elementary unipotent. Conversely, let $i: G \rightarrow \mathbb{G}_a^r$ 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 (15.44), it must be an isomorphism (5.13), and so G is in the essential image of the functor U . □

REMARK 15.47. Let G be an algebraic group over k . If G is elementary unipotent, then $V_G = 0$ (see 13.55). We sketch a proof of the converse statement: if $V_G = 0$ then G is elementary unipotent.

To show that G is elementary unipotent, it suffices to show that the homomorphism $v_G: G \rightarrow U(P(G))$ 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 extension of Q by \mathbb{G}_a comes by pullback from the extension (13.58)

$$0 \rightarrow \mathbb{G}_a \rightarrow W_2 \rightarrow \mathbb{G}_a \rightarrow 0. \tag{110}$$

Now consider an algebraic group G such that $V_G = 0$. 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 extend each of canonical projections $N \hookrightarrow \mathbb{G}_a^r \rightarrow \mathbb{G}_a$ to G , then we will get an embedding of G into $\mathbb{G}_a^r \times \mathbb{G}_a$, as required. Let $\varphi: N \rightarrow \mathbb{G}_a$ be a homomorphism, and form the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 0 \\ & & \downarrow \varphi & & \downarrow & & \parallel & & \\ 0 & \longrightarrow & \mathbb{G}_a & \longrightarrow & G' & \longrightarrow & Q & \longrightarrow & 0 \end{array}$$

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 pullback from (110). But $V_{G'} = 0$ because G' is a quotient of $G \times \mathbb{G}_a$, and so the homomorphism $G' \rightarrow W_2$ factors through $\mathbb{G}_a \subset W_2$, and so again φ extends to G . For more details, see DG IV, §3, 6.6, p.521.

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 15.48. *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 proof is the same as for $k[T]$. □

When k is perfect, the map $\sigma: k \rightarrow k$ 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 15.49. *Let k be a perfect field of characteristic $p > 0$. Every finitely generated left $k_\sigma[F]$ -module M is a direct sum of cyclic modules; if, moreover, M has no torsion, then it is free.*

PROOF. The proof is the same as for $k[T]$. See [Berrick and Keating 2000](#), Chapter 3, or [Jacobson 1943](#), Chapter 3. □

PROPOSITION 15.50. *Over a perfect field k of characteristic p , every elementary unipotent algebraic group G is a product of algebraic groups of the form $\mathbb{G}_a, \alpha_{p^r}$ for some r , or an étale group of order a power of p .*

PROOF. Let $A = k_\sigma[G]$. According to (15.49), $P(G)$ 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 15.51. *The only one-dimensional unipotent connected group variety over a perfect field is \mathbb{G}_a .*

PROOF. Immediate consequence of (15.50). □

PROPOSITION 15.52. *Every smooth connected commutative group G of exponent p over a perfect field k is isomorphic to \mathbb{G}_a^r .*

PROOF. Because G is smooth of exponent p , we have $V_G = 0$ (13.55), and so G is an elementary unipotent group (15.47). Therefore it corresponds in (15.46) to the $k_\sigma[F]$ -module $P(G) \simeq \text{Hom}(G, \mathbb{G}_a)$, 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 (15.46). □

COROLLARY 15.53. *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 15.54. Let k be a nonperfect field of characteristic p . For every finite sequence a_0, \dots, 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

$$Y^{p^n} = a_0X + a_1X^p + \dots + a_mX^{p^m}$$

is a form of \mathbb{G}_a , and every form of \mathbb{G}_a arises in this way (Russell 1970, 2.1). Rosenlicht's group (1.43) is of this form. Note that G is the fibred product

$$\begin{array}{ccc} G & \longrightarrow & \mathbb{G}_a \\ \downarrow & & \downarrow a_0 F + \dots + a_m F^{p^m} \\ \mathbb{G}_a & \xrightarrow{F^n} & \mathbb{G}_a. \end{array}$$

In particular, G is an extension of \mathbb{G}_a by a finite subgroup of \mathbb{G}_a (so it does satisfy 15.23). There is a criterion for when two forms are isomorphic (ibid. 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^n th 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. For the classification of elementary unipotent algebraic groups, we have followed DG IV, §3. See also Springer 1998, 3.3, 3.4.

e. *Split and wound unipotent groups: a survey*

Recall the following definition (8.17, 15.23).

DEFINITION 15.55. A unipotent algebraic group G is *split* if it admits a subnormal series whose quotients are isomorphic to \mathbb{G}_a .

Note that a split unipotent algebraic group is automatically smooth and connected (10.1).

15.56. Recall (15.23) that every unipotent algebraic group admits a subnormal series whose quotients are subgroups of \mathbb{G}_a . In characteristic zero, \mathbb{G}_a has no proper subgroups (15.26), and so all unipotent algebraic groups are split.

15.57. Every smooth connected unipotent algebraic group over a perfect field is split. In characteristic $p \neq 0$, this follows easily (15.52). Hence every smooth connected unipotent algebraic group splits over a finite purely inseparable extension.

15.58. A form of \mathbb{G}_a^r is split if and only if it is the trivial form. Therefore, every split smooth connected commutative algebraic group of exponent p is isomorphic to \mathbb{G}_a^r for some r (15.53). (See also Tits 1968, 3.3.9: let G be a commutative smooth algebraic group of exponent p ; every algebraic subgroup of G isomorphic to \mathbb{G}_a is a direct factor of G .)

15.59. The algebraic group \mathbb{U}_n is split (8.46). More generally, the unipotent radicals of the parabolic subgroups of a reductive algebraic group are split.

15.60. A Weil restriction of a split unipotent algebraic group is split.

DEFINITION 15.61. A unipotent group variety G is *wound* if every morphism from the affine line to G is constant (i.e., has image a point).

15.62. If k is perfect, then the wound unipotent group varieties are those that are finite.

15.63. A unipotent group variety G is wound if and only if G does not contain a subgroup variety isomorphic to \mathbb{G}_a . For example, a form of \mathbb{G}_a is wound if and only if it is nontrivial. In particular, Rosenlicht's group $Y^p - Y = tX^p$ is wound.

15.64. If G is wound, then it admits a subnormal series formed of wound characteristic subgroups whose quotients are wound commutative and killed by p (proof by induction on the dimension of G).

15.65. Subgroups and extensions of wound group varieties are wound (but not necessarily quotients).

15.66. Every unipotent group variety G is isomorphic to a subgroup variety of a split unipotent group variety H (15.3). If G is commutative, H can be chosen commutative. If G is commutative of exponent p , then it is elementary unipotent (15.47; see also Tits 1968, 3.3.1). In general, it is not possible to choose H so that G is a normal subgroup.

15.67. (Structure theorem). Let G be a connected unipotent group variety G . Then G contains a unique normal connected split subgroup variety G_{split} such that $W = G/G_{\text{split}}$ is wound:

$$e \rightarrow G_{\text{split}} \rightarrow G \rightarrow W \rightarrow e.$$

The subgroup variety G_{split} contains all connected split subgroup varieties of G , and its formation commutes with separable (not necessarily algebraic) extensions (Tits 1968, 4.2; Conrad et al. 2010 B.3.4).

NOTES. 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 “*totalemtent ployé*” (totally folded or bent) for “wound”.

NOTES. To paraphrase Oesterlé (1984), the paternity of these results is not always easy to attribute. Most of the questions treated in this section were considered for the first time by Rosenlicht (1963), reconsidered and developed in detail by Tits (1968), and extended to schemes in DG.

NOTES. Some references for unipotent groups: Tits 1968; Schoeller 1972; Kambayashi et al. 1974; Takeuchi 1975; Oesterlé 1984, Chapter V; Conrad et al. 2010, Appendix B.

Exercises

EXERCISE 15-1. Show that every group variety G contains a greatest unipotent normal algebraic subgroup.

EXERCISE 15-2. Use Theorem 15.46 to prove Russell’s theorem, 15.54.

EXERCISE 15-3. (SHS, Exposé 12, 1.4; DG IV, §2, 1.1, p.483). Let H be an algebraic subgroup of \mathbb{G}_a (k algebraically closed). Prove:

- H has a subnormal series whose terms are characteristic subgroups and whose quotients are \mathbb{G}_a , α_p , or $(\mathbb{Z}/p\mathbb{Z})_k^m$.
- Either $\mathbb{G}_a/H \simeq \mathbb{G}_a$ or $\mathbb{G}_a/H = e$.

Cohomology and extensions

As usual, we fix a field k , and all algebraic schemes and morphisms are over k unless indicated otherwise. By a functor (resp. group functor) we mean a functor $\text{Alg}_k^0 \rightarrow \text{Set}$ (resp. $\text{Alg}_k^0 \rightarrow \text{Grp}$).

a. Crossed homomorphisms

Let $G \times M \rightarrow M$ be an action of a group functor G on a group functor M by group homomorphisms. Such an action corresponds to a homomorphism $G \rightarrow \underline{\text{Aut}}(M)$. A map of functors $f: G \rightarrow M$ is a **crossed homomorphism** if

$$f(gg') = f(g) \cdot gf(g')$$

for all small k -algebras R and $g, g' \in G(R)$. When G is smooth algebraic group it suffices to check the condition for $g, g' \in G(k^{\text{sep}})$ (1.9d, 1.12). For $m \in M(k)$, the map

$$g \mapsto m^{-1} \cdot gm: G \rightarrow M$$

is a crossed homomorphism. The crossed homomorphisms of this form are said to be **principal**.

EXAMPLE 16.1. Let $G \times M \rightarrow M$ be an action of a group functor G on a group functor M , and let $\theta: G \rightarrow \underline{\text{Aut}}(M)$ be the corresponding homomorphism. As in Chapter 5, we can define a semidirect product $M \rtimes_{\theta} G$. Specifically $(M \rtimes_{\theta} G)(R) = M(R) \times G(R)$ for all small k -algebras R , and if $m, m' \in M(R)$ and $g, g' \in G(R)$, then

$$(m, g) \cdot (m', g') = (m \cdot \theta(g)m', gg').$$

There is an exact sequence

$$e \rightarrow M \rightarrow M \rtimes_{\theta} G \rightarrow G \rightarrow e.$$

The group sections to the homomorphism $M \rtimes_{\theta} G \rightarrow G$ 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 16.2. Let U be a unipotent algebraic group, and let e be an integer not divisible by the characteristic of k . Then the map $x \mapsto x^e: U(k^{\text{al}}) \rightarrow U(k^{\text{al}})$ 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 $N(k^{\text{al}})$ is injective, and so it is bijective. As every unipotent group admits a filtration whose quotients are subgroups of \mathbb{G}_a (15.23), and the functor $U \rightsquigarrow U(k^{\text{al}})$ is exact (5.33), the general case follows. \square

PROPOSITION 16.3. *Let G be a diagonalizable group variety over an algebraically closed field k , and let M be a commutative unipotent group variety over k on which G acts. Then every crossed homomorphism $f: G \rightarrow M$ is a 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 . Moreover, $\bigcup G_n(k)$ is dense in $|G|$ (see 14.33).

Let $f: G \rightarrow M$ 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

$$M(n) \stackrel{\text{def}}{=} \{m \in M(k) \mid f(x) = x \cdot m - m \text{ for all } x \in G_n(k)\}$$

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 that f agrees with the principal crossed homomorphism $x \mapsto x \cdot m - m$ on G . \square

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 all k -algebras R . Much of the basic formalism of group cohomology (e.g., Chapter II of my Class Field Theory notes) carries over to this setting. We first define the standard complex.

Let M be a G -module. Define

$$C^n(G, M) = \text{Map}(G^n, M)$$

(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

$$\partial^n: C^n(G, M) \rightarrow C^{n+1}(G, M)$$

is defined by the usual formula: let $g_1, \dots, g_{n+1} \in G(R)$; then

$$(\partial^n f)(g_1, \dots, g_{n+1}) = g_1 f(g_2, \dots, g_{n+1}) + \sum_{j=1}^n (-1)^j f(g_1, \dots, g_j g_{j+1}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n).$$

Define

$$\begin{aligned} Z^n(G, M) &= \text{Ker}(\partial^n) && \text{(group of } n\text{-cocycles)} \\ B^n(G, M) &= \text{Im}(\partial^{n-1}) && \text{(group of } n\text{-coboundaries)} \\ H_0^n(G, M) &= Z^n(G, M)/B^n(G, M). \end{aligned}$$

For example,

$$\begin{aligned} H_0^0(G, M) &= M(k)^G \\ H_0^1(G, M) &= \frac{\text{crossed homomorphisms } G \rightarrow M}{\text{principal crossed homomorphisms}} \end{aligned}$$

If G acts trivially on M , then

$$\begin{aligned} H_0^0(G, M) &= M(k) \\ H_0^1(G, M) &= \text{Hom}(G, M) \quad (\text{homomorphisms of group functors}). \end{aligned}$$

The group $H_0^r(G, M)$ is called the *r*th **Hochschild cohomology group** of G in M .

Let

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

be an exact sequence of G -modules. By this we mean that

$$0 \rightarrow M'(R) \rightarrow M(R) \rightarrow M''(R) \rightarrow 0 \tag{111}$$

is exact for all small k -algebras R . Then

$$0 \rightarrow C^\bullet(G, M') \rightarrow C^\bullet(G, M) \rightarrow C^\bullet(G, M'') \rightarrow 0 \tag{112}$$

is an exact sequence of complexes. For example, if G is an algebraic group, then (112) is obtained from (111) by replacing R with $\mathcal{O}(G)$. By a standard argument (112), gives rise to a long exact sequence of cohomology groups

$$0 \rightarrow H_0^0(G, M') \rightarrow H_0^0(G, M) \rightarrow \dots \rightarrow H_0^n(G, M'') \rightarrow H_0^{n+1}(G, M') \rightarrow H_0^{n+1}(G, M) \rightarrow \dots$$

Let M be a commutative group functor, and let $\underline{\text{Hom}}(G, M)$ denote the functor $R \mapsto \text{Hom}(G_R, M_R)$. Then $\underline{\text{Hom}}(G, M)$ becomes a G -module by the usual rule, $(gf)(g') = g(f(g^{-1}g'))$.

PROPOSITION 16.4 (SHAPIRO'S LEMMA). *Let M be a commutative group functor. For all $n > 0$,*

$$H_0^n(G, \underline{\text{Hom}}(G, M)) = 0.$$

PROOF. Note that

$$C^n(G, \underline{\text{Hom}}(G, M)) \simeq \text{Hom}(G \times G^n, M) = C^{n+1}(G, M).$$

Define

$$s^n: \text{Hom}(G^{n+2}, M) \rightarrow \text{Hom}(G^{n+1}, M)$$

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 $C^{n+1}(G, \underline{\text{Hom}}(G, M)) \rightarrow C^n(G, \underline{\text{Hom}}(G, M))$, we find (by direct calculation), that

$$s^n \partial^n + \partial^{n-1} s^{n-1} = \text{id}$$

for $n > 0$. Therefore $(s^n)_n$ is a homotopy operator, and the cohomology groups vanish. \square

REMARK 16.5. 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 $H_0^i(G, M)$.

Now let G be an algebraic group over k with coordinate ring A , and let M 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 $k \rightarrow R_0$ is flat, it follows that

$$H^n(G_{R_0}, M_{R_0}) \simeq R_0 \otimes H^n(G, M).$$

EXAMPLES.

PROPOSITION 16.6. *Let Γ_k be the constant algebraic group defined by a finite abstract group Γ . For all Γ_k -modules M ,*

$$H_0^n(\Gamma_k, M) \simeq H^n(\Gamma, M(k)) \quad (\text{usual group cohomology}).$$

PROOF. The standard complexes $C^\bullet(\Gamma_k, M)$ and $C^\bullet(\Gamma, M(k))$ are equal. \square

PROPOSITION 16.7. *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 (14.29). 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

$$\partial^n = \begin{cases} \text{id} & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

from which the statement follows. \square

PROPOSITION 16.8. *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 (14.29). The Hochschild complex $C^\bullet(\mathbb{G}_m^r, \mathbb{G}_m)$ has

$$C^n(\mathbb{G}_m^r, \mathbb{G}_m) = k[T_{11}, T_{11}, \dots, T_{1n}, T_{1,n}^{-1}, \dots, T_{rn}, T_{rn}^{-1}]^\times \simeq k^\times \times \mathbb{Z}^{nr}$$

and boundary maps that can be made explicit. A direct calculation gives the statement (DG III, §6, p.453). \square

PROPOSITION 16.9. *Let $\mu: G \times H \rightarrow H$ 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 $F_H^n: H \rightarrow H^{(p^n)}$. Then the induced action of G on H/H_n is trivial, and the canonical map*

$$H_0^i(G, H_n) \rightarrow H_0^i(G, H)$$

is bijective for all $i \geq 2$.

PROOF. From the functoriality of the Frobenius map, we get a commutative diagram

$$\begin{array}{ccc} G \times H & \xrightarrow{\mu} & H \\ F_G^n \times F_H^n \downarrow & & \downarrow F_H^n \\ G^{(p^n)} \times H^{(p^n)} & \xrightarrow{\mu^{(p^n)}} & H^{(p^n)} \end{array}$$

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 $\text{Map}(G^i, H(n)) \simeq \text{Map}(G^i, H)$ (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

$$0 \rightarrow H_n \rightarrow H(n) \rightarrow H(k)_k \rightarrow 0. \tag{113}$$

Here $H(k)_k$ is the constant group scheme associated with the group $H(k)$ and the trivial G -action. As $\text{Map}(G^i, H(k)_k) = H(k)$ 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 (113). \square

For example,

$$H_0^i(\alpha_p, \mu_p) \simeq H_0^i(\alpha_p, \mathbb{G}_m)$$

for all $i \geq 2$.

NOTES. For more details, see DG II, §3, n°1, pp.185–188.

c. Hochschild extensions

Let G be a group functor. Let M be a commutative group functor, and let

$$0 \rightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \tag{114}$$

be an exact sequence of group functors, i.e.,

$$0 \rightarrow M(R) \xrightarrow{i(R)} E(R) \xrightarrow{\pi(R)} G(R)$$

is exact for all (small) k -algebras R . A sequence (114) is a **Hochschild extension** if there exists a map of set-valued functors $s: G \rightarrow E$ such that $\pi \circ s = \text{id}_G$. For a Hochschild extension, the sequence

$$0 \rightarrow M(R) \xrightarrow{i(R)} E(R) \xrightarrow{\pi(R)} G(R) \rightarrow 0$$

is exact for all k -algebras R . Conversely, if $\pi(R)$ is surjective with $R = \mathcal{O}(G)$, then (114) is a Hochschild extension. A Hochschild extension (E, i, π) is **trivial** if there exists a homomorphism of group functors $s: G \rightarrow E$ such that $\pi \circ s = \text{id}_G$. This means that E is a semidirect product $M \rtimes_{\theta} G$ for the action θ of G on M defined by the extension. Two Hochschild extensions (E, i, π) and (E', i', π') of G by M are **equivalent** if there exists a homomorphism $f: E \rightarrow E'$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 0 \\ & & \parallel & & \downarrow f & & \parallel & & \\ 0 & \longrightarrow & M & \xrightarrow{i'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 0 \end{array}$$

commute.

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 .

PROPOSITION 16.10. *Let M be a G -module. There is a canonical bijection*

$$E(G, M) \simeq H_0^2(G, M). \tag{115}$$

PROOF. Let (E, i, π) be a Hochschild extension of G by M , and let $s: G \rightarrow E$ be a section to π . Define $f: G^2 \rightarrow M$ 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. \square

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 16.11. *Let M be a commutative group functor. Assume that G is commutative. There is a canonical one-to-one correspondence between the equivalence classes of Hochschild extensions (E, i, π) with E commutative and the elements of $H_s^2(G, M)$.*

PROOF. Follows without difficulty from (16.10). \square

HIGHER HOCHSCHILD EXTENSIONS

We wish to define a sequence of functors $E^0(G, -), E^1(G, -), \dots$ 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 its augmentation ideal $J = \text{Ker}(\mathbb{Z}[G] \xrightarrow{g \mapsto g^{-1}} \mathbb{Z})$; thus $\mathbb{Z}[G] \simeq \mathbb{Z} \oplus J$. The map

$$\delta: G \rightarrow J, \quad \delta(g) = g - 1$$

is a crossed homomorphism, and it is universal, i.e.,

$$\varphi \leftrightarrow \varphi \circ \delta: \text{Hom}_{G\text{-module}}(J, M) \simeq Z^1(G, M) \quad (\text{crossed homomorphisms})$$

for all G -modules M .

From an exact sequence of G -modules,

$$\mathcal{E}: 0 \rightarrow M \xrightarrow{i} E \xrightarrow{\pi} J \rightarrow 0,$$

we can construct a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E(\mathcal{E}) & \longrightarrow & G & \longrightarrow & e \\ & & \parallel & & \downarrow & & \downarrow_{g \mapsto (g-1, g)} & & \\ 0 & \longrightarrow & M & \xrightarrow{m \mapsto (i(m), 0)} & M \rtimes G & \xrightarrow{\pi \times \text{id}} & J \rtimes G & \longrightarrow & 0 \end{array}$$

with $E(\mathcal{E})$ is the fibred product. Let $F(\mathcal{E})$ denote the top row. Then the map $\mathcal{E} \mapsto F(\mathcal{E})$ defines a bijection from $\text{Ext}_{G\text{-module}}^1(J, M)$ onto the set of equivalence classes of extensions of G by M . This allows us to define

$$E^i(G, M) = \text{Ext}_{G\text{-module}}^i(G, M).$$

In particular, $E^0(G, M) = Z^1(G, M)$.

Similar arguments work for a group functor G . Thus, we obtain a sequence of functors $E^0(G, -), E^1(G, -), E^2(G, -), \dots$ of G -modules such that

$$\begin{cases} E^0(G, M) \simeq Z^1(G, M) & \text{set of crossed homomorphisms} \\ E^1(G, M) \simeq E(G, M) & \text{set of Hochschild extensions.} \end{cases} \quad (116)$$

NOTES. For more details, see DG II, §3, n°2, p.189; ibid. III, §6, n°1, p.431.

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 $V_a: R \rightsquigarrow V \otimes R$, and we set

$$H^i(G, V) \stackrel{\text{def}}{=} H_0^i(G, V_a).$$

Let $A = \mathcal{O}(G)$, and let $\rho: V \rightarrow V \otimes A$ be the corresponding co-action. Then

$$C^n(G, V_a) \stackrel{\text{def}}{=} \text{Hom}(G^n, V) \simeq V(A^{\otimes n}) = V \otimes A^{\otimes n}.$$

Thus, $C^\bullet(G, V_a)$ is a complex

$$0 \rightarrow V \rightarrow V \otimes A \rightarrow \dots \rightarrow V \otimes A^{\otimes n} \xrightarrow{\partial^n} V \otimes A^{\otimes n+1} \rightarrow \dots$$

The map ∂^n has the following description (DG II, §3, 3.1, p.191): let $v \in V$ and $a_1, \dots, a_n \in A$; then

$$\begin{aligned} \partial^n(v \otimes a_1 \otimes \cdots \otimes a_n) &= \rho(v) \otimes a_1 \otimes \cdots \otimes a_n + \sum_{j=1}^n (-1)^j v \otimes a_1 \otimes \cdots \otimes \Delta a_j \otimes \cdots \otimes a_n \\ &\quad + (-1)^{n+1} v \otimes a_1 \otimes \cdots \otimes a_n \otimes 1. \end{aligned}$$

If

$$0 \rightarrow V' \rightarrow V \rightarrow V'' \rightarrow 0$$

is an exact sequence of representations, then

$$0 \rightarrow V' \otimes R \rightarrow V \otimes R \rightarrow V'' \otimes R \rightarrow 0$$

is exact for all k -algebras R , and so there is a long exact sequence of cohomology groups

$$0 \rightarrow H^0(G, V') \rightarrow H^0(G, V) \rightarrow \cdots \rightarrow H^n(G, V'') \rightarrow H^{n+1}(G, V') \rightarrow H^{n+1}(G, V) \rightarrow \cdots.$$

PROPOSITION 16.12. *Let V be a k -vector space, and let $V \otimes A$ be the free comodule on V (Section 4.e). Then*

$$H^n(G, V \otimes A) = 0 \text{ for } n > 0.$$

PROOF. For a (small) k -algebra R ,

$$\begin{aligned} (V \otimes A)_a(R) &= V \otimes A \otimes R && \text{(definition)} \\ &\simeq (V \otimes R) \otimes_R (A \otimes R) && \text{(linear algebra)} \\ &= (V_a)_R(A_R) && \text{(change of notation)} \\ &\simeq \text{Nat}(h^{A_R}, (V_a)_R) && \text{(Yoneda lemma A.27)} \\ &= \text{Hom}(G_R, (V_a)_R). && \text{(change of notation).} \end{aligned}$$

As these isomorphisms are natural in R , they form an isomorphism of functors

$$(V \otimes A)_a \simeq \underline{\text{Hom}}(G, V_a).$$

Therefore the statement follows from Shapiro's lemma (16.4). \square

REMARK 16.13. 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 $V \rightarrow W$ such that $H^n(G, W) = 0$ for $n > 0$, but the homomorphism $V \rightarrow V_0 \otimes A$ in (4.9) has this property because of (16.12).

As the category of representations of G is isomorphic to the category of A -comodules, and $H^0(G, V) = \text{Hom}_A(k, V)$ (homomorphisms of A -comodules), we see that

$$H^n(G, V) \simeq \text{Ext}_A^n(k, V), \quad \text{all } n,$$

(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 . According to (4.7), (V, r) is a directed union of its finite-dimensional subrepresentations,

$$(V, r) = \bigcup_{\dim(W) < \infty} (W, r|_W).$$

Correspondingly,

$$H^i(G, V) = \varinjlim H^i(G, W) \tag{117}$$

(because direct limits are exact in the category of abelian groups).

LEMMA 16.14. *Let $x \in H^i(G, V)$. Then x maps to zero in $H^i(G, W)$ for some finite-dimensional representation W containing V .*

PROOF. Recall (4.9) that the co-action $\rho: V \rightarrow V_0 \otimes A$ is an injective homomorphism of A -comodules. According to (16.12), the element x maps to zero in $H^i(G, V_0 \otimes A)$, and it follows from (117) that x maps to zero in $H^i(G, W)$ for some finite-dimensional G -submodule W of $V_0 \otimes A$ containing $\rho(V)$. \square

PROPOSITION 16.15. *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. \implies : Let $x \in H^1(G, V)$. According to (16.14), x maps to zero in $H^1(G, W)$ for some finite-dimensional representation W of G containing V . Hence x lifts to an element of $(W/V)^G$ in the cohomology sequence

$$0 \rightarrow V^G \rightarrow W^G \rightarrow (W/V)^G \rightarrow H^1(G, V) \rightarrow H^1(G, W).$$

But, because G is linearly reductive, the sequence $0 \rightarrow V \rightarrow W \rightarrow W/V \rightarrow 0$ splits as a sequence of G -modules, and so $W^G \rightarrow (W/V)^G$ is surjective. Therefore $x = 0$.

\impliedby : When (V, r) and (W, s) are finite-dimensional representations of G , we let $\text{Hom}(V, W)$ denote the space of k -linear maps $V \rightarrow W$ equipped with the G -action given by the rule

$$(gf)(v) = g(f(g^{-1}v)).$$

We have to show that every exact sequence

$$0 \rightarrow V' \rightarrow V \rightarrow V'' \rightarrow 0 \tag{118}$$

of finite-dimensional representations of G splits. From (118), we get an exact sequence of G -modules

$$0 \rightarrow \text{Hom}(V'', V') \rightarrow \text{Hom}(V'', V) \rightarrow \text{Hom}(V'', V'') \rightarrow 0,$$

and hence an exact cohomology sequence of vector spaces

$$0 \rightarrow \text{Hom}(V'', V')^G \rightarrow \text{Hom}(V'', V)^G \rightarrow \text{Hom}(V'', V'')^G \rightarrow H^1(G, \text{Hom}(V'', V')).$$

By assumption, the last group is zero, and so $\text{id}_{V''}$ lifts to an element of $\text{Hom}(V'', V)^G$. This element splits the original sequence (118). \square

PROPOSITION 16.16. *If G is linearly reductive, then $H^n(G, V) = 0$ for all $n > 0$ and all representations V of G .*

PROOF. Because of (117), 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 $1 \leq i < n$ 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 (16.14), and so x lifts to an element of $H^{n-1}(G, V/W)$ in the cohomology sequence

$$H^{n-1}(G, V/W) \rightarrow H^n(G, V) \rightarrow H^n(G, W).$$

But $H^{n-1}(G, V/W) = 0$ (induction), and so $x = 0$. \square

REMARK 16.17. In particular, $H^n(G, V) = 0$ ($n > 0$) for groups G of multiplicative type (14.22). It is possible to deduce this directly from (16.12) by showing that the homomorphism of G -modules $\rho: V \rightarrow V_0 \otimes A$ (see 4.9) has a section. See DG II, §3, 4.2, p.195.

f. Applications to homomorphisms

We can now prove a stronger form of (15.18).

PROPOSITION 16.18. *Let T and U be algebraic groups over k with T of multiplicative type and U unipotent, and let R be a k -algebra. Every homomorphism $T_R \rightarrow U_R$ is trivial.*

PROOF. Let α be such a homomorphism, and let H be minimal among the algebraic subgroups of U such that $\alpha(T_R) \subset H_R$. If $H \neq e$, then there exists a nontrivial homomorphism $\beta: H \rightarrow \mathbb{G}_a$ (15.24), and the composite $\beta_R \circ \alpha: T_R \rightarrow (\mathbb{G}_a)_R$ is nontrivial because otherwise $\alpha(T_R)$ would be contained in the kernel of β and H wouldn't be minimal. But when we endow $\mathbb{G}_a R$ with the trivial action of T_R , we find that

$$\mathrm{Hom}_R(T_R, \mathbb{G}_a R) = H_0^1(T_R, \mathbb{G}_a R) \stackrel{(16.5)}{\simeq} R \otimes H_0^1(T, \mathbb{G}_a) \stackrel{(16.16)}{=} 0,$$

giving a contradiction. Therefore $H = e$ and α is trivial. \square

REMARK 16.19. There may exist nontrivial homomorphisms $U_R \rightarrow T_R$. For example,

$$\underline{\mathrm{Hom}}((\mathbb{Z}/p\mathbb{Z})_k, \mathbb{G}_m) \simeq \mu_p$$

(13.31), and so $\mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})_R, \mathbb{G}_m R) \neq 0$ if R contains an element $\neq 1$ whose p th power is 1. Similarly,

$$\underline{\mathrm{Hom}}(\alpha_p, \mathbb{G}_m) \simeq \alpha_p$$

(13.32), and so $\mathrm{Hom}(\alpha_p R, \mathbb{G}_m R) \neq 0$ if R contains an element $\neq 0$ whose p th power is 0.

g. Applications to centralizers

We present two more proofs that the centralizer of a multiplicative subgroup is smooth (14.62, 14.79). This section will be deleted from the final version.

TRADITIONAL APPROACH (SHS)

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 16.20 (SMOOTHNESS OF CENTRALIZERS). *Let G be a smooth algebraic group, and let H be an algebraic group acting on G . If $H^1(H, \mathfrak{g}) = 0$, then G^H is smooth.*

PROOF. In order to show that G^H is smooth, it suffices to show that, for all k -algebras S and ideals I in S such that $I^2 = 0$, the map

$$G^H(S) \rightarrow G^H(S/I)$$

is surjective (see 1.22). Define group functors

$$\mathcal{G}: R \rightsquigarrow G(S \otimes R)$$

$$\bar{\mathcal{G}}: R \rightsquigarrow \text{image of } G(S \otimes R) \text{ in } G((S/I) \otimes R)$$

After (12.28), there is an exact sequence of group functors

$$0 \rightarrow (I \otimes \mathfrak{g})_{\mathfrak{a}} \rightarrow \mathcal{G} \rightarrow \bar{\mathcal{G}} \rightarrow 0.$$

Now H acts on this sequence, and so we get an exact cohomology sequence:

$$0 \rightarrow H^0(H, I \otimes \mathfrak{g}) \rightarrow H^0(H, \mathcal{G}) \rightarrow H^0(H, \bar{\mathcal{G}}) \rightarrow H^1(H, I \otimes \mathfrak{g}). \quad (119)$$

From (9.3),

$$G^H(S) = \{g \in G(S) \mid h_{S \otimes R} g_{S \otimes R} = g_{S \otimes R} \forall h \in H(R), \text{ all } R\}.$$

It follows that

$$H^0(H, \mathcal{G}) \stackrel{\text{def}}{=} \mathcal{G}^H(k) = G^H(S).$$

Similarly,

$$H^0(H, \bar{\mathcal{G}}) = \{g \in G^H(S/I) \text{ lifting to } G(S)\}.$$

As G is smooth, $G(S) \rightarrow G(S/I)$ is surjective, and so the last equality becomes

$$H^0(H, \bar{\mathcal{G}}) = G^H(S/I).$$

Finally,

$$H^i(H, I \otimes \mathfrak{g}) = I \otimes H^i(H, \mathfrak{g})$$

(as a representation of H , $I \otimes \mathfrak{g}$ is a direct sum of copies of \mathfrak{g}). Therefore, the sequence (119) becomes an exact sequence

$$0 \rightarrow H^0(H, \mathfrak{g}) \otimes I \rightarrow G^H(S) \rightarrow G^H(S/I) \rightarrow H^1(H, \mathfrak{g}) \otimes I,$$

Hence $G^H(S) \rightarrow G^H(S/I)$ is surjective if $H^1(H, \mathfrak{g}) = 0$. \square

COROLLARY 16.21. *Let H be a linearly reductive algebraic group acting on a smooth algebraic group G . Then G^H is smooth.*

PROOF. As H is linearly reductive, $H^1(H, \mathfrak{g}) = 0$ (16.15). \square

COROLLARY 16.22. *Let H be a commutative algebraic subgroup of a smooth algebraic group G . If*

$$H^1(H, \mathfrak{h}) = 0 = H^1(H, \mathfrak{g}),$$

then $C_G(H)$ and $N_G(H)$ are smooth, and $C_G(H)$ is open in $N_G(H)$.

PROOF. Let H act on G by inner automorphisms. Then $G^H = C_G(H)$. If $H^1(H, \mathfrak{g}) = 0$, then $C_G(H)$ is smooth (16.20). If $H^1(H, \mathfrak{h}) = 0$, then $\mathfrak{g}^H \rightarrow (\mathfrak{g}/\mathfrak{h})^H$ is surjective, and so $C_G(H)$ is open in $N_G(H)$ (12.33). Hence $N_G(H)$ is also smooth. \square

COROLLARY 16.23. *Let H be a multiplicative algebraic subgroup of a smooth algebraic group G . Then $C_G(H)$ and $N_G(H)$ are smooth, and $C_G(H)$ is open in $N_G(H)$.*

PROOF. The hypotheses of (16.22) hold (see 14.22, 16.15). \square

ABSTRACT APPROACH

We sketch a more abstract version of the proof of the smoothness of $C_G(H)$.

LEMMA 16.24. *Let G and H be algebraic groups over k . Let R be a k -algebra, let $R_0 = R/I$ with $I^2 = 0$, and let $* \rightsquigarrow *_0$ denote base change $R \rightarrow R_0$. The obstruction to lifting a homomorphism $u_0: H_0 \rightarrow G_0$ to R is a class in $H^2(H_0, \text{Lie}(G_0) \otimes I)$; if the class is zero, then the set of lifts modulo the action of $\text{Ker}(G(R) \rightarrow G(R_0))$ by conjugation is a principal homogeneous space for the group $H^1(H_0, \text{Lie}(G_0) \otimes I)$.*

PROOF. Omitted. \square

LEMMA 16.25. *Let H and G be algebraic groups over a ring R , and let $R_0 = R/I$ with $I^2 = 0$. If H is of multiplicative type, then every homomorphism $u_0: H_{R_0} \rightarrow G_{R_0}$ lifts to a homomorphism $u: H \rightarrow G$; if u' is a second lift, then $u' = \text{inn}(g) \circ u$ for some $g \in \text{Ker}(G(R) \rightarrow G(R_0))$.*

PROOF. The cohomology groups $H^1(H_0, \text{Lie}(G_0) \otimes I)$ and $H^2(H_0, \text{Lie}(G_0) \otimes I)$ vanish (16.17), and so this follows from (16.24). \square

PROPOSITION 16.26. *Let G be an algebraic group over a field k , acting on itself by conjugation, and let H and H' be subgroups of G . If G is smooth and H is of multiplicative type, then the transporter $T_G(H, H')$ is smooth.*

PROOF. We use the following criterion (A.53):

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 $X(R) \rightarrow X(R/I)$ is surjective.

We may replace k with its algebraic closure. Let $g_0 \in T_G(H, H')(R_0)$. Because G is smooth, g_0 lifts to an element $g \in G(R)$. On the other hand, because H is of multiplicative type, the homomorphism

$$\text{inn}(g_0): H_0 \rightarrow H'_0$$

lifts to a homomorphism $u: H \rightarrow H'$ (see 16.25). The homomorphisms

$$\begin{aligned} \text{inn}(g): H &\rightarrow G \\ u: H &\rightarrow H' \hookrightarrow G \end{aligned}$$

both lift $\text{inn}(g_0): H_0 \rightarrow G_0$, and so $u = \text{inn}(g') \circ \text{inn}(g)$ for some $g' \in G(R)$ mapping to e in $G(R_0)$ (see 16.25). Now $g'g$ is an element of $T_G(H, H')(R)$ lifting g_0 . \square

COROLLARY 16.27. *Let H be a multiplicative algebraic subgroup of an algebraic group G . Then $C_G(H)$ and $N_G(H)$ are smooth.*

PROOF. This follows from the proposition because

$$\begin{aligned} N_G(H) &= T_G(H, H) \\ C_G(H) &= T_G(H, H). \end{aligned}$$

See 1.59 and 1.67. □

LEMMA 16.28. *Let G and H be diagonalizable group varieties and let X be a connected algebraic variety (over an algebraically closed field for simplicity); let $\phi: G \times X \rightarrow H$ be a regular map such that $\phi_x: G \rightarrow H$ is a homomorphism for all $x \in X(k)$; then ϕ is constant on X , i.e., ϕ factors through the map $G \times X \rightarrow G$.*

PROOF. Omitted. □

PROPOSITION 16.29. *Let H be a diagonalizable subgroup of a group variety G ; then $N_G(H)^\circ = C_G(H)^\circ$.*

PROOF. Apply (16.28) to

$$\varphi: H \times N_G(H)^\circ \rightarrow H, \quad \varphi(h, g) = ghg^{-1};$$

as this is constant on $N_G(H)^\circ$, we have $\varphi(h, g) = \varphi(h, e) = h$, and so $N_G(H)^\circ \subset C_G(H)^\circ$. □

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

$$0 \rightarrow M \xrightarrow{i} E \xrightarrow{\pi} G \rightarrow 0 \tag{120}$$

that is exact as a sequence of sheaves of groups. This means that the sequence

$$0 \rightarrow M(R) \rightarrow E(R) \rightarrow G(R)$$

is exact for all small k -algebras, and π is a quotient map of sheaves, i.e., $\pi(E)$ is a fat subfunctor of G . 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 16.30. For a G -module sheaf M , $\text{Ext}(G, M)$ 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, $\text{Ext}(G, M)$ is equal the set of equivalence classes of extensions (120) with E an algebraic group (Exercise 6-6).

Let M be a G -module sheaf, and let (E, i, π) 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

$$E(G, M) \rightarrow \text{Ext}(G, M)$$

whose image consists of the classes of extensions (120) such that π has a section (as a map of functors). One strategy for computing $\text{Ext}(G, M)$ is to show that every extension is a Hochschild extension, and then use the description of $E(G, M)$ in terms of Hochschild cohomology in (16.10). Let

$$0 \rightarrow N \rightarrow E \rightarrow G \rightarrow 0 \quad (121)$$

be an extension of algebraic groups. Then E is an N -torsor over G , and (121) is a Hochschild extension if this torsor is trivial.

More generally, we define $\text{Ext}^i(G, -)$ to be the i th right derived functor of

$$M \rightsquigarrow Z^1(G, M) \quad (\text{functor of } G\text{-module sheaves})$$

(cf. the definition of E^i in Section 16.c). For $i = 1$, this agrees with the previous definition (ibid. 1.4, p.434). Thus

$$\left\{ \begin{array}{l} \text{Ext}^0(G, M) = Z^1(G, M) \quad \text{set of crossed homomorphisms} \\ \text{Ext}^1(G, M) \simeq \text{Ext}(G, M) \quad \text{set of sheaf extensions.} \end{array} \right. \quad (122)$$

NOTES. DG III, §6, 2, p.438, write Ex^i and Ex^i where we write E^i and Ext^i .

EXTENSIONS WITH ÉTALE QUOTIENT

PROPOSITION 16.31. *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. Then*

$$\text{Ext}^i(\Gamma_k, M) \simeq H^{i+1}(\Gamma, M(k)) \text{ all } i \geq 1.$$

Here $H^{i+1}(\Gamma, M(k))$ denotes the usual group cohomology of Γ acting on $M(k)$.

PROOF. Because k is algebraically closed, the functor $M \rightsquigarrow M(k)$ is exact. Hence the functor $M \rightsquigarrow C^\bullet(\Gamma, M(k))$ is exact, and so an exact sequence

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

of sheaves of commutative groups gives rise to an exact sequence

$$0 \rightarrow Z^1(\Gamma, M'(k)) \rightarrow Z^1(\Gamma, M(k)) \rightarrow Z^1(\Gamma, M''(k)) \rightarrow H^2(\Gamma, M'(k)) \rightarrow H^2(\Gamma, M(k)) \rightarrow \dots$$

of commutative groups. By definition

$$\text{Ext}^0(\Gamma_k, M) = Z^1(\Gamma_k, M) \simeq Z^1(\Gamma, M(k)),$$

and so 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 $N \rightsquigarrow N_k$,

$$\text{Hom}(N, M(k)) \simeq \text{Hom}(N_k, M).$$

If M is injective, then $N \rightsquigarrow \text{Hom}(N_k, M) \simeq \text{Hom}(N, M(k))$ is exact, and so $M(k)$ is injective. \square

COROLLARY 16.32. *Let k , Γ , and M be as in (16.31). If Γ is of finite order n , and $x \mapsto nx: M(k) \rightarrow M(k)$ is an isomorphism, then*

$$\mathrm{Ext}^i(\Gamma_k, M) = 0 \text{ for all } i \geq 0.$$

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 $i > 0$ (see, for example, my Class Field Theory notes, II, 1.31). If $x \mapsto nx: N \rightarrow N$ is bijective, then n acts bijectively on $H^i(\Gamma, N)$. If both are true, $H^i(\Gamma, N) = 0$, $i > 0$, and so the statement follows from (16.31). \square

COROLLARY 16.33. *Let D be a diagonalizable algebraic group. If k is algebraically closed, then $\mathrm{Ext}^i(\mathbb{Z}/p\mathbb{Z}, D) = 0$ for all $i > 0$.*

PROOF. This follows from (16.32) because $p: D(k) \rightarrow D(k)$ is an isomorphism (recall that every diagonalizable algebraic group is a product of the following groups: \mathbb{G}_m ; μ_n with $\mathrm{gcd}(p, n) = 1$; μ_{p^r} ; 14.3). \square

EXTENSIONS WITH ADDITIVE QUOTIENT

PROPOSITION 16.34. *Let D be a diagonalizable group. Every action of \mathbb{G}_a on D is trivial, and*

$$\mathrm{Ext}^0(\mathbb{G}_a, D) = 0 = \mathrm{Ext}^1(\mathbb{G}_a, D).$$

PROOF. The first assertion follows from (14.29). For the second assertion, we first consider the case $D = D(\mathbb{Z}) = \mathbb{G}_m$. Because the action is trivial, $\mathrm{Ext}^0(\mathbb{G}_a, \mathbb{G}_m) = \mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_m)$, which is 0 (15.17). Consider an extension

$$0 \rightarrow \mathbb{G}_m \rightarrow E \rightarrow \mathbb{G}_a \rightarrow 0.$$

Then E is a \mathbb{G}_m -torsor over \mathbb{A}^1 (5.61), and hence corresponds to an element of $\mathrm{Pic}(\mathbb{A}^1)$, which is zero. Therefore this is a Hochschild extension, and we can apply (16.10):

$$E(\mathbb{G}_a, \mathbb{G}_m) \simeq H_0^2(\mathbb{G}_a, \mathbb{G}_m).$$

But the second group is zero (16.7).

Now let $D = D(M)$. There exists an exact sequence

$$0 \rightarrow \mathbb{Z}^s \rightarrow \mathbb{Z}^r \rightarrow M \rightarrow 0$$

for some $r, s \in \mathbb{N}$, which gives an exact sequence of algebraic groups

$$0 \rightarrow D(M) \rightarrow \mathbb{G}_m^r \rightarrow \mathbb{G}_m^s \rightarrow 0$$

(14.9b). This is exact as a sequence of sheaves of commutative groups, and so there is a long exact sequence

$$0 \rightarrow \mathrm{Ext}^0(\mathbb{G}_a, D(M)) \rightarrow \mathrm{Ext}^0(\mathbb{G}_a, \mathbb{G}_m)^r \rightarrow \mathrm{Ext}^0(\mathbb{G}_a, \mathbb{G}_m)^s \rightarrow \mathrm{Ext}^1(\mathbb{G}_a, D(M)) \rightarrow \dots$$

Thus the statement follows from the case $D = \mathbb{G}_m$. \square

EXTENSIONS WITH MULTIPLICATIVE QUOTIENT

PROPOSITION 16.35. *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*

$$\mathrm{Ext}^i(M, \mathbb{Z}^r) \simeq \mathrm{Ext}^i(\mathbb{G}_m^r, D(M))$$

for $i = 0, 1$.

PROOF. The first assertion follows from (14.29). It follows from (14.9) that the functor D gives isomorphisms

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}\text{-modules}}(M, \mathbb{Z}^r) &\simeq \mathrm{Hom}(\mathbb{G}_m^r, D(M)) \\ \mathrm{Ext}_{\mathbb{Z}\text{-modules}}^1(M, \mathbb{Z}^r) &\simeq \mathrm{Ex}^1(\mathbb{G}_m^r, D(M)). \end{aligned}$$

where $\mathrm{Ex}^1(\mathbb{G}_m^r, D(M))$ 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,

$$\mathrm{Ext}^0(\mathbb{G}_m^r, D(M)) = \mathrm{Hom}(\mathbb{G}_m^r, D(M)).$$

It remains to show that the map

$$\mathrm{Ext}_{\mathbb{Z}\text{-modules}}^1(M, \mathbb{Z}^r) \simeq \mathrm{Ex}^1(\mathbb{G}_m^r, D(M)) \rightarrow \mathrm{Ext}^1(\mathbb{G}_m^r, D(M))$$

is surjective. By a five-lemma argument, it suffices to prove this with $M = \mathbb{Z}$ (so $D(M) = \mathbb{G}_m$).

Consider an extension

$$0 \rightarrow \mathbb{G}_m \rightarrow E \rightarrow \mathbb{G}_m^r \rightarrow 0.$$

Then E is a \mathbb{G}_m -torsor over \mathbb{G}_m^r , and hence corresponds to an element of $\mathrm{Pic}(\mathbb{G}_m^r)$, which is zero. Therefore, the extension is a Hochschild extension, and so

$$\mathrm{Ext}^1(\mathbb{G}_m^r, \mathbb{G}_m) = E(\mathbb{G}_m^r, \mathbb{G}_m) \stackrel{(16.10)}{=} H_0^2(\mathbb{G}_m^r, \mathbb{G}_m) \stackrel{(16.8)}{=} 0,$$

as required. \square

Recall (12.10) 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 16.36. *Let G 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 $\mathbb{G}_a = V_a$. Then $H_0^i(G, \mathbb{G}_a) \stackrel{\mathrm{def}}{=} H^i(G, V) = 0$ for $i > 0$ (16.16). Consider the exact sequence

$$e \rightarrow N \rightarrow \mathbb{G}_a \rightarrow \mathbb{G}_a/N \rightarrow e. \quad (123)$$

Either $\mathbb{G}_a/N = 0$ or it is isomorphic to \mathbb{G}_a (Exercise 15-3). In the first case, $N \simeq \mathbb{G}_a$ and so $H_0^i(G, N) = 0$ for $i > 0$. In the second case, (123) becomes an exact sequence

$$e \rightarrow N \rightarrow \mathbb{G}_a \rightarrow \mathbb{G}_a \rightarrow e,$$

whose exact cohomology sequence gives the result. \square

COROLLARY 16.37. *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

$$0 \rightarrow \alpha_p \rightarrow \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \rightarrow 0$$

as an exact sequence of G -modules. Its cohomology sequence gives the result. \square

PROPOSITION 16.38. *Let G be an algebraic group of multiplicative type, and let (V, r) be a finite-dimensional representation of G . Then $\text{Ext}^0(G, V_a) \simeq V/V^G$ and $\text{Ext}^i(G, V_a) = 0$ all $i > 0$.*

PROOF. By assumption, $U = V_a$ as a G -module for some representation (V, r) of G . Now

$$H_0^i(G, U) \stackrel{\text{def}}{=} H^i(G, V) = 0$$

for $i > 0$ (16.17). \square

PROPOSITION 16.39. *Let G be an algebraic group of multiplicative type, acting trivially on a commutative unipotent group U . Then $\text{Ext}^i(G, U) = 0$ for all $i \geq 0$.*

PROOF. For $U = \mathbb{G}_a$, this follows from (16.38). Every algebraic subgroup of \mathbb{G}_a is the kernel of an epimorphism $\mathbb{G}_a \rightarrow \mathbb{G}_a$ (Exercise 15-3), and so the statement is true for such groups. Now use that U has a filtration whose quotients are of these types (15.23). \square

COROLLARY 16.40. *Let G be of multiplicative type, and let $\varphi: G \rightarrow \underline{\text{Aut}}(\alpha_p) \simeq \mathbb{G}_m$ be a nontrivial homomorphism. Then $\text{Ext}^i(G, \alpha_p) = 0$ for $i \geq 2$. If φ factors through $\mu_p \subset \mathbb{G}_m$, then*

$$\left\{ \begin{array}{l} \text{Ext}^0(G, \alpha_p) \simeq k \\ \text{Ext}^1(G, \alpha_p) = 0 \end{array} \right\} ; \quad \text{otherwise} \quad \left\{ \begin{array}{l} \text{Ext}^0(G, \alpha_p) = 0 \\ \text{Ext}^1(G, \alpha_p) \simeq k/k^p. \end{array} \right.$$

PROOF. As $\underline{\text{Aut}}(\alpha_p) \simeq \mathbb{G}_m$, every action of D on α_p extends to a linear action of D on \mathbb{G}_a . We have an exact sequence

$$0 \rightarrow \alpha_p \rightarrow \mathbb{G}'_a \xrightarrow{F} \mathbb{G}''_a \rightarrow 0$$

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,

$$\text{Ext}^i(G, \mathbb{G}'_a) = 0 = \text{Ext}^i(G, \mathbb{G}''_a), \quad i \geq 1,$$

and

$$\text{Hom}(D, \mathbb{G}_a) \rightarrow \text{Ext}^1(D, \alpha_p) \rightarrow \text{Ext}^1(D, \mathbb{G}_a)$$

and (16.38) prove the statement show that $\text{Ext}^1(D, \alpha_p) = 0$. \square

THEOREM 16.41. *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 $\text{Ext}^1(G, U) = 0$ in each of the following cases:*

- (a) $U = \mathbb{G}_a$ and the action of G on U is linear or 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 (16.38).

(b) This follows from (16.39) using the exact sequences

$$0 \rightarrow \alpha_p \rightarrow \alpha_{p^r} \rightarrow \alpha_{p^{r-1}} \rightarrow 0.$$

(c) The action of G on U is trivial, and so we have an exact sequence of G -modules with trivial action,

$$0 \rightarrow U \rightarrow \mathbb{G}_a \rightarrow \mathbb{G}_a \rightarrow 0$$

(see Exercise 15-3). In the exact sequence

$$\mathrm{Ext}^0(G, \mathbb{G}_a) \rightarrow \mathrm{Ext}^1(G, U) \rightarrow \mathrm{Ext}^1(G, \mathbb{G}_a),$$

the two end terms are zero (16.36).

(d,e) The statement follows from (a) if $U = \mathbb{G}_a$. Otherwise, there is an exact sequence

$$0 \rightarrow U \rightarrow \mathbb{G}_a \xrightarrow{\alpha} \mathbb{G}_a \rightarrow 0,$$

(see Exercise 15-3), and hence an exact sequence

$$\mathrm{Ext}^0(G, \mathbb{G}_a) \rightarrow \mathrm{Ext}^0(G, \mathbb{G}_a) \rightarrow \mathrm{Ext}^1(G, U) \rightarrow \mathrm{Ext}^1(G, \mathbb{G}_a).$$

But $\mathrm{Ext}^1(G, \mathbb{G}_a) = 0$, and $\mathrm{Hom}(G, \mathbb{G}_a)$ equals 0 if the action is trivial (14.24) 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. \square

EXTENSIONS OF UNIPOTENT GROUPS BY DIAGONALIZABLE GROUPS

PROPOSITION 16.42. *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 (16.9). For the second isomorphism, it suffices (after 16.10) to show that every extension

$$0 \rightarrow \mathbb{G}_m \xrightarrow{i} E \xrightarrow{\pi} \alpha_p \rightarrow 0$$

is a Hochschild extension, i.e., there exists a map $s: \alpha_p \rightarrow E$ 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. \square

PROPOSITION 16.43. *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. For the first assertion, we have $\underline{\text{Aut}}(D(M)) \simeq \underline{\text{Aut}}(M)_k$, which is a constant group scheme (not necessarily of finite type) — see Exercise 14.35. As α_p is connected, every homomorphism $\alpha_p \rightarrow \underline{\text{Aut}}(D)$ is trivial.

We now prove the second assertion. As $\text{Hom}(\alpha_p, \mathbb{G}_m) = 0$, from the Ext-sequence of

$$0 \rightarrow \mu_p \rightarrow \mathbb{G}_m \xrightarrow{x \mapsto x^p} \mathbb{G}_m \rightarrow 0,$$

we find that

$$\text{Ext}^1(\alpha_p, \mu_p) \rightarrow \text{Ext}^1(\alpha_p, \mathbb{G}_m)$$

is injective. From (16.42), we find that

$$\text{Ext}^1(\alpha_p, \mu_p) \simeq \text{Ext}^1(\alpha_p, \mathbb{G}_m) \simeq H_0^2(\alpha_p, \mu_p) \simeq \text{Ext}^1(\text{Lie}(\alpha_p), \text{Lie}(\mu_p)).$$

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 $\text{Lie}(\alpha_p)$ by $\text{Lie}(\mu_p)$ splits as an extension of vector spaces, and so it is equivalent to an extension

$$\mathcal{L}_\lambda: 0 \rightarrow ke \xrightarrow{j} ke \oplus kf_\lambda \xrightarrow{q} kf \rightarrow 0$$

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

$$\begin{array}{ccccccc} \mathcal{L}_\lambda: & 0 & \longrightarrow & ke & \xrightarrow{j} & ke \oplus kf_\lambda & \longrightarrow & kf & \xrightarrow{q} & 0 \\ & & & \parallel & & \downarrow u & & \parallel & & \\ \mathcal{L}_\mu: & 0 & \longrightarrow & ke & \xrightarrow{j} & ke \oplus kf_\mu & \longrightarrow & kf & \xrightarrow{q} & 0 \end{array}$$

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}_λ and \mathcal{L}_μ 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, p.455; *ibid.* 8.6, p.463; *ibid.* 8.7, p.464 for more details.

THEOREM 16.44. *Let D and U be algebraic groups over an algebraically closed field k with D diagonalizable and U unipotent. Then $\text{Ext}^1(U, D) = 0$.*

PROOF. Consider an exact sequence

$$e \rightarrow D \xrightarrow{i} G \xrightarrow{\pi} U \rightarrow e$$

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, α_p , or $(\mathbb{Z}/p\mathbb{Z})_k$ ($p \neq 1$) (15.24, 15.50). Consider the commutative diagram

$$\begin{array}{ccccccc}
 & & & e & & e & \\
 & & & \downarrow & & \downarrow & \\
 e & \longrightarrow & D & \xrightarrow{i_1} & \pi^{-1}(U_1) & \xrightarrow{\pi_1} & U_1 \longrightarrow e \\
 & & \parallel & & \downarrow & & \downarrow \\
 e & \longrightarrow & D & \xrightarrow{i} & G & \xrightarrow{\pi} & U \longrightarrow e \\
 & & & & \downarrow & & \downarrow \\
 & & & & H & \xrightarrow{\cong} & U/U_1 \\
 & & & & \downarrow & & \downarrow \\
 & & & & e & & e.
 \end{array}$$

Arguing by induction on the length of a subnormal series for U , we may suppose that i_1 admits a retraction $r_1: \pi^{-1}(U_1) \rightarrow D$. We form the pushout of the middle column of the diagram by r_1 :

$$\begin{array}{ccccccc}
 e & \longrightarrow & \pi^{-1}(U_1) & \longrightarrow & G & \longrightarrow & H \longrightarrow e \\
 & & \downarrow r_1 & & \downarrow u & & \downarrow \\
 e & \longrightarrow & D & \xrightarrow{i_2} & K & \longrightarrow & H \longrightarrow e.
 \end{array}$$

After (16.33, 16.34, 16.43) we have $\text{Ext}^1(H, D) = 0$ and so i_2 admits a retraction r_2 . Now $r = r_2 \circ u: G \rightarrow D$ is a retraction of i , which completes the proof. \square

EXTENSIONS OF MULTIPLICATIVE GROUPS BY MULTIPLICATIVE GROUPS

PROPOSITION 16.45. Every action of μ_p on \mathbb{G}_m or μ_p is trivial, and

$$\begin{aligned}
 \text{Ext}^1(\mu_p, \mathbb{G}_m) &\simeq k/\wp(k), \quad \text{where } \wp(x) = x^p - x \\
 \text{Ext}^1(\mu_p, \mu_p) &\simeq \mathbb{Z}/p\mathbb{Z} \oplus k/\wp(k).
 \end{aligned}$$

PROOF. The proof is similar to that of (16.43). \square

THEOREM 16.46. Every extension of a connected algebraic group of multiplicative type by an algebraic group of multiplicative type is of multiplicative type.

PROOF. We may assume that k is algebraically closed. Let $A(G'', G')$ denote the statement: for every exact sequence

$$e \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow e, \tag{124}$$

the algebraic group G is diagonalizable. We prove $A(G'', G')$ by an induction argument on the dimension of G'' . We may suppose $G'' \neq e$.

Consider an extension (124) with G' of multiplicative type. To show that G is diagonalizable, it suffices to show that every finite-dimensional representation (V, r) of G is diagonalizable (14.12). As G' is diagonalizable,

$$(V, r|_{G'}) = \bigoplus_{\chi \in X^*(G')} V_\chi.$$

Moreover, G' is contained in the centre of G (14.30), 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

$$\begin{array}{ccccccc} e & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' \longrightarrow e \\ & & \downarrow \chi & & \downarrow r & & \downarrow \bar{r} \\ e & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_V & \xrightarrow{q} & \mathrm{GL}_V / \mathbb{G}_m \longrightarrow e, \end{array}$$

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 (p the characteristic exponent of k) it suffices to prove $A(\mathbb{G}_m, \mathbb{G}_m)$ and $A(\mu_p, \mathbb{G}_m)$. In (16.35) (resp. 16.45) 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 (14.12).

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 14.9). Let G_1 denote the inverse image of N in G , and consider the diagram

$$\begin{array}{ccccccc} & & & & e & & e \\ & & & & \downarrow & & \downarrow \\ e & \longrightarrow & G' & \longrightarrow & G_1 & \longrightarrow & N \longrightarrow e \\ & & \parallel & & \downarrow & & \downarrow \\ e & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' \longrightarrow e \\ & & & & \downarrow & & \downarrow \\ & & & & G/G_1 & \xrightarrow{\cong} & G''/N \\ & & & & \downarrow & & \downarrow \\ & & & & e & & e. \end{array}$$

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 induction. □

COROLLARY 16.47. *Let G and G' be algebraic groups of multiplicative type with G connected. The map*

$$\mathrm{Ext}^1(G, G') \rightarrow \mathrm{Ext}^1_{\mathbb{Z}\Gamma\text{-modules}}(X^*(G'), X^*(G)), \quad \Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k),$$

defined by the functor X^ is a bijection.*

EXERCISE 16-1. Show that there are no noncommutative extensions of α_p by \mathbb{G}_m without using p -Lie algebras (see mo183139).

The structure of solvable algebraic groups

This chapter will be extensively revised for the final version.

a. Trigonalizable algebraic groups

DEFINITION 17.1. An algebraic group G is **trigonalizable** if every nonzero representation of G contains a one-dimensional subrepresentation (equivalently, if every simple representation is one-dimensional).

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 $\rho(v) = v \otimes a$, some $a \in \mathcal{O}(G)$.

For example, diagonalizable groups and unipotent algebraic groups are trigonalizable (14.12, 15.2). We now show that the trigonalizable groups are exactly the extensions of diagonalizable groups by unipotent algebraic groups. They are also the algebraic groups that arise as algebraic subgroups of \mathbb{T}_n for some n .

PROPOSITION 17.2. *The following conditions on an algebraic group G are equivalent:*

- (a) G is trigonalizable;
- (b) for every representation (V, r) of G , there exists a basis of V for which $r(G) \subset \mathbb{T}_n$, $n = \dim V$;
- (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 . We may suppose that $V \neq 0$; then there exists a nonzero e_1 in V such that $\langle e_1 \rangle$ is stable under G . The induction hypothesis applied to the representation of G on $V/\langle e_1 \rangle$ shows that there exist elements e_2, \dots, e_n of V forming a basis for $V/\langle e_1 \rangle$ and such that, relative to this basis, G acts on $V/\langle e_1 \rangle$ through \mathbb{T}_{n-1} . Now $\{e_1, e_2, \dots, e_n\}$ is a basis for V with the required property.

(b) \Rightarrow (c). Apply (b) to a faithful finite-dimensional representation of G (which exists by 4.8).

(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 an algebraic subgroup of a unipotent group

(15.5). Moreover, $G/U \hookrightarrow \mathbb{T}_n/\mathbb{U}_n \simeq \mathbb{G}_m^n$, and so G/U is an algebraic subgroup of a diagonalizable group; hence it is diagonalizable (14.9c).

(d) \Rightarrow (a). Let U be as in (d), and let (V, r) be a representation of G on a nonzero vector space. Because U is unipotent, $V^U \neq 0$, and because U is normal in G , V^U is stable under G (5.24). Hence G/U acts on V^U , and because G/U is diagonalizable, V^U is a sum of one-dimensional subrepresentations (14.12). In particular, it contains a one-dimensional subrepresentation. \square

COROLLARY 17.3. *Subgroups and quotients (but not necessarily extensions) of trigonalizable algebraic groups are trigonalizable.*

PROOF. Let H be an algebraic subgroup of a trigonalizable group G . As G is isomorphic to an algebraic subgroup of \mathbb{T}_n , so also is H . 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. \square

The group of 2×2 monomial matrices is an extension of trigonalizable algebraic groups without itself being trigonalizable (17.8).

COROLLARY 17.4. *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. \square

PROPOSITION 17.5. *Let G be an algebraic group that becomes trigonalizable over a separable field extension of k . Then G contains a unique normal unipotent algebraic subgroup G_u such that G/G_u is of multiplicative type; moreover, G_u contains all unipotent algebraic subgroups 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 algebraic subgroup V of G , because the composite $V \rightarrow G \rightarrow G/U$ is trivial (15.17); in particular, there exists at most one such U .

Now suppose that there exists a finite Galois extension k' of k such that $G_{k'}$ is trigonalizable. According to (17.2d), $G_{k'}$ contains a U as above, which, being unique, is stable under $\text{Gal}(k'/k)$, and therefore arises from an algebraic subgroup G_u of G (1.41). Now G_u is unipotent because $(G_u)_{k'}$ is unipotent (15.9), and G/G_u is of multiplicative type because $(G/G_u)_{k'}$ is diagonalizable (see the definition 14.16). \square

COROLLARY 17.6. *An algebraic group G becomes trigonalizable over a separable field extension of k if and only if it is an extension of a group of multiplicative type by a unipotent group.*

PROOF. Let G be an extension of a multiplicative group D by a unipotent group U . Then $G_{k^{\text{sep}}}$ is an extension of $D_{k^{\text{sep}}}$ by $U_{k^{\text{sep}}}$, and $D_{k^{\text{sep}}}$ is diagonalizable (14.16) and $U_{k^{\text{sep}}}$ is unipotent (15.9). Therefore $G_{k^{\text{sep}}}$ is trigonalizable (17.2d). The converse is proved in the proposition. \square

COMPLEMENTS

17.7. The algebraic group G_u of G in (17.5) is characterized by each of the following properties: (a) it is the greatest unipotent algebraic subgroup of G ; (b) it is the smallest normal algebraic subgroup H such that G/H is multiplicative type; (c) it is the unique normal unipotent algebraic subgroup H of G such that G/H is of multiplicative type. It follows from (c) that the formation of G_u commutes with extension of the base field.

17.8. Over an algebraically closed field, every commutative group variety is trigonalizable (see 17.16 below), but not every solvable group variety is trigonalizable. In particular, extensions of trigonalizable groups need not be trigonalizable. For example, the algebraic group of monomial $n \times n$ matrices is solvable if $n \leq 4$ (see 5.55), 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 .

17.9. Let G be as in (17.5) with k perfect. Let (V, r) be a faithful representation of G . By assumption, there exists a basis of $V_{k^{\text{al}}}$ for which $r(G)_{k^{\text{al}}} \subset \mathbb{T}_n$, and then (by definition)

$$r(G_u)_{k^{\text{al}}} = \mathbb{U}_n \cap r(G)_{k^{\text{al}}}.$$

As $\mathbb{U}_n(k^{\text{al}})$ consists of the unipotent elements of $\mathbb{T}_n(k^{\text{al}})$, it follows that $G_u(k^{\text{al}})$ consists of the unipotent elements of $G(k^{\text{al}})$:

$$G_u(k^{\text{al}}) = G(k^{\text{al}})_u.$$

17.10. Let G be as in (17.5). Later (17.26 et seq.) we shall give various conditions under which the exact sequence

$$1 \rightarrow G_u \rightarrow G \rightarrow G/G_u \rightarrow 1 \tag{125}$$

splits.

17.11. Let G be a *smooth* algebraic group as in (17.5). Because the sequence (125) splits over k^{al} (see 17.27 below), G becomes isomorphic to $G_u \times G/G_u$ (as a scheme) over k^{al} , and so G_u is smooth. When k is perfect, G_u is the unique smooth algebraic subgroup of G such that

$$G_u(k^{\text{al}}) = G(k^{\text{al}})_u.$$

A smooth algebraic group G over a field k is trigonalizable if and only if its geometric unipotent radical U (8.40) is defined over k and G/U is a split torus.

ASIDE 17.12. The term “trigonalizable” is used in Borel 1991, p. 203, and Springer 1998, p.237. In French “trigonalisable” is standard (e.g., DG IV, §2, 3.1, p.491). Other names used: “triangular”; “triagonalizable” (Waterhouse 1979, p.72).

ASIDE 17.13. In DG IV, §2, 3.1, p. 491, a group scheme G over a field is defined to be trigonalizable if it is affine and has a normal unipotent algebraic subgroup U such that G/U is diagonalizable. This agrees with our definition (see 17.2).

In Springer 1998, 14.1, a group variety over k is defined to be trigonalizable over k if it is isomorphic to a group subvariety of \mathbb{T}_n for some n . This agrees with our definition (see 17.2).

b. Commutative algebraic groups

Let u be an endomorphism of a finite-dimensional vector space V over k . If the eigenvalues of u all lie in k , then there exists a basis for V relative to which the matrix of u lies in

$$\mathbb{T}_n(k) = \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\}$$

(11.10). We extend this elementary statement to sets of commuting endomorphisms, and then to solvable group varieties over algebraically closed fields.

LEMMA 17.14. *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 for which S is contained in the group of upper triangular matrices, i.e., a basis e_1, \dots, e_n such that*

$$u(\langle e_1, \dots, e_i \rangle) \subset \langle e_1, \dots, e_i \rangle \text{ for all } i. \quad (126)$$

In more down-to-earth terms, for any commuting set S of $n \times n$ matrices, there exists an invertible matrix P such that PAP^{-1} is upper triangular for all $A \in S$.

PROOF. We prove this by induction on the dimension of V . If every $u \in S$ 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 $V_a \neq V$. Because every element of S commutes with u , V_a is stable under the action of the elements of S : for $s \in S$ and $x \in V_a$,

$$u(sx) = s(ux) = s(ax) = a(sx).$$

The induction hypothesis applied to S acting on V_a and V/V_a shows that there exist bases e_1, \dots, e_m for V_a and $\bar{e}_{m+1}, \dots, \bar{e}_n$ for V/V_a such that

$$\begin{aligned} u(\langle e_1, \dots, e_i \rangle) &\subset \langle e_1, \dots, e_i \rangle \quad \text{for all } i \leq m \\ u(\langle \bar{e}_{m+1}, \dots, \bar{e}_{m+i} \rangle) &\subset \langle \bar{e}_{m+1}, \dots, \bar{e}_{m+i} \rangle \quad \text{for all } i \leq n - m. \end{aligned}$$

Let $\bar{e}_{m+i} = e_{m+i} + V_a$ with $e_{m+i} \in V$. Then e_1, \dots, e_n is a basis for V satisfying (17). \square

PROPOSITION 17.15. *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 1.9), this implies that $G \cap \mathbb{T}_n = G$, and so $G \subset \mathbb{T}_n$. \square

COROLLARY 17.16. *Every smooth commutative algebraic group G over an algebraically closed field is trigonalizable.*

PROOF. Let $r: G \rightarrow \text{GL}_V$ be a representation of G . Then $r(G)$ is a smooth commutative algebraic group (5.8), and so it is contained in \mathbb{T}_n for some choice of a basis $\{e_1, \dots, e_n\}$. Now $\langle e_1 \rangle$ is a one-dimensional subrepresentation of V . \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 11.17 shows that

$$G(k) = G(k)_s \times G(k)_u \quad (\text{product of sets}). \tag{127}$$

This is not usually a decomposition of groups because products do not generally respect Jordan decompositions. When G is commutative, the product map $m: G \times G \rightarrow G$ is a homomorphism of algebraic groups, and so it *does* respect the Jordan decompositions (11.20):

$$(gg')_s = g_s g'_s \quad (gg')_u = g_u g'_u$$

(this can also be proved directly). Thus, in this case (127) realizes $G(k)$ as a product of abstract subgroups. We can do better.

THEOREM 17.17. *Let G be a commutative algebraic group over a field k .*

- (a) *There exists a greatest 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 G also contains a greatest unipotent algebraic subgroup G_u , and*

$$G = G_s \times G_u$$

(unique decomposition of G into a product of a multiplicative algebraic subgroup and a unipotent subgroup); when G is connected (resp. smooth) then G_s and G_u are both connected (resp. smooth).

PROOF. (a) Let G_s denote the intersection of the algebraic subgroups H of G such that G/H is unipotent. Then $G/G_s \rightarrow \prod G/H$ is an embedding, and so G/G_s is unipotent (15.7).

A nontrivial homomorphism $G_s \rightarrow \mathbb{G}_a$ would have a kernel H such that G/H is an extension of unipotent groups,

$$0 \rightarrow G_s/H \rightarrow G/H \rightarrow G/G_s \rightarrow 0$$

(here we use that G is commutative), and hence is unipotent (15.7), but this contradicts the definition of G_s . Therefore no such homomorphism exists and G is of multiplicative type (14.24c). If H is a second algebraic subgroup of G of multiplicative type, then the homomorphism $H \rightarrow G/G_s$ is trivial (15.18), and so $H \subset G_s$. Therefore G_s is the greatest algebraic subgroup of G of multiplicative type.

Let α be an endomorphism of G_R for some k -algebra R . The composite

$$(G_s)_R \rightarrow G_R \xrightarrow{\alpha} G_R \rightarrow (G/G_s)_R$$

is trivial (16.18), and so $\alpha(G_{sR}) \subset G_{sR}$. Hence G_s is characteristic (1.40).

(b) Assume that k is perfect. It suffices to prove that there exists a greatest unipotent subgroup when k algebraically closed (1.41b, 15.9). We have an exact sequence

$$1 \rightarrow G_s \rightarrow G \rightarrow G/G_s \rightarrow 1$$

with G/G_s unipotent, and (16.44) shows that the sequence splits. Therefore, $G = G_s \times U$ with U unipotent. For any other unipotent affine subgroup U' of G , the homomorphism $U' \rightarrow G/U \simeq T$ is zero (15.17), and so $U' \subset U$. Therefore U is the greatest unipotent algebraic subgroup of G . It follows that the decomposition is unique.

The last statement follows from the fact that G_s and G_u are quotients of G . □

COROLLARY 17.18. *Let G be a smooth connected algebraic group of dimension 1 over a perfect field. Either $G = \mathbb{G}_a$ or it becomes isomorphic to \mathbb{G}_m over k^{al} .*

PROOF. We know that G is commutative (15.27), and hence a product $G = G_s \times G_u$ of algebraic groups. Because G is smooth and connected, so also are G_s and G_u (they are quotients of G). Either $G = G_u$, in which case it is isomorphic to \mathbb{G}_a (15.51), or $G = G_s$, in which case it is a one-dimensional torus. \square

COROLLARY 17.19. *A smooth connected commutative algebraic group G over a perfect field k is a product of a torus with a smooth connected commutative unipotent algebraic group. When k has characteristic zero, every smooth commutative unipotent algebraic group is a vector group (product of copies of \mathbb{G}_a).*

PROOF. Write $G = G_s \times G_u$ (as in 17.17). Both G_s and G_u are smooth connected commutative algebraic groups (because G is). A smooth connected algebraic group of multiplicative type is a torus, and a connected commutative unipotent algebraic group in characteristic zero is a product of copies of \mathbb{G}_a (15.32). \square

NOTES. The first published proof that the only connected algebraic groups of dimension 1 are \mathbb{G}_a and \mathbb{G}_m is that given by Grothendieck in Chevalley 1956-58 (Section 7.4).

COMPLEMENTS

17.20. The algebraic subgroup G_s of G in (17.17) is characterized by each of the following properties: (a) it is the greatest algebraic subgroup of G of multiplicative type; (b) it is the smallest algebraic subgroup H of G such that G/H is unipotent; (c) it is the unique algebraic subgroup H of G of multiplicative type such that G/H is unipotent. It follows from (c) that the formation of G_s commutes with extension of the base field. Therefore G_s is connected (resp. smooth) if G is connected (resp. smooth) because it becomes so over k^{al} (17.17b).

17.21. Let G be a commutative group variety over a perfect field k . Then $G = G_s \times G_u$ where G_s and G_u are the unique subgroup varieties of G such that $G_s(k^{\text{al}}) = G(k^{\text{al}})_s$ and $G_u(k^{\text{al}}) = G(k^{\text{al}})_u$. Indeed, the groups G_s and G_u in (17.17b) satisfy these conditions. Thus, we have realized the decomposition (127) on the level of group varieties.

17.22. In general, G_u is not a characteristic subgroup. The argument in the proof of (17.17) for G_s fails because there may exist nontrivial homomorphisms $G_{uR} \rightarrow G_{sR}$ (16.19).

17.23. It is necessary that k be perfect in (b) of Theorem 17.17. Let k be a separably closed field of characteristic p , and let k' be a (purely inseparable) extension of k of degree p . Let $G = (\mathbb{G}_m)_{k'/k}$ be the algebraic group over k obtained from \mathbb{G}_m by restriction of scalars. Then G is a smooth connected commutative algebraic group over k . The canonical embedding $i: \mathbb{G}_m \rightarrow G$ (2.37) has unipotent cokernel, and so realizes \mathbb{G}_m as the greatest algebraic subgroup of G of multiplicative type. However, G contains no complementary unipotent algebraic subgroup because $G(k) = (k')^\times$ has no p -torsion. (See Chapter 22 for more details. The group G is a basic example of a pseudoreductive algebraic group.)

c. Structure of trigonalizable algebraic groups

Recall that a trigonalizable algebraic group G has a greatest unipotent algebraic subgroup G_u ; moreover, G_u is normal, and G/G_u is diagonalizable (17.10).

THEOREM 17.24. *Let G be a trigonalizable algebraic group over a field k . There exists a normal series,*

$$G \supset G_0 \supset G_1 \supset \cdots \supset G_r = e$$

such that

- (a) $G_0 = G_u$, and
- (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

$$e \rightarrow \mathbb{U}_n \rightarrow \mathbb{T}_n \xrightarrow{q} \mathbb{D}_n \rightarrow e$$

we obtain an exact sequence

$$e \rightarrow G \cap \mathbb{U}_n \rightarrow G \rightarrow q(G) \rightarrow e.$$

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 $G_u \stackrel{\text{def}}{=} G \cap \mathbb{U}_n$ is the greatest unipotent subgroup 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 8.46).

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 it through an action that extends to a linear action on \mathbb{G}_a , and the action of $G_u \subset G$ is trivial. \square

COROLLARY 17.25. *Let G be a trigonalizable algebraic group over an algebraically closed field k . There exists a normal series of G ,*

$$G \supset G_u = G_0 \supset G_1 \supset \cdots \supset G_s = e$$

such that, for each $i \geq 0$,

- (a) each quotient G_i/G_{i+1} is isomorphic to \mathbb{G}_a , α_p , or $(\mathbb{Z}/p\mathbb{Z})_k^m$, and
- (b) the action by inner automorphisms of G (resp. G_u) on each quotient is linear (resp. trivial).

PROOF. Immediate consequence of the theorem and Exercise 15-3. \square

THEOREM 17.26. *Let G be a trigonalizable algebraic group over k . The sequence*

$$e \rightarrow G_u \rightarrow G \rightarrow D \rightarrow e$$

splits in each of the following cases;

- (a) *k is algebraically closed;*
- (b) *G_u is split (15.55);*
- (c) *k is perfect and G/G_u is connected.*

PROOF. If $G = D$, there is nothing to prove, and so we may suppose that $G_u \neq e$. Let $N = G^{(i)}$ be the last nontrivial group in the normal series for G_u defined in (17.24). Then G/N is trigonalizable (17.3), and we have an exact sequence

$$e \rightarrow G_u/N \rightarrow G/N \rightarrow D \rightarrow e \tag{128}$$

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 .

With the notations of the proof of (17.24), we know that N is a subgroup of $U^{(i)}/U^{(i+1)} \simeq \mathbb{G}_a$, and that D acts linearly on \mathbb{G}_a . We therefore have an exact sequence

$$e \rightarrow N \rightarrow \mathbb{G}_a \rightarrow \mathbb{G}_a/N \rightarrow e$$

on which D acts linearly. The quotient \mathbb{G}_a/N is either trivial or isomorphic to \mathbb{G}_a (Exercise 15-3).

We now prove the theorem. Let $\bar{s}: D \rightarrow G/N$ be a section to (128), and form the exact commutative diagram

$$\begin{array}{ccccccccc} e & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & D & \longrightarrow & e \\ & & \parallel & & \downarrow h & & \downarrow \bar{s} & & \\ e & \longrightarrow & N & \longrightarrow & G & \xrightarrow{p} & G/N & \longrightarrow & e \end{array}$$

In each case, the top extension splits: (a) see (16.41d); (b) see (16.41a); (c) apply (16.41b) and (16.41c) to the end terms of

$$e \rightarrow G_u^\circ \rightarrow G_u \rightarrow \pi_0(G_u) \rightarrow e.$$

Let $s'': D \rightarrow G'$ be a section to $G' \rightarrow D$; then $s \stackrel{\text{def}}{=} h \circ s''$ is a section of $G \rightarrow D$. □

THEOREM 17.27. *Let*

$$e \rightarrow U \rightarrow G \rightarrow D \rightarrow e$$

be an extension of a diagonalizable group D by a unipotent group U over an algebraically closed field k . If $s_1, s_2: D \rightarrow G$ are two sections to $G \rightarrow D$ (as a homomorphism of algebraic groups), then there exists a $u \in U(k)$ such that $s_2 = \text{inn}(u) \circ s_1$.

PROOF. We begin with an observation. Let $s: D \rightarrow G$ be a section to $G \rightarrow D$. When we use s to write G as a semidirect product $G = U \rtimes D$, the remaining sections to $G \rightarrow D$ are of the form $d \mapsto (f(d), d)$ with $f: D \rightarrow U$ a crossed homomorphism. Such a section is of the form $\text{inn}(u) \circ s$ if and only if the crossed homomorphism f is principal (see 16.1).

Let s and s_1 be two sections to $G \rightarrow D$. Let N be the last nontrivial term in the normal series (17.24) for G . Let $\bar{s} = p \circ s$ and form the commutative diagram

$$\begin{array}{ccccccc} e & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & D \longrightarrow e \\ & & \parallel & & \downarrow h & & \downarrow \bar{s} \\ e & \longrightarrow & N & \longrightarrow & G & \xrightarrow{p} & G/N \longrightarrow e. \end{array}$$

Now \bar{s} and $p \circ s_1$ are two sections of

$$e \rightarrow U/N \rightarrow G/N \rightarrow D \rightarrow e.$$

By induction on the length of the normal series of G , there exists a $\bar{u} \in (U/N)(k)$ such that $\text{inn}(\bar{u}) \circ p \circ s_1 = \bar{s}$. Let $u \in U(k)$ lift \bar{u} ; then

$$p \circ \text{inn}(u) \circ s_1 = \bar{s},$$

and, by replacing s_1 with $\text{inn}(u) \circ s_1$, we may suppose that $p \circ s_1 = \bar{s}$. From the construction of G' as a pull-back, we see that there exists a sections $\sigma, \sigma_1: D \rightarrow G'$ such that $s = h \circ \sigma$ and $s_1 = h \circ \sigma_1$. As $H^1(D, N) = 0$ (16.3), there exists a $u \in N(k)$ such that $\text{inn}(u) \circ \sigma = \sigma_1$, and therefore $\text{inn}(u) \circ s = s_1$, which completes the proof. \square

THEOREM 17.28. *Let G be a trigonalizable algebraic group over an algebraically closed field. The sequence*

$$e \rightarrow G_u \rightarrow G \rightarrow D \rightarrow e$$

splits. Every diagonalizable subgroup of G is contained in a maximal diagonalizable subgroup, the maximal diagonalizable subgroups are those of the form $s(D)$ with s a section to $G \rightarrow D$, and any two maximal diagonalizable subgroups are conjugate by an element of $G_u(k)$.

PROOF. The first statement follows directly from (17.26). For the second statement, let s be a section of $q: G \rightarrow D$ and let S be a diagonalizable subgroup of G . We have $S \cap G_u = e$, and so q induces an isomorphism of S onto $q(S)$. Let $G' = q^{-1}(q(S))$ and $q' = q|_{G'}$. The sequence

$$e \rightarrow G_u \rightarrow G' \xrightarrow{q'} q(S) \rightarrow e$$

is split by $s' = s|_{q(S)}$. As S is a section of q' , there exists by (17.26) a $u \in G_u(k)$ such that $S = \text{inn}(u)s'q(S)$. We deduce that $S \subset \text{inn}(u)s(G/G_u)$. This shows that $s(G/G_u)$ is a maximal diagonalizable subgroup of G , and that such subgroups are conjugate, which completes the proof. \square

COROLLARY 17.29. *Let G be a smooth connected trigonalizable algebraic group over an algebraically closed field. Then G_u and G/G_u are smooth and connected, and there exists a sequence*

$$G_u = G_0 \supset G_1 \supset \cdots \supset G_n = e$$

of smooth connected normal unipotent subgroups of G such that each quotient G_i/G_{i+1} is isomorphic to \mathbb{G}_a with G acting linearly and G_u acting trivially.

PROOF. We know (17.27) that $G \approx G_u \times G/G_u$ as algebraic schemes. It follows that G_u and G/G_u are smooth and connected. With the notations of the proof of (17.24), consider the groups $(G^{(i)})_{\text{red}}^\circ$ — these are smooth connected unipotent subgroups of G_u . Moreover, each $g \in G(k)$ normalizes $G^{(i)}$, hence $(G^{(i)})^\circ$, and hence $(G^{(i)})^\circ(k) = (G^{(i)})_{\text{red}}^\circ(k)$. As G and $(G^{(i)})_{\text{red}}^\circ$ are smooth and k is algebraically closed, this implies that $(G^{(i)})_{\text{red}}^\circ$ is normal in G (1.62). Finally, $(G^{(i)})_{\text{red}}^\circ / (G^{(i+1)})_{\text{red}}^\circ$ is a smooth connected algebraic subgroup of $U^{(i)} / U^{(i+1)}$, which is isomorphic to \mathbb{G}_a . It is therefore either e or $U^{(i)} / U^{(i+1)}$. Therefore, the groups $(G^{(i)})_{\text{red}}^\circ$, with duplicates omitted, form a sequence with the required properties. \square

COROLLARY 17.30. *Let G be a smooth connected unipotent algebraic group over an algebraically closed field. There exists a sequence*

$$G_u = G_0 \supset G_1 \supset \cdots \supset G_n = e$$

of smooth connected normal unipotent subgroups of G such that each quotient is isomorphic to \mathbb{G}_a with G acting trivially.

PROOF. Special case of 17.29. \square

COROLLARY 17.31. *Let*

$$e \rightarrow D \rightarrow G \rightarrow U \rightarrow e$$

be an exact sequence of algebraic groups over an algebraically closed field with D diagonalizable and U smooth connected and unipotent. The sequence has a unique splitting:

$$G \simeq D \times U.$$

PROOF. Because U is connected, it acts trivially on D (14.29). If $s: U \rightarrow G$ is a section, then $s(U) = G_u$, and s is uniquely determined. We prove that a section s exists by induction on the dimension of U . If $\dim(U) > 0$, then G contains a central subgroup isomorphic to \mathbb{G}_a . Arguing as in the proof of (17.26), we find that it suffices to prove that there exists a section in the case $U = \mathbb{G}_a$, but this follows from (16.7). \square

COROLLARY 17.32. *Assume that k is algebraically closed. If U is smooth connected and unipotent and D is diagonalizable, then*

$$H^1(U, D) = 0 = H^2(U, D).$$

NOTES. Many of the results in this section hold for extensions of algebraic groups of multiplicative type by unipotent groups — see SGA 3, XVii, 5.6.1, p.351. It will be rewritten for the final version.

d. Solvable algebraic groups

Recall that an algebraic group is unipotent if it admits a faithful unipotent representation, in which case every representation is unipotent (15.3, 15.5). Therefore, an algebraic subgroup U of an algebraic group G is unipotent if and only if the restriction to U of every finite-dimensional representation of G is unipotent.

THEOREM 17.33 (LIE-KOLCHIN). *Let G be a solvable algebraic group over k . If G is smooth and connected and k is algebraically closed, then G is trigonalizable.*

PROOF. Assume the hypotheses, and 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 (17.16).

Let N be the derived group of G . Then N is a smooth connected normal algebraic subgroup of G (8.21) and, because G is solvable, $\dim(N) < \dim(G)$. By induction, 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 (4.17), 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 $\chi^g \stackrel{\text{def}}{=} (n \mapsto \chi(g^{-1}ng))$ 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

$$\chi(n) = \chi(g^{-1}ng) \text{ for all } n \in N(k). \tag{129}$$

Clearly H is a subgroup of finite index in $G(k)$, and it is closed for the Zariski topology on $G(k)$ because (129) 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 8.22), 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 $\chi: N \rightarrow \mathbb{G}_m$ is contained in μ_d . As N is smooth and connected, this implies that $\chi(N) = e$ (8.10), 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 (17.16). \square

COROLLARY 17.34. *A solvable algebraic group G becomes trigonalizable over a separable extension of k if and only if $(G_{k^{\text{al}}})_u$ is defined over k .*

PROOF. Suppose $(G_{k^{\text{al}}})_u = (G_u)_{k^{\text{al}}}$ with G_u an algebraic subgroup of G . Then G_u is unipotent, and G/G_u is of multiplicative type, and so G becomes trigonalizable over a separable extension of k by (17.6). Conversely, if G becomes trigonalizable over a separable extension of k , then it contains a normal unipotent subgroup U such that G/U is of multiplicative type. Clearly $U_{k^{\text{al}}} = (G_{k^{\text{al}}})_u$. \square

COROLLARY 17.35. *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. Apply the theorem to G_{red}° , and note that $G_{\text{red}}^\circ(k) = G^\circ(k)$. \square

17.36. All the hypotheses in the theorem are needed.

CONNECTED: The algebraic group G of monomial 2×2 matrices is solvable but not trigonalizable (17.8).

