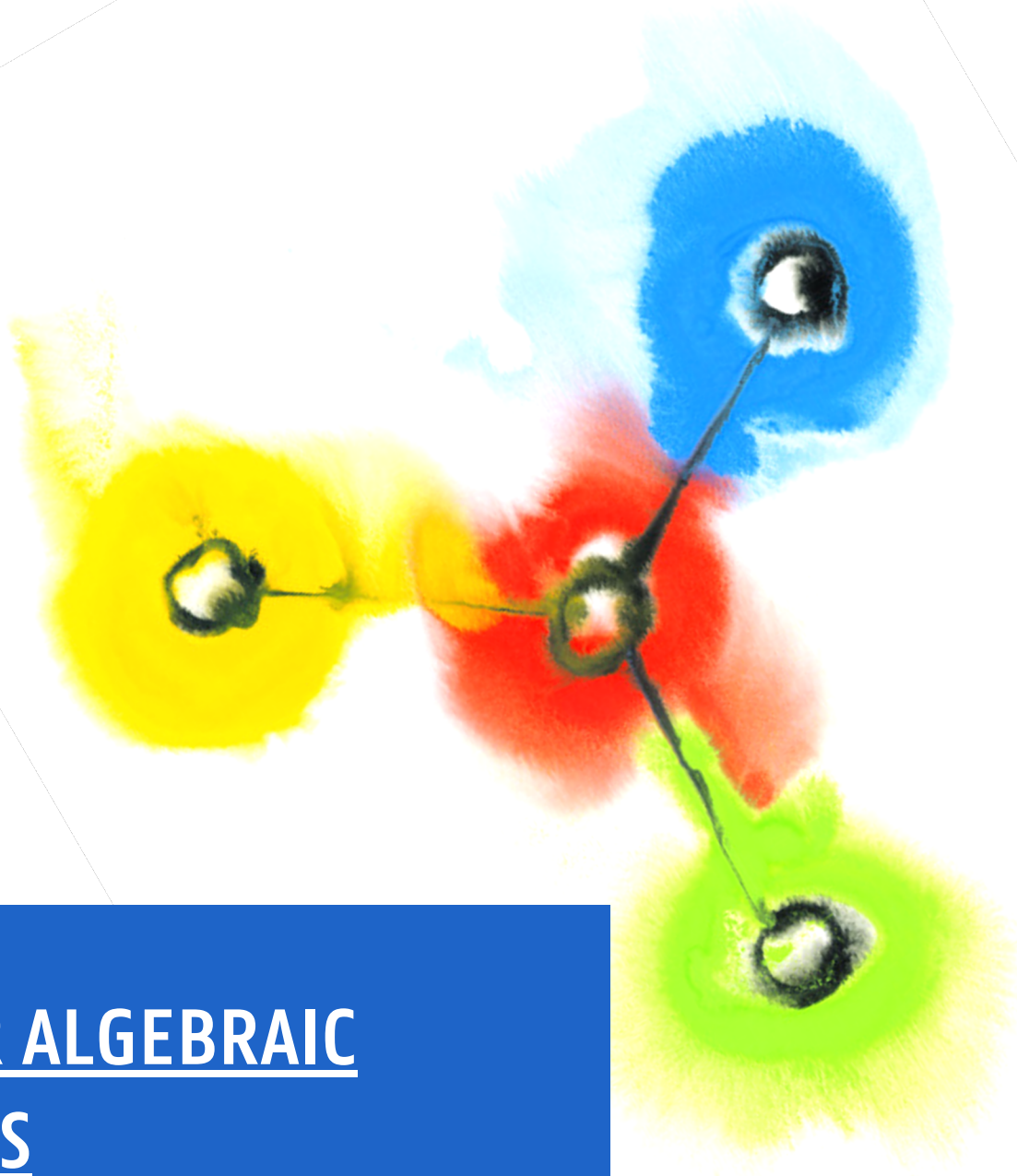
FACULTY OF SCIENCES



LINEAR ALGEBRAIC GROUPS

Tom De Medts
Department of Mathematics: Algebra and Geometry

Master of Mathematics
Academic year 2024–2025

GHENT UNIVERSITY

The picture on this front page is taken from "The Book of Involutions". It represents a Dynkin diagram of type D_4.

Preface

> *The leading pioneer in the development of the theory of algebraic groups was C. Chevalley. Chevalley's principal reason for interest in algebraic groups was that they establish a synthesis between the two main parts of group theory — the theory of Lie groups and the theory of finite groups. Chevalley classified the simple algebraic groups over an algebraically closed field and proved the existence of analogous groups over any field, in particular the finite Chevalley groups.*
>
> —R.W. Carter

Linear algebraic groups are matrix groups defined by polynomials; a typical example is the group SL_n of matrices of determinant one. The theory of algebraic groups was inspired by the earlier theory of Lie groups, and the classification of algebraic groups and the deeper understanding of their structure was one of the important achievements of last century, mainly led by A. Borel, C. Chevalley and J. Tits.

For a long time, the three main standard references on the topic were the books by Borel [Bor91], Humphreys [Hum75] and Springer [Spr09]. However, they all three have the disadvantage of taking the "classical" approach to algebraic groups, or more generally to algebraic geometry. Also the recent book by Malle and Testerman [MT11] follows this approach.

We have opted to follow the more "modern" approach, which describes algebraic groups as functors, and describes their coordinate algebra as Hopf algebras (which are not necessarily reduced, in constrast to the classical approach). This essentially means that we take the scheme-theoretical point of view on algebraic geometry. This might sound overwhelming and needlessly complicated, but it is not, and in fact, we will only need the basics in order to develop a deep understanding of linear algebraic groups. It will quickly become apparent that this functorial approach is very convenient.

Of course, this approach is not new, and the first reference (which is still an excellent introduction to the subject) is the book by Waterhouse [Wat79]. The most recent book covering the theory in great depth is the excellent monograph by Milne [Mil17] that I can highly recommend for further reading.

The current lecture notes are based mainly on online course notes by Milne that predated this book [Mil12a, Mil12b, Mil12c], in addition to online lecture notes by McGerty [McG10] and Szamuely [Sza12]. In fact, some

paragraphs have been copied almost ad verbatim, and I should perhaps apologize for not mentioning these occurrences throughout the text.

The interested reader who wants to understand the theory over arbitrary fields should have a look at Chapter VI of the Book of Involutions [KMRT98], which is rather condensely written, but in the very same spirit as the approach that we are taking in these course notes.

So why another version? For several reasons: I found the course notes of Milne and his more recent book, although extremely detailed and complete, in fact *too* detailed, and very hard to use in a practical course with limited time. In contrast, McGerty's notes —which unfortunately seem to have disappeared from the web— are too condensed for a reader not familiar with the topic. Szamuely's notes are very much to the point, but they don't go deep enough into the theory at various places. Finally, these course notes were written to be used in a Master course in Ghent University, and they are especially adapted to the background knowledge and experience of the students following this course.

This is why these course notes take off with a fairly long preliminary part: after an introductory chapter, there are three chapters on algebras, category theory and algebraic geometry. Linear algebraic groups —the main objects of study in this course— will be introduced only in Chapter 5.

I have chosen the classification of reductive linear algebraic groups over algebraically closed fields as the ultimate goal in this course. Of course, there is much to do beyond this —in some sense, the interesting things only start happening when we leave the world of algebraically closed fields— but already reaching this point is quite challenging. In particular, and mainly in the later chapters, some of the proofs have been omitted. I have nevertheless tried to indicate the lines of thought behind the structure theory, and my hope is that a reader who has reached the end of these course notes will have acquired some feeling for the theory of algebraic groups.

One of the main shortcomings in these course notes is the lack of (more) examples. However, the idea is that these course notes are accompanied by exercise classes, and this is where the examples should play a prominent role.

It has been exactly 10 years now since I wrote the first version of these course notes. Year after year, I have been making changes, sometimes minor, sometimes much more substantial. In many cases, these changes were based on excellent feedback that I received from students that took this course. I am always open for further comments and suggestions for improvement.

Tom De Medts (Ghent, January 2023) — Tom.DeMedts@UGent.be

Contents

Chapter 1 Introduction

Before we formally develop the theory of linear algebraic groups, we will give some examples that should give an impression of what to expect from this theory. We will also give an overview of the different types of algebraic groups that we will (or will not) encounter.

1.1 First examples

Definition 1.1.1. Let k be a (commutative) field. Roughly speaking, an *algebraic group* over k is a group that is defined by polynomials, by which we mean that the underlying set is defined by a system of polynomial equations, and also that the multiplication and the inverse in the group are given by polynomials. If the underlying set is defined as a subset of k^n (for some n), then we call it an *affine algebraic group*, and one of the fundamental results that we will prove later actually shows that every affine algebraic group is a *linear algebraic group* in the sense that it can be represented as a matrix group.

This definition admittedly is rather vague; we will later give a much more precise definition, which will require quite some more background, so the above definition will do for now. Some examples will clarify what we have in mind.

Examples 1.1.2. (1) SL_n.

If $A = (a_{ij}) \in \mathrm{Mat}_n(k)$ is an arbitrary matrix, then A belongs to $\mathsf{SL}_n(k)$ if and only if

$$\det A = \sum_{\sigma \in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = 1,$$

and this is clearly a polynomial expression in the a_{ij}'s. (Note that we have identified $\mathrm{Mat}_n(k)$ with k^{n^2} here.) Moreover, the multiplication of matrices in $\mathsf{SL}_n(k)$ is given by n^2 polynomials, as is the inverse (because the determinant of the matrices in $\mathsf{SL}_n(k)$ is 1).

(2) GL_n.

If $A = (a_{ij}) \in \mathrm{Mat}_n(k)$ is an arbitrary matrix, then A belongs to $\mathsf{GL}_n(k)$ if and only if

$$\det A = \sum_{\sigma \in \mathrm{Sym}_n} \mathrm{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \neq 0.$$

This doesn't look like a polynomial equation in the a_{ij}'s. Moreover, the inverse looks problematic because it is given by a rational function. Luckily, we can actually solve both problems simultaneously by *Rabinowitch's trick*:

$$\mathsf{GL}_n(k) = \big\{(a_{ij}, d) \in k^{n^2+1} \mid \det(a_{ij}) \cdot d = 1\big\}.$$

Observe that d plays the role of the inverse of the determinant of A; in particular, the inverse of A now involves *multiplying* with d, which results in a polynomial expression again.

(3) $\mathbb{G}_m$.

The group $\mathbb{G}_m$ is defined as GL_1, and it is simply called the *multiplicative group* of k. Notice that the formula from above now simplifies to the form

$$\mathbb{G}_m(k) = \big\{(s, t) \in k^2 \mid st = 1\big\}.$$

(4) $\mathbb{G}_a$.

The group $\mathbb{G}_a$ is called the *additive group* of k, and is defined by

$$\mathbb{G}_a(k) = k$$

(as a variety) with the addition in k as group operation. It is obvious that this is an affine algebraic group. In order to view it as a *linear* algebraic group, the addition has to correspond to matrix multiplication, which can be realized by the isomorphism

$$(k, +) \cong \left\{ \left(\begin{smallmatrix} 1 & a \\ & 1 \end{smallmatrix}\right) \mid a \in k \right\}.$$

1.2 The building bricks

We will now give an overview of five different types of algebraic groups, from which all other algebraic groups are built up. For the sake of simplicity, we will assume that $\mathrm{char}(k) = 0$.

1.2.1 Finite algebraic groups

Every finite group G can be realized as a subgroup of some $\mathsf{GL}_n(k)$, via

$$G \xhookrightarrow{\text{Cayley rep.}} \mathrm{Sym}_n \xhookrightarrow{\text{permutation mat.}} \mathsf{GL}_n(k).$$

The group G is indeed defined by polynomials, simply because it is a finite set. Indeed, a single element $g \in G$ can clearly be defined by n^2 linear equations, and a finite union of something that can be described with polynomial equations, can again be described with polynomial equations[1].

Such finite algebraic groups will be called *constant finite algebraic groups*.

1.2.2 Abelian varieties

Whereas affine algebraic groups are those algebraic groups that can be embedded into affine space, abelian varieties are algebraic groups that can be embedded into projective space.

Definition 1.2.1. An algebraic group is *connected* if it does not admit proper normal subgroups of finite index, or equivalently, if every finite quotient is trivial.

Definition 1.2.2. An *abelian variety* is a connected algebraic group which is projective as an algebraic variety.

The one-dimensional abelian varieties are precisely the *elliptic curves*. Abelian varieties are related to the integrals studies by Abel, and it is a happy coincidence that all abelian varieties are commutative[2].

1.2.3 Semisimple linear algebraic groups

Definition 1.2.3. Let G be a connected linear algebraic group. Then G is *simple* if G is non-abelian and does not admit any proper non-trivial algebraic normal subgroups. The group G is called *almost simple* or *quasisimple* if $Z(G)$ is finite and $G/Z(G)$ is simple.

Example 1.2.4. The group SL_n (with $n > 1$) is almost simple. Indeed, the center

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

[1] More formally, a finite union of algebraic varieties is again an algebraic variety; see Chapter 4 later.

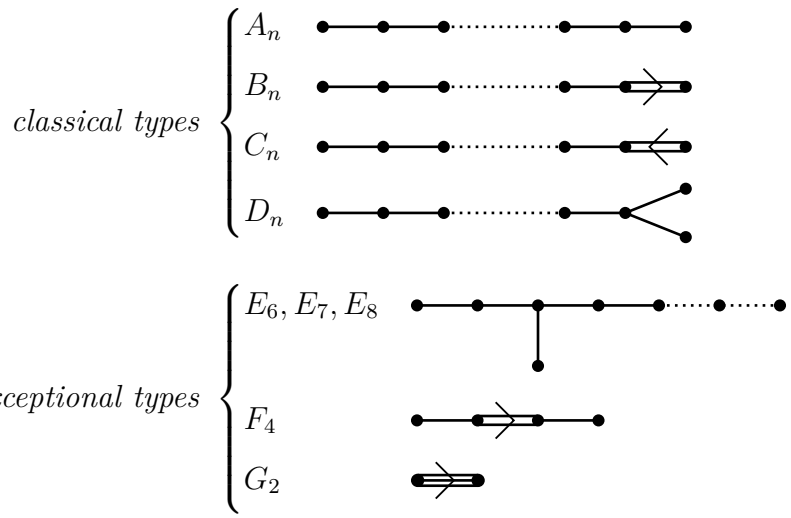
[2] This is a non-trivial fact, depending on the fact that a projective variety is *complete*. See also Definition 10.2.1 below.

is finite, and $\mathsf{PSL}_n = \mathsf{SL}_n/Z$ is simple[3].

Definition 1.2.5. Let G, H be linear algebraic groups. An *isogeny* from G to H is a surjective morphism $\varphi\colon G \twoheadrightarrow H$ with finite kernel. Two linear algebraic groups H_1 and H_2 are called *isogenous* if there exists a linear algebraic group G and isogenies $H_1 \twoheadleftarrow G \twoheadrightarrow H_2$. Being isogenous is an equivalence relation (exercise!).

The following classification result will certainly look very mysterious at this point, and one of the main goals of this course is precisely to understand the meaning of this major theorem.

Theorem 1.2.6. *Let k be an algebraically closed field with $\operatorname{char}(k) = 0$. Then every almost simple linear algebraic group over k is isogenous to exactly one of the following.*



The groups of type A_n are groups isogenous to the special linear group SL_{n+1}; the groups of type B_n are groups isogenous to the orthogonal group SO_{2n+1}; the groups of type C_n are groups isogenous to the symplectic group Sp_{2n}; the groups of type D_n are groups isogenous to the orthogonal group SO_{2n}.

Definition 1.2.7. A linear algebraic group G is an *almost direct product* of its subgroups $G_1, \ldots, G_r$ if the product map

$$\begin{aligned} G_1 \times \cdots \times G_r &\to G \\ (g_1, \ldots, g_r) &\mapsto g_1 \cdots g_r \end{aligned}$$

is an isogeny.

[3]We are ignoring the subtle fact that PSL_n is not even an algebraic group (but PGL_n is). See Remark 5.3.4(2) below.

Example 1.2.8. The group $G = (\mathsf{SL}_2 \times \mathsf{SL}_2)/N$ where $N = \{(I, I), (-I, -I)\}$ is an almost direct product of SL_2 and SL_2. Note, however, that it is *not* a direct product of almost simple subgroups.

Definition 1.2.9. A linear algebraic group G is *semisimple* if it is an almost direct product of almost simple subgroups.

We will later see a very different (but equivalent) definition in terms of the radical of the group; see Definition 11.1.2 below.

Remark 1.2.10. The group GL_n is *not* semisimple, but as we will see in a moment, it is a so-called reductive group; these groups are not too far from being semisimple (in a precise sense).

1.2.4 Groups of multiplicative type and tori

Definition 1.2.11. Let T be an algebraic subgroup of $\mathsf{GL}(V)$ for some n-dimensional vector space V over k. Then T is *of multiplicative type* if it is diagonalizable over the algebraic closure $\overline{k}$, i.e. if there exists a basis for $V(\overline{k}) = \overline{k}^n$ such that T is contained in

$$\mathbb{D}_n \coloneqq \left\{ A = \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \;\middle|\; A \text{ is invertible} \right\}.$$

If in addition T is connected, then we call T an *(algebraic) torus*.

We also recall the corresponding definition for individual elements of a group.

Definition 1.2.12. Let $G \leq \mathsf{GL}(V)$ be a linear algebraic group, and let $g \in G(k)$. Then g is *diagonalizable* if there exists a basis for $V(k)$ such that $g \in \mathbb{D}_n(k)$, and g is called *semisimple* if it is diagonalizable over $\overline{k}$.

1.2.5 Unipotent groups

Definition 1.2.13. Let G be an algebraic subgroup of $\mathsf{GL}(V)$ for some n-dimensional vector space V over k. Then G is *unipotent* if there exists a basis for $V(k)$ such that G is contained in

$$\mathbb{U}_n \coloneqq \left\{ \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Definition 1.2.14. Let $G \leq \mathsf{GL}(V)$ be a linear algebraic group, and let $g \in G(k)$. Then g is *unipotent* if the following equivalent conditions are satisfied:

(i) $g-1$ is nilpotent, i.e. $(g-1)^N = 0$ for some N;

(ii) the characteristic polynomial $\chi_g(t)$ for g is a power of $(t-1)$;

(iii) all eigenvalues of g in $\overline{k}$ are equal to 1.

1.3 Extensions

1.3.1 Solvable groups

Definition 1.3.1. A linear algebraic group G is *solvable* if there is a chain of algebraic subgroups

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1$$

such that each factor G_i/G_{i+1} is abelian.

Examples 1.3.2. (1) The group $\mathbb{U}_n$ is solvable.

(2) The group

$$\mathbb{T}_n \coloneqq \left\{ A = \begin{pmatrix} * & * & * \\ 0 & \ddots & * \\ 0 & 0 & * \end{pmatrix} \;\middle|\; A \text{ is invertible} \right\}$$

is solvable; notice that $\mathbb{T}_n/\mathbb{U}_n \cong \mathbb{D}_n$.

The following important result (which we will come back to later) shows that when k is algebraically closed, every connected solvable algebraic group can be realized as a group of upper triangular matrices.

Theorem 1.3.3 (Lie–Kolchin)**.** *Let k be an algebraically closed field, and let $G \leq \mathsf{GL}(V)$ be a connected linear algebraic group. Then G is solvable if and only if there is a basis for $V(k)$ such that $G \leq \mathbb{T}_n$.*

1.3.2 Reductive groups

Definition 1.3.4. A connected linear algebraic group is called *reductive* if it does not admit any non-trivial connected unipotent normal subgroups.

When $\mathrm{char}(k) = 0$, any reductive group is an extension of a semisimple group by a torus:

$$1 \to T \to G \to G/T \to 1,$$

where G/T is semisimple. This is no longer true for fields of positive characteristic, but it is still almost true (in a precise sense); this has recently led to the study of so-called pseudo-reductive groups [CGP15, CP16].

Example 1.3.5. The group GL_n is reductive:

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

1.3.3 Disconnected groups

Recall that an algebraic group is disconnected if it admits an algebraic normal subgroup of finite index > 1. We will give two different examples illustrating that disconnected groups come up naturally in certain situations.

Examples 1.3.6. (1) The *orthogonal group* O_n is defined by

$$\mathsf{O}_n(k) \coloneqq \{A \in \mathsf{GL}_n(k) \mid A^t A = I\}.$$

Since the determinant of an orthogonal matrix is always 1 or -1, the *special orthogonal subgroup* SO_n defined by

$$\mathsf{SO}_n(k) \coloneqq \{A \in \mathsf{O}_n(k) \mid \det A = 1\}$$

is a normal subgroup of index 2:

$$1 \to \mathsf{SO}_n \to \mathsf{O}_n \xrightarrow{\det} \mathbb{Z}/2\mathbb{Z} \to 1.$$

Therefore, the group O_n is not connected. (The group SO_n is connected, but that is certainly a non-trivial fact.)

(2) A matrix is called *monomial* if it has exactly one non-zero entry on each row and each column. The group Mon_n defined by

$$\mathrm{Mon}_n(k) \coloneqq \{A \in \mathsf{GL}_n \mid A \text{ is monomial}\}$$

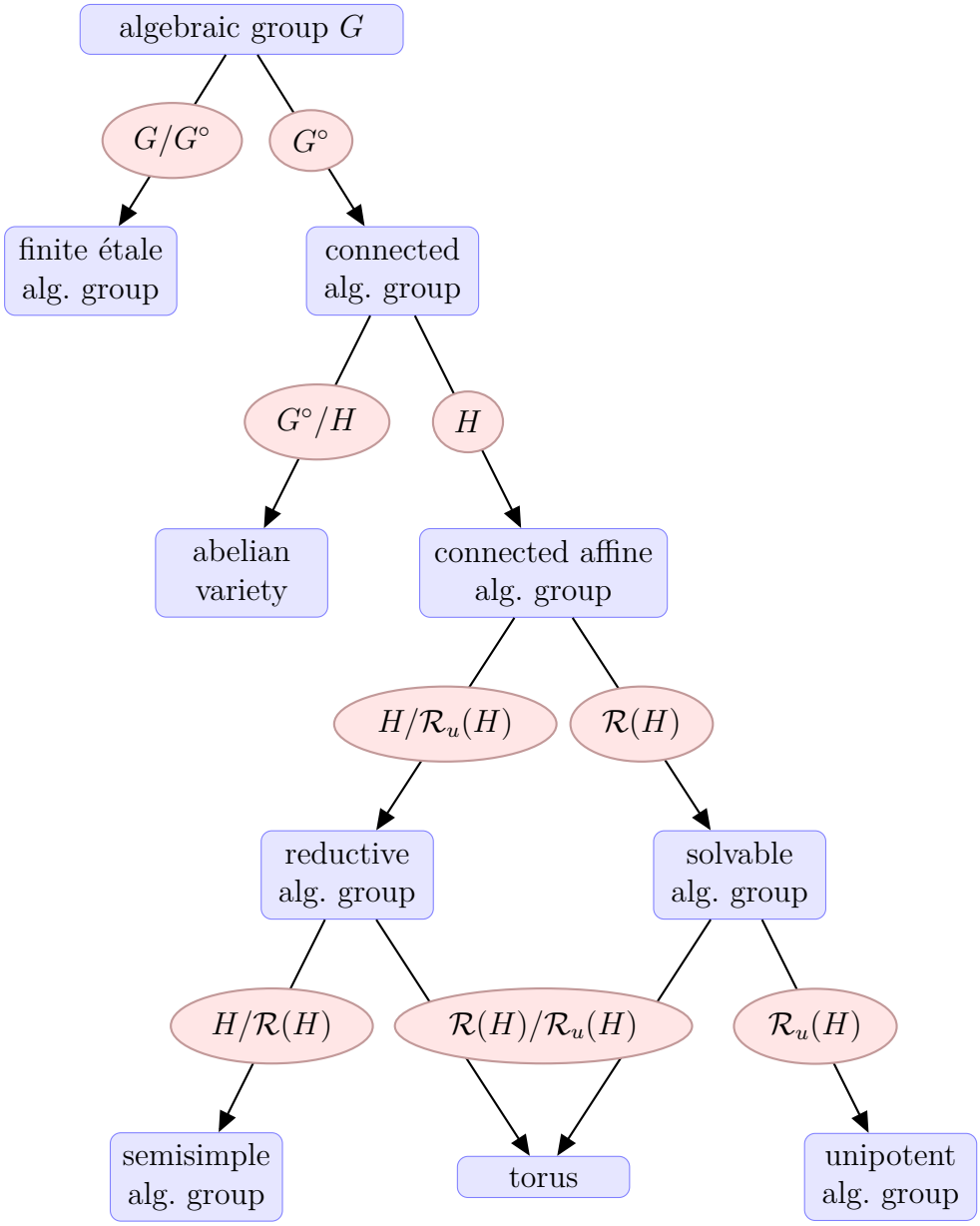
is disconnected:

$$1 \to \mathbb{D}_n \to \mathrm{Mon}_n \to \mathrm{Sym}_n \to 1.$$

Notice that this group arises naturally as the normalizer of $\mathbb{D}_n$ inside GL_n.

1.4 Overview

We finish this introductary chapter by presenting an overview of how an arbitrary algebraic group can be decomposed into smaller pieces that we are more likely to understand. We assume that $\mathrm{char}(k) = 0$.


algebraic group G
G/G°
G°
finite étale alg. group
connected alg. group
G°/H
H
abelian variety
connected affine alg. group
$H/\mathcal{R}_u(H)$
$\mathcal{R}(H)$
reductive alg. group
solvable alg. group
$H/\mathcal{R}(H)$
$\mathcal{R}(H)/\mathcal{R}_u(H)$
$\mathcal{R}_u(H)$
semisimple alg. group
torus
unipotent alg. group

Chapter 2 Algebras

In order to build up the theory of linear algebraic groups, it will be essential to have a good understanding of commutative k-algebras. We take the opportunity to introduce the theory of k-algebras in general (not restricting to commutative algebras), since these algebras will allow us to give interesting examples of certain types of linear algebraic groups anyway.

We will often use K for a commutative ring (always assumed to be a ring with 1) and k for a commutative field.

2.1 Definitions and examples

Definition 2.1.1. Let K be a commutative ring.

(i) An *algebra over* K or a K*-algebra* is a (not necessarily commutative) ring A with 1 which is also a K-module, such that the multiplication in A is K-bilinear:

$$\alpha x \cdot y = x \cdot \alpha y = \alpha(xy)$$

for all $x, y \in A$ and all $\alpha \in K$.

(ii) A *morphism* of K-algebras is a K-linear ring morphism.

(iii) A *subalgebra* of a K-algebra is a subring which is also a K-submodule.

(iv) A *left ideal* of a K-algebra A is a K-submodule I of A such that $AI \subseteq I$; a *right ideal* is defined similarly. A *two-sided ideal* (or simply an *ideal*) is a submodule which is simultaneously a left and right ideal.

(v) The *center* of a K-algebra A is the subalgebra

$$Z(A) := \{z \in A \mid zx = xz \text{ for all } x \in A\}.$$

(vi) The natural map

$$\eta\colon K \to A\colon \alpha \mapsto \alpha \cdot 1$$

is a ring morphism from K to $Z(A)$, which is called the *structure morphism* of A.

Remarks 2.1.2. (i) The structure morphism η is not necessarily injective, and hence K is not always a subalgebra of A. (For instance, $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-algebra.) On the other hand, if $K = k$ is a field, then η is always injective, and then we can consider k as a subalgebra of A by identifying k with $k \cdot 1 \subseteq A$.

(ii) Given a not necessarily commutative ring A with 1 and a ring morphism $\eta\colon K \to Z(A)$, we can make A into a K-algebra by endowing it with the K-module structure

$$\alpha \cdot x \coloneqq \eta(\alpha)x$$

for all $\alpha \in K$ and all $x \in A$; the map η is then precisely the structure morphism of the K-algebra A.

(iii) It is also possible to define a K-algebra more generally as a K-module A endowed with a K-bilinear multiplication, without assuming A to be a ring. In particular, A might not have a unit 1, and A might not be associative. If A has a unit 1, then it is called a *unital K-algebra*. These not necessarily associative algebras turn up very often in the study of the exceptional linear algebraic groups. For instance, each algebraic group of type G_2 can be realized as the automorphism group of a so-called *octonion algebra*, which is a certain 8-dimensional non-associative unital algebra.
Another important family of non-associative non-unital algebras is given by the *Lie algebras*, which we will study in more detail in Chapter 7.

(iv) If $K = k$ is a field, then any k-algebra A (in the general sense from above) is in particular a vector space over k, with some basis $(u_i)_{i\in I}$. In this case, the multiplication on A is completely determined by its *structure constants* $\gamma_{ijr} \in k$:

$$u_i \cdot u_j = \sum_{r\in I} \gamma_{ijr} u_r,$$

for all $i, j \in I$, and where for fixed i and j, the constants γ_{ijr} are non-zero for finitely many $r \in I$ only.

Definition 2.1.3. If every non-zero element of a K-algebra A has an inverse, then we call A a *skew field*. Of course, this implies in particular that $Z(A)$ is a field, and A is a k-algebra for $k = Z(A)$. (Notice that k might be different from K, however, and K is not necessarily a field.) If in addition $\dim_k A$ is finite, then we call A a *division algebra* or a *division ring*[1].

[1]Some care is needed, since some authors do not make this distinction between skew fields and division rings. Most of the time, however, this should be clear from the context.

Examples 2.1.4. Let K be a commutative ring.

(1) Every ring is a $\mathbb{Z}$-algebra, and conversely.

(2) The set $T_n(K)$ of all[2] upper-triangular n by n matrices over K is a K-algebra, with structure morphism

$$\eta\colon K \to T_n(K)\colon \alpha \mapsto \operatorname{diag}(\alpha, \dots, \alpha).$$

(3) Let V be a K-module, and $A = \operatorname{End}_K(V)$. Then A is a K-module defined by

$$(\alpha \cdot f)(x) \coloneqq \alpha f(x) \quad \text{for all } x \in V,$$

for all $\alpha \in K$ and all $f \in A$. This K-module structure makes the ring A into a K-algebra.
If V is free of rank n, then $A \cong \operatorname{Mat}_n(K)$.

(4) Let M be a *monoid*, i.e. a set endowed with a binary associative operation with a neutral element[3]. Let A be the free K-module over M, and endow A with the multiplication induced by M. Then A is a K-algebra, which we denote by $A = KM$, and which we call the *monoid K-algebra* induced by M. If $M = G$ is a group, then we call $A = KG$ the *group K-algebra* induced by G. We give some concrete examples.

   (a) Let $M = \{1, x, x^2, \dots\}$. Then M is a monoid which is not a group; the corresponding monoid algebra KM is isomorphic to the polynomial algebra $K[x]$.

   (b) Let $M = \langle x \rangle$ be an infinite cyclic group. Then the group algebra KM is isomorphic to the algebra of Laurent polynomials $K[x, x^{-1}]$.

   (c) Let $M = \langle x \rangle$ be a cyclic group of order n. Then $KM \cong K[x]/(x^n - 1)$.

   (d) Let M be the free monoid on $\{x_1, \dots, x_n\}$. Then KM is called the *free associative algebra* on $x_1, \dots, x_n$, and is denoted by $K\langle x_1, \dots, x_n \rangle$.

It is an easy but important fact that every finite-dimensional k-algebra can be embedded into a matrix algebra. (This fact can be compared to the Cayley representation for finite groups, which embeds an arbitrary finite group into a symmetric group.)

Definition 2.1.5. Let A be a finite-dimensional k-algebra. A *(matrix) representation* for A is a k-algebra morphism $\rho\colon A \to \operatorname{Mat}_r(k)$ for some natural number r. If ρ is injective, then the representation is called *faithful*.

[2] including the non-invertible ones, so this is not the same as $\mathbb{T}_n(K)$ defined above.
[3] Informally, a monoid is a group without inverses.

Theorem 2.1.6. *Let A be a finite-dimensional k-algebra. Then A is isomorphic to a subalgebra of* $\mathrm{Mat}_n(k)$*, i.e. A has a faithful representation.*

Proof. For each $a \in A$, the map

$$\lambda_a \colon A \to A \colon x \mapsto ax$$

is an element of $\mathrm{End}_k(A) \cong \mathrm{Mat}_n(k)$. The corresponding map

$$\lambda \colon A \to \mathrm{Mat}_n(k) \colon a \mapsto \lambda_a$$

is an algebra morphism. Clearly, λ_a is the zero map only for $a = 0$, hence the morphism λ is injective. □

The representation λ that we have constructed in the previous proof is called the *left regular representation* for A. Of course, one can similarly define the *right regular representation* for A.

2.2 Tensor products

In our future study of algebraic varieties, the tensor product of (commutative) k-algebras will be invaluable. In fact, in the category of commutative[4] k-algebras, the tensor product turns out to be precisely the so-called coproduct, which already illustrates its importance. But first, we will have a closer look at tensor products of K-modules in general (where K is still a commutative ring with 1).

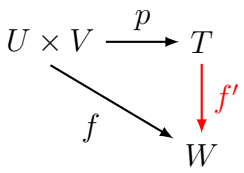
2.2.1 Tensor products of K-modules

Tensor products are intimately related to bilinear forms, and in fact, the tensor product is, in a precise sense that we will describe below, the most universal object to which a bilinear form from the pair U, V can map, in the sense that every other bilinear map *factors through* the tensor product.

Definition 2.2.1. Let U and V be two K-modules. The *tensor product* of U and V is defined to be a pair (T, p) consisting of a K-module T and a K-bilinear map $p \colon U \times V \to T$, such that for every K-module W and every K-bilinear map $f \colon U \times V \to W$, there is a unique K-module morphism

[4]It is *not* true that the tensor product is the coproduct in the category of all k-algebras.

$f' \colon T \to W$ such that $f = f' \circ p$.