SMOOTH: Let k have characteristic 2, and let G be the algebraic subgroup of SL_2 of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a^2 = 1 = d^2$ and $b^2 = 0 = c^2$. Then G is nonsmooth and connected, and the exact sequence

$$e \longrightarrow \mu_2 \xrightarrow{a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}} G \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (ab, cd)} \alpha_2 \times \alpha_2 \longrightarrow e$$

shows that it is solvable, but no line is fixed in the natural action of G on k^2 . Therefore G is not trigonalizable. See Exercise 17-1. Note that $G(k) = \{e\}$.

SOLVABLE: This condition is necessary because every algebraic subgroup of \mathbb{T}_n is solvable.

k ALGEBRAICALLY CLOSED: If $G(k) \subset \mathbb{T}_n(k)$, then the elements of $G(k)$ have a common eigenvector, namely, $e_1 = (1 \ 0 \ \dots \ 0)^t$. If k is not algebraically closed, then an endomorphism of k^n need not have an eigenvector. For example,

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}, \quad a^2 + b^2 = 1 \right\}$$

is a connected commutative algebraic group over \mathbb{R} that is not trigonalizable over \mathbb{R} .

THEOREM 17.37. *Let G be a smooth connected solvable algebraic group over a perfect field k .*

(a) *There exists a unique connected normal algebraic subgroup G_u of G such that G_u is unipotent and G/G_u is of multiplicative type.*

(b) *The subgroup G_u in (a) contains all unipotent algebraic subgroups of G (it is the greatest unipotent algebraic subgroup of G), and its formation commutes with extension of the base field.*

(c) *The subgroup G_u in (a) is smooth and G/G_u is a torus; moreover, G_u is the unique smooth algebraic subgroup of G such that*

$$G_u(k^{\mathrm{al}}) = G(k^{\mathrm{al}})_u.$$

(d) *Assume 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 17.33 shows that G becomes trigonalizable over a finite (separable) extension of k , and so this summarizes earlier results (17.5, 17.7, 17.9, 17.28). As a scheme, G is isomorphic to $G_u \times T$, which shows that G_u is smooth. \square

PROPOSITION 17.38. *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 admits a normal series with quotients \mathbb{G}_a or \mathbb{G}_m (i.e., 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). 17.29

(b) \Rightarrow (c). By induction, each term in the normal series $G \supset G_1 \supset \cdots$ is smooth and connected. Moreover, $G(k) \supset G_1(k) \supset \cdots$ is a normal series for $G(k)$ with commutative quotients, and so $G(k)$ is solvable.

(c) \Rightarrow (d). Recall (p.133) that the derived series for G is the normal series

$$G \supset DG \supset D^2G \supset \cdots.$$

Each group $D^i G$ is smooth and connected (8.21), and $D^{i+1}(G)(k)$ is the derived group of $D^i(G)(k)$ (8.22). Therefore $D^i(G)(k) = e$ for i large, which implies that $D^i(G) = e$ of i large. Hence the derived series terminates with e , and so G is solvable.

(d) \Rightarrow (a). This is the Lie-Kolchin theorem (17.33). \square

ASIDE 17.39. The above proof of Theorem 17.33 is essentially Kolchin's original proof (Kolchin 1948a, §7, Theorem 1, p. 19). Lie proved the analogous result for Lie algebras in 1876.

ASIDE 17.40. The implication (c) \Rightarrow (a) in (17.38) is sometimes called the Lie-Kolchin theorem.

e. Solvable algebraic groups (variant)

For group varieties over an algebraically closed field, Doković 1988 gave a simpler approach to the main theorems of this chapter. In the final version, this will be incorporated into the rest of the chapter (see aside 18.46).

Throughout, G is a connected group variety and k is algebraically closed.

Let N be a normal algebraic subgroup of G , and let $s \in G(k)$. Then $C_N(s)$ is the subscheme of N on which $n \mapsto sns^{-1}$ agrees with the identity map.

PROPOSITION 17.41. *Let s be a semisimple element of $G(k)$, and let S be the closure of the subgroup of $G(k)$ generated by s . Then $C_G(s)$ is smooth, and $C_G(S) = C_G(s)$.*

PROOF. The algebraic group S is linearly reductive, and $s \in S(k)$ is dense in S . Therefore the statement is a special case of (14.61). \square

LEMMA 17.42. *Let N be a connected normal subgroup variety of G , and let $s \in G(k)$. If N is commutative and unipotent, and s is semisimple, then $C_N(s)$ is connected; moreover, the map $N \times C_N(s) \rightarrow N$, $u, v \mapsto [s, u] \cdot v$ is surjective.*

PROOF. As N is commutative, the regular map

$$N \rightarrow N, \quad u \mapsto [s, u],$$

is a homomorphism of algebraic groups. Its kernel is $C_N(s)$, and we let M denote its image; thus

$$\dim N = \dim M + \dim C_N(s) \tag{130}$$

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 $x = 1$. Hence the multiplication map

$$\mu: M \times C_N(s) \rightarrow N$$

has finite connected kernel. Now (130) implies that it is surjective. As N is connected, so is $C_N(s)$. \square

THEOREM 17.43. *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 unipotent.*

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 $G \rightarrow G/N$. 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 $v \in C_N(s)$ (17.42). 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 $v = 1$ because of the uniqueness of the Jordan decomposition. Thus $u^{-1}z \in C_G(s)$. We have shown that $C_G(s)(k) \rightarrow C_{\bar{G}}(\bar{s})(k)$ is surjective, which implies that $C_G(s) \rightarrow C_{\bar{G}}(\bar{s})$ is surjective, because $C_{\bar{G}}(\bar{s})$ is smooth. Therefore, the sequence

$$e \rightarrow C_N(s) \rightarrow C_G(s) \rightarrow C_{\bar{G}}(\bar{s}) \rightarrow e$$

is exact. By induction, $C_{\bar{G}}(\bar{s})$ are connected; as $C_N(s)$ is connected, so also is $C_G(s)$ (5.52).

By induction, $\bar{G} = U \cdot C_{\bar{G}}(\bar{s})$ 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 . \square

LEMMA 17.44. *Let $S \subset \mathbb{T}_n(k)$ be a commuting set of semisimple elements. Then there exists a $b \in \mathbb{T}_n(k)$ such that $b^{-1}Sb \subset \mathbb{D}_n$.*

PROOF. From elementary linear algebra, we know that there exists an $a \in \mathrm{GL}_n(k)$ such that $aSa^{-1} \subset \mathbb{D}_n(k)$. Hence, the subalgebra A of $M_n(k)$ generated by the elements of S is étale over k . Let it act on k^n by left multiplication. For each i , $1 \leq i \leq n$, $V_{i-1} \stackrel{\text{def}}{=} \langle e_1, \dots, e_{i-1} \rangle$ is an A -submodule of $V_i \stackrel{\text{def}}{=} \langle e_1, \dots, e_i \rangle$. Because A is semisimple, there exists a $v_i \in V_i \setminus V_{i-1}$ such that $Av_i = \langle v_i \rangle$. Let b be the matrix whose i th column is v_i . Then $b \in \mathbb{T}_n(k)$ and $b^{-1}Sb \subset \mathbb{D}_n$. \square

LEMMA 17.45. *Let G be a connected solvable group variety. Let T be a subgroup variety of G such that $T(k)$ consists of semisimple elements. If $G = U \cdot T$ with U a unipotent subgroup variety of G , then T is a torus and $G = U \rtimes T$.*

PROOF. By the Lie-Kolchin theorem, we may assume that G is an algebraic subgroup of some \mathbb{T}_n . From the quotient map $\mathbb{T}_n \rightarrow \mathbb{D}_n$ we get a short exact sequence

$$e \rightarrow U' \rightarrow G \xrightarrow{p} D \rightarrow e$$

with $U' = \mathbb{U}_n \cap G$ a unipotent group and D a subtorus of \mathbb{D}_n . As $p(U) = e$, we have $U \subset U'$, and so $G = U' \cdot T$. Now

$$D = p(G) = p(U' \cdot T) = p(T)$$

and so $D = D^\circ = p(T^\circ)$. Hence $G = U' \cdot T^\circ$. From the finiteness of $U' \cap T^\circ$ we conclude that $T = T^\circ$. In particular T is commutative, by Lemma 17.44 allows us to assume that $T \subset \mathbb{D}_n$, i.e., $T = D$. As $\mathbb{T}_n = \mathbb{U}_n \rtimes \mathbb{D}_n$ and $U \subset U' \subset \mathbb{U}_n$, $T = D \subset \mathbb{D}_n$, and $G = U \cdot T$, we conclude that $G = U \rtimes T$. \square

THEOREM 17.46. *Let G be a connected solvable group variety. Then there is a connected subgroup variety G_u such that $G_u(k) = G(k)_u$, and $G = G_u \rtimes T$ with T a maximal torus in G .*

PROOF. We use induction on $\dim G$. Assume first that $G(k)_s \subset Z(G)(k)$. Then $G(k)_s = Z(G)_s(k)$ is a closed subgroup of G , and $G = G_u \cdot G_s$. The assertion then follows from Lemma 17.45. Now assume that there exists a semisimple element s of $G(k)$ not in $Z(G)(k)$. Then $C_G(s)$ is proper smooth algebraic subgroup of G (14.55). By Theorem 17.43, it is connected and $G = G_u \cdot C_G(s)$. By the induction hypothesis, there exists a torus T such that $C_G(s) = C_G(s)_u \cdot T$. Now $G = G_u \cdot C_G(s) = G_u \cdot T$, and $G = G_u \rtimes T$ (17.45). \square

THEOREM 17.47. *Let $G = G_u \rtimes T$ be a connected solvable group variety. Then every semisimple element s of $G(k)$ is conjugate to an element of $T(k)$.*

PROOF. We use induction on $\dim G$. Let $s = ut$ with u unipotent and $t \in T(k)$. If G is commutative, then $u = 1$ and $s = t$. Otherwise, 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. By the induction hypothesis, there exists an $x \in G(k)$ such that $xsx^{-1} = tv$ with $v \in N$. By Lemma 17.42, $v = [t^{-1}, u] \cdot z$ for some $u \in N$ and $z \in C_N(t)$. Hence

$$xsx^{-1} = tv = utu^{-1}z.$$

As xsx^{-1} and utu^{-1} are semisimple and z commutes with u and t , it follows that $z = 1$, and so

$$xsx^{-1} = utu^{-1}. \quad \square$$

THEOREM 17.48. *Let G be a connected solvable group variety, let T be a maximal torus of G , and let S be a commuting set of semisimple elements of $G(k)$. Then $C_G(S)$ is connected, and $aSa^{-1} \subset T$ for some $a \in G$. In particular, all maximal tori in G are conjugate.*

PROOF. We use induction on $\dim G$. The assertions are obvious if $S \subset Z(G)(k)$. Otherwise, choose $s \in S \setminus Z(G)(k)$. By Theorem 17.47 we may assume that $s \in T$. Then $C_G(s)$ is a proper subgroup variety of G containing T and S . By Theorem 17.43, $C_G(s)$ is connected. As it is solvable (8.13) and $\dim C_G(s) < \dim G$, we can apply induction to conclude the proof. \square

We finally describe the nilpotent group varieties.

THEOREM 17.49. *A connected solvable group variety G is nilpotent if and only if one (hence every) maximal torus in G is contained in $Z(G)$.*

PROOF. Assume that G is nilpotent. We prove that $G_s = T \subset Z(G)$ by induction on G . We may assume that G is not commutative. Let N be the last nontrivial term in the lower central series of G . Let f be the quotient map $x \mapsto \bar{x}: G \rightarrow G/N$. Then $\bar{G} = f(G_u T) = (\bar{G})_u \cdot f(T)$. By the induction hypothesis, we have $f(T) = (\bar{G})_s \subset Z(\bar{G})$. Consequently, if $t \in T$ and $x \in G$, then $u \stackrel{\text{def}}{=} txt^{-1}x^{-1} \in N$. As $N \subset Z(G) \cap G_u$ and $xtx^{-1} = u^{-1}t = tu^{-1}$, we must have $u = 1$. Thus $T \subset Z(G)$, and, by Theorem 17.47, $G_s = T$. The converse is obvious. \square

COROLLARY 17.50. *The connected nilpotent group varieties are those of the form $U \times T$ with U a unipotent group variety and T a torus.*

f. Nilpotent algebraic groups

We extend the earlier results for commutative algebraic groups to nilpotent algebraic groups.

Recall (8.12) that an algebraic group is nilpotent if it admits central subnormal series. The last nontrivial term in such a series is contained in the centre of the group. Therefore, every nontrivial nilpotent algebraic group has nontrivial centre (and the centre of a nilpotent group variety of dimension > 0 has dimension > 0).

LEMMA 17.51. *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 (14.32) that the action of G on H by inner automorphisms is trivial. Therefore H is central, in particular, commutative, and so it is multiplicative (14.27). \square

LEMMA 17.52. *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*

$$(t, u) \mapsto tu: T \times U \rightarrow G, \quad (131)$$

is an isomorphism

PROOF. Note that $T \cap U = e$ (15.16). Elements $t \in T(R)$ and $u \in U(R)$ commute because $tut^{-1}u^{-1} \in (T \cap U)(R) = e$, and so (131) is a homomorphism. Its kernel is $T \cap U = e$, and its cokernel is a quotient of both G/T and G/U , hence both unipotent and multiplicative, and hence trivial (15.16). \square

LEMMA 17.53. *Let G be a connected nilpotent algebraic group, and let $Z(G)_s$ be the greatest multiplicative subgroup of its centre (17.17). 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 (17.51). Therefore $N \subset Z(G)_s$, and so $Z(G')_s = e$. \square

LEMMA 17.54. *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 $G_{k^{\text{al}}}$ is unipotent (15.9). 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 (17.53), and so is unipotent by induction.

(b) In the exact sequences

$$\begin{aligned} e &\rightarrow Z(N)_s \rightarrow N \rightarrow N/Z(N)_s \rightarrow e \\ e &\rightarrow Z(G) \rightarrow N \rightarrow Z(G')_s \rightarrow e, \end{aligned}$$

the groups $Z(N)_s$ and $Z(G')_s$ are of multiplicative type and $Z(G)$ and $N/Z(N)_s$ are unipotent. Therefore $N \simeq Z(N)_s \times Z(G)$ (17.52), which is commutative. As $Z(N)_s$ is characteristic in N (17.17), it is normal in G , and hence central in G (14.29). 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). \square

THEOREM 17.55. *Let G be a connected nilpotent algebraic group. Then $Z(G)_s$ is the greatest algebraic subgroup of G of multiplicative type; it is characteristic and central, and the quotient $G/Z(G)_s$ is unipotent.*

PROOF. The quotient $G/Z(G)_s$ has unipotent centre (17.53), and so it is unipotent (17.54). Therefore, every multiplicative algebraic subgroup of G maps to e in the quotient $G/Z(G)_s$ (15.18), and so is contained in $Z(G)_s$. Therefore $Z(G)_s$ is the greatest algebraic subgroup of G of multiplicative type. It is obviously central. The same argument as in the proof of (17.17) shows that it is characteristic. \square

COROLLARY 17.56. *Let G be a connected nilpotent algebraic group that becomes trigonalizable over k^{sep} . Then G has a unique decomposition into a product $G = G_u \times G_s$ with G_u unipotent and G_s of multiplicative type.*

PROOF. Because G becomes trigonalizable over k^{sep} , it contains a normal unipotent subgroup G_u such that G/G_u is of multiplicative type (17.5). Therefore the statement follows from (17.52) applied to G_u and $G_s \stackrel{\text{def}}{=} Z(G)_s$. \square

COROLLARY 17.57. *Every smooth connected nilpotent algebraic group over a perfect field k has a unique decomposition into a product of a torus and a connected unipotent group variety.*

PROOF. Such an algebraic group becomes trigonalizable over k^{al} by the Lie-Kolchin theorem, and so we can apply (17.56). \square

ASIDE 17.58. Corollary 17.56 fails for nonsmooth groups, even over algebraically closed fields — see Exercise 17-1.

PROPOSITION 17.59. *Let G be an algebraic group over an algebraically closed field k . The following conditions are equivalent:*

- (a) G is a direct product of a smooth connected unipotent group with a torus;
- (b) G admits a normal series with quotients \mathbb{G}_a or \mathbb{G}_m on which G acts trivially.
- (c) G is smooth and connected, and the abstract group $G(k)$ is nilpotent.

PROOF. To be added (SHS, Exposé 12, 5.3, p.345). \square

NILPOTENT GROUP VARIETIES (CLASSICAL APPROACH)

This subsection will be omitted in the final version.

THEOREM 17.60. *Let G be a connected nilpotent group variety over an algebraically closed field k , and let $Z = Z(G)_{\text{red}}$.*

- (a) Every semisimple element of $G(k)$ is contained in $Z(k)$.
- (b) Let G_s be the greatest algebraic subgroup of Z of multiplicative type (see 17.17). Then G_s is a torus containing every algebraic subgroup of G of multiplicative type, and

$$G = G_u \times G_s.$$

PROOF. We prove (a) by induction on $\dim G$. We may assume that $G \neq e$. Then $Z \neq e$ (because G is nilpotent), and we can apply induction to G/Z .

Let x be a semisimple element of $G(k)$, and let $y \in G(k)$. The image of x in G/Z is semisimple, and so (by induction) $yxy^{-1} = zx$ with $z \in Z(k)$. Note that $z = z_s z_u$ with $z_s, z_u \in Z(G)$ (11.17 et seq.); hence $zx = z_s z_u x_s = (z_s x_s) \cdot z_u$ is the Jordan decomposition of zx . On taking unipotent parts, we find that

$$\begin{aligned} z_u &= (zx)_u \quad (\text{because } x \text{ is semisimple and } z \text{ is central}), \\ &= (yxy^{-1})_u \\ &= e \quad (\text{because } x \text{ is semisimple}). \end{aligned}$$

Therefore z is a semisimple element of $G(k)$. On the other hand, z belongs to the commutator subgroup of G , which is contained in G_u (by the Lie-Kolchin theorem). Therefore $z = e$. As y was arbitrary, this shows that x lies in the centre of $G(k)$.

We now prove (b). By definition, G_s is a subgroup variety of multiplicative type such that $G_s(k) = Z(k)_s = G(k)_s$. On the other hand, G_u is a normal unipotent subgroup variety of G such that $G_u(k) = G(k)_u$ (17.37). Now $G_u \cap G_s = e$ (15.16) and $G = G_u G_s$ (because $G(k) = G_u(k)G_s(k)$). It follows that $G = G_u \rtimes_{\theta} G_s$ (5.35). But $G_s \subset Z(G)$, and so $\theta = 1$: we have $G = G_u \times G_s$. As G is connected, so are G_u and G_s . In particular, G_s is a torus.

Finally, let S be an algebraic subgroup of G of multiplicative type. Because G_u is unipotent (17.37), the image of S under the projection map $G \rightarrow G_u$ is trivial (15.18), and so $S \subset G_s$. \square

g. Split solvable groups

Recall (8.17) 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 . Clearly, a split solvable algebraic group is smooth and connected. Quotients and extensions of split solvable algebraic groups are split solvable.

THEOREM 17.61 (FIXED POINT THEOREM). *Let G be split solvable algebraic group acting on a complete algebraic scheme X . If $X(k) \neq \emptyset$, then $X^G(k) \neq \emptyset$.*

PROOF. Suppose first that $G = \mathbb{G}_a$ or \mathbb{G}_m . Let $x \in X(k)$. If x is not fixed by G , then $\lim_{t \rightarrow 0} t \cdot x$ is a fixed point (Section 14.k). In the general case G has a filtration $G \supset G_1 \supset G_2 \supset \dots \supset G_n \supset 0$ with quotients \mathbb{G}_a or \mathbb{G}_m . Now $X(k) \neq \emptyset \Rightarrow X^{G_n}(k) \neq \emptyset \Rightarrow X^{G_{n-1}}(k) \neq \emptyset \Rightarrow \dots$. \square

PROPOSITION 17.62. *Every split solvable algebraic group is trigonalizable.*

PROOF. Choose a faithful representation of G , and let G act on the algebraic scheme of maximal flag. Then G fixes a flag, and so it is trigonalizable. \square

PROPOSITION 17.63. *Let G be an algebraic group over k . Each of the following conditions implies that G is a split solvable group.*

- (a) k is perfect and G is trigonalizable, smooth, and connected.
- (b) k is algebraically closed and G is solvable, smooth, and connected.

PROOF. (a) This follows from (15.56).

(b) By using the derived series, we can reduce to the case that G is commutative. Then G is a product of a smooth connected diagonalizable algebraic group D with a smooth connected unipotent algebraic group U . Now D is a split torus, and U is split by (a). \square

THEOREM 17.64 (ROSENLICHT). *A reduced solvable algebraic group G is split if and only if there exists a dominant map of schemes $\mathbb{G}_m^N \rightarrow G$ for some integer N .*

PROOF. DG IV, §4, 3.9. □

Concretely, the theorem says that G is split if and only if there exists an injective homomorphism of k -algebras

$$\mathcal{O}(G) \rightarrow k[T_1, \dots, T_N, T_1^{-1}, \dots, T_N^{-1}].$$

h. Complements on unipotent algebraic groups

PROPOSITION 17.65. *Let G be a connected group variety over an algebraically closed field k . If G contains no subgroup isomorphic to \mathbb{G}_m , then it is unipotent.*

PROOF. Let (V, r) be a faithful representation of G , and let F be the variety of maximal flags in V (9.48). Then G acts on F , and there exists a closed orbit, say $O \simeq G/U$. The group U is solvable, and so, by the Lie-Kolchin theorem $U_{\text{red}}^\circ \subset \mathbb{T}_n$ for some choice of basis. Moreover, $U_{\text{red}}^\circ \cap \mathbb{D}_n = e$, because otherwise U_{red}° would contain a copy of \mathbb{G}_m , and so U_{red}° is unipotent. Now G/U_{red}° is affine and connected, and so its image in F is a point. Hence $G = U_{\text{red}}^\circ$. □

COROLLARY 17.66. *Let G be a connected group variety. The following conditions are equivalent:*

- (a) G is unipotent;
- (b) The centre of G is unipotent and $\text{Lie}(G)$ is nilpotent;
- (c) For every representation (V, r) of G , $\text{Lie}(r)$ maps the elements of $\text{Lie}(G)$ to nilpotent endomorphisms of V ;
- (d) Condition (c) holds for one faithful representation (V, r) .

PROOF. (a) \Rightarrow (c). There exists a basis for V such that G maps into \mathbb{U}_n (see 15.3).

(c) \Rightarrow (d). Trivial.

(a) \Rightarrow (b). Every algebraic subgroup, in particular, the centre, of a unipotent algebraic group is unipotent (15.7). Apply Lie to a subnormal series in G whose quotients are isomorphic to subgroups of \mathbb{G}_a (15.23).

(d) \Rightarrow (a). We may assume that k is algebraically closed (15.9). If G contains a subgroup H isomorphic to \mathbb{G}_m , then $V = \bigoplus_{n \in \mathbb{Z}} V_n$ where $h \in H(k)$ acts on V_n as h^n . Then $x \in \text{Lie}(H)$ acts on V_n as nx , which contradicts the hypothesis.

(b) \Rightarrow (a). If the centre of G is unipotent, then the kernel of the adjoint representation is an extension of unipotent algebraic groups (15.25), and so it is unipotent (15.7). Suppose that G contains a subgroup H isomorphic to \mathbb{G}_m . Then H acts faithfully on \mathfrak{g} , and its elements act semisimply, contradicting the nilpotence of \mathfrak{g} . □

i. The canonical filtration on an algebraic group

THEOREM 17.67. *Let G be an algebraic group over a field k .*

- (a) G contains a unique connected normal algebraic subgroup G° such that G/G° is an étale algebraic group.

Now assume that k is perfect.

- (b) G contains a greatest subgroup variety G_{red} (which is connected if G is).
- (c) Let G be a connected group variety; then G contains a unique connected normal solvable subgroup variety N such that G/N is a semisimple algebraic group.
- (d) Let G be a connected solvable group variety; then G contains a unique normal unipotent subgroup N such that G/N is of multiplicative type.

PROOF. (a) See (5.51).

(b) Because k is perfect, G_{red} is a subgroup variety of G (1.25). It is the greatest subgroup variety, because $\mathcal{O}(G_{\text{red}})$ is the greatest reduced quotient of $\mathcal{O}(G)$.

(c) The radical RG of G has these properties. Any other connected normal solvable subgroup variety N of G is contained in RG (by the definition of RG), and if $N \neq RG$ then G/N is not semisimple.

(d) See (17.59). □

j. Summary

A commutative algebraic group G over a field k contains an algebraic subgroup G_s of multiplicative type such that G/G_s is unipotent. If k is perfect, then G also contains a greatest unipotent subgroup G_u , and $G \simeq G_u \times G_s$ (unique decomposition).

An algebraic group G over k is trigonalizable if it satisfies any one of the following equivalent conditions (a) every nonzero representation of G contains an eigenvector; (b) every representation of G is trigonalizable; (c) G can be realized as an algebraic subgroup of \mathbb{T}_n for some n .

An algebraic group G over k becomes trigonalizable over a separable extension of k if and only if it contains a normal unipotent algebraic subgroup G_u such that $D = G/G_u$ is of multiplicative type; then G_u is unique with this property, and contains all unipotent subgroups of G . The extension $e \rightarrow G_u \rightarrow G \rightarrow D \rightarrow e$ splits if k is algebraically closed,

Every smooth connected solvable algebraic group over an algebraically closed field is trigonalizable (Lie-Kolchin).

Let G be a connected nilpotent algebraic group over a field k . Then $Z(G)_s$ is the greatest algebraic subgroup of G of multiplicative type; it is characteristic, and the quotient $G/Z(G)_s$ is unipotent. If k is perfect and G is smooth, then G also contains a greatest unipotent subgroup G_u , and $G \simeq Z(G)_s \times G_u$ (unique decomposition).

Exercises

EXERCISE 17-1. (Waterhouse 1979, 10, Exercise 3, p. 79.) Let k have characteristic 2, and let G be the algebraic subgroup of SL_2 of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a^2 = 1 = d^2$ and $b^2 = 0 = c^2$.

- (a) Show that G is a finite connected algebraic group.
- (b) Show that the sequence

$$e \longrightarrow \mu_2 \xrightarrow{a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}} G \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (ab, cd)} \alpha_2 \times \alpha_2 \longrightarrow e$$

is exact and that $\mu_2 \subset ZG$.

- (c) Show that G is nilpotent, but not commutative; in particular, $G \neq \mu_2 \times (\alpha_2 \times \alpha_2)$.
- (d) Show that the natural action of G on k^2 has no eigenvector. Therefore G is not trigonalizable.

EXERCISE 17-2. Show that an algebraic group G is trigonalizable if and only if there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \cdots$ of $\mathcal{O}(G)$ by subspaces C_i such that

$$\begin{cases} C_0 \text{ is spanned by the group-like elements of } \mathcal{O}(G), \\ \bigcup_{r \geq 0} C_r = \mathcal{O}(G), \\ \Delta(\bar{C}_r) \subset \sum_{0 \leq i \leq r} C_i \otimes C_{r-i}. \end{cases}$$

(Waterhouse 1979, Chapter 10, Exercise 5, p.72).

EXERCISE 17-3. Let G be an algebraic group over a field k , and let k' be a finite field extension of k . Show that $\Pi_{k'/k} G_{k'}$ is solvable if G is solvable. Hint: Use Exercise 2-3 and (8.29) with $k' = k^{\text{al}}$.

Borel subgroups; Cartan subgroups

a. Borel fixed point theorem

Throughout this section, G is a smooth connected solvable algebraic group over the field k .

THEOREM 18.1. *Let H be an algebraic subgroup of G . Then G/H does not contain a complete subscheme of dimension > 0 .*

PROOF. We may suppose that k is algebraically closed, and then that H is smooth because the map $G/H_{\text{red}} \rightarrow G/H$ is finite (9.26). 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 (8.21), distinct from G because G is solvable. If $G = G' \cdot H$, then $G/H \simeq G'/(G' \cap H)$ (5.37), and so the statement follows from the induction hypothesis.

In the contrary case, $G \neq G' \cdot H$ and the image \bar{H} of H in G/G' is a proper normal subgroup. Its inverse image $N = G' \cdot H$ in G is a normal algebraic subgroup of G such that $G/N \simeq (G/G')/\bar{H}$ (5.39). Moreover, N is smooth and connected because it is an extension of such groups (5.52, 10.1).

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 $q: G/H \rightarrow G/N$. Because N is normal, G/N is affine (9.45), and so the image of Z in G/N is a point (A.114). 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 by induction. □

COROLLARY 18.2. *Let H be an algebraic subgroup of G . If G/H is complete, then $H = G$.*

PROOF. The theorem implies that $\dim(G/H) = 0$. □

Let $\mu: G \times X \rightarrow X$ be an action of G on an algebraic scheme X over k , and let $x \in X(k)$. Recall (Section 9.c) that the image of the orbit map $\mu_x: G \rightarrow X, g \mapsto gx$, is locally closed, and that we define the orbit O_x through x to be $\mu_x(G)_{\text{red}}$.

COROLLARY 18.3 (ALLCOCK 2009, THEOREM 2). *No orbit of G acting on a separated algebraic scheme X contains a complete subscheme of dimension > 0 .*

PROOF. Let $x \in X(k)$. Because G is reduced, the orbit map $\mu_x: G \rightarrow X$ factors as

$$G \begin{array}{c} \xrightarrow{\text{faithfully}} \\ \text{flat} \end{array} O_x \xrightarrow{\text{immersion}} X,$$

and O_x is stable under G (9.4c). The pair (O_x, x) is the quotient of G by G_x (9.22), and so we can apply the theorem. \square

COROLLARY 18.4 (BOREL FIXED POINT THEOREM). *Every action of G on a complete algebraic scheme X has a fixed point in $X(k^{\text{al}})$.*

PROOF. We may replace k with its algebraic closure. Every orbit of minimum dimension is closed (9.10), hence complete (A.120(a)), and hence consists of a single fixed point. \square

COROLLARY 18.5. *Let G act on a complete algebraic scheme X ; then the fixed scheme X^G is nonempty.*

PROOF. The formation of X^G commutes with extension of the base field — this is obvious from its definition (9.1) — and $X^G(k^{\text{al}}) \neq \emptyset$ (18.4). \square

The Borel fixed point theorem provides an alternative proof the Lie-Kolchin theorem.

COROLLARY 18.6. *If k is algebraically closed, then G is trigonalizable.*

PROOF. Choose a faithful representation $G \hookrightarrow \text{GL}_V$ of V , and let X denote the collection of maximal flags in V . This has a natural structure of a projective variety (9.48), and G acts on it by a regular map

$$g, F \mapsto gF: G \times X \rightarrow X$$

where

$$g(V_n \supset V_{n-1} \supset \cdots) = gV_n \supset gV_{n-1} \supset \cdots.$$

According to Corollary 18.4, there is a fixed point, i.e., a maximal flag such that $gF = F$ for all $g \in G(k)$. Relative to a basis e_1, \dots, e_n of V adapted to the flag, i.e., such that e_1, \dots, e_i is a basis of V_i for each i , we have $G \subset \mathbb{T}_n$. \square

NOTES

18.7. Those tempted to drop the smoothness condition on G should note that there exists a connected nilpotent (nonreduced) algebraic group acting on \mathbb{P}^1 without fixed points (Exercise 17-1).

18.8. Corollary (18.4) is Borel's original theorem (Borel 1956, 15.5, 16.4), and (18.3) is the correct generalization of it to the case that X is not necessarily complete. Here is Borel's original proof of (18.4): We use induction on the dimension of G , which we may suppose to be nonzero. Because G is solvable, the derived group G' of G is a connected normal subgroup variety G' with $\dim(G') < \dim(G)$ (8.21). By induction, the closed subvariety $X_{\text{red}}^{G'}$ of X is nonempty. Because G' is normal, $X_{\text{red}}^{G'}$ is stable under G . According to (9.10), there exists an $x \in X^{G'}(k)$ whose G -orbit O_x is closed. Let G_x denote the isotropy group at x ; then $G/G_x \simeq O_x$ (9.5, 9.22). Because $G_x \supset G'$, it is normal in G , and so the quotient G/G_x is affine (9.45). It is connected (5.52), and O_x is complete, and so O_x must be a one-point scheme (A.114g).

18.9. Steinberg (1977, Oeuvres p.467) adapted Kolchin's proof of the Lie-Kolchin theorem to give a more elementary proof of the Borel fixed point theorem. In particular, his approach avoids using quotient varieties. See v1.00 of these notes.

b. Borel subgroups

Throughout this section, k is algebraically closed.

DEFINITION 18.10. Let G be a connected group variety over k (algebraically closed). A **Borel subgroup** of G is a maximal connected solvable subgroup variety of G .

For example, every connected solvable subgroup variety of maximum dimension is a Borel subgroup.

EXAMPLE 18.11. Let B be a Borel subgroup in GL_V (V a finite-dimensional k -vector space). Because B is solvable, there exists a basis of V for which $B \subset \mathbb{T}_n$ (17.33), 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 . As $\mathrm{GL}_V(k)$ acts transitively on the set of bases for V , any two Borel subgroups of GL_V are conjugate by an element of $\mathrm{GL}_V(k)$. More canonically, the Borel subgroups of GL_V (and SL_V) are the stabilizers of maximal flags in V .

Let ϕ be a nondegenerate bilinear form on V . The Borel subgroups of $\mathrm{SO}(\phi)$ are the stabilizers of flags that are maximal with respect to the property that ϕ is trivial on each subspace in the flag (they have length $\lfloor \dim(V)/2 \rfloor$). The Borel subgroups of the symplectic group have a similar description. See later.

THEOREM 18.12. Let G be a connected group variety over k (algebraically closed).

- (a) If B is a Borel subgroup of G , then G/B is complete (hence projective 9.39).
- (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. Apply (4.19) to obtain a representation $G \rightarrow \mathrm{GL}_V$ and a one-dimensional subspace L such that B is the algebraic subgroup of G stabilizing L . Then B acts on V/L , and the Lie-Kolchin theorem gives us a maximal flag in V/L stabilized by B . On pulling this back to V , we get a maximal flag,

$$F: V = V_n \supset V_{n-1} \supset \cdots \supset V_1 = L \supset 0$$

in V . Not only does B stabilize F , but (because of our choice of V_1) it is the isotropy group at F , and so $G/B \simeq B \cdot F$ (9.5, 9.43). This shows that, when we let G act on the variety of maximal flags, $G \cdot F$ is the orbit of smallest dimension (the dimension of $G \cdot F$ is the codimension of G_F , which is a solvable subgroup of G). Therefore $G \cdot F$ is a closed (9.5), and hence complete, subvariety of the variety of maximal flags in V . As $G/B \simeq G \cdot F$, G/B is complete (A.114).

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 $g \in G(k)$ (because the maximality of B' will then imply that $B' = gBg^{-1}$). Let B' act on G/B by left multiplication $(b', gB) \mapsto b'gB$. The Borel fixed point theorem shows that there is a fixed point, i.e., for some $g \in G(k)$, $B'gB \subset gB$. Then $B'g \subset gB$, and so $B' \subset gBg^{-1}$ as required. \square

COROLLARY 18.13. Every unipotent group variety G is solvable.

PROOF. Let B be a Borel subgroup of G ; we have to show that $G = B$. According to (4.19), there exists a representation (V, r) of G such that B is the stabilizer of a one-dimensional subspace L in V . As B is unipotent, $L^B \neq 0$ and so $L^B = L$. For a nonzero $x \in L$, the

regular map $g \mapsto gx: G/B \rightarrow V_a$ is an immersion (1.52). As G/B is complete and connected and V_a is affine, the image of the map is a single point (A.114). Hence G/B is a single point, and so $G = B$. (For a more explicit proof of the corollary, see 15.23.) \square

THEOREM 18.14. *Let G be a group variety (not necessarily connected). Any two maximal tori in G are conjugate by an element of $G^\circ(k)$.*

PROOF. Let T and T' be maximal tori. Being connected, they are both contained in G° , and so we may suppose that G is connected. Being smooth, connected, and solvable, they are contained in Borel subgroups, say $T \subset B$, $T' \subset B'$. For some $g \in G(k)$, $gB'g^{-1} = B$ (see 18.12), and so $gT'g^{-1} \subset B$. Now T and $gT'g^{-1}$ are maximal tori in the B , and we can apply the statement for connected solvable group varieties (17.37). \square

COROLLARY 18.15. *Let G be a connected group variety. Let T be a maximal torus in G , and let H be an algebraic subgroup 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*

$$\frac{(N_G(T)(k): N_G(T)(k) \cap H(k))}{(N_G(H)(k): H(k))}.$$

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 $hgTg^{-1}h^{-1} = T$ (18.14). 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 $hgTg^{-1}h^{-1} = T$ ((18.14)), 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

$$\frac{N(T) \cap N(H)}{N(T) \cap H} \rightarrow \frac{N(H)}{H}$$

is a bijection. Therefore

$$(N(T) \cap N(H): N(T) \cap H) = (N(H): H),$$

which completes the proof of the formula. \square

DEFINITION 18.16. Let G be a connected group variety. A pair (B, T) with B a Borel subgroup of G and T a maximal torus of G contained in B is called a **Borel pair**.

Every maximal torus T , being solvable, is contained in a Borel subgroup B . As any two Borel subgroups are conjugate, it follows that every Borel subgroup contains a maximal torus. This shows that every maximal torus and every Borel subgroup is part of a Borel pair (B, T)

PROPOSITION 18.17. *Let G be a connected group variety. Any two Borel pairs are conjugate by an element of $G(k)$.*

PROOF. Let (B, T) and (B', T') be Borel pairs in G . Then $B' = gBg^{-1}$ for some $g \in G(k)$ (18.12). Now T' and gTg^{-1} are both maximal tori in B' , and so $T' = bgTg^{-1}b^{-1}$ for some $b \in B(k)$ (17.37). Hence $(B', T') = bg \cdot (B, T) \cdot (bg)^{-1}$. \square

Recall (17.37) that every connected solvable group variety H (over a perfect field) contains a greatest unipotent algebraic subgroup H_u ; it is a connected normal subgroup variety of H .

PROPOSITION 18.18. *Let G be a connected group variety. 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 (15.23), 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 $(gBg^{-1})_u = gB_u g^{-1}$. \square

DEFINITION 18.19. Let G be a connected group variety. A subgroup variety P of G is **parabolic** if G/P is complete (hence projective 9.39).

EXAMPLE 18.20. Borel subgroups are parabolic (18.12). Let V be a finite-dimensional k -vector space, and let F be a flag in V , not necessarily maximal. The stabilizer P of F in GL_V is a parabolic subgroup of GL_V . For example,

$$P = \left\{ \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & * & * \end{pmatrix} \right\}$$

is a parabolic subgroup of GL_4 .

THEOREM 18.21. *Let G be a connected group variety. A subgroup variety P of G is parabolic if and only if it contains a Borel subgroup.*

PROOF. Suppose that P contains a Borel subgroup B . There is a regular map $G/B \rightarrow G/P$ (9.44). Because G/B is complete and the map is surjective, G/P is complete (A.114d).

Conversely, suppose that G/P is complete, and let B be a Borel subgroup of G . According to (18.5), B fixes a point xP in G/P . In other words, $BxP = xP$, and so P contains the Borel subgroup $x^{-1}Bx$ of G . \square

COROLLARY 18.22. *A connected group variety contains a proper parabolic subgroup if and only if it is not solvable.*

PROOF. If G is not solvable, then every Borel subgroup is a proper parabolic subgroup. If G is solvable, then a proper parabolic subgroup would contradict (18.1). \square

COROLLARY 18.23. *Let G be a connected group variety. The following conditions on a connected subgroup variety H of G are equivalent:*

- (a) H is maximal solvable (hence Borel);
- (b) H is solvable and G/H is complete;
- (c) H is minimal parabolic.

PROOF. (a) \Rightarrow (b). Assume H satisfies (a). Because H is Borel, G/H is complete (18.12), and so H satisfies (b).

(b) \Rightarrow (c). Assume H satisfies (b). Certainly it is parabolic. Let P be a parabolic subgroup of G contained in H . Then P contains a Borel subgroup B of G (18.21) which, being maximal connected solvable, must equal H . Hence $P = H$, and H is minimal.

(c) \Rightarrow (a). Assume H satisfies (c). As H is parabolic, it contains a Borel subgroup B (18.21), which being parabolic, must equal H . \square

PROPOSITION 18.24. *Let $q: G \rightarrow Q$ be a quotient map of connected group varieties, and let H be an algebraic subgroup 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 $G \rightarrow Q/q(H)$ factors through G/H , and so we get a surjective map $G/H \rightarrow Q/q(H)$.

If H is parabolic, then G/H is complete. As $G/H \rightarrow Q/q(H)$ is surjective, this implies that $Q/q(H)$ is complete (A.114d), and so $q(H)$ is parabolic.

If H is a Borel subgroup, then $q(H)$ is connected (5.52), solvable (8.13), and $Q/q(H)$ is complete, and so H is a Borel subgroup (18.23).

If H is a maximal unipotent subgroup variety, then $H = B_u$ for some Borel subgroup B (18.18), and $q(H) = q(B_u) \subset q(B)_u$. Let $g \in q(B)_u(k)$. Then $g = q(b)$ for some $b \in B(k)$. If $b = b_s b_u$ is the Jordan decomposition of b , then $g = q(b_s) \cdot q(b_u)$ is the Jordan decomposition of g (11.20), and so $q(b_s) = e$ and $g = q(b_u) \in q(B_u)$. Hence $q(H) = q(B)_u$, which is a maximal unipotent subgroup variety of G (18.18).

If H is a maximal torus, then H is contained in a Borel subgroup B and $B = B_u \cdot H$ (17.37). 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 (18.12) there exists a $g \in G(k)$ such that

$$B' = q(g)q(B)q(g)^{-1} = q(gBg^{-1}),$$

which 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 $H \stackrel{\text{def}}{=} q^{-1}(H')$ contains B , and so it is parabolic, but $q(H) = H'$. \square

PROPOSITION 18.25. *Let B be a Borel subgroup of a connected group variety G , and let R be a k -algebra. An automorphism of G_R that acts as the identity map on B_R is the identity map.*

PROOF. We prove this first in the case $R = k$. Let α be an automorphism of G such that $\alpha(x) = x$ for all $x \in B(k)$, and consider the regular map

$$\delta: G \rightarrow G, \quad x \mapsto \alpha(x) \cdot x^{-1}.$$

Then δ is constant on each coset of B , and so it defines a regular map $\delta^B: G/B \rightarrow G$ (9.44). As G/B is complete, δ^B is constant (A.114), with value e . This shows that α agrees with the identity map on G .

In proving the general case, we use that, for an algebraic scheme X over k and a k -algebra R ,

$$\mathcal{O}_{X_R}(X_R) \simeq R \otimes \mathcal{O}_X(X).$$

This is obvious if X is affine, and the general case can be proved by covering X with open affines and applying the sheaf condition.

Let α be an automorphism of G_R such that $\alpha|_{B_R} = \text{id}$, and let $\delta: G_R \rightarrow G_R$ be the morphism such that, for every R -algebra R' , $\delta(R'): G(R') \rightarrow G(R')$ sends x to $\alpha(x) \cdot x^{-1}$. Then δ is constant on each coset of B_R , and so it defines a regular map

$$(G/B)_R \simeq G_R/B_R \xrightarrow{\delta^B} G_R.$$

Because G is affine, we can embed it in \mathbb{A}^n for some n . The composite of the maps

$$(G/B)_R \xrightarrow{\delta^B} G_R \longrightarrow \mathbb{A}_R^n \xrightarrow{p_i} \mathbb{A}_R \quad (p_i \text{ the } i\text{th projection}),$$

is an element of $\mathcal{O}_{(G/B)_R}((G/B)_R) \simeq R \otimes \mathcal{O}_{G/B}(G/B)$. Because G/B is complete, $\mathcal{O}_{G/B}(G/B) = k$, and so this map is constant. Hence δ^B is constant, with value e . This shows that α agrees with the identity map on $G(R')$ for all R -algebras R' , and hence on G_R (Yoneda lemma A.28). \square

PROPOSITION 18.26. *Let B be a Borel subgroup of a connected group variety G . Then*

$$Z(G)^\circ \subset Z(B) \subset C_G(B) = Z(G).$$

PROOF. As $Z(G)^\circ$ is connected and commutative, it lies in some Borel subgroup. Because all Borel subgroups are conjugate (18.12), it lies in our particular Borel subgroup B , and hence in $Z(B)$.

The inclusions $Z(B) \subset C_G(B)$ and $Z(G) \subset C_G(B)$ are obvious. Thus, let $g \in C_G(B)(R)$ for some k -algebra R . Then $\text{inn}(g)$ acts as the identity map on B_R , and so it is the identity map on G_R (18.25). Thus $C_G(B)(R) \subset Z(G)(R)$. As this is true for all k -algebras R , $C_G(B) \subset Z(G)$. \square

PROPOSITION 18.27. *Let G be a connected group variety. The following conditions are equivalent:*

- (a) G has only one maximal torus;
- (b) any (one or every) Borel subgroup B of G is nilpotent;
- (c) G is nilpotent (hence $G = B$);
- (d) any (one or every) maximal torus T of G is contained in the centre of G .

PROOF. (a) \Rightarrow (b). Let B be a Borel subgroup of G , and let T be a maximal torus in B . Then T is normal in B , because otherwise some conjugate of it by an element of $B(k)$ would be a second maximal torus in G (1.61). Because T is maximal, the quotient B/T contains no copy of \mathbb{G}_m (16.46), and so it is unipotent (17.65). It follows that $B \simeq T \times U$ with U unipotent (17.31), and both T and U are nilpotent (15.23).

(b) \Rightarrow (c). We use induction on the dimension of B . If $\dim(B) = 0$, then $G = G/B$ is both affine and complete, hence trivial. Thus, we may suppose that $\dim(B) > 0$, and hence that $\dim(Z(B)) > 0$ (8.33). But $Z(B) \subset Z(G)$ (18.26), and so $Z(B)$ is normal in G . The quotient $B/Z(B)$ is a Borel subgroup of $G/Z(B)$ (18.24). By induction $G/Z(B) = B/Z(B)$, and so $G = B$.

(c) \Rightarrow (d). The centre of a connected nilpotent group contains *every* subgroup of multiplicative type (17.55).

(d) \Rightarrow (a). Any two would be conjugate by an element of $G(k)$ (18.14). \square

EXAMPLE 18.28. In particular, a connected solvable group variety is nilpotent if and only if it has exactly one maximal torus. For $n > 1$, the group \mathbb{T}_n is solvable but not nilpotent because its maximal torus of diagonal matrices is not normal:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -a+c \\ 0 & c \end{pmatrix}.$$

COROLLARY 18.29. *Let G be a connected group variety. If all elements of $G(k)$ are semisimple, then G is a torus.*

PROOF. Let (B, T) be a Borel pair in G . Then $B = B_u \cdot T$ (17.37), and the hypothesis implies that $B_u = e$. Hence B is nilpotent, and so $G = B = T$. \square

COROLLARY 18.30. *Let G be a connected group variety.*

(a) *A maximal torus of G is contained in only finitely many Borel subgroups.*

(b) *For a Borel subgroup B of G , $B = N_G(B)^\circ$.*

PROOF. (a) Let T be a maximal torus in G , and let B be Borel subgroup containing T . After (18.15) it suffices to show that

$$(N_G(T)(k): N_G(T)(k) \cap B(k)) < \infty.$$

Recall (16.23) that $N_G(T)$ is smooth and that $N_G(T)^\circ = C_G(T)^\circ$. As $N_G(T)^\circ$ contains a maximal torus T in its centre, it is nilpotent (18.27), and so it lies in some Borel subgroup B' containing T . But $N_G(T)(k)$ acts transitively on the Borel subgroups containing T (18.15), and so $N_G(T)^\circ$ lies in B . Hence

$$(N_G(T)(k): N_G(T)(k) \cap B(k)) \leq (N_G(T)(k): N_G(T)^\circ(k)) < \infty.$$

(b) Let B be a Borel subgroup of G , and let T be a maximal torus of G contained in B . We saw in the proof of (18.15) that $(N_G(B)(k): B(k))$ divides $(N_G(T)(k): N_G(T)(k) \cap B(k))$, and so it is finite. \square

COROLLARY 18.31. *Let G be a connected group variety. If $\dim G \leq 2$, 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 $G = B = e$. If $\dim B = 1$, then we write $B = B_u \cdot T$ with T a maximal torus in G (17.37). Either $B = B_u$ or $B = T$. In each case, B is nilpotent, and so $G = B$. Finally, if $\dim B = 2$, then certainly $G = B$. \square

The bound in (18.31) is sharp — SL_2 is not solvable.

PROPOSITION 18.32. *Let T be a maximal torus in a group variety G , and let $C = C_G(T)^\circ$. Then C is nilpotent, and equals $N_G(C)^\circ$.*

PROOF. Recall (16.23) that C is smooth. The maximal torus T is contained in the centre of C , and so C is nilpotent (18.27).

Now C has a unique decomposition, $C = U \times T$ with U unipotent (17.57). Every automorphism of C preserves the decomposition. In particular, the action of $N_G(C)^\circ$ on C by inner automorphisms preserves T . By rigidity (14.29), the action of $N_G(C)^\circ$ on T is trivial, and so $N_G(C)^\circ \subset C_G(T)$. Hence $C \subset N_G(C)^\circ \subset C_G(T)^\circ \stackrel{\text{def}}{=} C$. \square

COROLLARY 18.33. *Let T be a maximal torus of a connected group variety 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 (18.14), $B = xB'x^{-1}$ for some $x \in N_G(T)$, and so

$$C_G(T)^\circ = C_G(xTx^{-1})^\circ = x(C_G(T)^\circ)x^{-1} \subset B. \quad \square$$

REMARK 18.34. Let I denote the reduced identity component of the intersection of the Borel subgroups of G : $I = \left(\bigcap_{B \subset G \text{ Borel}} B\right)_{\text{red}}^\circ$. By definition, this is a connected subgroup variety of G . It is also solvable and normal (because Borel subgroups are solvable, and the set 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 (21.32), and so it is contained in I . Therefore I is the greatest connected solvable normal subgroup variety of G , i.e.,

$$RG = \left(\bigcap_{B \subset G \text{ Borel}} B\right)_{\text{red}}^\circ.$$

This is sometimes adopted as the definition of RG (e.g., in SHS, Vortrag 15, p.386).

c. The density theorem

Throughout this section, k is algebraically closed. Recall that we often write G for $|G|$ (underlying topological space of G) and that, because k is algebraically closed, we can identify $|G|$ with $G(k)$.

LEMMA 18.35. *Let G be a connected group variety, and let H be a connected subgroup variety of G .*

- (a) *If G/H is complete, then $\bigcup_{g \in G(k)} gHg^{-1}$ is a closed subset of G .*
- (b) *If there exists an element of $H(k)$ fixing only finitely many elements of $|G/H|$, then $\bigcup_{g \in G(k)} gHg^{-1}$ contains a nonempty open subset of G .*

PROOF. Consider the composite of the maps

$$\begin{array}{ccc} G \times G & \xrightarrow{\tau} & G \times G & \xrightarrow{q \times \text{id}} & G/H \times G \\ (x, y) & \mapsto & (x, xyx^{-1}) & & \end{array}$$

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 (9.20), 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 (1.27).

(a) Now assume that G/H is complete. Then (by definition) the projection map $G/H \times G \rightarrow G$ is closed. In particular, the image of S under this map is closed, but the image is exactly $\bigcup_{g \in G(k)} gHg^{-1}$.

(b) Now suppose that there exists an $h \in H(k)$ whose set of fixed points in $|G/H|$ is finite. This means that the pre-image of h in S with respect to the projection from S to G is finite. This implies that the dimension of S is the same as the dimension of the closure of its image in G (A.99), and so the regular map $S \rightarrow G$ is dominant, which implies the second statement (A.68). □

PROPOSITION 18.36. *Let G be a connected group variety, and let T be a torus in G . There exists a $t \in T(k)$ such that every element of $G(k)$ that commutes with t belongs to $C_G(T)(k)$ (i.e., the centralizer of T in G is equal to the centralizer of t).*

PROOF. Choose a finite-dimensional faithful representation (V, r) of G , and write V as a sum of eigenspaces $V = \bigoplus V_{\chi_i}$ of T (14.12). For each pair (i, j) with $i \neq j$, let $T_{ij} = \{t \in T(k) \mid \chi_i(t) = \chi_j(t)\}$. Then T_{ij} is a proper closed subset of $T(k)$, and so there exists a $t \in T(k) \setminus \bigcup_{i \neq j} T_{ij}$. If an element x of $G(k)$ commutes with t , then it stabilizes each V_{χ_i} , and so it commutes with T . \square

THEOREM 18.37. *Let G be a connected group variety.*

- (a) *Let T be a maximal torus in G , and let $C = C_G(T)^\circ$. Then $\bigcup_{g \in G(k)} gCg^{-1}$ contains a nonempty open subset of G .*
- (b) *Let B be a Borel subgroup of G . Then $G = \bigcup_{g \in G(k)} gBg^{-1}$.*

PROOF. (a) As C is nilpotent (18.32) and T is a maximal torus in C , we have $C = C_u \times C_s$ with $C_s = T$ (see 17.60). Let $t \in T(k)$ be as in (18.36). We shall show that t fixes only finitely many elements of G/C , and so (a) follows from (18.35).

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 (16.23), we know that $N_G(C)^\circ = C$. Therefore $xC \mapsto xN_G(C)^\circ$ is an injection from the fixed point set for 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 $C \subset B$ (18.33), 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 (18.35), and so it equals G . \square

COROLLARY 18.38. *Let B be a Borel subgroup of G . Then*

$$B = N_G(B)_{\text{red}}^\circ.$$

PROOF. Clearly, B is a Borel subgroup of $N_G(B)_{\text{red}}^\circ$. As it is normal in $N_G(B)_{\text{red}}^\circ$, (b) of the theorem shows that it equals $N_G(B)_{\text{red}}^\circ$. \square

COROLLARY 18.39. *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 $B' \subset N_G(B)_{\text{red}}^\circ = B$, and so $B' = B$. \square

d. Centralizers of tori are connected

In this section we prove that the centralizer of a torus in a connected group variety is connected (hence smooth and connected, 16.23). Since it suffices to prove this after an extension of the base field, we suppose throughout that k is algebraically closed.

In the final version, Lemma 18.42 will be deduced more simply from Theorem 17.43 and Proposition 18.36.

LEMMA 18.40. *Let G be a connected group variety, and let U be a commutative connected unipotent subgroup variety of G . Let s be a semisimple element of G that normalizes U . Then the centralizer of s in U is connected.*

PROOF. Let S be the closure of the subgroup of $G(k)$ generated by s . As s is semisimple, the algebraic group S is diagonalizable (14.26), and hence its centralizer $U^S = U^s$ in U is smooth (16.21).

Let $U_s(k)$ be the subgroup of $U(k)$ consisting of the elements $[s, u] \stackrel{\text{def}}{=} sus^{-1}u^{-1}$ with $u \in U(k)$. We claim that $U^s(k) \cap U_s(k) = \{e\}$. To see this, let $u \in U(k)$ be such that $[s, u]$ lies in the intersection, say, $[s, u] = v \in U^s(k)$. Then $sus^{-1} = vu$, and so $s^m u s^{-m} = v^m u$ for all $m \in \mathbb{Z}$. Therefore $[s^m, u] \in U^s(k)$ for all $m \in \mathbb{Z}$. Consider the map

$$x \mapsto [x, u]: S \rightarrow U^s.$$

It is a homomorphism of group varieties. As S is diagonalizable and U^s is unipotent, it is trivial (15.18). In particular, $[s, u] = e$, and so $U^s(k) \cap U_s(k) = \{e\}$.

Now consider the map

$$u \mapsto [s, u]: U \rightarrow U_s.$$

This is a surjective homomorphism of group varieties, and so U_s is connected. Its kernel is U^s , and so (5.19)

$$\dim(U) = \dim(U^s) + \dim(U_s). \quad (132)$$

The homomorphism

$$(u, v) \mapsto uv: U^s \times U_s \rightarrow U$$

has kernel $U^s \cap U_s$, which is finite, and so

$$\dim((U^s)^\circ \cdot U_s) = \dim((U^s)^\circ \times U_s) \stackrel{(132)}{=} \dim(U).$$

It follows that

$$(U^s)^\circ \times U_s \rightarrow U$$

is a surjective homomorphism of group varieties, and so

$$(U^s)^\circ(k) \cdot U_s(k) = U(k).$$

Let $u \in U^s(k)$. Then $u = u^s \cdot u_s$ with $u^s \in (U^s)^\circ(k)$ and $u_s \in U_s(k)$. But $u_s \in U^s(k) \cap U_s(k) = \{e\}$, and so $u \in (U^s)^\circ(k)$. Hence $U^s(k) = (U^s)^\circ(k)$, i.e., $|U^s| = |(U^s)^\circ|$, and so U^s is connected. \square

LEMMA 18.41. *Let S be a torus acting on a connected unipotent group variety U . The centralizer U^S of S in U is connected.*

PROOF. Let $G = U \rtimes S$ and let $s \in S$ generate a dense subgroup of S (see 18.36). Then $U^S = U^s$, and so (18.40) proves the statement when U is commutative.

We prove the general statement by induction on the dimension of U . Because U is unipotent, it is nilpotent (15.23), and so it contains a nontrivial connected subgroup variety Z in its centre (8.33). By induction, $(U/Z)^s$ is connected. Consider the exact sequence

$$1 \rightarrow Z^s \rightarrow U^s \rightarrow (U/Z)^s.$$

We shall show that the last map is surjective. As Z^s and $(U/Z)^s$ are connected, this will show that U^s is connected (5.52).

Let $u \in U(k)$ be such that $uZ \in (U/Z)^s(k)$. Then $sus^{-1}u^{-1} \in Z(k)$. As s is dense in S , this implies that $xux^{-1}u^{-1} \in Z(k)$ for every $x \in S(k)$. The regular map

$$\delta: S \rightarrow Z, \quad x \mapsto xux^{-1}u^{-1},$$

is a crossed homomorphism, and so it is a coboundary (16.3), i.e., there exists a $z \in Z(k)$ such that

$$xux^{-1}u^{-1} = xzx^{-1}z^{-1}$$

for all $x \in S$. Now $z^{-1}u \in U^s(k)$. □

LEMMA 18.42. *Let S be a torus in a connected solvable group variety G . Then $C_G(S)$ is connected.*

PROOF. Let T be a maximal torus in G containing S . Then $G = G_u \rtimes T$ with G_u unipotent (17.37), and so

$$C_G(S) = G_u^S \rtimes T.$$

By Lemma 18.41, G_u^S is connected, and so $C_G(S)$ is connected. □

LEMMA 18.43. *Let T be a torus in a connected group variety G . Then*

$$C_G(T) \subset \bigcup_{T \subset B} B$$

(union over the Borel subgroups of G containing T).

PROOF. Let $c \in C_G(T)(k)$, and let B be a Borel subgroup of G . Let

$$X = \{gB \in G/B \mid cgB = gB\} = (G/B)^c.$$

As c is contained in a connected solvable subgroup of G (18.37), the Borel fixed point theorem (18.5) shows that X 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 X , and the Borel fixed point theorem shows that it has a fixed point in X . This means that there exists a $g \in G$ such that

$$\begin{aligned} cgB &= gB && \text{(hence } cg \in gB) \\ TgB &= gB && \text{(hence } Tg \subset gB). \end{aligned}$$

Thus, both c and T lie in gBg^{-1} , as required. □

THEOREM 18.44. *Let T be a torus in a connected group variety G . Then $C_G(T)$ is connected.*

PROOF. From (18.43) we know that

$$C_G(T) = \bigcup_{T \subset B} C_B(T).$$

As each $C_B(T)$ is connected, and $\bigcap C_B(T) \neq \emptyset$, this implies that $C_G(T)$ is connected. □

COROLLARY 18.45. *Let T be a maximal torus in G . Then $C_G(T)$ is contained in every Borel subgroup containing T .*

PROOF. If $T \subset B$, then $C_G(T)^\circ \subset B$ by (18.33). But $C_G(T) = C_G(T)^\circ$. □

ASIDE 18.46. Theorem 18.44 is true for tori in algebraic groups (not necessarily smooth). For an argument deducing this from the smooth case, see SHS Exposé 13, §4, p.358.

DEFINITION 18.47. Let G be a connected group variety. A **Cartan subgroup** in G is the centralizer of a maximal torus.

PROPOSITION 18.48. *Let G be a group variety. Every Cartan subgroup in G is smooth, connected, and nilpotent; any two are conjugate by an element of $G(k)$; the union of the Cartan subgroups of G contains a dense open subset of G .*

PROOF. Let $C = C_G(T)$ be a Cartan subgroup. Then C is smooth (16.23), connected (18.44), and nilpotent (18.32).

Let C and C' be Cartan subgroups, say, $C = C_G(T)$ and $C' = C_G(T')$ with T and T' maximal tori. Then $T' = gTg^{-1}$ for some $g \in G(k)$ (18.14), and so

$$C' = C_G(gTg^{-1}) = g \cdot C_G(T) \cdot g^{-1} = g \cdot C \cdot g^{-1}.$$

Let C be a Cartan subgroup of G . Every conjugate of C is a Cartan subgroup of G , and we know (18.37) that $\bigcup_{g \in G(k)} gCg^{-1}$ contains a nonempty open subset of G . \square

COROLLARY 18.49. *Let $C = C_G(T)$ be a Cartan subgroup. Then $C = C_u \times T$ with C_u unipotent.*

PROOF. As C is nilpotent, we can apply (17.56). \square

PROPOSITION 18.50. *Let G be a connected group variety, and let B be a Borel subgroup of G . Then $Z(G) = Z(B)$.*

PROOF. As $Z(G) = C_G(B)$ (18.26) and $Z(B) = C_G(B) \cap B$, it suffices to show that $Z(G) \subset B$. Let T be a maximal torus in G . Then $Z(G) \subset C_G(T)$. As $C_G(T)$ is connected nilpotent subgroup variety of G (18.48), it is contained in some Borel subgroup B' . Now $B = gB'g^{-1}$ for some $g \in G(k)$, and $gB'g^{-1} \supset gZ(G)g^{-1} = Z(G)$. \square

APPLICATIONS

THEOREM 18.51. *Let G be a connected group variety. Let S be a torus in G , and let B be a Borel subgroup containing S . Then $C_G(S) \cap B$ is a Borel subgroup of $C_G(S)$, and every Borel subgroup of $C_G(S)$ is of this form.*

PROOF. Let $C = C_G(S)$, and let $\pi: G \rightarrow G/B$ be the quotient map. To show that $C \cap B$ is a Borel subgroup of C , it suffices to show that $\pi(C)$ is closed, hence complete, because $C/C \cap B \simeq \pi(C)$ and we can apply (18.23).

As π is open, it suffices to show that CB is closed (meaning, that the set $|C||B|$ is closed in $|G|$). Let \overline{CB} be the closure of CB in G — it has the structure of a group subvariety of G (see 1.31). Note that \overline{CB} is connected because CB is the image of $C \times B$ under the multiplication map.

For $y = cb \in CB$ with $c \in C$ and $b \in B$, we have

$$y^{-1}Sy = b^{-1}c^{-1}Scb = b^{-1}Sb \subset B$$

because $S \subset B$. Therefore,

$$y \in \overline{CB} \implies y^{-1}Sy \subset B.$$

Let $\varphi: B \rightarrow B/B_u$ denote the quotient map, and consider the regular map

$$\psi: \overline{CB} \times S \rightarrow B/B_u, \quad (y, s) \mapsto \varphi(y^{-1}sy).$$

As \overline{CB} is a connected (affine) group variety and S and B/B_u are of multiplicative type, the rigidity theorem (14.29) shows that $\varphi(y^{-1}sy)$ is independent of y , i.e., $\varphi(y^{-1}sy) = \varphi(s)$ for all y and s .

Let T be a maximal torus of B containing S . The map φ induces an isomorphism from T onto B/B_u . Let $y \in \overline{CB}$. Then $y^{-1}Sy$ is a torus in B , and so there exists a $u \in B_u$ such that $u^{-1}y^{-1}Sy u \subset T$ (17.37). As $CB \cdot B \subset CB$, we have $\overline{CB} \cdot B \subset \overline{CB}$ by continuity. Therefore $yu \in \overline{CB}$, and so

$$\varphi(u^{-1}y^{-1}syu) = \varphi((yu)^{-1}s(yu)) = \varphi(s)$$

for all $s \in S$. But $u^{-1}y^{-1}syu$ and s both lie in T and φ is injective on T , and so

$$u^{-1}y^{-1}syu = s.$$

As this holds for all $s \in S$, the element $yu \in C$, 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 $B_0 = c(B \cap C)c^{-1}$. But $c(B \cap C)c^{-1} = cBc^{-1} \cap cCc^{-1} = cBc^{-1} \cap C$, which prove the statement. \square

e. The normalizer of a Borel subgroup

Throughout this section, k is algebraically closed.

LEMMA 18.52. *Let H be a subgroup variety of a group variety G . If H contains a Cartan subgroup of G , then $N_G(H)^\circ = H^\circ$ (and so $N_G(H)$ is smooth).*

PROOF. Let $N = N_G(H)$. As $N \supset H$, it suffices to show that $\dim N = \dim H$. Now

$$\dim \mathfrak{h} = \dim H \leq \dim N \leq \dim \mathfrak{n},$$

and so it suffices to show that $\mathfrak{n} = \mathfrak{h}$.

Assume that H contains the Cartan subgroup $C = C_G(T)$. Recall (12.31) that $\mathfrak{c} = \mathfrak{g}^T$ and $\mathfrak{n}/\mathfrak{h} = (\mathfrak{g}/\mathfrak{h})^H$. Because $H \supset C$, its Lie algebra $\mathfrak{h} \supset \mathfrak{c} = \mathfrak{g}^T$, and so there is an exact sequence

$$0 \rightarrow \mathfrak{h}/\mathfrak{g}^T \rightarrow \mathfrak{g}/\mathfrak{g}^T \rightarrow \mathfrak{g}/\mathfrak{h} \rightarrow 0.$$

Because T is diagonalizable, its representations are semisimple (14.12), and so $(\mathfrak{g}/\mathfrak{g}^T)^T \rightarrow (\mathfrak{g}/\mathfrak{h})^T$ 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 $\mathfrak{n} = \mathfrak{h}$. \square

THEOREM 18.53. *Let B be a Borel subgroup of a connected group variety G . Then*

$$B = N_G(B).$$

PROOF. Every Borel subgroup contains a maximal torus (p.316), hence the centralizer of such a torus (18.45), and so (18.52) shows that $N_G(B)$ is smooth. Therefore it suffices to show that $N_G(B)(k) \subset B(k)$. We prove this by induction on $\dim(G)$. If G is solvable, for example, if $\dim(G) \leq 2$ (18.31), then $B = G$, and the statement is obvious.

Let $x \in N_G(B)(k)$. 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 of $B(k)$ (18.12); thus we may suppose that $T = xTx^{-1}$. Consider the homomorphism

$$\varphi: T \rightarrow T, \quad t \mapsto [x, t] = xtx^{-1}t^{-1}.$$

If $\varphi(T) \neq T$, then $S \stackrel{\text{def}}{=} \text{Ker}(\varphi)^\circ$ is a nontrivial torus. Moreover, x lies in $C \stackrel{\text{def}}{=} C_G(S)$, and normalizes $C \cap B$, which is a Borel subgroup of C (18.51). If $C \neq G$, then $x \in B(k)$ by induction. If $C = G$, then $S \subset Z(G)$, and we can apply the induction hypothesis to G/S to deduce that $x \in B(k)$.

It remains to consider the case $\varphi(T) = T$. According to (4.19), there exists a representation $r: G \rightarrow \text{GL}_V$ such that $N_G(B)$ is the stabilizer of one-dimensional subspace $L = \langle v \rangle$ in V . Then B_u fixes v because B_u is unipotent, and T fixes v because $T \subset \mathcal{D}G$. Therefore $B = B_u \cdot T$ fixes v , and the map

$$g \mapsto r(g) \cdot v: G \rightarrow V$$

factors through G/B . Because G/B is complete, this implies that the map has image $\{v\}$, and so G fixes v . Hence $G = N_G(B)$, and so B is normal in G . Hence $B = G$ (18.37), and the statement is obvious. \square

COROLLARY 18.54. *Every subgroup variety P of G containing a Borel subgroup is connected, and $P = N_G(P)$.*

PROOF. As P contains a Borel subgroup of G , it contains a Cartan subgroup (18.45), and so $N_G(P)$ is smooth (18.52). 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

$$xBx^{-1} = p(xBx^{-1})p^{-1} = (px)B(px)^{-1}$$

(18.14). As px normalizes B , it lies in $B(k)$ (18.53), and so

$$x = p^{-1} \cdot px \in P^\circ(k) \cdot B(k) = P^\circ(k),$$

as required. \square

REMARK 18.55. It follows from the corollary that the Borel subgroups of G are maximal among the solvable subgroup varieties (not necessarily connected) of G . However, not every maximal solvable subgroup variety of a connected algebraic group G is Borel. 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 $\neq 2$). It is a product of copies of $(\mathbb{Z}/2\mathbb{Z})_k$, and equals its own centralizer. If it were contained in a Borel subgroup of G , it would be contained in a torus (17.37), which would centralize it.

COROLLARY 18.56. *For every Borel subgroup B of G , $B = N_G(B_u)$.*

PROOF. Let $P = N_G(B_u)$. As P contains B , it is connected. From the conjugacy of Borel subgroups, it follows that B_u is maximal in the family of connected unipotent subgroups of G . Hence P/B_u has no non-trivial connected unipotent subgroups. Therefore, if C is a Borel subgroup of P/B_u , then C is a torus, in particular nilpotent, and so $P/B_u = C$ (18.27). As P/B_u is commutative, P is solvable, and so $P = B$. \square

Let B be a Borel subgroup of G , and let \mathcal{B} be the set of all Borel subgroups of G . We define a map

$$\gamma: (G/B)(k) \rightarrow \mathcal{B}, \quad xB \mapsto xBx^{-1}.$$

By (18.12) and (18.53), γ is bijective. Let L be a subset of $G(k)$, and let $(G/B)^L$ be the fixed point set for L . Then γ maps $(G/B)^L$ bijectively onto the set $\mathcal{B}(L)$ of Borel subgroups of G containing L .

COROLLARY 18.57. *Let T be a maximal torus in G , and let B be a Borel subgroup of G containing T . Then $N_G(T)$ acts transitively $(G/B)^T$.*

PROOF. Clearly, $(G/B)^T$ is stable under the action of $N_G(T)$. By the above, to say that $N_G(T)$ acts transitively on $(G/B)^T$ is equivalent to saying that $N_G(T)$ acts transitively on $\mathcal{B}(T)$ by conjugation. Let $X, Y \in \mathcal{B}(T)$. There exists a $g \in G$ such that $gXg^{-1} = Y$. Now T and gTg^{-1} are maximal tori in Y . Therefore, there exists a $y \in Y$ such that $yg \in N_G(T)$. Since $(yg)X(yg)^{-1} = Y$, this proves the transitivity. \square

It follows that the action of $N_G(T)$ on $(G/B)^T$ factors through the finite group

$$N_G(T)/N_G(T)^\circ = N_G(T)/C_G(T).$$

In particular, $\mathcal{B}(T)$ is finite. Finally, suppose that x is an element of $N_G(T)$ such that $xBx^{-1} = B$. Then $x \in B$ by (18.53). Thus $x \in N_B(T)$. Hence, for every $t \in T$, we have

$$xtx^{-1}t^{-1} \in T \cap [B, B] \subset T \cap B_u = \{e\},$$

so that $x \in C_G(T)$.

DEFINITION 18.58. Let T be a maximal torus in G . The **Weyl group** of G with respect to T is

$$W(G, T) = N_G(T)/C_G(T).$$

Since all maximal tori are conjugate, the isomorphism class of the Weyl group is determined by G . We have proved the following statement:

COROLLARY 18.59. *Let T be a maximal torus in G . The Weyl group acts simply transitively on the finite set of Borel subgroups of G containing T .*

COROLLARY 18.60. *The map sending $x \in (G/B)(k)$ to its isotropy group G_x is a bijection from $(G/B)(k)$ onto the set of Borel subgroups of G .*

PROOF. Immediate from the above. \square

COROLLARY 18.61. *$B(k)$ is a maximal solvable subgroup of $G(k)$.*

f. Borel and parabolic subgroups over an arbitrary base field

Throughout this section, G is a connected group variety over an arbitrary base field k .

DEFINITION 18.62. A **Borel subgroup** of G is a connected solvable subgroup variety B of G such that G/B is complete.

According to (18.23), this agrees with the earlier definition (18.10) when k is algebraically closed. Let k' be a field containing k ; then an algebraic subgroup B of G is a Borel subgroup if and only if $B_{k'}$ is a Borel subgroup of $G_{k'}$ (1.14, 8.29). Thus the Borel subgroups of G are exactly those that become Borel subgroups in the sense of (18.10) over the algebraic closure of k .

A connected group variety need not contain a Borel subgroup (see 18.55). A reductive group that does is said to be *quasi-split*.

If B is a Borel subgroup of G , then $N_G(B) = B$ — this follows from (18.53) because the formation of normalizers commutes with extension of the base field. Similarly

$$Z(G)^\circ \subset Z(B) \subset C_G(B) = Z(G)$$

follows from (18.26).

Connected group varieties of dimension at most 2 are all solvable (18.31).

DEFINITION 18.63. A **parabolic subgroup** of G is a subgroup variety such that G/P is complete.

Let k' be a field containing k ; then an algebraic subgroup P of G is parabolic if and only if $P_{k'}$ is parabolic in $G_{k'}$. Every parabolic subgroup P of G is connected, and $P = N_G(P)$ (18.54).

A parabolic subgroup of G need not contain a Borel subgroup. For smooth algebraic groups without Borel subgroups, the minimal parabolic subgroups play a role similar to that of Borel subgroups in the quasi-split case.

g. Maximal tori and Cartan subgroups over an arbitrary base field

Throughout this section, G is a connected group variety over an arbitrary base field k .

PROPOSITION 18.64. Let S be a torus in G . Then $C_G(S)$ is a smooth connected algebraic subgroup of G .

PROOF. As the formation of centralizers commutes with extension of the base field, this follows from (16.23) and (18.42). \square

THEOREM 18.65. There exists a torus T in G such that $T_{k^{\text{al}}}$ is maximal in $G_{k^{\text{al}}}$.

PROOF. For nilpotent G , this follows from (17.55). The general case is deduced by an induction argument. To be included in the final version. See Springer 1998, 13.3.6. \square

PROPOSITION 18.66. Let T be a torus in G , and let k' be a field containing k ; then T is maximal in G if and only if $T_{k'}$ is maximal in $G_{k'}$.

PROOF. Clearly a torus in G is maximal if and only if it is maximal in its centralizer, and so (18.64) allows us to replace G with $C_G(T)$ and assume that T is central (hence normal) in G .

If T is maximal and central in G , then G/T contains no nontrivial torus (16.46), and so $(G/T)_{k^{\text{al}}}$ contains no nontrivial torus (18.65). Hence $(G/T)_{k^{\text{al}}}$ is unipotent (17.65), which implies that G/T is unipotent (15.9), and it follows that $(G/T)_{k'}$ is unipotent. As $(G/T)_{k'} \simeq G_{k'}/T_{k'}$, the latter contains no nontrivial torus (15.16), and so $T_{k'}$ is maximal.

The converse is trivial. \square

Let T be a torus in G . Then T is maximal in G if and only if it is maximal in $G_{k^{\text{al}}}$.

THEOREM 18.67. *If k is separably closed, then any two maximal tori in G are conjugate by an element of $G(k)$.*

PROOF. Let T and T' be maximal tori in G , and consider the functor

$$X: R \rightsquigarrow \{g \in G(R) \mid gT_Rg^{-1} = T'_R\}.$$

When we let G act on itself by inner automorphisms, X is the transporter of T into T' , and so it is represented by a closed subscheme of G (1.58). According to (18.14), there exists a $g \in X(k^{\text{al}})$. Then $X = g \cdot N_G(T)$ (inside G), and so X is smooth and nonempty; as k is separably closed, $X(k) \neq \emptyset$ (A.61). \square

Even when k is not separably closed, any two *split* maximal tori are conjugate.

THEOREM 18.68. *Any two split maximal tori in G are conjugate by an element of $G(k)$.*

PROOF. It is possible to deduce this from (18.67). See [Borel and Tits 1965](#), 4.21, 11.6; [Conrad et al. 2010](#), Appendix C, 2.3, p. 506. The proof will be included in the final version (probably in a later chapter). \square

In general, the maximal tori in G fall into many conjugacy classes.

EXAMPLE 18.69. The torus \mathbb{D}_n is maximal in GL_n because $\mathbb{D}_n(k^{\text{sep}})$ is its own centralizer in $\text{GL}_n(k^{\text{sep}})$. In fact, 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 all the matrices $I + E_{ii}$.

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 (see below). The (unique) conjugacy class of split maximal tori corresponds to the étale k -algebra $k \times \cdots \times k$ (n -copies).

Let V be a vector space of dimension n . 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.

Let $A = \prod_i k_i$ be an étale k -algebra of degree n over k . Let $V = \bigoplus_i V_i$ with V_i a one-dimensional k_i -vector space. Then V has dimension n , and GL_V contains a maximal torus with $T(k) = A^\times = \prod_i k_i^\times$. On the other hand, let T be a maximal torus in GL_V . As a T -module, V decomposes into a direct sum of simple T -modules, $V = \bigoplus_i V_i$. The endomorphism ring of V_i (as a T -module) is a field k_i such that $\dim_{k_i} V_i = 1$, and GL_V contains a maximal torus T with $T(k) = \prod_i k_i^\times$.

DEFINITION 18.70. A *Cartan subgroup* of G is the centralizer of some maximal torus.

Thus, every Cartan subgroup is a nilpotent connected subgroup variety of G (18.64, 18.32).

THEOREM 18.71. *Let G be connected group variety over k . If k is infinite, then G is generated by the Cartan subgroups of its maximal tori.*

PROOF. See Springer 1998, 13.3.6. The proof will be included in the final version. \square

COROLLARY 18.72. *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 (and $G(k)$ is dense in G).*

PROOF. The hypothesis implies that there exists a surjective morphism $C_1 \times \cdots \times C_m \rightarrow G$ with the C_i unirational, and so G is unirational. \square

ASIDE 18.73. Let k be an algebraically closed field, and let F be a subfield. Let G be a linear algebraic group over F in the classical sense (e.g., Springer 1998, 2.1), and let G' be the corresponding group variety over F in our sense. A Borel subgroup of G in the classical sense is a Borel subgroup of G'_k .

Exercises

EXERCISE 18-1. Let $G = B \rtimes T$ be a solvable group with T a split torus, and write $\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$ with R a set of nonzero characters of T . Assume that $\mathfrak{g}_0 = \mathfrak{t}$ and that each \mathfrak{g}_α has dimension 1. Show that a homomorphism $G \rightarrow G$ must be the identity map if it acts as the identity map on T and on R .

The variety of Borel subgroups

Throughout this chapter, k is algebraically closed.

a. The variety of Borel subgroups

Throughout this section, G is a connected group variety. Let \mathcal{B} denote the set of Borel subgroups in G . Then G acts transitively on \mathcal{B} by conjugation,

$$(g, B) \mapsto gBg^{-1}: G \times \mathcal{B} \rightarrow \mathcal{B} \tag{133}$$

(see 18.12).

Let B be a Borel subgroup of G . As $B = N_G(B)$ (18.51), the orbit map $g \mapsto gBg^{-1}$ induces a bijection

$$\phi_B: G/B \rightarrow \mathcal{B}.$$

We endow the set \mathcal{B} with the structure of an algebraic variety for which ϕ_B is an isomorphism. Then the action (133) 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 $G \xrightarrow{\text{inn}(g)} G \rightarrow G/B'$ factors through G/B , and gives a commutative diagram

$$\begin{array}{ccc} G/B & \xrightarrow{\text{inn}(g)} & G/B' \\ \downarrow \phi_B & & \downarrow \phi_{B'} \\ \mathcal{B} & \xrightarrow{g \cdot} & \mathcal{B}, \end{array}$$

in which 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} , equipped with its G -action, is called the **flag variety** of G .

LEMMA 19.1. *Let S be a subset of $G(k)$, and let $\mathcal{B}^S = \{B \in \mathcal{B} \mid s \cdot B = B \text{ for all } s \in S\}$. 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 $s \cdot B = B \iff s \in N_G(B) \stackrel{18.53}{=} B$, from which the second part of the statement follows. \square

For example, if T is a torus in G , then \mathcal{B}^T consists of the Borel subgroups of G containing T .

Recall (18.58) that the Weyl group of G with respect to a maximal torus T is $W(G, T) = N_G(T)/C_G(T)$. By rigidity, $N_G(T)$ acts on T through the finite quotient $\pi_0(N_G(T))$, and as $C_G(T)$ is connected, it equals $N_G(T)^\circ$, and so $W(G, T) = \pi_0(N_G(T))$.

PROPOSITION 19.2. *Let T be a maximal torus in G . Then $W(G, T)$ acts simply transitively on \mathcal{B}^T . Hence \mathcal{B}^T is finite.*

PROOF. See 18.59. □

Thus, for any $B \in \mathcal{B}^T$, the orbit map $n \mapsto n \cdot B: W(G, T) \rightarrow \mathcal{B}^T$ is bijective.

PROPOSITION 19.3. *Let $\phi: G \rightarrow G'$ be a surjective homomorphism 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 $\text{Ker}(\phi)$ 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 $W(\phi): W(G, T) \rightarrow W(G', T')$. If $\text{Ker}(\phi)$ 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 (18.24). The regularity of $\phi_{\mathcal{B}}$ follows from the definition of the algebraic structure on the flag varieties. If $\text{Ker}(\phi)$ 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 (18.24) 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 $n \mapsto \phi(n)$ induces a homomorphism $W(G, T) \rightarrow W(G', T')$.

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

$$\begin{array}{ccc} W(G, T) & \xrightarrow{W(\phi)} & W(G', T') \\ 1:1 \downarrow n \mapsto n \cdot B & & 1:1 \downarrow n \mapsto n \cdot \phi(B) \\ \mathcal{B}^T & \xrightarrow{\phi_{\mathcal{B}}} & \mathcal{B}'^{T'} \end{array}$$

Therefore $W(\phi): W(G, T) \rightarrow W(G', T')$ is surjective (resp. bijective) if and only if $\phi_{\mathcal{B}}: \mathcal{B}^T \rightarrow \mathcal{B}'^{T'}$ 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 $\text{Ker}(\phi)$ is contained in Borel subgroup, then $\phi_{\mathcal{B}}: \mathcal{B} \rightarrow \mathcal{B}'$ is injective, which implies that its restriction to $\mathcal{B}^T \rightarrow \mathcal{B}'^{T'}$ is injective. □

NOTES

19.4. In the course of proving (19.3), we showed that, if P is a parabolic subgroup of G and B a Borel subgroup of P , then B is also a Borel subgroup of G .

19.5. 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 a Borel subgroup of G (18.23). The map $x \mapsto G_x$ is a G -equivariant isomorphism of algebraic varieties $X \rightarrow \mathcal{B}$.

If X is not of maximum dimension, then its points correspond to the elements of a conjugacy class of parabolic subgroups of G (see 18.54).

b. *Decomposition of a projective variety under the action of a torus (Białynicki-Birula)*

Our goal is to study the decomposition of \mathcal{B} under the action of various tori in G , but first we obtain some general results.

When G acts on an affine algebraic scheme X , we let $g \in G(k)$ act on $f \in \mathcal{O}(X)$ by ${}^g f = f \circ g^{-1}$.

LUNA MAPS

19.6. Let $\mu: \mathbb{G}_m \times X \rightarrow X$ be a linear action of \mathbb{G}_m on a projective variety X (9.35), and let $x \in X(k)$. Then either x is fixed by \mathbb{G}_m , or its orbit O_x in X is a curve with exactly two boundary points, namely, $\lim_{t \rightarrow 0} \mu_x(t)$ and $\lim_{t \rightarrow \infty} \mu_x(t)$, and these are exactly the fixed points of the action of \mathbb{G}_m on $\overline{O_x}$. This statement is an immediate consequence of (14.47).

19.7. Let X be an affine algebraic scheme over k equipped with an action of a torus T , and let $x \in X(k)^T$. Let $\mathfrak{m}_x \subset \mathcal{O}(X)$ be the maximal ideal at x . Because the representations of T are semisimple (14.22), there exists a T -stable complement to \mathfrak{m}_x^2 in \mathfrak{m}_x , i.e., a k -subspace W of \mathfrak{m}_x , stable under T , mapping isomorphically onto $\mathfrak{m}_x/\mathfrak{m}_x^2$. The inclusion $W \rightarrow \mathcal{O}(X)$ extends uniquely to a k -algebra homomorphism $\text{Sym}_k(W) \rightarrow \mathcal{O}(X)$, which defines a regular map $\varphi: X \rightarrow (T_x X)_a$ (cf. 14.76). The map φ is T -equivariant and sends x to 0; it is étale if and only if x is smooth. A map

$$\varphi: X \rightarrow (T_x X)_a$$

arising in this way is called a **Luna map**.

Let X be an algebraic 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 $T_x X$, which therefore decomposes into a direct sum

$$T_x X = \bigoplus_{i \in \mathbb{Z}} T_x(X)_i$$

of eigenspaces (so $t \in T(k)$ acts on $T_x(X)_i$ as multiplication by t^i). We call i the **weight** of $(T_x X)_i$. Let

$$T_x^+ X = \bigoplus_{i > 0} (T_x X)_i \quad (\text{contracting subspace})$$

$$T_x^- X = \bigoplus_{i < 0} (T_x X)_i.$$

Let \mathfrak{m}_x denote the maximal ideal at x ; then

$$T_x(X) = \text{Hom}(\mathfrak{m}_x/\mathfrak{m}_x^2, k),$$

and so the weights of \mathbb{G}_m on $T_x(X)$ are the negatives of those on $\mathfrak{m}_x/\mathfrak{m}_x^2$.

EXAMPLE 19.8. Let \mathbb{G}_m act on $X = \mathbb{A}^n$ according to the rule

$$t(x_1, \dots, x_n) = (t^{m_1}x_1, \dots, t^{m_n}x_n), \quad m_i > 0.$$

The only fixed point is $o = (0, \dots, 0)$. The maximal ideal at o in $\mathcal{O}(X) = k[T_1, \dots, T_n]$ is $\mathfrak{m} = (T_1, \dots, T_n)$, and the weights of \mathbb{G}_m acting on $\mathfrak{m}/\mathfrak{m}^2$ are $-m_1, \dots, -m_n$. 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 $X \rightarrow \text{Sym}(W)$ is the identity map $\mathbb{A}^n \rightarrow \mathbb{A}^n$. Note that the weights of \mathbb{G}_m on $T_o(X)$ are m_1, \dots, m_n .