Notice that it is not immediately obvious that the tensor product exists at all, but as we will see in a minute, it is not too hard to see that if it exists, it is necessarily unique; we will denote T by $U \otimes_K V$ or by $U \otimes V$ if the ring K is clear from the context (which is *not* always the case!). We will rarely explicitly write down p, i.e. we will simply say that $T = U \otimes_K V$ *is* the tensor product of U and V.

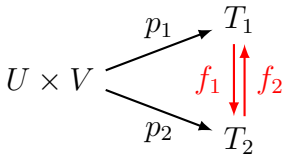
Lemma 2.2.2. *Let U and V be two K-modules. If the tensor product of U and V exists, then it is unique.*

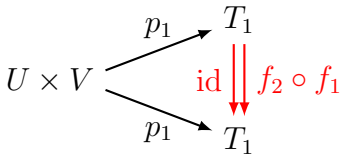
Proof. The proof will only use the universality of the defining property; the fact that U and V are K-modules will turn out to be irrelevant.

So assume that (T_1, p_1) and (T_2, p_2) are two tensor products of U and V. We first invoke the universal property for T_1 to obtain a (unique) morphism $f_1 \colon T_1 \to T_2$ such that $p_2 = f_1 \circ p_1$; similarly, there is a unique morphism $f_2 \colon T_2 \to T_1$ such that $p_1 = f_2 \circ p_2$. Hence

$$p_1 = (f_2 \circ f_1) \circ p_1 \quad \text{and} \quad p_2 = (f_1 \circ f_2) \circ p_2.$$

We now use the universal property for T_1 again, but this time with $W = T_1$ and $f = p_1$. By the uniqueness aspect of the universal property, we get that $f_2 \circ f_1 = \mathrm{id}_{T_1}$, and similarly $f_1 \circ f_2 = \mathrm{id}_{T_2}$. We conclude that f_1 is an isomorphism from T_1 to T_2, and hence the pairs (T_1, p_1) and (T_2, p_2) are isomorphic.





□

We will now show how to construct the tensor product of two K-modules; this will at the same time prove the existence of the tensor product. The idea is that we first consider a free object, from which we construct the tensor product by modding out the required relations.

Construction 2.2.3. Let U and V be two K-modules. Define A to be the free K-module over the set $U \times V$. Now consider the submodule

$$B \coloneqq \left\langle \begin{matrix} (u+u',v)-(u,v)-(u',v), \\ (u,v+v')-(u,v)-(u,v'), \\ (\alpha u,v)-\alpha(u,v),\ (u,\alpha v)-\alpha(u,v) \end{matrix} \;\middle|\; u,u' \in U, v,v' \in V, \alpha \in K \right\rangle.$$

Finally, let $T \coloneqq A/B$, and let $p\colon U \times V \to T$ be the composition

$$p\colon U \times V \hookrightarrow A \twoheadrightarrow T.$$

It is not too hard to check that the pair (T,p) satisfies the universal property defining the tensor product, and hence T is indeed the tensor product $U \otimes_K V$.

Remarks 2.2.4. (i) We will usually write $T = U \otimes_K V$, even though the tensor product is in principle only defined up to isomorphism. Typically, we have the above construction in mind when we write such an equality (rather than an isomorphism). In particular, the image $p(u,v)$ of a pair $(u,v) \in U \times V$ under p will be written as $u \otimes v$.

(ii) It is a common beginners' mistake to write an arbitrary element of $T = U \otimes_K V$ as $u \otimes v$. These elements only *generate* T as a K-module, and hence an arbitrary element of T is a finite sum

$$x = \sum_i u_i \otimes v_i,$$

where $u_i \in U$ and $v_i \in V$.

(iii) The universal property of tensor products can conveniently be rephrased by the isomorphism

$$\mathrm{Hom}_K(U \otimes_K V, W) \cong \mathrm{Hom}_K(U, \mathrm{Hom}_K(V,W)).$$

This property is known as *adjoint associativity*.

We now list a few properties of the tensor product, the proof of which we leave to the reader.

Properties 2.2.5. *Let U,V,W be K-modules. Then*

(i) $U \otimes V \cong V \otimes U$;

(ii) $U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$;

(iii) $U \otimes (V \oplus W) \cong (U \otimes V) \oplus (U \otimes W)$;

(iv) $U \otimes K^n \cong U^n$;

(v) $K^n \otimes K^m \cong K^{nm}$.

In fact, we can make properties (iv) and (v) more precise, as follows.

Proposition 2.2.6. *Let U be a K-module and V a free K-module of rank n, with basis $(e_1, \ldots, e_n)$. Then every element x of $U \otimes_K V$ can be uniquely written as*

$$x = \sum_{i=1}^{n} u_i \otimes e_i$$

with $u_i \in U$.

Proof. First prove the statement for $n = 1$ using the universal property of tensor products. Then deduce the general statement by induction on n, using the distributive property 2.2.5(iii). We leave the details as an exercise. □

Definition 2.2.7. If $f\colon U \to V$ and $g\colon U' \to V'$ are two K-module morphisms, then we define

$$f \otimes g\colon U \otimes_K U' \to V \otimes_K V'\colon u \otimes v \mapsto f(u) \otimes g(v).$$

By the universal property defining tensor products, this is a well defined K-module morphism.

Remark 2.2.8. If $f\colon U \to V$ is an injective K-module morphism, then the induced morphism

$$f \otimes \mathrm{id}\colon U \otimes W \to V \otimes W$$

is *not* always injective! (Consider for instance the map $f\colon 2\mathbb{Z} \to \mathbb{Z}$ given by inclusion, and let $W = \mathbb{Z}/2\mathbb{Z}$.) If K is a field, however, then $f \otimes \mathrm{id}$ remains injective.

In fact, this leads to an important notion: a K-module W is called *flat* precisely when, for *each* injective morphism $f\colon U \to V$ of K-modules, the induced morphism $f \otimes \mathrm{id}\colon U \otimes W \to V \otimes W$ is injective.

2.2.2 Tensor products of K-algebras

Recall that a K-algebra is a K-module equipped with a K-bilinear multiplication (which is not necessarily associative and does not necessarily have a neutral element). In fact, by the universal property of tensor products, we can view the multiplication as a morphism

$$\mathbf{m}\colon A \otimes A \to A.$$

It is interesting to express the unit element and the associativity in terms of this morphism $\mathbf{m}$. The algebra A is associative if and only if the maps $\mathbf{m} \circ (\mathbf{m} \otimes \mathrm{id})$ and $\mathbf{m} \circ (\mathrm{id} \otimes \mathbf{m})$ from $A \otimes A \otimes A$ to A coincide, i.e. if and only if the following diagram commutes:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mathbf{m} \otimes \mathrm{id}} & A \otimes A \\ {\scriptstyle \mathrm{id} \otimes \mathbf{m}} \downarrow & & \downarrow {\scriptstyle \mathbf{m}} \\ A \otimes A & \xrightarrow{\mathbf{m}} & A \end{array}$$

On the other hand, the algebra A is unital, with unit $e \in A$, if and only if

$$\mathbf{m}(e \otimes x) = x = \mathbf{m}(x \otimes e)$$

for all $x \in A$. This can be expressed in a more fancy fashion, using the structure morphism η:

$$\mathbf{m} \circ (\eta \otimes \mathrm{id}) = \pi_A = \mathbf{m} \circ (\mathrm{id} \otimes \eta),$$

where π_A is the natural isomorphism from $K \otimes_K A$ to A. Equivalently, the following diagrams commute:

$$\begin{array}{ccc} K \otimes A & \xrightarrow{\eta \otimes \mathrm{id}} & A \otimes A \\ {\scriptstyle \pi_A} \downarrow & & \downarrow {\scriptstyle \mathbf{m}} \\ A & = & A \end{array} \qquad \begin{array}{ccc} A \otimes K & \xrightarrow{\mathrm{id} \otimes \eta} & A \otimes A \\ {\scriptstyle \pi_A} \downarrow & & \downarrow {\scriptstyle \mathbf{m}} \\ A & = & A \end{array}$$

With this in mind, we can give an intrinsic description of the tensor product of two K-algebras.

Definition 2.2.9. Let A and B be two K-algebras, with multiplication morphisms $\mathbf{m}$ and $\mathbf{n}$, respectively. Let $C = A \otimes_K B$ as a K-module. In order to make C into a K-algebra, it only remains to describe the multiplication morphism $\mathbf{z}$. First, define[5] a morphism

$$\tau \colon A \otimes B \to B \otimes A \colon a \otimes b \mapsto b \otimes a$$

[5]Recall that an arbitrary element of $A \otimes B$ is of the form $\sum_i a_i \otimes b_i$, but in order to describe a morphism from $A \otimes B$ to a third module M, it suffices to prescribe the morphism on the set of generators $\{a \otimes b \mid a \in A, b \in B\}$.

for all $a \in A$ and all $b \in B$. Now let

$$\mathbf{z} \coloneqq (\mathbf{m} \otimes \mathbf{n}) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \colon A \otimes B \otimes A \otimes B \to A \otimes B.$$

Explicitly, if $a_1, a_2 \in A$ and $b_1, b_2 \in B$, then the multiplication satisfies

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2,$$

and by K-bilinearity, this formula also uniquely defines the multiplication of two arbitrary elements of $A \otimes B$.

Examples 2.2.10. (1) Let A be an arbitrary K-algebra. We claim that

$$A \otimes_K \mathrm{Mat}_n(K) \cong \mathrm{Mat}_n(A).$$

Indeed, note that this isomorphism certainly holds as K-modules. By Proposition 2.2.6, every element of $A \otimes \mathrm{Mat}_n(K)$ can be uniquely written as

$$x = \sum_{i,j=1}^{n} a_{ij} \otimes e_{ij}$$

with $a_{ij} \in A$, and where (e_{ij}) is the canonical basis of $\mathrm{Mat}_n(K)$. By the definition of the tensor product of K-algebras, it is now clear that the K-module isomorphism

$$\varphi \colon A \otimes \mathrm{Mat}_n(K) \to \mathrm{Mat}_n(A) \colon \sum_{i,j=1}^{n} a_{ij} \otimes e_{ij} \mapsto (a_{ij})$$

is indeed a K-algebra isomorphism.

(2) A special case of the previous example is obtained if A is itself a full matrix algebra:

$$\mathrm{Mat}_r(K) \otimes_K \mathrm{Mat}_n(K) \cong \mathrm{Mat}_{rn}(K).$$

(3) Consider the polynomial algebra $K[x]$ in one variable. Then

$$K[x] \otimes_K K[x] \cong K[x, y],$$

the polynomial algebra over K in two variables.

(4) Another important example is given by *extension of scalars*. Let A be a k-algebra (where k is a field), and suppose that E/k is a field extension. Then $A \otimes_k E$ is not only a k-algebra, but also an E-algebra, with $\dim_E(A \otimes_k E) = \dim_k A$. This algebra is often simply denoted by A_E. Notice that by Proposition 2.2.6, if $(e_1, \ldots, e_n)$ is a basis for A as a k-vector space, then $(e_1 \otimes 1, \ldots, e_n \otimes 1)$ is a basis for A_E as an E-vector space.

Chapter 3 Categories

Category theory often looks quite daunting when first encountered. It is a theory that looks too abstract to be meaningful. However, as we will see, it is actually very powerful when used appropriately. It is not only a useful "language", but it also allows to switch from one interpretation to another in a mathematically rigorous fashion.

We will later introduce linear algebraic groups as *functors*, which go from one category to another. This will allow us to switch viewpoints between linear algebraic groups as group functors on the one hand, and Hopf algebras on the other hand. The abstract tool that will connect these two viewpoints is the Yoneda Lemma, which is sometimes referred to as a "deep triviality".

3.1 Definition and examples

Definition 3.1.1. A *category* $\mathcal{C}$ consists of a class $\mathrm{ob}(\mathcal{C})$ of *objects* and a class $\mathrm{mor}(\mathcal{C})$ or $\hom(\mathcal{C})$ of *morphisms*. Each morphism $\alpha \in \hom(\mathcal{C})$ has two associated objects, called the *source* ($X \in \mathrm{ob}(\mathcal{C})$) and the *target* ($Y \in \mathrm{ob}(\mathcal{C})$), and we write

$$\alpha \colon X \to Y \quad \text{or} \quad X \xrightarrow{\alpha} Y.$$

The class of all morphisms with source X and target Y will be denoted by $\hom(X, Y)$. Moreover, the category $\mathcal{C}$ comes equipped with a *composition* of morphisms

$$\hom(X, Y) \times \hom(Y, Z) \to \hom(X, Z) \colon (\alpha, \beta) \mapsto \alpha \cdot \beta = \alpha\beta.$$

(We sometimes write $\beta \circ \alpha$ for $\alpha\beta$.) In order to be a category, the objects, morphisms and composition have to satisfy the following two axioms:

Associativity of composition. If $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \xrightarrow{\gamma} T$, then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Identity morphisms. For each $X \in \mathrm{ob}(\mathcal{C})$ there is an $\mathrm{id}_X \in \hom(X, X)$ such that for each $X \xrightarrow{\alpha} Y$ we have $\mathrm{id}_X \cdot \alpha = \alpha = \alpha \cdot \mathrm{id}_Y$.

Remarks 3.1.2. (i) Observe that $\mathrm{ob}(\mathcal{C})$ and $\hom(\mathcal{C})$ are classes and not sets. This is important from a set-theoretic point of view, but we will not have to worry about these subtleties. It is worth pointing out that many categories are *locally small* in the sense that $\hom(X, Y)$ is a set for all $X, Y \in \mathrm{ob}(\mathcal{C})$. If this is the case, then it is natural (and often part of the definition) to require[1] in addition that

$$\hom(X, Y) \cap \hom(X', Y') = \emptyset \quad \text{unless } X = X' \text{ and } Y = Y'.$$

(ii) It is customary to say that a morphism $\alpha \in \hom(X, Y)$ is a morphism *from X to Y*. Some care is needed, however, since morphisms might behave very differently from ordinary maps in the set-theoretic sense.

Examples 3.1.3. (1) We list some common categories.

Name	Objects	Morphisms
Set	sets	maps
Grp	groups	group morphisms
AbGrp	abelian groups	group morphisms
Top	topological spaces	continuous maps
$\mathbf{Top^0}$	top. spaces with base pt.	cont. maps preserving base pts.
$\mathbf{Mod}_R$	right R-modules	R-module morphisms
${}_R\mathbf{Mod}$	left R-modules	R-module morphisms
Ring	rings with 1	ring morphisms preserving 1
Rng	rings	ring morphisms
$\mathbf{Vec}_k$	vector spaces over k	linear maps
k-**alg**	comm. assoc. k-algebras	algebra morphisms

(2) There exist categories of a very different nature. For instance, let M be an arbitrary monoid. Then we can view M as a category with *one* object (often denoted by $*$), such that the morphisms in the category correspond to the elements of M and composition of morphisms corresponds to the monoid operation in M.

Definition 3.1.4. (i) Let $X \xrightarrow{\alpha} Y$. A morphism $\beta\colon Y \to X$ such that $\alpha\beta = \mathrm{id}_X$ and $\beta\alpha = \mathrm{id}_Y$ is called an *inverse* for α. The inverse of α is unique if it exists, and is then denoted by α^{-1}. In this case, α is called an *isomorphism*, and X and Y are *isomorphic* objects.

(ii) A category $\mathcal{C}$ is called *small* if both $\mathrm{ob}(\mathcal{C})$ and $\hom(\mathcal{C})$ are sets (rather than classes). For instance, the categories from Example 3.1.3(2) are small.

[1] Observe that this requirement only makes sense because $\hom(X, Y)$ and $\hom(X', Y')$ are sets, and hence can be intersected.

(iii) A *subcategory* of a category $\mathcal{C}$ is a collection of objects and morphisms from $\mathcal{C}$ that form a category under the composition of $\mathcal{C}$. In particular, if $\mathcal{D}$ is a subcategory of $\mathcal{C}$, then

$$\hom_{\mathcal{D}}(X, Y) \subseteq \hom_{\mathcal{C}}(X, Y)$$

for all $X, Y \in \mathrm{ob}(\mathcal{D})$.

(iv) If $\mathcal{D}$ is a subcategory of $\mathcal{C}$ such that

$$\hom_{\mathcal{D}}(X, Y) = \hom_{\mathcal{C}}(X, Y)$$

for all $X, Y \in \mathrm{ob}(\mathcal{D})$, then we call $\mathcal{D}$ a *full subcategory* of $\mathcal{C}$. For instance, **AbGrp** is a full subcategory of **Grp**.

(v) If $\mathcal{C}$ is a category, then we can define its *opposite category* $\mathcal{C}^{\mathrm{op}}$ by "reversing the arrows": $\mathrm{ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{ob}(\mathcal{C})$, and for all $X, Y \in \mathrm{ob}(\mathcal{C})$, we declare

$$\hom_{\mathcal{C}^{\mathrm{op}}}(Y, X) \coloneqq \hom_{\mathcal{C}}(X, Y).$$

For clarity, we denote the morphism in $\mathcal{C}^{\mathrm{op}}$ corresponding to the morphism $\alpha \in \hom(X, Y)$ by $\alpha^{\mathrm{op}} \in \hom(Y, X)$. The composition in $\mathcal{C}^{\mathrm{op}}$ is also reversed: $(\alpha\beta)^{\mathrm{op}} = \beta^{\mathrm{op}}\alpha^{\mathrm{op}}$ for all suitable $\alpha, \beta \in \hom(\mathcal{C})$. Observe that for such a category, the typical intuition of elements of $\hom(X, Y)$ as "morphisms from X to Y" is meaningless!

3.2 Functors and natural transformations

Informally, functors are morphisms between categories. We distinguish between "arrow preserving" (covariant) and "arrow reversing" (contravariant) functors.

Definition 3.2.1. Let $\mathcal{C}, \mathcal{D}$ be two categories.

(i) A *(covariant) functor* F from $\mathcal{C}$ to $\mathcal{D}$ is a map[2] associating with each object $X \in \mathrm{ob}(\mathcal{C})$ an object $F(X) \in \mathrm{ob}(\mathcal{D})$, and with each morphism $\alpha \in \hom_{\mathcal{C}}(X, Y)$ a morphism $F(\alpha) \in \hom_{\mathcal{D}}(F(X), F(Y))$, such that:

- $F(\alpha\beta) = F(\alpha)F(\beta)$ (whenever this makes sense);
- $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ for all $X \in \mathrm{ob}(\mathcal{C})$.

[2]Formally, a functor F is a *pair* of maps $(F_{\mathrm{ob}}, F_{\mathrm{hom}})$, where $F_{\mathrm{ob}} \colon \mathrm{ob}(\mathcal{C}) \to \mathrm{ob}(\mathcal{D})$ and $F_{\mathrm{hom}} \colon \hom(\mathcal{C}) \to \hom(\mathcal{D})$.

(ii) A *contravariant functor* F from $\mathcal{C}$ to $\mathcal{D}$ is a map associating with each object $X \in \mathrm{ob}(\mathcal{C})$ an object $F(X) \in \mathrm{ob}(\mathcal{D})$, and with each morphism $\alpha \in \hom_{\mathcal{C}}(X, Y)$ a morphism $F(\alpha) \in \hom_{\mathcal{D}}(F(Y), F(X))$, such that:

- $F(\alpha\beta) = F(\beta)F(\alpha)$ (whenever this makes sense);
- $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ for all $X \in \mathrm{ob}(\mathcal{C})$.

Examples 3.2.2. (1) Let $F\colon \mathbf{Ring} \to \mathbf{AbGrp}$ be given by mapping each ring $(R, +, \cdot)$ to the corresponding additive group $(R, +)$, and each ring morphism to the corresponding group morphism. Such a functor is called a *forgetful functor* since it "forgets" some of the underlying information (in this case the multiplication).

(2) Let $F\colon \mathbf{Grp} \to \mathbf{Grp}$ be given by mapping each group G to its derived subgroup $[G, G]$, and each morphism to its restriction to the derived subgroup. Then F is a covariant functor.

(3) There is no functor $F\colon \mathbf{Grp} \to \mathbf{Grp}$ with the property that each group G is mapped to its center $Z(G)$. (This is an interesting exercise; this is not completely obvious at first sight.)

(4) Let k be a field. There is a contravariant functor $F\colon \mathbf{Vec}_k \to \mathbf{Vec}_k$ which assigns to each vector space its dual, and to each linear transformation its dual (or transpose) transformation.

(5) Let G be a group, and let $\mathcal{C}$ be the corresponding category with a single object $*$, as defined in Example 3.1.3(2). Then a covariant functor $F\colon \mathcal{C} \to \mathbf{Set}$ assigns a set $F(*)$ to the object $*$, and assigns to each morphism in $\mathcal{C}$ (i.e., to each element $g \in G$) a map $F(g)$ from $F(*)$ to itself. Since g is an invertible morphism in $\mathcal{C}$, also $F(g)$ is an invertible morphism in $\mathbf{Set}$, in other words, $F(g)$ is a permutation of $F(*)$. Since $F(gh) = F(g)F(h)$ for all $g, h \in G$, we see that F describes a permutation representation of G.
Conversely, every permutation representation of G gives rise to a functor from $\mathcal{C}$ to $\mathbf{Set}$.

Remark 3.2.3. Very often, we will write down functors by indicating what they do on objects and assume that it is clear what they do on morphisms. To emphasize this, it is customary to use the notation $\rightsquigarrow$. For instance, the functor from Example 3.2.2(2) will be denoted by

$$F\colon \mathbf{Grp} \to \mathbf{Grp}\colon G \rightsquigarrow [G, G].$$

We now go one step further in the abstractness, and we will introduce natural transformations, which are some kind of morphisms between functors.

Definition 3.2.4. (i) Let $\mathcal{C}, \mathcal{D}$ be two categories, and F, G two covariant functors from $\mathcal{C}$ to $\mathcal{D}$. A *natural transformation* T from F to G is a family of $\mathcal{D}$-morphisms

$$T_X \colon F(X) \to G(X)$$

such that for each $X \xrightarrow{\alpha} Y$, the diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{F(\alpha)} & F(Y) \\ {\scriptstyle T_X}\downarrow & & \downarrow{\scriptstyle T_Y} \\ G(X) & \xrightarrow{G(\alpha)} & G(Y) \end{array}$$

commutes. (The definition for natural transformations between contravariant functors is similar.)

(ii) A natural transformation which has an inverse (in the obvious sense), is called a *natural isomorphism*. If $T \colon F \to G$ is a natural isomorphism between the functors F and G, then F and G are called *isomorphic*.

(iii) Two categories $\mathcal{C}, \mathcal{D}$ are *isomorphic* if there exist functors $F \colon \mathcal{C} \to \mathcal{D}$ and $G \colon \mathcal{D} \to \mathcal{C}$ such that $FG = 1_{\mathcal{C}}$ and $GF = 1_{\mathcal{D}}$. Although this definition looks natural, this notion is (too) restrictive.

(iv) Two categories $\mathcal{C}, \mathcal{D}$ are *equivalent* if there exist functors $F \colon \mathcal{C} \to \mathcal{D}$ and $G \colon \mathcal{D} \to \mathcal{C}$ such that FG and $1_{\mathcal{C}}$ are isomorphic and GF and $1_{\mathcal{D}}$ are isomorphic.

(v) Two categories $\mathcal{C}, \mathcal{D}$ are *anti-equivalent* or *dual* if there exist contravariant functors $F \colon \mathcal{C} \to \mathcal{D}$ and $G \colon \mathcal{D} \to \mathcal{C}$ such that FG and $1_{\mathcal{C}}$ are isomorphic and GF and $1_{\mathcal{D}}$ are isomorphic.

Example 3.2.5. The categories **AbGrp** and $\mathbf{Mod}_{\mathbb{Z}}$ are isomorphic. On the other hand, consider the categories $\mathbf{FVec}_k$ of finite-dimensional vector spaces over k, with linear transformations as morphisms, and the category $\mathbf{FCol}_k$ of the column spaces k^n for all finite n, with linear transformations as morphisms. Then $\mathbf{FVec}_k$ and $\mathbf{FCol}_k$ are certainly not isomorphic (indeed, $\mathbf{FCol}_k$ is a small category but $\mathbf{FVec}_k$ is not), but they are equivalent. (Work out the details as an exercise. This becomes easier if you use Lemma 3.2.8 below.)

Definition 3.2.6. Let $F \colon \mathcal{C} \to \mathcal{D}$ be a functor. Then for each pair of objects $X, Y \in \mathrm{ob}(\mathcal{C})$, the functor F induces a map

$$F_{X \to Y} \colon \hom_{\mathcal{C}}(X, Y) \to \hom_{\mathcal{D}}(F(X), F(Y)).$$

(i) The functor F is *faithful* if $F_{X\to Y}$ is injective for all $X, Y \in \mathrm{ob}(\mathcal{C})$.

(ii) The functor F is *full* if $F_{X\to Y}$ is surjective for all $X, Y \in \mathrm{ob}(\mathcal{C})$.

(iii) The functor F is *fully faithful* if $F_{X\to Y}$ is bijective for all $X, Y \in \mathrm{ob}(\mathcal{C})$.

(iv) The functor F is *dense* (also called *essentially surjective*) if each $Y \in \mathrm{ob}(\mathcal{D})$ is isomorphic to an object $F(X)$ for some $X \in \mathrm{ob}(\mathcal{C})$.

(v) The functor F is an *equivalence* if and only if F is fully faithful and dense.

Definition 3.2.7. The notions "faithful", "full", "fully faithful" and "dense" can be defined similarly for a *contravariant* functor $F\colon \mathcal{C} \to \mathcal{D}$. The functor F is then called a *duality* or an *anti-equivalence* if F is fully faithful and dense.

Lemma 3.2.8. (i) *Two categories $\mathcal{C}$ and $\mathcal{D}$ are equivalent (in the sense of Definition* 3.2.4(iv)*) if and only if there exists an equivalence from $\mathcal{C}$ to $\mathcal{D}$.*

(ii) *Two categories $\mathcal{C}$ and $\mathcal{D}$ are dual (in the sense of Definition* 3.2.4(v)*) if and only if there exists a duality from $\mathcal{C}$ to $\mathcal{D}$.*

Proof. This is left to the reader as a rather lengthy exercise. Some care is needed, though: to explicitly construct the "inverse" functor of an equivalence, the axiom of choice is needed. We invite the interested reader to look up the fine details (such as a possible extension to *anafunctors* to avoid the axiom of choice). □

Lemma 3.2.9. *Let $\mathcal{C}, \mathcal{D}$ be two categories, and let F be a fully faithful functor from $\mathcal{C}$ to $\mathcal{D}$. Then F is injective on the isomorphism classes of objects, i.e.*

$$F(X) \cong F(Y) \iff X \cong Y$$

for all $X, Y \in \mathrm{ob}(\mathcal{C})$.

Proof. Assume that $F(X) \cong F(Y)$; then there exist morphisms

$$F(X) \xrightarrow{\gamma} F(Y) \quad \text{and} \quad F(Y) \xrightarrow{\delta} F(X)$$

such that $\gamma\delta = \mathrm{id}_{F(X)}$ and $\delta\gamma = \mathrm{id}_{F(Y)}$. Since F is full, $\gamma = F(\alpha)$ and $\delta = F(\beta)$ for certain morphisms

$$X \xrightarrow{\alpha} Y \quad \text{and} \quad Y \xrightarrow{\beta} X.$$

It follows that $\alpha\beta$ and id_X are two morphisms from X to X which are mapped by F to the morphism $\mathrm{id}_{F(X)}$; since F is faithful, it follows that $\alpha\beta = \mathrm{id}_X$. Similarly $\beta\alpha = \mathrm{id}_Y$, and we conclude that $X \cong Y$. □

3.3 The Yoneda Lemma

The Yoneda Lemma is a quite general abstract result in category theory that almost looks too abstract to be useful, but as we will see, it has very powerful consequences. The idea is that instead of studying the category $\mathcal{C}$ directly, we study the functors from $\mathcal{C}$ to **Set**, and **Set** is of course a category that we understand very well. We can think of such a functor as a "representation" of $\mathcal{C}$, very much like the Cayley representation tells us how we can understand a group[3] by considering it as a collection of permutations, i.e. a collection of isomorphisms in the category **Set**.

This general idea of a representation is caught by the notion of *representable functors*, which we now define.

Definition 3.3.1. Let $\mathcal{C}$ be a locally small[4] category.

(i) Every object $A \in \mathrm{ob}(\mathcal{C})$ defines a functor

$$h^A \colon \mathcal{C} \to \mathbf{Set}$$

given on objects by

$$X \mapsto \hom_{\mathcal{C}}(A, X)$$

and on morphisms by

$$\left(X \xrightarrow{f} Y\right) \mapsto \begin{pmatrix} \hom_{\mathcal{C}}(A, X) \to \hom_{\mathcal{C}}(A, Y) \\ g \mapsto g \cdot f \end{pmatrix}.$$

(ii) A functor $F \colon \mathcal{C} \to \mathbf{Set}$ is called *representable* if there is an object $A \in \mathrm{ob}(\mathcal{C})$ such that F is isomorphic to h^A; we say that F is *represented by* the object A. As we will see in Corollary 3.3.4(ii) below, a representable functor is represented by a unique object (up to isomorphism).

(iii) Every morphism $B \xrightarrow{\alpha} A$ defines a natural transformation

$$T^\alpha \colon h^A \to h^B$$

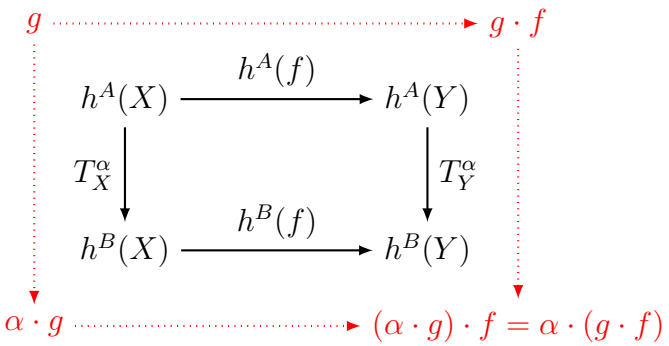
via

$$T^\alpha_X \colon h^A(X) = \hom_{\mathcal{C}}(A, X) \to h^B(X) = \hom_{\mathcal{C}}(B, X) \colon g \mapsto \alpha \cdot g.$$

[3]Remember that every group can be made into a category with a single object, and in this sense the Yoneda Lemma is really a generalization of Cayley's Theorem. See Example 3.2.2(5).

[4]Recall that $\mathcal{C}$ is locally small if the classes $\hom_{\mathcal{C}}(A, B)$ are sets for all objects A, B. This condition is necessary to ensure that the functors h^A end up in **Set**.

This is indeed a natural transformation:



Conversely, if $T\colon h^A \to h^B$ is a natural transformation, then

$$\alpha := T_A(\mathrm{id}_A) \in h^B(A)$$

defines a morphism $B \xrightarrow{\alpha} A$.

(iv) More generally, let $F\colon \mathcal{C} \to \mathbf{Set}$ be a functor, and $A \in \mathrm{ob}(\mathcal{C})$. Every natural transformation $T\colon h^A \to F$ defines an element

$$a_T := T_A(\mathrm{id}_A) \in F(A).$$

Conversely, for each $a \in F(A)$ we define a natural transformation $T^a\colon h^A \to F$ given by

$$T^a_X\colon h^A(X) \to F(X)\colon g \mapsto F(g)(a). \tag{3.1}$$

Observe that $g \in \hom_{\mathcal{C}}(A, X)$ and hence $F(g) \in \hom_{\mathbf{Set}}(F(A), F(X))$, so the element $F(g)(a)$ does indeed belong to $F(X)$. Check for yourself that T^a is a natural transformation.

We are now ready to state the Yoneda Lemma.

Theorem 3.3.2 (The Yoneda Lemma)**.** *Let $\mathcal{C}$ be a locally small category, $F\colon \mathcal{C} \to \mathbf{Set}$ be a functor, and $A \in \mathrm{ob}(\mathcal{C})$. The map*

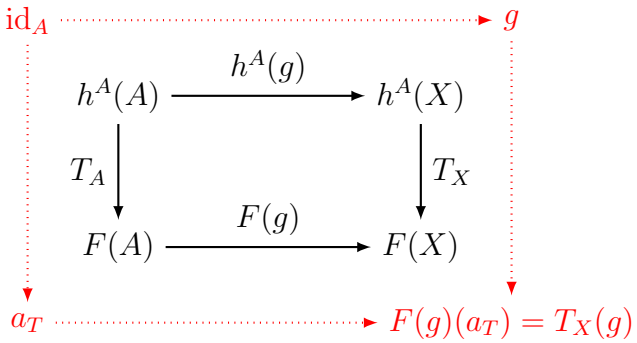
$$\xi\colon \mathrm{Nat}(h^A, F) \to F(A)\colon T \mapsto a_T$$

is a bijection; its inverse is given by the map

$$\psi\colon F(A) \to \mathrm{Nat}(h^A, F)\colon a \mapsto T^a.$$

This bijection is natural both in A and in F.

Proof. We first show that $\xi \cdot \psi$ is the identity. So let $T \in \mathrm{Nat}(h^A, F)$ be arbitrary; then for each $g \in h^A(X) = \hom_{\mathcal{C}}(A, X)$, we have a commutative diagram



(3.2)

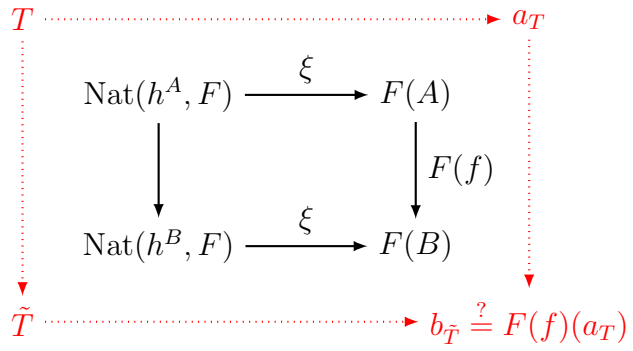
showing that each T_X coincides with $T_X^{a_T}$, and hence the natural transformations T and T^{a_T} are equal.

Next, we show that $\psi \cdot \xi$ is the identity. So let $a \in F(A)$ be arbitrary; then

$$a_{T^a} = T_A^a(\mathrm{id}_A) = F(\mathrm{id}_A)(a) = \mathrm{id}_{F(A)}(a) = a,$$

proving that $\psi \cdot \xi = \mathrm{id}_{F(A)}$ as claimed.

We now show that ξ is natural in A, i.e. if $A \xrightarrow{f} B$, then the following diagram has to commute.



where the natural transformation $\tilde{T}$ is obtained from T by composition with f, i.e. for each object X we have

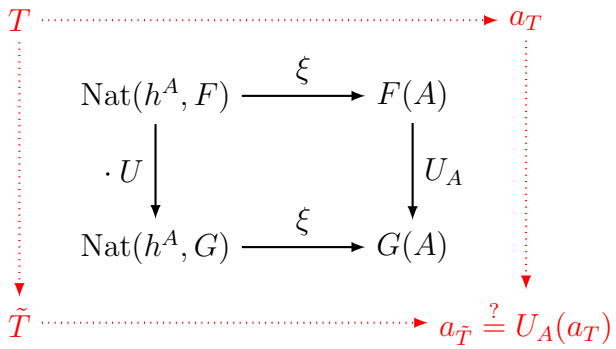
$$\tilde{T}_X \colon h^B(X) \to F(X) \colon g \mapsto T_X(fg).$$

Observe that $F(f)(a_T) = T_B(f)$ by the previous commutative diagram (3.2). On the other hand,

$$b_{\tilde{T}} = \tilde{T}_B(\mathrm{id}_B) = T_B(f \cdot \mathrm{id}_B) = T_B(f),$$

proving that the diagram does indeed commute.

We finally show naturality in F, i.e. if F and G are two functors from $\mathcal{C}$ to **Set**, and $U \in \mathrm{Nat}(F, G)$ is a natural transformation from F to G, then the following diagram has to commute:



where the natural transformation $\tilde{T}$ is obtained from T by composition with U, i.e. for each object X we have

$$\tilde{T}_X \colon h^A(X) \to G(X) \colon g \mapsto U_X(T_X(g)).$$

It follows that

$$a_{\tilde{T}} = \tilde{T}_A(\mathrm{id}_A) = U_A(T_A(\mathrm{id}_A)) = U_A(a_T),$$

proving that the diagram does indeed commute, and finishing the proof of the theorem. □

An important special case of the Yoneda Lemma is given by the following corollary, which establishes some kind of duality between morphisms and natural transformations.

Definition 3.3.3. Let $\mathcal{C}$ be a locally small category. The *functor category* $\mathcal{C}^\vee$ (also denoted by $\mathbf{Set}^{\mathcal{C}}$) is the category with as objects the functors from $\mathcal{C}$ to **Set**, and as morphisms the natural transformations between these functors. Its full subcategory of representable functors is sometimes denoted by $\mathcal{C}^\vee_{\mathrm{rep}}$.

Corollary 3.3.4. *Let $\mathcal{C}$ be a locally small category.*

(i) *For each pair of objects $A, B \in \mathrm{ob}(\mathcal{C})$, there is a natural bijection*

$$\mathrm{Nat}(h^A, h^B) \simeq \hom_{\mathcal{C}}(B, A).$$

In particular, there is a contravariant fully faithful functor

$$\mathcal{C} \to \mathcal{C}^\vee \colon A \rightsquigarrow h^A,$$

and hence $\mathcal{C}$ and $\mathcal{C}^\vee_{\mathrm{rep}}$ are dual categories.

(ii) *The functors h^A and h^B are isomorphic if and only if A and B are isomorphic objects.*

Proof. The first statement is nothing else than the Yoneda Lemma with $F = h^B$. The second statement now follows from Lemma 3.2.9. □

Remark 3.3.5. A particularly colorful way to express what Yoneda's Lemma does, is given by the following quote (due to Ravi Vakil) that I saw on MathOverflow:

> *You work at a particle accelerator. You want to understand some particle. All you can do are throw other particles at it and see what happens. If you understand how your mystery particle responds to all possible test particles at all possible test energies, then you know everything there is to know about your mystery particle.*

Chapter 4 Algebraic geometry

It is of course impossible to give a decent introduction to algebraic geometry in a single chapter of this course, but luckily the amount of algebraic geometry that we will require is rather limited. In particular, we will mainly be dealing with affine varieties and affine schemes, and we will have little need for developing the general theory of varieties or schemes formed by gluing together affine parts through the machinery of sheaves.

On the other hand, we will need to develop the basic intuition behind algebraic geometry, which consists precisely of relating algebraic objects (commutative k-algebras) and geometric objects (affine varieties, or more generally, affine schemes). This fundamental relationship will be continued and enriched when we will be dealing with affine algebraic groups in the next chapter.

4.1 Affine varieties

During this section, we will assume that k is a commutative field, and all rings will be assumed to be commutative rings with 1. We will be dealing with the category

$$k\text{-}\mathbf{alg} := \text{category of commutative, associative } k\text{-algebras with 1.}$$

Let A_n be the k-algebra

$$A_n := k[t_1, \ldots, t_n]$$

of polynomials over k in n variables; we can think of A_n geometrically as the algebra of k-valued polynomial functions on the affine space k^n.

Definition 4.1.1. (i) An *affine variety*[1] is a subset of k^n defined as the common zeroes of a collection of polynomials in A_n. More precisely, let $S \subseteq A_n$ be any collection of polynomials; then we define the affine variety $V(S)$ as

$$V(S) := \{x \in k^n \mid f(x) = 0 \text{ for all } f \in S\}.$$

[1] Some authors require affine varieties to be *irreducible*, and refer to our affine varieties as *(affine) algebraic sets* instead.

(ii) Conversely, if $X \subseteq k^n$ is an arbitrary subset of the affine space k^n, then we set

$$I(X) \coloneqq \{f \in A_n \mid f(x) = 0 \text{ for all } x \in X\};$$

then $I(X)$ is an ideal in A_n, which we refer to as the ideal of polynomials *vanishing on* X.

Every affine variety is defined by a finite number of polynomials:

Theorem 4.1.2 (Hilbert's Basis Theorem)**.** *Every ideal $I \trianglelefteq A_n$ is finitely generated.*

Proof omitted. □

Lemma 4.1.3. *Let I, J be two ideals in A_n, and let C be any collection of ideals in A_n. Then:*

(i) *if $I \subseteq J$, then $V(I) \supseteq V(J)$;*

(ii) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$;

(iii) $\bigcap_{I \in C} V(I) = V(\langle I \mid I \in C \rangle)$;

(iv) $V((0)) = k^n$ *and* $V((1)) = \emptyset$.

Proof. The only not completely trivial part is (ii). First, observe that I and J both contain $I \cap J$, which in turn contains IJ; so (i) implies that

$$V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ).$$

Now let $x \in V(IJ)$ be arbitrary, and assume that $x \notin V(I)$. Then there is some $f \in I$ with $f(x) \neq 0$. On the other hand, for each $g \in J$ we have $fg \in IJ$, and hence $f(x)g(x) = 0$. It follows that $g(x) = 0$ for each $g \in J$, hence $x \in V(J)$. □

An immediate consequence of the previous lemma is that the affine varieties make the affine k^n into a topological space.

Definition 4.1.4. The sets of the form $V(I) \subseteq k^n$ are the closed sets of a topology on k^n, which we call the *Zariski topology*. (Indeed, Lemma 4.1.3 tells us that the union of a finite number of closed sets is again closed, that the intersection of an arbitrary collection of closed sets is again closed, and that the empty space and the whole space are closed.) Moreover, every affine variety $V(I)$ inherits this topology of k^n, which we also refer to as the Zariski topology on $V(I)$.

Lemma 4.1.5. *The open sets of the form*

$$D(f) \coloneqq \{x \in k^n \mid f(x) \neq 0\}$$

for $f \in A_n$ form a basis for the Zariski topology on k^n; these sets $D(f)$ are called the principal open sets *(or simply the* principal opens*).*

Proof. This follows from the definitions, since every closed set can be written as the intersection of closed sets of the form $V(f)$, and hence every open set can be written as the union of open sets of the form $D(f)$. (In fact, by Hilbert's Basis Theorem 4.1.2, every open set is the *finite* union of principal opens.) □

Notice that for every set of polynomials $S \subseteq A_n$, we have the inclusion $S \subseteq I(V(S))$, and conversely, for every subset $X \subseteq k^n$ of the affine space, the inclusion $X \subseteq V(I(X))$ holds. It is natural to ask when equality holds. Of course, we have $X = V(I(X))$ precisely when X is an affine variety, i.e. when X is closed in the Zariski topology; in fact, for general $X \subseteq k^n$, the set $V(I(X))$ is precisely the closure $\overline{X}$ of X in the Zariski topology.

The question when $S = I(V(S))$ is more interesting. Assume that I is an ideal of the form $I(V)$ for some subset $V \subseteq k^n$. Observe that I has the property that whenever $f^m \in I$ for some $f \in A_n$ and some $m \geq 1$, then $f \in I$. Such an ideal is called a radical ideal.

Definition 4.1.6. Let $I \trianglelefteq R$ be an ideal in some ring[2] R. Define the *radical* of I as the ideal

$$\operatorname{rad} I \coloneqq \sqrt{I} \coloneqq \{r \in R \mid r^m \in I \text{ for some } m \geq 1\}.$$

The ideal I is called a *radical ideal* when $I = \operatorname{rad} I$.

Radical ideals in noetherian rings behave nicely:

Theorem 4.1.7 (Lasker–Noether Theorem)**.** *Every radical ideal I in a noetherian ring is the intersection of a finite number of prime ideals. Moreover, there is a unique irredundant*[3] *intersection into prime ideals up to reordering.*

Proof omitted. □

[2]Remember that our rings are commutative rings with 1.

[3]An intersection of sets $A_1 \cap \cdots \cap A_n$ is called *irredundant* if removing any of the A_i's changes the intersection.

Remark 4.1.8. The Lasker–Noether Theorem states more generally that *every* ideal in a noetherian ring R is a finite intersection of *primary ideals*, i.e. of ideals I such that in the ring R/I, each zero divisor is nilpotent. We will not need this more general statement.

For algebraically closed fields, the observation that the ideals of the form $I(V)$ are radical is the only required restriction.

Theorem 4.1.9 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field, and let $I \trianglelefteq A_n$ be an ideal. Then $I(V(I)) = I$ if and only if I is a radical ideal.*

Proof. We will omit the proof. There exist various rather different proofs; notice that by the Lasker–Noether Theorem, it suffices to consider the case when I is a prime ideal. □

Remark 4.1.10. The assumption for k to be algebraically closed, is essential. For instance, consider the principal ideal $I = (x^2 + y^2 + 1)$ in $\mathbb{R}[x, y]$. Then $V(I) = \emptyset$, and hence $I(V(I)) = \mathbb{R}[x, y] \neq I$.

Corollary 4.1.11. *Let k be an algebraically closed field. The rule*

$$I \mapsto V(I)$$

is an inclusion-reversing bijection between radical ideals in A_n and affine varieties in k^n. Maximal ideals correspond to points, and are thus of the form

$$M = (t_1 - a_1, \ldots, t_n - a_n).$$

Every affine variety can be decomposed into *irreducible* affine varieties. In order to make this notion precise, we have to introduce some topological terminology.

Definition 4.1.12. Let X be a topological space.

(i) We call X *connected* if there are no non-empty open subspaces $U_1, U_2 \subseteq X$ such that $X = U_1 \cup U_2$ and $U_1 \cap U_2 = \emptyset$.

(ii) We call X *irreducible* if there are no non-empty open subspaces $U_1, U_2 \subseteq X$ such that $U_1 \cap U_2 = \emptyset$, i.e., every two non-empty open subspaces of X intersect non-trivially.

(iii) Let $U \subseteq X$. Then we call U connected, resp. irreducible, if it is connected, resp. irreducible in the subspace topology induced by X.

(iv) An *irreducible component* of X is a maximal irreducible subset. Notice that irreducible components are always closed.

Clearly every irreducible space is also connected, but the converse is not true.

Example 4.1.13. Consider the real line $X = \mathbb{R}$ with the ordinary real topology. Then X is connected, but is certainly not irreducible; there are plenty of open subspaces intersecting trivially.

On the other hand, consider the real line $Y = \mathbb{R}$ equipped with the Zariski topology. Then Y is irreducible. Indeed, every closed subspace of Y is a finite set, and hence any two open subspaces are cofinite and hence intersect non-trivially.

Lemma 4.1.14. *Let X be a topological space. The following conditions are equivalent:*

(a) *X is irreducible.*

(b) *X cannot be written as the union of two closed proper subsets.*

(c) *Every non-empty open subset of X is dense.*

Proof. Exercise. □

Observe that when U is itself a closed subspace of X, then U is irreducible if and only if U cannot be written as the union of two closed subspaces of X different from U.

When k is algebraically closed, the irreducible affine varieties correspond to prime ideals.

Lemma 4.1.15. *Assume that k is an algebraically closed field. Let I be a radical ideal in A_n. Then $V(I)$ is irreducible if and only if I is a prime ideal.*

Proof. This follows from the Lasker–Noether Theorem 4.1.7, but we will give a direct proof instead. Assume first that $V(I)$ is irreducible, and let $f, g \in A_n$ such that $fg \in I$. Then $V = V(I) \subseteq V(fg) = V(f) \cup V(g)$, i.e.

$$V = \big(V \cap V(f)\big) \cup \big(V \cap V(g)\big).$$

Since V is irreducible, we have either $V \subseteq V(f)$ or $V \subseteq V(g)$ (or both), and hence, by Corollary 4.1.11, $f \in I$ or $g \in I$.

Conversely, assume that I is prime, and that $V = V(I_1) \cup V(I_2)$ for certain radical ideals I_1 and I_2. By Corollary 4.1.11 again, this implies that $I \subseteq I_1$ and $I \subseteq I_2$. Assume that $V \neq V(I_1)$. Then $I \neq I_1$, so we can pick some $f \in I_1 \setminus I$. For all $g \in I_2$, we now have $fg \in I$ since fg vanishes on $V(I_1) \cup V(I_2)$; because I is prime, we must have $g \in I$. This shows that $I_2 \subseteq I$, and hence $V = V(I_2)$, proving that V is irreducible. □

Corollary 4.1.16. *Every affine variety V is a* finite *union of irreducible affine varieties; these irreducible affine varieties are uniquely determined, and are precisely the irreducible components of V.*

Proof. This follows from the Lasker–Noether Theorem 4.1.7. □

4.2 The coordinate ring of an affine variety

In this section, we will always assume that k is an algebraically closed field. By Hilbert's Nullstellensatz (or its Corollary 4.1.11), there is a bijective correspondence between affine varieties (geometric objects) and radical ideals (algebraic objects).

We will take this correspondence even further. To each affine k-variety, we will associate an algebraic object, namely its coordinate ring (which will be a k-algebra). As we will soon see, this algebra carries all information of the geometric object, and in fact, we will often jump back and forth between the geometric objects and the algebraic objects. We will make this correspondence very strong and formal: these objects will form dual categories.

Definition 4.2.1. Let V be an affine variety in k^n, and let $I = I(V) \trianglelefteq A_n$ the corresponding ideal of polynomials vanishing on V. Then the restrictions of the elements of A_n to the set V form a ring A, called the *ring of regular functions* on V or the *coordinate ring* or *coordinate algebra* of V; it is denoted by $A = k[V]$ or by $A = \mathcal{O}[V]$. Explicitly,

$$k[V] = \mathcal{O}[V] = A_n/I(V),$$

since two elements of A_n restricted to V coincide if and only if their difference is zero on V, i.e. belongs to $I(V)$.

Proposition 4.2.2. *Let V be an affine variety in k^n, and $I = I(V) \trianglelefteq A_n$.*

(i) *The k-algebra $A = k[V]$ is finitely generated and reduced, i.e. does not contain non-zero nilpotent elements.*

(ii) *There is a bijection*

$$V \to \hom_{k\text{-}\mathbf{alg}}(A, k) \colon x \mapsto e_x,$$

where for each $x \in V$, the evaluation morphism e_x *is defined by*

$$e_x \colon A \to k \colon f \mapsto f(x).$$

Proof. (i) The k-algebra A is a quotient of A_n, which is finitely generated; hence A is finitely generated as well. Assume that $f \in A$ is a nilpotent element, i.e. $f^N = 0$ for some positive integer N. Let $\tilde{f}$ be an element of A_n representing $f \in A_n/I$; then $\tilde{f}^N \in I$. Since I is a radical ideal, it follows that $\tilde{f} \in I$, and hence $f = 0$.

(ii) Observe that for each $x \in V$, the evaluation morphism e_x is indeed a k-algebra morphism from A to k. We will show that the map $x \mapsto e_x$ is a bijection.
To show injectivity, let $t_i \in A_n$ be the i-th coordinate map (for each i), and let s_i be the image of t_i in $A = A_n/I$. We will show that the element x is uniquely determined by the morphism e_x. Indeed, let $x = (x_1, \ldots, x_n) \in V$; then

$$e_x(s_i) = s_i(x) = t_i(x) = x_i,$$

and hence

$$x = \big(e_x(s_1), \ldots, e_x(s_n)\big).$$

To show surjectivity, let $\alpha \in \hom_{k\text{-}\mathbf{alg}}(A, k)$ be arbitrary, and define

$$x \coloneqq \big(\alpha(s_1), \ldots, \alpha(s_n)\big) \in k^n.$$

Let $\tilde{\alpha} \in \hom_{k\text{-}\mathbf{alg}}(A_n, k)$ be given by the composition

$$A_n \xrightarrow{\text{proj}} A_n/I = A \xrightarrow{\alpha} k;$$

then $\alpha(s_i) = \tilde{\alpha}(t_i)$ for all i. For each $f \in I$, we have $\tilde{\alpha}(f) = 0$, and hence

$$f(x) = f\big(\tilde{\alpha}(t_1), \ldots, \tilde{\alpha}(t_n)\big) = \tilde{\alpha}(f) = 0$$

because $\tilde{\alpha}$ is a k-algebra morphism. We conclude that $x \in V(I) = V$, and $e_x = \alpha$. □

Conversely, every finitely generated reduced k-algebra arises from an affine variety:

Proposition 4.2.3. *Let A be a finitely generated reduced k-algebra. Then there is an affine variety X with coordinate ring A.*

Proof. Let Y be the set $Y \coloneqq \hom_{k\text{-}\mathbf{alg}}(A, k)$; we will endow Y with the structure of an affine variety. Assume that the k-algebra A is generated by some finite set $\{s_1, \ldots, s_n\}$, and define

$$\varphi \colon Y \to k^n \colon \alpha \mapsto \big(\alpha(s_1), \ldots, \alpha(s_n)\big).$$

Observe that φ is injective because $s_1, \ldots, s_n$ generate A. On the other hand, let $A_n = k[t_1, \ldots, t_n]$ and let φ^* be the k-algebra morphism defined by

$$\varphi^* \colon A_n \to A \colon t_i \mapsto s_i$$

for each i. Then φ^* is surjective because A is generated by $s_1, \ldots, s_n$. If we denote its kernel by I, then $A \cong A_n/I$; note that I is a radical ideal because A is reduced.

Let $X = \operatorname{im} \varphi \subseteq k^n$; it remains to show that $X = V(I)$. Notice that this will then also imply that $I(X) = I(V(I)) = I$ since I is radical, and hence $k[X] = A_n/I(X) = A_n/I \cong A$.

For each $x \in k^n$, there is a corresponding evaluation morphism $e_x \in \hom_{k\text{-}\mathbf{alg}}(A_n, k)$. Then $x \in X = \operatorname{im} \varphi$ if and only if there is some $\alpha \in Y$ such that $e_x = \alpha \circ \varphi^*$. This happens precisely when e_x vanishes on the kernel of φ^*, i.e., when $e_x(I) = 0$, or equivalently, when $x \in V(I)$. □

The previous discussion reveals a beautiful duality between finitely generated reduced k-algebras on the one hand, and affine varieties on the other hand. Notice that we have not yet defined the notion of a morphism between affine varieties. It is possible to do this directly in terms of the explicit coordinatization of the affine varieties, but it is nicer to use duality to get an intrinsic definition. In fact, it is also convenient to have a coordinate-free definition of affine varieties at hand.

Definition 4.2.4. (i) An *(abstract) affine k-variety* is a pair (X, A), where X is a set, and A is a ring of k-valued functions on X, such that A is a finitely generated k-algebra, and such that the map

$$X \to \hom_{k\text{-}\mathbf{alg}}(A, k) \colon x \mapsto e_x$$

(where e_x is the evaluation morphism at x, as defined previously) is a bijection. We often denote an abstract affine k-variety (X, A) simply by X, and we refer to A as its ring of regular functions, or its coordinate algebra, and denote it as $A = k[X]$ or $A = \mathcal{O}[X]$ as before. Note that Propositions 4.2.2 and 4.2.3 show precisely that every affine k-variety is also an abstract affine k-variety, and conversely. The advantage of abstract affine k-varieties is that the definition does not refer to an embedding in some k^n. Observe that the algebra A is automatically reduced since it is an algebra of k-valued functions.

(ii) In particular, if A is a finitely generated reduced k-algebra, we can consider the set $X = \hom_{k\text{-}\mathbf{alg}}(A, k)$ —or more precisely, the pair (X, A)— as *the* abstract affine variety corresponding to A. Explicitly, if $f \in A$,

then f is a k-valued function on X, defined by the funny looking equality

$$f(x) \coloneqq x(f) \quad \text{for all } x \in X.$$

We could think of this as a "pairing" between X and A without favoring one of the two objects as acting on the other.

(iii) Let X and Y be two (abstract) affine k-varieties. A *morphism* from X to Y is a (set-theoretic) map f from X to Y such that the corresponding dual map

$$f^*\colon \hom_{\mathbf{Set}}(Y,k) \to \hom_{\mathbf{Set}}(X,k)\colon \alpha \mapsto \alpha \circ f$$

induces a morphism from $k[Y]$ to $k[X]$, which we also denote by f^*.

Proposition 4.2.5. *The abstract affine k-varieties, with morphisms as defined above, form a category, which is dual to the category of finitely generated reduced k-algebras.*

Proof. Let $\mathcal{C}$ be the category of abstract affine varieties over k and $\mathcal{D}$ be the category of finitely generated reduced k-algebras. In order to show that $\mathcal{C}$ and $\mathcal{D}$ are dual to each other, we will use Lemma 3.2.8. So let F be the contravariant functor from $\mathcal{C}$ to $\mathcal{D}$, mapping each affine variety X to its coordinate algebra $k[X]$, and each morphism $f\colon X \to Y$ to the corresponding morphism $f^*\colon k[Y] \to k[X]$. We claim that F is a duality, i.e., that it is fully faithful and dense.

To show that it is fully faithful, let X and Y be two abstract affine varieties and consider

$$F_{X\to Y}\colon \hom_{\mathcal{C}}(X,Y) \to \hom_{\mathcal{D}}(k[Y],k[X])\colon f \mapsto f^*.$$

We have to show that for each algebra morphism $g\colon k[Y] \to k[X]$, there is a unique map $f\colon X \to Y$ such that $g = f^*$. Since $X \simeq \hom_{k\text{-}\mathbf{alg}}(k[X],k)$ and $Y \simeq \hom_{k\text{-}\mathbf{alg}}(k[Y],k)$ (by definition of abstract affine varieties), it is now easy to check that the unique f we are looking for is precisely the map

$$f\colon \hom_{k\text{-}\mathbf{alg}}(k[X],k) \to \hom_{k\text{-}\mathbf{alg}}(k[Y],k)\colon \varphi \mapsto \varphi \circ g.$$

Finally, the fact that F is dense is just a reformulation of the fact that each finitely generated reduced k-algebra arises as the coordinate algebra of some abstract affine variety; see Definition 4.2.4(ii). □

To finish this section, we introduce the important notion of dimension of a variety, and we mention some facts without proofs.

Definition 4.2.6. Let k be an algebraically closed field and let V be an affine k-variety.

(i) When V is irreducible, its coordinate algebra $k[V]$ is a domain, so we can consider its fraction field $k(V) := \mathrm{Frac}(k[V])$. The *dimension* of V, $\dim(V)$, is defined to be the transcendence degree of $k(V)$ over k (i.e., the largest possible size of an algebraically independent subset of $k(V)$ over k).

(ii) In general, write V as a finite union $V = \bigcup V_i$ of its irreducible components. Then we define $\dim(V) = \max \dim(V_i)$.

Theorem 4.2.7. *Let V be an irreducible subvariety of $\mathbb{A}^n$ and let $f \in A_n = k[t_1, \ldots, t_n]$. Let $W = V \cap V(f)$. Then either $W = V$, or $W = \emptyset$, or W is a* hypersurface *of V, which means that every irreducible component of W has dimension $\dim V - 1$.*

Theorem 4.2.8 (Topological characterization of dimension)**.** *Suppose V is irreducible and that*

$$V \supset V_1 \supset \cdots \supset V_d \neq \emptyset$$

is a maximal chain of distinct closed irreducible subsets of V. (Maximal means that the chain cannot be refined.) Then $\dim(V) = d$.

4.3 Affine varieties as functors

Let k be an arbitrary field; we will drop our earlier restriction on k to be algebraically closed. As we have observed, in this case the geometry does not carry enough information, due to the failure of Hilbert's Nullstellensatz (think for example about the imaginary circle $x^2+y^2+1 = 0$ over $\mathbb{R}$). Simply extending our base field to its algebraic closure is not the right solution, since we would then lose the specific nature of our objects over the original base field. We would like to understand our objects over all field extensions *simultaneously*, and that is where functors come into play. In fact, we will at once allow extensions over all k-algebras, not just fields; it will soon become clear why we do this.

Definition 4.3.1. Let k be an arbitrary field, let $I \trianglelefteq A_n = k[t_1, \ldots, t_n]$, and let $A = A_n/I$. For any $R \in k\text{-}\mathbf{alg}$, we let

$$V_R(I) := \{x \in R^n \mid f(x) = 0 \text{ for all } f \in I\},$$

and we call this the set of *R-points of A*. Observe that we can identify the set $V_R(I)$ with $\hom_{k\text{-}\mathbf{alg}}(A, R)$, in exactly the same fashion as we did in Proposition 4.2.2(ii).

We are now ready to introduce the notion of affine k-functors.

Definition 4.3.2. (i) A *k-functor* F is a functor from the category k-**alg** to the category **Set**.

(ii) Recall from Definition 3.3.1(i) that for each $A \in k$-**alg**, there is a corresponding functor

$$h^A \colon k\text{-}\mathbf{alg} \to \mathbf{Set} \colon R \rightsquigarrow \hom_{k\text{-}\mathbf{alg}}(A, R).$$

A k-functor F is an *affine k-functor* if there exists a *finitely generated* k-algebra A such that $F \cong h^A$; recall that A is unique up to isomorphism by the Yoneda Lemma (see Corollary 3.3.4). We also say that F is *represented* by A, and we call A the *coordinate ring* or the *coordinate algebra* of the affine k-functor F. We denote it by $A = k[F]$.

(iii) Let F and G be two affine k-functors. A *morphism* $\varphi \colon F \to G$ is defined to be a natural transformation from F to G. By the Yoneda Lemma, each such morphism φ corresponds to a unique algebra morphism $\varphi^* \colon k[G] \to k[F]$.

Example 4.3.3. (i) Consider the k-functor

$$\mathbb{A}^n \colon k\text{-}\mathbf{alg} \to \mathbf{Set} \colon R \rightsquigarrow R^n.$$

Then $\mathbb{A}^n$ is an affine k-functor represented by $A_n = k[t_1, \ldots, t_n]$ since

$$R^n \cong \hom_{k\text{-}\mathbf{alg}}(A_n, R)$$

for all $R \in k$-**alg**.

(ii) Let $I \trianglelefteq A_n$, and consider the k-functor

$$\mathbb{V} \colon k\text{-}\mathbf{alg} \to \mathbf{Set} \colon R \rightsquigarrow V_R(I).$$

Then $\mathbb{V}$ is an affine k-functor represented by $A = A_n/I$, precisely because of the observation we made in Definition 4.3.1. The functor $\mathbb{V}$ is sometimes called the *functor of points* corresponding to I.

Definition 4.3.4. Let F be an affine k-functor with coordinate algebra $A = k[F]$, and let K/k be a field extension. Then we obtain a K-functor F_K (also denoted by $F \times_k K$) simply by restricting the functor F to K-algebras (since every K-algebra is of course also a k-algebra). Notice that

$$\hom_{k\text{-}\mathbf{alg}}(A, R) \simeq \hom_{K\text{-}\mathbf{alg}}(A_K, R)$$

for all $R \in K$-**alg**, where $A_K = k[F] \otimes_k K$ (see Example 2.2.10(4)). This implies that F_K is again an affine functor, with coordinate algebra

$$K[F_K] = k[F] \otimes_k K = A_K.$$

This procedure is called *base change* or *extension of scalars*.

Remark 4.3.5. Note that the coordinate algebras are no longer assumed to be reduced, i.e. they may have non-zero nilpotents. This might sound awkward from a classical point of view, but it is actually very convenient. For instance, it might very well happen that a k-algebra A is reduced, but becomes non-reduced after base change (e.g. if A is a purely inseparable field extension of k, then $A \otimes_k \overline{k}$ will have non-zero nilpotents).

By Yoneda's Lemma (Theorem 3.3.2), or more precisely its Corollary 3.3.4, the map $A \rightsquigarrow h^A$ is a fully faithful contravariant functor from k-**alg** to k-**func**, the category of k-functors. In other words, the category of affine k-functors is anti-equivalent (i.e. dual) to the category of finitely generated k-algebras. In particular, we do not lose any information by replacing a k-algebra A by its associated k-functor h^A.

We should think of the k-functors as *geometric* objects: just as the affine k-varieties form a category which is dual to the category of finitely generated reduced k-algebras when k is algebraically closed, so do the affine k-functors form a category which is dual to the category of finitely generated k-algebras (not necessarily reduced!) when k is arbitrary. The fact that the affine k-functors h^A contain enough information to recover A solves our earlier issue that the set of k-points $V_k(I)$ alone is not rich enough.

In addition, we have gained more: we do not only have affine k-functors at our disposal, but the whole category of k-functors. This brings us into the realm of affine schemes, even though we will not formally develop the theory of schemes here.

We end this section with the construction of products.

Definition 4.3.6. Let F and G be two k-functors. Then the *product* of F and G is the functor

$$F \times G \colon k\text{-}\mathbf{alg} \to \mathbf{Set} \colon R \rightsquigarrow F(R) \times G(R).$$

The product of two affine k-functors is again affine:

Proposition 4.3.7. *Let F and G be two affine k-functors, represented by the k-algebras A and B, respectively. Then $F \times G$ is again an affine k-functor, with coordinate algebra $A \otimes_k B$.*

Proof. For each k-algebra R, we have

$$F(R) \times G(R) \cong \hom_{k\text{-}\mathbf{alg}}(A, R) \times \hom_{k\text{-}\mathbf{alg}}(B, R) \cong \hom_{k\text{-}\mathbf{alg}}(A \otimes_k B, R),$$

where the last bijection is given by mapping a pair $(f, g) \in \hom_{k\text{-}\mathbf{alg}}(A, R) \times \hom_{k\text{-}\mathbf{alg}}(B, R)$ to $f \otimes g$; see Definition 2.2.7. (In a categorical setting, this is precisely the statement that the tensor product is the *coproduct* in the category k-**alg**.) $\square$

Chapter 5 Linear algebraic groups

We are now ready to introduce the main objects of this course. We will continue to adopt the functorial approach that we have started in the last section 4.3, and introduce affine algebraic groups as certain functors. We will see in section 5.4 that every affine algebraic group is *linear*, and in fact, it is much more common to refer to our objects as *linear algebraic groups* instead.

5.1 Affine algebraic groups

Definition 5.1.1. (i) A *k-group functor* G is a functor G from the category k-**alg** to the category **Grp**. Every k-group functor G has an associated k-functor $G^{\mathbf{Set}}$ obtained by the composition

$$k\text{-}\mathbf{alg} \xrightarrow{G} \mathbf{Grp} \xrightarrow{\text{forget}} \mathbf{Set}.$$

(ii) An *affine algebraic group* is a k-group functor G such that the corresponding k-functor $G^{\mathbf{Set}}$ is affine.

(iii) If G is an affine algebraic group, then $G^{\mathbf{Set}}$ is represented by a unique finitely generated k-algebra A, which we call the *coordinate ring* or *coordinate algebra* of G, and which we denote by $k[G]$ or by $\mathcal{O}[G]$.

(iv) If G and H are two affine algebraic groups over k, then a *morphism* $\varphi\colon G \to H$ is defined to be a natural transformation from the functor G to the functor H.

Our main goal in this section is to understand the additional structure on $k[G]$ which is imposed by the fact that the k-functor arises from a k-group functor.

Before we proceed, we will give some examples. Recall that, in order to describe the functors, we will usually only describe what happens with the objects and omit the description of the corresponding map between morphisms (see Remark 3.2.3).

Examples 5.1.2. (1) Define $\mathbb{G}_a$ as the functor

$$k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \rightsquigarrow (R, +).$$

Then for each $R \in k\text{-}\mathbf{alg}$, we can identify $\mathbb{G}_a(R)$ with $\hom_{k\text{-}\mathbf{alg}}(k[t], R)$, and hence

$$k[\mathbb{G}_a] \cong k[t],$$

the ring of polynomials over k in one variable. The affine algebraic group $\mathbb{G}_a$ is called the *additive (algebraic) group over k*.