PROPOSITION 19.9. *Let X be a connected affine algebraic variety over k equipped with an action of \mathbb{G}_m , and let $x \in X(k)$ be fixed by \mathbb{G}_m . If the weights of \mathbb{G}_m on $T_x X$ are nonzero and all of the same sign, then every Luna map $\varphi: X \rightarrow T_x X$ is a closed immersion (isomorphism if x is smooth), and x is the only fixed point of T in $X(k)$.*

PROOF. After possibly composing the action with $t \mapsto t^{-1}$, we may suppose that $T_x X = T_x^- X$. Let $A = \mathcal{O}(X)$ and let $\mathfrak{m}_x \subset A$ be the maximal ideal at x . Then $A = \bigoplus_{i \in \mathbb{Z}} A_i$ and $\mathfrak{m}_x = \bigoplus_{i \in \mathbb{Z}} \mathfrak{m}_i$ where $t \in \mathbb{G}_m(k)$ acts on A_i and \mathfrak{m}_i as multiplication by t^i . As $A/\mathfrak{m}_x = k$, we have $A_i = \mathfrak{m}_i$ for all $i \neq 0$. Let φ be the Luna map defined by a \mathbb{G}_m -stable complement W to \mathfrak{m}^2 in \mathfrak{m} (19.7). As the weights of \mathbb{G}_m on $T_x X$ are strictly negative, its weights on W are strictly positive: $W = \bigoplus_{i > 0} W_i$. The canonical map

$$\text{Sym}^j(W) \rightarrow \mathfrak{m}_x^j/\mathfrak{m}_x^{j+1}$$

is surjective, and so $(\mathfrak{m}_x^j/\mathfrak{m}_x^{j+1})_i = 0$ for $i \leq 0$.

We now prove the proposition in the case that X is irreducible. In this case A is an integral domain; hence it embeds into $A_{\mathfrak{m}_x}$, and the Krull intersection theorem (for $A_{\mathfrak{m}_x}$) implies that $\bigcap_{j \geq 0} \mathfrak{m}_x^j = 0$. Therefore a nonzero element of \mathfrak{m}_x of weight i gives a nonzero element of weight i in $\mathfrak{m}_x^j/\mathfrak{m}_x^{j+1}$ for some j . It follows that $\mathfrak{m}_i = 0$ for $i \leq 0$. Now

$$A_0 = k, \quad A_i = 0 \quad \text{for } i < 0, \quad \mathfrak{m}_x = \bigoplus_{i > 0} A_i,$$

and so the graded Nakayama lemma (19.10 below) shows that the canonical map $\text{Sym}_k(W) \rightarrow A$ is surjective, which means that the Luna map $\varphi: X \rightarrow \text{Sym}_k(W)$ is a closed immersion.

Because the weights of \mathbb{G}_m on $T_x X$ are strictly negative, $\lim_{t \rightarrow \infty} tz = 0$ for all $z \in T_x X$ (14.46). It follows that $\lim_{t \rightarrow \infty} tz = x$ for all $z \in X$, and so x is the unique fixed point in X (by 19.6). This completes the proof in the irreducible case.

Now assume only that X is connected. Because \mathbb{G}_m is connected, every irreducible component of X is stable under \mathbb{G}_m . Let X_1 be an irreducible component of X containing x . Then $x = \lim_{t \rightarrow \infty} tz$ 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 \mathbb{G}_m . Let $z \in X_1 \cap X'$; then $x = \lim_{t \rightarrow \infty} tz \in X_1 \cap X'$. 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 $\bigcap_{j \geq 0} \mathfrak{m}_x^j \subset \mathfrak{p}_i$ for all i , and so $\bigcap_{j \geq 0} \mathfrak{m}_x^j = 0$. Now the same argument as in the irreducible case applies.

Finally, if x is smooth, then it is irreducible and $\dim(X) = \dim T_x(X)$, and so the closed immersion $X \hookrightarrow (T_x X)_a$ is an isomorphism. \square

LEMMA 19.10 (NAKAYAMA'S LEMMA FOR A GRADED RING). *Let $A = \bigoplus_{n \geq 0} A_n$ be a graded commutative k -algebra with $A_0 = k$. Let $\mathfrak{M} \stackrel{\text{def}}{=} \bigoplus_{n > 0} A_n$ be the irrelevant ideal, and let E be a graded k -subspace of A such that $\mathfrak{M} = E \oplus \mathfrak{M}^2$. Then the canonical map $\text{Sym}_k(E) \rightarrow A$ is surjective.*

PROOF. The image of $\text{Sym}_k(E) \rightarrow A$ is the k -subalgebra $k[E]$ generated by E . Let $a \in A_n$. We prove by induction on n that $a_n \in k[E]$. Certainly this is true if $n = 0$, and so we may suppose that $a \in \mathfrak{M}$. There exists an $e \in E$ such that $a - e \in \mathfrak{M}^2$, and so we may suppose that $a \in \mathfrak{M}^2$. Write $a_n = \sum_i b_i c_i$ with b_i and c_i homogeneous elements of \mathfrak{M} . The equality remains true when we omit any terms $b_i c_i$ with $\deg(b_i) + \deg(c_i) \neq n$. For the remaining terms, $\deg(b_i) < n$ and $\deg(c_i) < n$, and so $b_i, c_i \in k[E]$. \square

BIAŁYNIICKI-BIRULA DECOMPOSITION

LEMMA 19.11. *Let (V, r) be a finite-dimensional representation of a torus T . Then $\mathbb{P}(V)$ admits a covering by T -stable open affine subsets.*

PROOF. Let $\{e_1, \dots, e_n\}$ be a basis of eigenvectors for the action of T on V , and let $\{e_1^\vee, \dots, e_n^\vee\}$ be the dual basis. Then the sets $D(e_i^\vee) \stackrel{\text{def}}{=} \{[v] \in \mathbb{P}(V) \mid e_i^\vee(v) \neq 0\}$ form a covering with the required properties. \square

THEOREM 19.12. (*Białynicki-Birula decomposition*) *Let (V, r) be a finite-dimensional representation of \mathbb{G}_m , and let X be a smooth closed connected subvariety of $\mathbb{P}(V)$ stable under \mathbb{G}_m . For $x \in X^{\mathbb{G}_m}$, let*

$$X(x) = \{y \in |X| \mid \lim_{t \rightarrow 0} t \cdot y = x\}.$$

(a) *The set $X(x)$ is locally closed in $|X|$, $X(x)_{\text{red}} \approx \mathbb{A}^{n(x)}$ with $n(x) = \dim T_x^+(X)$, and*

$$X = \bigsqcup_{x \in X^{\mathbb{G}_m}} X(x).$$

(b) *If $X(k)^{\mathbb{G}_m}$ is finite, then there is a unique fixed point x_- (called the attracting point) such that $X(x_-)$ is open (and dense) in X , and a unique fixed point x^+ (called the repelling point) such that $X(x^+) = \{x^+\}$.*

EXAMPLE 19.13. Let \mathbb{G}_m act on $X = \mathbb{P}^n$ according to the rule

$$t(x_0 : \dots : x_i : \dots : x_n) = (t^0 x_0 : \dots : t^i x_i : \dots : t^n x_n).$$

The fixed points are P_0, \dots, P_n with $P_i = (0 : \dots : 0 : 1 : 0 : \dots : 0)$. On the open affine neighbourhood

$$U_i = \{(x_0 : \dots : x_i : \dots : x_n) \mid x_i \neq 0\}$$

of P_i , the action is

$$t(x_0 : \dots : 1 : \dots : x_n) = (t^{-i} x_0 : \dots : 1 : \dots : t^{n-i} x_n).$$

It follows that

$$X(P_i) = \{(0 : \cdots : 0 : 1 : x_{i+1} : \cdots : x_n)\} \simeq \mathbb{A}^{n-i}.$$

Certainly,

$$\mathbb{P}^n = X(P_0) \sqcup \cdots \sqcup X(P_n),$$

and P_0 is the attracting point and P_n is the repelling point.

PROOF. (a) Let $x \in X(k)$ be a fixed point of \mathbb{G}_m . Let $U = \text{Spm}(A)$ be an open affine containing x and invariant under \mathbb{G}_m (19.11), and let $\mathfrak{m}_x \subset A$ be the maximal ideal at x . Let $\varphi: U \rightarrow (T_x X)_\mathfrak{a}$ be the Luna map at x defined by a \mathbb{G}_m -stable complement W to \mathfrak{m}_x^2 in \mathfrak{m}_x . Let Y be the connected component of $\varphi^{-1}(T_x^+ X)$ containing x ; it is a closed \mathbb{G}_m -stable subset of U , which we regard as a subvariety of U :

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & (T_x X)_\mathfrak{a} \\ \text{closed} \uparrow & & \text{closed} \uparrow \\ Y & \xrightarrow{\varphi|_Y} & (T_x^+ X)_\mathfrak{a}. \end{array}$$

We shall show that $\varphi|_Y$ is a Luna map.

Write

$$W = W^- \oplus W^{\geq 0}, \quad W^- = \bigoplus_{i < 0} W_i, \quad W^{\geq 0} = \bigoplus_{i \geq 0} W_i.$$

By definition, Y is the zero-set in U of the subset $W^{\geq 0}$ of A . Hence

$$\dim X - \dim Y \leq \dim W^{\geq 0}$$

(A.41). As X is smooth, $\dim X = \dim T_x(X) = \dim W$, and so this implies that

$$\dim Y \geq \dim W - \dim W^{\geq 0} = \dim W^-. \quad (134)$$

The ring $\mathcal{O}(Y)$ is the quotient of A by the radical \mathfrak{a} of the ideal in A generated by the elements of $W^{\geq 0}$, and so the cotangent space to Y at x is

$$T_x(Y)^\vee = (\mathfrak{m}_x/\mathfrak{a})/(\mathfrak{m}_x^2 + \mathfrak{a}/\mathfrak{a}) \simeq \mathfrak{m}_x/(\mathfrak{m}_x^2 + W^{\geq 0}) \simeq W^-. \quad (135)$$

From (134) and (135) we find that $\dim Y \geq \dim T_x(Y)$, hence

$$\dim Y = \dim T_x(Y) = \dim W^-.$$

It follows that Y is smooth at x , that $T_x(Y) = T_x^+(X)$, and that $\varphi|_Y$ is the Luna map defined by W^- . Hence $\varphi|_Y$ is an isomorphism (19.9).

We next show that $Y = X(x)$. Let $y \in X(x)$, so that $\lim_{t \rightarrow 0} t \cdot y = x$. The orbit O_y contains x in its closure, and so meets U . But U is \mathbb{G}_m -invariant, and so $O_y \subset U$. On applying φ to $\lim_{t \rightarrow 0} t \cdot y = x$, we find that $\lim_{t \rightarrow 0} t \cdot \varphi(y) = 0$, and so $\varphi(y) \in T_x^+ X$. Hence $y \in Y$. Conversely, let $y \in Y$. Then $\varphi(y) \in T_x^+ X$, and so $\lim_{t \rightarrow 0} t \cdot \varphi(y) = 0$. Hence $y \in X(x)$.

As $X(x) = Y$, it is closed in U . Hence it is locally closed in X , and so $X(x)_{\text{red}} \simeq T_x^+(X)_\mathfrak{a}$.

Finally, let $z \in X$. Then either z is fixed by \mathbb{G}_m , or its orbit O_z in X is a curve with exactly two boundary points $\lim_{t \rightarrow 0} tz$ and $\lim_{t \rightarrow \infty} tz$, and these are exactly the fixed points

of \mathbb{G}_m acting on $\overline{O_z}$ (see 19.6). Let $x = \lim_{t \rightarrow 0} tz$; then x is fixed by \mathbb{G}_m and $z \in X(x)$. This completes the proof of (a).

(b) Assume that $X(k)^{\mathbb{G}_m}$ is finite, so there are only finitely many sets $X(x)$. Each set $X(x)$ is open in its closure, and so there is unique point x_- such that $X(x_-)$ is dense in X . Note that, for $x \in X$,

$$\begin{aligned} X(x) \text{ is dense in } X &\iff X(x) \text{ is open in } X \\ &\iff T_x(X) = T_x^+(X) \\ &\iff \dim(X(x)) = \dim(X). \end{aligned}$$

By considering the reciprocal action (i.e., composing with $t \mapsto t^{-1}$), we see that there is a unique point x_+ such that $T_{x_+}(X) = T_{x_+}^-(X)$. Note that, for $x \in X$,

$$T_x(X) = T_x^-(X) \iff \dim(X(x^+)) = 0 \iff X(x^+) = \{x^+\}. \quad \square$$

Let (V, r) be a finite-dimensional representation of a torus T . Let X be a closed irreducible subvariety of $\mathbb{P}(V)$ stable under T . Recall (21.19) that there exists a cocharacter $\lambda: \mathbb{G}_m \rightarrow T$ such that $\mathbb{P}(V)^{\mathbb{G}_m} = \mathbb{P}(V)^T$. On applying (19.12) to the action of $\lambda(\mathbb{G}_m)$ on X , we obtain a decomposition

$$X = \bigsqcup_{x \in X^T} X(x, \lambda), \quad X(x, \lambda) = \{y \in X \mid \lim_{t \rightarrow 0} \lambda(t)y = x\},$$

where $X(x, \lambda)$ is an affine space, isomorphic to the contracting subspace of $\lambda(\mathbb{G}_m)$ on the tangent space $T_x X$. If X^T is finite, then there exists a unique attracting fixed point x_- and a unique repelling point x_+ .

LEMMA 19.14. *For every $x \in X^T$, the set*

$$U(x) = \{y \in X \mid x \in \overline{T \cdot y}\}$$

is an open affine in X .

PROOF. Let λ be as in (21.19), so $\mathbb{P}(V)^{\lambda(\mathbb{G}_m)} = \mathbb{P}(V)^T$. On applying (19.12), we see that there exists a unique point $x_- \in X^T$ such that $X(x_-, \lambda)$ is open in X ; moreover, $T_{x_-}(X) = T_{x_-}^+(X)$. We shall show that $U(x_-) = X(x_-, \lambda)$.

If $\lim_{t \rightarrow 0} \lambda(t)y = x_-$, then $x_- \in \overline{T \cdot y}$, and so $X(x_-, \lambda) \subset U(x_-)$. Conversely, let $y \in U(x_-)$. 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 $y \in X(x_-, \lambda)$. \square

Recall (9.37) 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 19.15. *Let (V, r) be a finite-dimensional representation of a torus T , and let X be a closed irreducible subvariety of $\mathbb{P}(V)$ stable under T . Assume that the embedding $X \rightarrow \mathbb{P}(V)$ is nondegenerate and that $X(k)^T$ is finite. Let \mathcal{E} be the set of characters of T occurring in V . Let λ be a cocharacter of T such the the integers $\langle \chi, \lambda \rangle$, $\chi \in \mathcal{E}$, are distinct.*

- (a) *Let $\chi_- \in \mathcal{E}$ 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 $\chi_+ \in \mathcal{E}$ 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 $X \rightarrow \mathbb{P}(V)$ is nondegenerate, there exists a line $[v] \in X$ with $v = \sum_{\chi \in \mathcal{E}} v_\chi$, $v_\chi \in V_\chi$, $v_{\chi_-} \neq 0$. Then

$$\lim_{t \rightarrow 0} [\lambda(t)v] = [v_{\chi_-}];$$

in particular, $x_- = [v_{\chi_-}]$ is a fixed point of X . The action of $\lambda(\mathbb{G}_m)$ on the tangent space $T_{x_-}(\mathbb{P}(V))$ 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 $X \rightarrow \mathbb{P}(V)$ 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 $-\lambda$. □

c. Chevalley's theorem on the Borel subgroups containing a maximal torus

Let G be a connected group variety. Recall (18.34) that

$$R(G) = \left(\bigcap_{B \subset G \text{ Borel}} B \right)_{\text{red}}^\circ.$$

The following is a more precise statement.

THEOREM 19.16. (Chevalley's theorem). *Let G be a connected group variety, and let T be a maximal torus in G . Then*

$$\begin{aligned} R_u(G) \cdot T &= \left(\bigcap_{B \supset T \text{ Borel}} B \right)_{\text{red}}^\circ \\ R_u(G) &= \left(\bigcap_{B \supset T \text{ Borel}} B_u \right)_{\text{red}}^\circ. \end{aligned}$$

In other words, $|R_u(G) \cdot T|$ is the identity component of $\bigcap_{B \supset T \text{ Borel}} |B|$, and $|R_u(G)|$ is the identity component of $\bigcap_{B \supset T \text{ Borel}} |R_u(B)|$.

Before proving the theorem, we list some consequences.

COROLLARY 19.17. *Let S be a subtorus of a connected group variety G . Then*

$$R_u(C_G(S)) = R_u(G) \cap C_G(S).$$

In particular, $C_G(S)$ is reductive if G is reductive.

PROOF. Let S act on G by conjugation. Then $C_G(S) = G^S$, and so $R_u(G) \cap C_G(S) = R_u(G)^S$. This shows that $R_u(G) \cap C_G(S)$ is smooth and connected (16.21, 18.41). As it is unipotent (15.7) 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 containing S . For any Borel subgroup B of G containing T , $B \cap C_G(S)$ is a Borel subgroup of $C_G(S)$ (18.51), and so $B \supset R_u(C_G(S))$. Therefore

$$R_u(C_G(S)) \subset \left(\bigcap_{B \in \mathcal{B}^T} B \right)_{\text{red}}^\circ \stackrel{19.16}{=} R_u(G) \cdot T,$$

and so

$$R_u(C_G(S)) \subset (R_u(G) \cdot T)_u = R_u(G). \quad \square$$

COROLLARY 19.18. *Let S be a torus acting on a connected group variety 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

$$R_u(G^S) = R_u(C_{G'}(S)) \stackrel{19.17}{=} R_u(G') \cap C_{G'}(S) = R_u(G)^S. \quad \square$$

COROLLARY 19.19. *Let G be a reductive group over a field k (not necessarily algebraically closed).*

- (a) *If T is a maximal torus, then $C_G(T) = T$.*
- (b) *We have $Z(G) \subset \bigcap_{T \text{ maximal}} T$; if k is algebraically closed, then*

$$Z(G)_{\text{red}} = \left(\bigcap_{T \text{ maximal}} T \right)_{\text{red}}.$$

- (c) *If S is a torus in G , then $C_G(S)$ is reductive and connected.*

PROOF. (a) The torus T remains maximal over k^{al} (19.19), and so we may suppose that k is algebraically closed. Every Borel subgroup containing T contains $C_G(T)$ (18.45), and $C_G(T)$ is smooth and connected (16.21, 18.41), and so

$$C_G(T) \subset \left(\bigcap_{B \in \mathcal{B}_T} B \right)_{\text{red}} \stackrel{19.16}{=} R_u(G) \cdot T = T.$$

(b) Certainly, $Z(G) \subset \bigcap_{T \text{ maximal}} C_G(T) = \bigcap_{T \text{ maximal}} T$. Conversely, if g lies in the intersection of all maximal tori, then it commutes with all elements of all Cartan subgroups, but these elements contain a dense open subset of G (18.48), and so $g \in Z(G)(k)$.

- (c) The algebraic group $C_G(S)$ is smooth and connected (16.21, 18.41), and

$$R_u(C_G(S)_{k^{\text{al}}}) \stackrel{19.17}{=} R_u(G_{k^{\text{al}}}) \cap C_{G_{k^{\text{al}}}}(S_{k^{\text{al}}}) = e. \quad \square$$

Recall that for an algebraic group $D = D(M)$ of multiplicative type, the greatest torus in D is $D_t = D(M/M_{\text{tors}})$.

COROLLARY 19.20. *Let G be a reductive group over a field k (not necessarily algebraically closed).*

- (a) *The centre $Z(G)$ of G is of multiplicative type.*
- (b) *$R(G) = Z(G)_t$.*
- (c) *The formation of $R(G)$ commutes with extension of the base field.*
- (d) *The quotient $G/R(G)$ is semisimple.*

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 (1.63). It is also connected and commutative (by definition), and so $Z(G)_t \subset R(G)$. Conversely, $R(G)_{k^{\text{al}}} \subset R(G_{k^{\text{al}}})$, which is a torus because $R_u(G_{k^{\text{al}}}) = e$. Therefore $R(G)$ is a torus. Rigidity (14.29) 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 greatest subtorus, commute with extension of the base field, and so this follows from (b).

(d) We have

$$(G/R(G))_{k^{\text{al}}} \simeq G_{k^{\text{al}}}/R(G)_{k^{\text{al}}} \stackrel{(c)}{\simeq} G_{k^{\text{al}}}/R(G_{k^{\text{al}}}),$$

which is semisimple (8.39). By definition, this means that $G/R(G)$ is semisimple. \square

COROLLARY 19.21. *Let G be a reductive group over an infinite field k . Then G is unirational, and so $G(k)$ is dense in G .*

PROOF. Let T be a maximal torus in G . Then $C_G(T) = T$, which is unirational (14.41), and so the statement follows from (18.72). \square

COROLLARY 19.22. *Let G be a connected group variety over a perfect infinite field. Then G is unirational, and so $G(k)$ is dense in G .*

PROOF. Study the exact sequence

$$e \rightarrow R_u G \rightarrow G \rightarrow G/R_u G \rightarrow e$$

using that $G/R_u G$ is reductive (because k is perfect). \square

ASIDE 19.23. Let S be a torus in a reductive group G . The classical proof (e.g., Borel 1991, 13.17) of (19.19c) only shows that $C_G(S)_{\text{red}}$ is reductive. However, together with (16.21), this proves that $C_G(S)$ itself is reductive.

ASIDE 19.24. Let G be a connected group variety. The formation of $R_u(G)$ does not commute with inseparable extensions of the base field. See Example 8.43.

d. Proof of Chevalley's theorem (Luna)

THEOREM 19.25 (KOSTANT-ROSENLICHT). *Let G be a unipotent algebraic group acting on an affine algebraic variety X . Then every orbit 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 $Z = X \setminus O$. As $Z \neq X$, the ideal $I(Z)$ in $\mathcal{O}(X)$ is nonzero. Because Z is stable under G , the ideal $I(Z)$ is stable under G , and because G is unipotent, there exists a nonzero $f \in I(Z)^G$ (15.2). Because f is fixed by G , it is constant on O , and hence also on X . Hence $I(Z)$ contains a nonzero scalar, and so Z is empty. \square

For example, the orbits of \mathbb{U}_2 acting on k^2 are the horizontal lines, which are closed.

THEOREM 19.26 (LUNA). *Let G be a connected group variety, and let T be a maximal torus in G . For all Borel subgroups B of G containing T ,*

$$\mathcal{B}(B) \stackrel{\text{def}}{=} \{B' \in \mathcal{B} \mid B \in \overline{T \cdot B'}\}$$

is an open affine subset of \mathcal{B} , and it is stable under $I_u(T)$.

PROOF. Let $r: G \rightarrow \mathrm{GL}_V$ be such that B is the stabilizer of a line $[v]$ and such that the projective embedding $G/B \rightarrow \mathbb{P}(V)$ is nondegenerate. Let X denote the image of \mathcal{B} in $\mathbb{P}(V)$ — it is a closed irreducible subvariety of $\mathbb{P}(V)$ stable under G . A Borel subgroup B of G corresponds to a point $x \in X$ fixed by T , and $\mathcal{B}(B)$ corresponds to the set

$$U_x \stackrel{\text{def}}{=} \{y \in X \mid x \in \overline{T \cdot y}\}.$$

Thus, we have to show that U_x is an open affine subset of X stable under $I \stackrel{\text{def}}{=} I_u(T)$.

That U_x is an open affine subset of X is proved in (19.14).

Let $V = \bigoplus_{\chi \in \mathcal{E}} V_\chi$ be the decomposition of V into eigenspaces for the action of T , and let $\lambda: \mathbb{G}_m \rightarrow T$ be a cocharacter of T such that the integers $\langle \lambda, \chi \rangle$, $\chi \in \mathcal{E}$, are distinct.

Let $\chi_- \in \mathcal{E}$ be such that $\langle \lambda, \chi_- \rangle$ is minimal. Then V_{χ_-} has dimension 1 and v_- is the unique attracting point x_- of X . We have seen (19.15) that the 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 $r^\vee: G \rightarrow \mathrm{GL}(V^\vee)$ 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 $\mathbb{P}(V^\vee) \setminus V_-^\perp$. 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 $I \subset P$. Therefore, it fixes the line $[v^\vee]$ and dually it leaves invariant the open $X_{x_-}(\lambda)$.

For another fixed point x of X^T , there exists an $n \in N(T)$ such that $n(x_-) = x$. It suffices to replace λ with $n(\lambda)$. □

PROOF OF CHEVALLEY'S THEOREM 19.16

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

$$I_u(T) \subset \left(\bigcap_{B \subset G \text{ Borel}} B \right)_{\text{red}}^{\circ} \stackrel{18.34}{=} R(G);$$

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 (18.5), 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 a $I_u(T)$ -fixed point B'' in $\overline{I_u(T) \cdot B'}$ (18.5). This point is contained in some $\mathcal{B}(B)$ for $B \in \mathcal{B}^T$. The set $\mathcal{B} \setminus \mathcal{B}(B)$ 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.

e. *Proof of Chevalley's theorem (following SHS)*

This is a free translation of part of SHS, Exposé 16, La Grosse Cellule. It will be omitted in favour of Luna's proof. Recall that k is algebraically closed.

COMPLEMENTS ON CONNECTED UNIPOTENT ALGEBRAIC GROUPS

LEMMA 19.27. *Let U be a connected unipotent group variety, and let V be a proper connected subgroup variety. Then*

$$|V| \neq |N_G(V)^\circ|.$$

In particular, if V is of codimension 1 in U , then it is normal in U , and U/V is isomorphic to \mathbb{G}_a .

PROOF. We argue by induction on $\dim(U)$. The statement being trivial if $\dim(U) = 1$, we may suppose that $\dim(U) > 1$. Then U contains a subgroup Z in its centre isomorphic to \mathbb{G}_a (15.23). If $Z \subset V$, we apply the induction hypothesis to $V/Z \subset U/Z$. Otherwise, VZ is a connected subgroup variety of U normalizing V and properly containing it. \square

LEMMA 19.28. *Let U be a connected unipotent group variety, and let V be a connected subgroup variety of U . Let T be a torus acting on U and normalizing V . Suppose that for exactly one subtorus S of T of codimension 1, V^S has codimension 1 in U^S , and for every other such subtorus S' , $U^{S'} \subset V$. Then V has codimension 1 in U .*

PROOF. Let

$$\mathfrak{u} = \bigoplus_{m \in X^*(T)} \mathfrak{u}_m \quad \text{and} \quad \mathfrak{v} = \bigoplus_{m \in X^*(T)} \mathfrak{v}_m$$

and be the decompositions of the Lie algebras of U and V with respect to the action of T . For $m \in X^*(T)$, let

$$Q_m = (\text{Ker } m)_{\text{red}}^\circ;$$

it is a subtorus of T of codimension 0 or 1. One sees immediately that

$$\text{Lie}(U^{Q_m}) = \mathfrak{u}^{Q_m} = \bigoplus_{n \in m\mathbb{Q}} \mathfrak{u}_n,$$

and similarly for \mathfrak{v} . The hypothesis implies immediately that \mathfrak{v} has codimension 1 in \mathfrak{u} , and therefore V has codimension 1 in U . \square

PROPOSITION 19.29. *Let U be a connected unipotent algebraic group with an action by a torus T . All algebraic subgroups of U containing U^T and stable under T are connected.*

PROOF. Let V be such a subgroup of U . As T is smooth, it acts on U_{red} and V_{red} ; as $(U_{\text{red}})^T$ is smooth (16.21),

$$U_{\text{red}} \supset V_{\text{red}} \supset (U_{\text{red}})^T.$$

Therefore, we may suppose that U is smooth. We argue by induction on the dimension of U . We may suppose that $\dim U > 0$. Let H be a central subgroup of U , normalized by T , and isomorphic to \mathbb{G}_a . As $H^1(T, H) = 0$ (16.3), the canonical morphism $U^T \rightarrow (U/H)^T$ is faithfully flat, and the induction hypothesis applied to U/H shows that $V/H \cap V$ is connected. It remains to prove that $H \cap V$ is connected. But T acts on H through a character χ . If $\chi = 1$, then $H \subset U^T \subset V$, and so $H \cap V = H$ is connected. If $\chi \neq 1$, $H \cap V$ is isomorphic to a subgroup of \mathbb{G}_a stable by homotheties, and is therefore \mathbb{G}_a or α_{p^n} , which are connected. \square

COROLLARY 19.30. *Let Q be a subgroup of a torus T acting on a connected trigonalizable group G ; then G^Q is connected.*

PROOF. The unipotent part G_u of G is stable under all automorphisms of G (17.7). Consequently, the normalizer of G_u in T contains $T(k)$, and therefore coincides with T . Hence G_u is normal in the semidirect product $H = G \rtimes T$. The quotient H/G_u is an extension of a connected diagonalizable group by a diagonalizable group (I hope), and therefore is diagonalizable (14.27). This shows that H is trigonalizable. Let S be a maximal diagonalizable subgroup of H containing T . We have $H_u = G_u$, and therefore $H = G_u \cdot S$ and $H^Q = (G_u)^Q \cdot S = G^Q \cdot T$. As S is connected, it suffices to prove that $(G_u)^Q$ is connected, and so we may suppose that G is unipotent. But then G^Q is a subgroup of G stable by T and containing G^T , and so we can apply (19.29).

PROPOSITION 19.31. *Let U be a connected unipotent group variety, and let T be a torus acting on U . Then $U(k)$ is generated by the subgroups $U^Q(k)$ where Q runs over the set of subtori of T of codimension 1.*

PROOF. Arguing as usual by induction on the dimension of U , we consider a central subgroup H of U , stable under T , and isomorphic to \mathbb{G}_a . For any subtorus Q of T , we have an exact sequence

$$1 \rightarrow H^Q(k) \rightarrow U^Q(k) \rightarrow (U/H)^Q(k) \rightarrow 1$$

(16.3). It follows immediately that $U(k)$ is generated by the $U^Q(k)$ and $H(k)$. But T acts on H through a character χ . If Q' is a subtorus of codimension 1 of T in the kernel of χ , then $U^{Q'}(k) \supset H(k)$, and therefore $U(k)$ is certainly generated by the $U^Q(k)$. \square

INTERSECTION OF THE BOREL GROUPS CONTAINING A MAXIMAL TORUS

In this subsection, G denotes a connected group variety and T is a maximal torus in G .

LEMMA 19.32. *The group $G(k)$ is generated by $T(k)$ and the subgroups $(B_u \cap C_G(Q))(k)$, where B runs over the set of Borel subgroups of G containing T and Q runs over the set of subtori of T of codimension 1.*

PROOF. In virtue of (19.31), it suffices to prove the $G(k)$ is generated by the $B(k)$. In virtue of (1.31), there exists a smooth connected subgroup H of G such that $H(k)$ is the subgroup of $G(k)$ generated by the $B(k)$. As H contains a Borel subgroup of B , it is its own normalizer (18.54); as $N_G(T)$ obviously normalizes H , it follows that $N_G(T) \subset H$; on the other hand, if $G \neq H$, G/H is a complete connected scheme over k of dimension > 0 . In virtue of (21.20), $(G/H)(k)$ contains at least two points fixed by T . Therefore, let $x \in G(k)$ be such that the image of x^{-1} in $(G/H)(k)$ is fixed by T ; we have $\text{inn}(x)T \subset H$, and so there exists an $h \in H(k)$ such that $\text{inn}(x)T = \text{inn}(h)T$, and therefore $x^{-1}h \in N_G(T)(k) \subset H(k)$; then $x \in H(k)$, and the image of x^{-1} in $(G/H)(k)$ is the marked point; $(G/H)^T(k)$ is therefore a single point, and so $G = H$. \square

LEMMA 19.33. *Let B be a Borel subgroup of G containing T , and let Q and S be singular subtori of codimension 1 in T . If $Q \neq S$, there exists a Borel subgroup B' containing T such that $B'^S = B^S$ and $B'^Q \neq B^Q$.*

PROOF. Let α (resp. β) be the root of G relative to T attached to B and Q (resp. B and S). Let γ be a regular cocharacter of T such that $\langle \gamma, \alpha \rangle < 0$ and $\langle \gamma, \beta \rangle > 0$. We know that there exists an open subset U of G/B and a point $b' \in U(k)$ such that, for all $x \in U(k)$, $\gamma(\infty)x = b'$. We shall show that the stabilizer B' of b' is the required Borel subgroup. It is certainly a Borel subgroup of G containing T , and the statement follows from SHS, Exp15 (Reductive groups of semisimple rank 1). \square

LEMMA 19.34. *Let B be a Borel subgroup containing T , and let S be a singular subtorus of T of codimension 1 (so B^S is a Borel subgroup of $C_G(S)$, after SHS, Exp14, Singular Tori). For each subgroup H of B , write $I(H)$ for the reduced intersection of the Borel subgroups of G containing H . Then $I(T)$ is a normal subgroup of $I(B^S)$, and the quotient is isomorphic to \mathbb{G}_a .*

PROOF. Let $I(T) = T \cdot I(T)_u$ and $I(B^S) = T \cdot I(B^S)_u$. It suffices to show that $V = I(T)_u$ is a normal subgroup of codimension 1 in U . On the other hand, because U and V contain $C_B(T) = B^T$, they are connected (19.29). We check that the hypotheses of (19.28) hold. Therefore, let Q be a subtorus of T of codimension 1 distinct from S . If Q is regular, $C(Q)$ is contained in all Borel subgroups containing T (Exp. 14), therefore in $I(T)$, and $V^Q \subset U$. If Q is singular, there exists a Borel subgroup B' of G containing T and such that $B'^S = B^S$ and $B'^Q \neq B^Q$ (19.28). We therefore have

$$U^Q \subset B \cap B' \cap C(Q) = B^Q \cap B'^Q.$$

But as B^Q and B'^Q are distinct Borel subgroups of $C(Q)$ containing T , we know that $B^Q \cap B'^Q$ is the intersection of $C(Q)$ with the intersection of all Borel subgroups containing T . We therefore have $U^Q \subset V$. It remains to calculate U^S and V^S . But $(T \cdot U)^S = T \cdot U^S$ is a connected trigonalizable subgroup of $C(S)$ containing B^S , and so $U^S = (B^S)^u$; on the other hand, $U^S \not\subset V^S$, because there exist Borel subgroups of G containing T cutting $C(S)$, for example, the opposite Borel subgroup to B^S . Finally, $R_u(C(S))$, which is contained in all Borel subgroups of $C(S)$, is contained in V^S and is of codimension 1 in $(B^S)^u$ (Exp. 15). It follows that V^S has codimension 1 in U^S . The hypotheses of (19.28) are now satisfied, and therefore V is a normal subgroup of codimension 1 in U and $V/U \approx \mathbb{G}_a$. \square

PROPOSITION 19.35. *The reduced intersection of the Borel subgroups containing T is $T \cdot R_u(G)$.*

PROOF. With the notation of (19.34), we have to show that V_{red} is the unipotent radical of G . As obviously $R_u(G) \subset V_{\text{red}}$, and as V_{red} is connected, smooth, and unipotent, it suffices to show that $G(k)$ normalizes V_{red} . After (19.32), it suffices to prove that for all Borel groups B containing T and all subtori Q of T of codimension 1, $(B^Q)_u$ normalizes V_{red} , or that B^Q normalizes V . If Q is regular, $C(Q)$ is contained in all Borel subgroups of G containing T , and therefore in V , and B^Q normalizes V . If Q is singular, Lemma 19.34 shows that B^Q normalizes V (because $B^Q \subset I(B^Q)$, and $I(B^Q)$ normalizes V). \square

f. Summary

Let G be a group variety over an algebraically closed field k . A Borel subgroup G is a maximal connected solvable subgroup variety of G . For example, the group of invertible upper-triangular matrices is a Borel subgroup in GL_n . Borel (1956) was the first to carry out a systematic study of such subgroups.

Borel subgroups are characterized by being minimal among the parabolic subgroups of G (those subgroups such that G/H is projective). All Borel subgroups of G are conjugate and if G and its Borel subgroups B_1, B_2 are defined over a subfield k_0 of k , then B_1 and B_2 are conjugate by an element of $G(k_0)$.

The intersection of any two Borel subgroups of a group G contains a maximal torus of G ; if the intersection equals the maximal torus, then the Borel subgroups are said to be opposite. Opposite Borel subgroups exist in G if and only if G is a reductive group.

If G is connected, then it is the union of all its Borel subgroups, and every parabolic subgroup coincides with its normalizer in G . In this case a Borel subgroup is maximal among all (and not only algebraic and connected) solvable subgroups of $G(k)$. Nevertheless, maximal solvable subgroups in $G(k)$ that are not Borel subgroups usually exist.

The commutator subgroup of a Borel subgroup B is equal to its unipotent part B_u , and the normalizer of B_u in G equals B .

When k has characteristic 0, the subalgebra \mathfrak{b} in the Lie algebra \mathfrak{g} of G defined by a Borel subgroup B of G is often referred to as a Borel subalgebra in \mathfrak{g} . The Borel subalgebras in \mathfrak{g} are its maximal solvable subalgebras.

When G is a group variety over an arbitrary field k , the minimal parabolic subgroups in G play a role in the theory of algebraic groups over k similar to that of the Borel groups when k is algebraically closed. For example, two such parabolic subgroups are conjugate by an element of $G(k)$ (Borel and Tits 1965).

(Adapted from the entry for “Borel subgroup” in the *Encyclopedia of Mathematics*; V. Platonov)

The geometry of reductive algebraic groups

In this chapter, following [Iversen 1976](#), we study the geometry of algebraic groups, especially reductive algebraic groups. The proofs assume more algebraic geometry than usual, but most statements will be given more conventional proofs later, and so the proofs can be skipped.

a. Definitions

Let G' and G be connected group varieties. Recall (2.17, 8.4) that an isogeny $\varphi: G' \rightarrow G$ is a surjective homomorphism with finite kernel. If the order of the kernel is prime to the characteristic, then $\text{Ker}(\varphi)$ is étale (13.7), hence of multiplicative type, and hence contained in the centre of G' (rigidity 14.30). In nonzero characteristic, there exist isogenies with noncentral kernel, for example, the Frobenius map (2.16). The isogenies in nonzero characteristic that behave as the isogenies in characteristic zero are those whose kernel is of multiplicative type.

DEFINITION 20.1. A *multiplicative* (resp. *central*) isogeny¹ $\varphi: G' \rightarrow G$ is surjective homomorphism of connected group varieties whose kernel is finite of multiplicative type (resp. finite and contained in the centre of G).

If φ is multiplicative, then it is central (rigidity 14.30). Conversely, if G' is reductive and φ is central, then it is multiplicative (because the centre of a reductive group is of multiplicative type 19.20).

PROPOSITION 20.2. A composite of multiplicative isogenies is a multiplicative isogeny.

PROOF. Let φ_1 and φ_2 be composable multiplicative isogenies. Then

$$e \rightarrow \text{Ker}(\varphi_1) \rightarrow \text{Ker}(\varphi_2 \circ \varphi_1) \xrightarrow{\varphi_1} \text{Ker}(\varphi_2) \rightarrow e$$

is exact (Exercise 6-5), and $\text{Ker}(\varphi_2 \circ \varphi_1)$ is central (14.32), hence of multiplicative type (14.27). □

¹Iversen (1976) defines a central isogeny to be an isogeny whose kernel is of multiplicative type. I find this confusing, and so changed the terminology.

b. The universal covering

DEFINITION 20.3. A connected group variety G is **simply connected** if every multiplicative isogeny $G' \rightarrow G$ of connected group varieties is an isomorphism.

For semisimple groups, this agrees with the usual terminology.²

REMARK 20.4. Let G be a connected group variety, and let $\varphi: G' \rightarrow G$ be a surjective homomorphism with finite kernel of multiplicative type (G' not necessarily smooth or connected). Assume that k is perfect and that G is simply connected. Then $(G')_{\text{red}}^\circ$ is a connected group variety, and $(G')_{\text{red}}^\circ \xrightarrow{\varphi} G$ is a multiplicative isogeny, and hence an isomorphism. Therefore φ induces an isomorphism $(G')_{\text{red}}^\circ \rightarrow G$, and so $G' \simeq \text{Ker}(\varphi) \rtimes G = \text{Ker}(\varphi) \times G$ (2.21).

DEFINITION 20.5. A multiplicative isogeny $\tilde{G} \rightarrow G$ of connected group varieties is called a **universal covering** of G when \tilde{G} is simply connected. Its kernel is denoted $\pi_1(G)$, and is called the **fundamental group** of G . If G is semisimple, then \tilde{G} is also semisimple. In this case $\tilde{G} \rightarrow G$ is sometimes called a **simply connected central cover** of G .

Later (20.21) we shall see that a universal covering exists if $\text{Hom}(G, \mathbb{G}_m) = 0$. Here we prove that, if it exists, it is unique up to a unique isomorphism.

PROPOSITION 20.6. Let G be connected group variety over a perfect field k , and let $\pi: \tilde{G} \rightarrow G$ be a universal covering of G . For every multiplicative isogeny $\varphi: G' \rightarrow G$ of connected group varieties, there exists a unique homomorphism $\tilde{G} \rightarrow G'$ making the following diagram commute

$$\begin{array}{ccc} \tilde{G} & & \\ \downarrow & \searrow \pi & \\ G' & \xrightarrow{\varphi} & G. \end{array}$$

In particular, $\pi: \tilde{G} \rightarrow G$ is uniquely determined up to a unique isomorphism.

PROOF. The map $G' \times_G \tilde{G} \rightarrow \tilde{G}$ is surjective with finite kernel of multiplicative type. Its restriction $(G' \times_G \tilde{G})_{\text{red}}^\circ \rightarrow \tilde{G}$ is a multiplicative isogeny, and hence is an isomorphism. The composite of the inverse of this map with the homomorphism $(G' \times_G \tilde{G})_{\text{red}}^\circ \rightarrow G'$

If $\beta: \tilde{G} \rightarrow G'$ is a second homomorphism such that $\varphi \circ \beta = \pi$, then $g \mapsto \alpha(g)/\beta(g)$ maps \tilde{G} to $\text{Ker}(\varphi)$, and is therefore trivial (because \tilde{G} is connected and smooth). Hence $\alpha = \beta$. □

ASIDE 20.7. We shall see later that a split semisimple groups (G, T) is simply connected if and only if the coroots generate $X_*(T)$.

ASIDE 20.8. Let \mathfrak{g} be a Lie semisimple Lie algebra over a field k of characteristic zero. The group attached by Tannakian theory (Chapter 11) to the tensor category $\text{Rep}(\mathfrak{g})$ is the universal covering of G . This observation makes it possible to deduce the theory of reductive algebraic groups in characteristic zero from the similar theory for reductive Lie algebras. See my notes *Lie Algebras, Algebraic Groups, and Lie Groups*.

²For example, Conrad et al. 2010, p.419, say that a connected semisimple group is simply connected if every central isogeny $G' \rightarrow G$ with G' a connected semisimple group is an isomorphism.

c. Line bundles and characters

In this section, following Iversen 1976, we assume that k is algebraically closed. Let $X(G) = \text{Hom}(G, \mathbb{G}_m)$.

20.9. We assume (for the moment) that the reader is familiar with the notion of a vector bundle (for the Zariski topology or, equivalently, for the flat topology). Let G be an algebraic group acting on a variety X over k . Then there is a notion of a G -vector bundle on X (ibid. p.59, where it called a G -homogeneous vector bundle on X).

20.10. Let V be a vector space over k . The projective space $\mathbb{P}(V)$ has a universal line bundle L_{univ} on $\mathbb{P}(V)$ (ibid. 1.2).

20.11. Let (V, r) be a representation of G . Then G acts on L_{univ} if and only if r factors through PGL_V . More precisely, given $f: G \rightarrow \text{PGL}_V$, the actions of G on L_{univ} are in one-to-one correspondence with the liftings of f to GL_V (ibid. 1.3).

Now let G be a connected group variety and let B be a Borel subgroup of G . 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 -line bundle on G , and we let $L(\chi)$ denote the corresponding vector bundle on G/B .³

PROPOSITION 20.12. *The map $\chi \mapsto L(\chi)$ gives a bijection from $X(B)$ to the set of isomorphism classes of B -line bundles on G/B .*

PROOF. Let L be a B -line bundle on G/B . Then $p(e) \stackrel{\text{def}}{=} eB$ is a fixed point for the action of B on G/B , and so B acts on the fibre of L at $p(e)$. This action gives a character χ_L of B , which depends only on the isomorphism class of L . The map $L \mapsto \chi_L$ gives an inverse to the map sending χ to the isomorphism class of $L(\chi)$. \square

Let T be a maximal torus of G contained in B . Every character of T extends uniquely to a character of B (17.31), and so we get a linear map

$$\chi \mapsto L(\chi): X(T) \rightarrow \text{Pic}(G/B).$$

This is called the *characteristic map* for G .

The basic fact we need is the following.

THEOREM 20.13. *Let G be connected group variety, and let (B, T) be a Borel pair in G . Then the following sequence is exact:*

$$0 \rightarrow X(G) \rightarrow X(T) \rightarrow \text{Pic}(G/B) \rightarrow \text{Pic}(G) \rightarrow 0. \quad (136)$$

The proof, being mainly algebraically geometry, is deferred (at least) to the end of the chapter.

³The proof that $L(\chi)$ is locally trivial for the Zariski topology uses that $p: G \rightarrow G/B$ has a section locally for the Zariski topology (cf. 22.78). Alternatively, use that $G \rightarrow G/B$ has a section locally for the flat topology (because it is faithfully flat), and then use that a vector bundle is locally trivial for the Zariski topology if it is for the flat topology.

EXAMPLE 20.14. Let T be the diagonal maximal torus in $G = \mathrm{SL}_2$, and let B be the standard (upper triangular) Borel subgroup. Consider the natural action of G on \mathbb{A}^2 . Then G acts on \mathbb{P}^1 and B is the stabilizer of the point $(0 : 1)$. 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 $(0 : 1)$ through the character

$$\begin{pmatrix} z & x \\ 0 & z^{-1} \end{pmatrix} \mapsto z^{-1}.$$

In this case the characteristic map

$$X(T) \rightarrow \mathrm{Pic}(\mathrm{SL}_2/B)$$

is an isomorphism. Therefore, $X(\mathrm{SL}_2) = 0 = \mathrm{Pic}(\mathrm{SL}_2)$. (See (21.49) and the proof of (21.53) for direct proofs that $X(\mathrm{SL}_2) = 0$ and $\mathrm{Pic}(\mathrm{SL}_2) = 0$.)

LEMMA 20.15. *Let $G \rightarrow Q$ be a surjective homomorphism of connected group varieties. The inverse image of a Borel pair in Q is a Borel pair in G .*

PROOF. See (18.24). □

PROPOSITION 20.16. *Let $\varphi: G' \rightarrow G$ be a surjective homomorphism of connected group varieties whose kernel is of multiplicative type. Then there is an exact sequence*

$$0 \rightarrow X(G) \rightarrow X(G') \rightarrow X(\mathrm{Ker}(\varphi)) \rightarrow \mathrm{Pic}(G) \rightarrow \mathrm{Pic}(G') \rightarrow 0. \quad (137)$$

PROOF. Let (B, T) be a Borel pair in G , and let (B', T') be its inverse image in G' (so $G/B \simeq G'/B'$). The columns in the following commutative diagram are the exact sequences (136) for (G, B) and (G', B') :

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ & & X(G) & \longrightarrow & X(G') & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X(T) & \longrightarrow & X(T') & \longrightarrow & X(\mathrm{Ker} \varphi) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Pic}(G/B) & \xrightarrow{\simeq} & \mathrm{Pic}(G'/B') & \longrightarrow & 0 \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \\ & & \mathrm{Pic}(G) & \longrightarrow & \mathrm{Pic}(G') & & \\ & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & \end{array}$$

Now the snake lemma gives the required exact sequence. □

PROPOSITION 20.17. *Let G be a connected group variety. If $X(G) = 0$ and $\mathrm{Pic}(G) = 0$, then G is simply connected.*

PROOF. Let $\varphi: G' \rightarrow G$ be a multiplicative isogeny of connected group varieties. In the exact sequence (137)

$$X(G) \rightarrow X(G') \rightarrow X(\text{Ker } \varphi) \rightarrow \text{Pic}(G),$$

the groups $X(G)$ and $\text{Pic}(G)$ are zero, the group $X(\text{Ker } \varphi)$ is finite, and the group $X(G')$ is torsion free (because G' is smooth and connected). Therefore $X(\text{Ker } \varphi) = 0$, which implies that $\text{Ker}(\varphi) = e$. \square

EXAMPLE 20.18. The algebraic group SL_2 is simply connected because $X(\text{SL}_2) = 0 = \text{Pic}(\text{SL}_2)$ (see 20.14).

d. Existence of a universal covering

The existence of a universal covering $\tilde{G} \rightarrow G$ for a semisimple group G is usually deduced from the classification theorems (including the existence and isogeny theorems) for reductive groups, see, for example, Conrad et al. 2010 A.4.11. But the proof of such a basic fact, shouldn't require knowing the whole theory. In the rest of this section we sketch the proof in Iversen 1976. Throughout k is algebraically closed.

LEMMA 20.19. *Let G be a connected group variety, and let B be a Borel subgroup of G . The group $\text{Pic}(G/B)$ is finitely generated, and its generators can be chosen to be line bundles L with $\Gamma(G/B, L) \neq 0$.*

PROOF. This follows from the fact that G/B is a rational variety (Bruhat decomposition; cf. 22.78). \square

PROPOSITION 20.20. *Let G be a connected group variety. Then there exists a multiplicative isogeny $\tilde{G} \rightarrow G$ with \tilde{G} a connected group variety such that $\text{Pic}(\tilde{G}) = 0$.*

PROOF. Let B be a Borel subgroup of G . Note that, because of (20.16, 20.17), it suffices to prove that there exists a multiplicative isogeny $\varphi: G' \rightarrow G$ such that the map $\text{Pic}(G) \rightarrow \text{Pic}(G')$ is zero. After (20.19, 20.12, 20.13), 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 multiplicative isogeny $\varphi: G' \rightarrow G$ such that the pull back of L to $G'/\varphi^{-1}(B)$ is a $\varphi^{-1}(B)$ -line bundle.

Let $B' = \varphi^{-1}(B)$, so that $G'/B' \simeq G/B$. Let $V = \Gamma(G/B, L)$. We have canonical maps $s: G \rightarrow \text{PGL}(V)$ and $t: G/B \rightarrow \mathbb{P}(V)$ such that $t^*L_{\text{univ}} = L$. Let $\varphi: G' \rightarrow G$ denote the pull back of the multiplicative isogeny $\text{SL}_V \rightarrow \text{PGL}_V$ along s . Because L_{univ} is a SL_V -vector bundle, its pull back to G'/B' is a G' -vector bundle (hence also a B' -vector bundle). \square

COROLLARY 20.21. *Every connected group variety G such that $X(G) = 0$ admits a universal covering.*

PROOF. Let $\varphi: \tilde{G} \rightarrow G$ be as in (20.20). Because \tilde{G} is smooth and connected, $X(\tilde{G})$ is torsion free. Now the exact sequence (137) shows that

$$X(\tilde{G}) = 0 = \text{Pic}(\tilde{G})$$

and so \tilde{G} is simply connected (20.17). \square

COROLLARY 20.22. *Let G be a connected group variety. Then $\text{Pic}(G)$ is finite.*

PROOF. Let $\varphi: \tilde{G} \rightarrow G$ be as in (20.20). Then the exact sequence (20.16),

$$X(\text{Ker}(\varphi)) \rightarrow \text{Pic}(G) \rightarrow \text{Pic}(\tilde{G}) = 0$$

shows that $\text{Pic}(G)$ is finite. □

COROLLARY 20.23. *Let G be a connected group variety. If G is simply connected, then $\text{Pic}(G) = 0$.*

PROOF. If G is simply connected, then the multiplicative isogeny in (20.20) is an isomorphism, and so $\text{Pic}(G) \simeq \text{Pic}(\tilde{G}) = 0$. □

COROLLARY 20.24. *Let G be a connected group variety such that $X(G) = 0$. Then*

$$\text{Pic}(G) \simeq X(\pi_1 G).$$

PROOF. For the universal covering $\tilde{G} \rightarrow G$, the exact sequence (137) becomes

$$0 \rightarrow X(\pi_1 G) \rightarrow \text{Pic}(G) \rightarrow 0. \quad \square$$

e. Applications

The base field k is arbitrary.

PROPOSITION 20.25. *Let*

$$e \rightarrow D \rightarrow G' \rightarrow G \rightarrow e$$

be an extension of algebraic groups with G smooth, connected, simply connected, and perfect. The extension splits in each of the following cases.

- (a) D is a torus;
- (b) k is perfect.

PROOF. (a) From (20.16), we have an exact sequence

$$X^*(G) \rightarrow X^*(G') \rightarrow X^*(D) \rightarrow \text{Pic}(G_{k^{\text{al}}}).$$

As G is simply connected, $\text{Pic}(G_{k^{\text{al}}}) = 0$ (see 20.23), and as G is perfect, $X^*(G) = 0$. Therefore the restriction map $X^*(G') \rightarrow X^*(D)$ is an isomorphism. On the other hand, $T \stackrel{\text{def}}{=} G'/DG'$ is a torus (14.72). Consider the maps

$$D \rightarrow G' \rightarrow T.$$

The maps on the character groups are isomorphisms

$$X^*(T) \rightarrow X^*(G') \rightarrow X^*(D)$$

and so the homomorphism $D \rightarrow T$ is an isomorphism. This shows that the complex splits.

(b) There is an exact sequence

$$e \rightarrow D' \rightarrow D \rightarrow D'' \rightarrow e$$

with D' a torus and D'' finite (14.18). This gives an exact sequence

$$\text{Ext}^1(G, D'') \rightarrow \text{Ext}^1(G, D) \rightarrow \text{Ext}^1(G, D'),$$

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 (20.4) and the second was proved in (a). □

REMARK 20.26. (a) Every simply connected semisimple algebraic group G satisfies the hypotheses of the proposition (22.123).

(b) Is the proposition true with k nonperfect? For example, does there exist an algebraic group G with a normal finite subgroup N of multiplicative type such that G/N is semisimple and simply connected but for which the quotient map $G \rightarrow G/N$ has no section. A variant of (1.43) or (1.44) may be such an example.

PROPOSITION 20.27. *Let G be a reductive algebraic group. Assume that the semisimple algebraic group G/RG admits a universal covering $H \rightarrow G/RG$ with H perfect. Then there exists a multiplicative isogeny $T \times H \rightarrow G$ with T the torus RG .*

PROOF. On pulling back the extension

$$e \rightarrow RG \rightarrow G \rightarrow G/RG \rightarrow e$$

by the universal covering map $H \rightarrow G/RG$, we get an exact sequence

$$e \rightarrow RG \rightarrow G' \rightarrow H \rightarrow e$$

and a multiplicative isogeny $G' \rightarrow G$. According to (20.25), this extension splits:

$$G' \approx RG \times H. \quad \square$$

PROPOSITION 20.28. *Let G be a semisimple algebraic group. Assume that G admits a universal covering $\tilde{G} \rightarrow G$ with \tilde{G} perfect. For any torus D ,*

$$\text{Hom}(\pi_1(G), D) \simeq \text{Ext}^1(G, D).$$

PROOF. Let $f: \pi_1(G) \rightarrow D$ be a homomorphism. Define $E(f)$ to be the cokernel of the homomorphism

$$x \mapsto (x, f(x^{-1})): \pi_1(G) \rightarrow \tilde{G} \times D.$$

Then $E(f)$ is an extension of G by D .

For the converse, let $h: G' \rightarrow G$ be an extension of G by D . Then $\pi: \tilde{G} \rightarrow G$ factors through h , say,

$$\tilde{G} \xrightarrow{f} G' \xrightarrow{h} G,$$

and the factorization is unique (cf. 20.5). The restriction of f to $\pi_1(G)$ maps into D .

These operations are inverse. □

f. Proof of theorem 20.13

Throughout this section, k is algebraically closed. For an algebraic variety X over k , we let $U(X) = \Gamma(X, \mathcal{O}_X^\times)/k^\times$. Recall (14.69) that for all algebraic varieties X and Y , the map

$$(u, v) \mapsto p^*u \cdot q^*v: U(X) \oplus U(Y) \rightarrow U(X \times Y)$$

is an isomorphism.

THEOREM 20.29. *Let H be a smooth connected algebraic group, let V be a smooth algebraic variety, and let $f: E \rightarrow V$ be a right H -torsor over V . Then the following sequence is exact*

$$0 \rightarrow U(V) \xrightarrow{U(f)} U(E) \xrightarrow{U(i_e)} X(H) \xrightarrow{\chi \mapsto L(\chi)} \text{Pic}(V) \xrightarrow{\text{Pic}(f)} \text{Pic}(E) \xrightarrow{\text{Pic}(i_e)} \text{Pic}(H) \rightarrow 0.$$

Here e is a fixed point of E and $i_e: H \rightarrow E$ is the map $h \mapsto he$. The vector bundle $L(\chi)$ is as in (20.12).

The proof will be included in the final version if I can make it reasonably concise (see Fossum and Iversen 1973).

Let H be a connected solvable group variety. Then the flat torsors for H are locally trivial for the Zariski topology (DG IV, §4, 3.7, p.532). Moreover $\text{Pic}(H) = 0$.

Let G be a connected group variety, and let P be a parabolic subgroup. The G -torsor $G \rightarrow G/P$ is locally trivial for the Zariski topology. When G is reductive, Fossum and Iversen 1973 refers to Borel and Tits 1965, 4.13.

Now for P and the map $G \rightarrow G/P$, the sequence in (20.29) becomes

$$0 \rightarrow X(G) \rightarrow X(P) \rightarrow \text{Pic}(G/P) \rightarrow \text{Pic}(G) \rightarrow \text{Pic}(P) \rightarrow 0.$$

Algebraic groups of semisimple rank at most one

A semisimple group is said to have rank 1 if its maximal tori have dimension 1, and a reductive group is said to have semisimple rank 1 if its semisimple quotient has rank 1. In a sense, all reductive groups are built up of reductive groups of semisimple rank 1. In preparation for the general case, we study such groups in this chapter. For example, we show that every split reductive group of semisimple rank 1 is isomorphic to exactly one of the following groups

$$\mathbb{G}_m^r \times \mathrm{SL}_2, \quad \mathbb{G}_m^r \times \mathrm{GL}_2, \quad \mathbb{G}_m^r \times \mathrm{PGL}_2, \quad r \in \mathbb{N}.$$

This chapter also includes many preliminaries that will be needed for the general case.

Unless we say otherwise, the field k is arbitrary. Usually in this chapter R is a set of roots; if it is a k -algebra we say so.

a. Brief review of reductive groups

Let G be a reductive group over k . Recall that this means that G is a connected group variety containing no nontrivial connected unipotent normal subgroup variety, even over the algebraic closure of k . The centre $Z(G)$ of G is of multiplicative type, and its largest subtorus $Z(G)_t$ is equal to the radical $R(G)$ of G (greatest connected solvable normal subgroup variety); the formation of $R(G)$ commutes with extension of the base field, and $G/R(G)$ is semisimple (8.41, 19.20).

DEFINITION 21.1. The **rank** of a group variety G over a field k is the dimension of a maximal torus. Since any two maximal tori in G remain maximal in $G_{k^{\mathrm{al}}}$ and become conjugate there (18.66, 18.67), the rank depends only on G and is invariant under extension of the base field. The **semisimple rank** of a group variety over a field k is the rank of $G_{k^{\mathrm{al}}}/R(G_{k^{\mathrm{al}}})$.

Thus the semisimple rank of a reductive group is the rank of its semisimple quotient G/RG .

PROPOSITION 21.2. *Let G be a reductive group.*

- (a) *The semisimple rank of G is $\mathrm{rank}(G) - \dim Z(G)$.*
- (b) *The algebraic group $Z(G) \cap \mathcal{D}(G)$ is finite.*

- (c) *The algebraic group $\mathcal{D}(G)$ is semisimple, and its rank is at most the semisimple rank of G .*

PROOF. (a) A maximal torus T of G contains $Z(G)_t$, and

$$\text{rank}(G) \stackrel{\text{def}}{=} \dim(T) = \dim(T/Z(G)_t) + \dim(Z(G)) = \text{rank}(G/R(G)) + \dim(Z(G)).$$

(b) For any connected group variety G and central torus T , the group $T \cap \mathcal{D}(G)$ is finite. Therefore $Z(G)_t \cap \mathcal{D}(G)$ is finite, and this implies that $Z(G) \cap \mathcal{D}(G)$ is finite.

(c) We may suppose that k is algebraically closed. Let $R = R(\mathcal{D}(G))$. Then R is weakly characteristic in $\mathcal{D}(G)$, and so it is normal in R (1.65); hence $R \subset R(G) = Z(G)_t$. From (b) we see that it is finite, hence trivial (being smooth and connected). Therefore $\mathcal{D}(G)$ is semisimple, and the restriction of the quotient map $G \rightarrow G/R(G)$ to $\mathcal{D}(G)$ has finite kernel, and so $\text{rank}(\mathcal{D}(G)) \leq \text{rank}(G/R(G))$. \square

b. Group varieties of semisimple rank 0

We first dispose of the easy case.

THEOREM 21.3. *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 in the proof that k is algebraically closed.

(a) To say that G has rank 0 means that it does not contain a copy of \mathbb{G}_m , but this is equivalent to it being unipotent (17.65).

(b) If G is solvable, then $RG = G$, and so G has semisimple rank 0. Conversely, if G has semisimple rank 0, then G/RG is unipotent, which contradicts its semisimplicity unless it equals e (15.23). Thus $G = RG$ 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 with $G_u = e$; this implies that G is a torus (17.37d). \square

c. Limits in algebraic varieties

Cf. Section 19.b.

21.4. Let T be a split torus over k . Because T is split,

$$\begin{aligned} X^*(T) &= \text{Hom}(T, \mathbb{G}_m) && \text{(group of characters of } T) \\ X_*(T) &= \text{Hom}(\mathbb{G}_m, T) && \text{(group of cocharacters of } T). \end{aligned}$$

There is a perfect pairing

$$\langle \cdot, \cdot \rangle: X^*(T) \times X_*(T) \xrightarrow{\circ} \text{End}(\mathbb{G}_m) \simeq \mathbb{Z}.$$

For $\chi \in X^*(T)$ and $\lambda \in X_*(T)$, we have

$$\chi(\lambda(t)) = t^{\langle \chi, \lambda \rangle} \tag{138}$$

for all $t \in T(k)$.

21.5. Let $\varphi: \mathbb{A}^1 \setminus \{0\} \rightarrow X$ be a regular map of algebraic varieties. If φ extends to a regular map $\tilde{\varphi}: \mathbb{A}^1 \rightarrow X$, then the extension $\tilde{\varphi}$ is unique, and we say that $\lim_{t \rightarrow 0} \varphi(t)$ exists and set it equal to $\tilde{\varphi}(0)$. Similarly, we set $\lim_{t \rightarrow \infty} \varphi(t) = \lim_{t \rightarrow 0} \varphi(t^{-1})$ when it exists. (See Section 14.k.)

When X is affine, φ corresponds to a homomorphism of k -algebras

$$f \mapsto f \circ \varphi: \mathcal{O}(X) \rightarrow k[T, T^{-1}],$$

and $\lim_{t \rightarrow 0} \varphi$ exists if and only if $f \circ \varphi \in k[T]$ for all $f \in \mathcal{O}(X)$. Similarly, $\lim_{t \rightarrow \infty} \varphi$ exists if and only if $f \circ \varphi \in k[T^{-1}]$ for all $f \in \mathcal{O}(X)$.

21.6. An action $\mu: \mathbb{G}_m \times X \rightarrow X$ of \mathbb{G}_m on an affine algebraic variety X 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 $t \mapsto t^n$ (see 14.13).¹ Note that

$$\mathcal{O}(X)_m \cdot \mathcal{O}(X)_n \subset \mathcal{O}(X)_{m+n},$$

and so this is a gradation of $\mathcal{O}(X)$ as a k -algebra. For $x \in X(k)$, the orbit map

$$\mu_x: \mathbb{G}_m \rightarrow X, \quad t \mapsto tx,$$

corresponds to the homomorphism of coordinate rings

$$f = \sum_n f_n \mapsto \sum_n f_n(x) T^n: \mathcal{O}(X) \rightarrow k[T, T^{-1}],$$

and so $\lim_{t \rightarrow 0} tx$ exists if and only if $f_n(x) = 0$ for all $n < 0$. Similarly, $\lim_{t \rightarrow \infty} tx$ exists if and only if $f_n(x) = 0$ for all $n > 0$. Thus, x is fixed by the action of \mathbb{G}_m if and only if $\lim_{t \rightarrow 0} tx$ and $\lim_{t \rightarrow \infty} tx$ both exist.

Let $X(1)$ be the closed subscheme of X determined by the ideal generated by $\bigoplus_{n < 0} \mathcal{O}(X)_n$. Then

$$X(1)(k) = \{x \in X(k) \mid \lim_{t \rightarrow 0} tx = 0\}.$$

More generally, an element $x \in X(R) = \text{Hom}_{k\text{-alg}}(\mathcal{O}(X), R)$ defines an orbit map in $X(R[T, T^{-1}]) = \text{Hom}_{k\text{-alg}}(\mathcal{O}(X), R[T, T^{-1}])$, namely,

$$f = \sum_n f_n \mapsto \sum_n x(f_n) T^n: \mathcal{O}(X) \rightarrow R[T, T^{-1}].$$

The element x lies in $X(1)(R)$ if and only if the orbit map lies in the image of $X(R[T]) \rightarrow X(R[T, T^{-1}])$.

21.7. More generally, an action $\mu: T \times X \rightarrow X$ of a split torus T on an affine algebraic variety X defines a $X^*(T)$ -gradation on $\mathcal{O}(X)$,

$$\mathcal{O}(X) = \bigoplus_{\chi \in X^*(T)} \mathcal{O}(X)_\chi,$$

with $\mathcal{O}(X)_\chi$ the subspace on which T acts through the character χ .

¹We are letting \mathbb{G}_m act on $\mathcal{O}(X)$ “on the right”, i.e., $(tf)(x) = f(tx)$ for $t \in \mathbb{G}_m(k)$, $f \in \mathcal{O}(X)$, $x \in X(k)$. Thus $f(tx) = t^n(f(x))$ for $f \in \mathcal{O}(X)_n$.

For $\lambda \in X_*(T)$ and $x \in X(k)$, the map

$$\mu_x \circ \lambda: \mathbb{G}_m \rightarrow X, \quad t \mapsto \lambda(t) \cdot x$$

corresponds to the homomorphism of coordinate rings

$$f = \sum_{\chi} f_{\chi} \mapsto \sum_{\chi} f_{\chi}(x) T^{\langle \chi, \lambda \rangle}: \mathcal{O}(X) \rightarrow k[T, T^{-1}],$$

and so $\lim_{t \rightarrow 0} \lambda(t) \cdot x$ exists if and only if $f_{\chi}(x) = 0$ for all χ with $\langle \chi, \lambda \rangle < 0$. Thus

$$X(k)(\lambda) \stackrel{\text{def}}{=} \{x \in X(k) \mid \lim_{t \rightarrow 0} \lambda(t) \cdot x \text{ exists}\}$$

is the zero set of

$$\bigoplus_{\langle \chi, \lambda \rangle < 0} \mathcal{O}(X)_{\chi}$$

in $X(k)$; in particular, it is closed in $X(k)$. Similarly, $X(k)(-\lambda)$ is the zero set of $\bigoplus_{\langle \chi, \lambda \rangle > 0} \mathcal{O}(X)_{\chi}$.

We define $X(\lambda)$ to be the closed subscheme of X determined by the ideal generated by $\bigoplus_{\langle \chi, \lambda \rangle < 0} \mathcal{O}(X)_{\chi}$. The formation of $X(\lambda)$ commutes with extension of the base field. Moreover,

$$X(\lambda) \cap X(-\lambda) = X^{\lambda(\mathbb{G}_m)}, \tag{139}$$

and

$$\bigcap_{\lambda \in X_*(T)} X(\lambda) \cap X(-\lambda) = X^T.$$

Note that X^T is smooth if X is smooth (14.55).

The above discussion extends without difficulty to show that $X(\lambda)$ represents the functor sending a k -algebra R to the set of points $x \in X(R)$ such that the morphism $\mu_x \circ \lambda_R: \mathbb{G}_m R \rightarrow X_R$ extends to an R -morphism $\mathbb{A}_R^1 \rightarrow X_R$. In other words, the following diagram is cartesian

$$\begin{array}{ccc} X(\lambda)(R) & \hookrightarrow & X(R) \\ \downarrow & & \downarrow b \\ X(R[T]) & \xrightarrow{a} & X(R[T, T^{-1}]). \end{array} \tag{140}$$

The map a is defined by the inclusion $R[T] \hookrightarrow R[T, T^{-1}]$ and the map b is defined by the pairing $\mathbb{G}_m \times X \rightarrow X$.

d. Limits in algebraic groups

By a *cocharacter* of an algebraic group G we mean a homomorphism $\mathbb{G}_m \rightarrow G$ (in the literature, this is often called a one-parameter subgroup of G).

Let G be an algebraic group, and let $\lambda: \mathbb{G}_m \rightarrow G$ be a cocharacter of G . Then λ defines an action of \mathbb{G}_m on G :

$$(t, g) \mapsto \lambda(t) \cdot g \cdot \lambda(t)^{-1}: \mathbb{G}_m \times G \rightarrow G.$$

We define $P(\lambda)$ to be the closed subscheme $G(\lambda)$ of G attached to λ , as in (21.7). Thus $P(\lambda)(R)$ consists of the $g \in G(R)$ such that $t \mapsto t g t^{-1}: \mathbb{G}_m R \rightarrow G_R$ extends to a morphism $\mathbb{A}_R^1 \rightarrow G_R$. We let $Z(\lambda) = C_G(\lambda \mathbb{G}_m)$. Note that $Z(\lambda)$ is smooth (resp. connected) if G is smooth (resp. connected) (14.55, 18.44).

PROPOSITION 21.8. *Let G be an algebraic group over k , and let λ be a cocharacter of G . Then $P(\lambda)$ is an algebraic subgroup of G , and*

$$P(\lambda) \cap P(-\lambda) = Z(\lambda).$$

PROOF. For the first assertion it suffices to show that $P(\lambda)(R)$ is a subgroup of $G(R)$ for all R , but the maps a and b in (140) are group homomorphisms, and so this is obvious.

The second statement is a special case of (21.7). \square

PROPOSITION 21.9. *The subfunctor*

$$R \rightsquigarrow \{g \in G(R) \mid \lim_{t \rightarrow 0} t \cdot g = 1\}$$

of G is represented by a normal algebraic subgroup $U(\lambda)$ of $P(\lambda)$.

PROOF. Clearly, $U(\lambda)(R)$ is the kernel of

$$P(\lambda)(R) \rightarrow G(R[T]) \xrightarrow{T \mapsto 0} G(R). \quad \square$$

EXAMPLE 21.10. Let $G = \mathrm{GL}_2$, and let λ be the homomorphism $t \mapsto \mathrm{diag}(t, t^{-1})$. 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 $\lim_{t \rightarrow 0} \begin{pmatrix} a & bt^2 \\ \frac{c}{t^2} & d \end{pmatrix}$ exists if and only if $c = 0$, in which case the limit equals $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. Therefore,

$$\begin{aligned} P(\lambda) &= \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, & U(\lambda) &= \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}, & Z(\lambda) &= \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\}; \\ P(-\lambda) &= \left\{ \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \right\}, & U(-\lambda) &= \left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\}, & Z(-\lambda) &= Z(\lambda). \end{aligned}$$

In more detail, $\mathcal{O}(\mathrm{GL}_2) = k[T_{11}, T_{12}, T_{21}, T_{22}]$ with T_{12} of weight 2, T_{21} of weight -2 , and T_{11} and T_{22} of weight 0. Thus $P(\lambda)$ is defined by the ideal (T_{21}) and $U(\lambda)$ by the ideal $(T_{11} - 1, T_{22} - 1, T_{21})$.

EXAMPLE 21.11. Let $G = \mathrm{SL}_2$, and let λ be the homomorphism $t \mapsto \mathrm{diag}(t, t^{-1})$. Then

$$P(\lambda) = \left\{ \begin{pmatrix} a & c \\ 0 & a^{-1} \end{pmatrix} \right\}, \quad U(\lambda) = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right\}, \quad Z(\lambda) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}.$$

EXAMPLE 21.12. Let $G = \mathrm{GL}_3$, and let λ be the homomorphism $t \mapsto \mathrm{diag}(t^{m_1}, t^{m_2}, t^{m_3})$ with $m_1 \geq m_2 \geq m_3$. Then

$$\begin{pmatrix} t^{m_1} & 0 & 0 \\ 0 & t^{m_2} & 0 \\ 0 & 0 & t^{m_3} \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} t^{-m_1} & 0 & 0 \\ 0 & t^{-m_2} & 0 \\ 0 & 0 & t^{-m_3} \end{pmatrix} = \begin{pmatrix} a & t^{m_1-m_2}b & t^{m_1-m_3}c \\ t^{m_2-m_1}d & e & t^{m_2-m_3}f \\ t^{m_3-m_1}g & t^{m_3-m_2}h & i \end{pmatrix}.$$

If $m_1 > m_2 > m_3$, then

$$P(\lambda) = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\}, \quad U(\lambda) = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad Z(\lambda) = \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\};$$

$$P(-\lambda) = \left\{ \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix} \right\}, \quad U(-\lambda) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix} \right\}, \quad Z(-\lambda) = Z(\lambda).$$

If $m_1 = m_2 > m_3$, then

$$P(\lambda) = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix} \right\}, \quad U(\lambda) = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad Z(\lambda) = \left\{ \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\}$$

$$P(-\lambda) = \left\{ \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix} \right\}, \quad U(-\lambda) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ * & * & 1 \end{pmatrix} \right\}, \quad Z(-\lambda) = Z(\lambda).$$

Let G be an algebraic group over k , and let $\lambda: \mathbb{G}_m \rightarrow G$ be a cocharacter of G . Then \mathbb{G}_m acts on the Lie algebra \mathfrak{g} of G through $\text{Ad} \circ \lambda$. 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 21.13. *Let G be a smooth algebraic group over k , and let $\lambda: \mathbb{G}_m \rightarrow G$ be a cocharacter of G .*

- $P(\lambda)$, $Z(\lambda)$, and $U(\lambda)$ are smooth algebraic subgroups of G , and $U(\lambda)$ is a unipotent normal subgroup of $P(\lambda)$.
- The multiplication map $U(\lambda) \times Z(\lambda) \rightarrow P(\lambda)$ is an isomorphism of algebraic groups.
- $\text{Lie}(U(-\lambda)) = \mathfrak{g}_-$, $\text{Lie}(Z(\lambda)) = \mathfrak{g}_0$, $\text{Lie}(U(\lambda)) = \mathfrak{g}_+$.
- The multiplication map $U(-\lambda) \times P(\lambda) \rightarrow G$ is an open immersion.
- If G is connected, then so also are $P(\lambda)$, $Z(\lambda)$, and $U(\lambda)$.

PROOF. For the proof, we may replace k with its algebraic closure.

We first prove the theorem for $G = \text{GL}_V$. According to (14.12), there exists a basis for V such that $\lambda(\mathbb{G}_m) \subset \mathbb{D}_n$, say,

$$\lambda(t) = \text{diag}(t^{m_1}, \dots, t^{m_n}), \quad m_1 \geq m_2 \geq \dots \geq m_n.$$

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. It is similarly obvious that $U(\lambda)$ is smooth, connected, and unipotent, and we already know that $Z(\lambda)$ is smooth and connected. For (b) it suffices to prove that the map is an isomorphism of algebraic varieties, which is obvious. Statement (c) can be proved by a direct calculation. From (c) we deduce that the multiplication map $U(-\lambda) \times P(\lambda) \rightarrow G$ 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, $U(-\lambda) \times P(\lambda) \rightarrow U(-\lambda) \cdot P(\lambda)$ 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 (1.52).

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 notations,

$$P_G(\lambda) = P_H(\lambda) \cap G, \quad U_G(\lambda) = U_H(\lambda) \cap G, \quad Z_G(\lambda) = Z_H(\lambda) \cap G$$

because this is true for the functors they define. We let $P_G(\lambda)' = P_G(\lambda)_{\mathrm{red}}$ and $U_G(\lambda)' = U_G(\lambda)_{\mathrm{red}}$, and we first prove (c) for these groups. We have

$$\mathrm{Lie}(P_G(\lambda)') \subset \mathrm{Lie}(P_H(\lambda)) \cap \mathfrak{g} = \mathfrak{g}_0(\lambda) + \mathfrak{g}_+(\lambda), \tag{141}$$

as we already know (c) for H . Similarly,

$$\mathrm{Lie}(U_G(\pm\lambda)') \subset \mathfrak{g}_{\pm}(\lambda). \tag{142}$$

From (d) for H , we deduce that

$$U \stackrel{\mathrm{def}}{=} U_H(-\lambda) \cdot P_H(\lambda) \cap G$$

is an open subset of G containing e .

Apply 4.19 to obtain a representation $r: H \rightarrow \mathrm{GL}_V$ and a line $L = kv$ in V such that G is the algebraic subgroup of H stabilizing L . Let $g \in U(k)$. Using that we know (b) and (d) for H , we write $g = xyz$ with $x \in U_H(-\lambda)$, $y \in U_H(\lambda)$, and $z \in Z_H(\lambda)$. We have $r(g)v = cv$ for some $c \in k^\times$; moreover, v is an eigenvector for \mathbb{G}_m acting on V via $r \circ \lambda$ because $\mathrm{Im}(\lambda) \subset G$. It follows that for $t \in k^\times$,

$$c \cdot r(\lambda(t) \cdot x^{-1} \cdot \lambda(t)^{-1})v = r(\lambda(t) \cdot y \cdot \lambda(t)^{-1}z)v. \tag{143}$$

By an easy computation in H , with a basis as at the beginning of the proof, we see that the coefficient of v on the right is a polynomial function of t and on the left is a polynomial function of t^{-1} . These polynomial functions must be constant. It follows that the left hand side equals cv and the right hand side $r(z)v$, and so $z \in G(k)$. Also $r(x)v = r(y)v = v$, and so $x, y \in G(k)$. We have shown that $U_G(-\lambda)' \cdot P_G(\lambda)'$ contains the open subset U of G , and so

$$\dim U_G(-\lambda)' + \dim P_G(\lambda)' = \dim G = \dim \mathfrak{g}_-(\lambda) + (\dim \mathfrak{g}_0(\lambda) + \dim \mathfrak{g}_+(\lambda)).$$

We conclude that equality holds in (141) and (142), and so (c) holds for G and the groups $P_G(\lambda)'$ and $U_G(\lambda)'$.

It follows that

$$\mathrm{Lie}(P_G(\lambda)') = \mathrm{Lie}(P_H(\lambda)) \cap \mathfrak{g}, \tag{144}$$

but this also equals $\mathrm{Lie}(P_G(\lambda))$ (see 12.12). Therefore

$$\dim \mathrm{Lie}(P_G(\lambda)) = \dim \mathrm{Lie}(P_G(\lambda)_{\mathrm{red}}) = \dim P_G(\lambda)_{\mathrm{red}} = \dim P_G(\lambda),$$

and so $P_G(\lambda)$ is smooth. Similarly, $U_G(\lambda)$ is smooth. Now statement (c) implies (d) as in the case of GL_n , and statement (d) obviously implies (e). Finally, $U_G(\lambda)$ is a unipotent normal algebraic subgroup of G , because it is the intersection with G of such a group, namely, $U_H(\lambda)$. □

REMARK 21.14. In the situation of the theorem:

(a) $P(\lambda)$ is the unique smooth algebraic subgroup of G such that

$$P(\lambda)(k^{\text{al}}) = \{g \in G(k^{\text{al}}) \mid \lim_{t \rightarrow 0} t \cdot g \text{ exists (in } G(k^{\text{al}}))\}. \tag{145}$$

(b) $U(\lambda)$ is the unique smooth algebraic subgroup of $P(\lambda)$ such that

$$U(\lambda)(k^{\text{al}}) = \{g \in P(\lambda)(k^{\text{al}}) \mid \lim_{t \rightarrow 0} t \cdot g = 1\}. \tag{146}$$

PROPOSITION 21.15. *The subgroup variety $U(\lambda)$ is unipotent, and the weights of \mathbb{G}_m on $\text{Lie}(U(\lambda))$ are strictly positive integers. If G is connected and solvable, then $\text{Lie}(U(\lambda))$ contains all the strictly positive weight spaces for \mathbb{G}_m on $\text{Lie}(G)$.*

PROOF. Choose a faithful representation (V, r) of G . There exists a basis for V such that $r(\lambda(\mathbb{G}_m)) \subset \mathbb{D}_n$ (14.12), say, $\lambda \circ r(t) = \text{diag}(t^{m_1}, \dots, t^{m_n})$, $m_1 \geq m_2 \geq \dots \geq m_n$. Then $U(\lambda) \subset \mathbb{U}_n$, from which the first statement follows.

Now assume that G is connected and solvable. Then there is a unique connected normal unipotent subgroup variety G_u of G such that G/G_u is a torus (17.37). We argue by induction on $\dim G_u$. If $\dim G_u = 0$, then G is a torus, and there are no nonzero weight spaces.

Thus, we may assume that $\dim G_u > 0$. Then there exists a surjective homomorphism $\varphi: G_u \rightarrow \mathbb{G}_a$ (15.23) and

$$\varphi(\lambda(t) \cdot g \cdot \lambda(t)^{-1}) = t^n \cdot \varphi(g), \quad g \in G_u(k), \quad t \in \mathbb{G}_m(k),$$

for some $n \in \mathbb{Z}$.

If $n \leq 0$, then the map

$$t \mapsto \varphi(\lambda(t) \cdot g \cdot \lambda(t)^{-1}): \mathbb{G}_m \rightarrow \mathbb{G}_a$$

doesn't extend to \mathbb{A}^1 unless $\varphi(g) = 0$. Hence $U(\lambda) \subset \text{Ker}(\varphi)$, and we can apply induction.

If $n > 0$, then $\varphi(U(\lambda)) = \mathbb{G}_a$, and we can again apply induction to $\text{Ker}(\varphi)$. □

COROLLARY 21.16. *If G is connected and solvable, then G is generated by its subgroups $U(\lambda)$, $Z(\lambda)$, and $U(-\lambda)$ (as a connected group variety).*

PROOF. Their Lie algebras span \mathfrak{g} , and so we can apply (12.13). □

PROPOSITION 21.17. *Let $\varphi: G \rightarrow G'$ be a separable surjective homomorphism of 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. See Springer p.235. □

NOTES. Modulo nilpotents, Theorem 21.13 was announced in Borel and Tits 1978. Our proof is adapted from that in Springer 1998, 13.4.2. Specifically, Springer defines $P(\lambda)$ as a *subgroup variety* of $G_{k^{\text{al}}}$ by describing its k^{al} -points, and then deduces from (144) that $P(\lambda)$ is defined over k . We define $P(\lambda)$ directly as an *algebraic subgroup* of G by describing its points in every k -algebra R , and then deduce from (144) that it is smooth.

For a generalization of the theorem to nonsmooth algebraic groups G , see Conrad et al. 2010, 2.1.8.

e. Actions of tori on a projective space

LEMMA 21.18. *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 $X \setminus H$, and hence of dimension 0, contradicting the hypothesis. The rest of the statement is a special case of Krull's principal ideal theorem (see, for example, AG 6.43). \square

LEMMA 21.19. *Let T be a split torus, and let (V, r) be a finite-dimensional representation of T . There exists a cocharacter $\lambda: \mathbb{G}_m \rightarrow T$ 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. Choose λ so that the integers $\langle \chi_i, \lambda \rangle$, $i = 1, \dots, m$, are distinct (there exists such a λ in $X_*(T)_{\mathbb{Q}}$ because we only have to avoid the finitely many hyperplanes $\langle \chi_i - \chi_j \rangle^{\perp}$, $i \neq j$, and then some multiple of λ lies in $X_*(T)$). Now $\lambda(\mathbb{G}_m)$ and T have the same eigenvectors in V , and hence the same fixed points in $\mathbb{P}(V)$. \square

PROPOSITION 21.20. *Let T be a torus, and let (V, r) be a finite-dimensional representation of T . Let X be a closed subvariety of $\mathbb{P}(V)$ stable under the action of T on $\mathbb{P}(V)$ defined by r . In $X(k^{\text{al}})$ 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 21.19 allows us to replace T with \mathbb{G}_m . We prove the statement by induction on $d + n$ where $d = \dim X$ and $n + 1 = \dim V$. We may suppose that $d > 0$.

Let $\{e_0, \dots, e_n\}$ 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 $W = \langle e_1, \dots, e_n \rangle$. By induction, we may suppose that $X \not\subset \mathbb{P}(W)$. By induction again, \mathbb{G}_m has at least d fixed points in $X \cap \mathbb{P}(W)$. Let $[v] \in X \setminus \mathbb{P}(W)$, and write

$$v = e_0 + a_1e_1 + \dots + a_n e_n, \quad a_0 \neq 0.$$

If $[v]$ is fixed by the action of \mathbb{G}_m , we have at least $d + 1$ fixed points. Otherwise, as \mathbb{G}_m acts on the affine space $D(e_0^{\vee}) = \mathbb{P}(V) \setminus \mathbb{P}(W)$ with nonnegative weights $0, \dots, m_n - m_0$, there exists a fixed point $\lim_{t \rightarrow 0} t[v]$ in $D(e_0^{\vee}) \cap X$ (14.46), and so again we have at least $d + 1$ fixed points. \square

COROLLARY 21.21. *Let P be a parabolic subgroup of a smooth connected algebraic group G and let T be a torus in G . In $(G/P)(k^{\text{al}})$ there are at least $1 + \dim(G/P)$ points fixed by T .*

PROOF. There exists a representation $G \rightarrow \text{GL}_V$ of V and an $o \in \mathbb{P}(V)$ such that the map $g \mapsto go: G \rightarrow \mathbb{P}(V)$ defines a G -equivariant isomorphism of G/P onto the orbit $G \cdot o$ (see the proof of 9.28). Now $G \cdot o$ is a complete subvariety of $\mathbb{P}(V)$ to which we can apply the proposition. \square

EXAMPLE 21.22. When \mathbb{G}_m acts on \mathbb{P}^n according to the rule

$$t(x_0 : \cdots : x_i : \cdots : x_n) = (x_0 : \cdots : t^i x_i : \cdots : t^n x_n),$$

the fixed points are P_0, \dots, P_n with $P_i = (0 : \cdots : 0 : 1 : 0 : \cdots : 0)$.

ASIDE 21.23. 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. We may suppose that the action has only isolated fixed points (otherwise X^T is infinite). For some $t \in T(k)$, X^T is the set of fixed points of t (cf. 18.36), and so

$$\#X^T = \sum_{i=0}^{2 \dim X} (-1)^i \operatorname{Tr}(t | H^i(X))$$

(Lefschetz trace formula). On letting $t \rightarrow 1$, we see that $\operatorname{Tr}(t | H^i(X)) = \dim H^i(X)$. 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 (Carrell 2002, 4.2.1). Therefore, the odd-degree groups vanish when X^T is finite. On the other hand $\dim H^{2i}(X) \geq 1$ for all i because the class of an intersection of hyperplane sections gives a nonzero element of the group. Therefore,

$$\#X^T = \sum_{0 \leq i \leq \dim(X)} \dim H^{2i}(X) \geq \dim(X) + 1.$$

f. Homogeneous curves

21.24. Let C be a smooth complete curve over k . The local ring \mathcal{O}_P at a point $P \in |C|$ is a discrete valuation ring with field of fractions $k(C)$ such that $k \subset \mathcal{O}_P$, 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 , we have $\mathcal{O}_C(U) = \bigcap_{P \in U} \mathcal{O}_P$. Thus, we can recover C from its function field $k(C)$. In particular, two smooth complete connected curves over k are isomorphic if they have isomorphic function fields.

21.25. According to the preceding remark, a smooth complete 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 (see, for example, my notes *Fields and Galois Theory*).

21.26. Let C be an curve (i.e., algebraic variety of dimension one) over k . If $C_{k^{\text{al}}} \approx \mathbb{P}^1$ and $C(k) \neq \emptyset$, then $C \approx \mathbb{P}^1$ (the hypothesis implies that C is a smooth complete curve over k of genus 0; projecting from a point $P \in C(k)$ defines an isomorphism from C onto \mathbb{P}^1).

PROPOSITION 21.27. *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 connected *solvable* group variety G . Then it admits a nontrivial action by a connected commutative group variety, and hence by \mathbb{G}_a or \mathbb{G}_m (17.38).

If \mathbb{G}_a acts nontrivially on C , then, for some $x \in C(k)$, the orbit map $\mu_x: \mathbb{G}_a \rightarrow C$ 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 (21.25). Hence $C \approx \mathbb{P}^1$ (21.24). The same argument applies with \mathbb{G}_m for \mathbb{G}_a .

We now prove the general case. If all Borel subgroups B of G act trivially on C , then $G(k) \stackrel{18.37}{=} \bigcup B(k)$ acts trivially on C . 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 . \square

21.28. There are alternative proofs of the proposition. 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).

g. The automorphism group of the projective line

Recall that

$$\mathbb{P}^1(R) = \{P \subset R^2 \mid P \text{ is a direct summand of } R^2 \text{ of rank } 1\}$$

for any k -algebra R (AG p.144). Moreover,

$$\begin{aligned} \mathrm{GL}_2(R) &= \mathrm{GL}(2, R) \\ \mathrm{PGL}_2 &= \mathrm{GL}_2 / \mathbb{G}_m \\ \underline{\mathrm{Aut}}(\mathbb{P}^1)(R) &= \mathrm{Aut}_R(\mathbb{P}_R^1). \end{aligned}$$

For each k -algebra R , the natural action of $\mathrm{GL}_2(R)$ on R^2 defines an action of $\mathrm{GL}_2(R)$ on $\mathbb{P}^1(R)$, and hence a homomorphism $\mathrm{GL}_2 \rightarrow \underline{\mathrm{Aut}}(\mathbb{P}^1)$. This factors through PGL_2 .

PROPOSITION 21.29. *The homomorphism $\mathrm{PGL}_2 \rightarrow \underline{\mathrm{Aut}}(\mathbb{P}^1)$ just defined is an isomorphism.*

This follows from the next two lemmas.

LEMMA 21.30. *Let $\alpha \in \underline{\mathrm{Aut}}(\mathbb{P}^1)(R) = \mathrm{Aut}(\mathbb{P}_R^1)$. If*

$$\alpha(0_R) = 0_R, \quad \alpha(1_R) = 1_R, \quad \alpha(\infty_R) = \infty_R,$$

then $\alpha = \mathrm{id}$.

PROOF. Recall that $\mathbb{P}_R^1 = U_0 \cup U_1$ with $U_0 = \mathrm{Spec} R[T]$ and $U_1 = \mathrm{Spec} R[T^{-1}]$. The diagram

$$U_0 \leftrightarrow U_0 \cap U_1 \leftrightarrow U_1$$

corresponds to

$$R[T] \leftrightarrow R[T, T^{-1}] \leftrightarrow R[T^{-1}].$$

The automorphism α preserves U_0 and U_1 , and its restrictions to U_0 and U_1 correspond to R -algebra homomorphisms

$$\begin{aligned} T &\mapsto P(T) = a_0 + a_1 T + \tilde{P}(T)T^2 \\ T^{-1} &\mapsto Q(T^{-1}) = b_0 + b_1 T^{-1} + \tilde{Q}(T^{-1})T^{-2} \end{aligned}$$

such that

$$P(T)Q(T^{-1}) = 1 \quad (\text{equality in } R[T, T^{-1}]). \tag{147}$$

As $\alpha(0_R) = 0_R$, the coefficient $a_0 = 0$, and as $\alpha(\infty_R) = \infty_R$, the coefficient $b_0 = 0$. The equality (147) implies that

$$\tilde{P}(T) = 0 = \tilde{Q}(T).$$

Finally, $a_1 = 1$ and $P(T) = T$ because $\alpha(1_R) = 1_R$. □

LEMMA 21.31. *Let P_0, P_1, P_2 be points on \mathbb{P}^1 with coordinates in R that remain distinct in $\mathbb{P}^1(\kappa(x))$ for all $x \in \text{spm}(R)$; then there exists an $\alpha \in \text{PGL}_2(R)$ such that $\alpha \cdot 0_R = P_0$, $\alpha \cdot 1_R = P_1$, and $\alpha \cdot \infty_R = P_2$.*

PROOF. Let S be a faithfully flat extension of R ; then each element of $\text{GL}_2(B)$, fixing the points $0_S, 1_S, \infty_S \in \mathbb{P}^1(S)$, already lies in $\mathbb{G}_m(B)$. Therefore there exists at most one $g \in \text{PGL}_2(S)$ with $g \cdot 0_R = P_0$, $g \cdot 1_R = P_1$, and $g \cdot \infty_R = x_\infty$. The direct summands P_0, P_1, P_∞ of R^2 are projective, hence locally free. Therefore, we can find an open covering $\text{spm}(R) = \bigcup_{i=1}^n \text{spm}(R_{f_i})$ such that $(P_0)_{f_i}, (P_1)_{f_i}, (P_\infty)_{f_i}$ are free for $i = 1, \dots, n$. Thus

$$(P_0)_{f_i} = R_{f_i} \begin{pmatrix} y_{0i} \\ x_{0i} \end{pmatrix}, \quad (P_1)_{f_i} = R_{f_i} \begin{pmatrix} y_{1i} \\ x_{1i} \end{pmatrix}, \quad (P_2)_{f_i} = R_{f_i} \begin{pmatrix} y_{2i} \\ x_{2i} \end{pmatrix}.$$

For each $\alpha \in \text{spm}(A_{f_i})$, by assumption,

$$(y_{0i}x_{\infty i} - y_{\infty i}x_{0i})(\alpha) \neq 0.$$

Therefore, $(y_{0i}x_{\infty i} - y_{\infty i}x_{0i})$ is invertible, and it follows that

$$H_i \stackrel{\text{def}}{=} \begin{pmatrix} y_{0i} & y_{\infty i} \\ x_{0i} & y_{\infty i} \end{pmatrix} \in \text{GL}_2(A_{f_i}). \quad \square$$

h. Review of Borel subgroups

In this section, k is algebraically closed.

We list the properties of Borel subgroups that we shall need to use in the next section. In the following G is a connected group variety, B is a Borel subgroup of G , and T is a maximal torus in G .

21.32. All Borel subgroups in G are conjugate by an element of $G(k)$ (see 18.12).

21.33. All maximal tori in G are conjugate by an element of $G(k)$ (18.14).

21.34. If B is nilpotent, then $G = B$ (18.27).

21.35. The only Borel subgroup of G normalized by B is B itself (18.39).

21.36. The connected centralizer $C_G(T)^\circ$ of T is contained in every Borel subgroup containing T (18.33).

21.37. The group $N_G(T)(k)$ acts transitively on the Borel subgroups containing T (18.15).

21.38. The reduced normalizer $N_G(B)_{\text{red}}$ of B contains B as a subgroup of finite index and is equal to its own normalizer. See (18.53) for a stronger result.

21.39. The centralizer of a torus S in G is smooth (16.23); therefore

$$\dim C_G(S) \stackrel{1.22}{=} \dim \text{Lie}(C_G(S)) \stackrel{12.31}{=} \dim \text{Lie}(G)^S.$$

i. Criteria for a group variety to have semisimple rank 1.

Throughout this section, k is algebraically closed.

THEOREM 21.40. *The following conditions on a connected group variety G over k and a Borel pair (B, T) are equivalent:*

- (a) *the semisimple rank of G is 1;*
- (b) *T lies in exactly two Borel subgroups;*
- (c) $\dim(G/B) = 1$;
- (d) *there exists an isogeny $G/RG \rightarrow \mathrm{PGL}_2$.*

The proof of this will occupy the rest of this section. Throughout, G is a connected group variety over k (algebraically closed). In proving the theorem, we may replace G with G/RG , and so assume that $RG = e$.

(a) \Rightarrow (b): A MAXIMAL TORUS IN A GROUP OF SEMISIMPLE RANK 1 LIES IN EXACTLY TWO BOREL SUBGROUPS

Let G be connected group variety of semisimple rank 1. Let T be a split maximal torus in G , and fix an isomorphism $\lambda: \mathbb{G}_m \rightarrow T$. Call a Borel subgroup positive if it contains $U(\lambda)$ and negative if it contains $U(-\lambda)$.

LEMMA 21.41. *The following hold:*

- (a) *T lies in at least two Borel subgroups, one positive and one negative.*
- (b) *If B (resp. B') is a positive (resp. negative) Borel subgroup containing T , then every Borel subgroup containing T lies in the subgroup generated by B and B' .*
- (c) *No Borel subgroup containing T is both positive and negative.*
- (d) *The normalizer of T in G contains an element acting on T as $t \mapsto t^{-1}$.*

PROOF. (a) The subgroup variety $U(\lambda)$ is connected, unipotent, and normalized by T . Therefore $TU(\lambda)$ is a connected solvable subgroup variety of G , and so lies in a Borel subgroup, which is positive (by definition). A similar argument applies to $U(-\lambda)$.

(b) Apply Corollary 21.16 with G equal to a Borel subgroup containing T .

(c) Otherwise (b) would imply that every Borel subgroup containing T is contained in a single Borel subgroup, which contradicts (a).

(d) The normalizer of T in G acts transitively on the set of Borel subgroups containing T (21.37). Any element taking a negative Borel subgroup to a positive Borel subgroup acts as $t \mapsto t^{-1}$ on T . \square

LEMMA 21.42. *Each maximal torus of G lies in exactly two Borel subgroups, one positive and one negative.*

PROOF. Let T be a maximal torus, and choose an identification of it with \mathbb{G}_m . We use induction on the common dimension d of the Borel subgroups of G (21.32).

If $d = 1$, then the Borel subgroups are commutative, and so G is solvable (21.34), contradicting the hypothesis.

Next suppose that $d = 2$. We already know that T lies in a positive and in a negative Borel subgroup. Suppose that T lies in two positive Borel subgroups B and B' . If $B_u \neq B'_u$, then they are distinct subgroups of $U(\lambda)$, and therefore generate a unipotent subgroup of

dimension > 1 . This implies that the Borel subgroups of G are unipotent, hence nilpotent, hence equal G , which contradicts the hypothesis. Therefore $B_u = B'_u$, and so

$$B \stackrel{17.37}{=} B_u \cdot T = B'_u \cdot T \stackrel{17.37}{=} B'.$$

Now suppose that $d \geq 3$. Let B be a positive Borel subgroup containing T . Let $N = N_G(B)_{\text{red}}$, and consider the action of B on G/N . Because of (21.35), B has a unique fixed point in G/N . Let O be an orbit of B in G/N of minimum nonzero dimension. The closure of O in G/N is a union of orbits of lower dimension, and so O is either a projective variety or a projective variety with one point omitted. This forces O to be a curve, because otherwise it would contain a complete curve, in contradiction with Theorem 21.28. Therefore, there exists a Borel subgroup B' such that $B \cap N_G(B')$ has codimension 1 in B .

Thus $H \stackrel{\text{def}}{=} (B \cap B')^\circ$ has codimension 1 in each of B and B' . Either $H = B_u = B'_u$ or it contains a torus. In the first case, $\langle B, B' \rangle$ normalizes H , and a Borel subgroup in $\langle B, B' \rangle/H$ has no unipotent part, and so $\langle B, B' \rangle$ is solvable, which is impossible.

Therefore H contains a torus. We conclude that B and B' are the only Borel subgroups of $\langle B, B' \rangle$ containing T , and one is positive and one negative. Then Lemma 21.41(d) shows that B and B' are interchanged by an element of $N_{\langle B, B' \rangle}(T)$ that acts a $t \mapsto t^{-1}$ on T . This implies that B' is negative as a Borel subgroup of G . Finally Lemma 21.41(b) implies that every Borel subgroup of G containing T lies in $\langle B, B' \rangle$, hence equals B or B' \square

(b) \Rightarrow (c): IF T LIES IN EXACTLY TWO BOREL SUBGROUPS, THEN $\dim(G/B) = 1$

Let (B, T) be a Borel pair in G , and let $N = N_G(B)_{\text{red}}$. Then $G/B \rightarrow G/N$ is a finite covering (21.38). As N contains B , the quotient G/N is complete, and as N is its own normalizer (21.38), it fixes only one point in B/N , and so the stabilizers of distinct points of G/N are the normalizers of distinct Borel subgroups. The fixed points of T in G/N correspond to the Borel subgroups that T normalizes, and hence contain T . Therefore T has exactly 2 fixed points in G/N . As G is nonsolvable, G/B (hence also G/N) has dimension ≥ 1 . In fact, G/N has dimension 1, because otherwise Corollary 21.21 would show that T has more than 2 fixed points.

(c) \Rightarrow (d): IF $\dim(G/B) = 1$, THEN THERE EXISTS AN ISOGENY $G/RG \rightarrow \text{PGL}_2$

If $\dim(G/B) = 1$, then G/B is a smooth complete curve. Because G acts nontrivially on G/B , it is isomorphic to \mathbb{P}^1 (21.27). On choosing an isomorphism $G/B \rightarrow \mathbb{P}^1$, we get an action of G on \mathbb{P}^1 , and hence a homomorphism $G \rightarrow \underline{\text{Aut}}(\mathbb{P}^1)$. On combining this with the canonical isomorphism $\underline{\text{Aut}}(\mathbb{P}^1) \rightarrow \text{PGL}_2$, we get a surjective homomorphism $G \rightarrow \text{PGL}_2$ whose kernel is the intersection of the Borel subgroups containing T . This gives the required isogeny.

(d) \Rightarrow (a) IF THERE EXISTS AN ISOGENY $G/RG \rightarrow \text{PGL}_2$, THEN G HAS SEMISIMPLE RANK 1

This is obvious.

NOTES. This section follows Allcock 2009.

j. Split reductive groups of semisimple rank 1.

In this section, k is arbitrary.

LEMMA 21.43. *Let (G, T) be a split reductive group of semisimple rank 1 over k . Then there exists a Borel subgroup B of G containing T .*

PROOF. First let (G, T) be a split semisimple group of rank 1. Then $R(G_{k^{\text{al}}}) = e$, and so there exists an isogeny $G_{k^{\text{al}}} \rightarrow \text{PGL}_2$. Hence G has dimension 3 and any Borel subgroup has dimension 2. Choose an isomorphism $\lambda: \mathbb{G}_m \rightarrow T$. Then $P(\lambda) = T \cdot U(\lambda)$ 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).

Now let (G, T) be a split reductive group of semisimple rank 1. The derived group G' of G has semisimple of rank ≤ 1 (21.2). If G' had rank 0, then it would be commutative, and G would be solvable, contradicting the hypotheses. Thus, G' is a split semisimple group of rank 1. Let T' be a maximal torus of G' contained in T , and choose an isomorphism $\lambda: \mathbb{G}_m \rightarrow T'$. Then $T \cdot U(\lambda)$ and $T \cdot U(-\lambda)$ are Borel subgroups of G containing T . \square

THEOREM 21.44. *Let G be a split reductive group over k of semisimple rank 1, and let B be a Borel subgroup of G . Then G/B is isomorphic to \mathbb{P}^1 , and the homomorphism*

$$G \rightarrow \underline{\text{Aut}}(G/B) \simeq \text{PGL}_2$$

is surjective with kernel $Z(G)$.

The algebraic group $G_{k^{\text{al}}}$ is reductive of semisimple rank 1, and $B_{k^{\text{al}}}$ is a Borel subgroup of $G_{k^{\text{al}}}$. Moreover, $(G/B)_{k^{\text{al}}} \simeq G_{k^{\text{al}}}/B_{k^{\text{al}}} \approx \mathbb{P}^1$, and so $G/B \approx \mathbb{P}^1$ (21.26). The map $G \rightarrow \underline{\text{Aut}}(G/B)$ is surjective because this is true after a base change to k^{al} . It remains to prove that the kernel of $G \rightarrow \underline{\text{Aut}}(G/B)$ is $Z(G)$. It suffices to prove this with k algebraically closed, and so for the remainder of the proof, k is algebraically closed.

Let T be a maximal torus in G , and write B^+ and B^- for the two Borel subgroups containing T (see 21.29). We choose the isomorphism $G/B^+ \rightarrow \mathbb{P}^1$ so that B^+ fixes 0 and B^- fixes ∞ . The action of G on $G/B^+ \simeq \mathbb{P}^1$ determines a homomorphism $\varphi: G \rightarrow \underline{\text{Aut}}(\mathbb{P}^1) \simeq \text{PGL}_2$. Let B^0 denote the Borel subgroup of PGL_2 fixing 0.

As G is not solvable, the unipotent part B_u^+ of B^+ is nonzero (18.27). As $R_u(G) = 0$, the homomorphism $B_u^+ \rightarrow B_u^0$ has finite kernel. Now B_u^+ is a smooth connected unipotent group of dimension 1, and hence is isomorphic to \mathbb{G}_a (17.18). Choose an isomorphism $i^+: \mathbb{G}_a \rightarrow B_u^+$; then the action of T on B_u^+ by inner automorphisms corresponds to the action of T on \mathbb{G}_a defined by a character $\alpha^+: T \rightarrow \mathbb{G}_m$ of T :

$$i^+(\alpha^+(t) \cdot x) = t \cdot i^+(x) \cdot t^{-1}, \quad t \in T(R), \quad x \in \mathbb{G}_a(R) = R. \quad (148)$$

This character does not depend on i^+ and is called the **root of G with respect to (B^+, T)** . Similarly, there is a root α^- of G with respect to (B^-, T) defined by the same equation (14) but with $-$ for $+$:

$$i^-(\alpha^-(t) \cdot x) = t \cdot i^-(x) \cdot t^{-1}, \quad t \in T(R), \quad x \in \mathbb{G}_a(R) = R. \quad (149)$$

PROPOSITION 21.45. *Let n be an element of $G(k)$ that normalizes T , but doesn't centralize it. Then*

$$\begin{aligned} nB^+n^{-1} &= B^- \\ \alpha^+ \circ (\text{inn}(n)|_T) &= \alpha^- = -\alpha^+. \end{aligned}$$

PROOF. The first equality was proved in (21.41d). The second equality can be proved by a direct calculation: let i^- denote the isomorphism

$$\text{inn}(n) \circ i^+ : \mathbb{G}_a \rightarrow B_u^-;$$

for $x \in B_u^+(R)$ and $t \in T(R)$,

$$\begin{aligned} i^+(\alpha^+(ntn^{-1}) \cdot x) &= ntn^{-1} \cdot i^+(x) \cdot nt^{-1}n^{-1} && \text{apply (148)} \\ &= nt \cdot i^-(x) \cdot t^{-1}n^{-1} && \text{definition of } i^- \\ &= n \cdot i^-(\alpha^-(t) \cdot x) \cdot n^{-1} && \text{apply (149)} \\ &= i^+(\alpha^-(t) \cdot x), \end{aligned}$$

and so

$$\alpha^+(ntn^{-1}) = \alpha^-(t).$$

On the other hand, because B^+ is not nilpotent (18.27), $\alpha^+ \neq 0$. Because $\text{Ker } \alpha^+$ is equal to the centre of $B^+ = i^+(\mathbb{G}_a) \cdot T$, it is also equal to the centre of G (18.50). On the other hand, $\text{inn}(n)$ induces the identity map on $\text{Ker}(\alpha^+)$, and gives a commutative diagram:

$$\begin{array}{ccccccc} e & \longrightarrow & \text{Ker}(\alpha^+) & \longrightarrow & T & \xrightarrow{\alpha^+} & \mathbb{G}_m & \longrightarrow & e \\ & & \simeq \downarrow \text{id} & & \simeq \downarrow \text{inn}(n) & & \simeq \downarrow \nu & & \\ e & \longrightarrow & \text{Ker}(\alpha^-) & \longrightarrow & T & \xrightarrow{\alpha^-} & \mathbb{G}_m & \longrightarrow & e \end{array}$$

where ν is induced by $\text{inn}(n)$. If $\nu = \text{id}$, then $\text{inn}(n) = \text{id} + \lambda$ with λ a homomorphism (of algebraic groups) $T \rightarrow \text{Ker}(\alpha^-)$. But then $\text{id} = (\text{inn}(n))^2 = \text{id} + 2\lambda$. As $\text{Hom}(T, \text{Ker}(\alpha^-))$ is torsion free, this implies that $\text{inn}(n) = \text{id}$, which contradicts our assumption that $n \notin C_G(T)$. Thus ν is an automorphism, equal to $-\text{id}$, as required. \square

COROLLARY 21.46. We have

$$B_u^+ \cap B_u^- = e.$$

PROOF. Note that T acts by inner automorphisms on $B_u^+ \cap B_u^-$. We use i^+ to identify B_u^+ with \mathbb{G}_a . Then T acts on B_u^+ through α^+ , and as α^+ is an epimorphism, $B_u^+ \cap B_u^-$ is a \mathbb{G}_m -submodule of \mathbb{G}_a . Therefore it equals α_{p^r} for some $r \geq 1$ or e . In the first case, T acts on $\alpha_p \subset \alpha_{p^r}$ via the map α^+ , but because $\alpha^- = -\alpha^+$, this is impossible. \square

COROLLARY 21.47. We have

$$B^+ \cap B^- = T.$$

PROOF. Clearly,

$$B^+ \cap B^- = (B_u^+ \cap B^-) \cdot T = (B_u^+ \cap B_u^-) \cdot T = T. \quad \square$$

COROLLARY 21.48. We have

$$\text{Ker}(\alpha^+) = Z(G) = \text{Ker}(\varphi).$$

PROOF. The first equality was proved above. For the second, the kernel of φ is contained in $B^+ \cap B^- = T$, and is therefore a diagonalizable normal subgroup of a connected group G . Hence $\text{Ker}(\varphi)$ lies in the centre of G (14.30). But $Z(G) \subset \text{Ker}(\varphi)$ because φ is surjective and $Z(\text{PGL}_2) = e$. \square

NOTES. This section follows SHS, Exposé 15, §3, p.395–397.

The remaining sections will be rearranged in the final version. Probably “Roots” will be inserted here.

k. Properties of SL_2

PROPOSITION 21.49. *The algebraic group SL_2 is perfect, i.e., it is equal to its derived group.*

PROOF. As SL_2 is smooth, it suffices to show that the abstract group $\mathrm{SL}_2(k^{\mathrm{al}})$ is perfect. In fact, we shall show that $\mathrm{SL}_2(k)$ is perfect if k has at least three elements. For $a \in k^\times$, let

$$t_{1,2}(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad t_{2,1}(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

An algorithm in elementary linear algebra shows that $\mathrm{SL}_2(k)$ is generated by these matrices. On the other hand, the commutator

$$\left[\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (b^2 - 1)c \\ 0 & 1 \end{pmatrix}.$$

Choose $b \neq \pm 1$, and then c can be chosen so that $(b^2 - 1)c = a$. Thus $t_{1,2}(a)$ is a commutator. On taking transposes, we find that $t_{2,1}(a)$ is also a commutator. \square

The group SL_2 acts on itself by inner automorphisms, and so we have a homomorphism of algebraic groups $\mathrm{SL}_2 \rightarrow \underline{\mathrm{Aut}}(\mathrm{SL}_2)$, which factors through PGL_2 .

PROPOSITION 21.50. *The homomorphism $\mathrm{PGL}_2 \rightarrow \underline{\mathrm{Aut}}(\mathrm{SL}_2)$ is an isomorphism of algebraic groups.*

PROOF. It suffices to show that every automorphism of SL_2 becomes inner over the algebraic closure of the base field. Thus, assume k to be algebraically closed, and let γ be an automorphism of SL_2 . Let T be the diagonal maximal torus in SL_2 , and let $U = \mathbb{U}_2$. After (possibly) composing γ with an inner automorphism of SL_2 , we may suppose that $\gamma(T) = T$, and after (possibly) composing it with $\mathrm{inn}(s)$, we may suppose that γ acts as the identity map on T . Then $U \xrightarrow{\gamma} \gamma(U)$ is a T -isomorphism, and so $\gamma(U) = U$ (as $\gamma(U)$ satisfies (152)). Hence γ stabilizes U , and therefore T . After composing γ with an inner automorphism by an element of T , we may suppose that $\gamma|_B = \mathrm{id}_B$ (here we may have to take a square root). Now $x \mapsto \gamma(x)x^{-1}$ factors through SL_2/B , and so is constant (18.25). \square

REMARK 21.51. The proposition says that every automorphism of SL_2 is inner in the sense that it becomes inner after a field extension. For $t \in k$,

$$\begin{pmatrix} \sqrt{t} & 0 \\ 0 & \sqrt{t^{-1}} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \sqrt{t^{-1}} & 0 \\ 0 & \sqrt{t} \end{pmatrix} = \begin{pmatrix} a & tb \\ t^{-1}c & d \end{pmatrix}, \tag{150}$$

and so conjugation by $\mathrm{diag}(\sqrt{t}, \sqrt{t^{-1}})$ is an inner automorphism of SL_2 over k . However, it is not of the form $\mathrm{inn}(A)$ with $A \in \mathrm{SL}_2(k)$ but only for $A \in \mathrm{SL}_2(k[\sqrt{t}])$. This reflects the fact that $\mathrm{SL}_2(k) \rightarrow \mathrm{PGL}_2(k)$ is not surjective.

PROPOSITION 21.52. *The algebraic group SL_2 is simply connected.*

In other words, every multiplicative isogeny $G \rightarrow \mathrm{SL}_2$ of connected group varieties is an isomorphism. It suffices to prove this over an algebraically closed field. There are several different proofs of this, which we now describe.

PROOF BY ELEMENTARY GROUP THEORY

See Springer 1998, 7.2.4.

PROOF BY ALGEBRAIC GEOMETRY

It satisfies the criterion $X(G) = 0 = \text{Pic}(G)$ — see (20.18).

PROOF USING ROOTS

It satisfies the criterion: a split semisimple group (G, T) is semisimple if $X_*(T)$ is generated by the coroots. See (22.104) et seq. This will be explained in the final version.

PROOF USING EXTENSIONS.

Recall (14.29) that the only action of a connected algebraic group on a group of multiplicative type is the trivial action.

PROPOSITION 21.53. *Let D be an algebraic group of multiplicative type. Then*

$$\begin{aligned} Z^1(\text{SL}_2, D) &= 0 = H^2(\text{SL}_2, D), \text{ i.e.,} \\ \text{Ext}^0(\text{SL}_2, D) &= 0 = \text{Ext}^1(\text{SL}_2, D). \end{aligned}$$

PROOF. Recall that $\text{GL}_2 = \text{SL}_2 \rtimes \mathbb{G}_m$. Therefore a (nontrivial) \mathbb{G}_m -torsor over SL_2 extends to a (nontrivial) \mathbb{G}_m -torsor over GL_2 . But GL_2 is the spectrum of a unique factorization domain, which implies that $\text{Pic}(\text{GL}_2) = \text{Pic}(\text{SL}_2) = 0$, and we can calculate the cohomology of SL_2 acting on \mathbb{G}_m by means of the Hochschild complex. In order to describe this complex, we must first determine the group $\text{Mor}(\text{SL}_2^i, \mathbb{G}_m)$ of invertible functions on SL_2^i . According to (14.68), every regular map $\text{SL}_2^i \rightarrow \mathbb{G}_m$ sending e to e is a homomorphism. But there are no nontrivial homomorphism $\text{SL}_2 \rightarrow \mathbb{G}_m$ because SL_2 is perfect. Therefore,

$$C^i(\text{SL}_2, \mathbb{G}_m) = k^\times,$$

and as in the computation of $H^i(\mathbb{G}_a, \mathbb{G}_m)$,

$$\begin{aligned} H_0^0(\text{SL}_2, \mathbb{G}_m) &= k^\times \\ H_0^i(\text{SL}_2, \mathbb{G}_m) &= 0, \quad i > 0. \end{aligned} \quad \square$$

1. Classification of the split reductive groups of semisimple rank 1

PROPOSITION 21.54. *For every multiplicative isogeny $G \rightarrow \text{PGL}_2$ of connected group varieties, there exists a unique homomorphism $\text{SL}_2 \rightarrow G$ making the following diagram commute*

$$\begin{array}{ccc} \text{SL}_2 & & \\ \downarrow \text{---} & \searrow \pi & \\ G & \longrightarrow & \text{PGL}_2. \end{array}$$

PROOF. The homomorphism $G' = G \times_{\text{PGL}_2} \text{SL}_2 \rightarrow \text{SL}_2$ is surjective with finite multiplicative kernel. If k has odd characteristic, then G' is smooth, and the restriction of the morphism to G'° has a section. If k is perfect, the restriction to $G'_{\text{red}} \rightarrow \text{SL}_2$ has a section. We omit the proof of the remaining case (k nonperfect of characteristic 2). Let φ, φ' be two such maps; then $g \mapsto \varphi(g)/\varphi'(g)$ is trivial because SL_2 has no finite quotients. \square

THEOREM 21.55. *Every split reductive group G of semisimple rank 1 is isomorphic to exactly one of the groups*

$$\mathbb{G}_m^r \times \mathrm{SL}_2, \quad \mathbb{G}_m^r \times \mathrm{GL}_2, \quad \mathbb{G}_m^r \times \mathrm{PGL}_2, \quad r \in \mathbb{N}.$$

FIRST PROOF

In the exact sequence

$$e \rightarrow RG \rightarrow G \rightarrow G/RG \rightarrow e \tag{151}$$

RG is a torus and G/RG is a split semisimple group of rank 1. According to (21.44), there is a surjective homomorphism $G/RG \rightarrow \mathrm{PGL}_2$ with kernel the centre Z of G/RG . Now the composed map $G \rightarrow \mathrm{PGL}_2$ realizes G as an extension of PGL_2 by an extension of Z by RG . Thus, we see that G arises as extension of PGL_2 by a split group of multiplicative type, and so it remains to classify such extensions.

PROPOSITION 21.56. *Let D be an algebraic group of multiplicative type. Then*

$$\mathrm{Hom}(\mu_2, D) \simeq \mathrm{Ext}^1(\mathrm{PGL}_2, D).$$

PROOF. We use the exact sequence

$$e \rightarrow \mu_2 \rightarrow \mathrm{SL}_2 \rightarrow \mathrm{PGL}_2 \rightarrow e$$

to deduce this from (21.53). See SHS, Exp. 10, 1.5.1, p.290-2. The idea is to use

$$\mathrm{Hom}(\mathrm{PGL}_2, D) \rightarrow \mathrm{Hom}(\mathrm{SL}_2, D) \rightarrow \mathrm{Hom}(\mu_2, D) \rightarrow \mathrm{Ext}^1(\mathrm{PGL}_2, D) \rightarrow 0.$$

In fact, defines

$$\mathrm{Hom}(\mu_2, D) \rightarrow \mathrm{Ext}^1(\mathrm{PGL}_2, D)$$

explicitly, and then defines an inverse.

Alternatively, we can argue directly as in (20.28). Let $f: \mu_2 \rightarrow D$ be a homomorphism. Define $E(f)$ to be the cokernel of the homomorphism

$$x \mapsto (x, f(x^{-1})): \mu_2 \rightarrow \mathrm{SL}_2 \times D.$$

Then $E(f)$ is a central extension of PGL_2 by D .

On the other hand, let $h: G' \rightarrow \mathrm{PGL}_2$ be a central extension of G by D . Then $\pi: \tilde{G} \rightarrow G$ factors through h ,

$$\tilde{G} \xrightarrow{f} G' \rightarrow G,$$

and the factorization is unique (cf. 20.5). The restriction of f to $\pi_1(G)$ maps into D .

These operations are inverse. □

Thus, the extensions of PGL_2 are classified by the elements of

$$\mathrm{Hom}(\mu_2, D) \stackrel{14.9}{\simeq} \mathrm{Hom}(X(D), \mathbb{Z}/2\mathbb{Z}).$$

Let μ be a homomorphism $X(D) \rightarrow \mathbb{Z}/2\mathbb{Z}$. There are three cases to consider.

In the first case $\mu = 0$. This corresponds to the trivial extension

$$e \rightarrow D \rightarrow D \times \mathrm{PGL}_2 \xrightarrow{q} \mathrm{PGL}_2 \rightarrow e$$

In the second case, there exists a decomposition $X(D) = N \oplus \mathbb{Z}$ such that $\mu|_N = 0$ and $\mu|_{\mathbb{Z}}$ is the quotient map $\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$. This corresponds to the extension

$$e \rightarrow D(N) \rightarrow D(N) \times \mathrm{GL}_2 \xrightarrow{q} \mathrm{PGL}_2 \rightarrow e$$

with q the obvious projection onto PGL_2 .

In the final case, there exists a decomposition $X(D) = N \oplus \mathbb{Z}/2\mathbb{Z}$ such that $\mu|_N = 0$ and $\mu|_{\mathbb{Z}/2\mathbb{Z}} = \mathrm{id}$. This corresponds to the extension

$$e \rightarrow D(N) \rightarrow D(N) \times \mathrm{SL}_2 \xrightarrow{q} \mathrm{PGL}_2 \rightarrow e$$

with q the obvious projection onto PGL_2 .

SECOND PROOF (USING 20.13)

Let G be a split reductive group of semisimple rank 1. Then G/RG admits a universal covering $\mathrm{SL}_2 \rightarrow G/RG$, which can be used to pull (151) back to an exact sequence

$$e \rightarrow RG \rightarrow G' \rightarrow \mathrm{SL}_2 \rightarrow e.$$

Because SL_2 is perfect, this extension splits, and so we have

$$RG \times \mathrm{SL}_2 \simeq G' \rightarrow G$$

with RG a torus and $G' \rightarrow G$ a central isogeny with kernel e or μ_2 . From this it is easy to deduce the theorem.

THIRD PROOF

We use that SL_2 is simply connected. Let T_2 be the standard (diagonal) maximal torus in SL_2 , and let α_2 be the root $\mathrm{diag}(t, t^{-1}) \mapsto t^2$.

PROPOSITION 21.57. *Let (G, T) be a split reductive group of semisimple rank 1. There exists a homomorphism $\pi: (\mathrm{SL}_2, T_2) \rightarrow (G, T)$ whose kernel is central and $\alpha \circ \pi = \alpha_2$. Moreover, π is unique up to an inner automorphism by an element of T_2 , and $\pi(s)$ normalizes T .*

By ‘‘an inner automorphism by an element of T_2 ’’ we allow (150).

PROOF. Let $R = RG = (ZG)_t$. We know that $\mathcal{D}(\mathrm{PGL}_2) = \mathrm{PGL}_2$, and so there is an exact sequence (14.72)

$$e \rightarrow R \cap \mathcal{D}G \rightarrow R \times \mathcal{D}G \rightarrow G \rightarrow e$$

with $R \cap \mathcal{D}G$ finite. On dividing by R , we get a central isogeny $\mathcal{D}G \rightarrow G/R$, and hence a central isogeny $\mathcal{D}G \rightarrow \mathrm{PGL}_2$ (21.5). As SL_2 is simply connected, the canonical homomorphism $\mathrm{SL}_2 \rightarrow \mathrm{PGL}_2$ lifts to a homomorphism $\mathrm{SL}_2 \rightarrow \mathcal{D}G$. \square

PROPOSITION 21.58. *Every split reductive group G of semisimple rank 1 is isomorphic to exactly one of the following:*

$$T \times \mathrm{SL}_2, \quad T \times \mathrm{GL}_2, \quad T \times \mathrm{PGL}_2.$$

Here T is an arbitrary split torus.

PROOF. It follows from (21.57) that G is a quotient of $T \times \mathrm{SL}_2$ by a finite central subgroup scheme N . If $N \subset T \times 1$, we get $T' \times \mathrm{SL}_2$ as the quotient; if $N \subset 1 \times \mathrm{SL}_2$, we get $T \times \mathrm{PGL}_2$ as the quotient; otherwise, we get $T \times \mathrm{GL}_2$. \square

m. Roots

THEOREM 21.59. *Let (G, T) be a split reductive group of rank 1, and assume that G is not solvable.*

- (a) *There exists an $\alpha \in X^*(T)$ such that*

$$\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

with $\dim \mathfrak{g}_\alpha = 1 = \dim \mathfrak{g}_{-\alpha}$.

- (b) *There exists a connected unipotent subgroup variety U_α (resp. $U_{-\alpha}$) with Lie algebra \mathfrak{g}_α (resp. $\mathfrak{g}_{-\alpha}$).*
 (c) *There exists an isomorphism $u: \mathbb{G}_a \rightarrow U_\alpha$, and for every such isomorphism*

$$t \cdot u(a) \cdot t^{-1} = u(\alpha(t)a), \quad \text{all } t \in T(R), a \in \mathbb{G}_a(R) \quad (R \text{ a } k\text{-algebra}).$$

- (d) *The Borel subgroups of G containing T are $B = TU_\alpha$ and $B^- = TU_{-\alpha}$; their Lie algebras are $\mathfrak{t} \oplus \mathfrak{g}_\alpha$ and $\mathfrak{t} \oplus \mathfrak{g}_{-\alpha}$.*
 (e) *The Weyl group $W(G, T)(k)$ has order 2; its nontrivial element s is represented by an $n \in N_G(T)(k)$, and for any such n , the orbit map*

$$U_\alpha \rightarrow G/B, \quad u \mapsto unB$$

is an isomorphism onto its image.

- (f) *The flag manifold $\mathcal{B} \approx \mathbb{P}^1$ and G is semisimple and perfect of dimension 3.*

PROOF. This has largely been proved (see especially the proofs of 21.43 and 21.44). For example, U_α is the group $U(\lambda)$ where λ is any isomorphism $\mathbb{G}_m \rightarrow T$. For statement (c), $U_\alpha \approx \mathbb{G}_a$ because it is smooth, unipotent, and of dimension 1 (15.52). Let $u: \mathbb{G}_a \rightarrow U_\alpha$ be an isomorphism. There is an action of T on \mathbb{G}_a such that $u(t \cdot x) = tu(x)t^{-1}$. This action is linear because conjugation respects the group structure. Therefore $t \cdot x = \chi(t)x$ for some character χ of \mathbb{G}_m , and $tu(x)t^{-1} = u(\chi(t)x)$. On applying Lie, we see that T acts on \mathfrak{g}_α through the character χ . But we know that T acts on \mathfrak{g}_α through α , and so $\chi = \alpha$. \square

EXAMPLE 21.60. Let T be the standard (diagonal) torus in $G = \text{SL}_2$. The Lie algebra \mathfrak{g} of SL_2 is

$$\mathfrak{sl}_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) \mid a + d = 0 \right\},$$

and T acts on \mathfrak{g} by conjugation,

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} a & t^2b \\ t^{-2}c & -a \end{pmatrix}.$$

Therefore

$$\mathfrak{sl}_2 = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

with α the character $\text{diag}(t, t^{-1}) \mapsto t^2$ and

$$\mathfrak{g}_\alpha = \left\{ \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \right\} \quad \mathfrak{g}_{-\alpha} = \left\{ \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix} \right\}.$$

Let $U_\alpha = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$. Then $\text{Lie}(U_\alpha) = \mathfrak{g}_\alpha$, and $B = TU$ is a Borel subgroup of SL_2 . Note that

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 1 & t^2 b \\ 0 & 1 \end{pmatrix},$$

and so the map $a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ is an isomorphism of algebraic groups $u: \mathbb{G}_a \rightarrow U$ with the property that

$$t \cdot u(a) \cdot t^{-1} = u(\alpha(t)a), \quad \text{all } t \in T(R), \quad a \in \mathbb{G}_a(R). \quad (152)$$

The Weyl group $W(G, T)(k) = \{1, s\}$ where s is represented by the matrix $n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

LEMMA 21.61. *Let (G, T) be a split reductive group of semisimple rank 1, and let H be a smooth algebraic subgroup of G normalized by T . If $\mathfrak{g}_\alpha \subset \text{Lie}(H)$ for some root α , then $U_\alpha \subset H$.*

PROOF. Because T normalizes H , TH is a smooth algebraic subgroup of G . Suppose that $U_\alpha \subset TH$; then the image of U_α in $TH/H \simeq T/T \cap H$ is trivial, and so $U_\alpha \subset H$. Thus we may replace H with TH and assume $T \subset H$.

Note that $\dim G = \dim T + 2$. As $\text{Lie}(H) \supset \mathfrak{t} \oplus \mathfrak{g}_\alpha$, the dimension of H is $\dim T + 1$ or $\dim T + 2$. In the second case, $H = G$ and so $H \supset U_\alpha$. In the first case, we let B denote a Borel subgroup of H containing T . If $B = T$, then B is nilpotent, and $H = B = T$, which contradicts the hypothesis. Thus $H = B$, and so H is a connected solvable subgroup variety of G of maximum dimension $\dim(G) - 1$. Therefore it is a Borel subgroup of G , and so it contains U_α because its Lie algebra contains \mathfrak{g}_α . \square

THEOREM 21.62. *Let (G, T) be a split reductive group of semisimple rank 1.*

- (a) *The derived group G' of G has semisimple rank 1, and the map $G' \rightarrow G/RG$ is an isogeny with kernel $RG \cap G'$.*
- (b) *There exists an $\alpha \in X^*(T)$ such that*

$$\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

with $\dim \mathfrak{g}_\alpha = 1 = \dim \mathfrak{g}_{-\alpha}$.

- (c) *There is a unique homomorphism $u_\alpha: (\mathfrak{g}_\alpha)_\alpha \rightarrow G$ such that $\text{Lie}(u_\alpha)$ is the given inclusion $\mathfrak{g}_\alpha \rightarrow \mathfrak{g}$.*
- (d) *Let $U_\alpha = \text{Im}(u_\alpha)$. Then U_α is the unique subgroup of G isomorphic to \mathbb{G}_a , normalized by T , and such that, for every homomorphism $u: \mathbb{G}_a \rightarrow U_\alpha$,*

$$t \cdot u(a) \cdot t^{-1} = u(\alpha(t)a), \quad \text{all } t \in T(R), \quad a \in \mathbb{G}_a(R) \quad (R \text{ a } k\text{-algebra}).$$

- (e) *The Borel subgroups of G containing T are $B_\alpha = TU_\alpha$ and $B_{-\alpha} = TU_{-\alpha}$. Their Lie algebras are $\mathfrak{b}_\alpha = \mathfrak{t} \oplus \mathfrak{g}_\alpha$ and $\mathfrak{b}_{-\alpha} = \mathfrak{t} \oplus \mathfrak{g}_{-\alpha}$.*
- (f) *Let T' be the unique maximal torus in G' contained in T . There exists a unique $\alpha^\vee \in X_*(T') \subset X_*(T)$ such that $\langle \alpha, \alpha^\vee \rangle = 2$.*

(g) The Weyl group $W(G, T)(k)$ contains exactly one nontrivial element s_α , and

$$\begin{aligned} s_\alpha(\chi) &= \chi - \langle \chi, \alpha^\vee \rangle \alpha \\ s_\alpha(\lambda) &= \lambda - \langle \alpha, \lambda \rangle \alpha^\vee, \end{aligned}$$

for all $\chi \in X^*(T)$ and $\lambda \in X_*(T)$.

(h) The algebraic group G is generated by T , U_α , and $U_{-\alpha}$.

PROOF. The algebraic subgroup $RG \cap G'$ is finite, and the sequence

$$e \rightarrow RG \cap G' \rightarrow RG \times G' \rightarrow G \rightarrow e$$

is exact because $G/RG \simeq \mathrm{PGL}_2$ is perfect (14.72). From this the statement (a) follows. The remaining statements follow from (21.59) applied to (G', T') , except for the uniqueness of U_α , which follows from the lemma.

Alternatively, the unscrupulous can prove it case-by-case using the classification (21.58). (Readers should check this; in particular, they should find the coroot α^\vee in each case.) \square

n. Forms of GL_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^{sep} , and so G is a k^{sep}/k -form of one of the groups in (21.55). Thus, to determine all reductive groups of semisimple rank 1 over k , it remains to determine the k -forms of these groups. For GL_2 , this is easy.

FORMS OF $M_2(k)$: QUATERNION ALGEBRAS

The k -forms of $M_2(k)$ are the quaternion algebras over k . Every quaternion algebra splits over a separable extension of k . Every automorphism of $M_2(k)$ is inner, and so its automorphism group is $\mathrm{PGL}_2(k)$. The isomorphism classes of the forms of $M_2(k)$ are classified by $H^1(k, \mathrm{PGL}_2)$ (Galois cohomology).

FORMS OF GL_2

Because $\underline{\mathrm{Aut}}(\mathrm{GL}_2) = \mathrm{PGL}_2$, the isomorphism classes of the forms of GL_2 are also classified by $H^1(k, \mathrm{PGL}_2)$. For each quaternion algebra A over k ,

$$G^A: R \rightsquigarrow (A \otimes R)^\times$$

is a k -form of GL_2 , and the cohomology classes of A and G^A agree. Therefore this functor induces 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 .

Reductive groups

In this chapter, we reap the benefit of our hard work in the earlier chapters to give a complete description of the structure of split reductive groups.

Usually in this chapter R is a set of roots; if it is a k -algebra we say so.

a. *Semisimple groups*

THE RADICAL

22.1. Let G be a connected group variety over k . Recall (8.39) that, among the connected normal solvable subgroup varieties of G there is a greatest one, containing all other such subgroup varieties. This is the radical $R(G)$ of G .

22.2. For example, if G is the group variety of invertible matrices $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ with A of size $m \times m$ and C of size $n \times n$, then $R(G)$ is the subgroup of matrices of the form $\begin{pmatrix} aI_m & B \\ 0 & cI_n \end{pmatrix}$ with aI_m and cI_n nonzero scalar matrices. The quotient G/RG is the semisimple group $SL_m \times SL_n$.

22.3. The formation of $R(G)$ commutes with *separable* field extensions k'/k (not necessarily finite). It suffices to prove this for a finite extension. We may suppose that k' is a finite Galois extension of k with Galois group Γ . By uniqueness, $R(G_{k'})$ is stable under the action of Γ , and therefore arises from a subgroup variety H of G (1.41). Clearly,

$$R(G)_{k'} \subset R(G_{k'}) = H_{k'},$$

and so $R(G) \subset H$. As $H_{k'}$ is connected normal and solvable, so also is H (5.48, 8.29), and so $R(G) = H$ by maximality.

SEMISIMPLE ALGEBRAIC GROUPS

22.4. Recall (8.39) that a connected group variety G over an algebraically closed field is semisimple if $R(G) = e$, and a connected group variety G over a field k is semisimple if $G_{k^{\text{al}}}$ is semisimple.

22.5. Let G be a group variety over k . If G is semisimple, then $G_{k'}$ is semisimple for all fields k' containing k ; conversely, if $G_{k'}$ is semisimple for some field k' containing k , then G is semisimple. This is obvious from the definition [actually, not quite; should prove (22.3) for not necessarily algebraic field extensions].

PROPOSITION 22.6. *Let G be a group variety over a perfect field k .*

- (a) *The group G is semisimple if and only if $RG = e$.*
- (b) *The quotient G/RG is semisimple.*

PROOF. (a) This follows from (22.3).

(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

$$e \rightarrow RG \rightarrow N \rightarrow R(G/RG) \rightarrow e.$$

of smooth connected solvable algebraic groups. Therefore it is smooth connected and solvable, and so $RG = N$. Hence $R(G/RG) = e$. \square

PROPOSITION 22.7. *Let G be a connected group variety over 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 $H_{k^{\text{al}}} \subset RG_{k^{\text{al}}} = e$, and so $H = e$.

For the converse, suppose that k is perfect and that G is not semisimple. Then $RG \neq e$ (22.6), and there is a chain of distinct subgroup varieties

$$RG \supset \mathcal{D}^1(RG) \supset \mathcal{D}^2(RG) \supset \cdots \supset \mathcal{D}^r(RG) = e$$

of G with $r \geq 1$. As RG is smooth and connected, each group $\mathcal{D}^n(RG)$ is smooth and connected; moreover $\mathcal{D}^n(RG)$ is characteristic in RG (8.21), hence normal in G , and each quotient $\mathcal{D}^n G / \mathcal{D}^{n+1} G$ is commutative (8.21). The last nontrivial term in the chain is a connected normal commutative subgroup variety of G . \square

22.8. If one of the conditions in (22.7) is dropped, then a semisimple group may have such an algebraic subgroup. Let $p = \text{char}(k)$.

- (a) The subgroup $\mathbb{Z}/2\mathbb{Z} = \{\pm I\}$ of SL_2 ($p \neq 2$) is normal, commutative, and smooth, but not connected.
- (b) The subgroup μ_2 of SL_2 ($p = 2$) is connected, normal, and commutative, but not smooth.
- (c) The subgroup $\mathbb{U}_2 = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$ of SL_2 is connected, commutative, and smooth, but not normal.
- (d) The subgroup $\{e\} \times \text{SL}_2$ of $\text{SL}_2 \times \text{SL}_2$ is connected, normal, and smooth, but not commutative.

22.9. Let $G = \text{SL}_n$. Let p be the characteristic exponent of k , and set $n = mp^r$ with $\text{gcd}(m, p) = 1$. Then $Z(G) = \mu_n$, $Z(G)^\circ = \mu_{p^r}$, $Z(G)_{\text{red}} = \mu_m$, and $R(G) = Z(G)_{\text{red}}^\circ = 1$.

b. Reductive groups

THE UNIPOTENT RADICAL

22.10. Let G be a connected group variety over k . Recall (8.41) that, among the connected normal unipotent subgroup varieties of G there is a greatest one, containing all other such subgroup varieties. This is the unipotent radical $R_u(G)$ of G .

22.11. For example, if G is the group variety of invertible matrices $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ with A of size $m \times m$ and C of size $n \times n$, then $R_u G$ is the subgroup of matrices of the form $\begin{pmatrix} I_m & B \\ 0 & I_n \end{pmatrix}$. The quotient $G/R_u G$ is isomorphic to the reductive group $\mathrm{GL}_m \times \mathrm{GL}_n$.

22.12. The formation of $R_u(G)$ commutes with *separable* field extensions. The proof of this is the same as for $R(G)$ (22.3).

REDUCTIVE ALGEBRAIC GROUPS

22.13. Recall (8.41) that a connected group variety G over an algebraically closed field is reductive if $R_u(G) = e$, and a connected group variety G over a field k is reductive if $G_{k^{\mathrm{al}}}$ is reductive.

Sometimes a group variety G is said to be reductive if G° is reductive in the above sense. For us, reductive group varieties are always connected.

22.14. Let G be a group variety over k . If G is reductive, then $G_{k'}$ is reductive for all fields k' containing k ; conversely, if $G_{k'}$ is reductive for some field k' containing k , then G is reductive. This is obvious from the definition.

22.15. Let G be a connected group variety over a perfect field k .

(a) The group G is reductive if and only if $R_u G = e$.

(b) The quotient $G/R_u G$ is reductive.

The proof of this is the same as that of (22.6).

22.16. Let G be a reductive group. The centre $Z(G)$ of G is of multiplicative type, and $R(G)$ is the greatest subtorus of $Z(G)$. The formation of $R(G)$ commutes with all extensions of the base field. This is proved in (19.20).

The centre of a reductive group need not be connected (e.g., SL_2 , $p \neq 2$) or smooth (e.g., SL_2 , $p = 2$).

22.17. Let G be a connected group variety over a field k . If G is reductive, then every connected normal commutative subgroup variety is a torus; the converse is true if k is perfect. The proof of this is the same as that of (22.7).

PROPOSITION 22.18. *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 , and because U is unipotent, it is nonzero. Therefore $W^U = W$. As V is a sum of its simple subrepresentations, it follows that U acts trivially on V . □

COROLLARY 22.19. *If a connected group variety G admits a faithful semisimple representation, then its unipotent radical is trivial.*

PROOF. The unipotent radical acts trivially on the faithful representation, and hence is trivial. □

COROLLARY 22.20. *A connected group variety G is reductive if it admits a faithful semisimple representation that remains semisimple over k^{al} .*

PROOF. The hypothesis implies that the unipotent radical of $G_{k^{\text{al}}}$ is trivial. \square

Proposition 22.18 shows that, for a connected group variety G ,

$$R_u G \subset \bigcap_{(V,r) \text{ simple}} \text{Ker}(r).$$

If k has characteristic zero, then all representations of a reductive group are semisimple (22.138), and so equality holds. In the general case, let (V, r) be a faithful representation of G , and let $V = V_0 \supset V_1 \supset \cdots \supset V_{s-1} \supset V_s = 0$ be a filtration of V by stable subspaces such that $(V_i/V_{i+1}, r_i)$ is simple for all i . Then $\bigcap \text{Ker}(r_i)$ is a normal unipotent subgroup of G , and so it is contained in $R_u G$ if it is smooth and connected.

EXAMPLE 22.21. The group varieties GL_n , SL_n , SO_n , and Sp_{2n} are reductive, because they are connected and their standard representations are simple and faithful.

MAXIMAL TORI IN REDUCTIVE GROUPS

22.22. Let G be a reductive algebraic group. The centralizer of a torus in G is reductive; in particular, it is smooth and connected (19.19). A torus T in G is maximal if and only if $C_G(T) = T$ (19.19). As the formation of centralizers commutes with extension of the base field, we see that maximal tori in reductive groups remain maximal after extension of the base field.

22.23. Every connected group variety contains a maximal torus (18.65). Any two split maximal tori in a reductive group G are conjugate by an element of $G(k)$ (18.68).

22.24. Let T be a maximal torus in a reductive group G . The Weyl group of G with respect to T is

$$W(G, T) = N_G(T)/C_G(T).$$

As $N_G(T)^\circ$ centralizes T (by rigidity), we see that $W(G, T)$ is the finite étale group $\pi_0(N_G(T))$.

EXAMPLE 22.25. The torus \mathbb{D}_n is maximal in GL_n because $\mathbb{D}_n(k^{\text{sep}})$ is its own centralizer in $\text{GL}_n(k^{\text{sep}})$. In fact, 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 all the matrices $I + E_{ii}$.

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 . The (unique) conjugacy class of split maximal tori corresponds to the étale k -algebra $k \times \cdots \times k$ (n -copies). See (18.69).

NOTES

22.26. In SGA 3, XIX, it is recalled that the unipotent radical of a smooth connected affine group scheme over an algebraically closed field is the greatest smooth connected normal unipotent subgroup of G (ibid. 1.2). A smooth connected affine group scheme over an algebraically closed field is defined to be reductive if its unipotent radical is trivial (ibid. 1.6). A group scheme G over a scheme S is defined to be reductive if it is smooth and affine over S and each geometric fibre of G over S is a connected reductive group (ibid. 2.7). When S is the spectrum of field, this definition coincides with our definition.

22.27. In SHS (Exp. 5, p.188), a reductive algebraic group is defined as follows:

Let k be an algebraically closed field, and let G be an algebraic group over k .

We say that G is reductive if it is affine and smooth over k and if it contains no normal subgroup isomorphic to \mathbb{G}_a^n with $n > 0$.

Let G be a connected group variety over an algebraically closed field. If G is not reductive (in our sense), then it contains a normal algebraic subgroup of the form \mathbb{G}_a^r , $r > 0$. To see this, note that if $R_u(G) \neq e$, then it has a centre Z of dimension ≥ 1 . Let H be the kernel of the Verschiebung on Z (SHS Exp 11). Then H_{red}° is stable under all automorphisms of Z , or $R_u G$, or G . Therefore H_{red}° is normal in G . After SHS Exp 11, H_{red}° is isomorphic to \mathbb{G}_a^r . (See also 15.51, 15.) Thus our definition of a reductive group coincides with that in SHS except that SHS doesn't require the group to be connected.

22.28. Borel and Tits (1965) define the unipotent radical $R_u(G)$ of a k -algebraic group G to be the greatest connected unipotent closed normal subgroup of G , and they say that G is reductive if $R_u(G^\circ) = e$. By the first definition, I think they mean that $R_u(G)$ is the abstract subgroup of $G^\circ(\Omega)$, where Ω is a universal field, with these properties. If so, their definitions agree with our definitions. Since they decline to say what they mean by an "algebraic group over k ", instead offering the reader a choice of three possibilities including an "affine algebraic group scheme geometrically reduced over k ", it is difficult to interpret many of their statements.

22.29. Let G be a semisimple group over an algebraically closed field k , and let $g, g' \in G(k)$. If g and g' are conjugate in $G(k)$, then $r(g)$ and $r(g')$ are conjugate in $\text{GL}(V)$ for every simple representation (V, r) of G . Is the converse true? The answer is yes if the characteristic of k is zero or "big" (depending on G), but the answer is (perhaps) not known in general (Steinberg 1978).

c. The roots of a split reductive group

In the theory of reductive groups, there are only two possibilities: either one proves everything case-by-case or one uses roots. The second is usually much more efficient.

SPLIT REDUCTIVE GROUPS

A reductive group is *split*¹ if it contains a split maximal torus.² Every reductive group over a separably closed field is split because it contains a maximal torus (22.23) and every torus over a separably closed field is split (14.25)).

We show later that, for every reductive group G over an algebraically closed field k and subfield k_0 of k , there exists a split reductive group G_0 over k_0 , unique up to isomorphism, that becomes isomorphic to G over k .

DEFINITION 22.30. A *split reductive group* over k is a pair (G, T) consisting of a reductive group G and a split maximal torus T in G .

¹Strictly, one should say that it is "splittable" (Bourbaki).

²Don't confuse "split maximal torus" with "maximal split torus". Every algebraic group contains a maximal split torus. The maximal split tori in a connected group variety G are conjugate and their common dimension is called the k -rank of G . The rank of G is the k^{al} -rank of $G_{k^{\text{al}}}$. A reductive group is split if its k -rank equals its rank. Every maximal split torus in a split reductive group is a maximal torus.

THE ROOTS OF A SPLIT REDUCTIVE GROUP

Let (G, T) be a split reductive group. Let

$$\text{Ad}: G \rightarrow \text{GL}_{\mathfrak{g}}, \quad \mathfrak{g} = \text{Lie}(G),$$

be the adjoint representation (12.19). Then T acts on \mathfrak{g} , and because T is a split torus, \mathfrak{g} decomposes into a direct sum of eigenspaces for T (14.12)

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha} \mathfrak{g}_{\alpha}$$

where \mathfrak{g}_0 is the subspace on which T acts trivially, and \mathfrak{g}_{α} is the subspace on which T acts through a nontrivial character α . The nontrivial characters α of T occurring in this decomposition are called the **roots** of (G, T) . They form a finite subset $R(G, T)$ of $X^*(T)$.³ By definition

$$\mathfrak{g}_0 = \mathfrak{g}^T = \text{Lie}(G^T)$$

As $\text{Lie}(G)^T = \text{Lie}(G^T)$ (12.31) and $G^T = C_G(T) = T$ (19.19), we find that $\mathfrak{g}_0 = \mathfrak{t}$ where $\mathfrak{t} = \text{Lie}(T)$,⁴ and so

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha} \mathfrak{g}_{\alpha}.$$

LEMMA 22.31. *Let (G, T) be a split reductive group. The action of $W(G, T)$ on $X^*(T)$ stabilizes $R(G, T)$.*

PROOF. Let $s \in W(G, T)(k^{\text{al}})$, and let $n \in G(k^{\text{al}})$ represent s . Then s acts on $X^*(T)$ (on the left) by

$$(s\chi)(t) = \chi(n^{-1}tn), \quad t \in T(k^{\text{al}}).$$

Let α be a root. Then, for $x \in (\mathfrak{g}_{\alpha})_{k^{\text{al}}}$ and $t \in T(k^{\text{al}})$,

$$t(nx) = n(n^{-1}tn)x = s(\alpha(s^{-1}ts)x) = \alpha(s^{-1}ts)sx,$$

and so T acts on $s\mathfrak{g}_{\alpha}$ through the character $s\alpha$, which must therefore be a root. \square

EXAMPLE: GL_2

22.32. We take T be the split maximal torus

$$T = \left\{ \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \mid t_1 t_2 \neq 0 \right\}.$$

Then

$$X^*(T) = \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2$$

where $a\chi_1 + b\chi_2$ is the character

$$\text{diag}(t_1, t_2) \mapsto \text{diag}(t_1, t_2)^{a\chi_1 + b\chi_2} = t_1^a t_2^b.$$

³There are several different notations used for the roots, $R(G, T)$, $\Phi(G, T)$, and $\Psi(G, T)$ all seem to be used, often by the same author. Conrad et al. 2010 write $R = \Phi(G, T)$ in 3.2.2, p. 94, and $R(G, T) = (X(T), \Phi(G, T), X_*(T), \Phi(G, T)^{\vee})$ in 3.2.5, p. 96.

⁴Usually, the Lie algebra of T is denoted by \mathfrak{h} .

The Lie algebra \mathfrak{g} of GL_2 is $\mathfrak{gl}_2 = M_2(k)$ with $[A, B] = AB - BA$, and T acts on \mathfrak{g} by conjugation,

$$\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{t_1}{t_2}b \\ \frac{t_2}{t_1}c & d \end{pmatrix}.$$

Write E_{ij} for the matrix with a 1 in the ij th-position, and zeros elsewhere. Then T acts trivially on $\mathfrak{g}_0 = kE_{11} + kE_{22}$, 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, $R(G, T) = \{\alpha, -\alpha\}$ 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 R becomes identified with $\{\pm(e_1 - e_2)\}$.

EXAMPLE: SL_2

22.33. We take T to be the split torus

$$T = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \right\}.$$

Then

$$X^*(T) = \mathbb{Z}\chi$$

where χ is the character $\mathrm{diag}(t, t^{-1}) \mapsto t$. The Lie algebra \mathfrak{g} of SL_2 is

$$\mathfrak{sl}_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k) \mid a + d = 0 \right\},$$

and T acts on \mathfrak{g} by conjugation,

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} a & t^2b \\ t^{-2}c & -a \end{pmatrix}$$

Therefore, the roots are $\alpha = 2\chi$ and $-\alpha = -2\chi$. When we use χ to identify $X^*(T)$ with \mathbb{Z} , the set $R(G, T)$ becomes identified with $\{2, -2\}$.

EXAMPLE: PGL_2

22.34. Recall that this is the quotient of GL_2 by its centre, $\mathrm{PGL}_2 = \mathrm{GL}_2 / \mathbb{G}_m$. For all local k -algebras R , $\mathrm{PGL}_2(R) = \mathrm{GL}_2(R) / R^\times$. We take T to be the torus

$$T = \left\{ \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \mid t_1 t_2 \neq 0 \right\} / \left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \mid t \neq 0 \right\}.$$

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 \mathfrak{g} of PGL_2 is

$$\mathfrak{g} = \mathfrak{pgl}_2 = \mathfrak{gl}_2 / \{\text{scalar matrices}\},$$

and T acts on \mathfrak{g} by conjugation:

$$\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{t_1}{t_2}b \\ \frac{t_2}{t_1}c & d \end{pmatrix}.$$

Therefore, the roots are $\alpha = \chi$ and $-\alpha = -\chi$. When we use χ to identify $X^*(T)$ with \mathbb{Z} , $R(G, T)$ becomes identified with $\{1, -1\}$.

EXAMPLE: GL_n

22.35. We take T to be the torus

$$T = \mathbb{D}_n = \left\{ \begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_n \end{pmatrix} \mid t_1 \cdots t_n \neq 0 \right\}.$$

Then

$$X^*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i$$

where χ_i is the character $\text{diag}(t_1, \dots, t_n) \mapsto t_i$. The Lie algebra \mathfrak{g} of GL_n is

$$\mathfrak{gl}_n = M_n(k) \text{ with } [A, B] = AB - BA,$$

and T acts on \mathfrak{g} by conjugation:

$$\begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & a_{ij} & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} t_1^{-1} & & 0 \\ & \ddots & \\ 0 & & t_n^{-1} \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & \frac{t_1}{t_n} a_{1n} \\ \vdots & \frac{t_i}{t_j} a_{ij} & \vdots \\ \vdots & & \vdots \\ \frac{t_n}{t_1} a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

Write E_{ij} for the matrix with a 1 in the ij -th-position, and zeros elsewhere. Then T acts trivially on $\mathfrak{g}_0 = kE_{11} + \cdots + kE_{nn}$ and through the character $\alpha_{ij} \stackrel{\text{def}}{=} \chi_i - \chi_j$ on $\mathfrak{g}_{\alpha_{ij}} = kE_{ij}$. Therefore

$$R(G, T) = \{\alpha_{ij} \mid 1 \leq i, j \leq n, \quad i \neq j\}.$$

When we use the χ_i to identify $X^*(T)$ with \mathbb{Z}^n , then $R(G, T)$ becomes identified with

$$\{e_i - e_j \mid 1 \leq i, j \leq n, \quad i \neq j\}$$

where e_1, \dots, e_n is the standard basis for \mathbb{Z}^n .

d. The centre of a reductive group

We explain how to compute the centre of a reductive group from its roots.

PROPOSITION 22.36. *Let G be a reductive algebraic group.*

- (a) *Every maximal torus T in G contains its centre $Z(G)$.*
- (b) *Let T be a maximal torus in G . The kernel of $\text{Ad}: T \rightarrow \text{GL}_{\mathfrak{g}}$ is $Z(G)$.*

PROOF. (a) Clearly $Z(G) \subset C_G(T)$, but $C_G(T) = T$ (see 22.22).

(b) Clearly, $Z(G) \subset \text{Ker}(\text{Ad})$, and so $Z(G) \subset \text{Ker}(\text{Ad}|_T)$. The quotient $\text{Ker}(\text{Ad})/Z(G)$ is a unipotent algebraic group (15.25). Therefore the image of $\text{Ker}(\text{Ad}|_T)$ in $\text{Ker}(\text{Ad})/Z(G)$ is trivial (15.15), which implies that $\text{Ker}(\text{Ad}|_T) \subset Z(G)$. \square

From the proposition,

$$Z(G) = \text{Ker}(\text{Ad}|_T) = \bigcap_{\alpha \in R(G, T)} \text{Ker}(\alpha).$$

For example,

$$\begin{aligned} Z(\mathrm{GL}_2) &= \mathrm{Ker}(\chi_1 - \chi_2) = \{\mathrm{diag}(t_1, t_2) \mid t_1 t_2 \neq 0, \quad t_1 = t_2\} \\ &\simeq \mathbb{G}_m; \\ Z(\mathrm{SL}_2) &= \mathrm{Ker}(2\chi) = \{\mathrm{diag}(t, t^{-1}) \mid t^2 = 1\} \\ &\simeq \mu_2; \\ Z(\mathrm{PGL}_2) &= \mathrm{Ker}(\chi) \\ &= 1; \\ Z(\mathrm{GL}_n) &= \bigcap_{i \neq j} \mathrm{Ker}(\chi_i - \chi_j) \\ &= \{\mathrm{diag}(t_1, \dots, t_n) \mid t_1 \cdots t_n \neq 0, \quad t_i = t_j \text{ if } i \neq j\} \\ &\simeq \mathbb{G}_m. \end{aligned}$$

On applying X^* to the exact sequence

$$0 \rightarrow Z(G) \rightarrow T \xrightarrow{t \mapsto (\alpha(t))_\alpha} \prod_{\alpha \in R(G, T)} \mathbb{G}_m \quad (153)$$

we get an exact sequence

$$\bigoplus_{\alpha \in R} \mathbb{Z} \xrightarrow{(m_\alpha)_\alpha \mapsto \sum m_\alpha \alpha} X^*(T) \rightarrow X^*(Z(G)) \rightarrow 0$$

(see 14.17), and so

$$\boxed{X^*(Z(G)) = \frac{X^*(T)}{\{\text{subgroup generated by } R(G, T)\}}} \quad (154)$$

For example,

$$\begin{aligned} X^*(Z(\mathrm{GL}_2)) &\simeq \mathbb{Z}^2 / \mathbb{Z}(e_1 - e_2) \simeq \mathbb{Z} \quad \text{by } (a_1, a_2) \mapsto a_1 + a_2; \\ X^*(Z(\mathrm{SL}_2)) &\simeq \mathbb{Z} / (2); \\ X^*(Z(\mathrm{PGL}_2)) &\simeq \mathbb{Z} / \mathbb{Z} = 0; \\ X^*(Z(\mathrm{GL}_n)) &\simeq \mathbb{Z}^n / \sum_{i \neq j} \mathbb{Z}(e_i - e_j) \simeq \mathbb{Z} \quad \text{by } (a_i) \mapsto \sum a_i. \end{aligned}$$

e. Root data and root systems

We briefly introduce the notions of a root datum and of a root system. These are explained in more detail in Chapter 23, which is logically independent of the rest of the book.

Let X be a free \mathbb{Z} -module of finite rank. We let X^\vee denote the linear dual $\mathrm{Hom}(X, \mathbb{Z})$ of X and $\langle \cdot, \cdot \rangle: X \times X^\vee \rightarrow \mathbb{Z}$ the perfect pairing $\langle x, f \rangle = f(x)$.

DEFINITION 22.37. A **root datum** is a triple $\mathcal{R} = (X, R, \alpha \mapsto \alpha^\vee)$ in which X is a free abelian group of finite rank, R is a finite subset of X , and $\alpha \mapsto \alpha^\vee$ is an injective 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_α is the homomorphism $X \rightarrow X$ defined by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \quad x \in X, \alpha \in R,$$

(rd3) the group 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 **(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**. Because $s_\alpha(\alpha) = -\alpha$,

$$s_\alpha(s_\alpha(x)) = s_\alpha(x - \langle x, \alpha^\vee \rangle \alpha) = (x - \langle x, \alpha^\vee \rangle \alpha) - \langle x, \alpha^\vee \rangle s_\alpha(\alpha) = x,$$

i.e.,

$$s_\alpha^2 = 1.$$

Clearly, also $s_\alpha(x) = x$ if $\langle x, \alpha^\vee \rangle = 0$. Thus, s_α should be considered an ‘‘abstract reflection in the hyperplane orthogonal to α^\vee ’’. We let R^\vee denote $\{\alpha^\vee \mid \alpha \in R\}$. The elements of R and R^\vee are called the **roots** and **coroots** of the root datum (and α^\vee is the **coroot** of α).

DEFINITION 22.38. Let V be a finite-dimensional vector space over \mathbb{Q} . 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 vector $\alpha^\vee \in V^\vee$ such that

- ◇ $\langle \alpha, \alpha^\vee \rangle = 2$,
- ◇ $s_\alpha(R) \subset R$, where s_α is the homomorphism $V \rightarrow V$ be defined by

$$s_\alpha: x \mapsto x - \langle x, \alpha^\vee \rangle \alpha,$$

- ◇ $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$ for all $\beta \in R$.

The map s_α , and hence the vector α^\vee , are uniquely determined by α (23.4). The map s_α is the reflection with vector α .

DEFINITION 22.39. Let R be a root system in V .

(a) The **root lattice** $Q(R)$ is the \mathbb{Z} -submodule of V spanned by R , $Q(R) = \mathbb{Z}R$;

(b) The **weight lattice** $P(R)$ is the \mathbb{Z} -submodule of V defined by

$$P(R) = \{v \in V \mid \langle v, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}.$$

Both $Q(R)$ and $P(R)$ are full lattices in V , and the last condition in (rs2) says that

$$Q(R) \subset P(R).$$

Because $P(R)$ and $Q(R)$ are full lattices in the same \mathbb{Q} -vector space, the quotient $P(R)/Q(R)$ is finite.

A root datum $(X, R, \alpha \mapsto \alpha^\vee)$ is **semisimple** if R spans the \mathbb{Q} -vector space $X_\mathbb{Q}$.

PROPOSITION 22.40. *If $(X, R, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum, then $(X_\mathbb{Q}, R)$ is a root system. Conversely, if (V, R) is a root system, then, for any choice of a lattice X in V such that*

$$Q(R) \subset X \subset P(R),$$

$(X, R, \alpha \mapsto \alpha^\vee)$ is a semisimple root datum.

PROOF. Let $(X, R, \alpha \mapsto \alpha^\vee)$ be a semisimple root datum. Certainly $0 \notin R$ because $\langle \alpha, \alpha^\vee \rangle = 2$, and $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$ because $\alpha^\vee \in X^\vee$. Therefore $(\mathbb{Q} \otimes_{\mathbb{Z}} X, R)$ is a root system.

Let (V, R) be a root system, and let X be a lattice between Q and P . As noted above, α^\vee is uniquely determined by α , and so there is a well-defined map $\alpha \mapsto \alpha^\vee$. 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). \square

DEFINITION 22.41. A **diagram** is a root system (V, R) together with a lattice X ,

$$Q(R) \subset X \subset P(R).$$

Thus, to give a semisimple root datum is the same as giving a diagram.

Let $(X, R, \alpha \mapsto \alpha^\vee)$ be a root datum, not necessarily semisimple. Then R is a root system in the \mathbb{Q} -subspace V of $X \otimes \mathbb{Q}$ spanned by R . To recover the map $\alpha \mapsto \alpha^\vee$ from (V, R) , we need a section to $(X \otimes \mathbb{Q})^\vee \rightarrow V^\vee$.

f. The root datum of a split reductive group

LEMMA 22.42. Let T be a split torus. If χ is a nonzero character of T then $S = \text{Ker}(\chi)^\circ$ is a subtorus of T of codimension one; moreover $S = \text{Ker}(m\chi)^\circ$ for all $m \neq 0$, and $S = \text{Ker}(m\chi)$ for some m . Every subtorus S of codimension one is the kernel of a character of T , and if $S = \text{Ker}(\chi)^\circ = \text{Ker}(\chi')^\circ$, then $m\chi = n\chi'$ for some nonzero integers m, n .

PROOF. Easy exercise using the duality between diagonalizable algebraic groups and \mathbb{Z} -modules (14.9). \square

THEOREM 22.43. Let (G, T) be a split reductive group, and let α be a root of (G, T) . Let $T_\alpha = \text{Ker}(\alpha)_{\text{red}}^\circ$, and let $G_\alpha = C_G(T_\alpha)$.

- (a) The pair (G_α, T_α) is a split reductive group of semisimple rank 1;

$$\text{Lie}(G_\alpha) = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

and $\dim \mathfrak{g}_\alpha = 1 = \dim \mathfrak{g}_{-\alpha}$.

- (b) There is a unique homomorphism $u_\alpha: (\mathfrak{g}_\alpha)_\alpha \rightarrow G$ such that $\text{Lie}(u_\alpha)$ is the given inclusion $\mathfrak{g}_\alpha \rightarrow \mathfrak{g}$.
- (c) Let $U_\alpha = \text{Im}(u_\alpha)$. Then U_α is the unique subgroup U_α of G isomorphic to \mathbb{G}_a , normalized by T , and such that, for every isomorphism $u: \mathbb{G}_a \rightarrow U_\alpha$,

$$t \cdot u(a) \cdot t^{-1} = u(\alpha(t)a), \text{ all } t \in T(R), a \in \mathbb{G}_a(R). \quad (155)$$

- (d) The algebraic group G_α is generated by T , U_α , and $U_{-\alpha}$.
- (e) The group $W(G_\alpha, T)(k)$ contains exactly one nontrivial element s_α , and there is a unique $\alpha^\vee \in X_*(T)$ such that

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \text{ for all } x \in X^*(T).$$

Moreover, $\langle \alpha, \alpha^\vee \rangle = 2$.

PROOF. Our assumption that there exists a root implies that $G \neq T$.

(a) That G_α is a (connected) reductive group is a particular case of (19.19c). Moreover,

$$\text{Lie}(G_\alpha) = \text{Lie}(G^{S_\alpha}) \stackrel{12.31}{=} \mathfrak{g}^{S_\alpha} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}. \tag{156}$$

Clearly $T_\alpha \subset Z(G_\alpha)$ and so $T_\alpha \subset R(G_\alpha)$. It follows that $T/R(G_\alpha)$ is a maximal torus in $G_\alpha/R(G_\alpha)$ of dimension 0 or 1. If the dimension were 0, then T would be central in G_α , i.e., $G_\alpha \subset C_G(T) = T$, and so $G_\alpha = T$; then $\text{Lie}(G_\alpha) = \mathfrak{t}$ contradicting (156). Therefore (G_α, T) has semisimple rank 1, and we have proved (a).

(b) This follows from (a) and (21.62).

(c) That U_α has this property follows from (a) and (21.62). Let H be a second algebraic subgroup of G with this property. It suffices to show that $H \supset U_\alpha$, and for this we may pass to the algebraic closure of k . Then $(H \cap G_\alpha)_{\text{red}}^\circ \supset U_\alpha$ because it is normalized by T and its Lie algebra contains \mathfrak{g}_α , and so we can apply (21.61).

(d,e) These statements follow from (a) and (21.62). □

The cocharacter α^\vee is called the coroot of α , and the group U_α in (a) is called the **root group** of α . Thus the root group U_α of α is the unique copy of \mathbb{G}_a in G normalized by T and such that T acts on it through α .

THEOREM 22.44. *Let (G, T) be a reductive group. For each $\alpha \in R(G, T)$, let α^\vee be the element of $X_*(T)$ defined by 22.43(e). Then $(X^*(T), R(G, T), \alpha \mapsto \alpha^\vee)$ is a reduced root datum.*

PROOF. Condition **(rd1)** holds by (b). The s_α attached to α lies in $W(G_\alpha, T)(k) \subset W(G, T)(k)$, and so stabilizes R by Lemma 22.31. Finally, all s_α lie in the Weyl group $W(G, T)(k)$, and so they generate a finite group. □

EXAMPLE 22.45. Let $G = \text{GL}_n$, and let $\alpha = \alpha_{12} = \chi_1 - \chi_2$. Then

$$T_\alpha = \{\text{diag}(x, x, x_3, \dots, x_n) \mid xx_3 \dots x_n \neq 1\}$$

and G_α consists of the invertible matrices of the form

$$\begin{pmatrix} * & * & 0 & & 0 \\ * & * & 0 & & 0 \\ 0 & 0 & * & & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & * \end{pmatrix}.$$

Clearly

$$n_\alpha = \begin{pmatrix} 0 & 1 & 0 & & 0 \\ 1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ & & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

represents the unique nontrivial element s_α of $W(G_\alpha, T)$. It acts on T by

$$\text{diag}(x_1, x_2, x_3, \dots, x_n) \mapsto \text{diag}(x_2, x_1, x_3, \dots, x_n).$$

For $x = m_1\chi_1 + \cdots + m_n\chi_n$,

$$\begin{aligned} s_\alpha x &= m_2\chi_1 + m_1\chi_2 + m_3\chi_3 + \cdots + m_n\chi_n \\ &= x - \langle x, \lambda_1 - \lambda_2 \rangle (\chi_1 - \chi_2). \end{aligned}$$

Thus (155), p.391, holds if and only if α^\vee is taken to be $\lambda_1 - \lambda_2$.

In general, the coroot α_{ij}^\vee of α_{ij} is

$$t \mapsto \text{diag}(1, \dots, 1, t^i, 1, \dots, 1, t^{-j}, 1, \dots, 1).$$

Clearly $\langle \alpha_{ij}, \alpha_{ij}^\vee \rangle = \alpha_{ij} \circ \alpha_{ij}^\vee = 2$.

SEMISIMPLE AND TORAL ROOT DATA

It is possible to determine whether a reductive group is semisimple or a torus from its root datum. Recall that a root datum $(X, R, \alpha \mapsto \alpha^\vee)$ is semisimple if the subgroup of X generated by R is of finite index. The root datum is *toral* if R is empty.

PROPOSITION 22.46. *A split reductive group is semisimple if and only if its root datum is semisimple.*

PROOF. A reductive group is semisimple if and only if its centre is finite, and so this follows from (154), p. 389. \square

PROPOSITION 22.47. *A split reductive group is a torus if and only if its root datum is toral.*

PROOF. If the root datum is toral, then (154) shows that $ZG = T$. Hence G has semisimple rank 0, and so it is a torus (21.3). Conversely, if G is a torus, then the adjoint representation is trivial and so $\mathfrak{g} = \mathfrak{g}_0$. \square

THE MAIN THEOREMS CONCERNING SPLIT REDUCTIVE GROUPS AND ROOT DATA

22.48. Let (G, T) be a split reductive group over a field k , with root datum $\mathcal{R}(G, T)$. If T' is a second split maximal torus, then T' is conjugate to T by an element g of $G(k)$. Conjugation by g induces an isomorphism of root data $\mathcal{R}(G, T) \rightarrow \mathcal{R}(G, T')$. Thus, to some extent, the root datum depends only on G . See (18.68).

22.49. (Isomorphism theorem) Let (G, T) and (G', T') be split reductive groups. An isomorphism $T \rightarrow T'$ extends to an isomorphism $G \rightarrow G'$ if and only if it induces an isomorphism $\mathcal{R}(G, T) \rightarrow \mathcal{R}(G', T')$ of the root data. Thus (G, T) is determined up to isomorphism by its root datum. In fact, with the appropriate definitions, every isogeny of root data (or even epimorphism of root data) arises from an isogeny (or epimorphism) of reductive groups $(G, T) \rightarrow (G', T')$. See Section 22.1.

22.50. (Existence theorem) Let k be a field. Every reduced root datum arises from a split reductive group (G, T) over k . Thus, the isomorphism classes of split reductive groups are completely classified by their root data. See Chapter 25.

ASIDE 22.51. (Deligne and Lusztig 1976, 1.1). “Suppose that in some category we are given a family $(X_i)_{i \in I}$ of objects and a compatible system of isomorphisms $\varphi_{ji}: X_i \rightarrow X_j$. This is as good as giving a single object X , the “common value” or “projective limit” of the family. This projective limit is provided with isomorphisms $\sigma_i: X \rightarrow X_i$ such that $\varphi_{ji} \circ \sigma_i = \sigma_j$. We will use such a construction to define *the* maximal torus T and *the* Weyl group W of a connected reductive algebraic group G over k (algebraically closed).

As index set I , we take the set of pairs (B, T) consisting of a maximal torus T and a Borel subgroup B containing T . For $i \in I$, $i = (B, T)$, we take $T_i = T$, $W_i = N(T)/T$. The isomorphism φ_{ji} is the isomorphism induced by $\text{ad } g$ where g is any element of $G(k)$ conjugating i into j ; these elements g form a single right T_i -coset, so that φ_{ji} is independent of the choice of g .

One similarly defines the root system of T , its set of simple roots, the action of W on T and the fundamental reflections in W .”

g. The root data of the classical semisimple groups

We compute the root system attached to each of the classical almost-simple groups. In each case the strategy is the same. We work with a convenient form of the group G in GL_n . We first compute the weights of the maximal torus of G on \mathfrak{gl}_n , and then check that each nonzero weight occurs in \mathfrak{g} (in fact, with multiplicity 1). Then for each α we find the group G_α centralizing T_α , and use it to find the coroot α^\vee .

EXAMPLE (A_n) : SL_{n+1} .

Take T to be the maximal torus of diagonal matrices

$$\text{diag}(t_1, \dots, t_{n+1}), \quad t_1 \cdots t_{n+1} \neq 0.$$

Then

$$X^*(T) = \bigoplus_i \mathbb{Z}\chi_i / \mathbb{Z}\chi, \quad \begin{cases} \chi_i: \text{diag}(t_1, \dots, t_{n+1}) \mapsto t_i \\ \chi = \sum \chi_i \end{cases}$$

$$X_*(T) = \{ \sum a_i \lambda_i \in \bigoplus_i \mathbb{Z}\lambda_i \mid \sum a_i = 0 \}, \quad \sum a_i \lambda_i: t \mapsto \text{diag}(t^{a_1}, \dots, t^{a_n}),$$

with the pairing such that

$$\langle \chi_j, \sum_i a_i \lambda_i \rangle = a_j.$$

Write $\bar{\chi}_i$ for 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 $\alpha_{ij} \stackrel{\text{def}}{=} \bar{\chi}_i - \bar{\chi}_j$ on kE_{ij} , $i \neq j$. Therefore

$$R(G, T) = \{ \alpha_{ij} \mid 1 \leq i, j \leq n+1, \quad i \neq j \}.$$

It remains to compute the coroots. Consider, for example, the root $\alpha = \alpha_{12}$. Then G_α in (22.43) consists of the matrices of the form

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

with determinant 1. As in (22.45), $W(G_\alpha, T) = \{1, s_\alpha\}$ 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

$$\begin{aligned} s_\alpha(\chi) &= a_2 \bar{\chi}_1 + a_1 \bar{\chi}_2 + \sum_{i=3}^{n+1} a_i \bar{\chi}_i \\ &= \chi - \langle \chi, \lambda_1 - \lambda_2 \rangle (\bar{\chi}_1 - \bar{\chi}_2). \end{aligned}$$

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 $\{1, 2, \dots, n+1\}$ is replaced with an unordered set, we find that everything is symmetric between the roots, and so the coroot of α_{ij} is

$$\alpha_{ij}^\vee = \lambda_i - \lambda_j$$

for all $i \neq j$.

EXAMPLE (B_n): SO_{2n+1} .

Consider the symmetric bilinear form ϕ on k^{2n+1} ,

$$\phi(\vec{x}, \vec{y}) = 2x_0y_0 + x_1y_{n+1} + x_{n+1}y_1 + \cdots + x_ny_{2n} + x_{2n}y_n$$

Then $\mathrm{SO}_{2n+1} \stackrel{\text{def}}{=} \mathrm{SO}(\phi)$ consists of the $2n+1 \times 2n+1$ matrices A of determinant 1 such that

$$\phi(A\vec{x}, A\vec{y}) = \phi(\vec{x}, \vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix}.$$

The Lie algebra of SO_{2n+1} consists of the $2n+1 \times 2n+1$ matrices A of trace 0 such that

$$\phi(A\vec{x}, \vec{y}) + \phi(\vec{x}, A\vec{y}) = 0,$$

i.e., such that

$$A^t \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I \\ 0 & I & 0 \end{pmatrix} A = 0.$$

Take T to be the maximal torus of diagonal matrices

$$\mathrm{diag}(1, t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1})$$

Then

$$X^*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i, \quad \chi_i: \text{diag}(1, t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) \mapsto t_i$$

$$X_*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\lambda_i, \quad \lambda_i: t \mapsto \text{diag}(1, \dots, t^{i+1}, \dots, 1)$$

with the pairing $\langle \cdot, \cdot \rangle$ such that

$$\langle \chi_i, \lambda_j \rangle = \delta_{ij}.$$

All the characters

$$\pm \chi_i, \quad \pm \chi_i \pm \chi_j, \quad i \neq j$$

occur as roots, and their coroots are, respectively,

$$\pm 2\lambda_i, \quad \pm \lambda_i \pm \lambda_j, \quad i \neq j.$$

EXAMPLE (C_n): Sp_{2n} .

Consider the skew symmetric bilinear form $k^{2n} \times k^{2n} \rightarrow k$,

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

Then Sp_{2n} consists of the $2n \times 2n$ matrices A such that

$$\phi(A\vec{x}, A\vec{y}) = \phi(\vec{x}, \vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The Lie algebra of Sp_n consists of the $2n \times 2n$ matrices A such that

$$\phi(A\vec{x}, \vec{y}) + \phi(\vec{x}, A\vec{y}) = 0,$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} + \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} A = 0.$$

Take T to be the maximal torus of diagonal matrices

$$\text{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}).$$

Then

$$X^*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\chi_i, \quad \chi_i: \text{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) \mapsto t_i$$

$$X_*(T) = \bigoplus_{1 \leq i \leq n} \mathbb{Z}\lambda_i, \quad \lambda_i: t \mapsto \text{diag}(1, \dots, t^i, \dots, 1)$$

with the obvious pairing $\langle \cdot, \cdot \rangle$. All the characters

$$\pm 2\chi_i, \quad \pm \chi_i \pm \chi_j, \quad i \neq j$$

occur as roots, and their coroots are, respectively,

$$\pm \lambda_i, \quad \pm \lambda_i \pm \lambda_j, \quad i \neq j.$$

EXAMPLE (D_n): SO_{2n} .