(2) Let n be a positive integer, and define SL_n as the functor

$$k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \rightsquigarrow \mathsf{SL}_n(R).$$

Then SL_n is an affine algebraic group with

$$k[\mathsf{SL}_n] \cong k[t_{11}, \ldots, t_{nn}] \,/\, (\det(t_{ij}) - 1).$$

(3) Let n be a positive integer, and define GL_n as the functor

$$k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \rightsquigarrow \mathsf{GL}_n(R).$$

Then by Rabinowitch's trick (see page 2), GL_n is an affine algebraic group with

$$k[\mathsf{GL}_n] \cong k[t_{11}, \ldots, t_{nn}, d] \,/\, (d \cdot \det(t_{ij}) - 1).$$

(4) The functor GL_1 is also written as $\mathbb{G}_m$, and called the *multiplicative (algebraic) group over k*. In this case,

$$\mathbb{G}_m\colon k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \rightsquigarrow (R^\times, \cdot),$$

and

$$k[\mathbb{G}_m] \cong k[t, d]/(dt - 1) \cong k[t, t^{-1}],$$

the ring of Laurent polynomials over k.

(5) The functor SL_1 maps every k-algebra R to the trivial group, and is called the *trivial algebraic group* over k. In this case,

$$k[1] \cong k[t]/(t - 1) \cong k.$$

(6) Let n be a positive integer, and define μ_n as the functor

$$\mu_n\colon k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \rightsquigarrow \{r \in R \mid r^n = 1\}.$$

Then μ_n is an affine algebraic group with

$$k[\mu_n] \cong k[t]/(t^n - 1).$$

It is called the *algebraic group of n-th roots of unity* over k, and is also referred to as a *multiplicative torsion group*. Note that $k[\mu_n]$ has nilpotent elements if $\mathrm{char}(k) = p \mid n$.

(7) Let p be a prime number, and let k be a field with $\mathrm{char}(k) = p$. We define the functor α_p by

$$\alpha_p \colon k\text{-}\mathbf{alg} \to \mathbf{Grp} \colon R \rightsquigarrow \big(\{r \in R \mid r^p = 0\}, +\big).$$

Then α_p is an affine algebraic group with

$$k[\alpha_p] \cong k[t]/(t^p).$$

Note that $k[\alpha_p]$ is never reduced.

The coordinate algebra $k[G]$, as a k-algebra, only describes the geometry of the k-functor G, not its group structure. We will now try to understand how the group structure imposes additional structure on $k[G]$.

Definition 5.1.3. Let G be a k-group functor. The multiplication, the inverse and the neutral element for each of the objects $G(R)$ defines natural transformations

$$\begin{aligned} \mu &\colon G \times G \to G, \\ \iota &\colon G \to G, \\ e &\colon 1 \to G. \end{aligned}$$

By the Yoneda Lemma (see Corollary 3.3.4), we have corresponding k-algebra morphisms

$$\begin{aligned} \Delta &\colon k[G] \to k[G] \otimes_k k[G], \\ S &\colon k[G] \to k[G], \\ \epsilon &\colon k[G] \to k. \end{aligned}$$

They are called the *comultiplication*, the *antipode* and the *counit*, respectively.

Before we will figure out which axioms these morphisms satisfy in general, we will try to get some feeling for these morphisms by some explicit examples.

Example 5.1.4. (1) Consider the additive algebraic group $G = \mathbb{G}_a \colon R \mapsto (R, +)$, and recall that $k[\mathbb{G}_a] \cong k[t]$. Explicitly, for each $R \in k\text{-}\mathbf{alg}$, there is a bijection

$$\beta \colon \hom_{k\text{-}\mathbf{alg}}(k[t], R) \to (R, +) \colon \alpha \mapsto \alpha(t).$$

Similary, for $\mathbb{G}_a \times \mathbb{G}_a$, we have

$$k[\mathbb{G}_a \times \mathbb{G}_a] \cong k[t] \otimes_k k[t] \cong k[t_1, t_2],$$

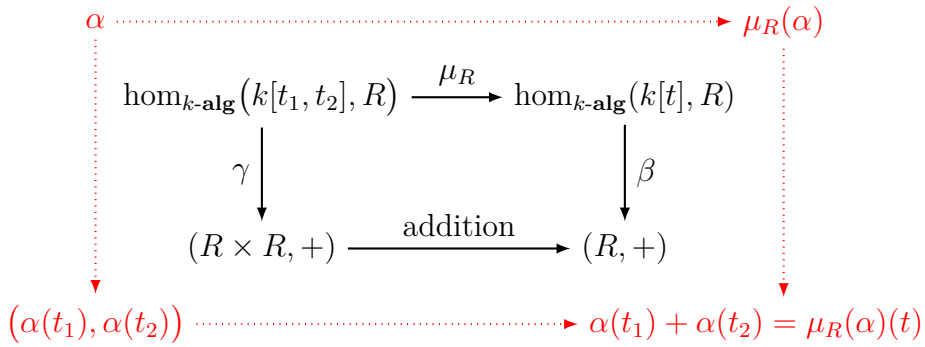
and there is a bijection

$$\gamma\colon\ \hom_{k\text{-}\mathbf{alg}}\big(k[t_1,t_2],R\big)\to(R\times R,+)\colon\alpha\mapsto\big(\alpha(t_1),\alpha(t_2)\big).$$

The natural transformation $\mu\colon\mathbb{G}_a\times\mathbb{G}_a\to\mathbb{G}_a$ induces, for each R, a morphism

$$\mu_R\colon\ \hom_{k\text{-}\mathbf{alg}}\big(k[t_1,t_2],R\big)\to\hom_{k\text{-}\mathbf{alg}}(k[t],R)$$

which should correspond, under the above bijections β and γ, to the addition map from $R\times R$ to R. We express this in a commutative diagram:



We conclude that

$$\mu_R(\alpha)(t)=\alpha(t_1)+\alpha(t_2)=\alpha(t\otimes 1+1\otimes t)$$

for each $R\in k\text{-}\mathbf{alg}$. By the Yoneda Lemma (Theorem 3.3.2), the comultiplication Δ is given by

$$\Delta=\mu_{k[G]\otimes k[G]}\big(\mathrm{id}_{k[G]\otimes k[G]}\big),$$

and hence

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

Notice that this completely determines the k-algebra morphism Δ. In a completely similar fashion, we get

$$S(t)=-t\qquad\text{and}\qquad\epsilon(t)=0.$$

(2) We now consider the multiplicative algebraic group $\mathbb{G}_m\colon R\mapsto(R^\times,\cdot)$, with $k[\mathbb{G}_m]=k[t,t^{-1}]$. In the same manner as in the previous example, we get

$$\mu_R(\alpha)(t)=\alpha(t_1)\alpha(t_2)=\alpha\big((t\otimes 1)(1\otimes t)\big)=\alpha(t\otimes t)$$

for each k-algebra R, and hence

$$\Delta(t) = t \otimes t;$$

similarly,

$$S(t) = t^{-1} \quad \text{and} \quad \epsilon(t) = 1.$$

(3) We finally consider the example $G = \mathsf{GL}_n$, with coordinate algebra $k[G] = k[t_{ij}, d]/(d \cdot \det(t_{ij}) - 1)$. We leave the details of the computation as an exercise; the outcome is as follows:

$$\begin{aligned}
\Delta(t_{ij}) &= \textstyle\sum_{\ell=1}^{n} t_{i\ell} \otimes t_{\ell j}, \\
\Delta(d) &= d \otimes d, \\
S(t_{ij}) &= d \cdot a_{ji} \ \text{ where } a_{ji} \text{ is the cofactor of } t_{ji}, \\
S(d) &= \det(t_{ij}), \\
\epsilon(t_{ij}) &= \delta_{ij} \ \text{ (the Kronecker delta)}, \\
\epsilon(d) &= 1.
\end{aligned}$$

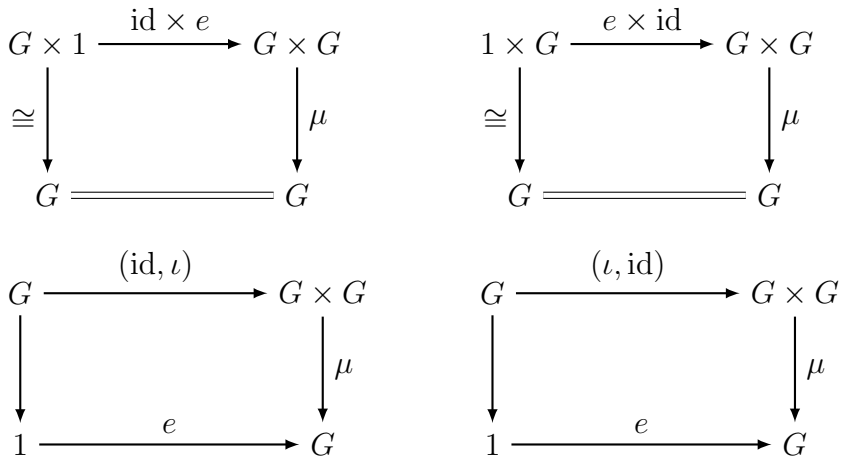
We would now like to understand what conditions our k-morphisms Δ, S and ϵ satisfy, and once again the Yoneda Lemma will give us the answer. Let us first express the axioms of a group in terms of commutative diagrams involving the natural transformations μ, ι and e.

Lemma 5.1.5. *Let G be a k-functor. Then $G = H^{\mathbf{Set}}$ for some k-group functor H if and only if there are natural transformations*

$$\begin{aligned}
\mu &\colon G \times G \to G, \\
\iota &\colon G \to G, \\
e &\colon 1 \to G,
\end{aligned}$$

such that the following diagrams commute:

$$\begin{array}{ccc}
G \times G \times G & \xrightarrow{\mathrm{id} \times \mu} & G \times G \\
{\scriptstyle \mu \times \mathrm{id}} \downarrow & & \downarrow {\scriptstyle \mu} \\
G \times G & \xrightarrow{\mu} & G
\end{array}$$



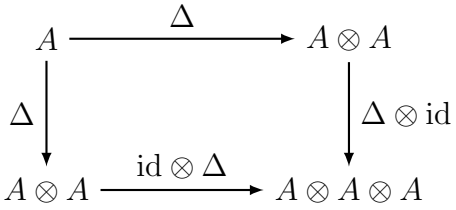
Proof. It is clear that for each $R \in k$-**alg**, the commutativity of each of the above diagrams translates into a similar commutative diagram for the set $G(R)$. The first diagram expresses the associativity of each μ_R, the second and third diagram express the existence of a unit (namely $e_R(1)$) for each $G(R)$, and the fourth and fifth diagram express the existence of an inverse map (namely ι_R) in each $G(R)$. □

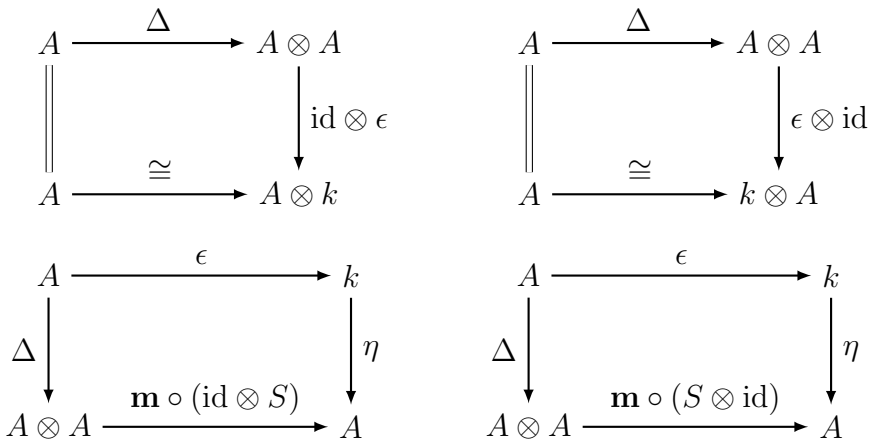
Yoneda's Lemma now immediately implies a similar statement for the corresponding coordinate algebras.

Proposition 5.1.6. *Let A be a finitely generated k-algebra, with multiplication map $\mathbf{m}\colon A \otimes A \to A$. Then A is the coordinate algebra of some affine algebraic k-group G if and only if there are k-algebra morphisms*

$$\begin{aligned} \Delta &\colon A \to A \otimes A, \\ S &\colon A \to A, \\ \epsilon &\colon A \to k, \end{aligned}$$

such that the following diagrams commute:





Proof. This follows immediately from Lemma 5.1.5 and Corollary 3.3.4. One subtle point is how to dualize the morphism $(\mathrm{id}, \iota)\colon G \to G \times G$. Notice that this morphism can be decomposed as

$$G \xrightarrow{\mathrm{diag}} G \times G \xrightarrow{\mathrm{id}\times\iota} G \times G,$$

where diag_R is the "diagonal map" $G(R) \to G(R) \times G(R)\colon g \mapsto (g, g)$. It only remains to show that the dual of $\mathrm{diag}\colon G \to G \times G$ is precisely $\mathbf{m}\colon A \otimes A \to A$. This follows immediately from the Yoneda Lemma, since $\mathrm{diag}_A(\mathrm{id}_A)\colon A \otimes A \to A\colon a \otimes b \mapsto \mathrm{id}_A(a)\mathrm{id}_A(b) = ab = \mathbf{m}(a \otimes b)$. □

Definition 5.1.7. (i) A k-algebra A equipped with k-algebra morphisms Δ, S and ϵ satisfying the requirements from Proposition 5.1.6 is called a *(commutative) Hopf algebra*[1]. Explicitly, we require the following axioms to hold, where $\eta\colon k \to A$ is the structure morphism of the k-algebra A, and where $\mathbf{m}\colon A \otimes A \to A$ is the multiplication map:

$$(\mathrm{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathrm{id}) \circ \Delta,$$
$$\mathbf{m} \circ (\mathrm{id} \otimes \epsilon) \circ \Delta = \mathrm{id} = \mathbf{m} \circ (\epsilon \otimes \mathrm{id}) \circ \Delta,$$
$$\mathbf{m} \circ (\mathrm{id} \otimes S) \circ \Delta = \eta \circ \epsilon = \mathbf{m} \circ (S \otimes \mathrm{id}) \circ \Delta.$$

(ii) Let A, B be two Hopf k-algebras. A *Hopf algebra morphism* from A to B is a k-algebra morphism $f\colon A \to B$ compatible with the morphisms Δ, S and ϵ, i.e., such that

$$\Delta_B \circ f = (f \otimes f) \circ \Delta_A,$$
$$S_B \circ f = f \circ S_A,$$
$$\epsilon_B \circ f = \epsilon_A.$$

[1]We will use the simple term *Hopf algebra* for a commutative Hopf algebra, but depending on the context, other authors might have the more general notion of not necessarily commutative Hopf algebras in mind.

In fact, it is sufficient to require f to be compatible with Δ; it then follows that it is also compatible with S and with ϵ.

(iii) Let A, B be two Hopf k-algebras. The *tensor product* of A and B (as Hopf algebras) is the Hopf algebra with underlying k-algebra equal to $A \otimes_k B$ as in Definition 2.2.9, and with Δ, S and ϵ defined in the obvious way, i.e.,

$$\begin{aligned}
\Delta_{A\otimes B} &= (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \circ (\Delta_A \otimes \Delta_B),\\
S_{A\otimes B} &= S_A \otimes S_B,\\
\epsilon_{A\otimes B} &= \mathbf{m}_k \circ (\epsilon_A \otimes \epsilon_B).
\end{aligned}$$

It is straightforward to verify that this makes $A \otimes_k B$ into a Hopf algebra.

Corollary 5.1.8. *The category of affine algebraic k-groups is anti-equivalent to the category of commutative finitely generated Hopf algebras over k.*

In particular, there is a one-two-one correspondence between morphisms $\varphi\colon G \to H$ between two affine algebraic k-groups and morphisms $\varphi^*\colon k[H] \to k[G]$ between the corresponding Hopf algebras.

Proof. This follows immediately from Proposition 5.1.6. Recall that morphisms between affine algebraic groups are defined as natural transformations between functors, so the final statement follows from Corollary 3.3.4. □

Remark 5.1.9. Let G be an affine algebraic k-group and let $R \in k$-**alg**.

(i) In what follows, we will very often identify the group $G(R)$ with the set $\hom_{k\text{-}\mathbf{alg}}(A, R)$ without explicitly writing the bijection β as in Example 5.1.4(1).

(ii) Observe that under this identification, the unit element $1 \in G(k)$ corresponds precisely to the counit $\epsilon\colon A \to k$; more generally, the unit element $1 \in G(R)$ corresponds to the composition $\eta_R \circ \epsilon\colon A \to R$, where $\eta_R\colon k \to R$ is the structure morphism of the k-algebra R.

Remark 5.1.10. Suppose that G and H are two affine algebraic k-groups, with coordinate algebras $k[G]$ and $k[H]$, respectively. By Proposition 4.3.7, the affine k-functor $G \times H$ has coordinate algebra $k[G \times H] \cong k[G] \otimes_k k[H]$. In fact, $G \times H$ is again an affine algebraic k-group, and the isomorphism $k[G \times H] \cong k[G] \otimes_k k[H]$ is an isomorphism of Hopf algebras. (We leave the details of the verification of this fact to the reader.)

We will now use this duality between the two categories to construct the so-called constant finite algebraic groups over k.

Definition 5.1.11. An affine algebraic k-group G is called *finite* if its coordinate algebra $k[G]$ is finite-dimensional.

Example 5.1.12 (Constant finite algebraic groups)**.** Let F be any finite group. Our goal is to construct an affine algebraic k-group G such that $G(R) \cong F$ "as often as possible". Let

$$A \coloneqq \hom_{\mathbf{Set}}(F, k)$$

with its natural k-algebra structure. Observe that as an algebra, we simply have the structure of a direct product

$$A \cong \prod_{g \in F} k.$$

For each $g \in F$, let

$$e_g \colon F \to k \colon \begin{cases} g \mapsto 1, \\ h \mapsto 0 \quad (h \neq g). \end{cases}$$

Then $\{e_g \mid g \in F\}$ forms a complete system of idempotents:

$$e_g^2 = e_g; \qquad e_g e_h = 0 \text{ for all } g \neq h; \qquad \sum e_g = 1.$$

We now make A into a Hopf algebra. We define k-algebra morphisms Δ, S and ϵ by setting

$$\begin{aligned} \Delta(e_g) &\coloneqq \sum_{a,b \in F \,|\, g=ab} e_a \otimes e_b, \\ S(e_g) &\coloneqq e_{g^{-1}}, \\ \epsilon(e_g) &\coloneqq \begin{cases} 1 & \text{if } g = 1, \\ 0 & \text{if } g \neq 1, \end{cases} \end{aligned}$$

for all $g \in F$. It is now an easy exercise to verify that these morphisms satisfy the defining relations of a Hopf algebra. The associated affine algebraic group F_k is now defined by

$$F_k(R) = h^A(R) = \hom_{k\text{-}\mathbf{alg}}(A, R).$$

If R is a k-algebra without non-trivial idempotents, then every k-algebra morphism from A to R necessarily maps exactly one element e_g ($g \in F$) to 1 and all others to 0; we conclude that in this case, $F_k(R) \cong F$, at least as a set. (Note, however, that if R does have non-trivial idempotents, then $F_k(R)$ is

always larger than F.) We verify that for such R, the group structure induced by Δ, S and ϵ coincides with the original group structure of F. Since the morphism Δ is the dual of the natural transformation μ, the multiplication μ_R is given by

$$\mu_R \colon h^{A\otimes A}(R) \to h^A(R) \colon f \mapsto f \circ \Delta.$$

The identification between F and $h^A(R)$ is given by the bijection

$$\beta \colon F \to h^A(R) \colon g \mapsto \beta_g \colon \begin{cases} e_g \mapsto 1, \\ e_h \mapsto 0 \text{ for all } h \neq g. \end{cases}$$

Now assume that $f \in h^{A\otimes A}(R) \cong F \times F$ is represented by $(g_1, g_2) \in F \times F$, i.e. $f = (\beta_{g_1}, \beta_{g_2}) \in h^A(R) \times h^A(R)$. We have to show that $\mu_R(f) = \beta_{g_1 g_2}$; it suffices to verify this for each generator e_h, i.e. we have to check whether

$$(f \circ \Delta)(e_h) = \beta_{g_1 g_2}(e_h)$$

for all $h \in F$. We leave this as an easy exercise.

The affine algebraic groups F_k are called *constant finite algebraic groups*.

Remark 5.1.13. Observe that in general, the constant algebraic group $\mathbb{Z}/n$ is different from the algebraic group μ_n. For instance, over $\mathbb{Q}$, the groups $\mathbb{Z}/3$ and μ_3 are not isomorphic because they have different coordinate algebras (or simply because $\mathbb{Z}/3(\mathbb{Q})$ has 3 elements whereas $\mu_3(\mathbb{Q})$ has only 1 element).

However, when n is not a multiple of $\mathrm{char}(k)$ and k contains an n-th root of unity, then $\mathbb{Z}/n \cong \mu_n$ (which is the case, for example, for $k = \mathbb{C}$).

5.2 Closed subgroups

As for every algebraic structure, it will be invaluable to study substructures. In our setting, this means that we are interested in subgroups of affine algebraic groups that become affine algebraic groups in their own right. This brings us to the notion of closed subgroups.

Definition 5.2.1. (i) Let $\mathcal{C}$ be a category, and let F be a functor from $\mathcal{C}$ to **Set**. A functor G from $\mathcal{C}$ to **Set** is a *subfunctor* of F, if

- for every $X \in \mathrm{ob}(\mathcal{C})$, the set $G(X)$ is a subset of $F(X)$; and
- for every $\alpha \in \hom_{\mathcal{C}}(X, Y)$, the morphism $G(\alpha)$ is the restriction of $F(\alpha)$ to $G(X)$.

(ii) Let $\mathcal{C}$ be a category, and let G be a functor from $\mathcal{C}$ to **Grp**. A functor H from $\mathcal{C}$ to **Grp** is a *subgroup* of G, if

- for every $X \in \mathrm{ob}(\mathcal{C})$, the group $H(X)$ is a subgroup of $G(X)$; and
- for every $\alpha \in \hom_{\mathcal{C}}(X, Y)$, the morphism $H(\alpha)$ is the restriction of $G(\alpha)$ to $H(X)$.

(iii) If, moreover,

- $H(X)$ is a normal subgroup of $G(X)$ for all $X \in \mathrm{ob}(\mathcal{C})$,

then we call H a *normal subgroup* of G.

(iv) Let G be an affine algebraic k-group with coordinate algebra $A = k[G]$. A subgroup H of G is *closed* (or *algebraic*), if H is representable by a quotient of A (as Hopf algebras).

Notice that a closed subgroup H of an affine algebraic group G is indeed again an affine algebraic group, because $k[H]$ is a quotient of the finitely generated k-algebra A, and hence is itself finitely generated.

Remark 5.2.2. Let G be an affine algebraic k-group with coordinate algebra $A = k[G]$ and let H be a subgroup of G. If H is representable, then it is automatically representable by a quotient of A (and hence H is a closed subgroup); this follows from Corollary 5.3.3 below.

Conversely, we would like to know which ideals I of A give rise to a closed subgroup of G. This brings us to the notion of a Hopf ideal.

Definition 5.2.3. Let A be a Hopf algebra over k, and let I be an ideal of the k-algebra A. Then I is called a *Hopf ideal* of A, if

- $\Delta(I) \subseteq I \otimes A + A \otimes I$;
- $S(I) \subseteq I$;
- $\epsilon(I) = 0$.

The notion of a Hopf ideal plays the same role as the notion of an ideal for rings with respect to homomorphisms:

Lemma 5.2.4. *Let $\varphi\colon A \to B$ be a homomorphism of Hopf algebras. Then* $\ker(\varphi)$ *is a Hopf ideal of A, and* $\mathrm{im}(\varphi)$ *is a Hopf subalgebra of B.*

Conversely, every Hopf ideal I of A is the kernel of some homomorphism $\varphi\colon A \to B$ of Hopf algebras, and the quotient A/I is again a Hopf algebra, isomorphic to $\mathrm{im}(\varphi)$.

Proof. We leave the proof of these facts as an exercise. □

The following correspondence between closed subgroups of G and Hopf ideals of A is now immediate.

Corollary 5.2.5. *Let G be an affine algebraic k-group with coordinate algebra $A = k[G]$. The closed subgroups of G are in natural one-to-one correspondence with the Hopf ideals of A.*

Proof. This follows from Definition 5.2.1(iv) and Lemma 5.2.4. □

We give one more result for later use.

Proposition 5.2.6. *Let G, H be two affine algebraic k-groups, with coordinate algebras $A = k[G]$ and $B = k[H]$, and let $\varphi\colon G \to H$ be a morphism. Then the kernel $N = \ker\varphi$ is a normal closed subgroup of G with coordinate algebra $k[N] = A/\overline{I_H}$, where I_H is the* augmentation ideal *of B, i.e. I_H is the kernel of the counit $\epsilon_H\colon B \to k$, and where $\overline{I_H} := \varphi^*(I_H)A$ is the corresponding ideal in A.*

Proof. Notice that N is defined to be the k-group functor

$$N\colon k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \mapsto \ker\big(G(R) \xrightarrow{\varphi_R} H(R)\big).$$

Then an element $g \in G(R) = \hom_{k\text{-}\mathbf{alg}}(A, R)$ lies in $N(R)$ if and only if its composite with $\varphi^*\colon B \to A$ factors through the counit $\epsilon_H\colon B \to k$ (see Remark 5.1.9(ii)). So let I_H be the kernel of ϵ_H, and let $\overline{I_H} := \varphi^*(I_H)A \trianglelefteq A$ be the corresponding ideal in A. Then an element $g \in G(R) = \hom_{k\text{-}\mathbf{alg}}(A, R)$ lies in $N(R)$ if and only if it is zero on $\varphi^*(I_H)$, and hence on $\overline{I_H}$. We conclude that $N(R) = \hom_{k\text{-}\mathbf{alg}}(A/\overline{I_H}, R)$ for all $R \in k\text{-}\mathbf{alg}$. □

5.3 Homomorphisms and quotients

Recall that a homomorphism $\varphi\colon G \to H$ between affine algebraic groups is uniquely determined by its dual homomorphism $\varphi^*\colon k[H] \to k[G]$ between Hopf algebras. Perhaps surprisingly[2], the injectivity and surjectivity of φ versus φ^* are related in a rather subtle fashion.

Definition 5.3.1. Let $\varphi\colon G \to H$ be a morphism between two affine algebraic k-groups G and H, with dual morphism $\varphi^*\colon k[H] \to k[G]$.

[2]The reason is that injectivity and surjectivity cannot be expressed in terms of morphisms in a category. The corresponding categorical notions are those of "monic" and "epic" morphisms, which for the category **Set** indeed amount to injectivity and surjectivity, but which are genuinely different notions in many other categories.

(i) The morphism φ is called *injective* if $\varphi_R\colon G(R) \to H(R)$ is injective for each $R \in k\text{-}\mathbf{alg}$.

(ii) The morphism φ is called a *quotient map* if φ^* is injective.

The following proposition is essential, but its proof requires more theory than we have covered (fibered products and faithful flatness of algebras).

Proposition 5.3.2. *A morphism $\varphi\colon G \to H$ is an isomorphism if and only if it is an injective quotient map.*

Proof omitted. □

Corollary 5.3.3. *A morphism $\varphi\colon G \to H$ is injective if and only if the dual morphism $\varphi^*\colon k[H] \to k[G]$ is surjective.*

Proof. Assume first that φ^* is surjective. Notice that for each $R \in k\text{-}\mathbf{alg}$, the map $\varphi_R\colon G(R) = \hom_{k\text{-}\mathbf{alg}}(k[G], R) \to H(R) = \hom_{k\text{-}\mathbf{alg}}(k[H], R)$ is simply given by $g \mapsto g \circ \varphi^*$, which is indeed an injective map if φ^* is surjective.

Conversely, assume that φ is injective and let $A := \operatorname{im}\varphi^*$, so that φ^* decomposes as

$$\varphi^*\colon k[H] \twoheadrightarrow A \hookrightarrow k[G].$$

Let G' be the affine algebraic k-group corresponding to the Hopf algebra A; then φ decomposes correspondingly as

$$\varphi\colon G \to G' \to H.$$

Since φ is injective, the same is true for the map $G \to G'$. It now follows from Proposition 5.3.2 that this map $G \to G'$ is an isomorphism, and we conclude that φ^* is indeed surjective. □

Remark 5.3.4. Notice that we did not give a name to morphisms φ for which each φ_R is surjective. As it turns out, this is not a very useful notion. In particular, if φ is a quotient map, then it is *not* necessarily true that each φ_R is surjective. (The converse is still true.) We give two typical examples.

(1) Let $k = \mathbb{Q}$ and let $\varphi\colon \mathbb{G}_m \to \mathbb{G}_m$ be the n-th power map, taking each $g \in \mathbb{G}_m(R)$ to $g^n \in \mathbb{G}_m(R)$. The dual morphism $\varphi^*\colon k[t, t^{-1}] \to k[t, t^{-1}]$ maps t to t^n; this map is clearly injective. However, the corresponding map $\varphi_{\mathbb{Q}}\colon \mathbb{G}_m(\mathbb{Q}) \to \mathbb{G}_m(\mathbb{Q})$ is not surjective. (On the other hand, $\varphi_{\overline{\mathbb{Q}}}\colon \mathbb{G}_m(\overline{\mathbb{Q}}) \to \mathbb{G}_m(\overline{\mathbb{Q}})$ is surjective.)

(2) Let $\varphi\colon \mathsf{SL}_n \to \mathsf{PGL}_n$ be the canonical projection. Then it can be checked that φ^* is injective. (We will do this in the exercises for $n = 2$.) On the

other hand, φ_R is in general of course not surjective; the image of φ_R is $\mathsf{PSL}_n(R)$. In fact, PSL_n is not an affine algebraic group — in other words, the functor $G\colon k\text{-}\mathbf{alg} \to \mathbf{Grp}\colon R \mapsto \mathsf{PSL}_n(R)$ is not representable. (Try to Google for "PSL is not an algebraic group" if you are interested to know more.)

The observation about $\overline{\mathbb{Q}}$ in the first example above is not a coincidence:

Proposition 5.3.5. *Let G and H be affine algebraic k-groups and denote the algebraic closure of k by $\overline{k}$. Let $\varphi\colon G \to H$ be a quotient map. Then the map $\varphi_{\overline{k}}\colon G(\overline{k}) \to H(\overline{k})$ is surjective.*

Proof omitted. □

Remark 5.3.6. The converse of this proposition is not true in general, but it is true whenever H is *smooth*; see section 8.5 below.

We will need the following proposition later; its proof again makes use of fibered products.

Proposition 5.3.7. *Let $\varphi\colon G \to H$ be a quotient map and let N be the kernel of φ. Assume that $\psi\colon G \to H'$ is another homomorphism whose kernel contains N. Then ψ factors uniquely through H, i.e., there is a unique homomorphism $\psi'\colon H \to H'$ such that $\psi = \psi' \circ \varphi$.*

Proof omitted. □

Remark 5.3.8. When $\varphi\colon G \to H$ is a quotient map with kernel N, then we can assemble this information in a short exact sequence

$$1 \to N \to G \to H \to 1.$$

In this case, we also denote H by G/N. We emphasize once again that this does *not* imply that there are corresponding exact sequences

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

in general, and correspondingly, it is *not* true in general that $(G/N)(R) \cong G(R)/N(R)$.

It is a *highly* non-trivial fact that quotients by closed normal subgroups always exist:

Theorem 5.3.9. *Let G be an affine algebraic k-group and let N be a closed normal subgroup of G. Then there exists a quotient map $\varphi\colon G \to H$ with kernel N; in particular, $H = G/N$ exists (and is unique up to isomorphism).*

Proof omitted. □

5.4 Affine algebraic groups are linear

So far, we have mainly been defining the objects we are interested in, but in some sense, we have not yet proven any non-trivial theorems about affine algebraic groups. In this section, we will use the theory we have built op so far to show a crucial fact about affine algebraic groups, namely that they are always *linear* in the sense that they can be embedded in a finite-dimensional matrix group. The right context to study such embeddings is *representation theory*, so we will first define the necessary relevant notions.

Definition 5.4.1. (i) Let G be an affine algebraic group over k, and let V be a k-vector space. A *representation* of G is a natural transformation

$$\rho\colon G \to \mathsf{GL}_V,$$

where GL_V is the k-group functor defined as

$$\mathsf{GL}_V(R) \coloneqq \mathsf{GL}(R \otimes_k V).$$

(We do not require V to be finite-dimensional, although that case will eventually be of main interest.) Note that $R \otimes_k V$ is a free R-module, and $\mathsf{GL}(R \otimes_k V)$ denotes the group of automorphisms of this R-module.

(ii) Let A be a Hopf algebra over k. An *A-comodule* is a pair (V, m), where V is a k-vector space, and where $m\colon V \to A \otimes_k V$ is a k-linear map such that[3]

$$\begin{aligned} \big(\mathrm{id}_A \otimes m\big) \circ m &= (\Delta \otimes \mathrm{id}_V) \circ m, \\ (\epsilon \otimes \mathrm{id}_V) \circ m &= \mathrm{id}_V, \end{aligned}$$

i.e. such that the following two diagrams commute.

$$\begin{array}{ccc} V & \xrightarrow{m} & A \otimes V \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle \mathrm{id} \otimes m} \\ A \otimes V & \xrightarrow{\Delta \otimes \mathrm{id}} & A \otimes A \otimes V \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{m} & A \otimes V \\ \| & & \downarrow{\scriptstyle \epsilon \otimes \mathrm{id}} \\ V & \xrightarrow{\cong} & k \otimes V \end{array}$$

These two definitions are closely related:

[3]The reader should compare the defining commutative diagrams with those of a G-module V.