Consider the symmetric bilinear form $k^{2n} \times k^{2n} \rightarrow k$,

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

Then $SO_n = SO(\phi)$ consists of the $n \times n$ matrices A of determinant 1 such that

$$\phi(A\vec{x}, A\vec{y}) = \phi(\vec{x}, \vec{y}),$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

The Lie algebra of SO_n consists of the $n \times n$ matrices A of trace 0 such that

$$\phi(A\vec{x}, \vec{y}) + \phi(\vec{x}, A\vec{y}) = 0,$$

i.e., such that

$$A^t \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} + \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} A = 0.$$

When we write the matrix as $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, then this last condition becomes

$$A + D^t = 0, \quad C + C^t = 0, \quad B + B^t = 0.$$

Take T to be the maximal torus of diagonal matrices

$$\text{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1})$$

and let χ_i , $1 \leq i \leq r$, be the character

$$\text{diag}(t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}) \mapsto t_i.$$

All the characters

$$\pm \chi_i \pm \chi_j, \quad i \neq j$$

occur, and their coroots are, respectively,

$$\pm \lambda_i \pm \lambda_j, \quad i \neq j.$$

REMARK 22.52. The subscript on A_n, B_n, C_n, D_n denotes the rank of the group, i.e., the dimension of a maximal torus.

h. The Weyl groups and Borel subgroups

Let (G, T) be a split reductive group over k . The Weyl group of (G, T) is

$$W(G, T) = N_G(T)/C_G(T) = \pi_0(N_G(T)).$$

Thus, $W(G, T)$ is an étale group scheme over k . It acts faithfully on T , and hence on $X^*(T)$. For each root $\alpha \in R(G, T)$, $W(G, T)(k)$ contains the reflection s_α . In this section, we show that $W(G, T)$ is generated by the s_α . In particular, this means $W(G, T)$ is a constant finite group scheme.

Let $\mathcal{R} = (X^*(T), R, \alpha \mapsto \alpha')$ be the root datum of (G, T) . Let $V = X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$ and $V^\vee = X_*(T) \otimes_{\mathbb{Z}} \mathbb{R}$. For a root $\alpha \in R$, 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} are the connected components of

$$V^\vee \setminus \bigcup_{\alpha \in R} H_\alpha.$$

DEFINITION 22.53. An cocharacter λ in $X_*(T)$ is **regular** if, for all $\alpha \in R$, $\langle \alpha, \lambda \rangle \neq 0$, i.e., λ is contained in a Weyl chamber.

LEMMA 22.54. *If the cocharacter λ is regular, then $\mathcal{B}^T = \mathcal{B}^{\lambda(\mathbb{G}_m)}$.*

PROOF. We may replace k with its algebraic closure. Let X be a connected component of $\mathcal{B}^{\lambda(\mathbb{G}_m)}$. Then X is complete and it is stable under T , and so it contains a fixed point B (18.4). We have an isomorphism $G/B \rightarrow \mathcal{B}$ mapping eB to B . In particular, the tangent space of \mathcal{B} at B is isomorphic to $\mathfrak{g}/\mathfrak{b}$. Now $\mathfrak{t} \subset \mathfrak{b}$, and so

$$T_B \mathcal{B} \simeq \mathfrak{g}/\mathfrak{b} = \bigoplus_{\alpha \in R(B)} \mathfrak{g}_\alpha$$

for some subset $R(B)$ of R . The weights of \mathbb{G}_m on this space are the integers $\langle \alpha, \lambda \rangle$ for $\alpha \in R(B)$, which are nonzero by assumption. On the other hand \mathbb{G}_m acts trivially on X and $T_B X$; therefore $T_B X = 0$ and X has dimension 0. Thus $\mathcal{B}^{\lambda(\mathbb{G}_m)}$ is finite and stable under T , and hence contained in \mathcal{B}^T . □

LEMMA 22.55. *Let $B \in \mathcal{B}^T$, and let $\alpha \in R(G, T)$. Then B contains exactly one of U_α or $U_{-\alpha}$.*

PROOF. Define T_α and G_α as in (22.43). Then G_α contains exactly two Borel subgroups containing T , namely, $T \cdot U_\alpha$ and $T \cdot U_{-\alpha}$. As $B \cap G_\alpha$ is a Borel subgroup of G_α containing T , the statement follows. □

LEMMA 22.56. *Let λ be a regular cocharacter of T . There is a unique Borel subgroup $B(\lambda) \in \mathcal{B}^T$ such that*

$$\text{Lie}(B(\lambda)) = \mathfrak{t} \oplus \bigoplus_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_\alpha.$$

The group $B(\lambda)$ depends only on the Weyl chamber containing λ .

PROOF. In fact, $P(\lambda)$ has this property (21.15). Any Borel subgroup B with $\mathfrak{b} = \mathfrak{t} \oplus \bigoplus_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_\alpha$ is generated by the subgroups T and U_α , $\langle \alpha, \lambda \rangle > 0$, and so equals $P(\lambda)$. If λ' lies in the same Weyl chamber as λ , then

$$\langle \alpha, \lambda \rangle > 0 \iff \langle \alpha, \lambda' \rangle > 0,$$

and so $B(\lambda) = B(\lambda')$. □

NOTATION 22.57. (a) Let C be a Weyl chamber; we set $B(C) = B(\lambda)$ for any $\lambda \in C$. It is a Borel subgroup containing T , which is independent of λ (22.56).

(b) For $B \in \mathcal{B}^T$, let $R^+(B) = \{\alpha \in R \mid U_\alpha \in B\} = \{\alpha \in R \mid \mathfrak{g}_\alpha \in \mathfrak{b}\}$.

(c) For $B \in \mathcal{B}^T$, let

$$C(B) = \{f \in V^\vee \mid \langle \alpha, f \rangle > 0 \text{ for all } \alpha \in R^+(B)\}.$$

THEOREM 22.58. *The map $C \mapsto B(C)$ is bijective, with inverse $B \mapsto C(B)$.*

PROOF. Let $B \in \mathcal{B}^T$, let C be a Weyl chamber, and let $\lambda \in C$. There exists an $n \in N_G(T)(k^{\text{al}})$ such that $B = nB(\lambda)n^{-1}$. Let $w = \dot{n}$ be the class of n in $W(G, T)(k^{\text{al}})$.

$$\begin{aligned} \mathfrak{b} &= \text{Lie}(B) = \text{Lie}(nB(\lambda)n^{-1}) \\ &= \mathfrak{h} \oplus \bigoplus_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_{w(\alpha)} \\ &= \mathfrak{h} \oplus \bigoplus_{\langle \beta, w^{-1}(\lambda) \rangle > 0} \mathfrak{g}_{\beta} \\ &= \mathfrak{b}_{w^{-1}(\lambda)}. \end{aligned}$$

Thus $B = B(w^{-1}(\lambda))$ and the map $C \mapsto B(C)$ is surjective. Furthermore, we have that $C(B)$ is the chamber $w^{-1}(C)$ proving that the map is injective. \square

THEOREM 22.59. *The group scheme $W(G, T)$ is generated by the s_{α} , $\alpha \in R$, i.e., the abstract group $W(G, T)(k^{\text{al}})$ is generated by the s_{α} .*

PROOF. Let $\mathcal{R} = (X^*(T), R, \alpha \mapsto \alpha^{\vee})$ be the root datum of (G, T) . By definition, its Weyl group $W(\mathcal{R})$ is the group of automorphisms of $X^*(T)$ generated by the reflections s_{α} , $\alpha \in R$. The Weyl group $W(\mathcal{R})$ of \mathcal{R} acts simply transitively on the set of Weyl chambers — this is an elementary statement about sets of hyperplanes in real vector spaces and groups generated by symmetries (see 23.16 or Bourbaki LIE V, §3). On the other hand, $W(G, T)(k^{\text{al}})$ acts simply transitively on the set of Borel subgroups of $G_{k^{\text{al}}}$ containing $T_{k^{\text{al}}}$ (18.59). Thus, it suffices to construct a bijection from the set of Weyl chambers of the root datum $\mathcal{R}(G, T)$ to the set of Borel subgroup of $G_{k^{\text{al}}}$ containing $T_{k^{\text{al}}}$ compatible with the actions of the Weyl groups. This Theorem 22.58 does. \square

COROLLARY 22.60. *Regard $W(\mathcal{R})$ as a constant finite group scheme. Then the canonical map $W(\mathcal{R}) \rightarrow \pi_0(N_G(T))$ is an isomorphism. Moreover, the homomorphism $N_G(T) \rightarrow \pi_0(N_G(T))$ has a section, and so*

$$N_G(T) = N_G(T)^{\circ} \rtimes \pi_0(N_G(T)).$$

PROOF. The first statement restates the theorem. For the second, we have to show that every element w of $W(G, T)(k)$ is represented by an element n_w of $N_G(T)(k)$. It suffices to check this for s_{α} , but s_{α} is represented by an element of $N_{G_{\alpha}}(T_{\alpha})(k)$ (21.59). \square

We can rewrite the displayed equation as

$$N_G(T) = C_G(T) \rtimes W(G, T).$$

EXAMPLE 22.61. Let $G = \text{SL}_2$ with T the standard (diagonal) torus. In this case, $C_G(T) = T$ and

$$N_G(T) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & a^{-1} \\ -a & 0 \end{pmatrix} \right\}.$$

Therefore $W(G, T) = \{1, s\}$ where s is represented by the matrix $n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Note that

$$n \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} n^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix},$$

and so s interchanges $\text{diag}(a, a^{-1})$ and $\text{diag}(a^{-1}, a)$.

EXAMPLE 22.62. Let $G = \mathrm{GL}_n$ and $T = \mathbb{D}_n$. In this case, $C_G(T) = T$ but $N_G(T)$ contains the permutation matrices (those obtained from the identity matrix I by permuting the rows). For example, let $E(ij)$ be the matrix obtained from I by interchanging the i th and j th 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 $\{1, \dots, n\}$, and let $E(\sigma)$ be the matrix obtained by using σ to permute the rows. Then $\sigma \mapsto E(\sigma)$ is an isomorphism from S_n onto the set of permutation matrices, and conjugating a diagonal matrix by $E(\sigma)$ simply permutes the diagonal entries. The $E(\sigma)$ form a set of representatives for $C_G(T)(k)$ in $N_G(T)(k)$, and so $W(G, T) \simeq S_n$.

i. Subgroups normalized by T

LEMMA 22.63. Let (G, T) be a split reductive group, and let H be a connected subgroup variety of G normalized by T . If $\mathfrak{g}_\alpha \subset \mathrm{Lie}(H)$ for some root α , then $U_\alpha \subset H$.

PROOF. We may suppose that k is algebraically closed. Then $(H \cap G_\alpha)_{\mathrm{red}}^\circ$ is a connected subgroup variety of G_α , which contains U_α because its Lie algebra contains \mathfrak{g}_α (21.61). Therefore H contains U_α . [Cf. 21.61.] \square

THEOREM 22.64. Let (G, T) be a split reductive group. Let B be a Borel subgroup containing T , and let $R^+(B) = \{\alpha_1, \dots, \alpha_r\}$ be the corresponding set of positive roots (22.57).

(a) The multiplication morphism

$$\Phi: U_{\alpha_1} \times \cdots \times U_{\alpha_r} \rightarrow B_u$$

is an isomorphism of algebraic varieties with an action of T .

(b) The morphism $B_u \rtimes T \rightarrow B$ is an isomorphism.

(c) Let U be a subgroup variety of B_u normalized by T , and let $\{\beta_1, \dots, \beta_s\}$ be the weights of T on $\mathrm{Lie}(U)$. Then U is connected, and the multiplication morphism

$$U_{\beta_1} \times \cdots \times U_{\beta_s} \rightarrow U$$

is an isomorphism of algebraic varieties with an action of T .

PROOF. (a) Let $V = U_{\alpha_1} \times \cdots \times U_{\alpha_r}$. There are natural actions of T on V and B_u for which the map Φ is equivariant. Note that Φ induces an isomorphism $d_e \Phi$ on the tangent spaces $T_e V \rightarrow T_e B_u$. Let λ lie in the Weyl chamber of B ; then the weights of $\lambda(\mathbb{G}_m)$ on V and B_u are positive. Now (19.9) shows that the Luna maps $V \rightarrow T_e V$ and $B_u \rightarrow T_e B_u$ are isomorphisms, and so Φ is an isomorphism.

(b) We saw in the proof of Lemma 22.56 that every Borel subgroup B containing T is of the form $P(\lambda)$ for some regular character λ . Then $B_u = U(\lambda)$ and $T = Z(\lambda)$, and so the required isomorphism is the isomorphism $U(\lambda) \rtimes Z(\lambda) \rightarrow P(\lambda)$ of (21.13).

(c) If U is connected, then, because of (22.63), the same proof applies as in (a). Therefore, it remains to show that U is connected. From (a) and (b) we obtain an isomorphism

$$U^\circ \times W \rightarrow B_u$$

with $W = \prod \{U_\alpha \mid \alpha \in R^+, U_\alpha \notin U^\circ\}$. On restricting to U , we get an isomorphism

$$U^\circ \times U \cap W \rightarrow U,$$

and on dividing by U° , we get an isomorphism $U \cap W \rightarrow U/U^\circ$. This last group is finite and stable under T (because U and W are). As T is connected, all the points of $U \cap W$ are fixed by T , and so lie in $C_G(T) = T$. Hence $U \cap W \subset B_u \cap T = \{e\}$, and it follows that U is connected. \square

j. Big cells and the Bruhat decomposition

Let $G = \text{GL}_n$ with T the diagonal torus and B the standard Borel subgroup. The Weyl group W is the group of permutation matrices, and every matrix can be written uniquely as a product $U_1 P U_2$ with U_1, U_2 upper triangular and P in W , i.e.,

$$G = \coprod_{w \in W} B(k)wB(k).$$

In this section, we show that every split reductive group has such a (Bruhat) decomposition.

Let (G, T) be a split reductive group, and let $B \in \mathcal{B}^T$. Let $R^+ = R^+(B)$ denote the set of positive roots defined by B (22.57). For $w \in W$, the coset wB is independent of w , and we let e_w denote the point wB/B in G/B — it is fixed by T .

DEFINITION 22.65. The *dominant Weyl chamber* for B is

$$C^+ = \{\lambda \in X_*(T) \otimes_{\mathbb{Z}} \mathbb{R} \mid \langle \alpha, \lambda \rangle > 0 \text{ for all } \alpha \in R^+\}.$$

Choose a representation (V, r) of G such that B is the stabilizer of a line in V , so that $G/B \hookrightarrow \mathbb{P}(V)$. Fix a $\lambda \in C^+$. When k is algebraically closed, we have a Białynicki-Birula decomposition (19.12):

$$G/B = \bigsqcup_{w \in W} C(w), \quad C(w) = \{x \in G/B \mid \lim_{t \rightarrow 0} \lambda(t) \cdot x = e_w\}.$$

Here $C(w)$ is a locally closed subset of $|X|$; for a unique (attracting) point, $C(w)$ is open and dense in G/B , and for a unique (repelling) point, $C(w)$ is a single point.

PROPOSITION 22.66. Suppose that k is algebraically closed. The cell $C(w)$ is the B_u -orbit Ue_w in G/B .

PROOF. Let \mathbb{G}_m act on G and G/B via the character λ , and let $x \in C(w)$. As the weights of \mathbb{G}_m on $\mathfrak{u} = \text{Lie}(B_u)$ are > 0 , for all $u \in B_u$ and $t \in \mathbb{G}_m$, we have $\lim_{t \rightarrow 0} \lambda(t) \cdot u \cdot \lambda(t)^{-1} = 1$. This implies that

$$\lim_{t \rightarrow 0} \lambda(t)ux = \lim_{t \rightarrow 0} \lambda(t)u\lambda(t)^{-1} \cdot \lambda(t)u = e_w.$$

This proves that $C(w)$ is stable under the action of U . Therefore $B_u e_w \subset C(w)$.

Conversely, if $B_u x$ is a nonempty open B_u -orbit in $C(w)$, then, by the Kostant-Rosenlicht theorem (19.25), this orbit is closed, and therefore $e_w \in B_u x$ and $B_u x = B_u e_w$. This proves that $C(w) = B_u e_w$. \square

As the Weyl group acts simply transitively on the Weyl chambers, there exists a unique $w_0 \in W$ such that $w_0(C^+) = -C^+$. Moreover, w_0 is an involution as $w_0^2(C^+) = C^+$. We choose a representative n_0 for w_0 in $N_G(T)(k)$.

THEOREM 22.67 (BRUHAT DECOMPOSITION). (a) *We have the cellular Bruhat decompositions*

$$\begin{aligned} G/B &= \bigsqcup_{w \in W} B_u n_w B/B \\ G &= \bigsqcup_{w \in W} B_u n_w B. \end{aligned}$$

(b) *The open orbit for the action of B_u on G/B is $B_u n_0 B/B$ and the open orbit for the action of $B_u \times B$ on G is $B_u n_0 B$.*

PROOF. (a) The first equality is the Białyński-Birula decomposition (19.12), and the second follows from it.

(c) Recall that the tangent space $T_{e_{w_0}}(G/B)$ can be identified with

$$\mathfrak{g}/n_0(\mathfrak{b}) \simeq \bigoplus_{\alpha \in R^+} \mathfrak{g}_\alpha.$$

Therefore, all the weights are positive in the tangent space, and so, by Theorem 19.12, this is a dense open orbit. \square

THE SUBGROUPS U_w AND U^w .

Let $U = B_u$. Let $R^- = -R^+$ and $U^- = n_0(U)$. Then U^- is a subgroup variety of G normalized by T , and hence equal to the product of the groups U_α such that $\mathfrak{g}_\alpha \subset U^-$. Note that

$$\begin{cases} U_\alpha \subset U & \iff \alpha \in R^+ \\ U_\alpha \subset U^- & \iff \alpha \in R^-. \end{cases} \quad (157)$$

DEFINITION 22.68. For $w \in W$, define

$$\begin{aligned} U_w &= U \cap n_w(U) \\ U^w &= U \cap n_w(U^-). \end{aligned}$$

LEMMA 22.69. *The algebraic subgroups U_w and U^w of G are smooth and normalized by T (hence equal to the product of the groups U_α they contain).*

PROOF. We may suppose that k is algebraically closed. Then $(U_w)_{\text{red}}$ is smooth and normalized by T , and so is equal to

$$\prod \{U_\alpha \mid \alpha \in R^+ \cap w(R)^+\}.$$

From the exact sequence

$$0 \rightarrow \text{Lie}(U_w) \rightarrow \text{Lie}(U) \times \text{Lie}(n_w(U)) \rightarrow \text{Lie}(G)$$

we see that the Lie algebra of U_w is

$$\bigoplus \{\text{Lie}(U_\alpha) \mid \alpha \in R^+ \cap w(R)^+\}.$$

Hence $\dim(U_w) = \dim(\text{Lie}(U_w))$, and so U_w is smooth. The proof for U^w is similar. \square

LEMMA 22.70. (a) *For all $w \in W$, $U_w \cap U^w = e$.*

(b) *Multiplication induces an isomorphism*

$$U_w \times U^w \rightarrow U.$$

PROOF. We may suppose k to be algebraically closed.

(a) The subgroup variety $(U_w \cap U^w)_{\text{red}}$ is normalized by T , and so is equal to the product of the U_α that it contains. But

$$\begin{aligned} U_\alpha \subset U_w &\iff \alpha \in R^+ \cap w(R^+) \\ U_\alpha \subset U^w &\iff \alpha \in R^+ \cap w(R^-). \end{aligned}$$

These conditions are exclusive, which proves that $(U_w \cap U^w)_{\text{red}} = e$. On the other hand, $\text{Lie}(U_w \cap U^w) = 0$, and so $U_w \cap U^w$ is smooth, and hence trivial.

(b) Every root α satisfies one of the above conditions and U is smooth. Therefore the homomorphism $U_w \times U^w \rightarrow U$ is surjective which, together with (a), proves (b). \square

PROPOSITION 22.71. (a) *For $w \in W$, the stabilizer of e_w in G (resp. U) is $n_w(B)$ (resp. U_w); hence the stabilizer of e_w in \mathfrak{g} (resp. \mathfrak{u}) is $n_w(\mathfrak{b})$ (resp. $\mathfrak{u} \cap n_w(\mathfrak{b}) = \text{Lie}(U_w)$).*

(b) *There is an equality $Ue_w = U^w e_w$ and the orbit map $U^w \rightarrow U^w e_w = Ue_w$ is an isomorphism. In particular, $\dim Ue_w = n(w)$ with $n(w) = |R^+ \cap w(R^-)|$.*

PROOF. (a) Let $\pi: G \rightarrow G/B$ be the quotient map. The stabilizer of $e_w = n_w B/B$ is obviously $n_w(B)$ since the stabilizer of $eB/B = e$ is B . Translating π by n_w , we get $\pi_w: G \rightarrow G/B$ defined by $\pi_w(g) = gn_w B/B$. The stabilizer of eG/B is now $n_w(B)$. The statement for the Lie algebras follows from the statement for groups by considering the $k[\varepsilon]$ -points.

The stabilizer of e_w in U is $U \cap n_w(B) = U \cap n_w(U) = U_w$, and the kernel of the restriction of $(d\pi_w)_e \cap \mathfrak{u} = n_w(\mathfrak{b}) \cap \mathfrak{u} = \text{Lie}(U_w)$. Since $U_w \times U^w \rightarrow U$ is an isomorphism, the morphism $U^w \rightarrow U^w e_w$ is bijective and the kernel of the differential is $\text{Lie}(U^w) \cap \text{Lie}(U_w) = 0$; therefore it is separable and an isomorphism. \square

THEOREM 22.72 (BRUHAT DECOMPOSITION). *Let G be a reductive algebraic group.*

(a) *There are decompositions*

$$\begin{aligned} G &= \bigsqcup_{w \in W} U^w n_w B \\ G/B &= \bigsqcup_{w \in W} U^w n_w B/B \end{aligned}$$

and for every $w \in W$, the morphism

$$U^w \times B \rightarrow U^w n_w B, \quad (u, b) \mapsto un_w b$$

is an isomorphism. In particular, every element $g \in G(k^{\text{al}})$ can be written uniquely as

$$g = un_w t u', \quad u \in U^w, \quad t \in T, \quad u' \in U.$$

(b) *There are open coverings*

$$\begin{aligned} G &= \bigcup_{w \in W} n_w U^- B \\ G/B &= \bigcup_{w \in W} n_w U^- B/B. \end{aligned}$$

PROOF. (a) This summarizes what was proved above.

(b) We have shown that U^-B and U^-B/B are open subsets containing e . Therefore, their translates by n_w are open subsets containing n_w . Their unions are all of G or G/B because $n_wU^-B = (n_wU^-n_w^{-1})n_wB \supset U^wn_wB$ and the decomposition in (a). \square

DEFINITION 22.73. For $w \in W$, let

$$N(w) = \{\alpha \in R^+ \mid w^{-1}(\alpha) \in R^-\} = R^+ \cap w(R^-),$$

and let $n(w) = |N(w)|$.

22.74. For $w \in W$,

$$(a) \dim C(w) = \dim U^w = n(w).$$

$$(b) n(w) = n(w^{-1}) \text{ and } n(w_0w) = n(ww_0) = |R^+| - n(w).$$

COROLLARY 22.75. We have

$$\dim G = \dim T + |R|.$$

PROOF. Count dimensions in

$$G = VTU = \prod_{\alpha \in R^+} U_{-\alpha} \cdot T \cdot \prod_{\alpha \in R^+} U_{\alpha}. \quad \square$$

EXAMPLE 22.76. Let (G, T) be GL_n with its diagonal torus. The roots are

$$\alpha_{ij}: \mathrm{diag}(t_1, \dots, t_n) \mapsto t_i t_j^{-1}, \quad i, j = 1, 2, \dots, n, \quad i \neq j.$$

The corresponding root groups are $U_{ij} = \{I + aE_{ij} \mid a \in k\}$. Let $R^+ = \{\alpha_{ij} \mid i < j\}$. Then U and V are, respectively, the groups of superdiagonal and subdiagonal unipotent matrices and C is the set of matrices for which the $i \times i$ minor in the upper left hand corner is nonzero for all i .

THE BIG CELL (FOLLOWING SHS)

THEOREM 22.77. Let (B, T) be a Borel pair in a connected group variety G . Then there exists a unique Borel subgroup B' of G containing T and such that

$$B \cap B' = T \cdot R_u(G).$$

Moreover, $B' \cdot B$ is an open subscheme of G .

For example, let B be the group of upper triangular matrices in GL_n , and let T be the diagonal torus. Then B' is the group of lower triangular matrices. 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.

Before proving the theorem, we list some consequences.

COROLLARY 22.78. Let (B, T) be a Borel pair in a reductive group G . Then there exists a unique Borel subgroup B' of G such that $B \cap B' = T$; the map

$$(b', t, b) \mapsto b'tb: B'_u \times T \times B_u \rightarrow G$$

is an open immersion.

PROOF. As $R_u G = e$, there exists a unique B' such that $B \cap B' = T$. Let $B'_u \times B$ act on B by left and right translations, and let H be the isotropy group at e . The canonical map $(B'_u \times B)/H \rightarrow G$ is an immersion (9.27). But $B'_u \cap B = e$, and so $H = e$ and

$$(b', b) \mapsto b'eb: B'_u \times B \rightarrow G$$

is an immersion. It is an open immersion because $\mathfrak{b} + \mathfrak{b}' = \mathfrak{g}$ (see 22.80). \square

COROLLARY 22.79. *Let G be a connected group variety. The field of rational functions of G is a pure transcendental extension of k .*

PROOF. If G is reductive, the open subscheme $B'_u \cdot T \cdot B_u$ of G is isomorphic to an open subscheme of affine space, which proves the statement in this case.

Let S be an algebraic scheme. Then $H^1(S, \mathbb{G}_a) = H^1(S, \mathcal{O}_S)$, which equals 0 if S is affine. It follows that $H^1(S, U) = 0$ if U has a filtration whose quotients are isomorphic to \mathbb{G}_a . The exact sequence

$$1 \rightarrow R_u(G) \rightarrow G \rightarrow G/R_u G \rightarrow 1$$

realizes G as a torsor under $R_u(G)$ over $G/R_u G$. It is the trivial torsor, and so G is isomorphic as a scheme to

$$R_u(G) \times (G/R_u(G)). \quad \square$$

PROOF OF THEOREM 22.77

Because of the one-to-one correspondence between Borel subgroups of G containing T and Borel subgroups of $G/R_u(G)$ containing the image of T (18.24), we may suppose that G is reductive.

Let λ be a regular cocharacter of T such that $B = P(\lambda)$, and let $B' = P(-\lambda)$. We prove that $B \cap B' = T$ and $B \cdot B'$ is an open subscheme of G . For this, we may suppose that k is algebraically closed.

Let

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$$

be the decomposition of $\mathfrak{g} \stackrel{\text{def}}{=} \text{Lie}(G)$ under the action of T . As B and B' contain T , and as

$$\mathfrak{g}_0 = \text{Lie}(C_G(T)) = \text{Lie}(T)$$

(19.19), we have

$$\begin{aligned} \mathfrak{b} &= \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha \cap \mathfrak{b} \\ \mathfrak{b}' &= \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha \cap \mathfrak{b}'. \end{aligned}$$

LEMMA 22.80. *We have*

$$\begin{aligned} \mathfrak{b} \cap \mathfrak{b}' &= \mathfrak{g}^0 \\ \mathfrak{b} + \mathfrak{b}' &= \mathfrak{g} \end{aligned}$$

PROOF. If this were false, then there would exist an $\alpha \in R$ with

$$\mathfrak{g}_\alpha \cap (\mathfrak{b} \cap \mathfrak{b}') \neq 0$$

or

$$\mathfrak{g}_\alpha \not\subset \mathfrak{b} + \mathfrak{b}'.$$

Consider $T_\alpha = (\text{Ker } \alpha)_{\text{red}}^\circ$ and $G_\alpha = C_G(T_\alpha)$. Then

$$\text{Lie}(G_\alpha) = \mathfrak{g}^{T_\alpha} \supset \mathfrak{g}_\alpha,$$

and therefore $G_\alpha \neq T$ and T_α is a singular torus. But G_α is a reductive group of semisimple rank 1, and $B \cap G_\alpha$ and $B' \cap G_\alpha$ are the two Borel subgroups of G_α containing T . But

$$(B \cap G_\alpha) \cap (B' \cap G_\alpha) = T$$

(21.47), and

$$\text{Lie}(B' \cap G_\alpha) = \text{Lie}(G_\alpha).$$

Therefore

$$\mathfrak{g}_\alpha \cap \mathfrak{b} \cap \mathfrak{b}' = 0$$

and

$$\mathfrak{g}_\alpha \subset \mathfrak{b} + \mathfrak{b}'.$$

Therefore

$$\text{Lie}(B \cap B') = \text{Lie}(T),$$

and so $\text{Lie}(B_u \cap B'_u) = 0$. As $B_u \cap B'_u$ is connected (19.29, which applies because $B_u^T = e$), we certainly have $B_u \cap B'_u = e$, and so $B \cap B' = T$. Make the group $B'_u \times B$ act by left and right translation on G :

$$(b, b')x = b'xb^{-1}.$$

Then $(B', B)(k) = (B'_u \cdot B)(k)$ and the orbit of e is therefore a locally closed subset of $G(k)$. As $B'_u \cap B = e$, its dimension is

$$\begin{aligned} \dim(B) + \dim(B'_u) &= \dim(B) + \dim(B') - \dim(T) \\ &= \dim(\mathfrak{b}) + \dim(\mathfrak{b}') - \dim(\mathfrak{g}_0) \\ &= \dim(\mathfrak{g}) \\ &= \dim(G). \end{aligned}$$

It follows that $\overline{(B' \cdot B)(k)} = G(k)$, hence $(B' \cdot B)(k)$ is open in $G(k)$, and $B' \cdot B$ is certainly an open subscheme of G .

Finally, we prove the uniqueness. Let B_1 be a Borel subgroup of G containing T and such that $B_1 \cap B = T$. For any torus S of codimension 1 in T , we have $B_1^S \cap B^S = T$, hence necessarily $B_1^S = B'^S$, which proves that $B_1 = B'$ by 19.31. \square

COROLLARY 22.81. *The intersection of the Borel subgroups of G is the product of the diagonalizable part of $Z(G)$ with $R_u(G)$.*

PROOF. It is the product of $R_u(G)$ with the intersection of the maximal tori of G . \square

COROLLARY 22.82. *Let B be a Borel subgroup of G , and let T be a maximal torus. Then*

$$\dim(G) = \dim(T) + 2\dim(B_u) - \dim(R_u(G)).$$

k. The parabolic subgroups

Let (G, T) be a split reductive group.

THEOREM 22.83. *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.*

If $P \supset T$, then $P = P(\lambda)$ for any cocharacter λ of T such that the set of weights of T acting on $\text{Lie}(P)$ consists of the roots α of (G, T) with $\langle \alpha, \lambda \rangle \geq 0$.

We now fix a Borel subgroup B of G containing T , and describe the parabolic subgroups of G containing B . Fix a base S for $R^+(B)$, and let I be a subset of S . Let $R_I = \mathbb{Z}I \cap R$, let $S_I = \left(\bigcap_{\alpha \in I} \text{Ker}(\alpha)\right)_{\text{red}}^\circ$, and let $L_I = C_G(S_I)$.

LEMMA 22.84. (a) *The pair (L_I, T) is a split reductive group with root datum $(X^*(T), R_I, \alpha \mapsto \alpha^\vee)$; its Weyl group W_I is the subgroup of W generated by the s_α with $\alpha \in I$.*

(b) *The intersection $B \cap L_I$ is a Borel subgroup B_I of L_I , and $R^+(B_I) = R_I \cap R^+(B)$ has base I .*

PROOF. Omitted for the moment (Perrin p.110, Springer p147). □

Recall that, for $w \in W(G, T)$,

$$C(w) = \{x \in G/B \mid \lim_{t \rightarrow 0} \lambda(t) \cdot x = wB/B\}$$

for any (one or all) λ in the dominant Weyl chamber for B , and that $C(w)$ is the B_u -orbit of wB/B .

THEOREM 22.85. *For each subset I of S , there is a unique parabolic subgroup P_I of G containing B such that*

$$P_I = \bigcup_{w \in W_I} C(w).$$

The unipotent radical of P_I is generated by the U_α with $\alpha \in R^+ \setminus R_I$, and the map

$$R_u(P_I) \rtimes L_I \rightarrow P_I$$

is an isomorphism. Every parabolic subgroup P of G containing B is of the form P_I for a unique subset I of S .

We prove these theorems in several steps.

STEP 1. **THEOREM 22.83** IS TRUE OVER k IF IT IS TRUE OVER k^{al} .

Let λ be a cocharacter of G . Then $P(\lambda)$ is parabolic because $P(\lambda)_{k^{\text{al}}} = P(\lambda_{k^{\text{al}}})$ is parabolic. For the converse, let P be a parabolic subgroup of G , and let T be a maximal torus in P . Let $R \subset X^*(T)$ be the set of roots of (G_k, T_k) . The nonzero weights of T on $\text{Lie}(P)$ form a subset R' of R stable under $\Gamma \stackrel{\text{def}}{=} \text{Gal}(k^{\text{sep}}/k)$. Let

$$\Lambda = \{\lambda \in X_*(T) \mid \langle \alpha, \lambda \rangle > 0 \iff \alpha \in R'\}.$$

By hypothesis, $P_{k^{\text{al}}} = P(\lambda)$ for some $\lambda \in X_*(T)$, and such a $\lambda \in \Lambda$. Therefore Λ is nonempty. Because R' is stable under Γ , so also is Λ . The group Γ acts on $X_*(T)$ through a finite quotient Γ' , and we let

$$\lambda' = \sum_{\gamma \in \Gamma'} \gamma \lambda.$$

Then $P = P(\lambda')$.

The remaining steps are omitted for the moment. See Springer 1998, 8.4.3, p.147, and 15.1.2, p.252.

22.86. Let G be a connected group variety over k . The subgroups of G of the form $P(\lambda)$ with λ a cocharacter of G are said to be **pseudo-parabolic**. They are smooth and connected (21.13). When G is reductive or k is perfect, the pseudo-parabolic subgroups are exactly the parabolic subgroups (22.83). In general, G contains a proper pseudo-parabolic subgroup if and only if $G/R_u(G)$ contains a split noncentral torus. If k is infinite, the unipotent group $U(\lambda)$ is split. Let P be a pseudo-parabolic subgroup of G . If k is infinite, the quotient map $G \rightarrow G/P$ has local sections for the Zariski topology, and so $G(k) \rightarrow (G/P)(k)$ is surjective. See Springer 1998, 15.1 (to be included).

1. The isogeny theorem: statements

All root data are reduced. The field k has characteristic exponent p (possibly 1).

Let (G, T) be a split reductive group, and let $R \subset X^*(T)$ be the root system of (G, T) . For each $\alpha \in R$, let U_α be the corresponding root group. Recall that U_α is the unique algebraic subgroup of G isomorphic to \mathbb{G}_a , normalized by T , and such that, for every isomorphism $u_\alpha: \mathbb{G}_a \rightarrow U_\alpha$,

$$t \cdot u_\alpha(a) \cdot t^{-1} = u_\alpha(\alpha(t)a), \quad t \in T(R), a \in \mathbb{G}_a. \quad (158)$$

Recall that a root datum is a triple $(X, R, \alpha \mapsto \alpha^\vee)$ with X a free \mathbb{Z} -module of finite rank, R a subset of X , and $\alpha \mapsto \alpha^\vee$ an injective homomorphism $R \rightarrow X^\vee$ satisfying the conditions (rd1–3), p. 389. Here X^\vee is the \mathbb{Z} -linear dual of X . We sometimes write f for the map $\alpha \mapsto \alpha^\vee$.

DEFINITION 22.87. An **isogeny** of root data $(X, R, \alpha \mapsto \alpha^\vee) \rightarrow (X', R', \alpha' \mapsto \alpha'^\vee)$ is a homomorphism $\varphi: X' \rightarrow X$ such that

- (a) φ is injective with finite cokernel (equivalently, both φ and its \mathbb{Z} -linear dual φ^\vee are injective);
- (b) there exists a bijection $\alpha \mapsto \alpha'$ from R to R' and a map $q: R \rightarrow p^{\mathbb{N}}$ such that

$$\begin{aligned} \varphi(\alpha') &= q(\alpha)\alpha \\ \varphi^\vee(\alpha'^\vee) &= q(\alpha)\alpha'^\vee \end{aligned}$$

for all $\alpha \in R$.

The isogeny is said to be **central** if $q(\alpha) = 1$ for all $\alpha \in R$. It is an **isomorphism** if it is central and φ is an isomorphism.

Because we are requiring root data to be reduced, given α , there exists a most one α' such that $\varphi(\alpha')$ is a positive multiple of α . Therefore, given $\varphi: X' \rightarrow X$, there exists at most one bijection $\alpha \mapsto \alpha'$ and one map $q: R \rightarrow p^{\mathbb{N}}$ such that the equations hold.

EXAMPLE 22.88. Let $\mathcal{R} = (X, R, \alpha \mapsto \alpha^\vee)$ be a root datum, and let q be a power of p . The map $x \mapsto qx$ is an isogeny $\mathcal{R} \rightarrow \mathcal{R}$, called the **Frobenius isogeny** (the bijection $\alpha \mapsto \alpha'$ is the identity, and $q(\alpha) = q$ for all α).

ASIDE 22.89. Our terminology is that of [Steinberg 1999](#).

Springer 1998, p.172, defines a p -morphism to be a homomorphism $\varphi: X' \rightarrow X$ equipped with a bijection $\alpha \mapsto \alpha'$ and a map $q: R \rightarrow \{p^n \mid n > 0\}$ satisfying the conditions of (22.87). [Conrad et al. 2010](#), follow Springer, except that they allow $q(\alpha)$ to be p^0 .

SGA 3, XXI, 6.8.1, p.100, define a p -morphism of root data to be a homomorphism $\varphi: X' \rightarrow X$ such that *there exists* a bijection $\alpha \mapsto \alpha': R \rightarrow R'$ and a map $q: R \rightarrow p^{\mathbb{N}}$ satisfying (b) of (22.87). This agrees with (22.87) except that they don't require $\varphi_{\mathbb{Q}}$ to be an isomorphism.

PROPOSITION 22.90. *Let $f: (G, T) \rightarrow (G', T')$ be an isogeny of split reductive groups. Then $\varphi = X^*(f): X^*(T') \rightarrow X^*(T)$ is an isogeny of root data. Moreover, roots $\alpha \in R$ and $\alpha' \in R'$ correspond if and only if $f(U_{\alpha}) = U_{\alpha'}$, in which case*

$$f(u_{\alpha}(a)) = u_{\alpha'}(c_{\alpha} a^{q(\alpha)}), \quad \text{all } a \in k, \quad (159)$$

where $c_{\alpha} \in k^{\times}$ and $q(\alpha)$ is such that $\varphi(\alpha') = q(\alpha)\alpha$.

PROOF. By definition,

$$\varphi(\chi') = \chi' \circ f|T \text{ for all } \chi' \in X^*(T').$$

Applying f to (158), we see that $f(U_{\alpha})$ is a one-dimensional unipotent subgroup of G' normalized by T' , and so equals $U_{\alpha'}$ for some $\alpha' \in R'$. From (15.40), we find that

$$f(u_{\alpha}(a)) = u_{\alpha'}(g(a)) \quad (160)$$

with $g(a)$ a polynomial $\sum c_j a^{p^j}$ in a having coefficients in k . On applying f to (158), we find that

$$f(t) \cdot f(u_{\alpha}(a)) \cdot f(t)^{-1} = f(u_{\alpha}(\alpha(t)a)).$$

Using that (160), we can rewrite this as

$$f(t) \cdot u_{\alpha'}(g(a)) \cdot f(t)^{-1} = u_{\alpha'}(g(\alpha(t)a)),$$

and using (158) in the group G' , we find that

$$u_{\alpha'}(\alpha'(f(t))g(a)) = u_{\alpha'}(g(\alpha(t)a)).$$

As $\alpha' \circ f = \varphi(\alpha')$, this implies that

$$\varphi(\alpha')(t) \cdot g(a) = g(\alpha(t) \cdot a). \quad (161)$$

It follows that $g(a)$ is a monomial, say,

$$g(a) = c a^{q(\alpha)}, \quad c \in k, \quad q(\alpha) \in p^{\mathbb{N}},$$

and

$$\varphi(\alpha')(t) = \alpha(t)^{q(\alpha)},$$

i.e., $\varphi(\alpha') = q(\alpha)\alpha$. Note that $f(w_{\alpha})$ normalizes T' in $G_{\alpha'}$ and acts nontrivially on it, and so we can take $w_{\alpha'} = f(w_{\alpha})$. Therefore

$$\varphi \circ (1 - w_{\alpha'}) = (1 - w_{\alpha}) \circ \varphi.$$

On applying this to $\chi' \in X^*(T')$ and using that $w_{\alpha'}\chi' = \chi' - \langle \chi', \alpha'^{\vee} \rangle \alpha$, we find that

$$\langle \chi', \alpha'^{\vee} \rangle \varphi(\alpha') = \langle \varphi(\chi'), \alpha^{\vee} \rangle \alpha,$$

which equals $\langle \chi', \varphi^{\vee}(\alpha^{\vee}) \rangle \alpha$. As this holds for all $\chi' \in X^*(T')$, it follows from $\varphi(\alpha') = q(\alpha)\alpha$ that $\varphi^{\vee}(\alpha^{\vee}) = q(\alpha)\alpha'^{\vee}$, and so condition (b) of (22.87) holds. Finally, $f|T$ is an isogeny, and so (a) holds. \square

Thus, an isogeny $(G, T) \rightarrow (G', T')$ defines an isogeny of root data. The isogeny of root data does not determine f , because an inner automorphism of (G, T) defined by an element of $(T/Z)(k)$ induces the identity map on the root datum of (G, T) . However, the next lemma shows that this is the only indeterminacy.

LEMMA 22.91. *If two isogenies $(G, T) \rightarrow (G', T')$ induce the same map on the root data, then they differ by an inner automorphism by an element of T .⁵*

PROOF. We may suppose that k is algebraically closed (because if f and g differ by an automorphism over k^{al} , their kernels are equal, and so they differ by an automorphism over k , and we are only claiming that the automorphism is of the form $\text{inn}(t)$ with $t \in T(k^{\text{al}})$).

Let f and g be such isogenies. Then they agree on T obviously. Let S be a base for R . For each $\alpha \in S$, it follows from $\varphi(\alpha') = q(\alpha)\alpha$ that $f(u_\alpha(a)) = u_{\alpha'}(c_\alpha a^{q(\alpha)})$, and similarly for g with c_α replaced by d_α . As S is linearly independent, there exists a $t \in T(k)$ such $a(t)^{q(\alpha)} = d_\alpha c_\alpha^{-1}$ for all $\alpha \in S$ (here we use k is algebraically closed). Let $h = f \circ \text{inn}(t)$. Then g and h agree on every U_α , $\alpha \in S$, as well as on T , and hence also on the Borel subgroup B that these groups generate. It follows that they agree on G because the regular map $x \mapsto h(x)g(x)^{-1}: G \rightarrow G'$ is constant on each coset, hence factors through G/B (9.44), and the resulting map $G/B \rightarrow G'$ is constant because G/B is complete and G' is affine (cf. 18.25). As $h(e)g(e)^{-1} = 1$, we see that $h(x) = g(x)$ for all x . \square

THEOREM 22.92. *Let (G, T) and (G', T') be split reductive algebraic groups over k , and let $f: T \rightarrow T'$ be an isogeny of tori. If $X^*(f): X(T') \rightarrow X(T)$ is an isogeny of root data, then f extends to an isogeny $G \rightarrow G'$.*

This will be proved in the next section.

THEOREM 22.93 (ISOGENY THEOREM). *Let (G, T) and (G', T') be split reductive algebraic groups over k . An isogeny $f: (G, T) \rightarrow (G', T')$ defines an isogeny of root data $\varphi: \mathcal{R}(G, T) \rightarrow \mathcal{R}(G', T')$, and every isogeny of root data φ arises from an isogeny f ; moreover, f is uniquely determined by φ up to an inner automorphism by an element of T .*

PROOF. Combine (22.90), (22.91), and (22.92). \square

THEOREM 22.94 (ISOMORPHISM THEOREM). *Let (G, T) and (G', T') be split reductive algebraic groups over a field k . An isomorphism $f: (G, T) \rightarrow (G', T')$ defines an isomorphism φ of root data, and every isomorphism of root data φ arises from an isomorphism f ; moreover, f is uniquely determined by φ up to an inner automorphism by an element of T .*

PROOF. This is an immediate consequence of the isogeny theorem. If $\varphi: X' \rightarrow X$ is an isomorphism of root data, then the isomorphisms $f_T: T \rightarrow T'$ and $f_T^{-1}: T' \rightarrow T$ extend to isomorphisms $f: (G, T) \rightarrow (G', T')$ and $g: (G', T') \rightarrow (G, T)$. The composite $g \circ f$ induces the identity map on the root datum of (G, T) and hence equals $\text{inn}(t)$ for some $t \in T(k)$. Let $g' = \text{inn}(t^{-1}) \circ g$. Then $g' \circ f = \text{id}$, and $f \circ g' \circ f = f$, which implies that $f \circ g' = \text{id}$ because f is surjective. Hence f is an isomorphism with g' as its inverse. \square

NOTES. The isogeny theorem was first proved by Chevalley in his famous 1956-58 seminar for semisimple groups (the extension to reductive groups is easy — see 22.103 below). Chevalley's proof works through semisimple groups of rank 2, and is long and complicated. The proofs in Humphreys

⁵By this, I mean that they differ by an automorphism of (G, T) that becomes of the form $\text{inn}(t)$, $t \in T(k^{\text{al}})$, over k^{al} . In fact, they differ by an automorphism $\text{inn}(t)$ with $t \in (T/Z)(k)$.

1975, Springer 1998, SGA 3, and elsewhere follow Chevalley (Borel 1991 doesn't prove the isogeny theorem). Takeuchi (1983) gave a proof of the isogeny theorem in terms of "hyperalgebras" that avoided using systems of rank 2, which inspired Steinberg to find his simple proof (Steinberg 1999). Our proof follows Steinberg except that we have rewritten it in the language of group schemes (rather than group varieties) and we have extended it to split reductive groups over arbitrary fields (instead of algebraically closed fields).⁶

GENERALIZATIONS

The next statement can be proved by similar methods (k algebraically closed for the moment).

THEOREM 22.95. *Let H be a group variety, let T be a maximal torus in H , and let S be a finite linearly independent subset of $X^*(T)$. Suppose that for each $\alpha \in S$ we are given a reductive subgroup (G_α, T) of G of semisimple rank 1 with roots $\pm\alpha$. Let U_α be the root group of α in G_α . If $U_{-\alpha}$ and U_β commute for all $\alpha, \beta \in S$, $\alpha \neq \beta$, then the algebraic group G generated by the G_α is reductive; moreover, T is a maximal torus in G , and S is a base for $\mathcal{R}(G, T)$.*

PROOF. Steinberg 1999, 5.4. □

THEOREM 22.96. *Let H, T , and $(G_\alpha)_{\alpha \in S}$ be as in 22.95. Let $\mathcal{R} = (X, R, \alpha \mapsto \alpha^\vee)$ be a root datum such that $X = X^*(T)$ and S is a base for R . Then $\mathcal{R} = \mathcal{R}(G, T)$.*

PROOF. The Weyl groups of \mathcal{R} and (G, T) are the same because their generators w_α , $\alpha \in S$, satisfy the same formulas. Hence, so are the root systems and coroot systems, given by $R = WS$ and $R^\vee = WS^\vee$. Thus (22.95) implies (22.96). □

THEOREM 22.97. *Let (G, T) be a split reductive group, let S be a base for the root system, and let $(G_\alpha)_{\alpha \in S}$ be the corresponding family of reductive subgroups of semisimple rank 1. Let $f: \bigcup_{\alpha \in S} G_\alpha \rightarrow H$ be a map such that $f|_{G_\alpha}$ is a homomorphism for each α . If $f_\alpha(U_{-\alpha})$ and $f_\beta(U_\beta)$ commute for all $\alpha, \beta \in S$, $\alpha \neq \beta$, then f extends to a homomorphism $f: G \rightarrow H$.*

PROOF. The graphs $G'_\alpha = \{(x, f(x)) \mid x \in G_\alpha\}$, $\alpha \in S$, in $G \times H$ satisfy the hypotheses of (22.95), and hence generate a reductive group L in $G \times H$ with $\mathcal{R}(G, T)$ as its root datum. The projection $p_1: L \rightarrow G$ is an isomorphism (isomorphism theorem 22.94), and $p_2 \circ p_1^{-1}$ is the required extension of f . □

⁶Steinberg 1999, p.368:

These theorems were first proved by Chevalley in his famous 1956-58 seminar, with slightly different formulation since he considered only semisimple groups. . . That is certainly the main case, and further the step from semisimple groups to reductive groups is a simple one. . . Chevalley's proofs are quite long, occupying the last five Exposés of his seminar. Other proofs and expositions have been given by Humphreys (1967, 1975), Demazure and Grothendieck (see SGA 3 and the guide Demazure 1965 to it), Springer (1998) (who, following Tits 1966, also considers the isomorphism theorem over an arbitrary base field), and Takeuchi (1983). In SGA 3 and Takeuchi 1983 the theorems are proved for group schemes. Our own proof, at least in broad outline, is patterned after that of Takeuchi.

m. The isogeny theorem: proofs

PRELIMINARY REDUCTIONS

LEMMA 22.98. Let $f: (G, T) \rightarrow (G', T')$ be a homomorphism of split reductive groups over k . If $X^*(f_T): X^*(T') \rightarrow X^*(T)$ is an isogeny of root data $\mathcal{R}(G, T) \rightarrow \mathcal{R}(G', T')$, then f is an isogeny.

PROOF. Certainly f is surjective, because it maps each U_α onto $U_{\alpha'}$ and T onto T' , and the subgroups $U_{\alpha'}$ and T' generate G' . As

$$\dim G = \dim T + |R| = \dim T' + |R'| = \dim G'$$

(22.75), this shows that f is an isogeny. \square

22.99. Every normal étale finite subgroup scheme of a connected algebraic group G is central. However, a normal (nonétale) finite subgroup scheme of even a reductive algebraic group need not be central (e.g., the kernel of a Frobenius isogeny).

LEMMA 22.100 (CHEVALLEY). Let $f_1: (G, T) \rightarrow (G_1, T_1)$ and $f_2: (G, T) \rightarrow (G_2, T_2)$ be isogenies of split reductive groups, and let $f_T: T_1 \rightarrow T_2$ be a homomorphism such that $f_T \circ f_1|_T = f_2|_T$. If $X^*(f_T)$ is an isogeny of root data, then f_T extends to a homomorphism $f: G_1 \rightarrow G_2$ such that $f \circ f_1 = f_2$.

PROOF. We have to show that the homomorphism f_2 factors through f_1 , which will be true if and only if $\text{Ker}(f_1) \subset \text{Ker}(f_2)$. If f_1 and f_2 are central isogenies (for example, k has characteristic zero), then the kernels are contained in T (because $T = C_G(T)$), and so this follows from the fact that $f_1|_T$ factors through $f_2|_T$.

Clearly the statement $\text{Ker}(f_1) \subset \text{Ker}(f_2)$ 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 $f_1(k)$ and $f_2(k)$ are central in $G(k)$, and so $f_1(k): G(k) \rightarrow G_1(k)$ factors through $f_2(k)$, say, $g \circ f_1(k) = f_2(k)$. It remains to show that $g: G_1(k) \rightarrow G_2(k)$ 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 $\varphi_1 = X^*(f_1|_T)$, $\varphi_2 = X^*(f_2|_T)$, and $\varphi = X^*(f)$. Then $f_1(U_\alpha(k)) = U_{\alpha_1}(k)$ and $f_2(U_\alpha(k)) = U_{\alpha_2}(k)$, so that $g(U_{\alpha_1}(k)) = U_{\alpha_2}(k)$. Moreover, $g: U_{\alpha_1} \rightarrow U_{\alpha_2}$ is a morphism because, for some $c \in k$, it has the form

$$g(u_{\alpha_1}(a)) = u_{\alpha_2}(ca^{q(\alpha_1)}), \quad a \in U_{\alpha_1}(k)$$

(cf. (159)). It follows that g is a morphism on the big cell of G_1 , and hence on the union of its translates, which is G_1 itself. Thus g is an isogeny of algebraic groups. \square

LEMMA 22.101 (CHEVALLEY). Let $f_1: (G_1, T_1) \rightarrow (G, T)$ and $f_2: (G_2, T_2) \rightarrow (G, T)$ be isogenies of reductive algebraic groups, and let $f_T: T_1 \rightarrow T_2$ be a homomorphism such that $f_2|_T \circ f_T = f_1|_T$. If $X^*(f_T)$ is an isogeny of root data, then f_T extends to a homomorphism $f: G_1 \rightarrow G_2$ such that $f_2 \circ f = f_1$.

PROOF. Let G_3 be the identity component of $G_1 \times_G G_2$:

$$\begin{array}{ccc} G_3 & \xrightarrow{p_2} & G_2 \\ \downarrow p_1 & \searrow f & \downarrow f_2 \\ G_1 & \xrightarrow{f_1} & G. \end{array}$$

It suffices to show that p_2 factors through p_1 , say $f \circ p_1 = p_2$, because then

$$f_2 \circ f \circ p_1 = f_2 \circ p_2 = f_1 \circ p_1,$$

and the surjectivity of p_1 implies that $f_2 \circ f = f_1$ as required.

Now p_2 factors through p_1 if and only if $\text{Ker}(p_1) \subset \text{Ker}(p_2)$, and it suffices to check this after an extension of the base field. Thus, we may suppose that k is algebraically closed, and we may replace G_3 with its reduced algebraic subgroup. The projections p_1 and p_2 of G_3 onto G_1 and G_2 are isogenies, and so G_3 is reductive. Let T_3 be the inverse image torus of T in G_3 (under $f_2 \circ p_2$ or $f_1 \circ p_1$). Then $f_T \circ p_1|_{T_3} = p_2|_{T_3}$, and so (22.100) applied to $p_1: (G_3, T_3) \rightarrow (G_1, T_1)$ and $p_2: (G_3, T_3) \rightarrow (G_2, T_2)$ shows that f_T extends to a homomorphism $f: G_1 \rightarrow G_2$ such that $f \circ p_1 = p_2$, as required. \square

LEMMA 22.102. *Let (G, T) and (G', T') be split reductive groups over a field k . An isogeny $f_T: T \rightarrow T'$ extends to an isogeny $G \rightarrow G'$ if the restriction of f_T to a homomorphism of finite group schemes $T \cap \mathcal{D}G \rightarrow T' \cap \mathcal{D}G'$ extends to a homomorphism $\mathcal{D}G \rightarrow \mathcal{D}G'$.*

PROOF. Use the diagram

$$\begin{array}{ccccccccc} e & \longrightarrow & T \cap \mathcal{D}G & \longrightarrow & T \times \mathcal{D}G & \longrightarrow & G & \longrightarrow & e \\ & & \downarrow & & \downarrow & & \downarrow & & \\ e & \longrightarrow & T' \cap \mathcal{D}G' & \longrightarrow & T' \times \mathcal{D}G' & \longrightarrow & G' & \longrightarrow & e. \end{array} \quad \square$$

PROPOSITION 22.103. *If Theorem 22.92 holds for split semisimple groups then it holds for split reductive groups.*

PROOF. Omitted for the moment. \square

PROOF OF THEOREM 22.92 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.

LEMMA 22.104. *Let (G, T) and (G', T') be split reductive algebraic groups over k of semisimple rank 1, and let $f_T: T \rightarrow T'$ be an isogeny of tori. If $\varphi = X^*(f_T)$ is an isogeny of root data, then f extends to a homomorphism $f: G \rightarrow G'$.*

PROOF. It suffices to prove this for semisimple groups (22.103).

Let (G, T) be a split semisimple group of rank 1. For such a group, the root datum is $(X, \{\pm\alpha\}, \alpha \mapsto \alpha^\vee)$ with $X \approx \mathbb{Z}$ and α^\vee the unique element of X^\vee with $\langle \alpha, \alpha^\vee \rangle = 2$. Let B be a Borel subgroup in G . Then $G/B \approx \mathbb{P}^1$, and we obtain an isogeny

$$f: G \rightarrow \underline{\text{Aut}}(G/B) \approx \text{PGL}_2,$$

and hence an isogeny φ of root data. We claim that the integers $q(\alpha) = q(-\alpha) \in p^\mathbb{N}$ arising from φ equal 1. To see this, let $B = TU_\alpha$ and $V = U_{-\alpha}$. For $v \in V$, we can recover v from $f(v)$ by applying the following sequence of morphisms: first restrict the action of $f(v)$ from G/B to VB/B , then evaluate at B/B to get vB/B , and finally apply the isomorphism $VB/B \rightarrow V$ which comes from the fact that $VB = V_\alpha TU_\alpha$ is a direct product of its factors. It follows that $f: V \rightarrow f(V)$ is an isomorphism, and hence that $q(-\alpha) = 1$.

We now prove the lemma when G and G' are semisimple of rank 1. Assume first that $G' = \mathrm{PGL}_2$. Let $f_1: (G, T) \rightarrow (\mathrm{PGL}_2, \mathbb{D}_2)$ be the isogeny of the previous paragraph and let $\varphi_1 = \mathcal{R}(f_1)$. We have $\varphi_1(\alpha') = \alpha$ and $\varphi(\alpha) = q(\alpha)\alpha$, so that $\varphi = q(\alpha)\varphi_1$. Therefore the composite $F_{q(\alpha)} \circ f_1$ of f_1 with the Frobenius map raising coordinates to their $q(\alpha)$ th powers is an isogeny that realizing φ . We now consider the case $G' \neq \mathrm{PGL}_2$. Let $g: G' \rightarrow \mathrm{PGL}_2$ be an isogeny and let $\psi = \mathcal{R}(g)$. By the previous case, there exists an isogeny $h: G \rightarrow \mathrm{PGL}_2$ with $\mathcal{R}(h) = \varphi \circ \psi$. Then (22.101) applied to the isogenies $h: G \rightarrow \mathrm{PGL}_2$ and $g: G' \rightarrow \mathrm{PGL}_2$ yields an isogeny $f: G \rightarrow G'$ with $\mathcal{R}(f) = \varphi$. \square

A consequence of Lemma 22.104 is that every split semisimple group of rank 1 is isomorphic to SL_2 or PGL_2 .

PROOF OF THEOREM 22.92 IN THE GENERAL CASE.

Let (G, T) and (G', T') be split reductive groups over k , with root data $(X^*(T), R, \alpha \mapsto \alpha^\vee)$ and $(X^*(T'), R', \alpha' \mapsto \alpha'^\vee)$. Let $f_T: T \rightarrow T'$ be a homomorphism such that $\varphi = X^*(f_T): X^*(T') \rightarrow X^*(T)$ is an isogeny of root data. It remains to show that f_T extends to a homomorphism $f: G \rightarrow G'$ (22.98).

22.105. *The set $S' \stackrel{\mathrm{def}}{=} \{\alpha' \mid \alpha \in S\}$ is a base for R' .*

PROOF. Because φ is an isogeny of root data, each element R' has a unique expression as a linear combination of elements of S' in which the coefficients are rational numbers all of the same sign. Clearly those elements of R' for which the signs are positive form a positive subsystem R'^+ of R' . From this and the fact that R' is reduced, it follows that a decomposition

$$\alpha' = \beta' + \gamma', \quad \alpha' \in S', \quad \beta', \gamma' \in R'^+$$

is impossible, and so S' is a base for R' . \square

For each $\alpha \in S$, let G_α be the subgroup defined in (22.43) (generated by T , U_α , and $U_{-\alpha}$). Similarly, let $G_{\alpha'}$ be the subgroup attached to $\alpha' \in S'$.

22.106. *For each $\alpha \in S$, the isogeny f_T extends to an isogeny $f_\alpha: G_\alpha \rightarrow G_{\alpha'}$.*

PROOF. As G_α and $G_{\alpha'}$ are both of semisimple rank 1, this was proved in (22.104). \square

It suffices to prove the following statement.

22.107. *The family of maps $f_\alpha: G_\alpha \rightarrow G'$ extends to a homomorphism $f: G \rightarrow G'$.*

See (22.97) for a more general result. We construct f by constructing its graph. Let G'' be the subgroup variety of $G \times G'$ generated by the family of maps $x \mapsto (x, f_\alpha(x)): G_\alpha \rightarrow G \times G'$ (see Section 2.f). It is connected because each G_α is connected. It suffices to prove the following statement (because then $p' \circ p^{-1}$ will be the map sought).

22.108. *The projection $p: G \times G' \rightarrow G$ maps G'' isomorphically onto G .*

We prove this (also) in several steps. We may suppose that k is algebraically closed.

22.109. *The projections of G'' to G and G' are both surjective.*

PROOF. The image of p contains $\bigcup_{\alpha \in S} G_\alpha$, which generates G because S is a base for R . Similarly for p' because of (22.105). \square

22.110. *The group G'' is reductive.*

PROOF. As G and G' are reductive, their radicals are tori, and it follows from (22.109) that the radical of G'' is also a torus. \square

For each $\alpha \in S$, let U''_α denote the graph of $f_\alpha|_{U_\alpha}$,

$$U''_\alpha = \{(x, f(x)) \mid x \in U_\alpha\}.$$

Define $U''_{-\alpha}$, T'' , and G''_α similarly, and let U'' and V'' be the group varieties generated by all U''_α and all $U''_{-\alpha}$ respectively. The groups U''_α , U'' , $U''_{-\alpha}$, and V'' are connected unipotent subgroup varieties of G'' , and they are all normalized by T'' , which is a torus isomorphic to T via p .

22.111. *The groups $U''_{-\alpha}$ and U''_β commute (elementwise) for all $\alpha, \beta \in S$, $\alpha \neq \beta$.*

PROOF. This follows from the corresponding results in G and G' , which hold because S and S' are bases for R and R' . \square

22.112. *The subset $C = V'' \cdot T'' \cdot U''$ of G'' is open and dense.*

PROOF. First C is dense and open in its closure because it is an orbit in the left \times right action of $V'' \times T''U''$ on G'' . For the proof that this closure is G'' , we use (22.111) and the definition of C . We first show by induction on n that

$$U''_\alpha U''_{-\alpha_1} U''_{-\alpha_2} \cdots U''_{-\alpha_n} \subset \bar{C} \tag{162}$$

for any elements $\alpha, \alpha_1, \dots, \alpha_n$ of S . 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 (22.111), and if $\alpha = \alpha_1$, then

$$U''_\alpha U''_{-\alpha_1} \subset G''_\alpha = \overline{U''_{-\alpha} T'' U''_\alpha}.$$

Thus in both cases (162) follows from the induction assumption. We have $U''_\alpha V'' \subset \bar{C}$ by (162) since $V'' = V''_{\alpha_1} V''_{\alpha_2} \cdots$ for some elements $\alpha_1, \alpha_2, \dots$ of S . It follows that $U''_\alpha \bar{C} \subset \bar{C}$ and clearly $U''_{-\alpha} \bar{C} \subset \bar{C}$ and $T'' \bar{C} \subset \bar{C}$. Since the subgroups U''_α , $U''_{-\alpha}$, $\alpha \in S$, and T'' generate G'' , the set \bar{C} equals G'' , as required. \square

22.113. *The torus T'' in G'' equals its centralizer, and so is maximal.*

PROOF. The centralizer of T'' in C is T'' because the corresponding result is true in G and G' . It follows from (22.112) that the centralizer of T'' in G'' , which is connected (18.44), contains T'' as a dense open subset and hence equals it. \square

22.114. *The projection $p: G''(k) \rightarrow G(k)$ is bijective and the induced map of maximal tori $T'' \rightarrow T$ is an isomorphism.*

PROOF. The last point was noted earlier, and the surjectivity of p holds by (22.109). For the injectivity, we note first that since $(\text{Ker } p)^\circ(k)$ is normal and disjoint from the maximal torus T'' , it consists of unipotent elements and therefore is solvable and equal to its own radical (Lie-Kolchin 17.38). On the other hand, this radical consists of semisimple elements since $\text{Ker}(p)^\circ_{\text{red}}$ is a connected normal subgroup of the reductive group G'' , and hence is itself reductive. Thus $\text{Ker}(p)^\circ(k)$ is trivial. Then $\text{Ker}(p)(k)$ is also trivial since it is finite and normal, hence also central and therefore contained in T'' . \square

We can now complete the proof of (22.108), which is all that remains to be done. The properties in (22.114) are not quite enough to make p an isomorphism, as shown by the examples following (22.116) 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 ($\alpha \in S$) 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 (22.108) is proved, and with it the isogeny theorem.

COMPLEMENTS

PROPOSITION 22.115. *The following conditions on an isogeny $f: G \rightarrow G'$ of reductive groups over an algebraically closed field are equivalent:*

- (a) f is central, i.e., $\text{Ker}(f) \subset Z(G)$;
- (b) $\text{Ker}(df)$ is central;
- (c) the map $X^*(f|T)$ on root data is central.

PROOF. Omitted for the moment. □

The rest of this subsection is quoted from [Steinberg 1999](#).

The central isogenies are the familiar ones from the theory of Lie groups, $\text{Spin}_n \rightarrow \text{SO}_n$, $\text{SL}_n \rightarrow \text{PGL}_n$, $G \rightarrow G^{\text{ad}}$, \dots . If $\text{char}(k) = 0$, these are the only isogenies, but if $\text{char}(k) = p \neq 0$ there are others and those enter into another important classification, that of the finite simple groups, a substantial subset of which (the finite Chevalley groups, twisted and untwisted — see [Steinberg 1968](#) and the references given there) can be constructed in terms of fixed-point-subgroups of isogenies that are endomorphisms of simple algebraic groups. We have already mentioned the simplest of these, the Frobenius F_q ($q = p^n$, $n \geq 0$) which, in terms of a suitable matrix realization, simply replaces each coordinate of the given group by its q th power. Accordingly the isogeny of root data is multiplication by q , or its composition with an automorphism, and the fixed-point-subgroup is finite since its coordinates are all in the finite field \mathbb{F}_q . More exotic examples occur when there are two root lengths whose ratio squared is just $p = \text{char}(k)$. Then, with α^\vee identified with $(2/(\alpha, \alpha))\alpha$, multiplication by $p^n(\alpha_0, \alpha_0)/2$ (α_0 any long root $n \geq 0$) effects an isogeny between $D = (X, R)$ and its dual $D^\vee = (X^\vee, R^\vee)$ which sends $\alpha^\vee \in R^\vee$ to $p^n\alpha$ or $p^{n+1}\alpha$ according as α is a long root or a short root. In case R^\vee is isomorphic to R , this leads us back to D , and hence to an endomorphism of the given algebraic group and yet other finite simple groups (the Suzuki groups and the Ree groups). There remains only the case $p = 2$, D of type B_n , and D^\vee of type C_n ($n \geq 3$), which enters into other interesting phenomenon.

PROPOSITION 22.116. *An isogeny $(G, T) \rightarrow (G', T')$ of simple algebraic groups is an isomorphism if it restricts to an isomorphism $T \rightarrow T'$, except for the isogenies $\text{SO}_{2n+1} \rightarrow \text{Sp}_{2n}$, $n \geq 1$, in characteristic 2 described below.*

PROOF. Exercise ([Steinberg 1999](#), 4.11). □

Let $G = \text{SO}_{2n+1}$ 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 $G' = \text{Sp}_{2n}$ the group variety attached to the skew-symmetric form $\sum_{i=1}^n (x_i x'_{n+i} - x_{n+i} x'_i)$ on k^{2n} . Then G fixes the basis vector e_0 (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' inducing an isomorphism on the diagonal maximal tori.

n. The structure of semisimple groups

SPLIT SEMISIMPLE ALGEBRAIC GROUPS AND THEIR ROOTS

By a *split semisimple group* we mean a pair (G, T) consisting of a semisimple algebraic group G and a split maximal torus T .

PROPOSITION 22.117. *Let (G, T) be a split semisimple algebraic group, and let $V = \mathbb{Q} \otimes X^*(T)$. Let $R = R(G, T) \subset V$. Then,*

- (a) *R is finite, spans V , and does not contain 0;*
- (b) *for each α , there exists an $\alpha^\vee \in V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \subset \mathbb{Z}$, and the reflection $s_\alpha: x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ maps R into R .*

PROOF. (a) Certainly R is finite and does not contain 0. That it spans V follows from (22.46).

(b) See (22.43, 22.44). □

The proposition says exactly that $R(G, T)$ is a root system in V (see 23.10). The coroot α^\vee attached to α in (b) is unique. An elementary argument (23.18) shows that R admits a base: this is a linearly independent subset S of R such that each root $\beta \in R$ can be written uniquely in the form $\beta = \sum_{\alpha \in S} m_\alpha \alpha$ with the m_α integers all of the same sign. If all the m_α are positive (resp. negative) then β is said to be *positive* for S .

Let B be a Borel subgroup of G containing T . Then the set of roots α whose root group U_α is contained in B is the set of positive roots for a (unique) base for R . In this way, we get a one-to-one correspondence between the Borel subgroups of G containing T and the bases for R (cf. 22.57, 22.58).

AUTOMORPHISMS OF A SEMISIMPLE ALGEBRAIC GROUP

The results in this section also follow directly from the isogeny theorem (22.93).

PROPOSITION 22.118. *Let G be a semisimple algebraic group over an algebraically closed field. The group of inner automorphisms of G has finite index in the full group of automorphisms of G .*

PROOF. Choose a Borel pair (B, T) in G , and let D denote the group of automorphisms of (G, B, T) . Let γ be an automorphism of G . According to (18.17), there exists an inner automorphism a such that $\gamma(B) = a(B)$ and $\gamma(T) = a(T)$. Now $a^{-1}\gamma \in D$. Thus $\text{Aut}(G) = \text{Inn}(G) \cdot D$, and so

$$\frac{\text{Aut}(G)}{\text{Inn}(G)} = \frac{\text{Inn}(G) \cdot D}{\text{Inn}(G)} \simeq \frac{D}{D \cap \text{Inn}(G)}.$$

The next lemma shows that $D/(D \cap \text{Inn}(G))$ acts faithfully on the set of roots of (G, T) , and hence is finite. □

LEMMA 22.119. *Let $\gamma \in \text{Aut}(G, B, T)$. If γ acts trivially on $R(G, T)$, then $\gamma = \text{inn}(t)$ for some $t \in T(k)$.*

PROOF. Let S be the base corresponding to B . Let $\alpha \in S$, and let $u_\alpha: \mathbb{G}_a \rightarrow U_\alpha$ be an isomorphism. As γ acts trivially on S , $\gamma(U_\alpha) = U_\alpha$ and so $\gamma(u_\alpha(a)) = u_\alpha(c_\alpha a)$ for some $c_\alpha \in k$. The set S is linearly independent, and so there exists a $t \in T(k)$ such $a(t) = c_\alpha^{-1}$

for all $\alpha \in S$. Now $\gamma \circ \text{inn}(t)$ is the identity map on U_α for all $\alpha \in S$. It is also the identity map on T . As T and the U_α with $\alpha \in S$ generate B , $\gamma \circ \text{inn}(t)$ is the identity map on B , and hence on G (18.25). Thus $\gamma = \text{inn}(t^{-1})$. \square

COROLLARY 22.120. *Let G be a semisimple algebraic group over k . Then $\underline{\text{Aut}}(G)$ is an algebraic group over k with $\underline{\text{Aut}}(G)^\circ \simeq G/Z(G)$. If G is split with split maximal torus T , then $\pi_0(\underline{\text{Aut}}(G))$ acts faithfully on the Dynkin diagram of the root system of (G, T) .*

THE DECOMPOSITION OF A SEMISIMPLE ALGEBRAIC GROUP

An algebraic group is *simple* (resp. *almost-simple*) if it is semisimple, noncommutative, and every proper normal subgroup is trivial (resp. finite). In particular, it is smooth and connected. For example, SL_n is almost-simple for $n > 1$, and $\text{PSL}_n = \text{SL}_n/\mu_n$ is simple.

Let N be an algebraic subvariety of a semisimple algebraic group G . If N is minimal among the nonfinite normal subgroups of G , then it is almost-simple.

An algebraic group G is said to be the *almost-direct product* of its algebraic subgroups G_1, \dots, G_r if the multiplication map

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

is a surjective homomorphism with finite kernel. In particular, this means that the G_i commute and each G_i is normal in G . For example,

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

is the almost-direct product of SL_2 and SL_2 , but it is not a direct product of two almost-simple algebraic groups.

THEOREM 22.121. *A semisimple algebraic group G has only finitely many almost-simple normal subgroup varieties G_1, \dots, G_r , and the map*

$$(g_1, \dots, g_r) \mapsto g_1 \cdots g_r: G_1 \times \cdots \times G_r \rightarrow G \tag{163}$$

is surjective with finite kernel. Each connected normal algebraic subgroup of G is a product of those G_i that it contains, and is centralized by the remaining ones.

In particular, an algebraic group is semisimple if and only if it is an almost-direct product of almost-simple algebraic groups. The algebraic groups G_i are called the *almost-simple factors* of G .

PROOF. Let G_1, G_2, \dots, G_r be distinct smooth subgroups of G , each of which is minimal among the nonfinite normal subgroup varieties of G .

For $i \neq j$, (G_i, G_j) is the algebraic subgroup generated by the map

$$G_i \times G_j \rightarrow G, \quad (a, b) \mapsto aba^{-1}b^{-1}.$$

Then (G_i, G_j) is a connected normal subgroup variety of G (8.26) contained in G_i and so it is trivial because G_i is minimal. Thus, the map

$$u: G_1 \times \cdots \times G_r \rightarrow G$$

is a homomorphism of algebraic groups, and $H \stackrel{\text{def}}{=} G_1 \cdots G_r$ is a connected normal subgroup variety of G . The kernel of u is finite, and so

$$\dim G \geq \sum_{i=1}^r \dim G_i.$$

This shows that r is bounded, and we may assume that our family contains them all. It then remains to show that $H = G$. For this we may assume that $k = k^{\text{al}}$. Let $H' = C_G(H)$. The action of G on itself by inner automorphisms defines a homomorphism

$$G(k) \rightarrow \text{Aut}(H)$$

whose image contains $\text{Inn}(H)$ and whose kernel is $H'(k)$ (which equals $H'_{\text{red}}(k)$). As $\text{Inn}(H)$ has finite index in $\text{Aut}(H)$ (see 20.1), this shows that $(G/H \cdot H'_{\text{red}})(k)$ is finite, and so the quotient $G/(H \cdot H'_{\text{red}})$ is finite. As G is connected and smooth, it is strongly connected, and so $G = H \cdot H'_{\text{red}}$; in fact, $G = H \cdot H'_{\text{red}}{}^{\circ}$.

Let N be a smooth subgroup of $H'_{\text{red}}{}^{\circ}$, and assume that N is minimal among the nonfinite normal subgroups of $H'_{\text{red}}{}^{\circ}$. 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 we conclude that $H'_{\text{red}}{}^{\circ} = 1$. \square

COROLLARY 22.122. *All nontrivial quotients and all connected normal subgroup varieties of a semisimple algebraic group are semisimple.*

PROOF. Every such group is an almost-product of almost-simple algebraic groups. \square

COROLLARY 22.123. *If G is semisimple, then $\mathcal{D}G = G$, i.e., a semisimple group has no commutative quotients. In particular, $X^*(G) = 0$.*

PROOF. This is obvious for almost-simple algebraic groups, and hence for an almost-product of such algebraic groups. \square

ASIDE 22.124. When k has characteristic zero, (22.121) is most easily proved using Lie algebras (see LAG).

COMPLEMENTS ON REDUCTIVE GROUPS

Let G be an almost-simple group. Then G has a faithful representation (V, r) , which has a simple subrepresentation (W, r_W) on which G acts nontrivially. The kernel of r_W is finite.

THEOREM 22.125. *Let G be a connected group variety over a perfect field k . The following conditions are equivalent:*

- (a) G is reductive;
- (b) $R(G)$ is a torus;
- (c) G is an almost direct product of a torus and its derived group $\mathcal{D}G$, which is semisimple.
- (d) G admits a semisimple representation with finite kernel.

PROOF. (a) \iff (b). See (20.7).

(c) \implies (d): The group G is an almost direct product of almost simple groups G_1, \dots, G_n . It suffices to take a direct sum of nontrivial simple representations of the quotients

$$G/(G_1 \dots G_{i-1} G_{i+1} \dots G_n).$$

(d) \implies (b): Let (V, r) be a semisimple representation, and let V_0 be a simple factor of V . Let $U = R_u(G)$. Then V_0^U is a nonzero subspace of V_0 stable under G , and hence equals V_0 . Therefore $V^U = V$, which implies that U is finite, hence trivial.

(b) \implies (c): Let $S = R(G)$. It is normal subtorus of G , hence central. The group G/S is semisimple, therefore equal to its commutator subgroup, which implies that $G = S \cdot \mathcal{D}G$. It remains to show that $S \cap \mathcal{D}G$ is finite, which is a consequence of the next lemma. \square

LEMMA 22.126. *Let H be a connected group variety, and let S be a central torus in H . Then $S \cap \mathcal{D}H$ is finite. (Duplicates 14.72.)*

PROOF. Embed H into GL_V for some V . Then V is a direct sum of subspaces V_i stable under G on which S acts by homotheties. The lemma follows from the fact that every homomorphism $H \rightarrow \mathrm{GL}_m$ maps $\mathcal{D}H$ into SL_m . \square

REMARK 22.127. Let G be a connected group variety over a field k (not necessarily perfect). The following conditions are equivalent:

- (a) G is reductive;
- (b) $R(G_{k^{\mathrm{al}}})$ is a torus;
- (c) G is an almost direct product of a torus and its derived group $\mathcal{D}G$, which is semisimple;
- (d) G admits an absolutely semisimple representation with finite kernel.

REMARK 22.128. From a reductive group G , we obtain a semisimple group G' (its derived group), a group Z of multiplicative type (its centre), and a homomorphism $\varphi: ZG' \rightarrow Z$. Moreover, G can be recovered from (G', Z, φ) : the map

$$z \mapsto (\varphi(z)^{-1}, z): ZG' \rightarrow Z \times G'$$

is an isomorphism from ZG' onto a central subgroup of $Z \times G'$, and the quotient is G . Clearly, every reductive group arises from such a triple (G', Z, φ) (and G' can even be chosen to be simply connected).

SIMPLY CONNECTED SEMISIMPLE ALGEBRAIC GROUPS

A semisimple algebraic group G is **simply connected** if every central isogeny $G' \rightarrow G$ of connected group varieties is an isomorphism — this agrees with (20.3). In characteristic zero, all isogenies of connected group varieties are central, and so this just says that the only isogenies $G' \rightarrow G$ are the isomorphisms.

For every semisimple algebraic group G over k , there is an initial object in the category of central isogenies $G' \rightarrow G$ (20.21, or deduce it from the isogeny theorem).

Let G be a simply connected semisimple group over a field k , and let $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Then $G_{k^{\mathrm{sep}}}$ decomposes into a product

$$G_{k^{\mathrm{sep}}} = G_1 \times \cdots \times G_r \tag{164}$$

of its almost-simple subgroups G_i . The set $\{G_1, \dots, G_r\}$ contains all the almost-simple subgroups of $G_{k^{\mathrm{sep}}}$. When we apply $\sigma \in \Gamma$ to (164), it becomes

$$G_{k^{\mathrm{sep}}} = \sigma G_{k^{\mathrm{sep}}} = \sigma G_1 \times \cdots \times \sigma G_r$$

with $\{\sigma G_1, \dots, \sigma G_r\}$ a permutation of $\{G_1, \dots, G_r\}$. Let H_1, \dots, H_s denote the products of G_i in the different orbits of Γ . Then $\sigma H_i = H_i$, and so H_i is defined over k (1.41), and

$$G = H_1 \times \cdots \times H_s$$

is a decomposition of G into a product of its almost-simple subgroups.

Now suppose that G itself is almost-simple, so that Γ acts transitively on the G_i in (164). Let

$$\Delta = \{\sigma \in \Gamma \mid \sigma G_1 = G_1\},$$

and let $K = (k^{\mathrm{sep}})^\Delta$.

PROPOSITION 22.129. We have $G \simeq (G_1)_{K/k}$ (restriction of base field).

PROOF. We can rewrite (164) as

$$G_{k^{\text{sep}}} = \prod \sigma G_{1k^{\text{sep}}}$$

where σ runs over a set of cosets for Δ in Γ . On comparing this with the decomposition of $((G_1)_{K/k})_{k^{\text{sep}}}$, we see that there is a canonical isomorphism

$$G_{k^{\text{sep}}} \simeq ((G_1)_{K/k})_{k^{\text{sep}}}$$

over k^{sep} . In particular, the isomorphism commutes with the action of Γ , and so is defined over k (A.41). □

The group G_1 over K is **geometrically almost-simple**, i.e., it is almost-simple and remains almost-simple over K^{al} (often “absolutely almost-simple” is used for “geometrically almost-simple”).

CLASSIFICATION OF SPLIT ALMOST-SIMPLE ALGEBRAIC GROUPS

It remains to classify the geometrically almost-simple algebraic groups over a field, and their centres. We do this here only for the split groups.

Let (V, R) be a reduced root system over \mathbb{Q} . For each $\alpha \in R$, let $\alpha^\vee \in V^\vee$ be the dual root. The **root lattice** $Q(R)$ in V is the \mathbb{Z} -submodule of V generated by the roots, and the **weight lattice** $P(R)$ is

$$\{v \in V \mid \langle v, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}.$$

If $S = \{\alpha_1, \dots, \alpha_r\}$ is a base for R (in particular, a basis for the \mathbb{Q} -vector space V), then $Q(R)$ is the free \mathbb{Z} -module on B — in particular, it is visibly a lattice in V . Moreover,

$$P(R) = \{v \in V \mid \langle v, \alpha_i \rangle \in \mathbb{Z} \text{ for } i = 1, \dots, r\}.$$

In terms of a W -invariant inner product on V ,

$$P(R) = \left\{ v \in V \mid \frac{2(r, \alpha)}{(\alpha, \alpha)} \in \mathbb{Z}, \text{ all } \alpha \in R \right\}.$$

PROPOSITION 22.130. The set of roots of (G, T) is a reduced root system R in $V \stackrel{\text{def}}{=} X^*(T) \otimes \mathbb{Q}$; moreover,

$$Q(R) \subset X^*(T) \subset P(R). \tag{165}$$

By a **diagram** (V, R, X) , we mean a reduced root system (V, R) over \mathbb{Q} and a lattice X in V that is contained between $Q(R)$ and $P(R)$.

THEOREM 22.131 (EXISTENCE). Every diagram arises from a split semisimple algebraic group over k .

THEOREM 22.132 (ISOGENY). Let (G, T) and (G', T') be split semisimple algebraic groups over k , and let (V, R, X) and (V', R', X') be their associated diagrams. An isogeny $(G, T) \rightarrow (G', T')$ defines an isomorphism $V \rightarrow V'$ sending R onto R' and X into X' , and every such isomorphism arises from an isogeny.

In characteristic zero, these statements can be deduced from the similar statements for Lie algebras (see my notes LAG). In the general case, the isogeny theorem for semisimple groups follows from the isogeny theorem for reductive groups (22.93); the existence theorem will be proved in Chapter 25.

o. Reductive groups in characteristic zero

Through out this section, k is a field of characteristic zero.

THE CASIMIR OPERATOR

A Lie algebra is said to be semisimple if its only commutative ideal is $\{0\}$. The Killing form $\kappa_{\mathfrak{g}}$ of a Lie algebra \mathfrak{g} is the trace form for the adjoint representation $\text{ad}: \mathfrak{g} \rightarrow \mathfrak{gl}_{\mathfrak{g}}$, i.e.,

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

Cartan's criterion says that a nonzero Lie algebra \mathfrak{g} is semisimple if and only if its Killing form is nondegenerate (LAG, I, 4.13).

Let \mathfrak{g} be a semisimple Lie algebra, and let $\mathfrak{g}^{\vee} = \text{Hom}_{k\text{-linear}}(\mathfrak{g}, k)$. Then $\kappa_{\mathfrak{g}}$ defines an isomorphism $\mathfrak{g}^{\vee} \rightarrow \mathfrak{g}$ and hence an isomorphism $\beta: \mathfrak{g} \otimes \mathfrak{g}^{\vee} \rightarrow \mathfrak{g} \otimes \mathfrak{g}$. The image of $\text{id}_{\mathfrak{g}}$ under the homomorphisms

$$\text{End}_{k\text{-linear}}(\mathfrak{g}) \simeq \mathfrak{g} \otimes \mathfrak{g}^{\vee} \xrightarrow{\beta} \mathfrak{g} \otimes \mathfrak{g} \subset T(\mathfrak{g}) \rightarrow U(\mathfrak{g}) \quad (166)$$

is called the *Casimir element*. It lies in the centre of $U(\mathfrak{g})$ because $\text{id}_{\mathfrak{g}}$ is invariant under the natural action of \mathfrak{g} on $\text{End}(\mathfrak{g})$ and the maps in (166) commute with the action of \mathfrak{g} . Let e_1, \dots, e_n be a basis for \mathfrak{g} , and let e'_1, \dots, e'_n be the dual basis with respect to $\kappa_{\mathfrak{g}}$. Then

$$c = \sum_{i=1}^n e_i \cdot e'_i.$$

For a representation (V, ρ) of \mathfrak{g} ,

$$c_V \stackrel{\text{def}}{=} \rho(c) = \sum_{i=1}^n e_{iV} \cdot e'_{iV}$$

is called the Casimir operator. Because c lies in the centre of $U(\mathfrak{g})$, c_V is a \mathfrak{g} -homomorphism $V \rightarrow V$. If (V, ρ) is a *faithful* representation of \mathfrak{g} , then

$$\text{Tr}(c_V|V) = \sum_{i=1}^n \text{Tr}(e_i \otimes e'_i|V) = \sum_{i=1}^n \delta_{ii} = n = \dim(\mathfrak{g})$$

(cf. Humphreys 1972, 6.2).

Now let G be a semisimple algebraic group over k . The Lie algebra \mathfrak{g} of G is semisimple (LGA, II, 4.1). Let (V, r) be a representation of G . The Casimir operator c_V for (V, dr) is a \mathfrak{g} -homomorphism $V \rightarrow V$. Thus, c_V is fixed under the natural action of \mathfrak{g} on $\text{End}(V)$, and hence the subspace $\langle c_V \rangle$ is stable under G (12.25). As $X(G) = 0$ (22.121), this implies that c_V is fixed by G .

SUMMARY 22.133. Let G be a semisimple algebraic group. For every nonzero representation (V, r) of G there is a canonical G -equivariant linear map $c_V: V \rightarrow V$ whose trace is nonzero.

SEMISIMPLICITY.

LEMMA 22.134 (SCHUR'S). Let (V, r) be a representation of an algebraic group G . If (V, r) is simple and k is algebraically closed, then $\text{End}(V, r) = k$.

PROOF. Let $\alpha: V \rightarrow V$ be a G -homomorphism of V . Because k is algebraically closed, α has an eigenvector, say, $\alpha(v) = av$, $a \in k$. Now $\alpha - a: V \rightarrow V$ is a G -homomorphism with nonzero kernel. Because V is simple, the kernel must equal V . Hence $\alpha = a$. \square

LEMMA 22.135. *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^{al} .*

PROOF. Let (V, r) be a representation of G . If $(V, r)_{k^{\text{al}}}$ is semisimple, then $\text{End}((V, r)_{k^{\text{al}}})$ is a matrix algebra over k^{al} (22.134). Now

$$\text{End}((V, r)_{k^{\text{al}}}) \simeq \text{End}(V, r) \otimes k^{\text{al}},$$

and so this implies that $\text{End}(V, r)$ is a semisimple k -algebra, which in turn implies that (V, r) is semisimple. (References to be added.) \square

LEMMA 22.136. *Let G be an algebraic group 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) \implies (b) \implies (c) are trivial.

(c) \implies (b). 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) \implies (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

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

They are both G -submodules of $\text{Hom}_{k\text{-linear}}(V, W)$. As V_1/W_1 has dimension 1,

$$V_1 = W_1 \oplus L$$

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 $V \rightarrow W$. As $f|_W = a \text{id}_W$ with $a \neq 0$, the kernel of f is a G -complement to W . \square

PROPOSITION 22.137. *Let G be a semisimple algebraic group over a field k of characteristic zero. Every finite-dimensional representation of G is semisimple.*

PROOF. After (22.135), 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 (22.136) we may suppose that W is simple of codimension 1. As $X(G) = 0$ (22.123) and V/W is one-dimensional, G acts trivially on V/W , and so the Casimir operator $c_{V/W} = 0$. On the other hand, c_V acts on W as scalar by Schur's lemma (22.134). This scalar is nonzero because otherwise $\text{Tr}_V c_V = 0$, which contradicts the nontriviality of the representation. Therefore the kernel of c_V is one-dimensional. It is a G -submodule of V which intersects W trivially, and so it is a G -complement for W . \square

THEOREM 22.138. *The following conditions on a connected algebraic group G over a field 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) \implies (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 $G \rightarrow \text{GL}_V$ 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 (14.50). 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 (22.137). Now $V = \bigoplus_{i,j} V_{ij}$ is a decomposition of V into a direct sum of simple G -modules.

(b) \implies (c): Obvious, because every algebraic group has a faithful finite-dimensional representation (4.8).

(c) \implies (a): This is true over any field (see 20.14). \square

COROLLARY 22.139. *Over a field of characteristic zero, all finite-dimensional representations of an algebraic group G are semisimple if and only if the identity component G° of G is reductive.*

PROOF. To be added (easy). \square

p. Roots of nonsplit reductive groups: a survey

This section will be completely rewritten. The present text has been extracted from Springer's Corvallis talk.

22.140. Let G be a reductive group over k , and let S be a maximal split torus in G , i.e., a subtorus of G that is maximal among the split tori in G . Any two such tori are conjugate by an element of $G(k)$. Their common dimension is called the **k -rank** of G .

22.141. The root system of G with respect to S is called the **relative root system** of (G, S) , and denoted ${}_k R(G, S)$. This is a root system (not necessarily reduced) in the subspace V of $X^*(S) \otimes \mathbb{Q}$ spanned by ${}_k R$. Its Weyl group is called the **relative Weyl group** of G (notation ${}_k W$ or ${}_k W(G)$). The quotient $N_G(S)/C_G(S)$ acts on ${}_k R$ in V . In fact, it can be identified with ${}_k W$. Every coset of $N_G(S)/C_G(S)$ can be represented by an element of $N_G(S)(k)$.

22.142. The centralizer $C_G(S)$ of S in G is a connected reductive group over k (19.17). Its derived group $C(S)'$ is an anisotropic semisimple group, i.e., its k -rank is 0. To a certain

extent, G can be recovered from $C(S)'$ and the relative root system ${}_k R$ (see Tits 1966 and Chapter 26 below). There is a decomposition of the Lie algebra \mathfrak{g} of G :

$$\mathfrak{g} = \mathfrak{g}_0 + \sum_{\alpha \in {}_k R} \mathfrak{g}_\alpha, \quad \mathfrak{g}_\alpha \stackrel{\text{def}}{=} \{X \in \mathfrak{g} \mid \text{Ad}(s)X = \alpha(s)X, \quad s \in S\}.$$

Here \mathfrak{g}_0 is the Lie algebra of $Z(S)$. For each $\alpha \in {}_k R$ there is a unique unipotent subgroup U_α of G normalized by S and with Lie algebra \mathfrak{g}_α .

22.143. If G is split over k , then S is a maximal torus, and ${}_k R$ coincides with the root system of (G, S) . In the general case, ${}_k R$ need not be reduced, and the dimension of \mathfrak{g}_α need not be 1.

PARABOLIC SUBGROUPS

22.144. Recall that a parabolic subgroup P of an algebraic group G is a subgroup variety such that G/P is a projective variety. Over an algebraically closed field, they are the subgroup varieties containing a Borel subgroup.

22.145. In the general case, any two minimal parabolic subgroups of G are conjugate by an element of $G(k)$. If P is one, then there is a maximal split torus S of G such that $P = R_u(P) \rtimes C_G(S)$. There is an ordering of ${}_k R$ such that P is generated by $C_G(S)$ and the U_α with $\alpha > 0$. The minimal parabolic subgroups containing a given S correspond to the Weyl chambers of ${}_k R$. They are permuted simply transitively by the relative Weyl group.

22.146. Fix an ordering of ${}_k R$ and let ${}_k \Delta$ be the basis of ${}_k R$ defined by it. For any other subset $\theta \subset {}_k \Delta$, denote by P_θ the subgroup generated by $C_G(S)$ and the U corresponding to the $\alpha \in {}_k R$ that are linear combinations of the roots of ${}_k \Delta$ in which all roots not in θ occur with a nonnegative coefficient. Then

$$P_{{}_k \Delta} = G, \quad P_\emptyset = P, \quad P_\theta \supset P.$$

22.147. The P_θ are the **standard parabolic subgroups** of G containing P . Every parabolic subgroup is conjugate by an element of $G(k)$ to a unique P_θ . The identity component S_θ of $\bigcap_{\alpha \in \theta} (\text{Ker } \alpha)$ is a k -split torus of G , and we have $P_\theta = R_u(P_\theta) \rtimes C_G(S_\theta)$. The unipotent radical $R_u(P_\theta)$ is generated by the U_α where α runs over the positive roots that are not linear combinations of elements of θ .

22.148. Let Q be a parabolic subgroup of G with unipotent radical V . A **Levi subgroup** of Q is a subgroup L such that Q is the semidirect product $Q = V \rtimes L$. It follows from the above that such L exist. Any two Levi subgroups of Q are conjugate by an element of $G(k)$. If A is a maximal split subtorus of G , then there is a parabolic subgroup Q of G with Levi subgroup L . Two such Q are not necessarily conjugate by an element of $G(k)$ (as they are when A is a maximal split torus). Two parabolic subgroups Q_1 and Q_2 are **associated** if they have Levi subgroups that are k -conjugate. This defines an equivalence relation on the set of parabolic subgroups.

22.149. If Q_1 and Q_2 are two parabolic subgroups, then $(Q_1 \cap Q_2) \cdot R_u(Q_1)$ is also a parabolic subgroup, which is contained in Q_1 . It equals Q_1 if and only if there is a Levi subgroup of Q_1 containing a Levi subgroup of Q_2 . The parabolic subgroups Q_1 and Q_2 are called **opposite** if $Q_1 \cap Q_2$ is a Levi subgroup of Q_1 and Q_2 .

BRUHAT DECOMPOSITION OF $G(k)$

22.150. Let P and S be as before, and let $U = R_u(P)$. For $w \in {}_k W$, let n_w represent w in $N(S)(k)$. The **Bruhat decomposition** of $G(k)$ states that $G(k)$ is the disjoint union of the double cosets $U(k)n_w P(k)$:

$$G(k) = \bigsqcup_{w \in {}_k W} U(k)n_w P(k).$$

We can rephrase this in a more precise way. For $w \in {}_k W$ there exist two subgroup varieties U'_w and U''_w of U such that the map

$$(x, y) \mapsto xn_w y: U'_w \times P \rightarrow U n_w P$$

is an isomorphism. We then have

$$(G/P)(k) = G(k)/P(k) = \bigcup_{w \in {}_k W} \pi(U'_w(k)),$$

where π is the projection $G \rightarrow G/P$.

When k is algebraically closed, this gives a cellular decomposition of the projective variety G/P .

22.151. For $\theta \in {}_k \Delta$, let W_θ denote the subgroup of ${}_k W$ generated by the reflections s_α , $\alpha \in {}_k \Delta$. For $\theta, \theta' \in {}_k \Delta$, there is a bijection of double cosets

$$P_\theta(k) \backslash G(k) / P_{\theta'}(k) \simeq W(\theta) \backslash {}_k W / W(\theta').$$

Let Σ be the set of generators of ${}_k W$ defined by ${}_k \Delta$. The above assertions (on the level of sets) all follow from the fact that $(G(k), P(k), Z(S)(k), \Sigma)$ is a Tits system in the sense of Bourbaki.

q. Pseudo-reductive groups: a survey

We briefly summarize Conrad, Gabber, and Prasad 2010, which completes earlier work of Borel and Tits (Borel and Tits 1978; Tits 1992, 1993; Springer 1998, Chapters 13–15).

DEFINITION 22.152. An algebraic group G is **pseudo-reductive** if it is smooth and connected, and $R_u(G) = e$.

A connected group variety is pseudo-reductive if it admits a faithful semisimple representation (22.19).

22.153. Let k be a separably closed field of characteristic p , and let $G = (\mathbb{G}_m)_{k'/k}$ where k' is an extension of k of degree p (necessarily purely inseparable). Then G is a commutative smooth connected algebraic group over k . The canonical map $\mathbb{G}_m \rightarrow G$ realizes \mathbb{G}_m as the greatest subgroup of G of multiplicative type, and the quotient G/\mathbb{G}_m is unipotent. Over k^{al} , G decomposes into $(\mathbb{G}_m)_{k^{\text{al}}} \times (G/\mathbb{G}_m)_{k^{\text{al}}}$ (see 17.31), and so G is not reductive. However, G contains no smooth unipotent subgroup because $G(k) = k'^{\times}$, which has no p -torsion. Therefore G is pseudo-reductive. (Recall 3.29 that if G is reductive, then $(G)_{k'/k}(k)$ is dense in $(G)_{k'/k}$ if k is infinite.)

22.154. Let k' be a finite field extension of k , and let G be a reductive group over k' . If k' is separable over k , then $(G)_{k'/k}$ is reductive, but otherwise it is only pseudoreductive.

22.155. 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 $\text{Gal}(k^{\text{sep}}/k)$ 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. 2010, p. xv).

22.156. Let k_1, \dots, k_n be finite field extensions of k . For each i , let G_i be a reductive group over k_i , and let T_i be a maximal torus in G_i . Define algebraic groups

$$G \leftarrow T \twoheadrightarrow \bar{T}$$

by

$$\begin{aligned} G &= \prod_i (G_i)_{k_i/k} \\ T &= \prod_i (T_i)_{k_i/k} \\ \bar{T} &= \prod_i (T_i/Z(G_i))_{k_i/k}. \end{aligned}$$

Let $\phi: T \rightarrow C$ be a homomorphism of commutative pseudoreductive groups that factors through the quotient map $T \rightarrow \bar{T}$:

$$T \xrightarrow{\phi} C \xrightarrow{\psi} \bar{T}.$$

Then ψ defines an action of C on G by conjugation, and so we can form the semidirect product

$$G \rtimes C.$$

The map

$$t \mapsto (t^{-1}, \phi(t)): T \rightarrow G \rtimes C$$

is an isomorphism from T onto a central subgroup of $G \rtimes C$, and the quotient $(G \rtimes C)/T$ is a pseudoreductive group over k . The main theorem (5.1.1) of Conrad et al. 2010 says that, except possibly when k has characteristic 2 or 3, every pseudoreductive group over k arises by such a construction (the theorem also treats the exceptional cases).

22.157. The maximal tori in reductive groups are their own centralizers. Any pseudoreductive group with this property is reductive (except possibly in characteristic 2; Conrad et al. 2010, 11.1.1).

22.158. If G is reductive, then $G = \mathcal{D}G \cdot (ZG)^\circ$ where $\mathcal{D}G$ is the derived group of G and $(ZG)^\circ$ is the greatest central connected reductive subgroup of G . This statement becomes false with “pseudoreductive” for “reductive” (Conrad et al. 2010, 11.2.1).

22.159. For a reductive group G , the map

$$RG = (ZG)^\circ \rightarrow G/\mathcal{D}G$$

is an isogeny, and G is semisimple if and only if one (hence both) groups are trivial. For a pseudoreductive group, the condition $RG = 1$ does not imply that $G = \mathcal{D}G$. Conrad et al. 2010, 11.2.2, instead adopt the definition: an algebraic group G is *pseudo-semisimple* if it is pseudoreductive and $G = \mathcal{D}G$. The derived group of a pseudoreductive group is pseudo-semisimple (ibid. 1.2.6, 11.2.3).

22.160. A reductive group G over any field k is unirational, and so $G(k)$ is dense in G if k is infinite. This fails for pseudoreductive groups: over every nonperfect field k there exists a commutative pseudoreductive group that is not unirational; when k is a nonperfect rational function field $k_0(T)$, such a group G can be chosen so that $G(k)$ is not dense in G (Conrad et al. 2010, 11.3.1).

r. Levi subgroups: a survey

We have studied reductive groups in this chapter. Every connected group variety G over a field k is an extension

$$e \rightarrow R_u(G) \rightarrow G \rightarrow G/R_u(G) \rightarrow e$$

of a pseudo-reductive group by a unipotent group. If k is perfect, then $G/R_u(G)$ is reductive and the unipotent group $R_u(G)$ is split. In good cases, the extension splits.

DEFINITION 22.161. 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 $G_{k^{\text{al}}} \rightarrow G_{k^{\text{al}}}/R_u G_{k^{\text{al}}}$ restricts to an isomorphism $L_{k^{\text{al}}} \rightarrow G_{k^{\text{al}}}/R_u G_{k^{\text{al}}}$. In other words, $G_{k^{\text{al}}}$ is the semidirect product

$$G_{k^{\text{al}}} = R_u G_{k^{\text{al}}} \rtimes L_{k^{\text{al}}}$$

of a reductive group $L_{k^{\text{al}}}$ with a unipotent group $R_u G_{k^{\text{al}}}$.

22.162. Suppose that there exists a unipotent subgroup R of G such that $R_{k^{\text{al}}} = R_u(G_{k^{\text{al}}})$ (so G/R is reductive). Then a Levi subgroup of G is a connected subgroup variety L such that the quotient map $G \rightarrow G/R$ restricts to an isomorphism $L \rightarrow G/R$. In this case, G is the semidirect product

$$G = R \rtimes L$$

of a reductive group L with a unipotent group R .

22.163. When k is perfect, a subgroup R as in (22.162) always exists. In characteristic zero, Levi subgroups always exist (Theorem of Mostow; Hochschild 1981, VIII, Theorem 4.3).

22.164. In nonzero characteristic, a connected group variety G need not have a Levi subgroup.

22.165. Every pseudo-reductive group with a split maximal torus has a Levi subgroup (Conrad et al. 2010, 3.4.1).

This section will be expanded somewhat. For the present, here are some references.
[mo133249](#).

Humphreys, J. E. Existence of Levi factors in certain algebraic groups. Pacific J. Math. 23 1967 543–546.

McNinch, George J. Levi decompositions of a linear algebraic group. Transform. Groups 15 (2010), no. 4, 937–964.

McNinch, George On the descent of Levi factors. Arch. Math. (Basel) 100 (2013), no. 1, 7–24.

McNinch, George J. Levi factors of the special fiber of a parahoric group scheme and tame ramification. Algebr. Represent. Theory 17 (2014), no. 2, 469–479.

s. Exercises

EXERCISE 22-1. 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 unipotent algebraic group by an anti-affine algebraic group. [Let G be an affine linearly reductive group scheme over a field. Suppose that there are only finitely many simple representations (up to isomorphism) and let X be the direct sum of them. Then every representation of G is isomorphic to a subquotient (in fact, direct factor) of X^n for some n . This implies that G is finite (see, for example, Deligne and Milne, Tannakian Categories, 2.20).]

EXERCISE 22-2. Let G be a reductive group.

- (a) Show that the kernel of the adjoint representation of G on $\text{Lie } G$ is the centre of G .
- (b) Show that $Z(G/Z(G)) = 1$.

EXERCISE 22-3. A semisimple algebraic group G over a field of characteristic zero has a faithful simple representation if and only if $X^*(ZG)$ is cyclic (mo29813). (Spin groups in even dimensions have center a non-cyclic group (of order 4) and so have no faithful simple representations.)

Root data and their classification

This chapter will be revised but not expanded (perhaps I'll include a direct proof that the Weyl group acts simply transitively on the Weyl chambers, 23.16).

Throughout, F is a field of characteristic zero, for example, \mathbb{Q} or \mathbb{R} .

a. Equivalent definitions of a root datum

The following is the standard definition (SGA 3, XXI, 1.1.1).

DEFINITION 23.1. A root datum 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 $\langle \cdot, \cdot \rangle: X \times X^\vee \rightarrow \mathbb{Z}$,
- ◇ R, R^\vee are finite subsets of X and X^\vee in bijection by a correspondence $\alpha \leftrightarrow \alpha^\vee$, satisfying the following conditions

RD1 $\langle \alpha, \alpha^\vee \rangle = 2$,

RD2 $s_\alpha(R) \subset R, s_\alpha^\vee(R^\vee) \subset R^\vee$, where

$$\begin{aligned} s_\alpha(x) &= x - \langle x, \alpha^\vee \rangle \alpha, & \text{for } x \in X, \alpha \in R, \\ s_\alpha^\vee(y) &= y - \langle \alpha, y \rangle \alpha^\vee, & \text{for } y \in X^\vee, \alpha \in R. \end{aligned}$$

Recall that RD1 implies that $s_\alpha(\alpha) = -\alpha$ and $s_\alpha^2 = 1$.

Thus in (23.1), the condition $s_\alpha^\vee(R^\vee) \subset R^\vee$ replaces the condition that $W(\mathcal{R})$ is finite in (22.37). Definition 23.1 has the merit of being self-dual, but (22.37) is usually easier to work with.

Set¹

$$\begin{aligned} Q &= \mathbb{Z}R \subset X & Q^\vee &= \mathbb{Z}R^\vee \subset X^\vee \\ V &= \mathbb{Q} \otimes_{\mathbb{Z}} Q & V^\vee &= \mathbb{Q} \otimes_{\mathbb{Z}} Q^\vee. \\ X_0 &= \{x \in X \mid \langle x, R^\vee \rangle = 0\} \end{aligned}$$

By $\mathbb{Z}R$ we mean the \mathbb{Z} -submodule of X generated by the $\alpha \in R$.

LEMMA 23.2. For $\alpha \in R, x \in X$, and $y \in X^\vee$,

$$\langle s_\alpha(x), y \rangle = \langle x, s_\alpha^\vee(y) \rangle, \tag{167}$$

and so

$$\langle s_\alpha(x), s_\alpha^\vee(y) \rangle = \langle x, y \rangle. \tag{168}$$

¹The notation Q^\vee is a bit confusing, because Q^\vee is not in fact the dual of Q .

PROOF. We have

$$\begin{aligned}\langle s_\alpha(x), y \rangle &= \langle x - \langle x, \alpha^\vee \rangle \alpha, y \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle \\ \langle x, s_\alpha^\vee(y) \rangle &= \langle x, y - \langle \alpha, y \rangle \alpha^\vee \rangle = \langle x, y \rangle - \langle x, \alpha^\vee \rangle \langle \alpha, y \rangle,\end{aligned}$$

which gives the first formula, and the second is obtained from the first by replacing y with $s_\alpha^\vee(y)$. \square

In other words, as the notation suggests, s_α^\vee (which is sometimes denoted s_{α^\vee}) is the transpose of s_α .

THEOREM 23.3. *Let (X, R, X^\vee, R^\vee) be a root system, and let $f: R \rightarrow R^\vee$ be the bijection $\alpha \mapsto \alpha^\vee$. Then (X, R, f) satisfies the conditions **(rd1)**, **(rd2)**, and **(rd3)** of (22.37). Conversely, let (X, R, f) be a system satisfying these conditions; let $X^\vee = \text{Hom}(X, \mathbb{Z})$ and let $R^\vee = f(R)$; then the system (X, R, X^\vee, R^\vee) together with the natural pairing $X \times X^\vee \rightarrow \mathbb{Z}$ and the bijection $\alpha \leftrightarrow f(\alpha)$ form a root system in the sense of (23.2).*

PROOF. For the first statement, we only have to check **(rd3)**: the group of automorphisms of X generated by the s_α is finite.

For the second statement, we have to show that

$$s_\alpha^\vee(R^\vee) \subset R^\vee \text{ where } s_\alpha^\vee(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

As in Lemma 23.2, $\langle s_\alpha(x), s_\alpha^\vee(y) \rangle = \langle x, y \rangle$.

Let $\alpha, \beta \in R$, and let $t = s_{s_\alpha(\beta)} s_\alpha s_\beta s_\alpha$. An easy calculation² shows that

$$t(x) = x + (\langle x, s_\alpha^\vee(\beta^\vee) \rangle - \langle x, s_\alpha(\beta)^\vee \rangle) s_\alpha(\beta), \quad \text{all } x \in X.$$

Since

$$\langle s_\alpha(\beta), s_\alpha^\vee(\beta^\vee) \rangle - \langle s_\alpha(\beta), s_\alpha(\beta)^\vee \rangle = \langle \beta, \beta^\vee \rangle - \langle s_\alpha(\beta), s_\alpha(\beta)^\vee \rangle = 2 - 2 = 0,$$

we see that $t(s_\alpha(\beta)) = s_\alpha(\beta)$. Thus,

$$(t - 1)^2 = 0,$$

and so the minimum polynomial of t acting on $\mathbb{Q} \otimes_{\mathbb{Z}} X$ divides $(T - 1)^2$. On the other hand, since t lies in a finite group, it has finite order, say $t^m = 1$. Thus, the minimum polynomial also divides $T^m - 1$, and so it divides

$$\text{gcd}(T^m - 1, (T - 1)^2) = T - 1.$$

This shows that $t = 1$, and so

$$\langle x, s_\alpha^\vee(\beta^\vee) \rangle - \langle x, s_\alpha(\beta)^\vee \rangle = 0 \text{ for all } x \in X.$$

Hence

$$s_\alpha^\vee(\beta^\vee) = s_\alpha(\beta)^\vee \in R^\vee. \quad \square$$

Thus, to give a root system in the sense of (23.1) amounts to giving a system (X, R, f) satisfying (22.37).

²Or so it is stated in Springer 1979, 1.4; details to be added.

b. Deconstructing root data

Explain how they are built up from semisimple root data and toral root data

c. Semisimple root data and root systems

An **inner product** on a real vector space is a positive-definite symmetric bilinear form.

GENERALITIES ON SYMMETRIES

A **reflection** of a vector space V is an endomorphism of V that fixes the vectors in a hyperplane and acts as -1 on a complementary line. Let α be a nonzero element of V . A **reflection with vector α** is an endomorphism s of V such that $s(\alpha) = -\alpha$ and the set of vectors fixed by s is a hyperplane H . Then $V = H \oplus \langle \alpha \rangle$ with s acting as $1 \oplus -1$, and so $s^2 = 1$. Let V^\vee be the dual vector space to V , and write $\langle \cdot, \cdot \rangle$ for the tautological pairing $V \times V^\vee \rightarrow k$. If α^\vee is an element of V^\vee such that $\langle \alpha, \alpha^\vee \rangle = 2$, then

$$s_\alpha: x \mapsto x - \langle x, \alpha^\vee \rangle \alpha \tag{169}$$

is a reflection with vector α , and every reflection with vector α is of this form (for a unique α^\vee)³.

LEMMA 23.4. *Let R be a finite spanning set for V . For any nonzero vector α in V , there exists at most one reflection s with vector α such that $s(R) \subset R$.*

PROOF. Let s and s' be such reflections, and let $t = ss'$. Then t acts as the identity map on both $F\alpha$ and $V/F\alpha$, and so

$$(t - 1)^2 V \subset (t - 1)F\alpha = 0.$$

Thus the minimum polynomial of t divides $(T - 1)^2$. On the other hand, because R is finite, there exists an integer $m \geq 1$ such that $t^m(x) = x$ for all $x \in R$, and hence for all $x \in V$. Therefore the minimum polynomial of t divides $T^m - 1$. As $(T - 1)^2$ and $T^m - 1$ have greatest common divisor $T - 1$, this shows that $t = 1$. □

LEMMA 23.5. *Let (\cdot, \cdot) be an inner product on a real vector space V . Then, for any nonzero vector α in V , there exists a unique symmetry s with vector α that is orthogonal for (\cdot, \cdot) , i.e., such that $(sx, sy) = (x, y)$ for all $x, y \in V$, namely*

$$s(x) = x - 2 \frac{(x, \alpha)}{(\alpha, \alpha)} \alpha. \tag{170}$$

PROOF. Certainly, (170) does define an orthogonal symmetry with vector α . Suppose s' is a second such symmetry, and let $H = \langle \alpha \rangle^\perp$. Then H is stable under s' , and maps isomorphically on $V/\langle \alpha \rangle$. Therefore s' acts as 1 on H . As $V = H \oplus \langle \alpha \rangle$ and s' acts as -1 on $\langle \alpha \rangle$, it must coincide with s . □

³The composite of the quotient map $V \rightarrow V/H$ with the linear map $V/H \rightarrow F$ sending $\alpha + H$ to 2 is the unique element α^\vee of V^\vee such that $\alpha(H) = 0$ and $\langle \alpha, \alpha^\vee \rangle = 2$.

GENERALITIES ON LATTICES

In this subsection V is a finite-dimensional vector space over F .

DEFINITION 23.6. A subgroup of V is a **lattice** in V if it can be generated (as a \mathbb{Z} -module) by a basis for V . Equivalently, a subgroup X is a lattice if the natural map $F \otimes_{\mathbb{Z}} X \rightarrow V$ is an isomorphism.

REMARK 23.7. (a) When $F = \mathbb{Q}$, every finitely generated subgroup of V that spans V is a lattice, but this is not true for $F = \mathbb{R}$ or \mathbb{C} . For example, $\mathbb{Z}1 + \mathbb{Z}\sqrt{2}$ is not a lattice in \mathbb{R} .

(b) When $F = \mathbb{R}$, the discrete subgroups of V are the **partial lattices**, i.e., \mathbb{Z} -modules generated by an \mathbb{R} -linearly independent set of vectors for V (see my notes on algebraic number theory 4.13).

DEFINITION 23.8. A **perfect pairing** of free \mathbb{Z} -modules of finite rank is one that realizes each as the dual of the other. Equivalently, it is a pairing into \mathbb{Z} with discriminant ± 1 .

PROPOSITION 23.9. Let

$$\langle , \rangle : V \times V^\vee \rightarrow k$$

be a nondegenerate bilinear pairing, and let X be a lattice in V . Then

$$Y = \{y \in V^\vee \mid \langle X, y \rangle \subset \mathbb{Z}\}$$

is the unique lattice in V^\vee such that \langle , \rangle restricts to a perfect pairing

$$X \times Y \rightarrow \mathbb{Z}.$$

PROOF. Let e_1, \dots, e_n be a basis for V generating X , and let e'_1, \dots, e'_n be the dual basis. Then

$$Y = \mathbb{Z}e'_1 + \dots + \mathbb{Z}e'_n,$$

and so it is a lattice, and it is clear that \langle , \rangle restricts to a perfect pairing $X \times Y \rightarrow \mathbb{Z}$.

Let Y' be a second lattice in V^\vee such that $\langle x, y \rangle \in \mathbb{Z}$ for all $x \in X, y \in Y'$. Then $Y' \subset Y$, and an easy argument shows that the discriminant of the pairing $X \times Y' \rightarrow \mathbb{Z}$ is $\pm(Y : Y')$, and so the pairing on $X \times Y'$ is perfect if and only if $Y' = Y$. \square

d. Root systems

In this section, we briefly explain the classification of root systems in terms of Dynkin diagrams. Omitted proofs can be found in LAG I, §8 or [Serre 1966](#), for example.

Let V be a finite-dimensional vector space over F .

DEFINITION 23.10. A subset R of V over F is a **root system** in V if

RS1 R is finite, spans V , and does not contain 0;

RS2 for each $\alpha \in R$, there exists a (unique) reflection s_α with vector α such that $s_\alpha(R) \subset R$;

RS3 for all $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ is an integer multiple of α .

In other words, R is a root system if it satisfies RS1 and, for each $\alpha \in R$, there exists a (unique) vector $\alpha^\vee \in V^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$, $\langle R, \alpha^\vee \rangle \in \mathbb{Z}$, and the reflection $s_\alpha : x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ maps R in R .

We sometimes refer to the pair (V, R) as a root system over F . The elements of R are called the **roots** of the root system. If α is a root, then $s_\alpha(\alpha) = -\alpha$ is also a root. The unique α^\vee attached to α is called its **coroot**. The dimension of V is called the **rank** of the root system.

By root system, we shall mean reduced root system.

EXAMPLE 23.11. Let V be the hyperplane in F^{n+1} of $n + 1$ -tuples $(x_i)_{1 \leq i \leq n+1}$ such that $\sum x_i = 0$, and let

$$R = \{\alpha_{ij} \stackrel{\text{def}}{=} e_i - e_j \mid i \neq j, \quad 1 \leq i, j \leq n + 1\}$$

where $(e_i)_{1 \leq i \leq n+1}$ is the standard basis for F^{n+1} . For each $i \neq j$, let $s_{\alpha_{ij}}$ be the linear map $V \rightarrow V$ that switches the i th and j th entries of an $n + 1$ -tuple in V . Then $s_{\alpha_{ij}}$ is a reflection with vector α_{ij} such that $s_{\alpha_{ij}}(R) \subset R$ and $s_{\alpha_{ij}}(\beta) - \beta \in \mathbb{Z}\alpha_{ij}$ for all $\beta \in R$. As R obviously spans V , this shows that R is a root system in V .

23.12. Let (\cdot, \cdot) be an inner product on a real vector space V . Then, for any nonzero vector α in V , there exists a unique symmetry s with vector α that is orthogonal for (\cdot, \cdot) , i.e., such that $(sx, sy) = (x, y)$ for all $x, y \in V$, namely

$$s(x) = x - 2 \frac{(x, \alpha)}{(\alpha, \alpha)} \alpha. \tag{171}$$

23.13. Let (V, R) be a root system over F , and let V_0 be the \mathbb{Q} -vector space generated by R . Then $c \otimes v \mapsto cv: F \otimes_{\mathbb{Q}} V_0 \rightarrow V$ is an isomorphism, and R is a root system in V_0 .

Thus, to give a root system over F is the same as giving a root system over \mathbb{Q} (or \mathbb{R} or \mathbb{C}). In the following, we assume that $F \subset \mathbb{R}$ (and sometimes that $F = \mathbb{R}$).

23.14. If $(V_i, R_i)_{i \in I}$ is a finite family of root systems, then

$$\bigoplus_{i \in I} (V_i, R_i) \stackrel{\text{def}}{=} (\bigoplus_{i \in I} V_i, \bigsqcup R_i)$$

is a root system (called the **direct sum** of the (V_i, R_i)).

A root system is **indecomposable** (or **irreducible**) if it can not be written as a direct sum of nonempty root systems.

23.15. Let (V, R) be a root system. There exists a unique partition $R = \bigsqcup_{i \in I} R_i$ of R such that

$$(V, R) = \bigoplus_{i \in I} (V_i, R_i), \quad V_i = \text{span of } R_i,$$

and each (V_i, R_i) is an indecomposable root system.

THE WEYL GROUP

Let (V, R) be a root system. The **Weyl group** $W = W(R)$ of (V, R) is the subgroup of $GL(V)$ generated by the reflections s_α for $\alpha \in R$. Because R spans V , the group W acts faithfully on R , and so is finite.

For $\alpha \in R$, we let H_α denote the hyperplane of vectors fixed by s_α . A **Weyl chamber** is a connected component of $V \setminus \bigcup_{\alpha \in R} H_\alpha$.

23.16. The group $W(R)$ acts simply transitively on the set of Weyl chambers (Bourbaki LIE, VI, §1, 5).

EXISTENCE OF AN INNER PRODUCT

23.17. For any root system (V, R) , there exists an inner product (\cdot, \cdot) on V such the $w \in R$, act as orthogonal transformations, i.e., such that

$$(wx, wy) = (x, y) \text{ for all } w \in W, x, y \in V.$$

Let $(\cdot, \cdot)'$ be any inner product $V \times V \rightarrow \mathbb{R}$, and define

$$(x, y) = \sum_{w \in W} (wx, wy)'.$$

Then (\cdot, \cdot) is again an inner product, and

$$(w_0x, w_0y) = \sum_{w \in W} (ww_0x, ww_0y)' = (x, y)$$

for any $w_0 \in W$, because as w runs through W , so also does ww_0 .

When we equip V with an inner product (\cdot, \cdot) as in (23.17),

$$s_\alpha(x) = x - 2 \frac{(x, \alpha)}{(\alpha, \alpha)} \alpha \text{ for all } x \in V.$$

Therefore the hyperplane of vectors fixed by α is orthogonal to α , and the ratio $(x, \alpha)/(\alpha, \alpha)$ is independent of the choice of the inner product:

$$2 \frac{(x, \alpha)}{(\alpha, \alpha)} = \langle x, \alpha^\vee \rangle.$$

BASES

Let (V, R) be a root system. A subset S of R is a **base** for R if it is a basis for V and if each root can be written $\beta = \sum_{\alpha \in S} m_\alpha \alpha$ with the m_α integers of the same sign (i.e., either all $m_\alpha \geq 0$ or all $m_\alpha \leq 0$). The elements of a (fixed) base are called the **simple roots** (for the base).

23.18. There exists a base S for R .

More precisely, let t lie in a Weyl chamber, so t is an element of V such that $\langle t, \alpha^\vee \rangle \neq 0$ if $\alpha \in R$, and let $R^+ = \{\alpha \in R \mid (\alpha, t) > 0\}$. Say that $\alpha \in R^+$ is **indecomposable** if it can not be written as a sum of two elements of R^+ . The indecomposable elements form a base, which depends only on the Weyl chamber of t . Every base arises in this way from a unique Weyl chamber, and so (23.16) shows that W acts simply transitively on the set of bases for R .

23.19. Let S be a base for R . Then W is generated by the $\{s_\alpha \mid \alpha \in S\}$, and $W \cdot S = R$.

23.20. Let S be a base for R . If S is indecomposable, there exists a root $\tilde{\alpha} = \sum_{\alpha \in S} n_\alpha \alpha$ such that, for any other root $\sum_{\alpha \in S} m_\alpha \alpha$, we have that $n_\alpha \geq m_\alpha$ for all α .

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**.

23.21. Let (V, R) be the root system in (23.11), and endow V with the usual inner product (assume $F \subset \mathbb{R}$). When we choose

$$t = ne_1 + \cdots + e_n - \frac{n}{2}(e_1 + \cdots + e_{n+1}),$$

then

$$R^+ \stackrel{\text{def}}{=} \{\alpha \mid (\alpha, t) > 0\} = \{e_i - e_j \mid i > j\}.$$

For $i > j + 1$,

$$e_i - e_j = (e_i - e_{i+1}) + \cdots + (e_{j+1} - e_j),$$

and so $e_i - e_j$ is decomposable. The indecomposable elements are $e_1 - e_2, \dots, e_n - e_{n+1}$. Obviously, they *do* form a base S for R . The Weyl group has a natural identification with S_{n+1} , and it certainly is generated by the elements $s_{\alpha_1}, \dots, s_{\alpha_n}$ where $\alpha_i = e_i - e_{i+1}$; moreover, $W \cdot S = R$. The highest root is

$$\tilde{\alpha} = e_1 - e_{n+1} = \alpha_1 + \cdots + \alpha_n.$$

ROOT SYSTEMS OF RANK 2

The root systems of rank 1 are the subsets $\{\alpha, -\alpha\}$, $\alpha \neq 0$, of a vector space V of dimension 1, and so the first interesting case is rank 2. Assume $F = \mathbb{R}$, and choose an invariant inner product. For roots α, β , we let

$$n(\beta, \alpha) = 2 \frac{(\beta, \alpha)}{(\alpha, \alpha)} = \langle \beta, \alpha^\vee \rangle \in \mathbb{Z}.$$

Write

$$n(\beta, \alpha) = 2 \frac{|\beta|}{|\alpha|} \cos \phi$$

where $|\cdot|$ denotes the length of a vector and ϕ is the angle between α and β . Then

$$n(\beta, \alpha) \cdot n(\alpha, \beta) = 4 \cos^2 \phi \in \mathbb{Z}.$$

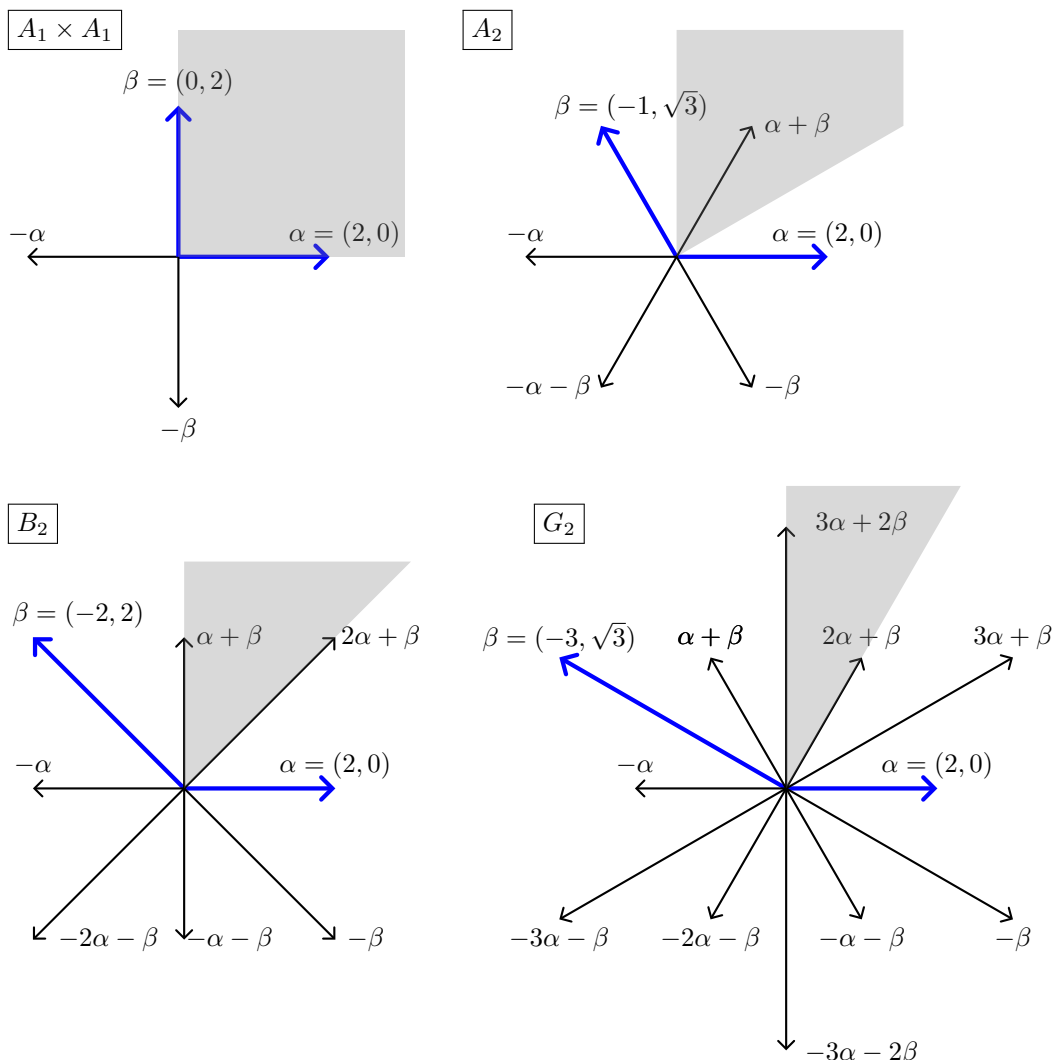
When we exclude the possibility that β is a multiple of α , there are only the following possibilities (in the table, we have chosen β to be the longer root):

$n(\beta, \alpha) \cdot n(\alpha, \beta)$	$n(\alpha, \beta)$	$n(\beta, \alpha)$	ϕ	$ \beta / \alpha $
0	0	0	$\pi/2$	
1	1 -1	1 -1	$\pi/3$ $2\pi/3$	1
2	1 -1	2 -2	$\pi/4$ $3\pi/4$	$\sqrt{2}$
3	1 -1	3 -3	$\pi/6$ $5\pi/6$	$\sqrt{3}$

If α and β are simple roots and $n(\alpha, \beta)$ and $n(\beta, \alpha)$ are strictly positive (i.e., the angle between α and β is acute), then (from the table) one, say, $n(\beta, \alpha)$, equals 1. Then

$$s_\alpha(\beta) = \beta - n(\beta, \alpha)\alpha = \beta - \alpha,$$

and so $\pm(\alpha - \beta)$ are roots, and one, say $\alpha - \beta$, will be in R^+ . But then $\alpha = (\alpha - \beta) + \beta$, contradicting the simplicity of α . We conclude that $n(\alpha, \beta)$ and $n(\beta, \alpha)$ are both negative. From this it follows that there are exactly the four nonisomorphic root systems of rank 2 displayed below. The set $\{\alpha, \beta\}$ is the base determined by the shaded Weyl chamber.



Note that each set of vectors does satisfy (RS1–3). The root system $A_1 \times A_1$ is decomposable and the remainder are indecomposable.

We have

	$A_1 \times A_1$	A_2	B_2	G_2
$s_\alpha(\beta) - \beta$	0α	1α	2α	3α
ϕ	$\pi/2$	$2\pi/3$	$3\pi/4$	$5\pi/6$
$W(R)$	D_2	D_3	D_4	D_6
$(\text{Aut}(R): W(R))$	2	2	1	1

where D_n denotes the dihedral group of order $2n$.

CARTAN MATRICES

Let (V, R) be a root system. As before, for $\alpha, \beta \in R$, we let

$$n(\alpha, \beta) = \langle \alpha, \beta^\vee \rangle \in \mathbb{Z},$$

so that

$$n(\alpha, \beta) = 2 \frac{(\alpha, \beta)}{(\beta, \beta)}$$

for any inner form satisfying (23.17). 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,

$$\begin{array}{cccc} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} & \begin{pmatrix} 2 & -1 \\ -2 & 2 \end{pmatrix} & \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} \\ A_1 \times A_1 & A_2 & B_2 & G_2 \end{array}$$

and the Cartan matrix for the root system in (23.11) 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 23.22. *The Cartan matrix of (V, R) is independent of S , and determines (V, R) up to isomorphism.*

In fact, if S' is a second base for R , then we know that $S' = wS$ for a *unique* $w \in W$ and that $n(w\alpha, w\beta) = n(\alpha, \beta)$. Thus S and S' give the same Cartan matrices up to re-indexing the columns and rows. Let (V', R') be a second root system with the same Cartan matrix. This means that there exists a base S' for R' and a bijection $\alpha \mapsto \alpha': S \rightarrow S'$ such that

$$n(\alpha, \beta) = n(\alpha', \beta') \text{ for all } \alpha, \beta \in S. \quad (172)$$

The bijection extends uniquely to an isomorphism of vector spaces $V \rightarrow V'$, which sends s_α to $s_{\alpha'}$ for all $\alpha \in S$ because of (172). But the s_α generate the Weyl groups (23.19), and so the isomorphism maps W onto W' , and hence it maps $R = W \cdot S$ onto $R' = W' \cdot S'$ (see 23.19). We have shown that the bijection $S \rightarrow S'$ extends uniquely to an isomorphism $(V, R) \rightarrow (V', R')$ of root systems.

CLASSIFICATION OF ROOT SYSTEMS BY DYNKIN DIAGRAMS

Let (V, R) be a root system, and let S be a base for R .

PROPOSITION 23.23. *Let α and β be distinct simple roots. Up to interchanging α and β , the only possibilities for $n(\alpha, \beta)$ are*

$n(\alpha, \beta)$	$n(\beta, \alpha)$	$n(\alpha, \beta)n(\beta, \alpha)$
0	0	0
-1	-1	1
-2	-1	2
-3	-1	3

If W is the subspace of V spanned by α and β , then $W \cap R$ is a root system of rank 2 in W , and so (23.23) can be read off from the Cartan matrices of the rank 2 systems.

Choose a base S for R . Then the **Coxeter graph** of (V, R) is the graph whose nodes are indexed by the elements of S ; two distinct nodes are joined by $n(\alpha, \beta) \cdot n(\beta, \alpha)$ edges. Up to the indexing of the nodes, it is independent of the choice of S .

PROPOSITION 23.24. *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.

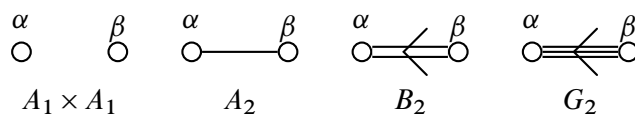
PROOF. A root system is decomposable if and only if R can be written as a disjoint union $R = R_1 \sqcup R_2$ with each root in R_1 orthogonal to each root in R_2 . Since roots α, β are orthogonal if and only if $n(\alpha, \beta) \cdot n(\beta, \alpha) = 4 \cos^2 \phi = 0$, this is equivalent to the Coxeter graph being disconnected. \square

The Coxeter graph doesn't determine the Cartan matrix because it only gives the number $n(\alpha, \beta) \cdot n(\beta, \alpha)$. However, for each value of $n(\alpha, \beta) \cdot n(\beta, \alpha)$ there is only one possibility for the unordered pair

$$\{n(\alpha, \beta), n(\beta, \alpha)\} = \left\{ 2 \frac{|\alpha|}{|\beta|} \cos \phi, 2 \frac{|\beta|}{|\alpha|} \cos \phi \right\}.$$

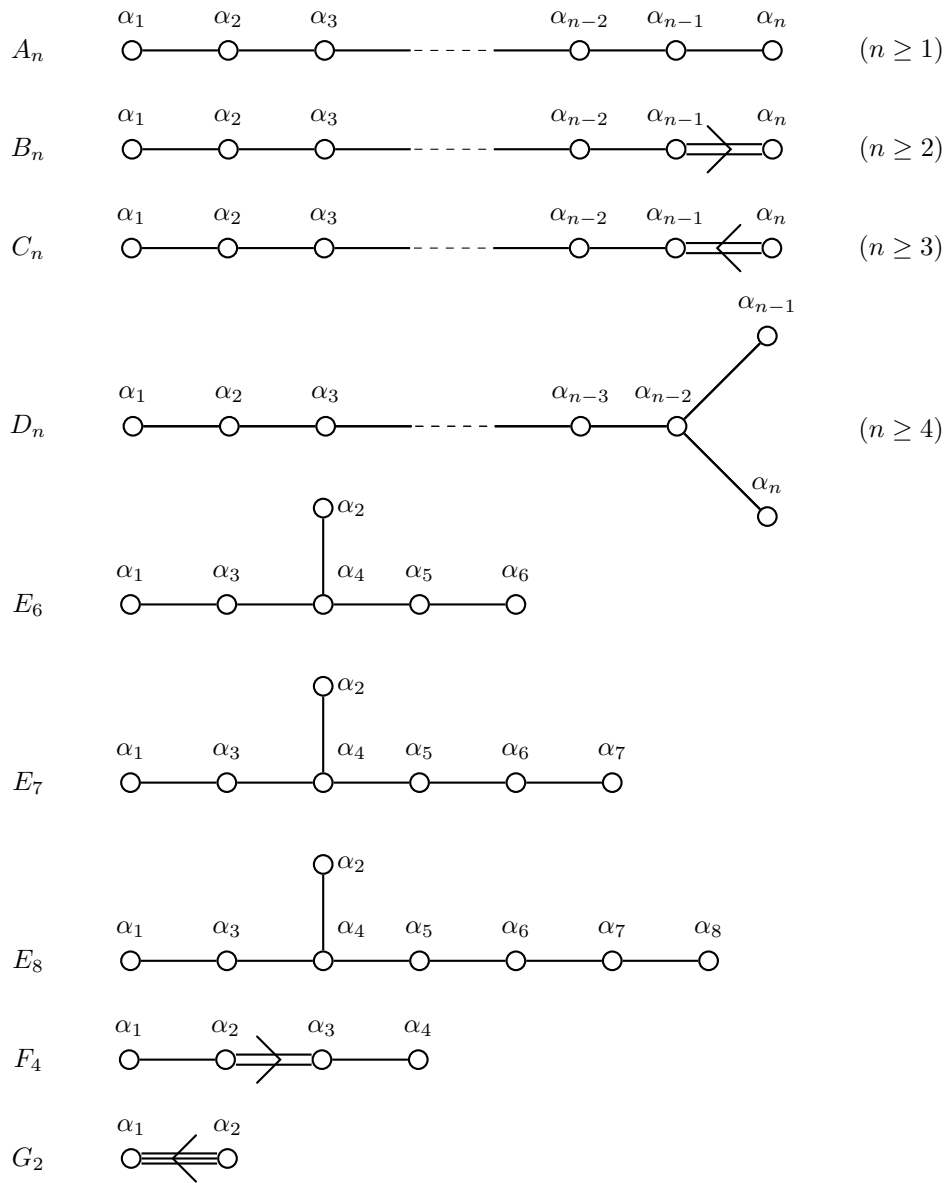
Thus, if we know in addition which is the longer root, then we know the *ordered* pair. To remedy this, we put an arrowhead on the lines joining the nodes indexed by α and β pointing towards the shorter root. The resulting diagram is called the **Dynkin diagram** of the root system. It determines the Cartan matrix and hence the root system.

For example, the Dynkin diagrams of the root systems of rank 2 are:



THEOREM 23.25. *The Dynkin diagrams arising from indecomposable root systems are exactly the diagrams A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), D_n ($n \geq 4$), E_6 , E_7 , E_8 , F_4 , G_2 listed below — we have used the conventional (Bourbaki) numbering for the simple roots.*

For example, the Dynkin diagram of the root system in (23.11) is A_n . Note that Coxeter graphs do not distinguish B_n from C_n .



Representations of reductive groups

This chapter will include proofs for the classification of semisimple representations and a brief survey of the field, which is vast. See [Jantzen 1987](#).

We begin by classifying the semisimple representations of a split reductive group over a field k . When k has characteristic zero, this is all of them ([22.138](#)).

CLASSIFICATION IN TERMS OF ROOTS AND WEIGHTS

THE DOMINANT WEIGHTS OF A ROOT DATUM

Let (X, R, X^\vee, R^\vee) be a root datum. We make the following definitions:

- ◇ $Q = \mathbb{Z}R$ (**root lattice**) is the \mathbb{Z} -submodule of X generated by the roots;
- ◇ $X_0 = \{x \in X \mid \langle x, \alpha^\vee \rangle = 0 \text{ for all } \alpha \in R\}$;
- ◇ $V = \mathbb{R} \otimes_{\mathbb{Z}} Q \subset \mathbb{R} \otimes_{\mathbb{Z}} X$;
- ◇ $P = \{\lambda \in V \mid \langle \lambda, \alpha^\vee \rangle \in \mathbb{Z} \text{ for all } \alpha \in R\}$ (**weight lattice**).

Now choose a base $S = \{\alpha_1, \dots, \alpha_n\}$ for R , so that:

- ◇ $R = R^+ \sqcup R^-$ where $R^+ = \{\sum m_i \alpha_i \mid m_i \geq 0\}$ and $R^- = \{\sum m_i \alpha_i \mid m_i \leq 0\}$;
- ◇ $Q = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n \subset V = \mathbb{R}\alpha_1 \oplus \dots \oplus \mathbb{R}\alpha_n$,
- ◇ $P = \mathbb{Z}\lambda_1 \oplus \dots \oplus \mathbb{Z}\lambda_n$ where λ_i is defined by $\langle \lambda_i, \alpha_j^\vee \rangle = \delta_{ij}$.

The λ_i are called the **fundamental (dominant) weights**. Define

- ◇ $P^+ = \{\lambda \in P \mid \langle \lambda, \alpha^\vee \rangle \geq 0 \text{ all } \alpha \in R^\vee\}$.

An element λ of X is **dominant** if $\langle \lambda, \alpha^\vee \rangle \geq 0$ for all $\alpha \in R^+$. Such a λ can be written uniquely

$$\lambda = \sum_{1 \leq i \leq n} m_i \lambda_i + \lambda_0 \tag{173}$$

with $m_i \in \mathbb{N}$, $\sum m_i \lambda_i \in X$, and $\lambda_0 \in X_0$.

THE DOMINANT WEIGHTS OF A SEMISIMPLE ROOT DATUM

To give a semisimple root datum amounts to giving a root system (V, R) and a lattice X ,

$$P \supset X \supset Q$$

(see [22.40](#)). Choose an inner product $(,)$ on V for which the s_α act as orthogonal transformations. Then, for $\lambda \in V$

$$\langle \lambda, \alpha^\vee \rangle = 2 \frac{(\lambda, \alpha)}{(\alpha, \alpha)}.$$

Since in this case $X_0 = 0$, the above definitions become:

- ◇ $Q = \mathbb{Z}R = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$,
- ◇ $P = \{\lambda \in V \mid 2\frac{(\lambda, \alpha)}{(\alpha, \alpha)} \in \mathbb{Z} \text{ all } \alpha \in R\} = \mathbb{Z}\lambda_1 \oplus \cdots \oplus \mathbb{Z}\lambda_n$ where λ_i is defined by

$$2\frac{(\lambda_i, \alpha)}{(\alpha, \alpha)} = \delta_{ij}.$$

- ◇ $P^+ = \{\lambda = \sum_i m_i \lambda_i \mid m_i \geq 0\} = \{\text{dominant weights}\}.$

THE CLASSIFICATION OF SIMPLE REPRESENTATIONS

Let G be a reductive group. We choose a maximal torus T and a Borel subgroup B containing T (hence, we get a root datum (X, R, X^\vee, R^\vee) and a base S for R). As every representation of G is (uniquely) a sum of simple representations, we only need to classify them.

THEOREM 24.1. *Let $r: G \rightarrow \text{GL}_W$ be a simple representation of G .*

- (a) *There exists a unique one-dimensional subspace L of W stabilized by B .*
- (b) *The L in (a) is a weight space for T , say, $L = W_{\lambda_r}$.*
- (c) *The λ_r in (b) is dominant.*
- (d) *If λ is also a weight for T in W , then $\lambda = \lambda_r - \sum m_i \alpha_i$ with $m_i \in \mathbb{N}$.*

PROOF. Omitted. □

Note that the Lie-Kolchin theorem implies that there does exist a one-dimensional eigenspace for B — the content of (a) is that when W is simple (as a representation of G), the space is unique. Since L is mapped into itself by B , it is also mapped into itself by T , and so lies in a weight space. The content of (b) is that it is the whole weight space. Because of (d), λ_r is called the **highest weight** of the simple representation r .

THEOREM 24.2. *The map $(W, r) \mapsto \lambda_r$ defines a bijection from the set of isomorphism classes of simple representations of G onto the set of dominant weights in $X = X^*(T)$.*

PROOF. Omitted. □

In the examples, k has characteristic zero (for the moment).

EXAMPLE: SL_2

Here the root datum is isomorphic to $\{\mathbb{Z}, \{\pm 2\}, \mathbb{Z}, \{\pm 1\}\}$. Hence $Q = 2\mathbb{Z}$, $P = \mathbb{Z}$, and $P^+ = \mathbb{N}$. Therefore, there is (up to isomorphism) exactly one simple representation for each $m \geq 0$. There is a natural action of $\text{SL}_2(k)$ 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 homogeneous polynomials of degree m is simple, and every simple representation is isomorphic to exactly one of these.

EXAMPLE: GL_n

As usual, let T be \mathbb{D}_n , and let B be the standard Borel subgroup. The characters of T are χ_1, \dots, χ_n . Note that GL_n has representations

$$\mathrm{GL}_n \xrightarrow{\det} \mathbb{G}_m \xrightarrow{t \mapsto t^m} \mathrm{GL}_1 = \mathbb{G}_m$$

for each m , and that any representation can be tensored with this one. Thus, given any simple representation of GL_n we can shift its weights by any integer multiple of $\chi_1 + \dots + \chi_n$. In this case, the simple roots are $\chi_1 - \chi_2, \dots, \chi_{n-1} - \chi_n$, and the root datum is isomorphic to

$$(\mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}, \mathbb{Z}^n, \{e_i - e_j \mid i \neq j\}).$$

In this notation the simple roots are $e_1 - e_2, \dots, e_{n-1} - e_n$, and the fundamental dominant weights are $\lambda_1, \dots, \lambda_{n-1}$ with

$$\lambda_i = e_1 + \dots + e_i - n^{-1}i(e_1 + \dots + e_n).$$

The dominant weights are the expressions

$$a_1\lambda_1 + \dots + a_{n-1}\lambda_{n-1} + m(e_1 + \dots + e_n), \quad a_i \in \mathbb{N}, \quad m \in \mathbb{Z}.$$

These are the expressions

$$m_1e_1 + \dots + m_n e_n$$

where the m_i are integers with $m_1 \geq \dots \geq m_n$. The simple representation with highest weight e_1 is the representation of GL_n on k^n (obviously), and the simple representation with highest weight $e_1 + \dots + e_i$ is the representation on $\bigwedge^i(k^n)$ (Springer 1998, 4.6.2).

EXAMPLE: SL_n

Let T_1 be the diagonal in SL_n . Then $X^*(T_1) = X^*(T)/\mathbb{Z}(\chi_1 + \dots + \chi_n)$ with $T = \mathbb{D}_n$. The root datum for SL_n is isomorphic to $(\mathbb{Z}^n/\mathbb{Z}(e_1 + \dots + e_n), \{\varepsilon_i - \varepsilon_j \mid i \neq j\}, \dots)$ where ε_i is the image of e_i in $\mathbb{Z}^n/\mathbb{Z}(e_1 + \dots + e_n)$. It follows from the GL_n case that the fundamental dominant weights are $\lambda_1, \dots, \lambda_{n-1}$ with

$$\lambda_i = \varepsilon_1 + \dots + \varepsilon_i.$$

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 $\varepsilon_1 + \dots + \varepsilon_i$ is the representation SL_n on $\bigwedge^i(k^n)$ (ibid.).

GROTHENDIECK GROUPS

Let T be a split torus, say $T = D(M)$. Then $\mathrm{Rep}(T)$ is a semisimple category whose simple objects are classified by the elements of M . It follows that the Grothendieck group of $\mathrm{Rep}(T)$ is the group algebra $\mathbb{Z}[M]$. Now let (G, T) be a split reductive group, and let W be the Weyl group of (G, T) . Then W acts on T , and hence on $M = X^*(T)$. There is a functor $\mathrm{Rep}(G) \rightarrow \mathrm{Rep}(T)$ that sends a representation of G to its restriction to T .

THEOREM 24.3. *The homomorphism from the Grothendieck group of $\mathrm{Rep}(G)$ to that of $\mathrm{Rep}(T)$ defined by the restriction functor is injective with image $\mathbb{Z}[M]^W$ (elements of $\mathbb{Z}[M]$ invariant under W).*

PROOF. Serre 1968, Thm 4. □

SEMISIMPLICITY

Perhaps move results on the semisimplicity of $\text{Rep}(G)$ to here.

THEOREM 24.4 (SERRE-DELIGNE). *Let G be an algebraic group over a field k of nonzero characteristic p . 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, Jean-Pierre, Sur la semi-simplicité des produits tensoriels de représentations de groupes. *Invent. Math.* 116 (1994), no. 1-3, 513–530.

Deligne, Pierre. Semi-simplicité de produits tensoriels en caractéristique p . *Invent. Math.* 197 (2014), no. 3, 587–611.

The existence theorem

This chapter will be completely rewritten, but not expanded.

Recall the statement:

Let k be a field. Every reduced root datum arises from a split reductive group (G, T) over k .

In fact, it suffices to prove the following statement:

Let k be a field. Every diagram (V, R, X) arises from a split semisimple group (G, T) over k .

There are four approaches to proving the existence theorem:

- (a) Characteristic zero: (original) classical approach.
- (b) Characteristic zero: Tannakian approach.
- (c) All characteristics: Chevalley's (original) approach.
- (d) All characteristics: explicit construction.

Of these approaches, (a) is only of historical significance (at least to algebraists), while (b) is developed in detail in my notes LAG. Thus, we shall concentrate on (c) and (d).

a. Characteristic zero: classical approach

Recall the classical statement. A diagram is reduced root system R over \mathbb{Q} and a lattice X contained between the root lattice $Q(R)$ of R and its weight lattice $P(R)$:

$$Q(R) \subset X \subset P(R).$$

Let k be an algebraically closed field. A (connected) semisimple algebraic group G over k and the choice of a maximal torus T in G define a diagram $(R(G, T), X(T))$ whose isomorphism class depends only on G .

25.1. (Existence theorem) The map $\delta: G, T \mapsto (R(G, T), X(T))$ induces a bijection between isomorphism classes of semisimple algebraic groups over k and isomorphism classes of diagrams.

Concerning the origins of this theorem in characteristic zero, I quote [Borel 1975](#), 1.5. "Over \mathbb{C} , 25.1 goes back to results of Killing, Weyl, Cartan, proved however in a different context. Briefly, it may be viewed as the conjunction of the following:

- (a) Classification of complex semisimple Lie algebras by reduced root systems.
- (b) Classification of connected complex semisimple Lie groups with a given Lie algebra \mathfrak{g} with root system R by means of lattices between $Q(R)$ and $P(R)$.
- (c) A complex connected semisimple Lie group has one and only one structure of affine algebraic group compatible with its complex analytic structure.

Statement (a) is in essence due to Killing and Cartan, although the connection with root systems emerged gradually only later. It is now standard (cf. e.g. [Serre 1966](#), [Humphreys 1972](#)).

It is more difficult to give a direct reference for (b). Results of H. Weyl and E. Cartan, as reformulated later by E. Stiefel (1942; see also [Adams 1969](#)) show that diagrams also classify compact semisimple Lie groups. One then uses the fact that the assignment,

$$\text{connected Lie group} \mapsto \text{maximal compact subgroup}, \quad (174)$$

induces a bijection between isomorphism classes of connected complex semisimple Lie groups and of connected semisimple Lie groups (see e.g., [Hochschild 1965](#)). In the course of proving this, one also sees that a complex connected semisimple Lie group always has a faithful finite dimensional representation (*ibid.* p. 200).

Finally, in view of this last fact, (c) amounts to showing that the \mathbb{C} -algebra of holomorphic functions on G whose translates span a finite dimensional space (the ‘representative functions’) is finitely generated. It is then the coordinate ring for the desired structure of algebraic group ([Hochschild and Mostow 1961](#)).”

b. Characteristic zero: Tannakian approach.

In this approach, the existence theorem for algebraic groups over a field of characteristic zero is derived from the similar theorem for Lie algebras by using Tannakian theory. Let \mathfrak{g} be a semisimple Lie algebra over a field k of characteristic zero. Then $\text{Rep}(\mathfrak{g})$ is a neutral Tannakian category, and the group attached to it is the simply connected semisimple algebraic group G with Lie algebra \mathfrak{g} . The other connected semisimple algebraic groups with Lie algebra \mathfrak{g} correspond to certain subcategories of $\text{Rep}(\mathfrak{g})$. This approach was suggested by Cartier in a *Comptes Rendus* note ([Cartier 1956](#)), and worked out in detail by the author ([Milne 2007](#)). We sketch the argument.

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

$$\alpha = (\alpha_V)_{V \in \mathcal{R}}, \quad \alpha_V \in \text{End}_{k\text{-linear}}(V),$$

such that

- ◇ $\alpha_{V \otimes W} = \alpha_V \otimes \text{id}_W + \text{id}_V \otimes \alpha_W$ for all $V, W \in \mathcal{R}$,
- ◇ $\alpha_V = 0$ if \mathfrak{g} acts trivially on V , and
- ◇ for all homomorphisms $\beta: V \rightarrow W$ of representations in \mathcal{R} ,

$$\alpha_W \circ \beta = \beta \circ \alpha_V.$$

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 $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$.

LEMMA 25.2. *If \mathcal{R} contains a faithful representation of \mathfrak{g} , then $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is injective.*

PROOF. Let (V, r) be a representation of \mathfrak{g} ; then the composite

$$\mathfrak{g} \xrightarrow{x \mapsto (r(x))} \mathfrak{g}_{\mathcal{R}} \xrightarrow{\alpha \mapsto \alpha_V} \mathfrak{gl}(V),$$

is r . Hence $\mathfrak{g} \rightarrow \mathfrak{g}_{\mathcal{R}}$ is injective if r is injective. \square

Let G be an affine group scheme over k , and let $\mathfrak{g} = \text{Lie}(G)$. A representation (V, r) of G defines a representation (V, dr) of \mathfrak{g} .

LEMMA 25.3. *Let G be an affine group scheme over k with Lie algebra \mathfrak{g} , and let \mathcal{R} be the ring of representations of \mathfrak{g} arising from a representation of G . Then $\mathfrak{g} \simeq \mathfrak{g}_{\mathcal{R}}$.*

PROOF. By definition, \mathfrak{g} is the kernel of $G(k[\varepsilon]) \rightarrow G(k)$. Therefore, to give an element of \mathfrak{g} is the same as giving a family of $k[\varepsilon]$ -linear maps

$$\text{id}_V + \alpha_V \varepsilon: V[\varepsilon] \rightarrow V[\varepsilon]$$

indexed by $V \in \mathcal{R}$ satisfying the three conditions of (11.2). The first of these conditions says that

$$\text{id}_{V \otimes W} + \alpha_{V \otimes W} \varepsilon = (\text{id}_V + \alpha_V \varepsilon) \otimes (\text{id}_W + \alpha_W \varepsilon),$$

i.e., that

$$\alpha_{V \otimes W} = \text{id}_V \otimes \alpha_W + \alpha_V \otimes \text{id}_W.$$

The second condition says that

$$\alpha_{\mathbb{1}} = 0,$$

and the third says that the α_V commute with all G -morphisms (= \mathfrak{g} -morphisms). Therefore, to give such a family is the same as giving an element $(\alpha_V)_{V \in \mathcal{R}}$ of $\mathfrak{g}_{\mathcal{R}}$. \square

Let \mathfrak{g} be a Lie algebra over k , and let $\text{Rep}(\mathfrak{g})$ be the category of all finite-dimensional representations of \mathfrak{g} . It has a tensor product, and the forgetful functor satisfies the conditions of Theorem 11.25, which provides us with an affine group scheme $G(\mathfrak{g})$ such that

$$\text{Rep}(G(\mathfrak{g})) \simeq \text{Rep}(\mathfrak{g}).$$

As $\mathcal{R} \stackrel{\text{def}}{=} \text{ob}(\text{Rep}(\mathfrak{g}))$ contains a faithful representation of \mathfrak{g} (Ado's theorem), we have (25.2, 25.3) an injective homomorphism

$$\mathfrak{g} \hookrightarrow \mathfrak{g}_{\mathcal{R}} \simeq \text{Lie}(G(\mathfrak{g})),$$

which we denote by η .

THEOREM 25.4. *Let \mathfrak{g} be a semisimple Lie algebra over a field k of characteristic zero.*

(a) *The homomorphism $\eta: \mathfrak{g} \rightarrow \text{Lie}(G(\mathfrak{g}))$ is an isomorphism.*

- (b) The affine group scheme $G(\mathfrak{g})$ is a connected semisimple algebraic group.
- (c) Let H be algebraic group, and $a: \mathfrak{g} \rightarrow \text{Lie}(H)$ a homomorphism of Lie algebras. There exists a unique homomorphism $b: G(\mathfrak{g}) \rightarrow H$ such that $a = \text{Lie}(b) \circ \eta$; hence

$$\text{Hom}(G(\mathfrak{g}), H) \simeq \text{Hom}(\mathfrak{g}, \text{Lie}(H)).$$

- (d) Let R be the root system of \mathfrak{g} and $Q(R)$ and $P(R)$ the corresponding root and weight lattices; then

$$X^*(Z(G(\mathfrak{g}))) \simeq P(R)/Q(R).$$

PROOF. (a) Because $\text{Rep}(G(\mathfrak{g}))$ is semisimple, $G(\mathfrak{g})^\circ$ is reductive (20.13). Therefore its Lie algebra $\text{Lie}(G(\mathfrak{g}))$ is reductive, and so $\text{Lie}(G(\mathfrak{g})) = \eta(\mathfrak{g}) \oplus \mathfrak{a} \oplus \mathfrak{c}$ with \mathfrak{a} semisimple and \mathfrak{c} commutative. If \mathfrak{a} or \mathfrak{c} is nonzero, then there exists a nontrivial representation r of $G(\mathfrak{g})$ such that $\text{Lie}(r)$ is trivial on \mathfrak{g} . But this is impossible because η defines an equivalence $\text{Rep}(G(\mathfrak{g})) \rightarrow \text{Rep}(\mathfrak{g})$.

(b) The group scheme $G(\mathfrak{g})$ is algebraic because its Lie algebra is finite-dimensional. To show that it is connected, we have to show that if a representation (V, ρ) of \mathfrak{g} has the property that the category of subquotients of direct sums of copies of V is stable under tensor products, then V is the trivial representations (11.49). This follows directly from the standard description of the representations of a semisimple Lie algebra. Finally, $G(\mathfrak{g})$ is semisimple because its Lie algebra is semisimple.

- (c) From a we get a tensor functor

$$\text{Rep}(H) \rightarrow \text{Rep}(\mathfrak{h}) \xrightarrow{a^\vee} \text{Rep}(\mathfrak{g}) \simeq \text{Rep}(G(\mathfrak{g})),$$

and hence a homomorphism $b: G(\mathfrak{g}) \rightarrow H$, which acts as a on the Lie algebras.

- (d) Omitted — see Milne 2007. □

For a detailed exposition of the theory of algebraic groups over fields of characteristic zero using this approach, see my notes *Lie Algebras, Algebraic Groups, and Lie Groups* (LAG).

c. All characteristics: Chevalley's approach

Again I quote Borel 1975, 1.5. "In positive characteristics, (25.1) is due to Chevalley. There are two parts to the proof.

25.5. Surjectivity of the map δ . More precisely, Chevalley associates with each diagram (Φ, Γ) a smooth group scheme G_0 over \mathbb{Z} such that $G_0 \otimes_{\mathbb{Z}} k$ is the k -group with diagram (Φ, Γ) for every k . This construction is given first in Chevalley 1955; see also Borel 1970, and, for a more general existence theorem over schemes (Demazure 1965; SGA 3, Tome III).

25.6. Injectivity of the map δ . This is proved in Chevalley 6 58; see also (Demazure 1965; SGA 3, Tome III).

See Borel 1975, §5, for a sketch of (a). Also Borel 1970.

d. All characteristics: explicit construction

Here one shows that every diagram arises from a simply connected algebraic group by exhibiting the group. This amounts to constructing the spin groups and the five exceptional groups. Note that, since we've proved the existence of simply connected covers, we know the spin groups exist.

We shall prove this by exhibiting simple algebraic group k for each simple reduced system. This will occupy the rest of the chapter.

e. Spin groups

Let ϕ be a nondegenerate bilinear form on a k -vector space V . The special orthogonal group $\text{SO}(\phi)$ is connected and almost-simple, and it has a 2-fold covering $\text{Spin}(\phi)$ which we now construct. Throughout this section, k is a field not of characteristic 2 and " k -algebra" means "associative (not necessarily commutative) k -algebra containing k in its centre". For example, the $n \times n$ matrices with entries in k become such a k -algebra $M_n(k)$ once we identify an element c of k with the scalar matrix cI_n .

QUADRATIC SPACES

Let k be a field not of characteristic 2, and let V be a finite-dimensional k -vector space. A **quadratic form** on V is a mapping

$$q: V \rightarrow k$$

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

$$q(x + y) = q(x) + q(y) + 2\phi_q(x, y), \quad (175)$$

and so ϕ_q is uniquely determined by q . A **quadratic space** is a pair (V, q) consisting of a finite-dimensional vector space and a quadratic form q . Often I'll write ϕ (rather than ϕ_q) for the associated symmetric bilinear form and denote (V, q) by (V, ϕ_q) or (V, ϕ) . A nonzero vector x in V is **isotropic** if $q(x) = 0$ and **anisotropic** if $q(x) \neq 0$. Note that q is zero (i.e., $q(V) = 0$) if and only if ϕ is zero (i.e., $\phi(V, V) = 0$). The **discriminant** of (V, q) is the determinant of the matrix $(\phi(e_i, e_j))$ where e_1, \dots, e_n is a basis of V . The choice of a different basis multiplies $\det(\phi(e_i, e_j))$ by a nonzero square, and so the discriminant is an element of $k/k^{\times 2}$. Let (V_1, q_1) and (V_2, q_2) be quadratic spaces. An **isometry** is an injective k -linear map $\sigma: V_1 \rightarrow V_2$ such that $q_2(\sigma x) = q_1(x)$ for all $x \in V$ (equivalently, $\phi(\sigma x, \sigma y) = \phi(x, y)$ for all $x, y \in V$). By $(V_1, q_1) \oplus (V_2, q_2)$ we mean the quadratic space (V, q) with

$$\begin{aligned} V &= V_1 \oplus V_2 \\ q(x_1 + x_2) &= q(x_1) + q(x_2), \quad x_1 \in V_1, \quad x_2 \in V_2. \end{aligned}$$

Let (V, q) be quadratic space. A basis e_1, \dots, e_n for V is said to be **orthogonal** if $\phi(e_i, e_j) = 0$ for all $i \neq j$.

PROPOSITION 25.7. *Every quadratic space has an orthogonal basis (and so is an orthogonal sum of quadratic spaces of dimension 1).*

PROOF. If $q(V) = 0$, then every basis is orthogonal. Otherwise, let $e \in V$ be such that $q(e) \neq 0$, and extend it to a basis e, e_2, \dots, e_n for V . Then

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

is again a basis for V , and the last $n - 1$ vectors span a subspace W for which $\phi(e, W) = 0$. Apply induction to W . \square

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

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

If every element of k is a square, for example, if k is algebraically closed, we can even scale the e_i so that each c_i is 0 or 1.

THEOREMS OF WITT AND CARTAN-DIEUDONNÉ

A quadratic space (V, q) is said to be **regular**¹ (or **nondegenerate**, ...) if for all $x \neq 0$ in V , there exists a y such that $\phi(x, y) \neq 0$. Otherwise, it is **singular**. Also, (V, q) is

- ◇ **isotropic** if it contains an isotropic vector, i.e., if $q(x) = 0$ for some $x \neq 0$,
- ◇ **totally isotropic** if every nonzero vector is isotropic, i.e., if $q(x) = 0$ for all x , and
- ◇ **anisotropic** if it is not isotropic, i.e., if $q(x) = 0$ implies $x = 0$.

Let (V, q) be a regular quadratic space. Then for any nonzero $a \in V$,

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

is a hyperplane in V (i.e., a subspace of dimension $\dim V - 1$). For an anisotropic $a \in V$, the **reflection in the hyperplane orthogonal to a** is defined to be

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

Then R_a sends a to $-a$ and fixes the elements of $W \stackrel{\text{def}}{=} \langle a \rangle^\perp$. Moreover,

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

and so R_a is an isometry. Finally, relative to a basis a, e_2, \dots, e_n with e_2, \dots, e_n a basis for W , its matrix is $\text{diag}(-1, 1, \dots, 1)$, and so $\det(R_a) = -1$.

THEOREM 25.8. *Let (V, q) be a regular quadratic space, and let σ be an isometry from a subspace W of V into V . Then there exists a composite of reflections $V \rightarrow V$ extending σ .*

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

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

¹With the notations of the last paragraph, (V, q) is regular if $c_1 \dots c_n \neq 0$.

as required. To see this, note that

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

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

$$\begin{aligned}\phi(x - y, x + y) &= 0 \\ \phi(x - y, x - y) &= 2\phi(x - y, x);\end{aligned}$$

hence

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

If $x - y$ is isotropic, then

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

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

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

We now proceed² by induction on

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

CASE W NOT TOTALLY ISOTROPIC: In this case, the argument in the proof of (25.7) shows that there exists an anisotropic vector $x \in W$, and we let $W' = \langle x \rangle^\perp \cap W$. Then, for $w \in W$, $w - \frac{\phi(w, x)}{q(x)}x \in W'$, and so $W = \langle x \rangle \oplus W'$ (orthogonal decomposition). As $m(W') = m(W) - 1$, we can apply induction to obtain a composite Σ' of reflections such that $\Sigma'|_{W'} = \sigma|_{W'}$. From the definition of W' , we see that $x \in W'^\perp$; moreover, for any $w' \in W'$,

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

and so $y \stackrel{\text{def}}{=} \Sigma'^{-1}\sigma x \in W'^\perp$. By the argument in the first paragraph, there exist reflections (one or two) of the form R_z , $z \in W'^\perp$, whose composite Σ'' maps x to y . Because Σ'' acts as the identity on W' , $\Sigma' \circ \Sigma''$ is the map sought:

$$(\Sigma' \circ \Sigma'')(cx + w') = \Sigma'(cy + w') = c\sigma x + \sigma w'.$$

CASE W TOTALLY ISOTROPIC: Let $V^\vee = \text{Hom}_{k\text{-lin}}(V, k)$ be the dual vector space, and consider the surjective map

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

(so $x \in V$ is sent to the map $y \mapsto \phi(x, y)$ on W). Let W' be a subspace of V mapped isomorphically onto W^\vee . Then $W \cap W' = \{0\}$ and we claim that $W + W'$ is a regular subspace of V . Indeed, if $x + x' \in W + W'$ with $x' \neq 0$, then there exists a $y \in W$ such that

$$0 \neq \phi(x', y) = \phi(x + x', y);$$

if $x \neq 0$, there exists a $y \in W'$ such that $\phi(x, y) \neq 0$. Endow $W \oplus W^\vee$ with the symmetric bilinear form

$$(x, f), (x', f') \mapsto f(x') + f'(x).$$

²Following Scharlau 1985, Chapter 1, 5.5.

Relative to this bilinear form, the map

$$x + x' \mapsto (x, \alpha(x')): W + W' \rightarrow W \oplus W^\vee \quad (176)$$

is an isometry. The same argument applied to σW gives a subspace W'' and an isometry

$$x + x'' \mapsto (x, \dots): \sigma W + W'' \rightarrow \sigma W \oplus (\sigma W)^\vee. \quad (177)$$

Now the map

$$W + W' \xrightarrow{(176)} W \oplus W^\vee \xrightarrow{\sigma \oplus \sigma^{\vee-1}} \sigma W \oplus (\sigma W)^\vee \xrightarrow{(177)} \sigma W + W'' \subset V$$

is an isometry extending σ . As

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

we can apply induction to complete the proof. \square

COROLLARY 25.9. *Every isometry of (V, q) is a composite of reflections.*

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

COROLLARY 25.10 (WITT CANCELLATION). *Suppose (V, q) has orthogonal decompositions*

$$(V, q) = (V_1, q_1) \oplus (V_2, q_2) = (V'_1, q'_1) \oplus (V'_2, q'_2)$$

with (V_1, q_1) and (V'_1, q'_1) regular and isometric. Then (V_2, q_2) and (V'_2, q'_2) are isometric.

PROOF. Extend an isometry $V_1 \rightarrow V'_1 \subset V$ to an isometry of V . It will map $V_2 = V_1^\perp$ isometrically onto $V'_2 = V'_1{}^\perp$. \square

COROLLARY 25.11. *All maximal totally isotropic subspaces of (V, q) have the same dimension.*

PROOF. Let W_1 and W_2 be maximal totally isotropic subspaces of V , and suppose that $\dim W_1 \leq \dim W_2$. Then there exists an injective linear map $\sigma: W_1 \rightarrow W_2 \subset V$, which is automatically an isometry. Therefore, by Theorem 25.8 it extends to an isometry $\sigma: V \rightarrow V$. Now $\sigma^{-1}W_2$ is a totally isotropic subspace of V containing W_1 . Because W_1 is maximal, $W_1 = \sigma^{-1}W_2$, and so $\dim W_1 = \dim \sigma^{-1}W_2 = \dim W_2$. \square

REMARK 25.12. In the situation of Theorem 25.8, Witt's theorem says simply that there exists an isometry extending σ to V (not necessarily a composite of reflections), and the Cartan-Dieudonné theorem says that every isometry is a composite of at most $\dim V$ reflections. When V is anisotropic, the proof of Theorem 25.8 shows this, but the general case is considerably more difficult — see Artin 1957.

DEFINITION 25.13. The **(Witt) index** of a regular quadratic space (V, q) is the maximum dimension of a totally isotropic subspace of V .

DEFINITION 25.14. A quadratic space (V, q) is a **hyperbolic plane** if it satisfies one of the following equivalent conditions:

- (a) (V, q) is regular and isotropic of dimension 2;
- (b) for some basis of V , the matrix of the form is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;

(c) V has dimension 2 and the discriminant of q is -1 (modulo squares).

THEOREM 25.15 (WITT DECOMPOSITION). *A regular quadratic space (V, q) with Witt index m has an orthogonal decomposition*

$$V = H_1 \oplus \cdots \oplus H_m \oplus V_a \quad (178)$$

with the H_i hyperbolic planes and V_a anisotropic; moreover, V_a is uniquely determined up to isometry.

PROOF. Let W be a maximal isotropic subspace of V , and let e_1, \dots, e_m be a basis for W . One easily extends the basis to a linearly independent set $e_1, \dots, e_m, e_{m+1}, \dots, e_{2m}$ such that $\phi(e_i, e_{m+j}) = \delta_{ij}$ (Kronecker delta) and $q(e_{m+i}) = 0$ for $i \leq m$. Then V decomposes as (178) with³ $H_i = \langle e_i, e_{m+i} \rangle$ and $V_a = \langle e_1, \dots, e_{2m} \rangle^\perp$. The uniqueness of V_a follows from the Witt cancellation theorem (25.10). \square

THE ORTHOGONAL GROUP

Let (V, q) be a regular quadratic space. Define $O(q)$ to be the group of isometries of (V, q) . Relative to a basis for V , $O(q)$ consists of the **automorphs** of the matrix $M = (\phi(e_i, e_j))$, i.e., the matrices T such that

$$T^t \cdot M \cdot T = M.$$

Thus, $O(q)$ is an algebraic subgroup of GL_V , called the **orthogonal group** of q (it is also called the orthogonal group of ϕ , and denoted $O(\phi)$). Let $T \in O(q)$. As $\det M \neq 0$, $\det(T)^2 = 1$, and so $\det(T) = \pm 1$. The subgroup of isometries with $\det = +1$ is an algebraic subgroup of SL_V , called the **special orthogonal group** $SO(q)$.

SUPER ALGEBRAS

A **superalgebra** (or $\mathbb{Z}/2\mathbb{Z}$ -graded algebra) over k is k -algebra C together with a decomposition $C = C_0 \oplus C_1$ of C as a k -vector space such that

$$k \subset C_0, \quad C_0 C_0 \subset C_0, \quad C_0 C_1 \subset C_1, \quad C_1 C_0 \subset C_1, \quad C_1 C_1 \subset C_0.$$

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

EXAMPLE 25.16. Let $c_1, \dots, c_n \in k$. Define $C(c_1, \dots, c_n)$ to be the k -algebra with generators e_1, \dots, e_n and relations

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

As a k -vector space, $C(c_1, \dots, c_n)$ has basis $\{e_1^{i_1} \dots e_n^{i_n} \mid i_j \in \{0, 1\}\}$, and so has dimension 2^n . When we set C_0 and C_1 equal to the subspaces

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

of $C(c_1, \dots, c_n)$, then it becomes a superalgebra.

³We often write $\langle S \rangle$ for the k -space spanned by a subset S of a vector space V .

Let $C = C_0 \oplus C_1$ and $D = D_0 \oplus D_1$ be two super k -algebras. The *super tensor product* of C and D , $C \hat{\otimes} D$, is defined to be the k -vector space $C \otimes_k D$ endowed with the superalgebra structure

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

The maps

$$\begin{aligned}i_C: C &\rightarrow C \hat{\otimes} D, & c &\mapsto c \otimes 1 \\ i_D: D &\rightarrow C \hat{\otimes} D, & d &\mapsto 1 \otimes d\end{aligned}$$

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

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

whose images anticommute in the sense that

$$f(c_i)g(d_j) = (-1)^{ij} g(d_j)f(c_i), \quad c_i \in C_i, d_j \in D_j,$$

there is a unique superalgebra homomorphism $h: C \hat{\otimes} D \rightarrow T$ such that $f = h \circ i_C$, $g = h \circ i_D$.

EXAMPLE 25.17. As a k -vector space, $C(c_1) \hat{\otimes} C(c_2)$ has basis $1 \otimes 1, e \otimes 1, 1 \otimes e, e \otimes e$, and

$$\begin{aligned}(e \otimes 1)^2 &= e^2 \otimes 1 = c_1 \cdot 1 \otimes 1 \\ (1 \otimes e)^2 &= 1 \otimes e^2 = c_2 \cdot 1 \otimes 1 \\ (e \otimes 1)(1 \otimes e) &= e \otimes e = -(1 \otimes e)(e \otimes 1).\end{aligned}$$

Therefore,

$$\begin{aligned}C(c_1) \hat{\otimes} C(c_2) &\simeq C(c_1, c_2) \\ e \otimes 1 &\leftrightarrow e_1 \\ 1 \otimes e &\leftrightarrow e_2.\end{aligned}$$

Similarly,

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

and so, by induction,

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

EXAMPLE 25.18. Every k -algebra A can be regarded as a k -superalgebra by setting $A_0 = A$ and $A_1 = 0$. If A, B are both k -algebras, then $A \otimes_k B = A \hat{\otimes}_k B$.

EXAMPLE 25.19. Let X be a manifold. Then $H(X) \stackrel{\text{def}}{=} \bigoplus_i H^i(X, \mathbb{R})$ becomes an \mathbb{R} -algebra under cup-product, and even a superalgebra with $H(X)_0 = \bigoplus_i H^{2i}(X, \mathbb{R})$ and $H(X)_1 = \bigoplus_i H^{2i+1}(X, \mathbb{R})$. If Y is a second manifold, the Künneth formula says that

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

(super tensor product).

BRIEF REVIEW OF THE TENSOR ALGEBRA

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

$$\begin{aligned} V^{\otimes 0} &= k, \\ V^{\otimes 1} &= V, \\ V^{\otimes n} &= V \otimes \cdots \otimes V \text{ (} n \text{ copies of } V \text{)} \end{aligned}$$

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

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

It is a k -algebra. If V has a basis e_1, \dots, e_m , then $T(V)$ is the k -algebra of noncommuting polynomials in e_1, \dots, e_m . There is a k -linear map $V \rightarrow T(V)$, namely, $V = V^{\otimes 1} \hookrightarrow \bigoplus_{n \geq 0} V^{\otimes n}$, and any other k -linear map from V to a k -algebra R extends uniquely to a k -algebra homomorphism $T(V) \rightarrow R$.

THE CLIFFORD ALGEBRA

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

DEFINITION 25.20. The **Clifford algebra** $C(V, q)$ is the quotient of the tensor algebra $T(V)$ of V by the two-sided ideal $I(q)$ generated by the elements $x \otimes x - q(x)$ ($x \in V$).

Let $\rho: V \rightarrow C(V, q)$ be the composite of the canonical map $V \rightarrow T(V)$ and the quotient map $T(V) \rightarrow C(V, q)$. Then ρ is k -linear, and⁴

$$\rho(x)^2 = q(x), \text{ all } x \in V. \quad (179)$$

Note that if x is anisotropic in V , then $\rho(x)$ is invertible in $C(V, q)$, because (179) shows that

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

EXAMPLE 25.21. If V is one-dimensional with basis e and $q(e) = c$, then $T(V)$ is a polynomial algebra in one symbol e , $T(V) = k[e]$, and $I(q) = (e^2 - c)$. Therefore, $C(V, q) \approx C(c)$.

EXAMPLE 25.22. If $q = 0$, then $C(V, q)$ is the exterior algebra on V , i.e., $C(V, q)$ is the quotient of $T(V)$ by the ideal generated by all squares x^2 , $x \in V$. In $C(V, q)$,

$$0 = (\rho(x) + \rho(y))^2 = \rho(x)^2 + \rho(x)\rho(y) + \rho(y)\rho(x) + \rho(y)^2 = \rho(x)\rho(y) + \rho(y)\rho(x)$$

and so $\rho(x)\rho(y) = -\rho(y)\rho(x)$.