Proposition 5.4.2. *Let G be an affine algebraic k-group, with coordinate algebra $A = k[G]$.*

(i) *Let $\rho\colon G \to \mathsf{GL}_V$ be a G-representation, and let m be the restriction of $\rho_A(\mathrm{id}_A) \in \mathsf{GL}_V(A) = \mathsf{GL}(A \otimes_k V)$ to V. Then (V, m) is an A-comodule.*

(ii) *Conversely, let (V, m) be an A-comodule, and let $\rho\colon G \to \mathsf{GL}_V$ be the natural representation given by*

$$\rho_R(g) \coloneqq (g \otimes \mathrm{id}_V) \circ m \quad \textit{for all } g \in G(R) = \hom_{k\text{-}\mathbf{alg}}(A, R). \tag{5.1}$$

Then ρ is a G-representation.

Because of this equivalence, we will often say that a comodule (V, m) *is a G-representation.*

Proof. Let End_V be the k-functor

$$\mathrm{End}_V\colon k\text{-}\mathbf{alg} \to \mathbf{Set}\colon R \rightsquigarrow \mathrm{End}(R \otimes_k V).$$

By the Yoneda Lemma, we have a natural bijection

$$\mathrm{Nat}(G^{\mathbf{Set}}, \mathrm{End}_V) \simeq \mathrm{End}_V(A) = \mathrm{End}(A \otimes_k V).$$

Since an element of $\mathrm{End}(A \otimes_k V)$ is uniquely determined by its restriction to a k-linear map $m\colon V \to A \otimes_k V$, this means that there is a one-to-one correspondence between natural transformation of k-functors ρ (not taking into account that they arise from k-group functors!) and k-linear maps $m\colon V \to A \otimes_k V$. Notice that the formula (5.1) is a direct consequence of the Yoneda Lemma: by equation (3.1), we have $\rho_R(g) = \mathrm{End}_V(g)(m)$ for all $g \in G(R) = \hom_{k\text{-}\mathbf{alg}}(A, R)$.

It remains to show that ρ is a natural transformation of k-group functors if and only if (V, m) is a comodule for A. In principle, this is a consequence of the Yoneda Lemma by dualizing the axioms for a G-module, in the category k-**vec** of k-vector spaces, identifying a vector space V inside its dual $\hom_{k\text{-}\mathbf{vec}}(V, k)$, but we will give an explicit argument instead.

To do this, we will first show that ρ preserves the identity if and only if $(\epsilon \otimes \mathrm{id}_V) \circ m = \mathrm{id}_V$ (which is the second defining identity for comodules). Indeed, notice that ρ preserves the identity if and only if ρ_k preserves the identity, which holds if and only if $\rho_k(\epsilon) = \mathrm{id}_V$. We now simply observe that $\rho_k(\epsilon) = (\epsilon \otimes \mathrm{id}_V) \circ m$ by equation (5.1).

We now show that ρ preserves the group multiplication if and only if $\big(\mathrm{id}_A \otimes m\big) \circ m = (\Delta \otimes \mathrm{id}_V) \circ m$ (which is the first defining identity for

comodules). Indeed, let $R \in k\text{-}\mathbf{alg}$, and let $g, h \in G(R)$. Then gh is, by definition, given by the composition

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

and hence $\rho_R(gh)$ acts on V as

$$V \xrightarrow{m} A \otimes V \xrightarrow{\Delta \otimes \mathrm{id}_V} A \otimes A \otimes V \xrightarrow{(g,h)\otimes \mathrm{id}_V} R \otimes V.$$

On the other hand, $\rho_R(g)\rho_R(h)$ acts on V as[4]

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

or equivalently, as

$$V \xrightarrow{m} A \otimes V \xrightarrow{\mathrm{id}_A \otimes m} A \otimes A \otimes V \xrightarrow{(g,h)\otimes \mathrm{id}_V} R \otimes V.$$

We conclude that $\rho_R(gh) = \rho_R(g)\rho_R(h)$ for all $R \in k\text{-}\mathbf{alg}$ and all $g, h \in G(R)$, if and only if $\big(\mathrm{id}_A \otimes m\big) \circ m = (\Delta \otimes \mathrm{id}_V) \circ m$. (For the non-trivial implication, choose $R = A \otimes A$ and let g, h be the natural inclusions as the first and second component, respectively, so that $(g, h) = \mathrm{id}_{A\otimes A}$.) □

An important example of a representation is given by $k[G]$ itself.

Definition 5.4.3. Let G be an arbitrary affine algebraic k-group, with coordinate algebra $k[G]$ equipped with the comultiplication Δ. Then $(k[G], \Delta)$ is a comodule for $k[G]$, and hence it induces a representation of G on $k[G]$. We call this the *regular representation* of G. Note, however, that $k[G]$ is almost never finite-dimensional.

The regular representation is faithful, but this is not obvious at this point. (This will follow from Theorem 5.4.6 below.) We will try to find a finite-dimensional subrepresentation of the regular representation which is still faithful.

Let us first formally define this notion:

Definition 5.4.4. Let G be an affine algebraic k-group, and let (V, m) be a G-representation.

[4]Since we have defined our comodules as *left* comodules, we have to consider the dual action on the right; in particular, the action of $\rho_R(g)\rho_R(h)$ on V is given by first applying $\rho_R(g)$, and then $\rho_R(h)$. Some authors prefer to use right comodules, in which case the dual action is on the left.

(i) A subrepresentation of (V, m) is a k-subspace[5] $W \leq V$ such that $m(W) \subseteq k[G] \otimes_k W$.

(ii) The G-representation (V, m) is *locally finite* if every finite-dimensional subspace $W \leq V$ is contained in some finite-dimensional subrepresentation.

The following lemma gives a crucial ingredient for Theorem 5.4.6 that we want to prove in a moment.

Lemma 5.4.5. *Let G be an affine algebraic k-group. Then every G-representation (V, m) is locally finite.*

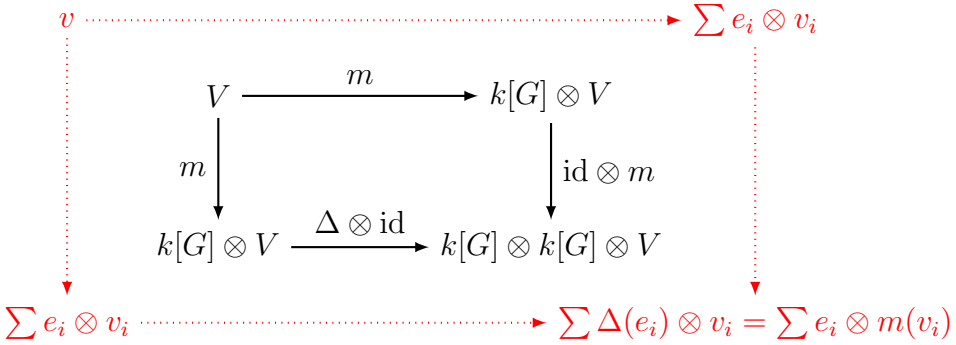
Proof. Let (V, m) be an arbitrary G-representation; it suffices to show that every $v \in V$ is contained in some finite-dimensional subrepresentation. Consider a basis $(e_i)_{i \in I}$ for the k-vector space $k[G]$, and write

$$m(v) = \sum_i e_i \otimes v_i,$$

where each $v_i \in V$, and almost all v_i are zero. On the other hand, we can write

$$\Delta(e_i) = \sum_{j,\ell} r_{ij\ell}(e_j \otimes e_\ell),$$

where each $r_{ij\ell} \in k$, and each of these sums is a finite sum. We now invoke the fact that m is a comodule for $k[G]$:



It follows that

$$\sum_{i,j,\ell} r_{ij\ell}(e_j \otimes e_\ell \otimes v_i) = \sum_j e_j \otimes m(v_j),$$

and comparing the coefficients of e_j yields

$$\sum_{i,\ell} r_{ij\ell}(e_\ell \otimes v_i) = m(v_j)$$

[5] We will sometimes say that V is a G-representation, and not mention m explicitly; more formally, the subrepresentation corresponding to W is the pair $(W, m_{|W})$.

for each j. We conclude that

$$W \coloneqq \langle v, v_i \mid i \in I \rangle$$

is a finite-dimensional subrepresentation of (V, m) containing v. □

We now come to the main theorem of this section.

Theorem 5.4.6. *Let G be an affine algebraic group over k. Then there exists a finite-dimensional vector space V over k and an injective morphism $\rho\colon G \hookrightarrow \mathsf{GL}_V$, so in particular G is a closed subgroup of GL_V.*

Proof. Recall that $A = k[G]$ is a finitely generated k-algebra; let W be a finite-dimensional k-vector space of A that generates A (as a k-algebra). By Lemma 5.4.5, W is contained in some finite-dimensional subrepresentation V of the regular representation (A, Δ); of course V still generates A as a k-algebra. Denote the corresponding natural transformation by

$$\rho\colon G \to \mathsf{GL}_V;$$

it remains to show that ρ is injective, or equivalently, by Corollary 5.3.3, that

$$\rho^*\colon k[\mathsf{GL}_V] \to A$$

is surjective. (Notice that it will also follow then that G (or more precisely, its isomorphic copy $\rho(G)$) is a *closed* subgroup of GL_V because its coordinate algebra will be a quotient of $k[\mathsf{GL}_V]$.)

Let $\{v_1, \ldots, v_n\}$ be a basis for V, and let

$$\Delta(v_j) = \sum_{i=1}^{n} f_{ij} \otimes v_i,$$

with $f_{ij} \in A$. Then by equation (5.1), the natural transformation ρ is given explicitly by

$$\rho_R(g)(v_j) = (g \otimes \mathrm{id}_V)(\Delta(v_j)) = \sum_{i=1}^{n} g(f_{ij}) \otimes v_i$$

for all $g \in G(R) \simeq \hom_{k\text{-}\mathbf{alg}}(A, R)$ and all $j \in \{1, \ldots, n\}$, and hence $\rho_R(g)$ is represented by the matrix

$$\rho_R(g) = \big(g(f_{ij})\big)_{ij} \in \mathsf{GL}_V(R).$$

It follows that

$$\rho^*(t_{ij}) = \rho_A(\mathrm{id}_A)(t_{ij}) = f_{ij}$$

for all i, j, where t_{ij} is the (i,j)-th coordinate function, with $k[\mathsf{GL}_V] \cong k[t_{11}, \ldots, t_{nn}, d]/(d \cdot \det(t_{ij}) - 1)$. On the other hand, it follows from Definition 5.1.7 that

$$v_j = \mathbf{m}(\mathrm{id} \otimes \epsilon)\Delta(v_j) = \mathbf{m}\left(\sum_{i=1}^{n} f_{ij} \otimes \epsilon(v_i)\right) = \sum_{i=1}^{n} \epsilon(v_i) \cdot f_{ij},$$

and hence $v_j \in \operatorname{im} \rho^*$, for all j. Since A is generated by the elements $v_1, \ldots, v_n$ as a k-algebra, we conclude that ρ^* is surjective. □

We have shown that every affine algebraic group is a linear algebraic group, and hence we will use the common terminology "linear algebraic group" from now on.

Example 5.4.7. Consider the algebraic group $\mathbb{G}_a$ over k, with coordinate algebra $A = k[t]$, and choose $W = \langle t \rangle$ as a generating k-subspace of A. Then W is contained in the subrepresentation $V = \langle 1, t \rangle$ of (A, Δ), and

$$\begin{aligned} \Delta(1) &:= 1 \otimes 1, \\ \Delta(t) &:= t \otimes 1 + 1 \otimes t. \end{aligned}$$

We can now immediately read off the corresponding matrix, which is

$$(f_{ij}) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

and we recover the familiar representation for $\mathbb{G}_a$ (see Example 1.1.2(4)).

Remark 5.4.8. In general, the matrix group that we get by applying this procedure has the *opposite* multiplication compared to the group $G(R)$. See also footnote 4 on page 61.

Chapter 6 Jordan decomposition

Now that we have shown that every affine algebraic group is linear, we can apply linear algebra to our study of linear algebraic groups. The Jordan decomposition in linear algebraic groups will allow us to decompose the elements in a semisimple and a unipotent part, and will have far-reaching consequences. We begin with the study of this decomposition in the classical setting, namely in the matrix group $\mathsf{GL}(V)$; we will then see how to extend our ideas to general linear algebraic groups.

6.1 Jordan decomposition in $\mathsf{GL}(V)$

Definition 6.1.1. Let k be an arbitrary commutative field, let V be a finite-dimensional vector space over k, and let $g \in \mathrm{End}_k(V)$. Then:

1. g is *diagonalizable* if V has a basis of eigenvectors for g;
2. g is *semisimple* if V has a basis of eigenvectors for g over the algebraic closure $\overline{k}$, i.e. if g is diagonalizable over $\overline{k}$;
3. g is *nilpotent* if $g^N = 0$ for some integer N;
4. g is *unipotent* if $g - 1$ is nilpotent.

We can now state the main theorem of this section. Recall that a commutative field is called *perfect* if every irreducible polynomial over k has distinct roots, or equivalently, if either $\mathrm{char}(k) = 0$, or $\mathrm{char}(k) = p$ and every element of k is a p-th power.

Theorem 6.1.2 (Jordan decomposition in $\mathsf{GL}(V)$)**.** *Let k be a perfect commutative field, let V be a finite-dimensional vector space over k, and let $g \in \mathsf{GL}(V)$. Then there exist unique elements $g_s, g_u \in \mathsf{GL}(V)$ such that:*

(a) *g_s is semisimple;*

(b) *g_u is unipotent;*

(c) *$g = g_s g_u = g_u g_s$.*

Moreover, both g_s and g_u can be expressed as polynomials in g without constant term.

Proof. We will prove the theorem for algebraically closed fields k only; the proof for general perfect fields k can either go along the same lines, or one can alternatively reduce the general case to the case of algebraically closed fields by some general arguments.

We will first show existence of the elements g_s and g_u. Choose a basis for V such that g is in its Jordan normal form

$$g = \left(\begin{array}{ccccc|c|ccccc} \lambda_1 & * & & & & & & & & & \\ & \lambda_1 & * & & & & & & & & \\ & & \ddots & * & & & & & & & \\ & & & \lambda_1 & & & & & & & \\ \hline & & & & & & \ddots & & & & \\ \hline & & & & & & & \lambda_m & * & & \\ & & & & & & & & \lambda_m & * & \\ & & & & & & & & & \ddots & * \\ & & & & & & & & & & \lambda_m \end{array}\right),$$

where each $*$ is either 0 or 1, and where $\lambda_1, \ldots, \lambda_m$ are the distinct eigenvalues of g. Notice that each λ_i is non-zero since g is invertible. For each $i \in \{1, \ldots, m\}$, we let V_i be the generalized eigenspace corresponding to λ_i; the decomposition $V = V_1 \oplus \cdots \oplus V_m$ corresponds to the lines in the above matrix for g. Let

$$g_s \coloneqq \left(\begin{array}{ccccc|c|ccccc} \lambda_1 & & & & & & & & & & \\ & \lambda_1 & & & & & & & & & \\ & & \ddots & & & & & & & & \\ & & & \lambda_1 & & & & & & & \\ \hline & & & & & & \ddots & & & & \\ \hline & & & & & & & \lambda_m & & & \\ & & & & & & & & \lambda_m & & \\ & & & & & & & & & \ddots & \\ & & & & & & & & & & \lambda_m \end{array}\right),$$

and let $g_u \coloneqq g_s^{-1} g = g g_s^{-1}$. Then g_s and g_u satisfy the requirements (a)–(c).

We now show uniqueness. So assume that $g = h_s h_u = h_u h_s$, where h_s is semisimple and h_u is unipotent. Let v be an arbitrary eigenvector for h_s,

with eigenvalue λ. Then

$$\begin{aligned}(g-\lambda)^N(v) = (h_u h_s - \lambda)^N(v) &= (h_u h_s - \lambda)^{N-1}(h_u - 1)\lambda v \\ &= \lambda(h_u - 1)(h_u h_s - \lambda)^{N-1}(v) = \cdots = \lambda^N (h_u - 1)^N(v);\end{aligned}$$

since h_u is unipotent, it follows that $(g-\lambda)^N(v) = 0$ for large enough N. Hence $v \in V_i$ for some i, and in particular $\lambda = \lambda_i$. It follows that the decomposition of V into eigenspaces for the semisimple element h_s coincides with the decomposition $V = V_1 \oplus \cdots \oplus V_m$, with the same eigenvalues, and hence $h_s = g_s$. This implies $h_u = g_u$, showing that the Jordan decomposition of g is unique.

We finally show that g_s and g_u can be expressed as polynomials in g. Let $n_i \coloneqq \dim V_i$. We apply the Chinese Remainder Theorem in $k[x]$ to get a polynomial $P(x)$ such that

$$\begin{aligned}P(x) &\equiv \lambda_i \mod (x-\lambda_i)^{n_i} \quad \text{for all } i \in \{1,\dots,m\}; \\ P(x) &\equiv 0 \mod x.\end{aligned}$$

Then for each $i \in \{1,\dots,m\}$, we have $P(g)(v) = \lambda_i v$ for all $v \in V_i$, and hence $P(g)$ coincides with g_s. The condition $P(x) \equiv 0 \mod x$ ensures that $P(g)$ is a polynomial in g without constant term. Finally, observe that g_s^{-1} is a polynomial in g_s (consider its minimal polynomial), and hence $g_u = g g_s^{-1}$ is also a polynomial in g without constant term. □

Remark 6.1.3. The theorem does not hold when k is not perfect. For instance, let k be a field with $\operatorname{char}(k) = 2$ such that there is some $a \in k \setminus k^2$. Then

$$M = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{pmatrix} \begin{pmatrix} 0 & 1/\sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix},$$

so if M would have a Jordan decomposition over k, then it would have at least two different Jordan decompositions over the algebraic closure $\overline{k}$, contradicting the uniqueness.

Jordan decompositions behave well with respect to linear transformations.

Corollary 6.1.4. (i) *Let V, W be finite-dimensional vector spaces over some perfect field k, and let $\varphi\colon V \to W$ be a linear transformation. Assume that $g \in \mathsf{GL}(V)$ and $h \in \mathsf{GL}(W)$ are such that $\varphi \circ g = h \circ \varphi$. Then*

$$\varphi \circ g_s = h_s \circ \varphi \quad \text{and} \quad \varphi \circ g_u = h_u \circ \varphi.$$

(ii) *If $U \leq V$ is a g-invariant subspace, then it is also g_s- and g_u-invariant, and we have $(g_{|U})_s = (g_s)_{|U}$ and $(g_{|U})_u = (g_u)_{|U}$.*

Proof. Statement (i) follows from the fact that φ maps generalized eigenspaces to generalized eigenspaces: if $(g-\lambda)^N(v) = 0$, then also

$$(h-\lambda)^N\big(\varphi(v)\big) = \varphi\big((g-\lambda)^N(v)\big) = 0.$$

It follows that $\varphi \circ g_s$ and $h_s \circ \varphi$ are identical on each generalized eigenspace, and hence on all of V. The same then holds for the unipotent part.

To prove (ii), consider the inclusion map $\varphi\colon U \to V$, and apply (i). $\square$

Although we are eventually interested in linear algebraic groups, which we know can be embedded in finite-dimensional matrix groups, we will have to consider the more general case of infinite-dimensional vector spaces first.

Definition 6.1.5. Let k be an arbitrary field, and let V be an arbitrary k-vector space, possibly infinite-dimensional. Let $g \in \mathrm{End}_k(V)$. Then:

(i) g is *diagonalizable* if V has a basis of eigenvectors for g;

(ii) g is *semisimple* if g is diagonalizable over $\overline{k}$;

(iii) g is *nilpotent* if for each $v \in V$, there is some positive integer N such that $g^N(v) = 0$;

(iv) g is *unipotent* if $g - 1$ is nilpotent;

(v) g is *locally finite* if for each $v \in V$, the subspace $\langle g^n(v) \mid n \in \mathbb{Z}_{\geq 0}\rangle$ is finite-dimensional.

Notice that unipotent elements and semisimple elements are locally finite.

Example 6.1.6. Let $V = k[t]$, and consider the linear transformation $D = \frac{d}{dt}$, formal derivation in the variable t. Then D is locally finite and nilpotent. On the other hand, there is no positive integer N such that $D^N = 0$.

Remark 6.1.7. Assume that $g \in \mathsf{GL}(V)$ is locally finite and let $L_v := \langle g^n(v) \mid n \in \mathbb{Z}_{\geq 0}\rangle$ for each $v \in V$. By definition, each L_v is finite-dimensional and is stabilized by g. Now observe that also g^{-1} stabilizes each subspace L_v. Indeed, $g(L_v) \leq L_v$, but since g is invertible, $g(L_v)$ and L_v have the same (finite!) dimension, hence $g(L_v) = L_v$, and applying g^{-1} on this equality gives $L_v = g^{-1}(L_v)$ as claimed.

The following proposition shows that Jordan decomposition continues to hold for locally finite automorphisms.

Proposition 6.1.8. *Let k be a perfect field, and let V be an arbitrary k-vector space, possibly infinite-dimensional. Let $g \in \mathsf{GL}(V)$ be locally finite. Then there exist unique elements $g_s, g_u \in \mathsf{GL}(V)$ such that:*

(a) g_s *is semisimple;*

(b) g_u *is unipotent;*

(c) $g = g_s g_u = g_u g_s$.

Moreover, every g-invariant subspace of V is also g_s- and g_u-invariant.

Proof. For every $v \in V$, we let

$$L_v \coloneqq \langle g^n(v) \mid n \in \mathbb{Z}_{\geq 0} \rangle.$$

Then each L_v is finite-dimensional, and $g \in \mathsf{GL}(V)$ implies that the restriction $g_{|L_v}$ belongs to $\mathsf{GL}(L_v)$ (see Remark 6.1.7). Hence we can apply Jordan decomposition to each L_v to obtain

$$g_{|L_v} = (g_{|L_v})_s \cdot (g_{|L_v})_u \,;$$

this allows us to define

$$g_s(v) \coloneqq (g_{|L_v})_s(v) \quad \text{and} \quad g_u(v) \coloneqq (g_{|L_v})_u(v)$$

for each $v \in V$. Linearity of g_s and g_u follows by restricting to the finite-dimensional g-invariant subspaces containing the relevant[1] elements of V, together with Corollary 6.1.4(ii).

It is clear that g_u is unipotent, because this is a local property. On the other hand, it is somewhat more subtle to see that g_s is semisimple; this follows from the fact that V is a direct limit of its g-invariant finite-dimensional subspaces. □

6.2 Jordan decomposition in linear algebraic groups

We now assume that G is a linear algebraic k-group. Our goal is to show that every element of $G(k)$ admits a (canonical) Jordan decomposition when k is perfect. To obtain this goal, we will first study the regular representation for G, and afterwards we will move on to the finite-dimensional representations, which we are interested in.

[1]For instance, if we want to show $g_s(v + w) = g_s(v) + g_s(w)$, then we consider the smallest g-invariant subspace containing v, w and $v + w$, which is the finite-dimensional subspace $\langle L_v, L_w, L_{v+w} \rangle$, and we apply Jordan decomposition for the restriction of g to that subspace, together with Corollary 6.1.4(ii).

Lemma 6.2.1. *Let G be a linear algebraic k-group with coordinate algebra $A = k[G]$, and consider its regular G-representation (A, Δ), with corresponding action*

$$\rho = \rho_k \colon G(k) \to \mathsf{GL}_A(k) = \mathsf{GL}(A)$$

given by equation (5.1)*. Then for every $g \in G(k)$, the automorphism $\rho(g)$ is locally finite.*

Proof. Let $v \in A$ be arbitrary. By Lemma 5.4.5, the representation (A, Δ) is locally finite in the sense of Definition 5.4.4(ii), and hence v is contained in some finite-dimensional subrepresentation $W \leq A$; this means that $\rho(g)(w) \in W$ for all $g \in G(k)$ and all $w \in W$. In particular, $\langle \rho(g)^n(v) \mid n \in \mathbb{Z}_{\geq 0} \rangle$ is contained in W, for all $g \in G(k)$. □

This allows us to transfer our earlier definitions to the context of linear algebraic groups:

Definition 6.2.2. Let G be a linear algebraic group defined over k, and consider its regular G-representation $(k[G], \Delta)$, with corresponding action $\rho \colon G(k) \to \mathsf{GL}(k[G])$. Let $g \in G(k)$.

(i) We call g semisimple if $\rho(g)$ is semisimple.

(ii) We call g unipotent if $\rho(g)$ is unipotent.

(iii) If $g = g_s g_u = g_u g_s$ with g_s semisimple and g_u unipotent, then we call the pair (g_s, g_u) the *Jordan decomposition* of g.

Remark 6.2.3. (i) If g has a Jordan decomposition, then it is necessarily unique because of Proposition 6.1.8; recall that ρ is injective because the regular representation is faithful.

(ii) Every $\rho(g)$ has a Jordan decomposition in $\mathsf{GL}(k[G])$, but it is not obvious at all that the corresponding elements $\rho(g)_s$ and $\rho(g)_u$ arise from elements of $G(k)$, i.e. whether they are contained in the image of ρ.

In order to proceed, we first need a connection between semisimple and unipotent elements of $\mathsf{GL}(V)$ on the one hand, and of $\mathsf{GL}(k[\mathsf{GL}_V])$ on the other hand. We will only sketch the proof of this result since it is rather specific and has some technical details that we will not need again.

Lemma 6.2.4. *Let V be a finite-dimensional vector space over k, and let G be the linear algebraic group $G = \mathsf{GL}_V$. Let $g \in G(k) = \mathsf{GL}(V)$. Then g is semisimple (unipotent) if and only if $\rho(g) \in \mathsf{GL}(k[G])$ is semisimple (unipotent).*

In particular, if $g \in G(k)$ has a Jordan decomposition (g_s, g_u), then $\rho(g)_s = \rho(g_s)$ and $\rho(g)_u = \rho(g_u)$.

Sketch of proof. The proof proceeds in three steps:

(1) $\rho(g)$ is semisimple (unipotent) on $k[\mathsf{GL}_V]$ if and only if $\rho(g)$ is semisimple (unipotent) on $k[\mathrm{End}(V)]$;

(2) $k[\mathrm{End}(V)] \cong k[x_{11}, \ldots, x_{nn}] \cong \mathrm{Sym}(\mathrm{End}(V)^*)$, where

$$\mathrm{Sym}(Z) \coloneqq \bigoplus_{m=0}^{\infty} Z^{\otimes m} / \langle x \otimes y - y \otimes x \mid x, y \in Z \rangle.$$

Then $\rho(g)$ is semisimple (unipotent) on $k[\mathrm{End}(V)]$ if and only if $\rho(g)$ is semisimple (unipotent) on $\mathrm{End}(V)^*$;

(3) $\rho(g)$ is semisimple (unipotent) on $\mathrm{End}(V)^*$ if and only if g is semisimple (unipotent) on V.

We refer, for instance, to [Sza12] for more details. □

We are now ready to state the Jordan decomposition for linear algebraic groups.

Theorem 6.2.5 (Jordan decomposition in linear algebraic groups)**.** *Let G be a linear algebraic group defined over some perfect field k, and let $g \in G(k)$. Then g has a unique Jordan decomposition (g_s, g_u). Moreover, for every embedding $\varphi\colon G \hookrightarrow \mathsf{GL}_n$, we have $\varphi(g_s) = \varphi(g)_s$ and $\varphi(g_u) = \varphi(g)_u$.*

Proof. Choose an arbitrary embedding $\varphi\colon G \hookrightarrow \mathsf{GL}_V$ with $\dim_k V < \infty$, and let $A = k[\mathsf{GL}_V]$. Consider the corresponding dual morphism

$$\varphi^*\colon A \to k[G];$$

by Corollary 5.3.3, φ^* is surjective. Let $I = \ker \varphi^*$. Notice that an element $h \in \mathsf{GL}_V(k) \simeq \hom_{k\text{-}\mathbf{alg}}(A, k)$ belongs to $G(k)$ if and only if $h(I) = 0$. (Indeed, $G(k) \simeq \hom_{k\text{-}\mathbf{alg}}(A/I, k)$, and hence the embedding $\varphi_k\colon G(k) \hookrightarrow \mathsf{GL}_V(k)$ is given explicitly by

$$\varphi_k\colon \hom_{k\text{-}\mathbf{alg}}(A/I, k) \to \hom_{k\text{-}\mathbf{alg}}(A, k)\colon f \mapsto f \circ \varphi^*.)$$

Next, we claim that for each $h \in \mathsf{GL}_V(k)$, we have

$$h = \epsilon \circ \rho(h), \tag{6.1}$$

where $\rho = \rho_k\colon \mathsf{GL}_V(k) \to \mathsf{GL}(A)$ is the regular representation of GL_V on the k-points given by equation (5.1) applied to the comodule (A, Δ), and where

$\epsilon\colon A \to k$ is the counit of the Hopf algebra A. Indeed,

$$\begin{aligned}\epsilon \circ \rho(h) &= \epsilon \circ \mathbf{m} \circ (h \otimes \mathrm{id}_A) \circ \Delta \\ &= \mathbf{m} \circ (\mathrm{id}_k \otimes \epsilon) \circ (h \otimes \mathrm{id}_A) \circ \Delta \\ &= \mathbf{m} \circ (h \otimes \mathrm{id}_k) \circ (\mathrm{id}_A \otimes \epsilon) \circ \Delta \\ &= h \circ \mathbf{m} \circ (\mathrm{id}_A \otimes \epsilon) \circ \Delta \\ &= h.\end{aligned}$$

We now claim that

$$h(I) = 0 \iff \rho(h)(I) \subseteq I. \tag{6.2}$$

It is clear from (6.1) that if $\rho(h)(I) \subseteq I$, then $h(I) = \epsilon(\rho(h)(I)) \subseteq \epsilon(I) = 0$ because I is a Hopf ideal. Conversely, if $h(I) = 0$, i.e., if $h \in G(k)$, then the regular representations of GL_V and of G are compatible for h, i.e. the following diagram commutes:

$$\begin{array}{ccccccc}
\rho(\varphi(h))\colon A & \xrightarrow{\Delta} & A \otimes A & \xrightarrow{\varphi(h) \otimes \mathrm{id}_A} & k \otimes A & \xrightarrow{\cong} & A \\
\downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^* \otimes \varphi^*} & & \downarrow{\scriptstyle \mathrm{id} \otimes \varphi^*} & & \downarrow{\scriptstyle \varphi^*} \\
\rho(h)\colon A/I & \xrightarrow{\Delta_G} & A/I \otimes A/I & \xrightarrow{h \otimes \mathrm{id}_{A/I}} & k \otimes A/I & \xrightarrow{\cong} & A/I
\end{array} \tag{6.3}$$

Therefore, $\rho(h)(I) \subseteq I$. (Alternatively, this can be deduced from the fact that $\Delta(I) \subseteq A \otimes I + I \otimes A$.) This proves the claim (6.2).

Notice that the commutative diagram (6.3) also shows that an element $g \in G(k)$ is semisimple or unipotent if and only if this holds for the corresponding element $\varphi(g) \in \mathsf{GL}_V(k)$.

Each element $g \in \mathsf{GL}_V(k)$ has a Jordan decomposition (g_s, g_u), so we only have to show that $g \in G(k)$ implies $g_s, g_u \in G(k)$ as well, or equivalently, that

$$g(I) = 0 \implies g_s(I) = g_u(I) = 0. \tag{6.4}$$

By Lemma 6.2.4, we have

$$\rho(g)_s = \rho(g_s) \quad \text{and} \quad \rho(g)_u = \rho(g_u).$$

If $g(I) = 0$, then by (6.2), the subspace I of A is $\rho(g)$-invariant. Because every $\rho(g)$-invariant subspace is also $\rho(g)_s$- and $\rho(g)_u$-invariant (Corollary 6.1.4(ii)), it follows that $\rho(g_s)(I) \subseteq I$ and $\rho(g_u)(I) \subseteq I$. Again invoking (6.2), we

conclude that $g_s(I) = g_u(I) = 0$ as claimed. Moreover, it follows from the uniqueness of the Jordan decomposition that

$$\varphi(g_s) = \varphi(g)_s \quad \text{and} \quad \varphi(g_u) = \varphi(g)_u$$

for each embedding $\varphi\colon G \hookrightarrow \mathsf{GL}_V$. □

The following important result is surprisingly delicate (although it is an immediate corollary of Theorem 6.2.5 when φ is injective), so we omit its proof.

Proposition 6.2.6. *If $\varphi\colon G \to H$ is a morphism of linear algebraic groups, then φ maps semisimple elements to semisimple elements and unipotent elements to unipotent elements. In particular, φ preserves the Jordan decomposition of elements.*

Proof omitted. □

We end this chapter by mentioning an important consequence of the Jordan decomposition for commutative linear algebraic groups.

Definition 6.2.7. Let G be a linear algebraic group defined over some algebraically closed field k. Then we define

$$G_s \coloneqq \{g \in G(k) \mid g \text{ is semisimple}\};$$
$$G_u \coloneqq \{g \in G(k) \mid g \text{ is unipotent}\}.$$

Observe that G_u is always a closed subset of G, since after embedding it into some GL_n, it is determined by the polynomial equation $(g-1)^n = 0$. On the other hand, the set G_s is *not* a closed subset in general. For commutative groups however, the situation is much nicer.

Theorem 6.2.8. *Let G be a commutative linear algebraic group defined over some algebraically closed field k. Then both G_s and G_u are closed subgroups of G, and the product map*

$$G_s \times G_u \to G$$

is an isomorphism.

Proof omitted. □

Chapter 7 Lie algebras and linear algebraic groups

In this chapter, we will see how we can associate a Lie algebra to every linear algebraic group; this algebra will arise as the tangent space of the corresponding algebraic variety, equipped with additional structure arising from the group structure of the linear algebraic group. We will soon see that our general point of view, describing a linear algebraic group G as a functor from k-**alg** to **Grp**, is also very convenient for this purpose: we will be using the $k[\varepsilon]$-points of G, where $k[\varepsilon]$ is the ring of dual numbers defined as $k + k\varepsilon$ with $\varepsilon^2 = 0$.