⁴For a k -algebra R , we are regarding k as a subfield of R . When one regards a k -algebra R as a ring with a $k \rightarrow R$, it is necessary to write (179) as

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

PROPOSITION 25.23. Let r be a k -linear map from V to a k -algebra D such that $r(x)^2 = q(x)$. Then there exists a unique homomorphism of k -algebras $\bar{r}: C(V, q) \rightarrow D$ such that $\bar{r} \circ \rho = r$:

$$\begin{array}{ccc} V & \xrightarrow{\rho} & C(V, q) \\ & \searrow r & \downarrow \bar{r} \\ & & D. \end{array}$$

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

$$r'(x_1 \otimes \cdots \otimes x_n) = r(x_1) \cdots r(x_n).$$

As

$$r'(x \otimes x - q(x)) = r(x)^2 - q(x) = 0,$$

r' factors uniquely through $C(V, q)$. □

As usual, $(C(V, q), \rho)$ is uniquely determined up to a unique isomorphism by the universal property in the proposition.

THE MAP $C(c_1, \dots, c_n) \rightarrow C(V, q)$

Because ρ is linear,

$$\rho(x + y)^2 = (\rho(x) + \rho(y))^2 = \rho(x)^2 + \rho(x)\rho(y) + \rho(y)\rho(x) + \rho(y)^2.$$

On comparing this with

$$\rho(x + y)^2 \stackrel{(179)}{=} q(x + y) = q(x) + q(y) + 2\phi(x, y),$$

we find that

$$\rho(x)\rho(y) + \rho(y)\rho(x) = 2\phi(x, y). \quad (180)$$

In particular, if f_1, \dots, f_n is an orthogonal basis for V , then

$$\rho(f_i)^2 = q(f_i), \quad \rho(f_j)\rho(f_i) = -\rho(f_i)\rho(f_j) \quad (i \neq j).$$

Let $c_i = q(f_i)$. Then there exists a surjective homomorphism

$$e_i \mapsto \rho(f_i): C(c_1, \dots, c_n) \rightarrow C(V, \phi). \quad (181)$$

THE GRADATION (SUPERSTRUCTURE) ON THE CLIFFORD ALGEBRA

Decompose

$$\begin{aligned} T(V) &= T(V)_0 \oplus T(V)_1 \\ T(V)_0 &= \bigoplus_{m \text{ even}} V^{\otimes m} \\ T(V)_1 &= \bigoplus_{m \text{ odd}} V^{\otimes m}. \end{aligned}$$

As $I(q)$ is generated by elements of $T(V)_0$,

$$I(q) = (I(q) \cap T(V)_0) \oplus (I(q) \cap T(V)_1),$$

and so

$$C(V, q) = C_0 \oplus C_1 \quad \text{with} \quad C_i = T(V)_i / I(q) \cap T(V)_i.$$

Clearly this decomposition makes $C(V, q)$ into a super algebra. In more down-to-earth terms, C_0 is spanned by products of an even number of vectors from V , and C_1 is spanned by products of an odd number of vectors.

THE BEHAVIOUR OF THE CLIFFORD ALGEBRA WITH RESPECT TO DIRECT SUMS

Suppose

$$(V, q) = (V_1, q_1) \oplus (V_2, q_2).$$

Then the k -linear map

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

has the property that

$$\begin{aligned} r(x)^2 &= (\rho_1(x_1) \otimes 1 + 1 \otimes \rho_2(x_2))^2 \\ &= (q(x_1) + q(x_2))(1 \otimes 1) \\ &= q(x), \end{aligned}$$

because

$$(\rho_1(x_1) \otimes 1)(1 \otimes \rho_2(x_2)) = \rho_1(x_1) \otimes \rho_2(x_2) = -(1 \otimes \rho_2(x_2))(\rho_1(x_1) \otimes 1).$$

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

$$C(V, q) \rightarrow C(V_1, q_1) \hat{\otimes} C(V_2, q_2). \quad (182)$$

EXPLICIT DESCRIPTION OF THE CLIFFORD ALGEBRA

THEOREM 25.24. *Let (V, q) a quadratic space of dimension n .*

(a) *For every orthogonal basis for (V, q) , the homomorphism (181)*

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

is an isomorphism.

(b) *For every orthogonal decomposition $(V, q) = (V_1, q_1) \oplus (V_2, q_2)$, the homomorphism (182)*

$$C(V, q) \rightarrow C(V_1, q_1) \hat{\otimes} C(V_2, q_2)$$

is an isomorphism.

(c) *The dimension of $C(V, q)$ as a k -vector space is 2^n .*

PROOF. If $n = 1$, all three statements are clear from (25.21). 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 (182) 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 (181). 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 (181) and (182) are isomorphisms. \square

COROLLARY 25.25. *The map $\rho: V \rightarrow C(V, q)$ is injective.*

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

REMARK 25.26. Let L be a field containing k . Then ϕ extends uniquely to an L -bilinear form

$$\phi': V' \times V' \rightarrow L, \quad V' = L \otimes_k V,$$

and

$$C(V', q') \simeq L \otimes_k C(V, q)$$

where q' is quadratic form defined by ϕ' .

THE CENTRE OF THE CLIFFORD ALGEBRA

Assume that (V, q) is regular, and that $n = \dim V > 0$. Let e_1, \dots, e_n be an orthogonal basis for (V, q) , and let $q(e_i) = c_i$. Let

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

We saw in (25.24) that

$$C(c_1, \dots, c_n) \simeq C(V, q).$$

Note that, in $C(c_1, \dots, c_n)$, $(e_1 \cdots e_n)^2 = \Delta$. Moreover,

$$\begin{aligned} e_i \cdot (e_1 \cdots e_n) &= (-1)^{i-1} c_i (e_1 \cdots e_{i-1} e_{i+1} \cdots e_n) \\ (e_1 \cdots e_n) \cdot e_i &= (-1)^{n-i} c_i (e_1 \cdots e_{i-1} e_{i+1} \cdots e_n). \end{aligned}$$

Therefore, $e_1 \cdots e_n$ lies in the centre of $C(V, q)$ if and only if n is odd.

PROPOSITION 25.27. (a) *If n is even, the centre of $C(V, q)$ is k ; if n is odd, it is of degree 2 over k , generated by $e_1 \cdots e_n$. In particular, $C_0 \cap \text{Centre}(C(V, q)) = k$.*

(b) *No nonzero element of C_1 centralizes C_0 .*

PROOF. First show that a linear combination of reduced monomials is in the centre (or centralizes C_0) if and only if each monomial does, and then find the monomials that centralize the e_i (or the $e_i e_j$). \square

In Scharlau 1985, Chapter 9, 2.10, there is the following description of the complete structure of $C(V, q)$:

If n is even, $C(V, q)$ is a central simple algebra over k , isomorphic to a tensor product of quaternion algebras. If n is odd, the centre of $C(V, q)$ is generated over k by the element $e_1 \cdots e_n$ whose square is Δ , and, if Δ is not a square in k , then $C(V, q)$ is a central simple algebra over the field $k[\sqrt{\Delta}]$.

THE INVOLUTION $*$

An **involution** of a k -algebra D is a k -linear map $*$: $D \rightarrow D$ such that $(ab)^* = b^*a^*$ and $a^{**} = 1$. For example, $M \mapsto M^t$ (transpose) is an involution of $M_n(k)$.

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

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

The map $\rho: V \rightarrow C(V, q)^{\text{opp}}$ is k -linear and has the property that $\rho(x)^2 = q(x)$. Thus, there exists an isomorphism $*$: $C(V, q) \rightarrow C(V, q)^{\text{opp}}$ inducing the identity map on V , and which therefore has the property that

$$(x_1 \cdots x_r)^* = x_r \cdots x_1$$

for $x_1, \dots, x_r \in V$. We regard $*$ as an involution of A . Note that, for $x \in V$, $x^*x = q(x)$.

THE SPIN GROUP

Initially we define the spin group as an abstract group.

DEFINITION 25.28. The group $\text{Spin}(q)$ consists of the elements t of $C_0(V, q)$ such that

- (a) $t^*t = 1$,
- (b) $tVt^{-1} = V$,
- (c) the map $x \mapsto txt^{-1}: V \rightarrow V$ has determinant 1.

REMARK 25.29. (a) The condition (a) implies that t is invertible in $C_0(V, q)$, and so (b) makes sense.

(b) We shall see in (25.33) below that the condition (c) is implied by (a) and (b).

THE MAP $\text{Spin}(q) \rightarrow \text{SO}(q)$

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

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

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

THEOREM 25.30. *The homomorphism*

$$\text{Spin}(q) \rightarrow \text{SO}(q)$$

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

PROOF. The kernel consists of those $t \in \text{Spin}(q)$ such that $txt^{-1} = x$ for all $x \in V$. As V generates $C(V, q)$, such a t must lie in the centre of $C(V, q)$. Since it is also in C_0 , it must lie in k . Now the condition $t^*t = 1$ implies that $t = \pm 1$.

For an anisotropic $a \in V$, let R_a be the reflection in the hyperplane orthogonal to a . According to Theorem 25.8, each element σ of $\text{SO}(q)$ can be expressed $\sigma = R_{a_1} \cdots R_{a_m}$ for some a_i . As $\det(R_{a_1} \cdots R_{a_m}) = (-1)^m$, we see that m is even, and so $\text{SO}(q)$ is generated by elements $R_a R_b$ with a, b anisotropic elements of V . If k is algebraically closed, we can even scale a and b so that $q(a) = 1 = q(b)$.

Now

$$\begin{aligned} axa^{-1} &= (-xa + 2\phi(a, x))a^{-1} && \text{as } (ax + xa = 2\phi(a, x), \text{ see (180)}) \\ &= -\left(x - \frac{2\phi(a, x)}{q(a)}a\right) && \text{as } a^2 = q(a) \\ &= -R_a(x). \end{aligned}$$

Moreover,

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

Therefore, if $q(a)q(b) = 1$, then $R_a R_b$ is in the image of $\text{Spin}(q) \rightarrow \text{SO}(q)$. As we noted above, such elements generate $\text{SO}(q)$ when k is algebraically closed. \square

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

THE CLIFFORD GROUP

Write γ for the automorphism of $C(V, q)$ that acts as 1 on $C_0(V, q)$ and as -1 on $C_1(V, q)$.

DEFINITION 25.31. The **Clifford group** is

$$\Gamma(q) = \{t \in C(V, q) \mid t \text{ invertible and } \gamma(t)Vt^{-1} = V\}.$$

For $t \in \Gamma(q)$, let $\alpha(t)$ denote the homomorphism $x \mapsto \gamma(t)xt^{-1}: V \rightarrow V$.

PROPOSITION 25.32. For all $t \in \Gamma(q)$, $\alpha(t)$ is an isometry of V , and the sequence

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

is exact (no condition on k).

PROOF. Let $t \in \Gamma(q)$. On applying γ and $*$ to $\gamma(t)V = Vt$, we find that $\gamma(t^*)V = Vt^*$, and so $t^* \in \Gamma(q)$. Now, because $*$ and γ act as 1 and -1 on V ,

$$\gamma(t) \cdot x \cdot t^{-1} = -\gamma(\gamma(t) \cdot x \cdot t^{-1})^* = -\gamma(t^{*-1}x\gamma(t^*)) = \gamma(t^{*-1})xt^*,$$

and so

$$\gamma(t^*)\gamma(t)x = xt^*t. \quad (183)$$

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

$$q(\alpha(t)(x)) = (\alpha(t)(x))^* \cdot (\alpha(t)(x)) = t^{*-1}x\gamma(t)^* \cdot \gamma(t)xt^{-1} \stackrel{(183)}{=} t^{*-1}xxt^*tt^{-1} = q(x).$$

As k is in the centre of $\Gamma(q)$, k^\times is in the kernel of α . Conversely, let $t = t_0 + t_1$ be an invertible element of $C(V, q)$ such that $\gamma(t)xt^{-1} = x$ for all $x \in V$, i.e., such that

$$t_0x = xt_0, \quad t_1x = -xt_1$$

for all $x \in V$. As V generates $C(V, q)$ these equations imply that t_0 lies in the centre of $C(V, q)$, and hence in k (25.27a), and that t_1 centralizes C_0 , and hence is zero (25.27b). We have shown that

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

It remains to show that α is surjective. For $t \in V$, $\alpha(t)(y) = -tyt^{-1}$ and so (see the proof of (25.30)), $\alpha(t) = R_t$. Therefore the surjectivity follows from Theorem 25.8. \square

COROLLARY 25.33. For an invertible element t of $C_0(V, q)$ such that $tVt^{-1} = V$, the determinant of $x \mapsto txt^{-1}: V \rightarrow V$ is one.

PROOF. According to the proposition, every element $t \in \Gamma(q)$ can be expressed in the form

$$t = ca_1 \cdots a_m$$

with $c \in k^\times$ and the a_i anisotropic elements of V . Such an element acts as $R_{a_1} \cdots R_{a_m}$ on V , and has determinant $(-1)^m$. If $t \in C_0(V, q)$, then m is even, and so $\det(t) = 1$. \square

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

ACTION OF $O(q)$ ON $\text{Spin}(q)$

25.34. An element σ of $O(q)$ defines an automorphism of $C(V, q)$ as follows. Consider $\rho \circ \sigma: V \rightarrow C(V, q)$. Then $(\rho(\sigma(x)))^2 = \phi(\sigma(x)) \cdot 1 = \phi(x) \cdot 1$ for every $x \in V$. Hence, by the universal property, there is a unique homomorphism $\tilde{\sigma}: C(V, q) \rightarrow C(V, q)$ rendering

$$\begin{array}{ccc} V & \xrightarrow{\rho} & C(V, q) \\ \downarrow \sigma & & \downarrow \tilde{\sigma} \\ V & \xrightarrow{\rho} & C(V, q) \end{array}$$

commutative. Clearly $\widetilde{\sigma_1 \circ \sigma_2} = \tilde{\sigma}_1 \circ \tilde{\sigma}_2$ and $\widetilde{\text{id}} = \text{id}$, and so $\widetilde{\sigma^{-1}} = \tilde{\sigma}^{-1}$, and so $\tilde{\sigma}$ is an automorphism. If $\sigma \in SO(\phi)$, it is known that $\tilde{\sigma}$ is an inner automorphism of $C(V, q)$ by an invertible element of $C^+(V, q)$.

RESTATEMENT IN TERMS OF ALGEBRAIC GROUPS

Let (V, q) be quadratic space over k , and let q_K be the unique extension of q to a quadratic form on $K \otimes_k V$. As we noted in (25.26), $C(V, q_K) = K \otimes_k C(V, q)$.

THEOREM 25.35. There exists a naturally defined algebraic group $\underline{\text{Spin}}(q)$ over k such that

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

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

$$\underline{\text{Spin}}(q) \rightarrow \text{SO}(q)$$

giving the homomorphism in (25.30) for each field K containing k . Finally, the action of $O(q)$ on $C(V, q)$ described in (25.30) defines an action of $O(q)$ on $\underline{\text{Spin}}(q)$.

PROOF. Show that, when k is infinite, the algebraic group attached to the subgroup $\text{Spin}(q)$ of $\text{GL}(V)$ has these properties. Alternatively, define a functor $R \rightsquigarrow \text{Spin}(q_R)$ that coincides with the previous functor when R is a field. \square

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

ASIDE 25.36. A representation of a semisimple algebraic group G gives rise to a representation of its Lie algebra \mathfrak{g} , and all representations of \mathfrak{g} arise from G only if G has the greatest possible centre. “When E. Cartan classified the simple representations of all simple Lie algebras, he discovered a new representation of the orthogonal Lie algebra [not arising from the orthogonal group]. But he did not give a specific name to it, and much later, he called the elements on which this new representation operates *spinors*, generalizing the terminology adopted by physicists in a special case for the rotation group of the three dimensional space” (C. Chevalley, *The Construction and Study of Certain Important Algebras*, 1955, III 6). This explains the origin and name of the Spin group.

f. Groups of types A, B, C, D

List a split almost-simple group of each type.

g. Groups of type E_6

See Springer...

h. Groups of type E_7

Wilson, Robert A. A quaternionic construction of E_7 . Proc. Amer. Math. Soc. 142 (2014), no. 3, 867–880. In this paper the author gives a construction of the Lie group of type E_7 by 28×28 -matrices over the quaternions. This then leads to a simply-connected split real form, acting on a 56-dimensional vector space and then to the finite quasi-simple groups of type E_7 . This approach simplifies those given by M. G. Aschbacher, R. B. Brown, and B. N. Cooperstein

i. Groups of type E_8

j. Groups of type F_4

k. Groups of type G_2

Nonsplit algebraic groups: a survey.

This chapter will contain a careful statement of the classification results of Satake-Selbach-Tits, but no proofs.

Relative root systems and the anisotropic kernel; classification of (nonsplit) reductive groups (Satake-Selbach-Tits). Everything from Springer Corvallis.

a. General classification (Satake-Tits)

Statements only.

In this chapter, we study algebraic groups, especially nonsplit reductive groups, over arbitrary fields.

Root data are also important in the nonsplit case. For a reductive group G , one chooses a torus that is maximal among those that are split, and defines the root datum much as before — in this case it is not necessarily reduced. This is an important approach to describing arbitrary algebraic groups, but clearly it yields no information about anisotropic groups (those with no split torus). We explain this approach this chapter following [Satake 1963, 1971, 2001](#); [Selbach 1976](#); [Tits 1966, 1971](#).

b. Relative root systems and the anisotropic kernel.

The aim of this section is to explain the Satake-Tits strategy for classifying nonsplit groups and their representations. Here is a brief overview.

The isomorphism classes of split semisimple algebraic groups are classified over any field. Given a semisimple algebraic group G over a field k , one knows that G splits over the separable algebraic closure K of k , and so the problem is to determine the isomorphism classes of semisimple algebraic groups over k corresponding to a given isomorphism class over K . Tits (1966) sketches a program for doing this. Let T_0 be a maximal split subtorus of G , and let T be a maximal torus containing T_0 . The derived group of the centralizer of T_0 is called the *anisotropic kernel* of G — it is a semisimple algebraic group over k whose split subtori are trivial. Let S be a simple set of roots for (G_K, T_K) , and let S_0 be the subset vanishing on T_0 . The Galois group of K/k acts on S , and the triple consisting of S , S_0 , and this action is called the *index* of G . Tits sketches a proof (corrected in the MR review of the article) that the isomorphism class of G is determined by the isomorphism class of G_K , its anisotropic kernel, and its index. It remains therefore to determine for each isomorphism class of semisimple algebraic groups over k (a) the possible indices, and (b) for each possible

index, the possible anisotropic kernels. Tits (ibid.) announces some partial results on (a) and (b).

Problem (b) is related to the problem of determining the central division algebras over a field, and so it is only plausible to expect a solution to it for fields k for which the Brauer group is known.

Tits's work was continued by his student Selbach. To quote the MR review of [Selbach 1976](#) (slightly edited):

This booklet treats the classification of quasisimple algebraic groups over arbitrary fields along the lines of [Tits 1966](#). Tits had shown that each such group is described by three data: the index, the anisotropic kernel and the connectedness type. For his general results Tits had given or sketched proofs, but not for the enumeration of possible indices, whereas the classification of possible anisotropic kernels was not dealt with at all. The booklet under review starts with an exposition with complete proofs of the necessary general theory. Some proofs are simplified using results on representation theory over arbitrary fields from another paper by Tits ([Crelle 1971](#)), and a different proof is given for the main result, viz., that a simply connected group is determined by its index and anisotropic kernel, because Tits's original proof contained a mistake, as was indicated in the review of that paper. Then it presents the detailed classifications with proofs of all possible indices, and of the anisotropic kernels of exceptional type. Questions of existence over special fields (finite, reals, p -adic, number) are dealt with only in cases which fit easily in the context ([Veldkamp](#)).

It is interesting to note that, while Tits's article has been cited 123 times, Selbach's has been cited only twice ([MR April 2010](#)) — for example, it is not cited in [Conrad and Prasad 2015](#) — despite being reviewed in the main reviewing journals and being available in many libraries.¹

Here is the MR review of [Tits 1971](#) (my translation).

The author proposes to study the linear irreducible k -representations of a reductive algebraic group G over k , where k is any field. When k is algebraically closed, Chevalley showed that the irreducible representations of G are characterized, as in the classical case, by the weights of G (characters of a maximal torus of G), every weight “dominant relative to a Borel subgroup” being the dominant weight of an irreducible representation. The author first shows that this correspondence continues when G is split over k . In the general case, it is necessary to start with a maximal k -torus T in G and a Borel subgroup B of G containing T in order to define the weights (forming a group Λ) and the set Λ_+ of dominant weights with respect to B ; let Λ_0 denote the subgroup of Λ generated by the roots and by the weights zero on the intersection $T \cap D(G)$; the quotient $C^* = \Lambda/\Lambda_0$ is the dual of the centre of G . The Galois group Γ of the separable closure k^{sep} of k over k acts canonically on Λ , Λ_0 , and Λ_+ ; the central result attaches to each dominant weight $\lambda \in \Lambda_+$ invariant under Γ an absolutely irreducible representation of G in a linear group $\text{GL}(m, D)$, well determined up to equivalence, D being a skew field with centre k , well determined up to isomorphism; moreover, if $\lambda \in \Lambda_0$ or if G is quasi-split (in which case the Borel group B is defined over k), then $D = k$. One attaches in this way to any weight λ of Λ_+ invariant by Γ an element $[D] = \alpha_{G,k}(\lambda)$ of the Brauer group $\text{Br}(k)$, and one shows that $\alpha_{G,k}$ extends to a homomorphism of the group

¹Including those of the University of Michigan and Stanford University.

Λ^Γ of weights invariant under Γ into $\text{Br}(k)$; moreover, the kernel of $\alpha_{G,k}$ contains Λ_0 , and so there is a fundamental homomorphism $\beta_{G,k}: C^{*\Gamma} \rightarrow \text{Br}(k)$ (where $C^{*\Gamma}$ is the subgroup of C^* formed of the elements invariant under Γ). The author shows that this homomorphism can be defined cohomologically, in relation with the “Brauer-Witt invariant” of the group G . A good part of the memoir is concerned with the study of the homomorphism β , notably the relations between $\beta_{G,k}$ and $\beta_{G_1,k}$, where G_1 is a reductive subgroup of G , as well as with majorizing the degree of $\beta(c)$ in $\text{Br}(k)$ when G is an almost-simple group and c is the class of the minuscule dominant weight. He examines also a certain number of examples, notably the groups of type E_6 and E_7 . Finally, he shows how starting from a knowledge of α , one obtains all the irreducible k -representations of G : start with a dominant weight $\lambda \in \Lambda_+$, and denote by k_λ the field of invariants of the stabilizer of λ in Γ ; then if $\alpha_{G,k_\lambda}(\lambda) = [D_\lambda]$, one obtains a k_λ -representation $G \rightarrow \text{GL}(m, D_\lambda)$, whence one deduces canonically a k -representation ${}^k\rho_\lambda$, which is irreducible; every irreducible k -representation is equivalent to a ${}^k\rho_\lambda$, and ${}^k\rho_\lambda$ and ${}^k\rho_{\lambda'}$ are k -equivalent if and only if λ and λ' are transformed into one another by an element of Γ (Dieudonné).

Cohomology: a survey

This chapter will be revised and slightly expanded to about 30 pages. Complete references will be added.

This chapter contains precise statements and references, but only sketches of proofs on the following topics: classification of the forms of an algebraic group; description of the classical algebraic groups in terms of algebras with involution; the Galois cohomology of algebraic groups.

We shall make frequent use of the following remark. Let X and Y be sets, and let \sim be an equivalence relation on Y . If there is given a surjection $Y \rightarrow X$ whose fibres are the equivalence classes, then we say that X classifies the elements of Y modulo \sim or that it classifies the \sim -classes of elements of Y . If (Y, \sim) and (Y', \sim') are both classified by X , then a map $(Y, \sim) \rightarrow (Y', \sim')$ compatible with the surjections $Y \rightarrow X$ and $Y' \rightarrow X$ induces a bijection from the set of equivalence classes in Y to the set of equivalence classes in Y' .

a. Definition of nonabelian cohomology; examples

We begin by reviewing the basic definitions and properties of the nonabelian cohomology sets (following [Serre 1964](#), I, §5). Let Γ be a group. A Γ -*set* is a set A with an action

$$(\sigma, a) \mapsto \sigma a: \Gamma \times A \rightarrow A$$

of Γ on A (so $(\sigma\tau)a = \sigma(\tau a)$ and $1a = a$). If, in addition, A has the structure of a group and the action of Γ respects this structure (i.e., $\sigma(aa') = \sigma a \cdot \sigma a'$), then we call A a Γ -**group**.

DEFINITION OF $H^0(\Gamma, A)$

Let A be a Γ -set A . Then $H^0(\Gamma, A)$ is defined to be the set A^Γ of elements left fixed by the operation of Γ on A , i.e.,

$$H^0(\Gamma, A) = A^\Gamma = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in \Gamma\}.$$

If A is a Γ -group, then $H^0(\Gamma, A)$ is a group.

DEFINITION OF $H^1(\Gamma, A)$

Let A be a Γ -group. A map $\sigma \mapsto a_\sigma$ of Γ into A is said to be a 1-**cocycle** of Γ in A if $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ for all $\sigma, \tau \in \Gamma$. Two 1-cocycles (a_σ) and (b_σ) are said to be **equivalent** if

there exists a $c \in A$ such that

$$b_\sigma = c^{-1} \cdot a_\sigma \cdot \sigma c \quad \text{for all } \sigma \in \Gamma.$$

This is an equivalence relation on the set of 1-cocycles of Γ in A , and $H^1(\Gamma, A)$ is defined to be the set of equivalence classes of 1-cocycles.

In general $H^1(\Gamma, A)$ is not a group unless A is commutative, but it has a distinguished element, namely, the class of 1-cocycles of the form $\sigma \mapsto b^{-1} \cdot \sigma b$, $b \in A$ (the **principal 1-cocycles**).

When A is commutative, $H^i(\Gamma, A)$ coincides with the usual cohomology groups for $i = 0, 1$.

COMPATIBLE HOMOMORPHISMS

Let Δ be a second group. Let A be Γ -group and B an Δ -group. Two homomorphisms $f: A \rightarrow B$ and $g: \Delta \rightarrow \Gamma$ are said to be **compatible** if

$$f(g(\sigma)a) = \sigma(f(a)) \quad \text{for all } \sigma \in \Delta, a \in A.$$

If (a_σ) is a 1-cocycle for A , then

$$b_\sigma = f(a_{g(\sigma)})$$

is a 1-cocycle of Δ in B , and this defines a mapping $H^1(\Gamma, A) \rightarrow H^1(\Delta, B)$, which is a homomorphism if A and B are commutative.

When $\Delta = \Gamma$, a homomorphism $f: A \rightarrow B$ compatible with the identity map on Γ , i.e., such that

$$f(\sigma a) = \sigma(f(a)) \quad \text{for all } \sigma \in \Gamma, a \in A,$$

f is said to be a Γ -**homomorphism** (or be Γ -**equivariant**).

EXACT SEQUENCES

PROPOSITION 27.1. *An exact sequence*

$$1 \rightarrow A \xrightarrow{u} B \xrightarrow{v} C \rightarrow 1 \tag{184}$$

of Γ -groups gives rise to an exact sequence of pointed sets

$$1 \rightarrow H^0(\Gamma, A) \xrightarrow{u^0} H^0(\Gamma, B) \xrightarrow{v^0} H^0(\Gamma, C) \xrightarrow{\delta} H^1(\Gamma, A) \xrightarrow{u^1} H^1(\Gamma, B) \xrightarrow{v^1} H^1(\Gamma, C).$$

More precisely:

- (a) The sequence $1 \rightarrow H^0(\Gamma, A) \xrightarrow{u^0} H^0(\Gamma, B) \xrightarrow{v^0} H^0(\Gamma, C)$ is exact as a sequence of groups.
- (b) There is a natural right action of C^Γ on $H^1(\Gamma, A)$ and
 - i) the map δ sends $c \in C^\Gamma$ to $1 \cdot c$, where 1 is the distinguished element of $H^1(\Gamma, A)$;
 - ii) the nonempty fibres of $u^1: H^1(\Gamma, A) \rightarrow H^1(\Gamma, B)$ are the orbits of C^Γ in $H^1(\Gamma, A)$;
 - iii) the kernel of v^1 is the quotient of $H^1(\Gamma, A)$ by the action of C^Γ .

We now define δ and the action of C^Γ on $H^1(\Gamma, A)$. Let $c \in C^\Gamma$, and choose a $b \in B$ mapping to it. Then $\sigma b = b \cdot a_\sigma$ for some $a_\sigma \in A$, and the family (a_σ) is a 1-cocycle whose class in $H^1(\Gamma, A)$ is $\delta(c)$. Let α be a class in $H^1(\Gamma, A)$ represented by a 1-cocycle (a'_σ) ; then $\sigma \mapsto b^{-1} a'_\sigma b a_\sigma = b^{-1} \cdot a'_\sigma \cdot \sigma b$ is a 1-cocycle, whose class in $H^1(\Gamma, A)$ is $\alpha \cdot c$.

PROPOSITION 27.2. *When A is contained in the centre of B , the above sequence extends to an exact sequence*

$$\dots \rightarrow H^1(\Gamma, B) \xrightarrow{v^1} H^1(\Gamma, C) \xrightarrow{\delta} H^2(\Gamma, A).$$

Let $c = (c_\sigma)$ be a 1-cocycle of C , and choose a $b_\sigma \in B$ mapping to c_σ for each σ . Then $b_\sigma \cdot \sigma b_\tau = b_{\sigma\tau} \cdot a_{\sigma,\tau}$ for some $a_{\sigma,\tau} \in A$, and $a = (a_{\sigma,\tau})$ is a 2-cocycle whose class in $H^2(\Gamma, A)$ is $\delta(c)$.

EXAMPLE 27.3. Let $B = A \rtimes C$. The composite $C \rightarrow B \rightarrow B/A \simeq C$ is the identity map. Therefore, the maps $H^0(\Gamma, B) \rightarrow H^0(\Gamma, C)$ and $H^1(\Gamma, B) \rightarrow H^1(\Gamma, C)$ are surjective, and $H^1(\Gamma, A) \rightarrow H^1(\Gamma, B)$ is injective with image the kernel of $H^1(\Gamma, B) \rightarrow H^1(\Gamma, C)$.

TWISTS

Proposition describes only the fibre of v^1 containing the neutral element. To describe the other fibres we need to twist. Let A be a G -group, and let S be a G -set with a left action of A compatible with the action of G . Let $a = (a_\sigma) \in Z^1(G, A)$, and let ${}_a S$ denote the set S on which G acts by

$$\sigma * s = a_\sigma \cdot \sigma s.$$

We say that ${}_a S$ is obtained from S by *twisting* by the 1-cocycle a .

Now consider an exact sequence (184), and let $b \in Z^1(\Gamma, B)$. The group B acts on itself by inner automorphisms leaving A stable, and so we can twist (184) by b to obtain an exact sequence

$$1 \rightarrow {}_b A \rightarrow {}_b B \rightarrow {}_b C \rightarrow 1.$$

The next proposition describes the fibre of v^1 containing the class of b .

PROPOSITION 27.4. *There is a commutative diagram*

$$\begin{array}{ccccccc} H^0(\Gamma, {}_b C) & \longrightarrow & H^1(\Gamma, {}_b A) & \longrightarrow & H^1(\Gamma, {}_b B) & \longrightarrow & H^1(\Gamma, {}_b C) \\ & & & & \downarrow \simeq & & \downarrow \simeq \\ H^0(\Gamma, C) & \longrightarrow & H^1(\Gamma, A) & \xrightarrow{u^1} & H^1(\Gamma, B) & \xrightarrow{v^1} & H^1(\Gamma, C) \end{array}$$

in which the vertical arrows map the distinguished elements in $H^1(\Gamma, {}_b B)$ and $H^1(\Gamma, {}_b C)$ to the classes of b and $v^1(b)$.

In more detail, the underlying group of ${}_b B$ is just B , but Γ acts by the formula

$$\sigma * b = b_\sigma \cdot \sigma b \cdot b_\sigma^{-1}.$$

For any $(b'_\sigma) \in Z^1(\Gamma, {}_b B)$, the map $\sigma \mapsto b'_\sigma \cdot b_\sigma$ is a 1-cocycle for B , and the first vertical map sends the class of (b'_σ) to its class. The second vertical map has a similar description.

The omission of an arrow from $H^1(\Gamma, {}_b A)$ to $H^1(\Gamma, A)$ in the above diagram is intentional: *there is in general no relation between the two groups*. If A' is an *inner* form of A , then $H^1(\Gamma, A') \approx H^1(\Gamma, A)$, but for an *outer* form A' of A , there need be no relation between $H^1(\Gamma, A')$ and $H^1(\Gamma, A)$.

PROFINITE GROUPS

Recall that a topological group Γ is profinite if it is an inverse (i.e., projective) limit of discrete finite groups. Such a group is compact, and the open normal subgroups form a base for the neighbourhoods of 1. In particular, every open subgroup contains an open normal subgroup, and $\Gamma = \varprojlim \Gamma/U$ where U runs over the open normal subgroups.

Let Γ be a profinite group. We say that A is a discrete Γ -module if the map $\Gamma \times A \rightarrow A$ is continuous for the given topology on Γ and the discrete topology on A . Equivalently,

$$A = \bigcup A^U \quad (185)$$

— every element of A is fixed by an open (normal) subgroup U of Γ . When Γ is a profinite group, we require the 1-cocycles to be continuous. Then

$$H^1(\Gamma, A) = \varinjlim H^1(\Gamma/U, A^U)$$

(limit over the open normal subgroups of Γ).

We are interested in the case that Γ is a Galois group of a Galois extension K/k equipped with the Krull topology. In this case, the open (resp. open normal) subgroups of G are the groups $\text{Gal}(K/k')$ with k' finite (resp. finite and Galois) over k . Let G be an algebraic group over k . Each K -point of G has coordinates in a subfield of K finite over k , and so

$$G(K) = \bigcup_{[k':k] < \infty} G(k').$$

As $G(k') = G(K)^{\text{Gal}(K/k')}$, we see that $G(K)$ is a discrete Γ -module. We set

$$H^1(K/k, G) = H^1(\text{Gal}(K/k), G(K))$$

and

$$\begin{aligned} H^1(k, G) &= H^1(\text{Gal}(k^{\text{sep}}/k), G(k^{\text{sep}})) \\ &= \varinjlim_{[k':k] < \infty, k' \subset K} H^1(k'/k, G). \end{aligned}$$

Let

$$e \rightarrow N \rightarrow G \rightarrow Q \rightarrow e$$

be an exact sequence of algebraic groups. If N is smooth¹ or k is perfect, the sequence

$$e \rightarrow N(k^{\text{sep}}) \rightarrow G(k^{\text{sep}}) \rightarrow Q(k^{\text{sep}}) \rightarrow e$$

is exact, and so we have an exact sequence of pointed sets

$$e \rightarrow N(k) \rightarrow G(k) \rightarrow Q(k) \rightarrow H^1(k, N) \rightarrow H^1(k, G) \rightarrow H^1(k, Q).$$

When N is commutative, the sequence continues to an exact sequence

$$\dots \rightarrow H^1(k, G) \rightarrow H^1(k, Q) \rightarrow H^2(k, N).$$

¹For nonsmooth groups, we should be using flat cohomology groups.

EXAMPLES

Let K be a Galois extension of k with Galois group Γ , and let V be a K -vector space. A **semi-linear action** of Γ on V is a homomorphism $\Gamma \rightarrow \text{Aut}_{k\text{-linear}}(V)$ such that

$$\sigma(cv) = \sigma c \cdot \sigma v \quad \text{all } \sigma \in \Gamma, c \in K, v \in V.$$

If $V = K \otimes_k V_0$, then there is a unique semi-linear action of Γ on V for which $V^\Gamma = 1 \otimes V_0$, namely,

$$\sigma(c \otimes v) = \sigma c \otimes v \quad \sigma \in \Gamma, c \in K, v \in V.$$

LEMMA 27.5. *Let $\Gamma \times V \rightarrow V$ be a semi-linear action of Γ on V . Then the map*

$$c \otimes v \mapsto cv: K \otimes_k V^\Gamma \rightarrow V$$

is an isomorphism.

PROOF. See 16.15 of my Algebraic Geometry notes. □

PROPOSITION 27.6. *The functor $V \mapsto K \otimes_k V$ from k -vector spaces to K -vector spaces endowed with a continuous semi-linear action of Γ is an equivalence of categories with quasi-inverse $V \mapsto V^\Gamma$.*

PROOF. Follows easily from (27.5). □

PROPOSITION 27.7. *Let $\phi_0: V_0 \times V_0 \rightarrow V_0$ be bilinear form on a finite-dimensional vector space over k , and let $G(\phi_0)$ denote the group of automorphisms of (V, ϕ_0) . The cohomology set $H^1(\Gamma, G(\phi_0))$ classifies the isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K .*

PROOF. Let (V, ϕ) be such a pair over k , and choose an isomorphism

$$f: (V_0, \phi_0)_K \rightarrow (V, \phi)_K.$$

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. Moreover, any other isomorphism $f': (V_0, \phi_0)_K \rightarrow (V, \phi)_K$ differs from f by a $g \in \mathcal{A}(K)$, and

$$a_\sigma(f \circ g) = g^{-1} \cdot a_\sigma(f) \cdot \sigma g.$$

Therefore, the cohomology class of $a_\sigma(f)$ depends only on (V, ϕ) . It is easy to see that, in fact, it depends only on the isomorphism class of (V, ϕ) , and that two pairs (V, ϕ) and (V', ϕ') giving rise to the same class are isomorphic. It remains to show that every cohomology class arises from a pair (V, ϕ) . Let $(a_\sigma)_{\sigma \in \Gamma}$ be a 1-cocycle, and use it to define a new action of Γ on $V_K = K \otimes_k V$:

$$\sigma x = a_\sigma \cdot \sigma x, \quad \sigma \in \Gamma, \quad x \in V_K.$$

Then

$$\sigma(cv) = \sigma c \cdot \sigma v, \quad \text{for } \sigma \in \Gamma, c \in K, v \in V,$$

and

$$\sigma(\tau v) = \sigma(a_\tau \tau v) = a_\sigma \cdot \sigma a_\tau \cdot \sigma \tau v = \sigma^\tau v,$$

and so this is a semi-linear action. Therefore,

$$V_1 \stackrel{\text{def}}{=} \{x \in V_K \mid \sigma x = x\}$$

is a subspace of V_K such that $K \otimes_k V_1 \simeq V_K$ (by 27.5). Because ϕ_{0K} arises from a pairing over k ,

$$\phi_{0K}(\sigma x, \sigma y) = \sigma \phi(x, y), \quad \text{all } x, y \in V_K.$$

Therefore (because $a_\sigma \in \mathcal{A}(K)$),

$$\phi_{0K}(\sigma^\sigma x, \sigma^\sigma y) = \phi_{0K}(\sigma x, \sigma y) = \sigma \phi_{0K}(x, y).$$

If $x, y \in V_1$, then $\phi_{0K}(\sigma^\sigma x, \sigma^\sigma y) = \phi_{0K}(x, y)$, and so $\phi_{0K}(x, y) = \sigma \phi_{0K}(x, y)$. By Galois theory, this implies that $\phi_{0K}(x, y) \in k$, and so ϕ_{0K} induces a k -bilinear pairing on V_1 . \square

COROLLARY 27.8. *For all n , $H^1(\Gamma, \text{GL}_n(K)) = 1$.*

PROOF. Apply Proposition 27.7 with $V_0 = k^n$ and ϕ_0 the zero form. It shows that $H^1(\Gamma, \text{GL}_n(K))$ classifies the isomorphism classes of k -vector spaces V such that $K \otimes_k V \approx K^n$. But such a k -vector space has dimension n , and all k -vector spaces of dimension n are isomorphic. \square

COROLLARY 27.9. *For all n , $H^1(\Gamma, \text{SL}_n(K)) = 1$*

PROOF. Because the determinant map $\det: \text{GL}_n(K) \rightarrow K^\times$ is surjective,

$$1 \rightarrow \text{SL}_n(K) \rightarrow \text{GL}_n(K) \xrightarrow{\det} K^\times \rightarrow 1$$

is an exact sequence of Γ -groups. It gives rise to an exact sequence

$$\text{GL}_n(k) \xrightarrow{\det} k^\times \rightarrow H^1(\Gamma, \text{SL}_n) \rightarrow H^1(\Gamma, \text{GL}_n)$$

from which the statement follows. \square

COROLLARY 27.10. *Let ϕ_0 be a nondegenerate alternating bilinear form on V_0 , and let Sp be the associated symplectic group. Then $H^1(\Gamma, \text{Sp}(K)) = 1$.*

PROOF. According to Proposition 27.7, $H^1(\Gamma, \text{Sp}(K))$ classifies isomorphism classes of pairs (V, ϕ) over k that become isomorphic to (V_0, ϕ_0) over K . But this condition implies that ϕ is a nondegenerate alternating form and that $\dim V = \dim V_0$. All such pairs (V, ϕ) are isomorphic. \square

COROLLARY 27.11. *Let ϕ be a nondegenerate bilinear symmetric form on V , and let $\text{O}(\phi)$ be the associated orthogonal group. Then $H^1(\Gamma, \text{O}(\phi)(K))$ classifies the isomorphism classes of quadratic spaces over k that become isomorphic to (V, ϕ) over K .*

PROOF. Special case of the proposition. \square

COROLLARY 27.12. *Assume $\text{char}(k) \neq 2$. The set $H^1(k, \text{O}(\phi))$ classifies the isomorphism classes of quadratic spaces over k with the same dimension as V .*

PROOF. Over k^{sep} , all nondegenerate quadratic spaces of the same dimension are isomorphic. \square

The set $H^1(k, O(\phi))$ can be very large; for example, when $k = \mathbb{Q}$ it is infinite.

EXAMPLE 27.13. From the exact sequence

$$1 \rightarrow \mathbb{G}_m(k^{\text{sep}}) \rightarrow \text{GL}_n(k^{\text{sep}}) \rightarrow \text{PGL}_n(k^{\text{sep}}) \rightarrow 1$$

we get an exact sequence

$$H^1(k, \text{GL}_n) \rightarrow H^1(k, \text{PGL}_n) \xrightarrow{\delta} H^2(k, \mathbb{G}_m).$$

The group $H^2(k, \mathbb{G}_m)$ can be identified with the Brauer group of k , and the image of δ consists of the elements of $\text{Br}(k)$ that can be represented by a central simple algebra of degree n^2 ; in particular, it is not necessarily a subgroup of $\text{Br}(k)$.

b. Generalities on forms

DEFINITION 27.14. Let K be an extension of k , and let G be an algebraic group over k . A K/k -form of G is an algebraic group G' over k such that $G'_K \approx G_K$. Two K/k -forms are isomorphic if they are isomorphic as algebraic groups over k . When $K = k^{\text{sep}}$, we omit it from the notation.

Let K be a Galois extension of k with Galois group Γ . Let G be an algebraic group over k , and let $\mathcal{A}(K)$ be the group of automorphisms of G_K . Then Γ acts on $\mathcal{A}(K)$ according to the rule:

$$\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}.$$

PROPOSITION 27.15. The cohomology set $H^1(\Gamma, \mathcal{A}(K))$ classifies the isomorphism classes of algebraic groups G over k that become isomorphic to G_0 over K .

PROOF. Let G be such an algebraic group over k , and choose an isomorphism

$$f: G_{0K} \rightarrow G_K.$$

Let

$$a_\sigma = f^{-1} \circ \sigma f.$$

As in the proof of Proposition 27.7, $(a_\sigma)_{\sigma \in \Gamma}$ is a 1-cocycle, and the map

$$G \mapsto \text{class of } (a_\sigma)_{\sigma \in \Gamma} \text{ in } H^1(\Gamma, \mathcal{A}(K))$$

is well-defined and its fibres are the isomorphism classes over k .

In proving that the map is surjective, it is useful to identify $\mathcal{A}(K)$ with the automorphism group of the Hopf algebra $\mathcal{O}(G_{0K}) = K \otimes_k \mathcal{O}(G_0)$. Let $A_0 = \mathcal{O}(G_0)$ and $A = K \otimes_k A_0$. As in the proof of Proposition 27.7, we use a 1-cocycle $(a_\sigma)_{\sigma \in \Gamma}$ to twist the action of Γ on A ; specifically, we define

$$\sigma a = a_\sigma \circ \sigma a, \quad \sigma \in \Gamma, \quad a \in A.$$

From Lemma 27.5 the k -subspace

$$B = \{a \in A \mid \sigma a = a\}$$

of A has the property that

$$K \otimes_k B \simeq A.$$

It remains to show that the Hopf algebra structure on A induces a Hopf algebra structure on B . Consider for example the comultiplication. The k -linear map

$$\Delta_0: A_0 \rightarrow A_0 \otimes_k A_0$$

has a unique extension to a K -linear map

$$\Delta: A \rightarrow A \otimes_K A.$$

This map commutes with the action of Γ :

$$\Delta(\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Because a_σ is a Hopf algebra homomorphism,

$$\Delta(a_\sigma a) = a_\sigma \Delta(a), \quad \text{all } \sigma \in \Gamma, a \in A.$$

Therefore,

$$\Delta(\sigma a) = \sigma(\Delta(a)), \quad \text{all } \sigma \in \Gamma, a \in A.$$

In particular, we see that Δ maps B into $(A \otimes_K A)^\Gamma$, which equals $B \otimes_k B$ because the functor in (27.6) preserves tensor products. Similarly, all the maps defining the Hopf algebra structure on A preserve B , and therefore define a Hopf algebra structure on B . Finally, one checks that the 1-cocycle attached to B and the given isomorphism $K \otimes_k B \rightarrow A$ is (a_σ) . \square

COROLLARY 27.16. *Let G be an algebraic group over k . The isomorphism classes of algebraic groups over k that become isomorphic to $G_{k^{\text{sep}}}$ over k^{sep} are classified by $H^1(\Gamma, \mathcal{A}(k^{\text{sep}}))$. Here $\Gamma = \text{Gal}(k^{\text{sep}}/k)$ and $\mathcal{A}(k^{\text{sep}})$ is the automorphism group of $G_{k^{\text{sep}}}$.*

PROOF. Special case of the proposition. \square

EXAMPLE: THE FORMS OF GL_2 .

What are the k -forms of groups GL_2 ? For any $a, b \in k^\times$, define $\mathbb{H}(a, b)$ to be the algebra over k with basis $1, i, j, ij$ as a k -vector space, and with the multiplication given by

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

This is a k -algebra with centre k , and it is either a division algebra or is isomorphic to $M_2(k)$. For example, $\mathbb{H}(1, 1) \approx M_2(k)$ and $\mathbb{H}(-1, -1)$ is the usual quaternion algebra when $k = \mathbb{R}$.

Each algebra $\mathbb{H}(a, b)$ defines an algebraic group $G = G(a, b)$ with $G(R) = (R \otimes \mathbb{H}(a, b))^\times$. These are exactly the algebraic groups over k becoming isomorphic to GL_2 over k^{sep} , and

$$G(a, b) \approx G(a', b') \iff \mathbb{H}(a, b) \approx \mathbb{H}(a', b').$$

Over \mathbb{R} , every \mathbb{H} is isomorphic to $\mathbb{H}(-1, -1)$ or $M_2(\mathbb{R})$, and so there are exactly two forms of GL_2 over \mathbb{R} .

Over \mathbb{Q} , the isomorphism classes of quaternion algebras are classified by the subsets of

$$\{2, 3, 5, 7, 11, 13, \dots, \infty\}$$

having a finite even number of elements. The proof of this uses the quadratic reciprocity law in number theory. In particular, there are infinitely many forms of GL_2 over \mathbb{Q} , exactly one of which, GL_2 , is split.

EXAMPLE: THE FORMS OF GL_n

Classifying the k -forms of GL_n turns out to be the same as classifying the k -forms of the k -algebra $M_n(k)$, and so we do that first. Proofs of 27.18–27.23 can be found, for example, in Chapter IV of my notes *Class Field Theory*.

DEFINITION 27.17. A k -algebra A is **central** if its centre is k , and it is **simple** if it has no 2-sided ideals (except 0 and A). If all nonzero elements have inverses, it is called a **division algebra** (or **skew field**).

For example, $M_n(k)$ and the quaternion algebra $\mathbb{H}(a, b)$ are central simple algebras.

THEOREM 27.18 (WEDDERBURN). For any division algebra D over k , $M_n(D)$ is a simple k -algebra, and every simple k -algebra is of this form; moreover, $M_n(D)$ is central if and only if D is central.

PROPOSITION 27.19. Let D be a central division algebra of degree n^2 over k . Then D contains a field k' separable of degree n over k .

COROLLARY 27.20. If k is separably closed, then the only central simple algebras over k are the matrix algebras $M_n(k)$.

PROOF. Combine the last two statements. □

PROPOSITION 27.21. The 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 of degree n^2 . Then $k^{\mathrm{sep}} \otimes_k A$ is again central simple, and so it is isomorphic to $M_n(k)$ by (27.20). Conversely, if A is a k -algebra that becomes isomorphic to $M_n(k^{\mathrm{sep}})$ over k^{sep} , then it is certainly central and simple, and has degree n^2 . □

PROPOSITION 27.22. All automorphisms of the k -algebra $M_n(k)$ are inner, i.e., of the form $X \mapsto YXY^{-1}$ for some Y .

PROOF. Let S be k^n regarded as an $M_n(k)$ -module. It is simple, and every simple $M_n(k)$ -module is isomorphic to it. Let α be an automorphism of $M_n(k)$, and let S' denote S , but with $X \in M_n(k)$ acting as $\alpha(X)$. Then S' is a simple $M_n(k)$ -module, and so there exists an isomorphism of $M_n(k)$ -modules $f: S \rightarrow S'$. Then

$$\alpha(X)f\vec{x} = fX\vec{x}, \quad \text{all } X \in M_n(k), \vec{x} \in S.$$

Therefore,

$$\alpha(X)f = fX, \quad \text{all } X \in M_n(k).$$

As f is k -linear, it is multiplication by an invertible matrix Y , and so this equation shows that

$$\alpha(X) = YXY^{-1}. \quad \square$$

COROLLARY 27.23. The isomorphism classes of k -algebras becoming isomorphic to $M_n(k)$ over k^{sep} are classified by $H^1(k, \mathrm{PGL}_n)$.

PROOF. The proposition shows that

$$\text{Aut}_{k^{\text{sep-algebra}}}(M_n(k^{\text{sep}})) = \text{PGL}_n(k^{\text{sep}}).$$

Let A be a k -algebra for which there exists an isomorphism $f: M_n(k^{\text{sep}}) \rightarrow k^{\text{sep}} \otimes_k A$, and let

$$a_\sigma = f^{-1} \circ \sigma f.$$

Then a_σ is a 1-cocycle, depending only on the k -isomorphism class of A .

Conversely, given a 1-cocycle, define

$${}^\sigma X = a_\sigma \cdot \sigma X, \quad \sigma \in \Gamma, X \in M_n(k^{\text{sep}}).$$

This defines a semi-linear action of Γ on $M_n(k^{\text{sep}})$ and $M_n(k^{\text{sep}})^\Gamma$ is a k -algebra becoming isomorphic to $M_n(k)$ over k^{sep} (27.5; see also the proof of 27.15). \square

For a central simple algebra A over k , we let G_A denote the algebraic group over k such that $G(R) = (A \otimes R)^\times$.

THEOREM 27.24. *The k -forms of GL_n are the groups G_A ; two k -forms G_A and $G_{A'}$ are isomorphic if and only if A and A' are isomorphic k -algebras.*

PROOF. We have map $A \mapsto G_A$ from k -forms of $M_n(k)$ to k -forms of GL_n . As the isomorphism classes of both sets are classified by $H^1(k, \text{PGL}_n)$ and the map is obviously compatible with the cohomology classes, we see that the map defines a bijection from the set isomorphism classes of k -forms of $M_n(k)$ to the set of isomorphism classes of k -forms of GL_n . \square

COROLLARY 27.25. *The k -forms of GL_n are the algebraic groups $\text{GL}_{D,m}$ with D a central division algebra over k of dimension $(n/m)^2$.*

REMARK 27.26. Let A be a central simple algebra over k . For some n , there exists an isomorphism $f: k^{\text{sep}} \otimes_k A \rightarrow M_n(k^{\text{sep}})$, unique up to an inner automorphism (27.21). Let $a \in A$, and let $\text{Nm}(a) = \det(f(a))$. Then $\text{Nm}(a)$ does not depend on the choice of f . Moreover, it is fixed by Γ , and so lies in k . It is called the **reduced norm** of a .

c. Forms of semisimple algebraic groups

We sometimes abbreviate “semisimple algebraic group” to “semisimple group”. [References will be added.]

27.27. Recall that $G^{\text{ad}} = G/Z(G)$. The action of G on itself by inner automorphisms factors through G^{ad} . A automorphism of G over k is said to be inner if it is defined by an element of $G^{\text{ad}}(k)$. When $Z(G)$ is smooth, $G^{\text{ad}}(k^{\text{sep}}) = G(k^{\text{sep}})/Z(k^{\text{sep}})$.

27.28. A semisimple group G over a field k is said to be split if it contains a split maximal torus. Since every semisimple group contains a maximal torus, and every torus over k splits over k^{sep} , we see that every semisimple group splits over k^{sep} .

27.29. Every semisimple group G over a separably closed field k determines a certain graph called its Dynkin diagram. Almost-simple group correspond to connected graphs. The connected Dynkin diagrams are exactly those in the following list: 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 . An almost-simple algebraic group over a separably closed field whose Dynkin diagram is X_y is said to have type X_y .

27.30. Two simply connected almost-simple groups over a separably closed field are isomorphic if and only if they have isomorphic Dynkin diagrams. Over an arbitrary field k , for each connected Dynkin diagram, there is a split almost-simple algebraic group over k of that type; it is unique up to isomorphism (over k) and is called the simply connected Chevalley group of that type.

27.31. The group of automorphisms of a simply connected semisimple group over a separably closed field can be read off from its Dynkin diagram: it contains the group of inner automorphisms as a normal subgroup, and the quotient is the group of symmetries $\text{Sym}(D)$ of its Dynkin diagram. Thus, for a simply connected semisimple group G over an arbitrary field k , there is an exact sequence

$$1 \rightarrow G(k^{\text{sep}}) \rightarrow \text{Aut}(G_{k^{\text{sep}}}) \rightarrow \text{Sym}(D) \rightarrow 1 \quad (186)$$

of $\Gamma = \text{Gal}(k^{\text{sep}}/k)$ -modules. The connected Dynkin diagram do not have many symmetries: for D_4 the symmetry group is S_3 (symmetric group on 3 letters), for A_n ($n \neq 1$), D_n ($n \neq 4$), and E_6 it has order 2, and otherwise it is trivial.

We set $\mathcal{A}(G) = \text{Aut}(G_{k^{\text{sep}}})$.

27.32. Let G be a split semisimple group over k . Then Γ acts trivially on $\text{Sym}(D)$, and the sequence (186) splits, i.e., there is subgroup of $\mathcal{A}(G)$ on which Γ acts trivially and which maps isomorphically onto $\text{Sym}(D)$. Thus, the map

$$H^1(\Gamma, G^{\text{ad}}(k^{\text{sep}})) \rightarrow H^1(\Gamma, \mathcal{A}(G))$$

is injective, with image the kernel of

$$H^1(\Gamma, \mathcal{A}(G)) \rightarrow H^1(\Gamma, \text{Sym}(D)).$$

27.33. Let G be a split semisimple group over k . The forms of G are classified by $H^1(\Gamma, \mathcal{A}(G))$. We say that a form of G is inner² if its class lies in the subset $H^1(k, G^{\text{ad}})$ of $H^1(\Gamma, \mathcal{A}(G))$; thus the inner forms of G are classified by $H^1(k, G^{\text{ad}})$.

27.34. Let G be a split simply connected geometrically almost-simple group over k of type X_y . A k -form G' defines a class in $H^1(\Gamma, \mathcal{A}(G))$, which maps to an element a of $H^1(\Gamma, \text{Sym}(D))$. As Γ acts trivially on $\text{Sym}(D)$,

$$H^1(\Gamma, \text{Sym}(D)) \simeq \text{Hom}(\Gamma, \text{Sym}(D)) \quad (\text{continuous homomorphisms}),$$

and so a is a continuous homomorphism $\Gamma \rightarrow \text{Sym}(D)$. Let L be the fixed field of the kernel of a . It is finite over k , of degree z say. We then say that G' is of type ${}^z X_y$.

Thus, G' is of type ${}^z X_y$ if it becomes an inner form of a split group of type X_y over an extension of k of degree z (but not of a smaller degree).

27.35. Let G be a simply connected geometrically almost-simple group over k . If G is split, then

$$X^*(Z(G)) = P(D)/Q(D)$$

²This definition of inner forms is correct only for split groups — see 2.33. In general, we call a k -form G' of G an *inner twist* of G if its class in $H^1(k, \mathcal{A}(G))$ lies in the image of $H^1(k, G^{\text{ad}}) \rightarrow H^1(k, \mathcal{A}(G))$. When this map is injective, “inner twist” coincides with “inner form”.

with Γ acting trivially; thus $Z(G)$ is a product of groups of the form μ_n . For the form G' of G defined by a 1-cocycle $a = (a_\sigma)$, we have $Z(G') = Z(G)$ but with Γ acting through a_σ :

$$\sigma z = a_\sigma \cdot \sigma z, \quad z \in Z(k^{\text{sep}}).$$

More precisely, let $f: G_{k^{\text{sep}}} \rightarrow G'_{k^{\text{sep}}}$ be an isomorphism, and let $\sigma f = f \circ a_\sigma$; then f restricts to an isomorphism $Z_{k^{\text{sep}}} \rightarrow Z'_{k^{\text{sep}}}$, and $\sigma(f|Z) = (f|Z) \circ a_\sigma|Z$.

For example, SL_n is the split group over k of type A_{n-1} , and its centre is μ_n .

d. Classical groups

In this section, $\text{char}(k) \neq 2$.

DEFINITION 27.36. Recall that every semisimple algebraic group G over k has a finite étale covering by a simply connected semisimple group \tilde{G} ; moreover, \tilde{G} can be written as a product

$$\tilde{G} = \prod (G_i)_{k_i/k}$$

with each G_i geometrically almost-simple over k_i . The semisimple group G is said to be classical if each G_i is of type A_n , B_n , C_n , or D_n , but not 3D_4 or 6D_4 . In other words, we exclude only factors of exceptional type and 3D_4 and 6D_4 .

INVOLUTIONS OF k -ALGEBRAS

DEFINITION 27.37. Let A be a k -algebra. An *involution* of k is a k -linear map $a \mapsto a^*: A \rightarrow A$ such that

$$\begin{aligned} (ab)^* &= b^*a^* \quad \text{all } a, b \in A, \\ a^{**} &= a. \end{aligned}$$

The involution is said to be of the *first* or *second kind* according as it acts trivially on the elements of the centre of A or not.

EXAMPLE 27.38. (a) On $M_n(k)$ there is the standard involution $X \mapsto X^t$ (transpose) of the first kind.

(b) On a quaternion algebra $\mathbb{H}(a, b)$, there is the standard involution $i \mapsto -i$, $j \mapsto -j$ of the first kind.

(c) On a quadratic field extension K of k , there is a unique nontrivial involution (of the second kind).

LEMMA 27.39. Let $(A, *)$ be a k -algebra with involution. An inner automorphism $x \mapsto axa^{-1}$ commutes with $*$ if and only if a^*a lies in the centre of A .

PROOF. To say that $\text{inn}(a)$ commutes with $*$ means that the two maps

$$\begin{aligned} x \mapsto axa^{-1} &\mapsto (a^*)^{-1}x^*a^* \\ x \mapsto x^* &\mapsto ax^*a^{-1} \end{aligned}$$

coincide, i.e., that

$$x^* = (a^*a)x^*(a^*a)^{-1}$$

for all $x \in A$. As $x \mapsto x^*$ is bijective, this holds if and only if a^*a lies in the centre of A . \square

REMARK 27.40. Let A have centre k . We can replace a with ca , $c \in k^\times$, without changing $\text{inn}(a)$. This replaces a^*a with $c^*c \cdot a^*a$. When $*$ is of the first kind, $c^*c = c^2$. Therefore, when k is separably closed, we can choose c to make $a^*a = 1$.

THE INNER FORMS OF SL_n (GROUPS OF TYPE ${}^1A_{n-1}$)

Let A be a central simple algebra over k of degree n^2 . Then

$$R \rightsquigarrow \{a \in A \otimes R \mid \text{Nm}(a) = 1\}$$

is an algebraic group, which we denote SL_A . Here $\text{Nm}(a)$ denotes the reduced norm of a . Recall that $A \simeq M_{n/m}(D)$ for some central division algebra D of degree m^2 over k . Thus, SL_A can also be described as the group

$$R \rightsquigarrow \{a \in M_{n/m}(D \otimes R) \mid \text{Nm}(a) = 1\}.$$

We know that A is a k -form of the k -algebra $M_n(k)$, and all k -forms of $M_n(k)$ of this shape. Moreover, the k -forms of $M_n(k)$ are classified by $H^1(k, \text{PGL}_n)$. As the k -forms of SL_n are also classified by $H^1(k, \text{PGL}_n)$ and the map $A \mapsto SL_A$ preserves cohomology classes, we see that the map induces a bijection on isomorphism classes.

THEOREM 27.41. *The inner forms of SL_n over k are the algebraic groups SL_A with A a central simple algebra of degree n^2 over k . Two groups SL_A and $SL_{A'}$ are isomorphic if and only if A and A' are isomorphic as k -algebras.*

THE OUTER FORMS OF SL_n (GROUPS OF TYPE 2A_n).

The Dynkin diagram of SL_n has a unique nontrivial automorphism, which is induced by the outer automorphism $X \mapsto (X^{-1})^t = (X^t)^{-1}$ of SL_n . Thus, the sequence (186), p.479, becomes

$$1 \rightarrow \text{PGL}_n \rightarrow \mathcal{A}(SL_n) \rightarrow \{\pm 1\} \rightarrow 1.$$

Now consider the k -algebra with involution of the second kind

$$M_n(k) \times M_n(k), \quad (X, Y)^* = (Y^t, X^t).$$

Every automorphism of $M_n(k) \times M_n(k)$ is either inner, or is the composite of an inner automorphism with $(X, Y) \mapsto (Y, X)$. This follows from the fact that the two copies of $M_n(k)$ are the *only* simple subalgebras of $M_n(k) \times M_n(k)$. According to (27.39), the inner automorphism by $a \in A$ commutes with $*$ if and only if $a^*a \in k \times k$. But $(a^*a)^* = a^*a$, and so $a^*a \in k$. When we work over k^{sep} , we can scale a so that $a^*a = 1$ (27.40): if $a = (X, Y)$, then

$$1 = a^*a = (Y^t X, X^t Y),$$

and so $a = (X, (X^t)^{-1})$. Thus, the automorphisms of $(M_n(k^{\text{sep}}) \times M_n(k^{\text{sep}}), *)$ are the inner automorphisms by elements $(X, (X^t)^{-1})$ and composites of such automorphisms with $(X, Y) \mapsto (Y, X)$. When we embed

$$X \mapsto (X, (X^t)^{-1}): SL_n(k^{\text{sep}}) \hookrightarrow M_n(k^{\text{sep}}) \times M_n(k^{\text{sep}}), \tag{187}$$

the image it is stable under the automorphisms of $(M_n(k^{\text{sep}}) \times M_n(k^{\text{sep}}), *)$, and this induces an isomorphism

$$\text{Aut}(M_n(k^{\text{sep}}) \times M_n(k^{\text{sep}}), *) \simeq \text{Aut}(SL_{nk^{\text{sep}}}).$$

Thus, the forms of SL_n correspond to the forms of $(M_n(k) \times M_n(k), *)$. Such a form is a simple algebra A over k with centre K of degree 2 over k and an involution $*$ of the second kind.

The map (187) identifies $SL_n(k^{\text{sep}})$ with the subgroup of $M_n(k^{\text{sep}}) \times M_n(k^{\text{sep}})$ of elements such that

$$a^*a = 1, \quad \text{Nm}(a) = 1.$$

Therefore, the form of SL_n attached to the form $(A, *)$ is the group G such that $G(R)$ consists of the $a \in R \otimes_k A$ such that

$$a^*a = 1, \quad \text{Nm}(a) = 1.$$

There is a commutative diagram

$$\begin{array}{ccc} \text{Aut}(SL_n k^{\text{sep}}) & \longrightarrow & \text{Sym}(D) \\ \parallel & & \parallel \\ \text{Aut}(M_n(k^{\text{sep}}) \times M_n(k^{\text{sep}}), *) & \longrightarrow & \text{Aut}_{k\text{-algebra}}(k^{\text{sep}} \times k^{\text{sep}}). \end{array}$$

The centre K of A is the form of $k^{\text{sep}} \times k^{\text{sep}}$ corresponding to the image of the cohomology class of G in $\text{Sym}(D)$. Therefore, we see that G is an outer form if and only if K is a field.

Let A be a simple algebra with centre a quadratic extension K of k , and let $*$ be an involution of the second kind on A . Then

$$R \rightsquigarrow \{a \in (A \otimes R) \mid a^* \cdot a = 1\}$$

is an algebraic group, which we denote $SL_{(A,*)}$. It is a form of SL_n where $n = [A: K]^{1/2}$.

THEOREM 27.42. *The outer forms of SL_n are the algebraic groups $SL_{(A,*)}$ with A a simple k -algebra whose centre is a quadratic field extension of k and with $*$ an involution of A of the second kind. Two groups $SL_{(A,*)}$ and $SL_{(A',*)}$ are isomorphic if and only if $(A, *)$ and $(A', *)$ are isomorphic as k -algebras with involution.*

THE FORMS OF Sp_{2n} (GROUPS OF TYPE C_n)

The k -algebra $M_{2n}(k)$ has an involution of the first kind:

$$X^* = SX^t S^{-1}, \quad S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

The inner automorphism defined by an invertible matrix U commutes with $*$ if and only if $U^*U \in k$ (see 27.39). When we pass to k^{sep} , we may suppose $U^*U = I$, i.e., that

$$SU^t S^{-1}U = I.$$

Because $S^{-1} = -S$, this says that

$$U^t SU = S$$

i.e., that $U \in Sp_{2n}(k^{\text{sep}})$. Since there are no symmetries of the Dynkin diagram C_n , we see that the inclusion

$$X \mapsto X: Sp_{2n}(k^{\text{sep}}) \hookrightarrow M_{2n}(k^{\text{sep}}) \tag{188}$$

induces an isomorphism

$$\text{Aut}(Sp_{2n} k^{\text{sep}}) \simeq \text{Aut}(M_{2n}(k^{\text{sep}}), *).$$

Therefore, the forms of Sp_{2n} correspond to the forms of $(M_{2n}(k), *)$. Such a form is a central simple algebra A over k with an involution $*$ of the first kind.

The map (188) identifies $\mathrm{Sp}_{2n}(k^{\mathrm{sep}})$ with the subgroup of $M_{2n}(k^{\mathrm{sep}})$ of elements such that

$$a^*a = 1.$$

Therefore, the form of Sp_{2n} attached to $(A, *)$ is the group $G = G_{(A,*)}$ such that $G(R)$ consists of the $a \in R \otimes_k A$ for which

$$a^*a = 1.$$

THEOREM 27.43. *The forms of Sp_{2n} are the algebraic groups $\mathrm{SL}_{(A,*)}$ with $(A, *)$ a form of $(M_{2n}(k), *)$. Two groups $\mathrm{SL}_{(A,*)}$ and $\mathrm{SL}_{(A',*)}$ are isomorphic if and only if $(A, *)$ and $(A', *)$ are isomorphic as k -algebras with involution.*

THE FORMS OF $\mathrm{Spin}(\phi)$ (GROUPS OF TYPE B AND D)

Let (V, ϕ) be a nondegenerate quadratic space over k with greatest possible Witt index (dimension of a totally isotropic subspace). The action of $O(\phi)$ on itself preserves $\mathrm{SO}(\phi)$, and there is also an action of $O(\phi)$ on $\mathrm{Spin}(\phi)$. These actions are compatible with the natural homomorphism

$$\mathrm{Spin}(\phi) \rightarrow \mathrm{SO}(\phi)$$

and realize $O(\phi)$ modulo its centre as the automorphism group of each. Therefore, the forms of $\mathrm{Spin}(\phi)$ are exactly the double covers of the forms of $\mathrm{SO}(\phi)$.

The determination of the forms of $\mathrm{SO}(\phi)$ is very similar to the last case. Let M be the matrix of ϕ relative to some basis for V . We use the k -algebra with involution of the first kind

$$M_n(k), \quad X^* = MX^tM^{-1}.$$

The automorphism group of $(M_n(k), *)$ is $O(\phi)$ modulo its centre, and so the forms of $\mathrm{SO}(\phi)$ correspond to the forms of $(M_{2n}(k), *)$. Such a form is a central simple algebra A over k with an involution $*$ of the first kind, and the form of $\mathrm{SO}(\phi)$ attached to $(A, *)$ is the group G such that $G(R)$ consists of the $a \in R \otimes_k A$ for which

$$a^*a = 1.$$

The symmetry group of a Dynkin diagram of type D_4 is S_3 . It is not possible to realize the automorphism group of a split group of type D_4 as the automorphism group of a central simple algebra, and so it is not possible to realize the groups of type 3D_4 and 6D_4 in terms of algebras with involution. For this reason, the groups are not said to be classical. In other words, the geometrically almost-simple classical algebraic groups are exactly those that can be described in terms for algebras with involution.

SPECIAL FIELDS

To continue, we need a description of the algebras with involution over a field k . For an arbitrary field, there is not much one can say, but for one important class of fields there is a great deal.

PROPOSITION 27.44. *If a central simple algebra A over k admits an involution of the first kind, then*

$$A \otimes_k A \approx M_{n^2}(k), \quad n^2 = [A:k]. \quad (189)$$

PROOF. Recall that the opposite algebra A^{opp} of A equals A as a k -vector space but has its multiplication reversed:

$$a^{\text{opp}}b^{\text{opp}} = (ba)^{\text{opp}}.$$

Let A_0 denote A regarded as a k -vector space. There are commuting left actions of A and A^{opp} on A_0 , namely, A acts by left multiplication and A^{opp} by right multiplication, and hence a homomorphism

$$A \otimes_k A^{\text{opp}} \rightarrow \text{End}_{k\text{-lin}}(A_0).$$

This is injective, and the source and target have the same dimension as k -vector spaces, and so the map is an isomorphism. Since an involution on A is an isomorphism $A \rightarrow A^{\text{opp}}$, the proposition follows from this. \square

Over any field, matrix algebras and quaternion algebras are central simple algebras admitting involutions. For many important fields, these are essentially the only such algebras. Consider the following condition on a field k :

27.45. *The only central division algebras over k or a finite extension of k satisfying (189) are the quaternion algebras and the field itself (i.e., they have degree 4 or 1).*

THEOREM 27.46. *The following fields satisfy (27.45): separably closed fields, finite fields, \mathbb{R} , \mathbb{Q}_p and its finite extensions, and \mathbb{Q} and its finite extensions.*

PROOF. The proofs become successively more difficult: for separably closed fields there is nothing to prove (27.20); for \mathbb{Q} it requires class field theory (see, for example, my notes *Class Field Theory*). \square

ASIDE 27.47. According to a theorem of Merkujev, the subgroup of elements of order 2 in the Brauer group of k is generated by the classes of quaternion algebras. An example of Brauer (1929) shows that not every such element is the class of a quaternion algebra. A theorem of Albert states that the tensor product of two quaternion algebras is a division algebra if and only if they do not have a common quadratic splitting field. Let F be a field not of characteristic 2, and let k be the purely transcendental extension $F(x, y, z, w)$ of F ; over this field, the tensor product of quaternion algebras

$$\mathbb{H}(x, y) \otimes_k \mathbb{H}(z, w)$$

is a division algebras by Albert's criteria, and hence has index 4. It has order 2 because each quaternion algebra does. See [mo110441](#).

THE INVOLUTIONS ON AN ALGEBRA

Given a central simple algebra admitting an involution, we next need to understand the set of all involutions of it.

THEOREM 27.48 (NOETHER-SKOLEM). *Let A be a central simple algebra over K , and let $*$ and \dagger be involutions of A that agree on K ; then there exists an $a \in A$ such that*

$$x^* = ax^\dagger a^{-1}, \quad \text{all } x \in A. \quad (190)$$

PROOF. Omitted — it is similar to the proof of (27.22). \square

Let A be a central simple algebra over K , and let \dagger be an involution A , either of the first kind, and so fixing the elements of K , or of the second kind, and so fixing the elements of a subfield k of K such that $[K:k] = 2$. For which invertible a in A does (190) define an involution?

Note that

$$x^{**} = (a^\dagger a^{-1})^{-1} x (a^\dagger a^{-1})$$

and so $a^\dagger a^{-1} \in K$, say

$$a^\dagger = ca, \quad c \in K.$$

Now,

$$a^{\dagger\dagger} = c(c^\dagger a^\dagger) = cc^\dagger \cdot a$$

and so

$$cc^\dagger = 1.$$

If \dagger is of the first kind, this implies that $c^2 = 1$, and so $c = \pm 1$.

If \dagger is of the second kind, this implies that $c = d/d^\dagger$ for some $d \in K$ (Hilbert's theorem 90). Since $*$ is unchanged when we replace a with a/d , we see that in this case (189) holds with a satisfying $a^\dagger = a$.

HERMITIAN AND SKEW-HERMITIAN FORMS

We need some definitions. Let

- ◇ $(D, *)$ be a division algebra with an involution $*$,
- ◇ V be a left vector space over D , and
- ◇ $\phi: V \times V \rightarrow D$ a form on V that is semilinear in the first variable and linear in the second (so

$$\phi(ax, by) = a^* \phi(x, y) b, \quad a, b \in D).$$

Then ϕ is said to **hermitian** if

$$\phi(x, y) = \phi(y, x)^*, \quad x, y \in V,$$

and **skew hermitian** if

$$\phi(x, y) = -\phi(y, x)^*, \quad x, y \in V.$$

EXAMPLE 27.49. (a) Let $D = k$ with $*$ = id_k . In this case, the hermitian and skew hermitian forms are, respectively, symmetric and skew symmetric forms.

(b) Let $D = \mathbb{C}$ with $*$ = complex conjugation. In this case, the hermitian and skew hermitian forms are the usual objects.

To each hermitian or skew-hermitian form, we attach the group of automorphisms of (V, ϕ) , and the special group of automorphisms of ϕ (the automorphisms with determinant 1, if this is not automatic).

THE GROUPS ATTACHED TO ALGEBRAS WITH INVOLUTION

In this subsection, we assume that the ground field k satisfies the condition (27.45), and compute the groups attached to the various possible algebras with involution.

CASE $A = M_n(k)$; INVOLUTION OF THE FIRST KIND.

In this case, the involution $*$ is of the form

$$X^* = aX^t a^{-1}$$

where $a^t = ca$ with $c = \pm 1$. Recall that the group attached to $(M_n(k), *)$ consists of the matrices X satisfying

$$X^* X = I, \quad \det(X) = 1,$$

i.e.,

$$aX^t a^{-1} X = I, \quad \det(X) = 1,$$

or,

$$X^t a^{-1} X = a^{-1}, \quad \det(X) = 1.$$

Thus, when $c = +1$, we get the special orthogonal group for the symmetric bilinear form attached to a^{-1} , and when $c = -1$, we get the symplectic group attached to the skew symmetric bilinear form attached to a^{-1} .

CASE $A = M_n(K)$; INVOLUTION OF THE SECOND KIND

Omitted for the present.

CASE $A = M_n(D)$; D A QUATERNION DIVISION ALGEBRA.

Omitted for the present.

CONCLUSION.

Let k be a field satisfying the condition (27.45). Then the geometrically almost-simple, simply connected, classical groups over k are the following:

- (A) The groups $SL_m(D)$ for D a central division algebra over k (the inner forms of SL_n); the groups attached to a hermitian form for a quadratic field extension K of k (the outer forms of SL_n).
- (BD) The spin groups of quadratic forms, and the spin groups of skew hermitian forms over quaternion division algebras.
- (C) The symplectic groups, and unitary groups of hermitian forms over quaternion division algebras.

It remains to classify the quaternion algebras and the various hermitian and skew hermitian forms. For the algebraically closed fields, the finite fields, \mathbb{R} , \mathbb{Q}_p , \mathbb{Q} and their finite extensions, this has been done, but for \mathbb{Q} and its extensions it is an application of class field theory.

ASIDE 27.50. The term “classical group” is much used, but rarely defined — see the discussion [mo50610](#). Our definition follows [Kneser 1969](#).

e. The Galois cohomology of algebraic groups; applications

Having persuaded the reader of the usefulness of Galois cohomology groups, we now study them in their own right.

GENERALITIES

PROPOSITION 27.51. *Let G be an algebraic group over a finite extension k' of k ; then*

$$H^i(k, (G)_{k'/k}) \simeq H^i(k', G)$$

for $i = 0, 1$ (and for all i if G is commutative).

PROOF. Shapiro's lemma. □

A torus T over a field k is said to be **quasi-trivial** if it is a product of tori of the form $(\mathbb{G}_m)_{k'/k}$ with k' a finite field extension of k . If $T = \prod_i (\mathbb{G}_m)_{k_i/k}$, then

$$H^1(k, T) \simeq \prod_i H^1(k_i, \mathbb{G}_m) = 0.$$

If T is quasi-trivial over k , then $T_{k'}$ is quasi-trivial over k' for all fields $k' \supset k$, and so $H^1(k', T_{k'}) = 0$. There is a converse to this.

THEOREM 27.52. *A torus T over k has the property that $H^1(k', T_{k'}) = 0$ for all fields k' containing k if and only if T is a direct factor of a quasi-trivial torus.*

PROOF. Omitted for the present. □

FINITE FIELDS

Let X be an affine scheme over \mathbb{F}_q . The \mathbb{F}_q -algebra homomorphism $f \mapsto f^q: \mathcal{O}(X) \rightarrow \mathcal{O}(X)$ defines a Frobenius morphism $\sigma: X \rightarrow X$. If $X \subset \mathbb{A}^n$, then σ acts on $X(\mathbb{F})$ by $(a_1, \dots) \mapsto (a_1^q, \dots)$.

DEFINITION 27.53. 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 $G_0 \hookrightarrow \text{GL}_n$, a power F^m of F acts as $(a_1, \dots) \mapsto (a_1^q, \dots)$.

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).

PROPOSITION 27.54. *Let $F: G \rightarrow G$ be a Steinberg endomorphism of a connected group variety G over \mathbb{F} . Then the morphism $g \mapsto g \cdot F(g^{-1}): G \rightarrow G$ 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 (9.10). 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 $\mu_x: G \rightarrow O_x$ over x is finite (A.99), and even that the equation $g^{-1}x F(g) = x$ has only finitely many solutions with g in $G(\mathbb{F})$. Rewrite this equation as $f(g) = g$, where $f(g) = x F(g) x^{-1}$. Because F is a Steinberg endomorphism, some multiple F^m of it is a Frobenius endomorphism fixing x . A direct calculation shows that $f^m(g) = y F^m(g) y^{-1}$ with $y = x F(x) \cdots F^{m-1}(x)$, 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 27.55. *Let G be a connected group variety over a finite field k , and let $F: G \rightarrow G$ be the Frobenius map relative to k . Then the morphism $g \mapsto g \cdot F(g^{-1}): G \rightarrow G$ is surjective.*

PROOF. The proposition shows that the morphism becomes surjective after passage to \mathbb{F} , and hence is surjective. \square

COROLLARY 27.56. *Let G be a connected group variety over a finite field k ; then $H^1(k, G) = 1$.*

PROOF. Let $f: \Gamma \rightarrow G(\mathbb{F})$ be a 1-cocycle. Let σ be the canonical generator of Γ . 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 cocycle defined by g . It follows that the two cocycles agree on all powers of σ , and hence on Γ (by continuity). \square

For nonconnected group varieties, the proposition fails already for $G = \mathbb{Z}/2\mathbb{Z}$.

ASIDE 27.57. Let $F: G \rightarrow G$ 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 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). Apart from quotients of finite groups of Lie type, every nonabelian finite simple group is an alternating group, the Tits group, or one of the 26 sporadic groups.

NOTES. Corollary 27.55 was first proved in Lang (1956). Each of the three statements (27.55–27.56) is referred to as Lang’s theorem. The above proof of (27.54) is from Müller 2003. Steinberg (1977) proves the stronger statement: let σ be an endomorphism of a smooth connected algebraic group G over an algebraically closed k fixing only finitely many elements of $G(k)$; then the morphism $g \mapsto g^{-1}\sigma(g): G \rightarrow G$ is surjective.

THE FIELD OF REAL NUMBERS

THEOREM 27.58 (CARTAN 1927). *Let G be a simply connected semisimple algebraic group over \mathbb{R} . Then $G(\mathbb{R})$ is connected.*

COROLLARY 27.59. *Let G be a reductive algebraic group over \mathbb{R} . Then $G(\mathbb{R})$ has only finitely many components (for the real topology).*

THEOREM 27.60. *Let G be a reductive algebraic group over \mathbb{R} , and let T_0 be a maximal compact torus in G . Then $T = C_G(T_0)$ is a torus, and $W_0 = N_G(T_0)/C_G(T_0)$ is a finite group acting on $H^1(\mathbb{R}, T)$. The map*

$$H^1(\mathbb{R}, T)/W_0(\mathbb{R}) \rightarrow H^1(\mathbb{R}, G)$$

induced by the map $H^1(\mathbb{R}, T) \rightarrow H^1(\mathbb{R}, G)$ is an isomorphism.

PROOF. Borovoi 2014 (arXiv:1401.5913). \square

COROLLARY 27.61 (BOREL AND SERRE 1964). *If G is compact, then*

$$T(\mathbb{R})_2/W \simeq H^1(\mathbb{R}, G)$$

where W is the Weyl group with its usual action.

ASIDE 27.62. Galois cohomology of real semisimple groups. Mikhail Borovoi, Dmitry A. Timashev. arXiv: 1506.06252. Let G be a connected, compact, semisimple algebraic group over \mathbb{R} . Using Kac diagrams, they describe combinatorially the cohomology sets $H^1(\mathbb{R}, H)$ for all inner forms H of G .

LOCAL FIELDS

THEOREM 27.63. *Let G be a semisimple algebraic group over a local field k .*

(a) *Let $\tilde{G} \rightarrow G$ be the simply connected covering of G ; then the boundary map δ in*

$$H^1(k, \tilde{G}) \rightarrow H^1(k, G) \xrightarrow{\delta} H^2(k, Z(\tilde{G}))$$

is surjective (hence bijective).

(b) *If k is nonarchimedean and G is simply connected, then $H^1(k, G) = 1$.*

When k has nonzero characteristic, $H^2(k, Z(\tilde{G}))$ should be taken to be the flat cohomology group (Thăng 2008).

THEOREM 27.64. *Let G be a group variety over a local field k ; then $H^1(k, G)$ is finite.*

THEOREM 27.65. *Let D be a finite-dimensional division algebra over a local field k . Then $\mathrm{SL}_1(D)$ is a simply connected simple anisotropic group over k , and every such algebraic group over k is of this form.*

GLOBAL FIELDS

THEOREM 27.66. *Let G be a semisimple algebraic group over a global field k , and let $\tilde{G} \rightarrow G$ be the simply connected covering of G . Then the boundary map δ in*

$$H^1(k, \tilde{G}) \rightarrow H^1(k, G) \xrightarrow{\delta} H^2(k, Z(\tilde{G}))$$

is surjective.

In the number field case, this was proved in Harder 1975. In the function field case, it is necessary to interpret $H^2(k, Z(\tilde{G}))$ as a flat cohomology group (Thăng 2008).

THEOREM 27.67. *Let G be a semisimple algebraic group over a number field k . The canonical map*

$$H^1(k, G) \rightarrow \prod_v H^1(k_v, G)$$

is injective in each of the following cases:

- (a) *G is simply connected;*
- (b) *G has trivial centre;*
- (c) *$G = O(\phi)$ for some nondegenerate quadratic space (V, ϕ) .*

PROOF. For (a), see Harder 1966 except for the case E_8 , which was proved in Chernousov 1989. Once the case (a) has been proved, (b) and (c) can be proved by writing some exact sequences. \square

Note that (c) implies that two quadratic spaces over \mathbb{Q} are isomorphic if and only if they become isomorphic over \mathbb{Q}_p for all p (including $p = \infty$, for which we set $\mathbb{Q}_p = \mathbb{R}$). This is a very important, and deep result, in number theory.

THEOREM 27.68. *Let G be a simply connected semisimple algebraic group over a number field k . Then*

$$H^1(k, G) \simeq \prod_{v \text{ real}} H^1(k_v, G).$$

PROOF. Combine (27.63) and (27.67). \square

THEOREM 27.69. *Let G be a semisimple algebraic group over a number field k . For any nonarchimedean prime v_0 , the canonical map*

$$H^1(k, G) \rightarrow \prod_{v \neq v_0} H^1(k_v, G)$$

is surjective.

PROOF. This is proved in [Borel and Harder 1978](#), 1.7. \square

Applied to the adjoint group of G , the theorem implies the following statement: 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 of G' of G over k such that $G'_{k_v} \approx G^{(v)}$ for all $v \neq v_0$.

THEOREM 27.70. *Let G be an geometrically almost-simple algebraic 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*

$$H^1(k, \mathcal{A}(G)) \rightarrow \prod_{v \in S} H^1(k_v, \mathcal{A}(G))$$

is surjective.

PROOF. [Borel and Harder 1978](#), Theorem B. See also [Prasad and Rapinchuk 2006](#) and [Tháng 2012](#). \square

In other words, given a k_v -form G_v of G_{k_v} for each $v \in S$, there exists a form of G' of G over k such that $G'_{k_v} \approx G_v$ for all $v \in S$.

THEOREM 27.71. *Let G be a reductive group over a number field k . If the derived group G' of G is simply connected and the torus $T = G/G'$ satisfies the Hasse principal for H^1 , then so also does G .*

PROOF. Diagram chase in

$$\begin{array}{ccccccc} T(k) & \longrightarrow & H^1(k, G') & \longrightarrow & H^1(k, G) & \longrightarrow & H^1(T) \\ & & \downarrow & & \downarrow & & \downarrow \\ G(\mathbb{R}) & \longrightarrow & T(\mathbb{R}) & \longrightarrow & \prod_v H^1(k_v, G) & \longrightarrow & \prod_v H^1(k_v, T) \end{array}$$

using that $T(\mathbb{Q})$ is dense in $T(\mathbb{R})$. \square

ASIDE 27.72. Every reductive group G over a local field k comes from a reductive group over a number field $k_0 \subset k$. See [mo199050](#).

NOTES. For more on the cohomology of algebraic groups, see [Kneser 1969](#) and [Platonov and Rapinchuk 1994](#).

To be continued.

Review of algebraic geometry

This is a list of the definitions and results from algebraic geometry used in the text. For the final version, irrelevant items will be deleted. I intend (eventually) to rewrite “Chapter 10” of my notes *Algebraic Geometry* to include proofs of all the statements here.

Throughout this appendix, everything takes place over a fixed field k , and “ k -algebra” means “finitely generated k -algebra”.

a. Affine algebraic schemes

Let A be 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
- ◇ $Z(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} \mathfrak{a}_i$ 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 $f \in \mathfrak{a} \setminus \mathfrak{m}$ and $g \in \mathfrak{b} \setminus \mathfrak{m}$; but then $fg \notin \mathfrak{a}\mathfrak{b} \setminus \mathfrak{m}$, 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 $\text{spm}(A)$ for X endowed with this topology.

For example, $\mathbb{A}^n \stackrel{\text{def}}{=} \text{spm}(k[T_1, \dots, T_n])$ 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 $\text{spm}(A)$, 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} . 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 $\text{spm}(A)$ because its complement is the closed set $Z((f))$. The sets of this form are called the **basic open subsets** of $\text{spm}(A)$. Let $Z = Z(\mathfrak{a})$ be a closed subset of $\text{spm}(A)$. According to the Hilbert basis theorem, A is noetherian, and so $\mathfrak{a} = (f_1, \dots, f_m)$ for some $f_i \in A$, and

$$X \setminus Z = D(f_1) \cup \dots \cup D(f_m).$$

This shows that every open subset of $\text{spm}(A)$ is a finite union of basic open subsets. In particular, the basic open subsets form a base for the Zariski topology on $\text{spm}(A)$.

A.4. Let $\alpha: A \rightarrow B$ 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). 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

$$\alpha^*: \text{spm}(B) \rightarrow \text{spm}(A), \quad \mathfrak{m} \mapsto \alpha^{-1}(\mathfrak{m}),$$

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, $S_f \stackrel{\text{def}}{=} \{1, f, f^2, \dots\}$, and

$$A_f \stackrel{\text{def}}{=} S_f^{-1}A \simeq A[T]/(1 - fT).$$

Let D be a basic open subset of X . Then

$$S_D \stackrel{\text{def}}{=} A \setminus \bigcup \{\mathfrak{m} \mid \mathfrak{m} \in D\}$$

is a multiplicative subset of A . If $D = D(f)$, then the map $S_f^{-1}A \rightarrow S_D^{-1}A$ 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

$$S_D^{-1}A \rightarrow S_{D'}^{-1}A. \quad (191)$$

A.6. There is a unique sheaf \mathcal{O}_X of k -algebras on $X = \text{Spm}(A)$ such that (a)

$$\mathcal{O}_X(D) = S_D^{-1}A$$

for every basic open subset D of X , and (b) the restriction map

$$\mathcal{O}_X(D) \rightarrow \mathcal{O}_X(D')$$

is the map (191) 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

$$\text{Hom}(A, B) \simeq \text{Hom}(\text{Spm}(B), \text{Spm}(A))$$

for all k -algebras A and B .

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 (a) $\mathcal{M}(D) = S_D^{-1}M$ for every basic open subset D of X , and (b) the restriction map $\mathcal{M}(D) \rightarrow \mathcal{M}(D')$ is the canonical map $S_D^{-1}M \rightarrow S_{D'}^{-1}M$ 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, which has 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 12.5).

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 $S = Z(f_1, \dots, f_m)$ with the $f_i \in k[X_1, \dots, X_n]$. Then

$$S = k^n \cap \{\text{zero set of } f_1, \dots, f_m \text{ in } K^n\}.$$

(b) Let $T = Z(f_1, \dots, f_m)$ with the $f_i \in K[X_1, \dots, X_n]$. 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 $f_{ij} \in k[X_1, \dots, X_n]$. 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 . An **algebraic scheme over k** is a k -ringed space (X, \mathcal{O}_X) that admits a finite covering by open affines. 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 $\kappa(x)$.

A.12. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes is said to be **surjective** (resp. **injective**, **open**, **closed**) if the map of topological spaces $|\varphi|: |Y| \rightarrow |X|$ is surjective (resp. injective, open, closed) (EGA I, 2.3.3).

A.13. Let X be an algebraic scheme over k , and let A be a k -algebra. By definition, a morphism $\varphi: X \rightarrow \text{Spm}(A)$ gives a homomorphism $\varphi^\sharp: A \rightarrow \mathcal{O}_X(X)$ of k -algebras (but $\mathcal{O}_X(X)$ need not be finitely generated!). In this way, we get an isomorphism

$$\varphi \leftrightarrow \varphi^\sharp: \text{Hom}_k(X, \text{Spm } A) \simeq \text{Hom}_k(A, \mathcal{O}_X(X)). \tag{192}$$

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 $\{W_1, \dots, W_r\}$ is uniquely determined, and its elements are called the **irreducible components** of X .

A noetherian topological space has only finitely many connected components, each open and closed, and it is a disjoint union of them.

A.15. (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 $X = \text{Spm}(A)$, then $X_K = \text{Spm}(K \otimes A)$.

A.16. 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 ,

$$X(R) \stackrel{\text{def}}{=} \text{Hom}(\text{Spm}(R), X).$$

For example, if $X = \text{Spm}(A)$, then $X(R) = \text{Hom}(A, R)$ (homomorphisms of k -algebras).

For a ring R containing k , we define

$$X(R) = \varinjlim X(R_i)$$

where R_i runs over the (finitely generated) k -subalgebras of R . Again $X(R) = \text{Hom}_k(A, R)$ if $X = \text{Spm}(A)$. Then $R \rightsquigarrow X(R)$ is functor from k -algebras (not necessarily finitely generated) to sets.

A.17. 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 $\mathcal{O}_X(U)$.

c. Subschemes

A.18. 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.19. Let $X = \text{Spm}(A)$ be an affine algebraic scheme over k , and let \mathfrak{a} be an ideal in A . Then $\text{Spm}(A/\mathfrak{a})$ 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 $(Z, (\mathcal{O}_X/\mathcal{I})|_Z)$ 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 affines, $Z = \bigcup U_i$. For each i , the chain $Z \cap U_i \supset Z_1 \cap U_i \supset \dots$ 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.20. 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.21. A regular map $\varphi: Y \rightarrow X$ is said to be 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**. An immersion can be written as a closed immersion into an open subscheme (and as an open immersion into a closed subscheme).

A.22. 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 said to be **reduced** if $\mathcal{O}_{X,P}$ is reduced for all $P \in X$. For example, $\text{Spm}(A)$ is reduced if and only if A is reduced. If \mathcal{O}_X is reduced, then $\mathcal{O}_X(U)$ is reduced for all open affine subsets U of X .

A.23. A finitely generated k -algebra A is reduced if and only if the intersection of the maximal ideals in A is zero (CA 13.10). 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). Let X be a reduced algebraic scheme; an $f \in \mathcal{O}_X(U)$ is 0 if $f(u) = 0$ for all $u \in |U|$; when k is algebraically closed, $\kappa(x) = k$ for all $x \in |X|$, and so \mathcal{O}_X can be identified with a sheaf of functions on X .

A.24. An algebraic scheme X is said to be **integral** if it is reduced and irreducible. For example, $\text{Spm}(A)$ 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.25. 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 $X = \text{Spm}(A)$, then $X_{\text{red}} = \text{Spm}(A/\mathfrak{N})$ where \mathfrak{N} is the nilradical of A .

Every regular map $Y \rightarrow X$ from a reduced scheme Y to X factors uniquely through the inclusion map $i: X_{\text{red}} \rightarrow X$. In particular,

$$X_{\text{red}}(R) \simeq X(R) \tag{193}$$

if R is a reduced k -algebra, for example, a field.

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 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 $X_{k^{\text{al}}}$ being reduced.

d. Algebraic schemes as functors

A.26. Recall that Alg_k is the category of *finitely generated* k -algebras. For a k -algebra A , let h^A denote the functor $R \rightsquigarrow \text{Hom}(A, R)$ from k -algebras to sets. A functor $F: \text{Alg}_k \rightarrow \text{Set}$

is said to be **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

$$T_a: h^A \rightarrow F, \quad (T_a)_R(f) = F(f)(a),$$

is an isomorphism. This means that, for each $x \in F(R)$, there is a unique homomorphism $A \rightarrow R$ such that $F(A) \rightarrow F(R)$ 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 $A \rightarrow A'$ sending a to a' .

A.27. (Yoneda lemma) Let B be a k -algebra and let F be a functor $\text{Alg}_k \rightarrow \text{Set}$. An element $x \in F(B)$ defines a homomorphism

$$\text{Hom}(B, R) \rightarrow F(R)$$

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

$$F(B) \rightarrow \text{Nat}(h^B, F).$$

The Yoneda lemma says that this is a bijection, natural in both B and F . For $F = h^A$, this says that

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

In other words, the contravariant functor $A \mapsto h^A$ is fully faithful. Its essential image consists of the representable functors.

A.28. Let h_X denote the functor $\text{Hom}(-, X)$ from algebraic schemes over k to sets. The Yoneda lemma in this situation says that, for algebraic schemes X, Y ,

$$\text{Hom}(X, Y) \simeq \text{Nat}(h_X, h_Y).$$

Let h_X^{aff} denote the functor $R \mapsto X(R): \text{Alg}_k \rightarrow \text{Set}$. Then $h_X^{\text{aff}} = h_X \circ \text{Spm}$, 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 $h_X^{\text{aff}} \rightarrow h_Y^{\text{aff}}$ extends uniquely to a natural transformation $h_X \rightarrow h_Y$,

$$\text{Nat}(h_X^{\text{aff}}, h_Y^{\text{aff}}) \simeq \text{Nat}(h_X, h_Y),$$

and so

$$\text{Hom}(X, Y) \simeq \text{Nat}(h_X^{\text{aff}}, h_Y^{\text{aff}}).$$

In other words, the functor $X \mapsto h_X^{\text{aff}}$ 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” $\text{Alg}_k \rightarrow \text{Set}$.

Fix a family $(T_i)_{i \in \mathbb{N}}$ of symbols indexed by the elements of \mathbb{N} , and let Alg_k^0 denote the full subcategory of Alg_k of objects of the form $k[T_0, \dots, T_n]/\mathfrak{a}$ for some $n \in \mathbb{N}$ and ideal \mathfrak{a} in $k[T_0, \dots, T_n]$. The inclusion $\text{Alg}_k^0 \hookrightarrow \text{Alg}_k$ is an equivalence of categories, but the objects of Alg_k^0 form a set, and so the set-valued functors on Alg_k^0 form a category. We call the objects of Alg_k^0 **small** k -algebras. We let \tilde{X} denote the functor $\text{Alg}_k^0 \rightarrow \text{Set}$ defined by an algebraic scheme. Then $X \mapsto \tilde{X}$ is fully faithful. We shall also refer to this statement as the *Yoneda lemma*.

Let F be a functor $\text{Alg}_k^0 \rightarrow \text{Set}$. If F is representable by an algebraic scheme X , then X is uniquely determined up to a unique isomorphism, and X extends F to a functor $\text{Alg}_k \rightarrow \text{Set}$.

A.29. By a functor in this paragraph we mean a functor $\text{Alg}_k^0 \rightarrow \text{Set}$. A subfunctor U of a functor X is **open** if, for all maps $\varphi: h^A \rightarrow X$, the subfunctor $\varphi^{-1}(U)$ of h^A is defined by an open subscheme of $\text{Spm}(A)$. 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

$$X(R) \rightarrow \prod_i X(R_{f_i}) \rightrightarrows \prod_{i,j} X(R_{f_i f_j})$$

is exact.

Let \mathbb{A}^1 denote the functor sending a k -algebra R to its underlying set. For a functor U , let $\mathcal{O}(U) = \text{Hom}(U, \mathbb{A}^1)$ — it is a k -algebra.¹ A functor U is **affine** if $\mathcal{O}(U)$ is finitely generated and the canonical map $U \rightarrow h^{\mathcal{O}(U)}$ is an isomorphism. A local functor admitting a finite covering by open affines is representable by an algebraic scheme (i.e., it is of the form \tilde{X} for an algebraic scheme X).²

A.30. Let

$$P^n(R) = \{\text{direct summands of rank 1 of } R^{n+1}\}.$$

Then P^n is a functor $\text{Alg}_k^0 \rightarrow \text{Set}$. One can show that the functor P^n is local in the sense of (A.29). 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 (A.29). We denote it by \mathbb{P}^n . When K is a field, every K -subspace of K^{n+1} is a direct summand, and so $\mathbb{P}^n(K)$ consists of the lines through the origin in K^{n+1} .

A.31. A morphism $\varphi: X \rightarrow Y$ 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, p10). Let $\varphi: X \rightarrow Y$ be a regular map of algebraic schemes. If $\tilde{X} \rightarrow \tilde{Y}$ is a monomorphism, then it is injective (ibid. 5.1, p.24). If X is irreducible and $\tilde{X} \rightarrow \tilde{Y}$ is a monomorphism, then there exists a dense open subset U of X such that $\varphi|_U$ is an immersion.

A.32. Let R be a k -algebra (finitely generated as always). An **algebraic R -scheme** is a pair (X, φ) consisting of an algebraic k -scheme X and a morphism $\varphi: X \rightarrow \text{Spm}(R)$. For example, if $f: R \rightarrow R'$ is a finitely generated R -algebra, then $\text{Spm}(f): \text{Spm}(R') \rightarrow \text{Spm}(R)$ 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 h_X denote the functor sending a small R -algebra R' to $\text{Hom}_R(\text{Spm}(R'), X)$; then $X \rightsquigarrow h_X$ is fully faithful.

ASIDE A.33. Originally algebraic geometers considered algebraic varieties X over algebraically closed fields k . Here it sufficed to consider the set $X(k)$ of k -points. Later algebraic geometers considered algebraic varieties X over arbitrary fields k . Here $X(k)$ doesn't tell you much about X (it is often empty), and so people worked with $X(K)$ where K is some (large) algebraically closed field containing k . For algebraic schemes, even $X(K)$ is inadequate because it doesn't detect nilpotents. This suggests that we consider $X(R)$ for all k -algebras, i.e., we consider the functor $\tilde{X}: R \rightsquigarrow X(R)$ defined by X . This certainly determines X but leads to set-theoretic difficulties — putting a condition on \tilde{X} involves quantifying over a proper class, and, in general, the natural transformations from one functor on k -algebras to a second functor form a proper class. These difficulties vanish when we consider the functor of *small* k -algebras defined by X . From our point-of-view, an algebraic scheme over k is determined by the functor it defines on *small* k -algebras, and it defines a functor on *all* k -algebras.

¹Here 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.

²This is the *definition* of a scheme in DG I, §1, 3.11, p.12.

e. Fibred products of algebraic schemes

A.34. Let $\varphi: X \rightarrow Z$ and $\psi: Y \rightarrow Z$ be regular maps of algebraic schemes over k . Then the functor

$$R \mapsto X(R) \times_{Z(R)} Y(R) \stackrel{\text{def}}{=} \{(x, y) \in X(R) \times Y(R) \mid \varphi(x) = \psi(y)\}$$

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

$$\begin{array}{ccc} X \times_Z Y & \longrightarrow & Y \\ \downarrow & & \downarrow \psi \\ X & \xrightarrow{\varphi} & Z. \end{array}$$

is cartesian. For example, if $R \rightarrow A$ and $R \rightarrow B$ are homomorphisms of k -algebras, then $A \otimes_R B$ is a finitely generated k -algebra, and

$$\text{Spm}(A) \times_{\text{Spm}(R)} \text{Spm}(B) = \text{Spm}(A \otimes_R B).$$

When φ and ψ are the structure maps $X \rightarrow \text{Spm}(k)$ and $Y \rightarrow \text{Spm}(k)$, the fibred product becomes the product, denoted $X \times Y$, and

$$\text{Hom}(T, X \times Y) \simeq \text{Hom}(T, X) \times \text{Hom}(T, Y).$$

The diagonal map $\Delta_X: X \rightarrow X \times X$ is the regular map whose composites with the projection maps equal the identity map of X .

The fibre $\varphi^{-1}(x)$ over x of a regular map $\varphi: Y \rightarrow X$ of algebraic schemes is defined to be the fibred product:

$$\begin{array}{ccc} Y & \longleftarrow & Y \times_X x \stackrel{\text{def}}{=} \varphi^{-1}(x) \\ \downarrow \varphi & & \downarrow \\ X & \longleftarrow & x = \text{Spm}(\kappa(x)). \end{array}$$

Thus, it is an algebraic scheme over the field $\kappa(x)$, which need not be reduced even if both X and Y are reduced.

A.35. For a pair of regular maps $\varphi_1, \varphi_2: X \rightarrow Y$, the functor

$$R \mapsto \{x \in X(R) \mid \varphi_1(x) = \varphi_2(x)\}$$

is represented by the fibred product. The subscheme $X \times_{Y \times Y} X$ of X is called the **equalizer** $\text{Eq}(\varphi_1, \varphi_2)$ of φ_1 and φ_2 . Its underlying set is $\{x \in X \mid \varphi_1(x) = \varphi_2(x)\}$.

A.36. 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 $X = \text{Spm}(A)$, $Z_1 = \text{Spm}(A/\mathfrak{a}_1)$, and $Z_2 = \text{Spm}(A/\mathfrak{a}_2)$, then $Z_1 \cap Z_2 = \text{Spm}(A/\mathfrak{a}_1 + \mathfrak{a}_2)$. 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.19), every infinite intersection is equal to a finite intersection.

f. Algebraic varieties

A.37. An algebraic scheme X over k is said to be *separated* if it satisfies the following equivalent conditions:

- (a) the diagonal in $X \times X$ is closed (so Δ_X is a *closed* immersion);
- (b) for every pair of regular maps $\varphi_1, \varphi_2: Y \rightarrow X$, the subset of $|Y|$ on which φ_1 and φ_2 agree is closed (so $\text{Eq}(\varphi_1, \varphi_2)$ is a *closed* subscheme of Y);
- (c) for every pair of open affine subsets U, U' in X , the intersection $U \cap U'$ is an open affine subset of X , and the map

$$f \otimes g \mapsto f|_{U \cap U'} \cdot g|_{U \cap U'}: \mathcal{O}_X(U) \otimes \mathcal{O}_X(U) \rightarrow \mathcal{O}_X(U \cap U')$$

is surjective.

A.38. An *affine* k -algebra³ is a k -algebra A such that $k^{\text{al}} \otimes A$ 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. When k is a perfect field, every reduced k -algebra is affine.

A.39. An algebraic scheme X is said to be *geometrically reduced* if $X_{k^{\text{al}}}$ is reduced. For example, $\text{Spm}(A)$ 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.38).

A.40. 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,

$$\begin{array}{ccc} \mathbb{A}^1 & \longleftarrow & \mathbb{A}^1 \times_{\mathbb{A}^1} \{a\} = \text{Spm}(k[T]/(T^p - a)) \\ x \mapsto x^p \downarrow & & \downarrow \\ \mathbb{A}^1 & \longleftarrow & \{a\}. \end{array}$$

This is one reason for working with algebraic schemes.

g. The dimension of an algebraic scheme

A.41. Let A be a noetherian ring (not necessarily a k -algebra). 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, \dots, a_m) ; then

$$\text{height}(\mathfrak{p}) \leq m.$$

³Sometimes an affine k -algebra is defined to be a reduced finitely generated k -algebra because these are exactly the ring of functions on an algebraic subset of k^n (e.g., Eisenbud 1995, p.35). However, this class of rings is not closed under the formation of tensor products or extension of the base field.

Conversely, if $\text{height}(\mathfrak{p}) = m$, then there exist $a_1, \dots, a_m \in \mathfrak{p}$ such that \mathfrak{p} is minimal among the prime ideals containing (a_1, \dots, a_m) .

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 are obviously the same). Clearly, the dimension of a local ring with maximal ideal \mathfrak{m} is the height of \mathfrak{m} , and for a general noetherian ring A ,

$$\dim(A) = \sup(\dim(A_{\mathfrak{m}})).$$

Since all prime ideals of A contain the nilradical \mathfrak{N} of A , we have

$$\dim(A) = \dim(A/\mathfrak{N}).$$

A.42. 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 $k[t_1, \dots, t_r]$ such that A is a finitely generated $k[t_1, \dots, t_r]$ -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 $\text{tr deg}_k(A)$. In particular, every maximal ideal in A has height $\text{tr deg}_k(A)$, and so A has dimension $\text{tr deg}_k(A)$.

A.43. Let X be an irreducible algebraic scheme over k . The **dimension** of X is the length of a maximal chain of irreducible closed subschemes

$$Z = Z_d \subset \dots \subset Z_1 \subset Z_0.$$

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 .

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.44. Let X an irreducible algebraic variety. Then there exists a transcendence basis t_1, \dots, t_d for $k(X)$ over k such that $k(X)$ is separable over $k(t_1, \dots, t_d)$ (such a basis is called a **separating transcendence basis**, and $k(X)$ is said to be **separably generated** over k). This means that X is birationally equivalent to a hypersurface $f(T_1, \dots, T_{d+1})$, $d = \dim X$, such 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.45. Let A be a noetherian local ring with maximal ideal \mathfrak{m} (not necessarily a k -algebra). Then the dimension of A is the height of \mathfrak{m} , and so (A.42),

$$\dim A \leq \text{minimum number of generators for } \mathfrak{m}.$$

When equality holds, A is said to be **regular**. The Nakayama lemma shows that a set of elements of \mathfrak{m} generates \mathfrak{m} if and only if it spans the k -vector space $\mathfrak{m}/\mathfrak{m}^2$, where $k = A/\mathfrak{m}$. Therefore

$$\dim(A) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$$

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.

A.46. 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 (i.e., reduced and irreducible), but not necessarily geometrically reduced.

A.47. 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 $\varepsilon \mapsto 0: k[\varepsilon] \rightarrow k$, we get a map

$$X(k[\varepsilon]) \rightarrow X(k).$$

The fibre of this over a point $x \in X(k)$ is the **tangent space** $T_x(X)$ of X at x . Thus $T_x(X)$ is defined for all $x \in |X|$ with $\kappa(x) = k$. To give a tangent vector at x amounts to giving a local homomorphism $\alpha: \mathcal{O}_{X,x} \rightarrow k[\varepsilon]$ 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 $\mathcal{O}_x \rightarrow k$, which induces a k -linear map $\mathfrak{m}/\mathfrak{m}^2 \rightarrow k$. In this way, we get canonical isomorphisms

$$T_x(X) \simeq \text{Der}_k(\mathcal{O}_x, k) \simeq \text{Hom}_{k\text{-linear}}(\mathfrak{m}/\mathfrak{m}^2, k). \quad (194)$$

The formation of the tangent space commutes with extension of the base field:

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

A.48. Let X be an irreducible algebraic scheme over k , and let x be a point on X such that $\kappa(x) = k$. Then

$$\dim T_x(X) \geq \dim X$$

with equality if and only if x is regular. This follows from (4.17).

A.49. Let X be a closed subscheme of \mathbb{A}^n , say

$$X = \text{Spm } A, \quad A = k[T_1, \dots, T_n]/\mathfrak{a}, \quad \mathfrak{a} = \mathfrak{a} = (f_1, \dots, f_r).$$

Consider the Jacobian matrix

$$\text{Jac}(f_1, f_2, \dots, f_r) = \begin{pmatrix} \frac{\partial f_1}{\partial t_1} & \frac{\partial f_1}{\partial t_2} & \cdots & \frac{\partial f_1}{\partial t_n} \\ \frac{\partial f_2}{\partial t_1} & & & \\ \vdots & & & \\ \frac{\partial f_r}{\partial t_1} & & & \frac{\partial f_r}{\partial t_n} \end{pmatrix} \in M_{r,n}(A).$$

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.

For example, if X is the hypersurface defined by a polynomial $f(T_1, \dots, T_{d+1})$, then

$$\text{Jac}(f) = \left(\frac{\partial f}{\partial t_1} \quad \frac{\partial f}{\partial t_2} \quad \cdots \quad \frac{\partial f}{\partial t_{d+1}} \right) \in M_{1,d+1}(A),$$

and X_{sing} is the closed subscheme of X defined by the equations

$$\frac{\partial f}{\partial T_1} = 0, \dots, \frac{\partial f}{\partial T_{d+1}} = 0.$$

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 U of X and affine embedding of U .

From its definition, one sees that the formation of the singular locus commutes with extension of the base field.

A.50. Let $\Omega_{X/k}$ be the sheaf of differentials on an algebraic scheme X over k . Then $\Omega_{X/k}$ is locally free of rank $\dim(X)$ (exactly) over an open subset U of X . The complement of U is X_{sing} .

A.51. 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.52. Let X be geometrically reduced and irreducible. Then X is birationally equivalent to a hypersurface $f(T_1, \dots, T_{d+1}) = 0$ with $\partial f / \partial T_{d+1} \neq 0$ (see A37). It follows that the singular locus of X is not the whole of X (A.49).

A.53. 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 $X(R) \rightarrow X(R/I)$ is surjective (DG I, §4, 4.6, p.111).

i. Galois descent for closed subschemes

A.54. Let $\Omega \supset k$ be an extension of fields, and let $\Gamma = \text{Aut}(\Omega/k)$. Assume that $\Omega^\Gamma = k$. This is true, for example, if Ω is a Galois extension of k . Then the functor $V \rightsquigarrow \Omega \otimes_k V$ from vector spaces over k to vector spaces over Ω equipped with a continuous action of Γ is an equivalence of categories.

A.55. 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').

Let $\Gamma = \text{Aut}(k'/k)$, and assume that $k'^\Gamma = k$. Then Y' arises from an algebraic subscheme of X if and only if it is stable under the action of Γ on X' . When X and Y' are affine, say, $X = \text{Spm}(A)$ and $Y' = \text{Spm}(A_{k'}/\mathfrak{a})$, to say that Y' is stable under the action of Γ means that \mathfrak{a} is stable under the action of Γ on $A_{k'} \stackrel{\text{def}}{=} A \otimes k'$. More generally, it means that the ideal defining Y' in $\mathcal{O}_{X'}$ is stable under the action of Γ on $\mathcal{O}_{X'}$.

Let $k' = k^{\text{sep}}$. 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 $X(k')$.

A.56. 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 $\varphi': X' \rightarrow Y'$ 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.55) to it. We deduce:

- ◇ There exists at most one regular map $\varphi: X \rightarrow Y$ such that $\varphi' = \varphi_{k'}$.
- ◇ Let $\Gamma = \text{Aut}(k'/k)$, and assume that $k'^\Gamma = k$. Then $\varphi': X' \rightarrow Y'$ 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 $k' = k^{\text{sep}}$, and assume that X and Y are algebraic varieties. Then φ' arises from a regular map over k if and only if the map

$$\varphi'(k'): X(k') \rightarrow Y(k')$$

commutes with the actions of Γ on $X(k')$ and $Y(k')$.

j. On the density of points

A.57. 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. In other words, $X(k')$ is dense in X if, for Z a closed subscheme of X ,

$$Z(k') = X(k') \implies Z = X \text{ (hence } Z(R) = X(R) \text{ for all } R).$$

A.58. If $X(k')$ is dense in X , then a regular map from X to a separated algebraic scheme is determined by its action on $X(k')$. Indeed, let φ_1, φ_2 be regular maps from X to a separated scheme Z . If φ_1 and φ_2 agree on $X(k')$, then their equalizer E is a closed subscheme of X with the property that $E(k') = X(k')$, and so $E = X$. This means that $\varphi_1 = \varphi_2$.

A.59. If $X(k')$ is dense in X , then X is reduced. Indeed, X_{red} is a closed subscheme of X such that $X_{\text{red}}(k') = X(k')$.

A.60. Assume that X is geometrically reduced. Then $X(k')$ is dense in X if the set $X(k')$ is dense in $|X_{k'}|$. Indeed, let Z be a closed subscheme of X such that $Z(k') = X(k')$. Because $X(k')$ is dense in $|X_{k'}|$, we have that $|Z_{k'}| = |X_{k'}|$ and, because $X_{k'}$ is reduced, we have that $Z_{k'} = X_{k'}$. This implies that $Z = X$ (A.55).

A.61. If X is geometrically reduced, then $X(k^{\text{sep}})$ is dense in X (see A.44).

SCHEMATICALLY DENSE SETS OF POINTS

Throughout, X is an algebraic scheme over a field k . Recall that we identify $X(k)$ with the set of $x \in |X|$ such that $\kappa(x) = k$. For a section f of \mathcal{O}_X over an open subset U of X and an $x \in U$, we write $f(x)$ for the image of f in $\kappa(x)$.

DEFINITION A.62. Let S be a subset of $X(k) \subset |X|$. Then S is **schematically dense**⁴ in X if the family of homomorphisms

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

is injective.

Concretely, the condition means that, for every open subset U of X , the family of maps

$$f \mapsto f(s): \mathcal{O}(U) \rightarrow \kappa(s) = k, \quad s \in S \cap U(k),$$

is injective. Clearly, this last condition is local: let $X = \bigcup_i U_i$ be an open covering of X ; a subset S of $X(k)$ is schematically dense if and only if $S \cap U_i(k)$ is schematically dense in U_i for each i .

EXAMPLE A.63. A subset S of $\mathbb{A}^1(k) = k$ is schematically dense if and only if it is infinite (because a nonzero polynomial $f(T)$ has only finitely many roots).

PROPOSITION A.64. Let S be a schematically dense subset of $X(k)$.

- (a) If Z is a closed subscheme of X such that $Z(k)$ contains S , then $Z = X$; in particular, X is reduced.

⁴This says that the family of subschemes $s \subset X$, $s \in S$, is schematically dense in the sense of EGA IV, 11.10.2.

(b) If $u, v: X \rightrightarrows Y$ is a pair of regular maps from X to a separated algebraic scheme Y over k such that $u(s) = v(s)$ for all $s \in S$, then $u = v$.

PROOF. (a). Because Z is a closed subscheme of X , the canonical homomorphism $\mathcal{O}_X \rightarrow \mathcal{O}_Z$ is surjective. Because $S \subset Z(k)$, the maps $f \mapsto f(s): \mathcal{O}_X \rightarrow \kappa(s)$, $s \in S$, factor through \mathcal{O}_Z , and so the map $\mathcal{O}_X \rightarrow \mathcal{O}_Z$ is also injective. Hence $Z = X$. In particular, $X_{\text{red}} = X$, and so X is reduced.

(b) Because Y is separated, the equalizer E of u and v is a closed subscheme of X . The condition $u(s) = v(s)$ for $s \in S$ implies that $E(k) \supset S$, and so $|E| = |X|$. As X is reduced, this implies that $E = X$. \square

PROPOSITION A.65. A subset S of $X(k)$ is schematically dense if and only if X is reduced and S is dense in $|X|$.

PROOF. \Rightarrow : Let Z denote the (unique) reduced closed subscheme of X such that $|Z|$ is the closure of S . Then $Z = X$ by (A.64a), and so X is reduced and $|Z| = |X|$.

\Leftarrow : Let U be an open affine in 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. \square

PROPOSITION A.66. A schematically dense subset remains schematically dense under extension of the base field.

PROOF. Let k' be a field containing k , and use a prime to denote base change $k \rightarrow k'$. For $x \in X(k)$, the map $\mathcal{O}_{X'} \rightarrow \kappa(x')$ is obtained from $\mathcal{O}_X \rightarrow \kappa(x)$ by tensoring with k' . Therefore, the family obtained by letting x run over schematically dense subset S of $X(k)$ is injective (because $k \rightarrow k'$ is flat). \square

COROLLARY A.67. If X admits a schematically dense subset $S \subset X(k)$, then it is geometrically reduced.

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

k. Schematically dominant maps

A.68. The image of a regular map $Y \rightarrow X$ of algebraic schemes is constructible; therefore it contains a dense open subset of its closure. The image of a dominant map $Y \rightarrow X$ of algebraic schemes contains a dense open subset of X .

A.69. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes is said to be **dominant** if $\varphi(|Y|)$ is dense in $|X|$, and **schematically dominant** if the canonical map $\mathcal{O}_X \rightarrow \varphi_* \mathcal{O}_Y$ is injective. Similarly, a family $\varphi_i: Y_i \rightarrow X$, $i \in I$, of regular maps is **schematically dominant** if the family of homomorphisms $\mathcal{O}_X \rightarrow \varphi_{i*}(\mathcal{O}_{Y_i})$ is injective.

For example, a subset S of $X(k)$ is schematically dense in X if and only if the family of maps $s \rightarrow X$, $s \in S$, is schematically dominant. The statements (A.64–A.67) and their proofs extend without difficulty to the situation of (A.69).

A.70. If the family of maps $\varphi_i: Y_i \rightarrow X$, $i \in I$, 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 (φ_i) is schematically dominant. A schematically dominant family of regular maps remains schematically dominant under extension of the base field. If the family $\varphi_i: Y_i \rightarrow X$ is schematically dominant, and the Y_i are geometrically reduced, then so also is X .

l. Separated maps; affine maps

A.71. For a regular map $\varphi: X \rightarrow S$ of algebraic schemes over k , the subscheme $\Delta_{X/S}$ of $X \times_S X$ is defined to be the equalizer of the two projection maps $\Delta_X \rightrightarrows S$. The map φ is said to be **separated** if $\Delta_{X/S}$ is a closed subscheme of $X \times_S X$. For example, let X be an algebraic scheme over k ; then $\Delta_{X/\mathrm{Spm}(k)} = \Delta_X$, and so the structure map $X \rightarrow \mathrm{Spm}(k)$ is separated if and only if X is separated.

A.72. A regular map $\varphi: X \rightarrow S$ is separated if there exists an open covering $S = \bigcup S_i$ of S such that $\varphi^{-1}(S_i) \xrightarrow{\varphi} S_i$ is separated for all i .

A.73. A regular map $\varphi: X \rightarrow S$ is separated if X and S are separated. (As X is separated, the diagonal Δ_X in $X \times X$ is closed; as S is separated, the equalizer of the projections $\Delta_X \rightrightarrows S$ is closed).

A.74. A regular map $\varphi: X \rightarrow S$ is said to be **affine** if, for all open affines U in S , $\varphi^{-1}(U)$ is an open affine in X .

A.75. Every affine map is separated. (A map of affines is separated (A.73), and so this follows from (A.72).)

m. Finite schemes

A.76. A k -algebra is finite if and only if it has Krull dimension zero, i.e., every prime ideal is maximal.

A.77. Let A be a finite k -algebra. For any finite set S of maximal ideals in A , the Chinese remainder theorem shows that the map $A \rightarrow \prod_{\mathfrak{m} \in S} A/\mathfrak{m}$ is surjective with kernel $\bigcap_{\mathfrak{m} \in S} \mathfrak{m}$. In particular, $|S| \leq [A:k]$, and so A has only finitely many maximal ideals. If S is the set of all maximal ideals in A , then $\bigcap_{\mathfrak{m} \in S} \mathfrak{m}$ is the nilradical \mathfrak{N} of A (A.76), and so A/\mathfrak{N} is a finite product of fields.

A.78. An algebraic scheme X over k is **finite** if it satisfies the following equivalent conditions:

- ◇ X is affine and $\mathcal{O}_X(X)$ is a finite k -algebra;
- ◇ X has dimension zero;
- ◇ $|X|$ is finite and discrete.

n. Finite algebraic varieties (étale schemes)

A.79. A k -algebra A is **diagonalizable** if it is isomorphic to the product algebra k^n for some $n \in \mathbb{N}$, and it is **étale** if $k' \otimes A$ is diagonalizable for some field k' containing k . In particular, an étale k -algebra is finite.

A.80. 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) $k' \otimes A$ is reduced for all fields k' containing k (i.e., A is an affine k -algebra);
- (d) $k^{\text{sep}} \otimes A$ is diagonalizable.

A.81. Finite products, tensor products, and quotients of diagonalizable (resp. étale) k -algebras are diagonalizable (resp. étale). The composite of any finite set of étale subalgebras of a k -algebra is étale. If A is étale over k , then $k' \otimes A$ is étale over k' for every field k' containing k .

A.82. Let A be an étale k -algebra. Then $\text{Spm}(A)$ is an algebraic variety over k of dimension zero, and every algebraic variety of dimension zero is of this form.

A.83. Let k^{sep} be a separable closure of k , and let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$. We say that a Γ -set S is **discrete** if the action $\Gamma \times S \rightarrow S$ is continuous relative to the Krull topology on Γ and the discrete topology on S . If X is a zero-dimensional variety over k , then $X(k^{\text{sep}})$ is a finite discrete Γ -set, and the functor

$$X \rightsquigarrow X(k^{\text{sep}})$$

is an equivalence from the category of zero-dimensional algebraic varieties over k to the category of finite discrete Γ -sets.

o. The algebraic variety of connected components of an algebraic scheme

A.84. Let X be an algebraic scheme over k . Among the regular maps from X to a zero-dimensional algebraic variety there is one $X \rightarrow \pi_0(X)$ that is universal. The fibres of the map $X \rightarrow \pi_0(X)$ are the connected components of X . The map $X \rightarrow \pi_0(X)$ commutes with extension of the base field, and $\pi_0(X \times Y) \simeq \pi_0(X) \times \pi_0(Y)$. The variety $\pi_0(X)$ is called the **variety of connected components** of X .

p. Flat maps

A flat morphism is the algebraic analogue of a map whose fibres form a continuously varying family. For example, a surjective morphism of smooth varieties is flat if and only if all fibres have the same dimension. A finite morphism to a reduced algebraic scheme is flat if and only if, over every connected component, all fibres have the same number of points (counting multiplicities). A flat morphism of finite type of algebraic schemes is open, and surjective flat morphisms are epimorphisms in a very strong sense.

A.85. A homomorphism $A \rightarrow B$ of rings is **flat** if the functor $M \mapsto B \otimes_A M$ of A -modules is exact. It is **faithfully flat** if, in addition,

$$B \otimes_A M = 0 \implies M = 0.$$

- (a) If $f: A \rightarrow B$ is flat, then so also is $S^{-1}f: S^{-1}A \rightarrow S^{-1}B$ for all multiplicative subsets S of A .
- (b) A homomorphism $f: A \rightarrow B$ is flat if and only if $A_{f^{-1}(\mathfrak{n})} \rightarrow B_{\mathfrak{n}}$ is flat for all maximal ideals \mathfrak{n} in B .
- (c) Let $A \rightarrow A'$ be a homomorphism of rings. If $A \rightarrow B$ is flat (resp. faithfully flat), then $A' \rightarrow A' \otimes B$ is flat (resp. faithfully flat).
- (d) Faithfully flat homomorphisms are injective.

A.86. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes over k is said to be **flat** if, for all $y \in |Y|$, the map $\mathcal{O}_{X, \varphi y} \rightarrow \mathcal{O}_{Y, y}$ is flat. A flat map φ is said to be **faithfully flat** if it is flat and $|\varphi|$ is surjective. For example, the map $\text{Spm}(B) \rightarrow \text{Spm}(A)$ defined by a homomorphism of k -algebras $A \rightarrow B$ is flat (resp. faithfully flat) if and only if $A \rightarrow B$ is flat (resp. faithfully flat).

A.87. A flat map $\varphi: Y \rightarrow X$ of algebraic schemes is open, and hence universally open.

A.88 (GENERIC FLATNESS). Let $\varphi: Y \rightarrow X$ be a regular map of algebraic schemes. If X is integral, there exists a dense open subset U of X such that $\varphi^{-1}(U) \xrightarrow{\varphi} U$ is faithfully flat.

A.89. Let $\varphi: Y \rightarrow X$ be a regular map of algebraic schemes. If $p_1: Y \times_X Y \rightarrow Y$ is faithfully flat, then so also is φ (DG III, §1, 2.10, 2.11).

q. Flat descent

A.90. Let $\varphi: Y \rightarrow X$ be a regular map, and let $X' \rightarrow X$ be faithfully flat. If $\varphi': Y \times_X X' \rightarrow X'$ is affine (resp. finite, flat, smooth), then φ is affine (resp. finite, flat, smooth).

A.91. Let $f: A \rightarrow B$ be faithfully flat. Then the sequence

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{e_0 - e_1} B \otimes_A B$$

is exact, where $e_0(b) = 1 \otimes b$ and $e_1(b) = b \otimes 1$. On tensoring this sequence with M , we get an exact sequence

$$0 \rightarrow M \rightarrow M \otimes_A B \rightarrow M \otimes_A B^{\otimes 2}.$$

A.92. Let $f: A \rightarrow B$ be a faithfully flat homomorphism, and let M be an A -module. Write M' for the B -module $f_*M = B \otimes_A M$. The module $e_{0*}M' = (B \otimes_A B) \otimes_B M'$ may be identified with $B \otimes_A M'$ where $B \otimes_A B$ acts by $(b_1 \otimes b_2)(b \otimes m) = b_1 b \otimes b_2 m$, and $e_{1*}M'$ may be identified with $M' \otimes_A B$ where $B \otimes_A B$ acts by $(b_1 \otimes b_2)(m \otimes b) = b_1 m \otimes b_2 b$. There is a canonical isomorphism $\phi: e_{1*}M' \rightarrow e_{0*}M'$ arising from

$$e_{1*}M' = (e_1 f)_*M = (e_0 f)_*M = e_{0*}M';$$

explicitly it is the map

$$\begin{aligned} M' \otimes_A B &\rightarrow B \otimes_A M' \\ (b \otimes m) \otimes b' &\mapsto b \otimes (b' \otimes m), \quad m \in M. \end{aligned}$$

Moreover, M can be recovered from the pair (M', ϕ) because

$$M = \{m \in M' \mid 1 \otimes m = \phi(m \otimes 1)\}$$

according to (A.91).

Conversely, every pair (M', ϕ) satisfying certain conditions does arise in this way from an A -module. Given $\phi: M' \otimes_A B \rightarrow B \otimes_A M'$ define

$$\begin{aligned} \phi_1: B \otimes_A M' \otimes_A B &\rightarrow B \otimes_A B \otimes_A M', \\ \phi_2: M' \otimes_A B \otimes_A B &\rightarrow B \otimes_A B \otimes_A M', \\ \phi_3: M' \otimes_A B \otimes_A B &\rightarrow B \otimes_A M' \otimes_A B \end{aligned}$$

by tensoring ϕ with id_B in the first, second, and third positions respectively. Then a pair (M', ϕ) arises from an A -module M as above if and only if $\phi_2 = \phi_1 \phi_3$. The necessity is easy to check. For the sufficiency, define

$$M = \{m \in M' \mid 1 \otimes m = \phi(m \otimes 1)\}.$$

There is a canonical map $b \otimes m \mapsto bm: B \otimes_A M \rightarrow M'$, and it suffices to show that this is an isomorphism (and that the map arising from M is ϕ). Consider the diagram

$$\begin{array}{ccc} M' \otimes_A B & \xrightarrow[\beta \otimes 1]{\alpha \otimes 1} & B \otimes_A M' \otimes_A B \\ \downarrow \phi & & \downarrow \phi_1 \\ B \otimes_A M' & \xrightarrow[e_1 \otimes 1]{e_0 \otimes 1} & B \otimes_A B \otimes_A M' \end{array}$$

in which $\alpha(m) = 1 \otimes m$ and $\beta(m) = \phi(m \otimes 1)$. As the diagram commutes with either the upper or the lower horizontal maps (for the lower maps, this uses the relation $\phi_2 = \phi_1 \phi_3$), ϕ induces an isomorphism on the kernels. But, by definition of M , the kernel of the pair $(\alpha \otimes 1, \beta \otimes 1)$ is $M \otimes_A B$, and, according to (A.91), the kernel of the pair $(e_0 \otimes 1, e_1 \otimes 1)$ is M' . This essentially completes the proof.

r. Finite maps and quasi-finite maps

A.93. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes over k is **finite** if, for every open affine $U \subset X$, $\varphi^{-1}(U)$ is affine and $\mathcal{O}_Y(\varphi^{-1}(U))$ is a finite $\mathcal{O}_X(U)$ -algebra. For example, the map $\text{Spm}(B) \rightarrow \text{Spm}(A)$ defined by a homomorphism of k -algebras $A \rightarrow B$ is finite if and only if $A \rightarrow B$ is finite.

A.94. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes over k is **quasi-finite** if, for all $x \in X$, the fibre $\varphi^{-1}(x)$ is a finite scheme over $k(x)$. We let $\deg_x(\varphi) = \dim_k(\mathcal{O}_{\varphi^{-1}(x)}(\varphi^{-1}(x)))$. A finite map $\varphi: Y \rightarrow X$ is quasi-finite. For example, if φ is the map of affine algebraic schemes defined by a homomorphism $A \rightarrow B$, then $\deg_x(\varphi) = \dim_k(B \otimes_A A/\mathfrak{m}_x)$.

A.95. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes with X integral is flat if and only if $\deg_x(\varphi)$ is independent of $x \in X$.

A.96. Let $\varphi: Y \rightarrow X$ be a finite map of integral schemes. The **degree** of φ is the degree of $k(Y)$ over $k(X)$, and the **separable degree** of φ is the degree of the greatest separable subextension of $k(Y)$ over $k(X)$.

(a) For all $x \in X$,

$$\deg_x(\varphi) \leq \deg(\varphi),$$

and the points x for which equality holds form a dense open subset of X .

(b) Assume that k is algebraically closed. For all $x \in X$,

$$\#\left|\varphi^{-1}(x)\right| \leq \text{sep deg}(\varphi),$$

and the points x for which equality holds form a dense open subset of X .

A.97. (Zariski's main theorem). Every separated map $\varphi: Y \rightarrow X$ factors into the composite

$$Y \xrightarrow{\iota} Y' \xrightarrow{\varphi'} X$$

of an open immersion ι and a finite map φ' .

A.98. Let $\varphi: Y \rightarrow X$ be a quasi-finite map of integral algebraic schemes. If φ is birational (i.e., of degree 1) and X is normal, then φ is an open immersion.

s. The fibres of regular maps

A.99. Let $\varphi: Y \rightarrow X$ be a dominant map of integral schemes. Let $P \in \varphi(X)$. Then

$$\dim(\varphi^{-1}(P)) \geq \dim(Y) - \dim(X).$$

The image of φ contains a dense open subset U of X , and U may be chosen so that equality holds for all $P \in U$. Equality holds for all P if φ is flat.

A.100. Let $\varphi: Y \rightarrow X$ 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.101. A surjective morphism of smooth algebraic k -schemes is flat (hence faithfully flat) if its fibres all have the same dimension.

t. Étale maps

A.102. Let $\varphi: Y \rightarrow X$ be a map of algebraic schemes over k , and let y be a nonsingular point of Y such that $x \stackrel{\text{def}}{=} \varphi(y)$ is nonsingular. We say that φ is **étale at y** if $(d\varphi)_y: T_y(Y) \rightarrow T_x(X)$ is bijective. When X and Y are nonsingular varieties, we say that φ is **étale** if it is étale at all points of Y .

A.103. If φ is étale at a point, then it is étale in an open neighbourhood of the point.

A.104. Let x be a point on an algebraic variety of dimension d . A **local system of parameters at x** is a family $\{f_1, \dots, f_d\}$ of germs of functions at x generating the maximal ideal \mathfrak{m}_x in \mathcal{O}_x . Given such a system, there exists a nonsingular open neighbourhood U of x and representatives $(\tilde{f}_1, U), \dots, (\tilde{f}_d, U)$ of f_1, \dots, f_d such that $(\tilde{f}_1, \dots, \tilde{f}_d): U \rightarrow \mathbb{A}^d$ is étale.

A.105. An **étale neighbourhood** of a point x on a nonsingular variety X is a pair $(\varphi: U \rightarrow X, u)$ with φ an étale map from a nonsingular variety U to X and u a point of U such that $\varphi(u) = x$.

A.106. (Inverse function theorem). Let $\varphi: Y \rightarrow X$ be a regular map of nonsingular varieties. If φ is étale at a point y of Y , then there exists an open neighbourhood V of y such that (V, y) is an étale neighbourhood of x .

u. Smooth maps

A.107. A regular map $\varphi: Y \rightarrow X$ of algebraic schemes is said to be **smooth** if it is flat and the fibres $\varphi^{-1}(x)$ are smooth for all $x \in X$. Equivalently, a regular map φ is smooth if and only if, locally, it factors into

$$Y \xrightarrow{\text{étale}} \mathbb{A}_X^n \rightarrow X.$$

A dominant map $\varphi: Y \rightarrow X$ of smooth algebraic varieties is smooth if and only if $(d\varphi)_y: T_y(Y) \rightarrow T_{\varphi(y)}(X)$ is surjective for all $y \in Y$.

A.108. (Rank theorem) Let $\varphi: Y \rightarrow X$ be a regular map of irreducible algebraic schemes of dimensions n and m respectively. Let Q be a nonsingular point of Y such that $P \stackrel{\text{def}}{=} \varphi(Q)$ is nonsingular. If $(d\varphi)_Q: T_Q(Y) \rightarrow T_P(X)$ is surjective, then there exists a commutative diagram

$$\begin{array}{ccc} (U_Q, Q) & \xrightarrow{\varphi|_{U_Q}} & (U_P, P) \\ \downarrow \text{étale} & & \downarrow \text{étale} \\ (\mathbb{A}^n, \mathcal{o}) & \xrightarrow{(x_1, \dots, x_n) \mapsto (x_1, \dots, x_m)} & (\mathbb{A}^m, \mathcal{o}) \end{array}$$

in which (U_Q, Q) and (U_P, P) are open neighbourhoods of Q and P and étale neighbourhoods of the origin \mathbb{A}^n and \mathbb{A}^m .

A.109. A dominant map $\varphi: Y \rightarrow X$ of integral algebraic schemes is **separable** if $k(Y)$ is a separably generated field extension of $k(X)$.

A.110. Let $\varphi: Y \rightarrow X$ be a dominant map of integral algebraic schemes.

- (a) If there exists a nonsingular point $Q \in Y$ such that $\varphi(Q)$ is nonsingular and $(d\varphi)_Q$ is surjective, then φ is separable.
- (a) If φ is separable, then the set of points $Q \in Y$ satisfying the condition in (a) is a dense open subset of W .

A.111. The pull-back of a separable map of irreducible algebraic varieties is separable.

A.112. Let Z_1 and Z_2 be closed subschemes of an algebraic scheme X . Then $Z_1 \cap Z_2 \stackrel{\text{def}}{=} Z_1 \times_X Z_2$ is a closed algebraic subscheme of X . If X , Z_1 , and Z_2 are algebraic varieties, then $Z_1 \cap Z_2$ is an algebraic variety if $T_P(Z_1)$ and $T_P(Z_2)$ cross transversally (in $T_P(X)$) for all P in an open subset of X .

v. Complete algebraic schemes

A.113. An algebraic scheme X is said to be **complete** if it is separated and if, for all algebraic schemes T , the projection map $q: X \times T \rightarrow T$ is closed. (It suffices to check this with $T = \mathbb{A}^n$.)

- A.114. (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 $\varphi: X \rightarrow S$ 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 $\varphi: X \rightarrow S$ 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 $X \rightarrow \mathbb{P}^1$ from a complete connected algebraic variety X is either constant or surjective.
- (f) The only regular functions on a complete connected algebraic variety are the constant functions.
- (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.

A.115. Projective algebraic schemes are complete.

A.116. Every quasi-finite map $Y \rightarrow X$ with Y complete is finite.

w. Proper maps

A.117. A regular map $\varphi: X \rightarrow S$ of algebraic schemes is **proper** if it is separated and universally closed (i.e., for all regular maps $T \rightarrow S$, the projection map $q: X \times_S T \rightarrow T$ is closed).

A.118. A finite map is proper.

A.119. An algebraic scheme X is complete if and only if the map $X \rightarrow \text{Spm}(k)$ is proper. The base change of a proper map is proper. In particular, if $\pi: X \rightarrow S$ is proper, then $\pi^{-1}(P)$ is a complete subscheme of X for all $P \in S$.

A.120. If $X \rightarrow S$ is proper and S is complete, then X is complete.

A.121. The inverse image of a complete algebraic scheme under a proper map is complete.

A.122. Let $\varphi: X \rightarrow S$ be a proper map. The image φZ of any complete algebraic subscheme Z of X is a complete algebraic subscheme of S .

A.123. Let $A = \bigoplus_{d \geq 0} A_d$ be a graded ring such that

- (a) as an A_0 -algebra, A is generated by A_1 , and
- (b) for every $d \geq 0$, A_d is finitely generated as an A_0 -module.

A map $\pi: \text{Proj}(A) \rightarrow \text{Spm}(A_0)$ is defined (to be added).

A.124. The map $\pi: \text{proj}(A) \rightarrow \text{spm}(A_0)$ is closed.

x. *Algebraic schemes as flat sheaves (will be moved to Chapter V)*

y. *Restriction of the base field (Weil restriction of scalars)*

Let A be a finite k -algebra. A functor F from A -algebras to sets defines a functor

$$(F)_{A/k}: \text{Alg}_k \rightarrow \text{Set}, \quad R \mapsto F(A \otimes R).$$

If F is representable, is $(F)_{A/k}$ also representable?

A.125. If $F: \text{Alg}_A \rightarrow \text{Set}$ is represented by a finitely generated A -algebra, then $(F)_{A/k}$ is represented by a finitely generated k -algebra.

PROOF. Let

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

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

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

and so there is a bijection

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

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

$$a_i = \sum_{j=1}^d b_{ij} e_j, \quad i = 1, \dots, n. \quad (195)$$

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

If F is represented by a finitely generated A -algebra, then F is a closed subfunctor of \mathbb{A}^n for some n . Therefore $(F)_{A/k}$ is a closed subfunctor of $(\mathbb{A}^n)_{A/k} \approx \mathbb{A}^{dn}$ (1.80), and so $(F)_{A/k}$ is represented by a quotient of $k[T_1, \dots, T_{dn}]$ (1.76).

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

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

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

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

when the a s and b s are related by (195). The polynomial g has coefficients in A , but we can write it (uniquely) as a sum

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

Clearly,

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

and so $(F)_{A/k}$ is isomorphic to the subfunctor of \mathbb{A}^{nd} defined by the polynomials g_1, \dots, g_d . This argument extends in an obvious way to the case that F is the subfunctor of \mathbb{A}^n defined by a finite set of polynomials. \square

A.126. *Let X be an algebraic scheme over A such that every finite subset of $|X|$ is contained in an open affine subscheme (e.g., X quasi-projective). Then $(X)_{A/k}$ is an algebraic scheme over k .*

PROOF. We use two obvious facts: (a) if U is an open subfunctor of F , then $(U)_{A/k}$ is an open subfunctor of $(F)_{A/k}$; (b) if F is local (see A.29), then $(F)_{A/k}$ is local. Let U be an open affine subscheme of X . Then $(U)_{A/k}$ is an open subfunctor of $(X)_{A/k}$ and it is an affine scheme over k by (A.125). It remains to show that a finite number of the functors $(U)_{A/k}$ cover $(X)_{A/k}$ (A.29).

Let $d = [A:k]$, and let $|X|^d$ be the topological product of d copies $|X|$. By assumption, the sets U^d with U open affine in $|X|$ cover $|X|^d$. As $|X|^d$ is quasi-compact, a finite collection U_1, \dots, U_n cover $|X|^d$.

Let U be the union of the subfunctors $(U_i)_{A/k}$ of $(X)_{A/k}$. It is an open subfunctor of $(X)_{A/k}$, and so if $U \neq (X)_{A/k}$, then $U(K) \neq (X)_{A/k}(K)$ for some field K containing k . A point $Q \in (X)_{A/k}(K)$ is an A -morphism $\text{Spm}(A \otimes K) \rightarrow X$. The image of $|Q|$ is contained in a subset of $|X|$ with at most d elements, and so Q factors through some U_i . Therefore $(X)_{A/k} = \bigcup (U_i)_{A/k}$. \square

Dictionary

We explain the relation between the language used in this work and in some other standard works.

a. Demazure and Gabriel 1970

They work more generally, so let k be a ring. DG define a scheme X over k to be a functor that is representable by a scheme over k in the sense of EGA. Thus, attached to every DG-scheme X there is a locally ringed space $|X| = (|X|^e, \mathcal{O}_{|X|})$. They often write X for $|X|$, which is sometimes confusing. For example, the statement (DG I, §1, 5.3, p.24),

If $f: X \rightarrow Y$ is a monomorphism of schemes, f is injective.

means the following. Here X and Y are functors representable by EGA-schemes and f is a monomorphism in the category of functors (equivalently, $f(R)$ is injective for all R). By f being injective, they mean that the morphism $|f|: |X| \rightarrow |Y|$ of schemes is injective, i.e., that the map $|f|^e: |X|^e \rightarrow |Y|^e$ on the underlying topological spaces is injective. Thus the statement means:

Let $f: X \rightarrow Y$ be a morphism of schemes; if $f(R)$ is injective for all (small) k -algebras R , then $|f|^e: |X|^e \rightarrow |Y|^e$ is injective.

Their notions of an algebraic scheme and an algebraic group over a field k agree with our notions except that, whereas we regard them as EGA-schemes first and as functors second, they do the opposite. Unlike us, they don't ignore the nonclosed points.

One problem they face is that the set-valued functors on the category of k -algebras (k a ring) is not a category because the morphisms from one object to a second do not generally form a set. To get around this problem, they fix two universes U and V such that $\mathbb{N} \in U$ and $U \in V$. A ring whose underlying set lies in U is called a "model". Let k be a model. A k -model is defined to be a k -algebra whose underlying set lies U . The k -models form a category M_k , and the functors from M_k to Set form a category ME_k . When $k = \mathbb{Z}$, it is omitted from the notation.

We avoid assuming the existence of universes by working with functors on Alg_k^0 , which is a small category.

b. Borel 1969/1991; Springer 1981/1998

Throughout Springer's books, k is an algebraically closed field and F is a subfield of k (Borel denotes the fields by K and k respectively).

Springer's notions of an algebraic variety over k and an algebraic group over k essentially agree with our notions of an algebraic variety over k and a group variety over k . In other words, an algebraic group over k in Springer's book is a smooth algebraic group over k in this work.

When a construction in the category of smooth algebraic group schemes over k takes one outside the category of smooth objects, Springer replaces the nonsmooth object with its reduced subobject. For example, for us $x \mapsto x^p: \mathbb{G}_a \rightarrow \mathbb{G}_a$ is a homomorphism of degree p with nontrivial kernel α_p ; for Springer, it is a homomorphism of degree p with trivial kernel.

For Springer, an F -variety is an algebraic variety X over k together with an " F -structure". This is an open affine covering \mathcal{U} of X together with, for each $U \in \mathcal{U}$, an F -structure on the k -algebra $\mathcal{O}_X(U)$, satisfying certain conditions. The notion of an F -variety essentially agrees with our notion of a variety over F . However, there are important differences in terminology. For Springer, a morphism $\phi: X \rightarrow Y$ of F -varieties is not required to preserve the F -structures, i.e., it is a morphism of k -varieties. If it preserves the F -structures, then it is called an F -morphism and is said to be defined over F . For Springer, the kernel of an F -homomorphism $\phi: G \rightarrow H$ is an algebraic group (i.e., smooth group subscheme) of G , i.e., it is an algebraic group over k . It may, or may not, admit an F -structure. (From our perspective, ϕ is a homomorphism of group varieties G and H over F ; Springer's kernel is $\text{Ker}(\phi_k)_{\text{red}}$; this may, or may not, arise from a subgroup variety of G — the problem is that $\text{Ker}(\phi)_{\text{red}}$ may fail to be a group variety. Cf. the statement Borel (1991, p.98) that the kernel of an F -homomorphism of F -groups is defined over F if the homomorphism is separable).

The terminology of Borel, and much of the literature on linear algebraic groups, agrees with that of Springer.

As noted earlier, 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. Worse, a statement loc. cit. may become false when interpreted in the language of modern (i.e., post 1960) algebraic geometry. Here are two: the kernel of $\text{SL}_p \rightarrow \text{PGL}_p$ is trivial in characteristic p ; every nonzero F -torus admits a homomorphism to \mathbb{G}_m (when read in the language of modern algebraic geometry, this is false unless F is separably closed).

In fact, much of [Springer 1998](#) adapts easily to the scheme-theoretic situation. For example, given a group variety G over a field k , he typically defines a subgroup H of G by describing its group of k^{al} -points in $G(k^{\text{al}})$ and then proving (in good cases) that H is defined over k . We define H as an algebraic subgroup of G (over k) by describing its R -points for all small k -algebras R , and then adapt his arguments to show that H is smooth. See, for example, the definition of $P(\lambda)$ (p. 364).

c. *Waterhouse 1979*

Let k be an infinite field. Waterhouse (1979), p.29 defines an *affine algebraic group* to be an algebraic group scheme G such that $G(k)$ is dense in G and $G(k)$ is a closed subset of k^n for some n . He defines a *matrix group* to be an algebraic group scheme G such that $G(k)$ is dense in G and $G(k)$ is a closed subgroup of $\text{SL}_n(k)$ for some n .

Solutions to the exercises

22-2 We may assume that k is algebraically closed.

(a) Let G be a connected algebraic group scheme, and let N be the kernel of the adjoint representation of G on $\text{Lie}(G)$. According to (15.25) $N/Z(G)$ is unipotent. Hence $N = N_u \rtimes Z(G)$ (17.37). If G is reductive, it follows that $N = Z(G)$.

(b) Let G be a reductive group and let $G' = G/Z(G)$. There is an exact sequence of Lie algebras:

$$0 \rightarrow \text{Lie}(Z(G)) \rightarrow \text{Lie}(G) \rightarrow \text{Lie}(G').$$

The subspace $\text{Lie}(Z(G))$ is stable under the adjoint action of G on $\text{Lie}(G)$, and G acts trivially on it. Let N be the kernel of the action of G on $\text{Lie}(G')$. Then N is a normal subgroup of G , and $N/Z(G)$ maps injectively into the group of automorphisms α of $\text{Lie}(G)$ with the property that $(1 - \alpha)(\text{Lie}(G))$ is contained in $\text{Lie}(Z(G))$. Therefore $N/Z(G)$ is unipotent, hence trivial. This implies that the kernel of the adjoint action of G' on $\text{Lie}(G')$ is trivial, and so $Z(G') = 1$. See also 16.46.

15-1 Because of the uniqueness, we may suppose that k is separably closed. It suffices to show that G contains a maximal unipotent normal algebraic subgroup (8.35). For this we use Zorn's lemma. Let

$$U_1 \subset U_2 \subset U_3 \subset \dots \tag{196}$$

be a chain of unipotent normal algebraic subgroups of G . Let H be the intersection of all algebraic subgroups of G containing all U_i , and let (V, r) be a representation of H . Then $W = \bigcap_i V^{U_i}$ is a nonempty subspace W . Let H' be the algebraic subgroup of H fixing W . Then H' contains all U_i and so $H' = H$. Therefore H fixes W , and so it is unipotent. It is also normal because it is obviously stable under $\text{inn}(g)$ for all $g \in G(k)$, and we can apply (1.61). Now H is an upper bound for the chain.

6-4 The simplest proof uses that the flat site has enough "points". This means that there is a family of functors s_x from sheaves of groups to Grp with the property that a sequence $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$ of sheaves is exact if and only if the sequences $1 \rightarrow s_x(A) \rightarrow s_x(B) \rightarrow s_x(C) \rightarrow 1$ are exact for all x . Now (6-4) follows from the usual extended snake lemma.

Bibliography

- ADAMS, J. F. 1969. Lectures on Lie groups. W. A. Benjamin, Inc., New York-Amsterdam.
- ALLCOCK, D. 2009. A new approach to rank one linear algebraic groups. *J. Algebra* 321:2540–2544.
- ALPER, J. 2010. On the local quotient structure of Artin stacks. *J. Pure Appl. Algebra* 214:1576–1591.
- ARTIN, E. 1957. Geometric algebra. Interscience Publishers, Inc., New York-London.
- ATIYAH, M. F. AND MACDONALD, I. G. 1969. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont.
- BARDSLEY, P. AND RICHARDSON, R. W. 1985. Étale slices for algebraic transformation groups in characteristic p . *Proc. London Math. Soc. (3)* 51:295–317.
- BARSOTTI, I. 1955. Un teorema di struttura per le varietà gruppalì. *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, volume 65 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge.
- 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, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131. Springer, Berlin.
- BOREL, A. 1975. Linear representations of semi-simple algebraic groups, pp. 421–440. In *Algebraic geometry (Proc. Sympos. Pure Math., Vol. 29, Humboldt State Univ., Arcata, Calif., 1974)*. Amer. Math. Soc., Providence, R.I.
- BOREL, A. 1985. On affine algebraic homogeneous spaces. *Arch. Math. (Basel)* 45:74–78.
- BOREL, A. 1991. Linear algebraic groups. Springer-Verlag, New York.
- 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 TITS, J. 1965. Groupes réductifs. *Inst. Hautes Études Sci. Publ. Math.* pp. 55–150.
- 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.
- BOSCH, S., LÜTKEBOHMERT, W., AND RAYNAUD, M. 1990. Néron models, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin.

- BOURBAKI, N. LIE. Groupes et Algèbres de Lie. *Éléments de mathématique*. Hermann; Masson, Paris. Chap. I, Hermann 1960; Chap. II,III, Hermann 1972; Chap. IV,V,VI, Masson 1981; Chap. VII,VIII, Masson 1975; Chap. IX, Masson 1982 (English translation available from Springer).
- BRION, M. 2009. Anti-affine algebraic groups. *J. Algebra* 321:934–952.
- BRION, M., SAMUEL, P., AND UMA, V. 2013. Lectures on the structure of algebraic groups and geometric applications. CMI Lecture Series in Mathematics 1. Hindustan Book Agency.
- CARRELL, J. B. 2002. Torus actions and cohomology, pp. 83–158. *In Algebraic quotients. Torus actions and cohomology. The adjoint representation and the adjoint action*, volume 131 of *Encyclopaedia Math. Sci.* Springer, Berlin.
- CARTIER, P. 1956. Dualité de Tannaka des groupes et des algèbres de Lie. *C. R. Acad. Sci. Paris* 242:322–325.
- CARTIER, P. 1962. Groupes algébriques et groupes formels, pp. 87–111. *In Colloq. Théorie des Groupes Algébriques* (Bruxelles, 1962). Librairie Universitaire, Louvain.
- CHERNOUSOV, V. I. 1989. The Hasse principle for groups of type E_8 . *Dokl. Akad. Nauk SSSR* 306:1059–1063.
- CHEVALLEY, C. 1960. Une démonstration d'un théorème sur les groupes algébriques. *J. Math. Pures Appl.* (9) 39:307–317.
- CHEVALLEY, C. C. 1955. Sur certains groupes simples. *Tôhoku Math. J.* (2) 7:14–66.
- CHEVALLEY, C. C. 1956–58. Classification des groupes de Lie algébriques, Séminaire ENS, Paris, mimeographed. Reprinted 2005 by Springer Verlag with a postface by P. Cartier.
- CHOW, W.-L. 1957. On the projective embedding of homogeneous varieties, pp. 122–128. *In Algebraic geometry and topology. A symposium in honor of S. Lefschetz*. Princeton University Press, Princeton, N. J.
- CLINE, E., PARSHALL, B., AND SCOTT, L. 1977. Induced modules and affine quotients. *Math. Ann.* 230:1–14.
- CONRAD, B., GABBER, O., AND PRASAD, G. 2010. Pseudo-reductive groups, volume 17 of *New Mathematical Monographs*. Cambridge University Press, Cambridge.
- 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 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. Springer-Verlag, Berlin.
- DEMAZURE, M. AND GABRIEL, P. 1970. Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. Masson & Cie, Éditeur, Paris.
- EISENBUD, D. 1995. Commutative algebra, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York. With a view toward algebraic geometry.
- ERNST, M. 2015. The prospects of unlimited category theory: doing what remains to be done. *Rev. Symb. Log.* 8:306–327.
- FOSSUM, R. AND IVERSEN, B. 1973. On Picard groups of algebraic fibre spaces. *J. Pure Appl. Algebra* 3:269–280.
- HARDER, G. 1966. Über die Galoiskohomologie halbeinfacher Matrizen Gruppen. II. *Math. Z.* 92:396–415.
- HARDER, G. 1975. Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. III. *J. Reine Angew. Math.* 274/275:125–138. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.
- HERPEL, S. 2013. On the smoothness of centralizers in reductive groups. *Trans. Amer. Math. Soc.* 365:3753–3774.

- HOCHSCHILD, G. 1965. The structure of Lie groups. Holden-Day, Inc., San Francisco-London-Amsterdam.
- HOCHSCHILD, G. 1971. Introduction to affine algebraic groups. Holden-Day Inc., San Francisco, Calif.
- HOCHSCHILD, G. AND MOSTOW, G. D. 1961. On the algebra of representative functions of an analytic group. *Amer. J. Math.* 83:111–136.
- HOCHSCHILD, G. P. 1981. Basic theory of algebraic groups and Lie algebras, volume 75 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.
- HUMPHREYS, J. E. 1967. Algebraic groups and modular Lie algebras. Memoirs of the American Mathematical Society, No. 71. American Mathematical Society, Providence, R.I.
- HUMPHREYS, J. E. 1972. Introduction to Lie algebras and representation theory. Springer-Verlag, New York.
- HUMPHREYS, J. E. 1975. Linear algebraic groups. Springer-Verlag, New York.
- 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. 1943. The Theory of Rings. AMS Mathematical Surveys, vol. I. Amer. Math. Soc., New York.
- JANTZEN, J. C. 1987. Representations of algebraic groups, volume 131 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA.
- KAMBAYASHI, T., MIYANISHI, M., AND TAKEUCHI, M. 1974. Unipotent algebraic groups. Lecture Notes in Mathematics, Vol. 414. Springer-Verlag, Berlin.
- KNESER, M. 1969. Lectures on Galois cohomology of classical groups. Tata Institute of Fundamental Research, Bombay.
- KOHL, M. 2011. A user friendly proof of Nagata’s characterization of linearly reductive groups in positive characteristics. *Linear Multilinear Algebra* 59:271–278.
- KOITABASHI, M. 1989. Some remarks on affine homogeneous spaces. *Osaka J. Math.* 26:229–244.
- KOLCHIN, E. R. 1948a. Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Ann. of Math. (2)* 49:1–42.
- KOLCHIN, E. R. 1948b. On certain concepts in the theory of algebraic matrix groups. *Ann. of Math. (2)* 49:774–789.
- LANG, S. 1956. Algebraic groups over finite fields. *Amer. J. Math.* 78:555–563.
- LUNA, D. 1972. Sur les orbites fermées des groupes algébriques réductifs. *Invent. Math.* 16:1–5.
- LUNA, D. 1973. Slices étales, pp. 81–105. Bull. Soc. Math. France, Paris, Mémoire 33. *In* Sur les groupes algébriques. Soc. Math. France, Paris.
- LUNA, D. 1999. Retour sur un théorème de Chevalley. *Enseign. Math. (2)* 45:317–320.
- MAC LANE, S. 1969. One universe as a foundation for category theory, pp. 192–200. *In* Reports of the Midwest Category Seminar. III. Springer, Berlin.
- MACLANE, S. 1971. Categories for the working mathematician. Springer-Verlag, New York. Graduate Texts in Mathematics, Vol. 5.
- MALLE, G. AND TESTERMAN, D. 2011. Linear algebraic groups and finite groups of Lie type, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge.
- MATSUSHIMA, Y. 1960. Espaces homogènes de Stein des groupes de Lie complexes. *Nagoya Math. J.* 16:205–218.
- MCNINCH, G. J. 2014. Linearity for actions on vector groups. *J. Algebra* 397:666–688.

- MEHTA, V. B. 2002. Representations of algebraic groups and principal bundles on algebraic varieties. *In* Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), pp. 629–635. Higher Ed. Press, Beijing.
- MILNE, J. S. 1986. Abelian varieties, pp. 103–150. *In* Arithmetic geometry (Storrs, Conn., 1984). Springer, New York.
- 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:math/1311.6060.
- MÜLLER, P. 2003. Algebraic groups over finite fields, a quick proof of Lang’s theorem. *Proc. Amer. Math. Soc.* 131:369–370.
- MUMFORD, D. 2008. Abelian varieties, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi. Corrected reprint of the second (1974) edition.
- NAGATA, M. 1961/1962. Complete reducibility of rational representations of a matric group. *J. Math. Kyoto Univ.* 1:87–99.
- 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.
- DOKOVIĆ, D. Ž. 1988. An elementary proof of the structure theorem for connected solvable affine algebraic groups. *Enseign. Math. (2)* 34:269–273.
- 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, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA.
- 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.
- PROCESI, C. 2007. Lie groups. Universitext. Springer, New York. An approach through invariants and representations.
- RICHARDSON, R. W. 1977. Affine coset spaces of reductive algebraic groups. *Bull. London Math. Soc.* 9:38–41.
- ROSENBLICHT, M. 1956. Some basic theorems on algebraic groups. *Amer. J. Math.* 78:401–443.
- ROSENBLICHT, M. 1957. Some rationality questions on algebraic groups. *Ann. Mat. Pura Appl. (4)* 43:25–50.
- ROSENBLICHT, M. 1961. Toroidal algebraic groups. *Proc. Amer. Math. Soc.* 12:984–988.
- ROSENBLICHT, 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, volume 16 of *Aportaciones Matemáticas: Textos*. 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. 1971. Classification theory of semi-simple algebraic groups. Marcel Dekker Inc., New York. With an appendix by M. Sugiura, Notes prepared by Doris Schattschneider, Lecture Notes in Pure and Applied Mathematics, 3. Originally available from the University of Chicago as mimeographed notes.
- SATAKE, I. 2001. On classification of semisimple algebraic groups, pp. 197–216. *In* Class field theory—its centenary and prospect (Tokyo, 1998), volume 30 of *Adv. Stud. Pure Math.* Math. Soc. Japan, Tokyo.
- SCHARLAU, W. 1985. Quadratic and Hermitian forms, volume 270 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin.
- SCHOELLER, C. 1972. Groupes affines, commutatifs, unipotents sur un corps non parfait. *Bull. Soc. Math. France* 100:241–300.
- SELBACH, M. 1976. Klassifikationstheorie halbeinfacher algebraischer Gruppen. Mathematisches Institut der Universität Bonn, Bonn. Diplomarbeit, Univ. Bonn, Bonn, 1973, Bonner Mathematische Schriften, Nr. 83.
- SERRE, J.-P. 1959. Groupes algébriques et corps de classes. Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris.
- SERRE, J.-P. 1962. Corps locaux. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris.
- SERRE, J.-P. 1964. Cohomologie Galoisienne, volume 5 of *Lecture Notes in Math.* Springer-Verlag, Berlin.
- SERRE, J.-P. 1966. Algèbres de Lie semi-simples complexes. W. A. Benjamin, inc., New York-Amsterdam. English translation published by Springer Verlag 1987.
- SERRE, J.-P. 1968. Groupes de Grothendieck des schémas en groupes réductifs déployés. *Inst. Hautes Études Sci. Publ. Math.* pp. 37–52.
- SERRE, J.-P. 1993. Gèbres. *Enseign. Math. (2)* 39:33–85.
- SPRINGER, T. A. 1979. Reductive groups, pp. 3–27. *In* Automorphic forms, representations and L -functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1, Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I.
- SPRINGER, T. A. 1998. Linear algebraic groups, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA.
- STEINBERG, R. 1968. Endomorphisms of linear algebraic groups. *Memoirs of the American Mathematical Society*, No. 80. American Mathematical Society, Providence, R.I.
- STEINBERG, R. 1977. On theorems of Lie-Kolchin, Borel, and Lang, pp. 349–354. *In* Contributions to algebra (collection of papers dedicated to Ellis Kolchin). Academic Press, New York.
- STEINBERG, R. 1978. Conjugacy in semisimple algebraic groups. *J. Algebra* 55:348–350.
- STEINBERG, R. 1998. The isomorphism and isogeny theorems for reductive algebraic groups, pp. 233–240. *In* Algebraic groups and their representations (Cambridge, 1997), volume 517 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.* Kluwer Acad. Publ., Dordrecht.
- STEINBERG, R. 1999. The isomorphism and isogeny theorems for reductive algebraic groups. *J. Algebra* 216:366–383.
- STIEFEL, E. 1942. Über eine Beziehung zwischen geschlossenen Lie'schen Gruppen und diskontinuierlichen Bewegungsgruppen euklidischer Räume und ihre Anwendung auf die Aufzählung der einfachen Lie'schen Gruppen. *Comment. Math. Helv.* 14:350–380.
- SUMIHIRO, H. 1974. Equivariant completion. *J. Math. Kyoto Univ.* 14:1–28.
- SUMIHIRO, H. 1975. Equivariant completion. II. *J. Math. Kyoto Univ.* 15:573–605.
- SWEEDLER, M. E. 1969. Hopf algebras. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York.

- TAKEUCHI, M. 1972. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.* 7:251–270.
- TAKEUCHI, M. 1975. On the structure of commutative affine group schemes over a non-perfect field. *Manuscripta Math.* 16:101–136.
- 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, New York.
- TATE, J. AND OORT, F. 1970. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)* 3:1–21.
- THĂNG, N. Q. 2008. Addendum: “On Galois cohomology of semisimple groups over local and global fields of positive characteristic” [Math. Z. 259 (2008), no. 2, 457–467; mr2390091]. *Math. Z.* 259:469–470.
- THĂNG, N. Q. 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 (Proc. Sympos. Pure Math., Boulder, Colo., 1965). Amer. Math. Soc., Providence, R.I., 1966.
- 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 (Course at the Collège de France 1991–92, see Annuaire du Collège de France).
- TITS, J. 1993. Théorie des groupes (Course at the Collège de France 1992–93, see Annuaire du Collège de France).
- 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, volume 179 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ].
- WATERHOUSE, W. C. 1979. Introduction to affine group schemes, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.
- WEIL, A. 1946. Foundations of Algebraic Geometry. American Mathematical Society Colloquium Publications, vol. 29. American Mathematical Society, New York.
- WU, X. L. 1986. On the extensions of abelian varieties by affine group schemes, pp. 361–387. *In* Group theory, Beijing 1984, volume 1185 of *Lecture Notes in Math*. Springer, Berlin.

Index

- action, 30, 139
 - linear, 148, 186
 - semi-linear, 473
- adjoint group, 49
- affine n -space, 491
- algebra
 - central, 477
 - Clifford, 457
 - diagonalizable, 205, 506
 - division, 477
 - étale, 42, 205, 506
 - finite, 42
 - graded, 455
 - Lie, 183
 - opposite, 460
 - simple, 477
 - small, 15
 - symmetric, 40
 - tensor, 456
 - universal enveloping, 194
- algebraic group
 - additive, 39
 - affine, 17
 - almost-simple, 418
 - anti-affine, 154
 - constant, 40
 - derived, 130
 - diagonalizable, 227
 - étale, 206
 - finite, 42, 204
 - general linear, 41
 - geometrically almost-simple, 421
 - linear, 72
 - multiplicative, 39, 231
 - multiplicative type, 230
 - of monomial matrices, 95
 - orthogonal, 455
 - over R , 20
 - perfect, 246
 - reductive, 136
 - semisimple, 135
 - simple, 418
 - simply connected, 350, 420
 - solvable, 129
 - split, 130
 - special orthogonal, 455
 - split reductive, 385
 - strongly connected, 129
 - toroidal, 246
 - trigonalizable, 291
 - trivial, 17, 40
 - unipotent, 252
 - split, 130, 266
- algebraic monoid, 17
- algebraic scheme, 493
 - affine, 492
 - complete, 511
 - étale, 206
 - finite, 505
 - integral, 495
 - nonsingular, 502
 - reduced, 495
 - regular, 501
 - separated, 499
 - singular, 502
- algebraic subgroup, 18
 - Cartan, 324
 - characteristic, 26
 - normal, 26
 - weakly characteristic, 34
- algebraic variety, 499
 - of connected components, 506
- almost-simple factor, 418
- α_p , 40
- anisotropic kernel, 465
- augmentation ideal, 28
- automorphism
 - inner, 49
 - automorphisms, 455
- base
 - for a root system, 436
- basis
 - orthogonal, 451
- bi-algebra, 178
- Borel pair, 316
- Borel subgroup
 - opposite, 404
- bracket, 183
- Campbell-Hausdorff series, 260
- Cartan subgroup, 324, 330
- Cartier pairing, 210
- Casimir element, 422
- Casimir operator, 422
- category
 - k -linear, 174
 - neutral Tannakian, 173
 - Tannakian, 173
 - tensor, 173
- central series, 129
- centralizer, 34
- centre, 34
 - of a Lie algebra, 192
- character, 75
- characteristic map, 351
- closed subfunctor, 31
- co-action, 70
- coalgebra, 174, 233
 - coétale, 233
- coboundaries, 271
- cocharacter
 - regular, 398
- cocommutative, 174, 233
- coconnected, 252
- cocycle, 469
- cocycles, 271
 - equivalent, 469
 - principal, 470
- coherent ideal, 494
- coherent module, 494
- coherent sheaf

- coherent, 493
- cokernel, 109
- commutative, 23
- comodule
 - free, 72
- component group, 93
- connected
 - strongly, 129
- connected components, 494
- connected-étale exact sequence, 94
- coordinate ring, 39
- coroots, 390
- crossed homomorphism, 269
 - principal, 269
- decomposition
 - Jordan, 168, 170
 - Jordan-Chevalley, 170
- defined over k , 27
- degree, 509
 - separable, 509
- dense, 503
 - schematically, 20
- DG , 130
- diagram, 421
- dimension
 - of an algebraic scheme, 500
- discrete Γ -set, 506
- \mathbb{D}_n , 41
- dominant, 443
- dual
 - Cartier, 209
- $E(G, M)$, 274
- effective epimorphism, 109
- eigenspace
 - generalized, 166
 - with character, 75
- eigenvalues
 - of an endomorphism, 166
- element
 - group-like, 75
 - semisimple, 170
 - unipotent, 170
 - universal, 496
- elementary unipotent, 263
- embedding, 82
- endomorphism
 - diagonalizable, 166
 - has all its eigenvalues, 166
 - locally finite, 169
 - nilpotent, 166
 - semisimple, 166
 - unipotent, 166
- equidimensional, 500
- étale, 247
- étale slice, 248, 249
- exact, 28
- exact sequence
 - connected étale, 94
- $\text{Ext}(G, M)$, 281
- extension
 - of algebraic groups, 28
- fat subfunctor, 81
- fibred product, 45
- finite algebraic p -group, 221
- flag, 149
 - maximal, 149
- flag variety, 149, 333
- form, 49
 - inner, 49
 - quadratic, 451
- Frobenius map, 44
- function
 - representative, 67
- functor
 - fibre, 173
 - representable, 19
- fundamental group, 350
- G° , 21
- G -module, 270
- G/N , 86
- \mathbb{G}_a , 39
- G^{der} , 130
- GL_n , 41
- \mathfrak{gl}_n , 184
- \mathfrak{gl}_V , 184
- \mathbb{G}_m , 39
- gradation, 172
- graded, 455
- group
 - affine, 171
 - Clifford, 462
 - Γ -, 469
 - isotropy, 142
 - of connected components, 93
 - root, 392
- group algebra, 226
- group-like element, 75, 225
- G_u , 302
- height
 - of a prime ideal, 499
- of an algebraic group, 44
- hermitian, 485
 - skew, 485
- Hochschild cohomology group, 271
- Hochschild extension, 274
 - equivalent, 274
 - trivial, 274
- $\underline{\text{Hom}}(G, G')$, 209, 235
- $\underline{\text{Hom}}(X, Y)$, 139
- homomorphism
 - faithfully flat, 507
 - flat, 507
 - Γ -, 470
 - normal, 105
 - of bialgebras, 178
 - of Lie algebras, 183
 - of superalgebras, 455
 - trivial, 17
- homomorphisms
 - compatible, 470
- Hopf algebra
 - coconnected, 252
- identity component, 21
- image, 85
- immersion, 495
 - closed, 495
 - open, 495
- index, 465
 - Witt, 454
- inner product, 433
- involution, 460, 480
 - of the first kind, 480
 - of the second kind, 480
- irreducible components, 494
- isogenous, 127
- isogeny, 44, 127
 - central, 44, 349
 - multiplicative, 349
 - of root data, 408
 - separable, 44
- isometry, 451
- Jacobi identity, 183
- Jordan decomposition, 168
- $k(X)$, 237
- k -algebra
 - affine, 499
 - small, 496
- kernel, 28
- Krull dimension, 500

- $\kappa(x)$, 493
- lattice, 434
 - partial, 434
 - root, 443
 - weight, 443
- Lemma
 - Yoneda, 496
- Lie subalgebra
 - separable, 245
- linear action, 137, 148
- linearly reductive, 241
- local system of parameters, 510
- locally finite endomorphism, 169
 - locally nilpotent, 169
 - locally unipotent, 169
 - semisimple, 169
- Luna map, 335
- map
 - lives in, 171
 - proper, 511
 - regular, 492, 493
- matrix group, 61
- module
 - Dieudonné, 222
- monomorphism, 83
- $\text{Mor}(X, Y)$, 32
- morphism
 - of affine algebraic schemes, 492
 - of algebraic schemes, 493
 - Verschiebung, 219
- μ_n , 40
- neighbourhood
 - étale, 510
- nilpotent series, 129
- nondegenerate, 148
- norm
 - reduced, 478
- normalizer, 33
- normalizes, 89
- object
 - monogenic, 175
- $\mathcal{o}(G)$, 42, 204
- open subset
 - basic, 492
- orbit, 142
- order
 - of a finite algebraic group, 42
- $\mathcal{O}_{X,x}$, 493
- part
 - semisimple, 170
 - unipotent, 170
- perfect pairing, 434
- plane
 - hyperbolic, 454
- point
 - nonsingular, 502
 - regular, 501
 - singular, 502
- primitive element, 261
- product, 44
 - almost direct, 418
 - semidirect, 45
 - semidirect defined by a map, 46
- quadratic space
 - anisotropic, 452
 - isotropic, 452
 - nondegenerate, 452
 - regular, 452
 - singular, 452
 - totally isotropic, 452
- quotient map, 82
- quotient object, 175
- radical, 135
 - geometric unipotent, 136
 - unipotent, 136
- rank, 357
 - of a root system, 435
- real algebraic envelope, 172
- reduced
 - geometrically, 499
- reductive group
 - split, 385
- reflection, 433, 452
 - with vector α , 433
- regular local ring, 242
- regular map
 - affine, 505
 - dominant, 504
 - 510
 - faithfully flat, 507
 - finite, 508
 - flat, 507
 - quasi-finite, 508
 - schematically dominant, 504
 - separable, 510
 - separated, 505
 - smooth, 510
 - surjective, 493
- regular system of parameters, 242
- $\text{Rep}(G)$, 165
- represent, 496
- representable, 98, 496
- representation
 - diagonalizable, 229
 - semisimple, 74
 - simple, 74
 - unipotent, 252
- rigid, 173
- ring
 - reduced, 495
 - regular, 500
- ringed space, 492
- root, 371
 - highest, 436
 - indecomposable, 436
 - special, 436
- root datum
 - semisimple, 393
 - toral, 393
- root system, 434
 - indecomposable, 435
- roots, 386, 390
 - of a root system, 435
 - simple, 436
- scheme
 - finite, 42
- semisimple abelian category, 232
- semisimple element, 170
- semisimple part, 168
- separably generated, 500
- series
 - characteristic, 125
 - composition, 127
 - derived, 133
 - normal, 125
 - subnormal, 125
 - central, 125
- set
 - Γ -, 469
- sheaf, 81
 - associated, 97
- simply connected central cover, 350
- singular locus, 501
- solvable series, 129
- space
 - primary, 166
 - quadratic, 451

- split solvable algebraic group, 130
- stabilizer, 71
- strong identity component, 129
- strongly connected, 129
- subalgebra
 - Lie, 183
- subgroup
 - Borel, 315
 - parabolic, 317
- subgroup variety, 18
- subobject, 175
 - generated by, 175
- subscheme, 495
 - closed, 494
 - open, 494
- sufficiently divisible, 166
- superalgebra, 455
- $\text{Sym}(V)$, 40
- tensor product
 - super, 455
- theorem
 - reconstruction, 165
- \mathbb{T}_n , 41
- topology
 - Zariski, 491
- torsor, 96, 145
- torus, 41, 230
 - quasi-trivial, 487
 - split, 230
- transcendence basis
 - separating, 500
- transcendence degree, 500
- transporter, 32
- trigonalizable, 167
- \mathbb{U}_n , 41
- unipotent element, 170
- unipotent part, 168
- universal covering, 350
- universal element, 496
- universal enveloping algebra, 194
- $V_{\mathfrak{a}}$, 40
- variety
 - flag, 149
 - rational, 237
 - unirational, 237
- vector
 - anisotropic, 451
 - isotropic, 451
- vector group, 41
- weight, 335
 - fundamental, 443
 - highest, 444
- Weyl chamber, 398
- Weyl group, 328, 390
- Witt vectors, 221
- $\langle X \rangle$, 175
- \tilde{X} , 496
- $X(G)$, 225
- $X^*(G)$, 231
- X^G , 140
- Zariski closure, 25
- zero functor, 31