The Lie algebra is a smaller object than the Hopf algebra, and frequently is easier to analyze, but it can give substantial information about G, especially in characteristic zero.

At the end of this chapter, we will use the Lie algebra to introduce a very important canonical representation for G, the so-called adjoint representation. This representation will be crucial in Chapter 11 when we study reductive groups.

7.1 Lie algebras

We begin by recalling what a Lie algebra is.

Definition 7.1.1. Let k be a commutative field. A *Lie algebra* over k is a k-vector space $\mathfrak{g}$, together with a map

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

such that:

(a) $[\cdot,\cdot]$ is k-bilinear;

(b) $[x, x] = 0$ for all $x \in \mathfrak{g}$;

(c) the Jacobi identity

$$\big[x,[y,z]\big] + \big[y,[z,x]\big] + \big[z,[x,y]\big] = 0$$

holds for all $x, y, z \in \mathfrak{g}$.

The map $[\cdot,\cdot]$ is called the *Lie bracket* of $\mathfrak{g}$.

Observe that by property (b), the Lie bracket is skew symmetric, i.e. for all $x, y \in \mathfrak{g}$, we have $[x,y] = -[y,x]$.

Definition 7.1.2. Let $\mathfrak{g}, \mathfrak{g}'$ be Lie algebras.

(i) A *Lie algebra morphism* from $\mathfrak{g}$ to $\mathfrak{g}'$ is a k-linear map $\alpha\colon \mathfrak{g} \to \mathfrak{g}'$ preserving the Lie bracket, i.e. such that $\alpha([x,y]) = [\alpha(x), \alpha(y)]$ for all $x, y \in \mathfrak{g}$.

(ii) A *Lie subalgebra* of $\mathfrak{g}$ is a k-subspace $\mathfrak{h} \leq \mathfrak{g}$ such that $[x,y] \in \mathfrak{h}$ for all $x, y \in \mathfrak{h}$, i.e. such that $[\mathfrak{h}, \mathfrak{h}] \subseteq \mathfrak{h}$.

(iii) An *ideal* of $\mathfrak{g}$ is a k-subspace $\mathfrak{i} \leq \mathfrak{g}$ such that $[\mathfrak{g}, \mathfrak{i}] \subseteq \mathfrak{i}$. It is called a *proper ideal* if it is not equal to $\mathfrak{g}$ itself.

(iv) The *dimension* of $\mathfrak{g}$ is simply defined to be the dimension of the underlying vector space.

Definition 7.1.3. Let A be an associative but not necessarily commutative k-algebra. Then we can associate a Lie algebra $\mathfrak{a}$ to A, by declaring $\mathfrak{a} = A$ as a k-vector space, and $[x,y] = xy - yx$ for all $x, y \in A$. We will denote $\mathfrak{a}$ by $\mathrm{Lie}(A)$. It is straightforward to check that $[x,x] = 0$ for all $x \in A$ and that the Jacobi identity holds.

Example 7.1.4. Let $A = \mathrm{End}_k(V)$ be the k-algebra of k-linear endomorphisms of a vector space V. Then we denote the corresponding Lie algebra $\mathrm{Lie}(A)$ by $\mathfrak{gl}_V$. In particular, if $\dim_k V = n < \infty$, then $A \cong \mathrm{Mat}_n(k)$, and the corresponding Lie algebra will be denoted by $\mathfrak{gl}_n$. If we denote by $E_{ij} \in \mathrm{Mat}_n(k)$ the matrix with a 1 on the (i,j)-th position, and a 0 everywhere else, then the Lie bracket satisfies the rule

$$[E_{ij}, E_{pq}] = \delta_{pj} E_{iq} - \delta_{iq} E_{pj}$$

for all i, j, p, q.

We will need one more construction of Lie algebras, namely the Lie algebra of derivations of a k-algebra.

Definition 7.1.5. Let A be a not necessarily commutative nor associative k-algebra.

(i) A *k-derivation* (or simply *derivation*) on A is a k-linear map $D\colon A \to A$ such that the *Leibniz rule*

$$D(a \cdot b) = D(a) \cdot b + a \cdot D(b)$$

holds, for all $a, b \in A$.

(ii) We denote the set of all k-derivations on A by $\mathrm{Der}_k(A)$ or by $\mathrm{Der}(A)$. Notice that $\mathrm{Der}(A)$ is a k-subspace of $\mathrm{End}_k(A)$; as we will see in Proposition 7.1.6 below, $\mathrm{Der}(A)$ is in fact a Lie subalgebra of $\mathfrak{gl}_A$.

Notice that the composition of two derivations is not necessarily a derivation again; we have

$$(D_1 \circ D_2)(a \cdot b) = (D_1 \circ D_2)(a) \cdot b + a \cdot (D_1 \circ D_2)(b) + D_1(a)D_2(b) + D_2(a)D_1(b) \quad (7.1)$$

for all $D_1, D_2 \in \mathrm{Der}(A)$ and all $a, b \in A$. However:

Proposition 7.1.6. *Let A be a not necessarily commutative nor associative k-algebra. Then $\mathrm{Der}(A)$ is a Lie subalgebra of $\mathfrak{gl}_A$.*

Proof. It follows immediately from equation (7.1) that for all $D_1, D_2 \in \mathrm{Der}(A)$, the map $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$ satisfies the Leibniz rule, and hence belongs to $\mathrm{Der}(A)$ again. □

When A is itself a Lie algebra $\mathfrak{g}$, an important class of derivations are the so-called inner derivations:

Definition 7.1.7. Let $\mathfrak{g}$ be a Lie algebra. Then for each $x \in \mathfrak{g}$, we define

$$\mathrm{ad}_{\mathfrak{g}} x \colon \mathfrak{g} \to \mathfrak{g} \colon y \mapsto [x, y]$$

for all $y \in \mathfrak{g}$; we call this the *inner derivation* induced by x, or the *adjoint linear map* of x.

Proposition 7.1.8. *Let $\mathfrak{g}$ be a Lie algebra. Then:*

(i) *For each $x \in \mathfrak{g}$, the inner derivation $\mathrm{ad}_{\mathfrak{g}} x$ is a derivation of $\mathfrak{g}$, where we consider $\mathfrak{g}$ as a k-algebra with multiplication given by the Lie bracket.*

(ii) *Let $\mathrm{ad}(\mathfrak{g}) \coloneqq \{\mathrm{ad}_{\mathfrak{g}} x \mid x \in \mathfrak{g}\}$. Then $\mathrm{ad}(\mathfrak{g})$ is an ideal of the Lie algebra $\mathrm{Der}(\mathfrak{g})$.*

(iii) *The map*

$$\mathrm{ad}_{\mathfrak{g}} \colon \mathfrak{g} \to \mathrm{Der}(\mathfrak{g}) \colon x \mapsto \mathrm{ad}_{\mathfrak{g}} x$$

is a Lie algebra homomorphism.

Proof. (i) We have to check that for all $x, y, z \in \mathfrak{g}$, the identity

$$\mathrm{ad}_{\mathfrak{g}} x\big([y, z]\big) = \big[\mathrm{ad}_{\mathfrak{g}} x(y), z\big] + \big[y, \mathrm{ad}_{\mathfrak{g}} x(z)\big]$$

holds. This identity is equivalent to the Jacobi identity.

(ii) This follows from the fact that

$$[\mathrm{ad}_{\mathfrak{g}} x, D] = \mathrm{ad}_{\mathfrak{g}}(-Dx)$$

for all $D \in \mathrm{Der}(\mathfrak{g})$ and all $x \in \mathfrak{g}$.

(iii) It follows from the Jacobi identity again that

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

for all $x, y, z \in \mathfrak{g}$. □

Definition 7.1.9. Let $\mathfrak{g}$ be a Lie algebra. The kernel of the map $\mathrm{ad}_{\mathfrak{g}}$ is called the *center* of $\mathfrak{g}$ and denoted by $Z(\mathfrak{g})$; observe that

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

7.2 The Lie algebra of a linear algebraic group

We will now explain how we can associate a Lie algebra to a linear algebraic group G. We will first define the underlying vector space, and afterwards we will make clear how to define the Lie bracket.

Definition 7.2.1. Let R be a commutative ring with 1. Then we define[1] the *ring of dual numbers over* R to be

$$R[\varepsilon] \coloneqq R[x]/(x^2) = R \oplus \varepsilon R$$

with $\varepsilon^2 = 0$. We will denote the canonical projection on the first component by π, i.e.

$$\pi \colon R[\varepsilon] \to R \colon a + \varepsilon b \mapsto a;$$

note that π is a ring homomorphism.

Notice that an element $a + \varepsilon b \in R[\varepsilon]$ is invertible if and only if a is invertible in R; in this case, the inverse is given by

$$(a + \varepsilon b)^{-1} = a^{-1} - \varepsilon a^{-2} b.$$

[1]Note the subtle difference in notation: we use ε for the dual numbers and ϵ for the counit of the Hopf algebra. This should not cause too much confusion, since the former is a ring element whereas the latter is a ring morphism.

Definition 7.2.2. Let G be a linear algebraic k-group. For each $R \in k$-**alg**, we define

$$\mathrm{Lie}_R(G) \coloneqq \ker\Big(G\big(R[\varepsilon]\big) \xrightarrow{G(\pi)} G(R)\Big).$$

The *Lie algebra of* G is now defined as

$$\mathrm{Lie}(G) \coloneqq \mathrm{Lie}_k(G) = \ker\Big(G\big(k[\varepsilon]\big) \xrightarrow{G(\pi)} G(k)\Big).$$

Notice that this definition only gives $\mathrm{Lie}(G)$ the structure of a group; it is not obvious that $\mathrm{Lie}(G)$ can be made into a k-vector space (it is not even obvious that it is an abelian group).

We will first have a look at the mother of all linear algebraic groups, GL_n.

Example 7.2.3. Consider the linear algebraic group $G = \mathsf{GL}_n$. Then[2]

$$G\big(k[\varepsilon]\big) = \{A + \varepsilon B \mid A \in \mathsf{GL}_n(k), B \in \mathrm{Mat}_n(k)\};$$

the inverse of an element $A + \varepsilon B \in G\big(k[\varepsilon]\big)$ is given by

$$(A + \varepsilon B)^{-1} = A^{-1} - \varepsilon A^{-1} B A^{-1}.$$

Hence

$$\mathrm{Lie}(G) = \{I_n + \varepsilon B \mid B \in \mathrm{Mat}_n(k)\},$$

and the map

$$E\colon\ \mathrm{Mat}_n(k) \to \mathrm{Lie}(G)\colon B \mapsto I_n + \varepsilon B$$

is a bijection; notice that $E(A)E(B) = E(A+B)$. In particular, we see that $\mathrm{Lie}(G)$ is indeed an abelian group. Observe that this law tells us that the map E behaves, in some sense, as an exponential map.

It is now clear that it makes sense to make $\mathrm{Lie}(\mathsf{GL}_n)$ into a Lie algebra, since $\mathrm{Mat}_n(k)$ has a natural Lie algebra structure, namely the Lie algebra $\mathfrak{gl}_n$ introduced in Example 7.1.4.

Since every linear algebraic group can be embedded into some GL_n, we can use this primary example to define the Lie algebra structure on $\mathrm{Lie}(G)$ for any linear algebraic group G.

[2]Recall that for each $R \in k$-**alg**, the set of R-points $G(R)$ is given as the set of solutions of the polynomial equation $d \cdot \det(t_{ij}) - 1 = 0$ in R^{n^2+1}. When $R = k[\varepsilon]$, write each t_{ij} as $a_{ij} + \varepsilon b_{ij}$ and $d = r + \varepsilon s$, and expand to get the above description for $G(k[\varepsilon])$. Alternatively, simply express that a matrix $A + \varepsilon B \in \mathrm{Mat}_n(R)$ is invertible.

Definition 7.2.4. Let G be a linear algebraic k-group, and let $\mathrm{Lie}(G)$ be as in Definition 7.2.2. Choose an arbitrary embedding $G \hookrightarrow \mathsf{GL}_n$, and notice that this induces an embedding of $\mathrm{Lie}(G)$ as a subgroup of $\mathrm{Lie}(\mathsf{GL}_n) = \mathfrak{gl}_n$. It turns out that $\mathrm{Lie}(G)$ is, in fact, a Lie subalgebra of $\mathrm{Lie}(\mathsf{GL}_n) = \mathfrak{gl}_n$, and that the Lie algebra $\mathrm{Lie}(G)$ is independent (up to isomorphism) of the chosen embedding $G \hookrightarrow \mathsf{GL}_n$.

It is a natural question whether it is possible to give a more intrinsic definition of the Lie algebra $\mathrm{Lie}(G)$, which does not depend on an embedding $G \hookrightarrow \mathsf{GL}_n$. This is indeed possible. We state the result without proof.

Definition 7.2.5. Let G be a linear algebraic group defined over k, and let $A = k[G]$ be its coordinate algebra. Then a k-derivation $D \in \mathrm{Der}_k(A)$ is called *left-invariant* if

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

We will denote the space of left-invariant k-derivations on A by $\mathrm{Der}_k^\ell(A)$.

The space of left-invariant k-derivations is a Lie subalgebra of $\mathrm{Der}_k(A)$:

Lemma 7.2.6. *Let G be a linear algebraic group defined over k, and let $A = k[G]$ be its coordinate algebra. Then $\mathrm{Der}_k^\ell(A)$ is a Lie subalgebra of $\mathrm{Der}_k(A)$.*

Proof. We have to check that when $D_1, D_2 \in \mathrm{Der}_k(A)$ are left-invariant, then so is $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$. This is an easy exercise. □

Theorem 7.2.7. *Let G be a linear algebraic group defined over k, and let $A = k[G]$ be its coordinate algebra. Then*

$$\mathrm{Lie}(G) \simeq \mathrm{Der}_k^\ell(A)$$

as Lie algebras.

Proof omitted. □

We will now give some more examples; we leave some of the details to the reader.

Example 7.2.8. (1) Let $G = \mathsf{SL}_n$. Then

$$\mathrm{Lie}(G) = \{I_n + \varepsilon A \in \mathrm{Mat}_n(k[\varepsilon]) \mid \det(I_n + \varepsilon A) = 1\}.$$

Since $\varepsilon^2 = 0$, we have $\det(I_n + \varepsilon A) = 1 + \varepsilon \operatorname{tr}(A)$, and hence

$$\begin{aligned}\mathrm{Lie}(\mathsf{SL}_n) &= \{I_n + \varepsilon A \mid A \in \mathrm{Mat}_n(k), \operatorname{tr}(A) = 0\} \\ &= \{E(A) \mid A \in \mathrm{Mat}_n(k), \operatorname{tr}(A) = 0\}.\end{aligned}$$

We observe that $\mathrm{Lie}(\mathsf{SL}_n)$ is indeed a Lie subalgebra of $\mathfrak{gl}_n$, which we denote by $\mathfrak{sl}_n$. In fact, we even have that the Lie bracket of any two elements of $\mathfrak{gl}_n$ belongs to $\mathfrak{sl}_n$, since for all $A, B \in \mathrm{Mat}_n(k)$, we have $\mathrm{tr}(AB - BA) = 0$.

(2) Let $G = \mathbb{T}_n$ be the linear algebraic group of invertible upper triangular matrices. Then $\mathrm{Lie}(G)$ is isomorphic to the Lie subalgebra of (all) upper triangular matrices

$$\mathrm{Lie}(\mathbb{T}_n) = \{E(A) \mid A \in \mathrm{Mat}_n(k), A_{ij} = 0 \text{ for all } i > j\}.$$

(3) Let $G = \mathbb{U}_n$ be the linear algebraic group of upper triangular matrices with 1's on the diagonal. Then $\mathrm{Lie}(G)$ is isomorphic to the Lie subalgebra

$$\mathrm{Lie}(\mathbb{U}_n) = \{E(A) \mid A \in \mathrm{Mat}_n(k), A_{ij} = 0 \text{ for all } i \geq j\}.$$

(4) Let $G = \mathbb{D}_n$ be the linear algebraic group of invertible diagonal matrices. Then $\mathrm{Lie}(G)$ is isomorphic to the Lie subalgebra of (all) diagonal matrices

$$\mathrm{Lie}(\mathbb{D}_n) = \{E(A) \mid A \in \mathrm{Mat}_n(k), A_{ij} = 0 \text{ for all } i \neq j\}.$$

Remark 7.2.9. (i) A morphism of linear algebraic groups $\alpha\colon G \to H$ induces a morphism of Lie algebras $\mathrm{Lie}(\alpha)\colon \mathrm{Lie}(G) \to \mathrm{Lie}(H)$, which is injective if the morphism $G \to H$ is a closed embedding, i.e. if α is injective and $\alpha(G)$ is a closed subgroup of H.
The fact that we have a morphism of abelian groups from $\mathrm{Lie}(G)$ to $\mathrm{Lie}(H)$ follows immediately from the definitions, and more precisely from the commutative diagram

$$\begin{array}{ccc} G\big(k[\varepsilon]\big) & \xrightarrow{G(\pi)} & G(k) \\ \Big\downarrow{\scriptstyle \alpha_{k[\varepsilon]}} & & \Big\downarrow{\scriptstyle \alpha_k} \\ H\big(k[\varepsilon]\big) & \xrightarrow{H(\pi)} & H(k) \end{array}$$

but it requires more effort to show that this morphism $\mathrm{Lie}(\alpha)$ preserves the Lie brackets.

(ii) The Lie algebra construction is functorial. More precisely, the construction described in (i) is the unique way of making $\mathrm{Lie}\colon G \mapsto \mathrm{Lie}(G)$ into a functor (from linear algebraic k-groups to Lie k-algebras) such that $\mathrm{Lie}(\mathsf{GL}_n) = \mathfrak{gl}_n$.

One important feature of the Lie algebra of an algebraic group is that it provides a natural representation, known as the adjoint representation. To define it, recall that

$$\pi\colon R[\varepsilon] \to R\colon a + \varepsilon b \mapsto a,$$

and define

$$\iota\colon R \to R[\varepsilon]\colon a \mapsto a + \varepsilon 0;$$

then $\pi \circ \iota = \mathrm{id}_R$. These maps give rise to homomorphisms

$$G(R) \xrightarrow{\iota} G(R[\varepsilon]) \xrightarrow{\pi} G(R), \quad \pi \circ \iota = \mathrm{id}_{G(R)},$$

where we have written π and ι instead of $G(\pi)$ and $G(\iota)$ to simplify the notation. Recall that

$$\mathfrak{g}(R) = \ker\Big(G\big(R[\varepsilon]\big) \xrightarrow{\pi} G(R)\Big).$$

It is a not completely trivial fact that

$$\mathfrak{g}(R) \cong \mathfrak{g}(k) \otimes_k R;$$

this follows most easily from the description of $\mathfrak{g}(R)$ in terms of derivations, but we will omit the details. Now define

$$\mathrm{Ad}_R\colon G(R) \to \mathrm{Aut}(\mathfrak{g}(R))\colon g \mapsto \mathrm{Ad}_R(g),$$

where

$$\mathrm{Ad}_R(g)\colon \mathfrak{g}(R) \to \mathfrak{g}(R)\colon x \mapsto \iota(g) \cdot x \cdot \iota(g)^{-1}$$

for all $g \in G(R)$. Notice that the map $\mathrm{Ad}_R(g)$ is in fact an R-linear map, and hence Ad_R maps $G(R)$ into $\mathsf{GL}(\mathfrak{g}(R))$. Since all the constructions are natural in R, this gives rise to a natural transformation

$$\mathrm{Ad}\colon G \to \mathsf{GL}_{\mathfrak{g}}.$$

Definition 7.2.10. Let G be a linear algebraic k-group. The *adjoint representation* of G is the representation Ad defined above.

As a useful example, we compute the adjoint representation for the group $G = \mathsf{GL}_n$.

Example 7.2.11. Let k be a field and let $G = \mathsf{GL}_n$ over k with Lie algebra $\mathfrak{g} = \mathfrak{gl}_n(k)$. Let $\mathrm{Ad}\colon G \to \mathsf{GL}_{\mathfrak{g}}$ be the adjoint representation of G. Then the adjoint action of $G = \mathsf{GL}_n$ on $\mathfrak{g}$ is given by conjugation: $\mathrm{Ad}(A)(X) = AXA^{-1}$ for all $A \in \mathsf{GL}_n(R)$ and all $X \in \mathfrak{g}(R)$.

Indeed, the elements of $\mathfrak{g}(R)$ are of the form $I + \varepsilon X$ for $X \in \mathrm{Mat}_n(R)$, and by definition, the adjoint action of an element $A \in \mathsf{GL}_n(R)$ is given by

$$I + \varepsilon X \mapsto \iota(A) \cdot (I + \varepsilon X) \cdot \iota(A)^{-1} = I + \varepsilon AXA^{-1}.$$

The adjoint representation can be used to give another (but equivalent) definition of the Lie bracket on $\mathfrak{g} = \mathrm{Lie}(G)$:

Theorem 7.2.12. *Let G be a linear algebraic k-group, with Lie algebra $\mathfrak{g}$, and with adjoint representation* $\mathrm{Ad}\colon G \to \mathsf{GL}_{\mathfrak{g}}$. *Let* ad *be the adjoint map of the Lie algebra $\mathfrak{g}$ as in Definition* 7.1.7. *Then* $\mathrm{Lie}(\mathrm{Ad}) = \mathrm{ad}$.

Proof. By Definition 7.2.4, it suffices to show this for $G = \mathsf{GL}_n$. The Lie algebra $\mathfrak{g} = \mathfrak{gl}_n$ comes equipped with the adjoint map

$$\mathrm{ad}\colon \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}\colon A \mapsto \mathrm{ad}(A),$$

where $\mathrm{ad}(A)$ acts on $\mathfrak{g}$ as $X \mapsto [A, X] = AX - XA$.

On the other hand, if we apply the functor Lie to the homomorphism Ad, we obtain a linear map

$$\mathrm{Lie}(\mathrm{Ad})\colon \mathrm{Lie}(G) \to \mathrm{Lie}(\mathsf{GL}_{\mathfrak{g}}) \cong \mathfrak{gl}_{\mathfrak{g}}.$$

We already know from Example 7.2.11 that $A \in \mathsf{GL}_n(R)$ acts on $\mathrm{Mat}_n(R)$ by mapping each X to AXA^{-1}, so when we apply the Lie functor, we obtain that an element $I + \varepsilon A \in \mathrm{Lie}(\mathsf{GL}_n(R))$ acts on $\mathrm{Mat}_n(R[\varepsilon])$ by mapping each $X + \varepsilon Y$ to

$$(I + \varepsilon A)(X + \varepsilon Y)(I + \varepsilon A)^{-1} = X + \varepsilon Y + \varepsilon(AX - XA).$$

In other words, $\mathrm{Lie}(\mathrm{Ad})(A)$ acts as $\mathrm{id} + \epsilon\,\mathrm{ad}(A)$, as required. □

Remark 7.2.13. The adjoint representation is *not* faithful in general. Notice, for instance, that $Z(G)$ is always contained in the kernel of Ad. In fact, when $\mathrm{char}(k) = 0$ and G is connected, then $Z(G) = \ker(\mathrm{Ad})$, but in general, this is not true. (If G is connected, then the quotient $\ker(\mathrm{Ad})/Z(G)$ is always a unipotent group.)

Chapter 8 Topological aspects

We will briefly study some of the topological aspects of linear algebraic groups, and in particular we will study connectedness. This crucial property will have a nice interpretation in terms of the Hopf algebra coordinatizing the linear algebraic group. At the end of this chapter, we will also say a few words about smoothness and the dimension of linear algebraic groups.

8.1 Connected components of matrix groups

Before we study connectedness for linear algebraic groups in general, it is enlightening to have a look at the "classical" case of closed[1] subgroups of $\mathsf{GL}_n(k)$, where k is an algebraically closed field. Recall from Corollary 4.1.16 that every affine variety is a finite union of its irreducible components (and in particular it is also a finite union of its connected components, each of which is a union of irreducible components).

Theorem 8.1.1. *Let k be an algebraically closed field, let G be a closed subgroup of $\mathsf{GL}_n(k)$, and let G° be the connected component containing the unit $1 \in G$. Then G° is a normal subgroup of finite index in G. The irreducible components of G coincide with the connected components; they are precisely the cosets of G° in G, so in particular there are precisely $[G : G^\circ]$ components.*

Proof. Let $G = V_1 \cup \cdots \cup V_r$ be the decomposition of G into its irreducible components. Then V_1 is not contained in any V_j $(2 \leq j \leq r)$, and since V_1 is irreducible, it is not contained in their union $V_2 \cup \cdots \cup V_r$ either; hence there is some $x \in V_1$ not contained in any other irreducible component. Since G is a group, every left translation $G \to G \colon y \mapsto gy$ (where $g \in G$ is fixed) is a homeomorphism, and hence every element of G is contained in exactly one irreducible component. It follows that the irreducible components are disjoint, and hence they coincide with the connected components.

[1] Of course, we are considering $\mathsf{GL}_n(k)$ as an affine variety over k endowed with the Zariski topology, as in Chapter 4.

If $x \in G^\circ$, then the set xG° is homeomorphic to G° and hence a component; since it contains $x \in G^\circ$, this implies that $xG^\circ = G^\circ$, and therefore G° is closed under multiplication. For similar reasons G° is closed under inverses and is invariant under conjugation by any $g \in G$. Finally, since we have already observed that each coset xG° is an irreducible component, we have precisely $[G : G^\circ]$ such components. □

8.2 The spectrum of a ring

Our next goal is to study connectedness for our more general notion of linear algebraic groups as k-group functors. Such an object G is completely determined by its coordinate algebra $k[G]$, and we would like to see how we can detect connectedness in terms of this Hopf algebra.

But what does connectedness even mean for a k-functor? When k is algebraically closed, it makes sense to consider the group of k-points $G(k)$, and algebraically the k-points are in one-to-one correspondence with the maximal ideals (see Corollary 4.1.11). This is no longer true for general fields k, and the collection of maximal ideals does not capture enough information in general, certainly not when we consider the group of R-points $G(R)$ for some k-algebra R.

It turns out that considering all prime ideals instead is more satisfying, and that is what we will do.

Definition 8.2.1. Let A be a commutative ring with 1. Then the *spectrum* of A is defined as the collection of its prime ideals

$$\operatorname{Spec} A \coloneqq \{I \trianglelefteq A \mid I \text{ is prime}\}.$$

We make $\operatorname{Spec} A$ into a topological space by declaring a subset of $\operatorname{Spec} A$ to be *closed* if it has the form

$$V(I) \coloneqq \{P \in \operatorname{Spec} A \mid P \supseteq I\}$$

for some ideal $I \trianglelefteq A$. This topology[2] is called the *Zariski topology* on $\operatorname{Spec} A$.

To see the connection with the classical geometric objects, assume that $A = k[V]$ for some affine variety $V \subseteq k^n$ over an algebraically closed field k. Then every point of V corresponds to a maximal ideal of A and hence to an element of $\operatorname{Spec} A$; this embedding $V \hookrightarrow \operatorname{Spec} A$ induces a homeomorphism

[2]It is not hard to check that $V(I) \cup V(J) = V(IJ)$ and $\bigcap V(I_\alpha) = V\big(\sum I_\alpha\big)$, so this does indeed define a topology.

from V onto its image. Moreover, the image is dense: if a closed set $V(I)$ contains V, then I is contained in the intersection of all maximal ideals, and since A is noetherian, this intersection coincides with the intersection of all prime ideals (see also the proof of Corollary 8.2.5(iii) below); this implies that indeed $V(I) = \operatorname{Spec} A$. Recall that a topological space is irreducible if and only if every non-empty open set is dense; it follows that V is irreducible if and only if $\operatorname{Spec} A$ is irreducible. Also, if V is connected, then $\operatorname{Spec} A$ is also connected; the converse is also true, but this is less obvious (see Corollary 8.2.5 below).

It is easy to detect irreducibility of $\operatorname{Spec} A$ from the structure of A. Compare this with Lemma 4.1.15.

Lemma 8.2.2. *Let A be a commutative ring with 1, and let N be its nilradical, i.e. the set of nilpotent elements of A. Then:*

(i) *N is an ideal; it coincides with the intersection of all prime ideals of A;*

(ii) *$\operatorname{Spec} A$ is irreducible if and only if A/N is an integral domain;*

(iii) *if A is noetherian, then $\operatorname{Spec} A$ is the union of finitely many maximal irreducible closed subsets, its irreducible components.*

Proof. (i) Let $a \in A$ be nilpotent, and $P \trianglelefteq A$ be prime. Then A/P is an integral domain, hence the image of a in A/P is zero, and hence $a \in P$. Therefore every nilpotent element is contained in the intersection of all prime ideals.
Conversely, let $a \in A$ be non-nilpotent, and let $A_a = A[a^{-1}]$ be the localization of A at a. Take a maximal ideal $I \trianglelefteq A_a$; its inverse image in A is prime and does not contain a.

(ii) Assume first that $\operatorname{Spec} A = Y_1 \cup Y_2$ for some proper closed subsets Y_1 and Y_2. Then there exists an element $a \in \big(\cap_{P \in Y_1} P\big) \setminus N$, and an element $b \in \big(\cap_{P \in Y_2} P\big) \setminus N$. Then each prime ideal $P \in \operatorname{Spec} A$ contains either a or b (or both), and hence contains ab; so $ab \in N$. Since neither $a \in N$ nor $b \in N$, this shows that A/N is not an integral domain.
Conversely, if A/N contains zero divisors, then we can find $a, b \in A$ such that $ab \in N$ but neither $a \in N$ nor $b \in N$. Since $ab \in N$, we have for each prime ideal $P \trianglelefteq A$ that either $a \in P$ or $b \in P$, and it follows that

$$\operatorname{Spec} A = \{P \in \operatorname{Spec} A \mid a \in P\} \cup \{P \in \operatorname{Spec} A \mid b \in P\}$$

decomposes $\operatorname{Spec} A$ as the union of two proper closed subspaces, hence $\operatorname{Spec} A$ is reducible.

(iii) Since A is noetherian, any non-empty collection of closed sets in $\operatorname{Spec} A$ has a minimal element. We will show that all closed sets are finite unions of irreducible closed subsets. Assume not; then by our previous observation, we can take a minimal closed set Y which is not a finite union of irreducible closed subsets. Then Y is certainly reducible, say $Y = Y_1 \cup Y_2$; by minimality, Y_1 and Y_2 would be finite unions of irreducible closed subsets, but then the same would be true for Y itself, which is a contradiction. Hence we can write every closed X as a finite irredundant union $X = X_1 \cup \cdots \cup X_r$ of irreducible closed subsets, and in particular this is true for $\operatorname{Spec} A$ itself. □

We now proceed to study connectedness of $\operatorname{Spec} A$. An important role is played by the idempotents in A.

Theorem 8.2.3. *Let A be a commutative ring with 1. A closed set $V(I)$ in $\operatorname{Spec} A$ is clopen (i.e. closed and open) if and only if $V(I) = V(e)$ for some idempotent element $e \in A$. Moreover, if $V(e) = V(f)$ for some idempotents $e, f \in A$, then $e = f$.*

Proof. Assume that $e \in A$ is idempotent; then $e + (1 - e) = 1$, so $V(e)$ and $V(1 - e)$ are disjoint closed sets. On the other hand, if $P \trianglelefteq A$ is prime, then $0 = e(1 - e) \in P$ implies $e \in p$ or $1 - e \in P$, and hence $V(1 - e)$ is the complement of $V(e)$, which implies that $V(e)$ is clopen.

Assume that $V(e) = V(f)$ for some idempotents $e, f \in A$. Then

$$V(f(1 - e)) = V(f) \cup V(1 - e) = \operatorname{Spec} A,$$

hence by Lemma 8.2.2(i), the element $f(1-e)$ is nilpotent. However, $f(1-e)$ is also idempotent, and hence $f(1-e) = 0$, implying $f = ef$. Similary $e = ef$ and we conclude that $e = f$.

Assume finally that $V(I)$ is clopen, and write its complement as $V(J)$. Then $V(I + J) = V(I) \cap V(J) = \emptyset$ and hence $I + J = A$, which implies that we can write $1 = a + b$ with $a \in I$ and $b \in J$. On the other hand, $\operatorname{Spec} A = V(I) \cup V(J) = V(IJ)$, and hence ab is nilpotent, so we have $(ab)^N = 0$ for some N. Notice that a maximal ideal containing a^N and b^N would contain a and b and hence $a+b = 1$, which is a contradiction; hence we can write $1 = ua^N + vb^N$ for some $u, v \in A$. Observe that ua^N is idempotent, since

$$(ua^N)^2 = ua^N \cdot (1 - vb^N) = ua^N - uv(ab)^N = ua^N.$$

On the other hand, we have

$$V(ua^N) \supseteq V(I) \quad \text{and} \quad V(vb^N) \supseteq V(J),$$

with $V(ua^N)$ disjoint from $V(vb^N)$; we conclude that $V(I) = V(ua^N)$. □

Remark 8.2.4. Notice that if A is a ring with a non-trivial idempotent e, then A decomposes as the product

$$A \cong eA \times (1-e)A,$$

where eA and $(1-e)A$ are rings with unit e and $1-e$, respectively. Conversely, if $A \cong B \times C$ for certain non-zero rings B and C, then A has non-trivial idempotents $e = (1,0)$ and $1-e = (0,1)$.

Corollary 8.2.5. *Let A be a commutative ring with 1.*

(i) $\operatorname{Spec} A$ *is connected if and only if A has no non-trivial idempotents.*

(ii) *If A is noetherian, then it has only finitely many idempotents.*

(iii) *If k is algebraically closed, and A is a finitely generated k-algebra, then* $\operatorname{Spec} A$ *is connected if and only if its subset*

$$\operatorname{SpecMax} A \coloneqq \{I \trianglelefteq A \mid I \text{ is a maximal ideal}\}$$

is connected.

(iv) *If k is algebraically closed, and V is an affine k-variety, then V is connected if and only if* $\operatorname{Spec} k[V]$ *is connected.*

Proof. (i) This follows immediately from Theorem 8.2.3.

(ii) If A is noetherian, then by Lemma 8.2.2(iii), $\operatorname{Spec}(A)$ has only finitely many irreducible components. Since every connected component is a union of irreducible components, this implies that $\operatorname{Spec}(A)$ has only finitely many connected components, and the result now follows again from Theorem 8.2.3.

(iii) The important point here is that Hilbert's Nullstellensatz implies that A is a *Jacobson ring*, i.e., every prime ideal is the intersection of the maximal ideals containing it; in particular, the nilradical N is equal to the intersection of all maximal ideals of A. The proof of Theorem 8.2.3 can now be adapted in order to get an idempotent element in A for each clopen subset of $\operatorname{SpecMax} A$.

(iv) This follows from (iii) because $V \cong \operatorname{SpecMax} k[V]$ as topological spaces. □

8.3 Separable algebras

We now have a good definition of connectedness using the spectrum of the coordinate algebra, but there is still an important problem that remains:

the number of connected components is not always invariant under base extension, i.e. extending the scalars of a k-algebra can create new idempotent elements. For example, consider the algebraic group of third roots of unity

$$\mu_3 \colon k\text{-}\mathbf{alg} \to \mathbf{Grp} \colon R \mapsto \{r \in R \mid r^3 = 1\},$$

with coordinate algebra

$$A = k[\mu_3] \cong k[t]/(t^3 - 1).$$

When $k = \mathbb{R}$, $\operatorname{Spec} A$ has only two elements, and A has only two non-trivial idempotents, namely $e = (t^2 + t + 1)/3$ and $1 - e$; this corresponds to the factorization $t^3 - 1 = (t - 1)(t^2 + t + 1)$. When $k = \mathbb{C}$, however, $\operatorname{Spec} A$ has three elements, corresponding to the three roots of unity in $\mathbb{C}$ (and A has six non-trivial idempotents).

To resolve these issues, we will need a theory that detects these idempotents over base field extensions, and this is where separable algebras come into play.

Definition 8.3.1. Let k be a field, and let $\overline{k}$ be its algebraic closure. A commutative k-algebra A is called *separable* if it is finite-dimensional and $A \otimes_k \overline{k}$ is reduced, i.e. does not have non-trivial nilpotent elements.

There exist several equivalent definitions; we mention just a few of them below, for later use.

Theorem 8.3.2. *Let k be a field, let $\overline{k}$ be its algebraic closure, and let k_s be its separable closure. Let $A \in k$-**alg** be finite-dimensional. Then the following statements are equivalent:*

(a) *A is separable;*

(b) *$A \otimes \overline{k} \cong \overline{k} \times \cdots \times \overline{k}$;*

(c) *$A \otimes k_s \cong k_s \times \cdots \times k_s$;*

(d) *A is a product of separable extension fields of k;*

(e) *$A \otimes \overline{k}$ is reduced;*

(f) *(only when k is perfect:) A is reduced.*

Proof omitted. □

Corollary 8.3.3. (i) *Subalgebras, quotients, products and tensor products of separable algebras are again separable.*

(ii) *Let K/k be a field extension. Then A is separable over k if and only if $A \otimes_k K$ is separable over K.*

Remark 8.3.4. (i) It can be shown that the category of separable k-algebras is anti-equivalent to the category of finite sets equipped with a continuous action of the absolute Galois group $\mathrm{Gal}(k_s/k)$. This is a simple case of what is known as *Galois descent*: the classification over the separable closure k_s is easy, and the problem over arbitrary fields reduces to the study of *k-forms*, i.e. algebraic structures defined over k that become isomorphic after a base change to the separable closure k_s.

(ii) A finite linear algebraic k-group G is called *étale*[3] if $k[G]$ is separable, and by (i), this corresponds to a finite set X on which $\mathrm{Gal}(k_s/k)$ acts continuously. In that case, the comultiplication $\Delta\colon k[G] \to k[G] \otimes k[G]$ gives a map $X \times X \to X$ commuting with the Galois action, and dualizing brings this action back to a continuous action by group automorphisms. Thus finite étale linear algebraic groups over k are equivalent to finite groups equipped with a continuous action of $\mathrm{Gal}(k_s/k)$ by automorphisms. If the Galois action on the finite group X is trivial, we recover the finite constant linear algebraic groups from Example 5.1.12, with $A = k^X$.

We now go back to the situation where we have an affine k-functor with some coordinate algebra A, which is a finitely generated k-algebra. The following definition will be our essential tool to study connectedness in general.

Definition 8.3.5. Let A be a finitely generated k-algebra. Then there is a unique maximal separable subalgebra of A, which we denote by $\pi_0(A)$.

In order to see that $\pi_0(A)$ is unique, notice that if B is any separable subalgebra, then its dimension is bounded by the number of connected components of $\operatorname{Spec} A \otimes \overline{k}$, since $B \otimes \overline{k}$ is also a separable $\overline{k}$-subalgebra of $A \otimes \overline{k}$, which is spanned by idempotents; moreover, if B and C are two separable subalgebras of A, then so is the compositum BC, since it is a quotient of $B \otimes C$.

The map $A \mapsto \pi_0(A)$ behaves well with respect to various constructions:

Proposition 8.3.6. *Let A and B be two finitely generated k-algebras, and let L/k be a field extension. Then:*

(i) *If $\varphi\colon A \to B$ is an algebra morphism, then $\varphi(\pi_0(A)) \subseteq \pi_0(B)$;*

(ii) $\pi_0(A \times B) = \pi_0(A) \times \pi_0(B)$;

[3] See also Definition 8.4.5(iii) below.

(iii) $\pi_0(A \otimes_k L) \cong \pi_0(A) \otimes_k L$;

(iv) $\pi_0(A \otimes_k B) \cong \pi_0(A) \otimes_k \pi_0(B)$.

Proof. For (i), we consider the restriction $\varphi_{|\pi_0(A)} \to B$. The image of this morphism is a quotient of $\pi_0(A)$, so by Corollary 8.3.3(i), it is a separable algebra, and is thus contained in $\pi_0(B)$.

To see that (ii) holds, note that $\pi_0(A \times B) \subseteq \pi_0(A) \times \pi_0(B)$ because the projections of $\pi_0(A \times B)$ to A and B are separable, and $\pi_0(A) \times \pi_0(B) \subseteq \pi_0(A \times B)$ because the product of two separable algebras is again separable.

The proof of (iii) and (iv) is more involved and will be omitted. □

Remark 8.3.7. Let X be an affine k-functor, with $A = k[X]$, and let $\pi_0(X)$ be the affine k-functor represented by the separable algebra $\pi_0(A)$. Then we can think of $\pi_0(X)$ as the functor describing the connected components of X. Notice that every idempotent $e \in A$ is contained in $\pi_0(A)$ because $k[e]$ is separable. More precisely, if $\pi_0(A) = K_1 \times \cdots \times K_r$ for separable field extensions K_i/k, then each idempotent $e \in A$ lies in $\pi_0(A)$ and must therefore be of the form $(e_1, \ldots, e_r)$ with $e_i \in K_i$ idempotent, i.e., each e_i is 0 or 1. Hence there are precisely 2^r idempotents, and precisely r of them cannot be written as a non-trivial sum of other idempotents. By Theorem 8.2.3, these r "minimal idempotents" correspond precisely to the r connected components of $\operatorname{Spec}(A)$ via the map $e \mapsto V(1-e)$.

Notice that connected components of X over k might break down into several connected components after base extension, corresponding to what we see on the level of $\pi_0(A)$, by Proposition 8.3.6(iii). In that sense, the *dimension* of the k-algebra $\pi_0(A)$ is sufficient to detect the potential number of connected components after base extension (even if those are not visible over k itself).

8.4 Connected components of linear algebraic groups

We are now fully prepared to study connectedness of linear algebraic groups in general.

Theorem 8.4.1. *Let G be a linear algebraic group defined over k, let $A = k[G]$ be its coordinate algebra and let N be the nilradical of A. Then the following are equivalent:*

(a) $\operatorname{Spec} A$ *is connected;*

(b) $\operatorname{Spec} A$ *is irreducible;*

(c) $\pi_0(A) = k$*;*

(d) A/N *is an integral domain.*

Proof. By Lemma 8.2.2(ii), (b) $\iff$ (d), and of course (b) $\implies$ (a). Now assume that $\operatorname{Spec} A$ is connected; then $\pi_0(A)$ is a separable extension field of k. The counit $\epsilon\colon A \to k$ restricts to a k-algebra homomorphism $\pi_0(A) \to k$, which implies that $\pi_0(A) = k$; hence (a) $\implies$ (c). Conversely, assume that $\pi_0(A) = k$. Then A does not have non-trivial idempotents, so by Corollary 8.2.5(i), $\operatorname{Spec} A$ is connected; hence (c) $\implies$ (a).

We finally show that (c) $\implies$ (d). So assume again that $\pi_0(A) = k$; then $\pi_0(A \otimes \overline{k}) = \overline{k}$ as well. In order to show that A/N is an integral domain, we may assume that $k = \overline{k}$. In that case[4], A/N is the ring of functions on the group of k-points $G(k)$. Since we have already shown that (c) $\implies$ (a), we know that $\operatorname{Spec} A$ is connected; Corollary 8.2.5(iv) now implies that also $G(k)$ is connected. By Theorem 8.1.1, we can now conclude that $G(k)$ is irreducible, and hence its ring of functions A/N is an integral domain. □

Definition 8.4.2. If G is a linear algebraic group satisfying each of the four equivalent conditions of Theorem 8.4.1, then we call G *connected*.

Corollary 8.4.3. *Let G be a linear algebraic group defined over k, and let K/k be a field extension. Then G is connected if and only if G_K is connected.*

Proof. This follows from Proposition 8.3.6(iii) and condition (c) of Theorem 8.4.1. □

When G is not connected, the algebra $\pi_0(k[G])$ is exactly what we need to analyze the connected components of G.

Proposition 8.4.4. *Let G be a linear algebraic group defined over k, and let $A = k[G]$ be its coordinate algebra. Then $\pi_0(A)$ is a Hopf subalgebra of A.*

Proof. Notice that every k-algebra homomorphism $f\colon A \to B$ maps separable subalgebras onto separable subalgebras, and in particular $f(\pi_0(A)) \subseteq \pi_0(B)$. Since $\Delta\colon A \to A \otimes A$ and $S\colon A \to A$ are k-algebra homomorphisms, we get

$$\Delta(\pi_0(A)) \subseteq \pi_0(A \otimes A) \cong \pi_0(A) \otimes \pi_0(A) \quad \text{and} \quad S(\pi_0(A)) \subseteq \pi_0(A);$$

moreover, the counit $\epsilon\colon A \to k$ restricts to a k-algebra morphism $\pi_0(A) \to k$. This shows that $\pi_0(A)$ is a Hopf subalgebra of A. □

[4]See also Remark 8.5.17 below.

Definition 8.4.5. Let G be a linear algebraic k-group, and let $A = k[G]$.

(i) The linear algebraic group associated to the Hopf subalgebra $\pi_0(A)$ of A will be denoted by $\pi_0(G)$, and is called the *group of connected components* of G.

(ii) The kernel of the quotient map $G \to \pi_0(G)$ is called the *identity component* of G, and is denoted by G°.

(iii) The linear algebraic group G is called *étale* if $\pi_0(A) = A$, or equivalently, if G° is trivial.

We list a few properties of $\pi_0(G)$ and G° in the next two propositions.

Proposition 8.4.6. *Let G be a linear algebraic k-group, and let $A = k[G]$, with counit $\epsilon\colon A \to k$. Then $k[G^\circ] \cong eA$ for some idempotent $e \in A$ with $\epsilon(e) = 1$ and $\pi_0(eA) = k$. In particular, G° is connected.*

Proof. Consider the counit $\epsilon\colon \pi_0(A) \to k$, and use Theorem 8.3.2(d) to write

$$\pi_0(A) = K_1 \times \cdots \times K_r$$

where each K_i is a separable extension field of k. Since every idempotent in $\pi_0(A)$ is mapped to 0 or 1, there is exactly one K_i which is mapped to k (and which is therefore isomorphic to k), while all others are mapped to 0. Assume that this happens for $i = 1$, and let $e = (1, 0, \ldots, 0) \in K_1 \times \cdots \times K_r$. Then we can write

$$A = eA \times (1 - e)A, \tag{8.1}$$

and in particular $\pi_0(eA) = k$ and $\pi_0((1-e)A) = K_2 \times \cdots \times K_r$; notice that the latter is precisely the augmentation ideal I of $\pi_0(A)$, i.e. the kernel of the counit $\epsilon\colon \pi_0(A) \to k$.

By Proposition 5.2.6, the kernel G° of the homomorphism $G \to \pi_0(G)$ is a closed normal subgroup of G, with coordinate algebra $k[G^\circ] \cong A/IA$. Explicitly, we have $I = (1-e)\pi_0(A)$, and hence, by (8.1),

$$k[G^\circ] \cong A/(1-e)A \cong eA.$$

It follows that $\pi_0(k[G^\circ]) \cong \pi_0(eA) = k$, and hence G° is connected. □

Proposition 8.4.7. *Let G, H be two linear algebraic k-groups and let $\alpha\colon G \to H$ be a homomorphism.*

(i) *If H is étale, then α factors through $G \to \pi_0(G)$.*

(ii) *If G is connected and H is étale, then α is trivial.*

(iii) *If G is connected, then α factors through $H^\circ \to H$.*

(iv) *The functors $G \mapsto \pi_0(G)$ and $G \mapsto G^\circ$ commute with base field extension.*

(v) *We have $\pi_0(G \times H) \cong \pi_0(G) \times \pi_0(H)$ and $(G \times H)^\circ \cong G^\circ \times H^\circ$.*

Proof. Write $A = k[G]$ and $B = k[H]$.

(i) We have already observed that every morphism from a separable algebra to A has its image in $\pi_0(A)$; the result follows by dualizing.

(ii) By (i), α factors through $G \to \pi_0(G)$. Since G is connected, however, $\pi_0(G) = 1$, and hence α is trivial.

(iii) By (ii), the composition $G \to H \to \pi_0(H)$ is trivial. Dually, this means that the composition $\pi_0(B) \hookrightarrow B \to A$ is trivial, in other words, the restriction of $\alpha^*\colon B \to A$ to $\pi_0(B)$ is trivial. In particular, α^* is the zero map on the augmentation ideal I of $\pi_0(B)$, hence $\alpha^*(IB) = 0$. By Proposition 8.4.6, $k[H^\circ] = B/IB$. Hence α^* induces a well defined Hopf algebra morphism from $k[H^\circ]$ to A through which α^* factors. By dualizing again, we find the required factorization of α.

(iv) Since $K[G_K] \cong k[G] \otimes_k K$ for every field extension K/k, this follows from Proposition 8.3.6(iii).

(v) Since $k[G \otimes H] \cong k[G] \otimes_k k[H]$, this follows from Proposition 8.3.6(iv). □

Corollary 8.4.8. *Let*

$$1 \to N \to G \to Q \to 1$$

be an exact sequence of linear algebraic k-groups. If N and Q are connected, then G is connected. Conversely, if G is connected, then Q is connected.

Proof. Assume first that N and Q are connected. Then N is contained in the kernel of the map $G \to \pi_0(G)$, so by Proposition 5.3.7, this map factors through $G \to Q$, and so it induces a quotient map from the connected group Q to an étale group $\pi_0(G)$. By Proposition 8.4.7(ii), this quotient map is trivial, which implies that $\pi_0(G) = 1$, showing that G is connected.

Conversely, assume that G is connected, and consider the composition of quotient maps $G \to Q \to \pi_0(Q)$. Again, Proposition 8.4.7(ii) implies that this map is trivial, and hence $\pi_0(Q) = 1$, showing that Q is connected. □

Example 8.4.9. (1) The linear algebraic groups $\mathbb{G}_a$, GL_n, $\mathbb{T}_n$, $\mathbb{U}_n$, $\mathbb{D}_n$ are connected because their coordinate algebra is an integral domain.

(2) Let G be the linear algebraic group of monomial matrices. Then $\pi_0(G)$ is the constant algebraic group Sym_n, and $G^\circ = \mathbb{D}_n$.

(3) The natural isomorphism (of affine k-functors, not of k-group functors!)

$$\mathsf{SL}_n(R) \times \mathbb{G}_m(R) \to \mathsf{GL}_n(R) \colon (A, r) \mapsto A \cdot \mathrm{diag}(r, 1, \ldots, 1)$$

defines an isomorphism of k-algebras

$$k[\mathsf{GL}_n] \cong k[\mathsf{SL}_n] \otimes_k k[\mathbb{G}_m] \cong k[\mathsf{SL}_n] \otimes_k k[t, t^{-1}],$$

and hence $k[\mathsf{GL}_n]$ contains $k[\mathsf{SL}_n]$ as a subring, which is therefore also an integral domain; this shows that SL_n is connected.

(4) Let k be a field of characteristic p, let $n \geq 2$ be an integer, and consider the algebraic group $G = \mu_n$ of n-th roots of unity over k. Recall that $A = k[\mu_n] \cong k[t]/(t^n - 1)$.

- If $p \neq 0$ and n is a power of p, then the nilradical of A is the ideal $N = (t-1)$; in this case, $A/N \cong k$, and hence G is connected. (Geometrically, G consists of one "thick point" with multiplicity n.)
- Assume next that $p = 0$ or $p > 0$ and $p \nmid n$. Then the nilradical of A is trivial, and A is not an integral domain (it has zero divisor $t - 1$); hence G is disconnected. (Geometrically, G consists of n points, each with multiplicity 1.)
- Finally, assume that $p > 0$ and $n = p^r \cdot m$ with $p \nmid m$ and $r \geq 1$. Then the nilradical of A is the ideal $N = (t^m - 1)$, but A/N is not an integral domain (again, it has zero divisor $t - 1$); hence G is disconnected. (Geometrically, G consists of m thick points, each with multiplicity p^r.) Notice that in this case, $\mu_n \cong \mu_{p^r} \times \mu_m$, so μ_n is the product of the connected group μ_{p^r} and the étale group μ_m.

8.5 Dimension and smoothness

We will briefly mention some aspects of dimension and smoothness of linear algebraic groups, without proofs.

Throughout this section, let k be an arbitrary field and let G be a linear algebraic k-group with coordinate algebra $A = k[G]$. Denote the nilradical of A by N.

We begin with the important and useful notion of dimension, which will, in particular, allow us later to prove certain statements by induction. The reader should compare this with the earlier Definition 4.2.6.

Definition 8.5.1. (i) Assume first that G is connected. Then we define $\dim G := \mathrm{trdeg}_k(\mathrm{Frac}(A/N))$, the transcendence degree over k of the field of fractions of A/N. (Notice that A/N is an integral domain by Theorem 8.4.1.)

(ii) When G is not connected, we define $\dim G := \dim G^\circ$.

Remark 8.5.2. Equivalently, the dimension of G can be defined to be the *Krull dimension* of its coordinate ring $A = k[G]$, i.e., the largest possible height of a maximal ideal in A (which is a finite number). (The *height* $\mathrm{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ is defined as the largest possible length n of a descending chain

$$\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$$

of prime ideals in A.) Moreover, every maximal chain of distinct prime ideals in A/N has length $\dim G$.

Example 8.5.3. (i) A group G is zero-dimensional if and only if A/N has transcendence degree 0 over k, if and only A has Krull dimension 0, if and only if A is finite-dimensional over k. (The last equivalence relies on the Noether Normalization Lemma.) By definition, these are precisely the finite linear algebraic groups.

(ii) Let $G = \mathsf{SL}_n$, $A = k[G] \cong k[t_{11}, \ldots, t_{nn}] \,/\, (\det(t_{ij}) - 1)$. Notice that A is itself an integral domain, and hence $\dim G$ is equal to the transcendence degree of $\mathrm{Frac}(A)$ over k, which is $n^2 - 1$.

There is a close relation between the dimension of a linear algebraic group and the dimension of its Lie algebra. They very often coincide, but not always; this is precisely what gives rise to the notion of smoothness.

Proposition 8.5.4. *Let G be a linear algebraic k-group, and let $\mathfrak{g} = \mathrm{Lie}(G)$. Then $\dim G \leq \dim \mathfrak{g}$.*

Definition 8.5.5. A linear algebraic group G is called *smooth* if $\dim G = \dim \mathrm{Lie}(G)$.

Example 8.5.6. Typical examples of non-smooth groups are the linear algebraic groups μ_p and α_p over fields k of characteristic p. Compute as an exercise that these 0-dimensional groups have a 1-dimensional Lie algebra.

Remark 8.5.7. We have preferred to give the shortest and most direct definition of smoothness, but the notion also makes sense for algebraic varieties (as k-functors) in general. In that setting, an affine k-functor V with coordinate algebra $A = k[V]$ is called *smooth* if $V_{\overline{k}}$ is *regular*, i.e., if for every maximal ideal $\mathfrak{m}$ of A, the local ring $A_{\mathfrak{m}}$ is regular.

For perfect fields, we can see directly from the coordinate algebra whether the linear algebraic group is smooth.

Proposition 8.5.8. *Let G be a linear algebraic k-group, where k is perfect, and let $A = k[G]$. Then G is smooth if and only if A is reduced, i.e. A does not contain non-zero nilpotent elements.*

Example 8.5.9. Let k be a non-perfect field of characteristic p, and let $a \in k$ be an element that is not a p-th power. Then the subgroup G of $\mathbb{G}_a \times \mathbb{G}_a$ defined by $Y^p = aX^p$ is reduced but not smooth.

On the other hand, for fields of characteristic zero, the situation is very nice.

Theorem 8.5.10 (Cartier, 1962)**.** *Let G be a linear algebraic k-group, where* $\mathrm{char}(k) = 0$*. Then G is smooth.*

Proposition 8.5.11. *Quotients and extensions of smooth linear algebraic groups are smooth.*

Remark 8.5.12. The kernel of a homomorphism of smooth linear algebraic groups need not be smooth. For example, in characteristic p, the kernels of $\mathbb{G}_m \to \mathbb{G}_m \colon x \mapsto x^p$ and of $\mathbb{G}_a \to \mathbb{G}_a \colon x \mapsto x^p$ are precisely μ_p and α_p, respectively, and these are not smooth.

The following useful results illustrate that dimensions behave nicer when the groups are smooth.

Proposition 8.5.13. *Let G be a smooth linear algebraic k-group and let H be a closed subgroup of G. Then the following are equivalent:*

(a) $\dim H = \dim G$*;*

(b) *H has finite index in G;*

(c) $G^\circ = H^\circ$*.*

Corollary 8.5.14. *Let G be a smooth connected linear algebraic k-group and let H be a proper closed subgroup of G. Then* $\dim H < \dim G$*.*

Proposition 8.5.15. *Let G be a smooth connected linear algebraic k-group and let H be a closed subgroup of G. If $H(\overline{k}) = G(\overline{k})$, then $H = G$.*

Theorem 8.5.16. *If $1 \to N \to G \to Q \to 1$ is exact, then*

$$\dim G = \dim N + \dim Q.$$

Remark 8.5.17. From now on, we will often restrict to smooth linear algebraic groups over an algebraically closed field k. In this case, the coordinate algebra $A = k[G]$ is reduced, and in fact, this means that it is the coordinate algebra of an algebraic variety in the classical sense (see Proposition 4.2.3). In such cases, it is safe to identify G with its group of k-points $G(k)$, and we will often do so. We will freely make use of well-known notions and constructions from group theory, such as normal subgroups, normalizers, centralizers, etc., the construction and definition of which is far from obvious in the general setting, but which coincides with the classical notions applied on $G(k)$ in the case of smooth linear algebraic groups over algebraically closed fields.

Of course, it is a restriction to only consider smooth linear algebraic groups over an algebraically closed field, but on the other hand, this will give us substantial information even for general linear algebraic groups. Indeed, if G is a linear algebraic group defined over an arbitrary field k, then we can base change to the algebraic closure to get a group $G_{\overline{k}}$ which is defined over an algebraically closed field; and if $G_{\overline{k}}$ is not smooth, then we can "smoothen" it by replacing its coordinate algebra $A = \overline{k}[G_{\overline{k}}]$ by A/N, where N is the nilradical of A, i.e. the ideal consisting of the nilpotent elements of A.

We make this final observation into a proper definition that we will need later.

Definition 8.5.18. Let G be an algebraic group over a *perfect* field k, with coordinate algebra $A = k[G]$, and let N be the nilradical of A. Then it turns out that N is a Hopf ideal of A, so the quotient A/N defines a closed subgroup of G that we denote by G_{red}. (In general, G_{red} need not be normal in G! Moreover, if k is not perfect, then N is not always a Hopf ideal, so the assumption that k be perfect is necessary to define G_{red}.)

Chapter 9 Tori and characters

An (algebraic) torus is a linear algebraic k-group that becomes isomorphic to $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$ over the algebraic closure, and as such, tori are rather easy to understand. However, we will see later that understanding the tori *inside* a given linear algebraic group G already reveals important aspects of the structure of G, and that is the main reason to study tori separately in this chapter.

We will begin, however, by studying *characters* in linear algebraic groups; these are, in some sense, dual to subtori, and the two notions are interrelated. Characters will also play an important role in the representation theory of linear algebraic groups.

9.1 Characters

Definition 9.1.1. Let G be a linear algebraic k-group, and let $A = k[G]$.

(i) A *character* of G is a homomorphism $\chi\colon G \to \mathbb{G}_m$, or equivalently, a Hopf algebra homomorphism $\chi^*\colon k[t, t^{-1}] \to A$.

(ii) Let $X(G)$ be the set of all characters of G. We make $X(G)$ into an abelian group by setting

$$(\chi + \chi')_R(g) \coloneqq \chi_R(g) \cdot \chi'_R(g) \in R^\times$$

for all $\chi, \chi' \in X(G)$, all $R \in k\text{-}\mathbf{alg}$, and all $g \in G(R)$; we call it the *character group* of G.

(iii) If Γ is a finitely generated abelian group, then the group algebra $k\Gamma$ is a finitely generated k-algebra (see Example 2.1.4(4)). If we define

$$\Delta(\gamma) \coloneqq \gamma \otimes \gamma, \quad S(\gamma) \coloneqq \gamma^{-1}, \quad \epsilon(\gamma) \coloneqq 1,$$

for all $\gamma \in \Gamma$, then $k\Gamma$ becomes a Hopf algebra.

(iv) A non-zero element $a \in A$ is *group-like* if $\Delta(a) = a \otimes a$. Any group-like element a automatically satisfies $S(a) = a^{-1}$ and $\epsilon(a) = 1$.

Lemma 9.1.2. *Let G be a linear algebraic k-group, and let $A = k[G]$. The map*

$$\alpha\colon X(G) \to \{a \in A \mid a \text{ is group-like}\}\colon \chi \mapsto \chi^*(t)$$

is a group isomorphism.

Proof. Notice that the set of group-like elements in A is indeed closed under multiplication in A because Δ is an algebra homomorphism. We first check that $\chi^*(t)$ is indeed group-like for every $\chi \in X(G)$. Indeed, we have $\Delta(t) = t \otimes t$ in $k[\mathbb{G}_m] = k[t, t^{-1}]$, and hence $\Delta(\chi^*(t)) = \chi^*(t) \otimes \chi^*(t)$ since χ^* is a Hopf algebra homomorphism.

Conversely, if $a \in A$ is group-like, then we define

$$\psi\colon k[t, t^{-1}] \to k[G]\colon t \mapsto a.$$

Then $(\Delta \circ \psi)(t) = \big((\psi \otimes \psi) \circ \Delta\big)(t)$, and this implies that ψ is a Hopf algebra homomorphism, and hence $\psi = \chi^*$ for some $\chi \in X(G)$. This already shows that α is a bijection.

We finally check that α is a group homomorphism. Indeed, let $\chi_1, \chi_2 \in X(G)$. Then

$$(\chi_1 + \chi_2)^*(t) = (\chi_1 + \chi_2)(\mathrm{id}_A)(t) = \chi_1(\mathrm{id}_A)(t) \cdot \chi_2(\mathrm{id}_A)(t) = \chi_1^*(t) \cdot \chi_2^*(t). \qquad \square$$

9.2 Diagonalizable groups

Before we move on to tori, we study the related class of diagonalizable groups.

Definition 9.2.1. Let G be a linear algebraic k-group, and let $A = k[G]$. Then G is called *diagonalizable* if there is a Hopf algebra isomorphism $A \cong k\Gamma$ for some finitely generated abelian group Γ.

This definition might look surprising, and the connection with the classical notion of diagonalizable matrix groups might be unclear at this point. This will become more transparant when we look at two examples.

Examples 9.2.2. (1) Let $\Gamma = \mathbb{Z}$, and recall that $k\mathbb{Z} \cong k[t, t^{-1}]$. (Notice that the isomorphism is indeed a Hopf algebra isomorphism.) We recognize this as the coordinate algebra of the linear algebraic group $G = \mathbb{G}_m$, i.e. $\mathbb{G}_m$ is diagonalizable.

(2) Let $\Gamma = \mathbb{Z}/n\mathbb{Z}$, and recall that $k[\mathbb{Z}/n\mathbb{Z}] \cong k[t]/(t^n - 1)$. (Again, notice that the isomorphism is indeed a Hopf algebra isomorphism.) We recognize this as the coordinate algebra of the linear algebraic group $G = \mu_n$; see Example 5.1.2(6). Hence μ_n is diagonalizable.

Recall that every finitely generated abelian group is a direct product of (finite or infinite) cyclic groups, which means that we have essentially discovered all diagonalizable groups.

Theorem 9.2.3. *Let G be a linear algebraic k-group. Then G is diagonalizable if and only if it is isomorphic to a finite direct product of $\mathbb{G}_m$'s and μ_n's.*

Proof. Observe that the group algebra $k(\Gamma \times \Gamma')$ is isomorphic, as a Hopf algebra, to $k\Gamma \otimes_k k\Gamma'$. The result now follows from the classification of finitely generated abelian groups together with Examples 9.2.2 and Remark 5.1.10. □

Remark 9.2.4. This is one of the many instances where the functorial approach to linear algebraic groups shows its advantages. In the classical setting, the corresponding result has an assumption on $\mathrm{char}(k)$, but this assumption is not needed here. Indeed, recall that when $\mathrm{char}(k) = p \mid n$, the coordinate algebra $k[\mu_n]$ is not reduced, and hence in this case μ_n does not arise from an affine variety in the classical sense; see Proposition 4.2.2.

Our next goal is to characterize diagonalizable groups by their characters, or equivalently, by their group-like elements. We first need a lemma.

Lemma 9.2.5. *Let G be a linear algebraic k-group, and let $A = k[G]$. Then the group-like elements of A are linearly independent over k.*

Proof. Exercise; use the fact that Δ is an algebra homomorphism. □

Proposition 9.2.6. *Let G be a linear algebraic k-group, and let $A = k[G]$. Then G is diagonalizable if and only if A is spanned by its group-like elements (as a vector space). Moreover, there is an anti-equivalence between diagonalizable groups and finitely generated abelian groups, given by*

$$G \leftrightarrow X(G).$$

Proof. Let $\Gamma \subseteq A$ be the set of group-like elements in A. Recall from Lemma 9.1.2 that Γ is an abelian group and that there is an isomorphism $\alpha\colon X(G) \to \Gamma$. Let $k\Gamma$ be the group k-algebra of the group Γ.

Assume first that $A = \langle \Gamma \rangle$; by Lemma 9.2.5, this implies that Γ is a basis for the k-vector space A. So we already have $A \cong k\Gamma$ as vector spaces. Now notice that by definition, the product of elements of Γ coincides with their product in the algebra A; hence $A \cong k\Gamma$ as k-algebras. Observe now that this isomorphism is also a Hopf algebra isomorphism since the comultiplication on the generating set Γ of both algebras coincides.

Conversely, assume that G is diagonalizable, with $A \cong k\Gamma$ for some finitely generated abelian group Γ. Then by definition, $A = \langle \Gamma \rangle$ as a vector space, and the elements of Γ are indeed group-like in $k\Gamma$.

Finally, notice that if $\varphi\colon G \to H$ is a morphism of linear algebraic groups, then the dual map $\varphi^*\colon k[H] \to k[G]$ maps group-like elements of $k[H]$ to group-like elements of $k[G]$. □

We now come to the important connection with representation theory.

Definition 9.2.7. Let G be a linear algebraic k-group and let (V, m) be a G-representation, with corresponding natural transformation $\rho\colon G \to \mathsf{GL}_V$.

(i) A non-zero $v \in V$ is an *eigenvector* for the representation, with corresponding character χ, if

$$\rho(g)(v) = \chi(g)v$$

for all $g \in G(R)$ and all $v \in V_R$, or equivalently, if

$$m(v) = \alpha(\chi) \otimes v$$

for all $v \in V$. (Notice that $g(\alpha(\chi)) = \chi(g)$.) Observe that eigenvectors correspond to one-dimensional subrepresentations.

(ii) Define V_χ to be the largest subspace of V such that G acts on V_χ through the character χ, i.e., V_χ is the subspace of V consisting of all eigenvectors with character χ:

$$V_\chi \coloneqq \big\{ v \in V \mid m(v) = \alpha(\chi) \otimes v \big\}.$$

If V_χ is non-trivial, we call it an *eigenspace* for the G-representation *with character* χ.

(iii) We call (V, m) *diagonalizable* if it can be written as a sum of one-dimensional subrepresentations, or in other words, if V is spanned by eigenvectors, i.e., V can be written as a sum of eigenspaces. (As we will see in a moment, it is then the *direct sum* of all its eigenspaces.)

Remark 9.2.8. If a non-zero $v \in V$ satisfies $m(v) = a \otimes v$ for *some* $a \in A$, then by the comodule axioms, a is necessarily group-like; Lemma 9.1.2 then implies that $a = \alpha(\chi)$ for some character χ, and hence v is an eigenvector.

Theorem 9.2.9. *Let G be a linear algebraic k-group, and let $A = k[G]$. Then G is diagonalizable if and only if every representation of G is diagonalizable, if and only if every representation (V, m) of G has a decomposition*

$$V = \bigoplus_{\chi \in X(G)} V_\chi. \tag{9.1}$$

Proof. Assume first that G is diagonalizable, and let (V, m) be a G-representation. We have to show that V is spanned by eigenvectors, i.e., by elements u such that $m(u) \in A \otimes ku$. By Proposition 9.2.6, we know that A is spanned, as a k-vector space, by its subset Γ of group-like elements.

Now let $v \in V$ be arbitrary, and write

$$m(v) = \sum_{\gamma \in \Gamma} \gamma \otimes u_\gamma,$$

where each $u_\gamma \in V$, and where the sum is a finite sum. We now apply the comodule identities (see Definition 5.4.1(ii)) on v:

$$\begin{aligned} (\mathrm{id}_A \otimes m)(m(v)) &= (\Delta \otimes \mathrm{id}_V)(m(v)) \quad \text{and} \\ (\epsilon \otimes \mathrm{id}_V)(m(v)) &= \mathrm{id}_V(v) \end{aligned}$$

yield

$$\sum_{\gamma \in \Gamma} \gamma \otimes m(u_\gamma) = \sum_{\gamma \in \Gamma} \gamma \otimes \gamma \otimes u_\gamma \quad \text{and} \tag{9.2}$$

$$\sum_{\gamma \in \Gamma} u_\gamma = v, \tag{9.3}$$

respectively. Since Γ is a basis of A, equation (9.2) shows that $m(u_\gamma) = \gamma \otimes u_\gamma \in A \otimes u_\gamma$ for each $\gamma \in \Gamma$; equation (9.3) shows that $v \in \langle u_\gamma \mid \gamma \in \Gamma \rangle$. This shows that V is spanned by elements u such that $m(u) \in A \otimes ku$.

Conversely, assume that every representation of G is diagonalizable. Then in particular, the regular representation $(V, m) = (A, \Delta)$ of G is diagonalizable, and hence A is spanned by its eigenvectors. Let $a \in A$ be an eigenvector for the regular representation with character χ; then $\Delta(a) = m(a) = \alpha(\chi) \otimes a$. Applying the identity $\mathrm{mult} \circ (\mathrm{id} \otimes \epsilon) \circ \Delta = \mathrm{id}$ on a yields

$$\epsilon(a)\alpha(\chi) = a,$$

i.e. a is a scalar multiple of $\alpha(\chi)$. It follows that A is spanned by its group-like elements, i.e. G is diagonalizable.

We finally show that a given G-representation (V, m) is diagonalizable if and only if (9.1) holds. Clearly, every subspace V_χ is diagonalizable, hence (9.1) implies that (V, m) itself is diagonalizable. Conversely, assume that (V, m) is diagonalizable. Then V is spanned by eigenvectors, and since every eigenvector belongs to some V_χ, we certainly have $V = \sum_{\chi \in X(G)} V_\chi$. In order to show that the sum is direct, assume that there exists a finite set of

characters $\chi_1, \ldots, \chi_\ell$ and corresponding non-zero eigenvectors $v_1, \ldots, v_\ell$ such that $v_1 + \cdots + v_\ell = 0$. Applying m yields

$$\alpha(\chi_1) \otimes v_1 + \cdots + \alpha(\chi_\ell) \otimes v_\ell = 0,$$

which contradicts Lemma 9.2.5. □

9.3 Tori

Definition 9.3.1. Let G be a linear algebraic k-group.

(i) The group G is a *torus* if $G_{\overline{k}} \cong (\mathbb{G}_m)^n$ for some integer $n \geq 1$, where $\overline{k}$ is the algebraic closure of k. Equivalently, G is a torus if and only if $G_{\overline{k}}$ is a smooth connected diagonalizable group.

(ii) The group G is called *of multiplicative type* if $G_{\overline{k}}$ is a diagonalizable group. In particular, every torus is of multiplicative type.

As we indicated, tori are especially useful when considered as subgroups of a larger linear algebraic group. We will now show how we can associate a finite group to every such torus; this finite group will play an important role later when we describe the structure of reductive linear algebraic groups.

Theorem 9.3.2. *Let G be a smooth linear algebraic group over an algebraically closed field k, and let T be a torus contained in G.*

(i) *Let V be a (not necessarily faithful) finite-dimensional G-representation. Let*

$$M \coloneqq \{\chi \in X(T) \mid V_\chi \neq 0\};$$

then M is a finite set. The normalizer[1] *$N_G(T)$ permutes the subspaces $\{V_\chi \mid \chi \in M\}$, and hence induces an action of $N_G(T)$ on M. The kernel of this action contains $C_G(T)$, and coincides with $C_G(T)$ if the representation is faithful.*

(ii) *The group $W(G,T) \coloneqq N_G(T)/C_G(T)$ is finite.*

Proof. (i) By Theorem 9.2.9, V decomposes as $V = \bigoplus_{\chi \in X(T)} V_\chi$ with respect to T. Since V is finite-dimensional, the set M is finite. Notice that when we identify G with $G(k)$ and V with $V(k)$, the subspaces V_χ can be interpreted as k-subspaces

$$V_\chi = \{v \in V \mid t.v = \chi(t)v \text{ for all } t \in T\},$$

[1] We define the normalizer and centralizer as concrete subgroups of $G(k)$; see Remark 8.5.17.

where we have written $t.v$ in place of $\rho(t)(v)$.
Assume now that $g \in N_G(T)$, and define, for each character $\chi \in X(T)$, a new character $g.\chi$ by

$$(g.\chi)(t) \coloneqq \chi(g^{-1}tg)$$

for all $t \in T$. We claim that g maps V_χ to $V_{g.\chi}$. Indeed, let $v \in V_\chi$ be arbitrary; then for all $t \in T$,

$$t.(g.v) = g.(g^{-1}tg).v = g.\chi(g^{-1}tg)v = \chi(g^{-1}tg)g.v = (g.\chi)(t) \cdot g.v, \tag{9.4}$$

showing that $g.v \in V_{g.\chi}$ indeed. Obviously, non-empty eigenspaces are mapped to non-empty eigenspaces, and hence $N_G(T)$ acts on the finite set M.
We will now determine the kernel of this action. So let $g \in N_G(T)$; then g is in the kernel of the action if and only if $g.\chi = \chi$ for all $\chi \in M$. By equation (9.4), this is equivalent to

$$t.g.v = \chi(t)g.v \tag{9.5}$$

for all $t \in T$, all $\chi \in M$, and all $v \in V_\chi$. Notice that $\chi(t)$ is a scalar, and $\chi(t)v = t.v$ since $v \in V_\chi$; hence $\chi(t)g.v = g.t.v$. It follows that (9.5) is in turn equivalent with

$$t.g.v = g.t.v$$

for all $t \in T$ and all $v \in V_\chi$, for all $\chi \in M$. Since V is spanned by the subspaces V_χ, this is equivalent with saying that the commutator $[g, t]$ acts trivially on V, for all $t \in T$. In particular, $C_G(T)$ is contained in the kernel of the action of $N_G(T)$ on M, and if the representation is faithful, then they coincide.

(ii) Consider an arbitrary finite-dimensional faithful representation for G (which always exists by Theoreom 5.4.6). Then by (i), $W(G,T)$ acts faithfully on the finite set M, and is thus isomorphic to a subgroup of $\mathrm{Sym}_{|M|}$. In particular, $W(G,T)$ is a finite group. □

Example 9.3.3. Let $G = \mathsf{GL}_n$, and consider the k-dimensional torus

$$T = \{\mathrm{diag}(a_1, \ldots, a_k, 1, \ldots, 1) \mid a_1, \ldots, a_k \in k^\times\}.$$

Then $N_G(T) = \mathrm{Mon}_k \times \mathsf{GL}_{n-k}$, whereas $C_G(T) = \mathbb{D}_k \times \mathsf{GL}_{n-k}$. Hence $W(G,T) \cong \mathrm{Sym}_k$.

We end this chapter by mentioning a result that we will need later (applied in the case when T is a k-torus).

Theorem 9.3.4 (Rigidity of tori)**.** *Let k be an arbitrary field, let G be a connected linear algebraic k-group, and let T be a linear algebraic k-group of multiplicative type. Assume that G acts on T by automorphisms. Then this action is trivial.*

Proof omitted. □

Remark 9.3.5. The rigidity of tori is a generalization of Theorem 9.3.2. Indeed, when we apply it to the situation where T is a subtorus of G, then $N_G(T)$ acts on T by inner automorphisms. Passing to the identity component $N_G(T)^\circ$ then implies that the action of the connected group $N_G(T)^\circ$ on T is trivial, i.e. $N_G(T)^\circ \leq C_G(T)$. Hence $N_G(T)^\circ = C_G(T)^\circ$, and in particular $N_G(T)/C_G(T)$ is a finite group.

Chapter 10 Solvable linear algebraic groups

We now come to the study of solvable linear algebraic groups. Giving a complete classification of such groups is beyond hope, but as we will see, we will nevertheless be able to prove some strong structure theorems for this class of algebraic groups.

We will then study solvable subgroups of general linear algebraic groups; this will lead us to the theory of Borel subgroups, which will play an important role in our later understanding of reductive groups.

10.1 The derived subgroup of a linear algebraic group

To give a rigorous definition of solvable linear algebraic groups, we need the notion of a derived subgroup, which is similar to but more delicate than the definition for concrete groups.

Definition 10.1.1. Let G be a linear algebraic k-group. Then we define the *derived subgroup* $\mathcal{D}(G)$ of G as the intersection of all closed normal subgroups N of G for which G/N is abelian.

Remark 10.1.2. Recall from section 5.3 that quotients of linear algebraic groups are a delicate matter. Fortunately, if G is a smooth linear algebraic group over an algebraically closed field k, then $(G/N)(k) \cong G(k)/N(k)$ for each closed normal subgroup N of G.

We will now give an explicit construction of the derived subgroup of any linear algebraic k-group. Recall that if Γ is a concrete group, then the derived subgroup $\mathcal{D}(\Gamma)$ is

$$\mathcal{D}(\Gamma) = \langle [g,h] \mid g,h \in \Gamma \rangle,$$

where $[g,h] = ghg^{-1}h^{-1}$ is the commutator[1] of g and h.

[1]Note that $[g,h]$ is sometimes defined to be $g^{-1}h^{-1}gh$, but the definition we have chosen agrees with the fact that our group actions are written as left actions.

Construction 10.1.3. Let G be a linear algebraic k-group, and let $A = k[G]$. For each $n \in \mathbb{Z}_{\geq 0}$, we define the map (between k-functors)

$$\psi_n \colon G^{2n} \to G \colon (g_1, h_1, \ldots, g_n, h_n) \mapsto \prod_{i=1}^{n} [g_i, h_i]$$

for all $g_i, h_i \in G_R$, for all $R \in k$-**alg**. There are corresponding maps

$$\psi_n^* \colon A \to A^{\otimes 2n},$$

and for each n, the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ \downarrow{\scriptstyle \psi_{2n}^*} & & \downarrow{\scriptstyle \psi_n^* \otimes \psi_n^*} \\ A^{\otimes 2n} & \xrightarrow{\sim} & A^{\otimes n} \otimes A^{\otimes n} \end{array} \tag{10.1}$$

Let $I_n \coloneqq \ker(\psi_n^*)$; then we have a descending chain of ideals

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \ldots$$

Let $I \coloneqq \cap_{n \geq 1} I_n$; then I is again an ideal in A. In fact, I is the defining ideal of some closed subgroup of G, i.e. a Hopf ideal of A. (Notice that the ideals I_n are *not* Hopf ideals in general, since the maps ψ_n are no morphisms.) Indeed, by the commutative diagram (10.1), the comultiplication Δ on A induces a homomorphism

$$A/I_{2n} \xrightarrow{\Delta} A/I_n \otimes A/I_n$$

for all n, and therefore a homomorphism

$$A/I \xrightarrow{\Delta} A/I \otimes A/I,$$

making A/I into a Hopf algebra.

The closed subgroup corresponding to the Hopf ideal I is precisely the derived subgroup $\mathcal{D}(G)$.

Remark 10.1.4. In a similar way, we can construct the commutator $[H_1, H_2]$ for all closed subgroups H_1, H_2 of a linear algebraic k-group G.

Proposition 10.1.5. *Let G be a smooth connected linear algebraic group over an algebraically closed field k. Then $\mathcal{D}(G)$ is also smooth and connected.*

Proof. Let $A = k[G]$, and let I_n and I be as in Construction 10.1.3. Notice that G is smooth if and only if A is reduced, i.e. has no non-trivial nilpotents, and that G is connected if and only if A has no non-trivial idempotents. Now observe that the map ψ_n^* induces an injective mapping $A/I_n \to A^{\otimes 2n} \cong k[G^{2n}]$. Since G^{2n} is smooth and connected, $k[G^{2n}]$ has no non-trivial nilpotents nor idempotents, and hence the same holds for A/I_n, for all n. We conclude that A/I has no non-trivial nilpotents or idempotents either. (Indeed, assume that $e \in A/I$ is idempotent and lift e to some $f \in A$; then $f^2 - f \in I$, so $f^2 - f \in I_n$ for all n. This can only happen if f is 0 or 1 in each A/I_n, but then e must be 0 or 1.) This shows that $\mathcal{D}(G)$ is indeed smooth and connected. □

We now come to the definition of nilpotent and solvable linear algebraic groups.

Definition 10.1.6. Let G be a linear algebraic k-group.

(i) Let $\mathcal{D}^0(G) \coloneqq G$ and $\mathcal{D}^i(G) \coloneqq \mathcal{D}(\mathcal{D}^{i-1}(G))$ inductively for all $i \geq 1$. Then
$$G = \mathcal{D}^0(G) \geq \mathcal{D}^1(G) \geq \mathcal{D}^2(G) \geq \dots$$
is called the *derived series* of G.

(ii) Let $\mathcal{D}^{[0]}(G) \coloneqq G$ and $\mathcal{D}^{[i]}(G) \coloneqq [G, \mathcal{D}^{[i-1]}(G)]$ inductively for all $i \geq 1$. Then
$$G = \mathcal{D}^{[0]}(G) \geq \mathcal{D}^{[1]}(G) \geq \mathcal{D}^{[2]}(G) \geq \dots$$
is called the *lower central series series* of G.

(iii) The k-group G is called *solvable* if $\mathcal{D}^n(G) = 1$ for some n.

(iv) The k-group G is called *nilpotent* if $\mathcal{D}^{[n]}(G) = 1$ for some n.

Remark 10.1.7. If k is algebraically closed, then $\mathcal{D}(G)(k) \cong \mathcal{D}(G(k))$, but this is false in general. For instance, if $k = \mathbb{F}_2$ and $G = \mathsf{SL}_2$, then $\mathcal{D}(G) = G$, and hence $\mathcal{D}(G)(k) \cong \mathsf{SL}_2(\mathbb{F}_2)$, but
$$\mathcal{D}(G(k)) = \mathcal{D}(\mathsf{SL}_2(\mathbb{F}_2)) \cong \mathcal{D}(\mathrm{Sym}_3) \ncong \mathrm{Sym}_3\,.$$

10.2 The structure of solvable linear algebraic groups

In this section, we will always assume that G is a smooth linear algebraic group over an algebraically closed field k. A crucial fact about connected

solvable groups (that we will not prove here) is the so-called Borel fixpoint theorem; a consequence of this result is the Lie–Kolchin theorem, stating that such a group can always be represented by upper-triangular matrices. We will only indicate this approach, and we will instead give a self-contained proof below.

In order to state the Borel fixpoint theorem, we first have to introduce the notion of a complete variety.

Definition 10.2.1. An algebraic variety[2] Z is *complete* if for every variety Y, the projection map $\pi\colon Y \times Z \to Y$ is a closed map, i.e. it maps closed subsets to closed subsets.

Examples 10.2.2. (1) The affine line $\mathbb{A}^1$ is not complete. For instance, the closed subset $S = \{(x, y) \in \mathbb{A}^2 \mid xy = 1\}$ of $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ is projected onto the non-closed subset $\pi(S) = \{x \in \mathbb{A}^1 \mid x \neq 0\}$ of $\mathbb{A}^1$.

(2) It turns out that for each integer $n \geq 1$, the projective space $\mathbb{P}^n$ is a complete variety. Since a closed subvariety of a complete variety is again complete, this implies that in fact every projective variety is complete.

We will mention a couple of useful facts about complete varieties, some of which we will need later.

Proposition 10.2.3. (i) *A closed subvariety of a complete variety is complete.*

(ii) *Every projective variety is complete.*

(iii) *If X is complete, then its image under any morphism $X \to Y$ is closed and complete.*

(iv) *An affine variety is complete if and only if it has dimension zero, i.e. if and only if it is a finite set of points.*

Proof omitted. □

We can now state the important Borel fixed-point theorem.

Theorem 10.2.4 (Borel fixed-point theorem)**.** *Let G be a smooth connected solvable linear algebraic group over an algebraically closed field k, acting on a non-empty complete k-variety X. Then this action has a fixed point, i.e. there is an $x \in X$ fixed by G.*

[2]We have not given a formal definition of an algebraic variety, and we will not attempt to do so (avoiding phrases such as "integral, separated scheme of finite type over an algebraically closed field"). It will be sufficient for our purposes to understand what a *projective variety* is: it is the set of zeroes $V(S)$ in projective space $\mathbb{P}^n$ for a set S of homogeneous polynomials in $n + 1$ variables.

Proof omitted. □

Theorem 10.2.5 (Lie–Kolchin theorem)**.** *Let G be a smooth connected solvable linear algebraic group over an algebraically closed field k, and let $\rho\colon G \to \mathsf{GL}_V$ be a finite-dimensional G-representation. Then V has a basis such that $\rho(G)$ is upper-triangular.*

Proof. Using Borel's fixed-point theorem, there are two different ways to prove this. The first approach is inductive. Observe that through the G-representation, G acts on the projective space $\mathbb{P}^{n-1}$, where $n = \dim_k V$. Since projective space is a complete variety, Borel's fixed-point theorem implies that there is a fixed point $x \in \mathbb{P}^{n-1}$ for the G-action, i.e. there is a one-dimensional subspace of V which is stabilized by G. Take the first basis vector of V to be a generator of this subspace, and proceed by induction.

The second approach is direct, and quite elegant, but requires some familiarity with Grassmann varieties. Let $\mathcal{F}(V)$ be the *flag variety* of V, i.e. the variety with as points the maximal flags $V_1 \subset V_2 \subset \cdots \subset V_n$ (with $\dim_k V_i = i$ for each i), viewed as a subvariety of the projective variety $\mathrm{Gr}_1(V) \times \cdots \times \mathrm{Gr}_n(V)$, where $\mathrm{Gr}_i(V)$ is the Grassmann variety consisting of the i-dimensional subspaces of V. Then $\mathcal{F}(V)$ is a complete variety, and hence the induced action of G on $\mathcal{F}(V)$ has a fixed point, i.e. $G(V_i) = V_i$ for all i. With respect to the corresponding basis of V, the group G is upper-triangular. □

Historically, the Borel fixed-point theorem was a generalization of the Lie–Kolchin triangularization theorem, so in a sense we have been cheating to prove Lie–Kolchin's theorem using Borel's theorem for which we omitted the proof. It is instructive to look at a direct proof of the Lie–Kolchin theorem. We first need a lemma.

Lemma 10.2.6. *Let V be a finite-dimensional vector space over an algebraically closed field k, and let S be a set of commuting elements in $\mathrm{End}_k(V)$. Then there exists a basis for V such that all elements of S are upper-triangular.*

Proof. We leave the proof of this fact as an exercise. Use induction on $\dim_k V$, and use the fact that if some $f \in S$ is not a scalar multiple of the identity, then f has an eigenspace $U \neq V$. Show that U is stable under all elements of S, and apply the induction hypothesis on U and V/U. □

Direct proof of Theorem 10.2.5. As we pointed out above, it suffices to show that the elements of $G(k)$ have a common eigenvector, because then we can apply induction on the dimension of V. We will prove this by induction on

the length of the derived series of G. If G is commutative, then the result follows from Lemma 10.2.6. (Notice that Lemma 10.2.6 shows that there is a basis for V such that $G(k) \leq \mathbb{T}_n(k)$, but since G is smooth, this implies that $G \leq \mathbb{T}_n$.)

Assume now that G is not commutative, and apply the induction hypothesis on $\mathcal{D}(G)$ to deduce that the elements of $N \coloneqq \mathcal{D}(G)$ have a common eigenvector. This means that there is some character χ of N for which the space

$$V_\chi = \{v \in V \mid g.v = \chi(g)v \text{ for all } g \in N\}$$

is non-trivial. Let S be the non-empty set of all $\chi \in X(N)$ for which $V_\chi \neq 0$, and let W be the sum of all eigenspaces V_χ for $\chi \in S$. Then W has a finite direct sum decomposition

$$W = \bigoplus_{\chi \in S} V_\chi.$$

Since G normalizes N, the same computation as in (9.4) shows that $G(k)$ permutes the subspaces $V_\chi, \chi \in S$.

Now choose $\chi \in S$ arbitrarily, and let $H \leq G(k)$ be the stabilizer of V_χ. Since S is finite, H is a finite index subgroup of $G(k)$. We claim that, in fact, $H = G(k)$. Notice that

$$H = \{g \in G(k) \mid \chi(n) = \chi(g^{-1}ng) \text{ for all } n \in N(k)\},$$

which is an algebraic condition[3], i.e. H is a closed subgroup of $G(k)$. Since $G(k)$ is connected and H has finite index, this implies that $H = G(k)$ as claimed. It follows that $G(k)$ stabilizes V_χ. In particular, there is a representation $\rho\colon G \to \mathsf{GL}(V_\chi) \cong \mathsf{GL}_d$, where $d = \dim V_\chi$.

Next, we claim that $N(k)$ acts trivially on V_χ. For each $n \in N(k)$ and each $v \in V_\chi$, we have $\rho(n).v = \chi(n)v$, with $\chi(n) \in k$. Since n is a product of commutators of elements of $G(k)$, and since every commutator in GL_d has determinant 1, this implies that $\rho(n)$ has determinant 1, and therefore $\chi(n)^d = 1$. We deduce that the image of the character $\chi\colon N \to \mathbb{G}_m$ takes values in $\mu_d \leq \mathbb{G}_m$. If $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p \nmid d$, then μ_d is étale, and since N is connected, it follows from Proposition 8.4.7(ii) that χ is trivial. If $p \mid d$, then this argument shows that the image of χ is contained in μ_{p^r} (where p^r is the highest p-power dividing d), but since $\mu_{p^r}(k) = 1$, we can again conclude that the action of $N(k)$ on V_χ is trivial. This proves the claim that $N(k)$ acts trivially on V_χ in all cases.

[3]Notice that χ is a morphism of algebraic groups, so expressing that $\chi(n) = \chi(g^{-1}ng)$ for a specific $n \in N(k)$ is an algebraic condition, i.e. it is a polynomial condition w.r.t. a given embedding in affine space. The intersection of (infinitely many) algebraic varieties is again an algebraic variety, so H is algebraic.

Therefore, there is an induced action of $G(k)/N(k)$ on V_χ. Since $G(k)/N(k)$ is an abelian group, we know that its elements have a common eigenvector in V_χ, and this is then also a common eigenvector for the elements of $G(k)$, which is what we had to prove. □

Remark 10.2.7. Each of the four hypotheses "smooth", "connected", "solvable" and "algebraically closed" is needed; the theorem becomes false as soon as one of these hypotheses is omitted.

As a consequence of the Lie–Kolchin theorem, we can prove that the set of unipotent elements in a connected solvable group behaves nicely. For commutative groups, we had already encountered this in Theorem 6.2.8.

Corollary 10.2.8. *Let G be a smooth connected solvable linear algebraic group over an algebraically closed field k. Then the set G_u is a closed connected nilpotent normal subgroup, and the quotient G/G_u is a torus.*

Proof. Without loss of generality, we may assume by Theorem 10.2.5 that G is a closed subgroup of $\mathbb{T}_n \leq \mathsf{GL}_n$. Then $g \in G(k)$ is a unipotent element if and only if it is a unipotent matrix in $\mathsf{GL}_n(k)$, i.e. if and only if all its diagonal elements are equal to 1. Hence the map

$$\varphi\colon G \to \mathbb{G}_m^n\colon g \mapsto \operatorname{diag}(g)$$

is a morphism, with kernel G_u, and hence G_u is a closed normal subgroup of G. Now observe that G_u is a subgroup of $\mathbb{U}_n \leq \mathsf{GL}_n$, which is easily seen to be nilpotent; hence G_u is nilpotent itself. Next, notice that $T = G/G_u$ is isomorphic to some subgroup of $\mathbb{G}_m^n$, and since it is smooth and connected (as a quotient of a smooth connected group), it follows that it is a torus.

We finally show that G_u is connected. Observe that when G is abelian, G_u is a quotient of G, which is therefore connected (see Theorem 6.2.8). This implies that $(G/\mathcal{D}(G))_u$ is connected. On the other hand, $\mathcal{D}(G) \leq G_u$, and the exact sequence

$$1 \to G_u/\mathcal{D}(G) \to G/\mathcal{D}(G) \to T \to 1$$

shows that every unipotent element of $G/\mathcal{D}(G)$ is contained in $G_u/\mathcal{D}(G)$, and hence $G_u/\mathcal{D}(G) = (G/\mathcal{D}(G))_u$ is connected. Since $\mathcal{D}(G)$ is itself also connected (see Proposition 10.1.5), it follows by Corollary 8.4.8 that G_u is connected as well. □

With some more effort, one can show the following structure theorem for solvable groups.

Theorem 10.2.9. *Let G be a smooth connected solvable linear algebraic group over an algebraically closed field k. Then:*

(i) *G_u is a closed connected nilpotent normal subgroup.*

(ii) *The quotient G/G_u is a torus.*

(iii) *There is a series of closed subnormal subgroups*

$$1 = N_0 \leq N_1 \leq \cdots \leq N_d = G_u$$

of G, such that for each $i \in \{1, \ldots, d\}$, the group N_{i-1} is normal in N_i and $N_i/N_{i-1} \cong \mathbb{G}_a$.

(iv) *The extension*

$$1 \to G_u \to G \to G/G_u \to 1$$

is split, i.e. G_u has a complement in G. Moreover, any two such complements are conjugate in G.

(v) *Every semisimple element $s \in G(k)$ is contained in a complement of G_u in G. Moreover, $C_G(s)$ is smooth and connected.*

Proof. We have already shown (i) and (ii), and we omit the proof of the other facts. □

Definition 10.2.10. Let G be a smooth connected linear algebraic group over an algebraically closed field k. A *maximal torus* of G is a torus of G that is not strictly contained in a larger torus of G.

If G is a smooth connected solvable linear algebraic group over an algebraically closed field k, then maximal tori are precisely the complements of G_u. Indeed, notice that such a complement is indeed a torus since it is isomorphic to G/G_u, and it is maximal w.r.t. inclusion since any subgroup of G properly containing it, would intersect G_u non-trivially and hence cannot be a torus. Conversely, the following corollary shows in particular that every torus is contained in a complement of G_u.

Corollary 10.2.11. *Let G be a smooth connected solvable linear algebraic group over an algebraically closed field k, and let H be a commutative subgroup of G consisting of semisimple elements only. Then H is contained in a complement of G_u (which is a maximal torus). Moreover, any two such maximal tori are conjugate by an element of $C_G(H)$.*

Proof. We will prove the result by induction on $\dim(G)$. Notice that the result is obvious if all elements of H are central in G, because a central semisimple element is contained in every complement of G_u, by Theorem 10.2.9(iv) and (v), and $C_G(H) = G$ in this case.

So assume that there is some $h \in H \setminus Z(G)$. Then $C_G(h)$ is a proper smooth connected subgroup of G, and $H \leq C_G(h)$. Since G is smooth and connected, $\dim C_G(h) < \dim G$. By the induction hypothesis, H is contained in a complement S of $C_G(h)_u$ in $C_G(h)$, and any two such maximal tori S and S' are conjugate by an element of $C_{C_G(h)}(H) = C_G(H)$.

It remains to show that S (and then also S') is a complement of G_u in G. By Theorem 10.2.9(v), h is contained in such a complement T of G_u, which is a maximal torus in G, so in particular $T \leq C_G(h)$. Since $C_G(h)_u$ is a subgroup of G_u, it follows that T is a complement of $C_G(h)_u$ in $C_G(h)$. By Theorem 10.2.9(iv) applied on $C_G(h)$, S and T are conjugate in $C_G(h)$, and hence S is also a complement of G_u in G. □

We mention the following classification result, which apart from the theory we have just seen, also requires a good deal of algebraic geometry.

Theorem 10.2.12. *Let G be a smooth connected 1-dimensional linear algebraic group over an algebraically closed field k. Then $G \cong \mathbb{G}_a$ or $G \cong \mathbb{G}_m$.*

Proof omitted. □

10.3 Borel subgroups

We now go back to the situation where G is a general (smooth) linear algebraic group over an algebraically closed field k. As we will see, understanding the solvable subgroups inside G will be important for determining the structure of G. This brings us to the notion of Borel subgroups.

Definition 10.3.1. Let G be a smooth linear algebraic group over an algebraically closed field k. A *Borel subgroup* of G is a maximal closed smooth connected solvable subgroup of G.

The following fact is an important feature of algebraic groups, but its proof requires more theory than we have covered.

Theorem 10.3.2. *Let G be a smooth linear algebraic group over an algebraically closed field k, and let B be a Borel subgroup of G. Then G/B is a projective k-variety.*

Proof omitted. □

Together with Borel's fixed-point theorem (Theorem 10.2.4), it has the following corollary.

Corollary 10.3.3. *Let G be a smooth linear algebraic group over an algebraically closed field k, and let B and B' be two Borel subgroups of G. Then B and B' are conjugate.*

Proof. Consider the action of B on the projective variety G/B' which is given by left multiplication on the set of left cosets of B' in G. Then by Borel's fixed-point theorem, this action has a fixed point, i.e. there is some left coset gB' which is stable under left multiplication by B, i.e. $bgB' = gB'$ for all $b \in B$. This implies $g^{-1}Bg \subseteq B'$. Since both $g^{-1}Bg$ and B' are Borel subgroups of G, the maximality of both implies that $g^{-1}Bg = B'$. □

We have seen that maximal tori inside solvable groups play an important role, but this is also true for general linear algebraic groups.

Proposition 10.3.4. *Let G be a smooth connected linear algebraic group over an algebraically closed field k. Then all maximal tori in G are conjugate. Even more, G acts transitively by conjugation on the set*

$$\big\{(T, B) \mid B \text{ a Borel subgroup of } G,\ T \text{ a maximal torus in } B\big\}.$$

Proof. Notice that a torus is a closed connected solvable subgroup, so by definition, every torus T of G is contained in some Borel subgroup B of G, and if T is a maximal torus in G, then it is also a maximal torus in B. The result now follows from Corollary 10.3.3 together with Theorem 10.2.9(iv). □

Remark 10.3.5. When k is not algebraically closed, it is no longer true that all maximal tori of G are conjugate, but by Proposition 10.3.4 they become conjugate after base change to $\overline{k}$. The classification of maximal tori over k thus becomes an "arithmetic problem" determined by $\overline{k}/k$, which is typically studied using Galois cohomology.

Since all maximal tori are conjugate, the dimension of a maximal torus is a well-defined number.

Definition 10.3.6. Let G be a smooth connected linear algebraic group over an algebraically closed field k. Then the *rank* $\mathrm{rk}(G)$ of G is defined to be the dimension of a maximal torus in G.

We will now further illustrate the importance of Borel subgroups by indicating that their structure already determines some of the structure of G. For instance, the center of B essentially determines the center of G, and if B is nilpotent, then already G was nilpotent to begin with. We start with a lemma.

Lemma 10.3.7. *Let G be a smooth linear algebraic group over an algebraically closed field k, and let B be a Borel subgroup of G.*

(i) *If G is connected and $G \neq 1$, then $B \neq 1$.*

(ii) *The index $[N_G(B) : B]$ is finite.*

(iii) $N_G(N_G(B)) = N_G(B)$.

Proof. (i) Assume $B = 1$. Then $G = G/B$ is simultaneously an affine variety and a projective variety. Since G is connected, this can only be true if $G = 1$.

(ii) Let $H = N_G(B)^\circ$ be the connected component of the normalizer of B in G. Then B is a Borel subgroup of H, which is normal. This implies that H/B is simultaneously an affine variety and a projective variety, which can only be true if $H/B = 1$, and hence $B = H = N_G(B)^\circ$. It follows that B is a finite index subgroup of $N_G(B)$.

(iii) Assume that $g \in G$ normalizes $N_G(B)$. Then it also normalizes the identity component $N_G(B)^\circ = B$. □

Remark 10.3.8. In fact, Borel subgroups are *self-normalizing*: we have $N_G(B) = B$. This is a deep and very useful fact, known as "Chevalley's normalizer theorem".

Proposition 10.3.9. *Let G be a smooth connected linear algebraic group over an algebraically closed field k, and let B be a Borel subgroup of G. Then*

$$Z(G)^\circ_{\mathrm{red}} \leq Z(B) \leq Z(G).$$

Proof. Notice that $Z(G)^\circ_{\mathrm{red}}$ is a closed connected smooth solvable subgroup, so by definition, it is contained in some Borel subgroup B' of G. Since B' is conjugate to B and conjugation acts trivially on $Z(G)^\circ_{\mathrm{red}}$, this implies that in fact $Z(G)^\circ_{\mathrm{red}} \leq B$, and consequently $Z(G)^\circ_{\mathrm{red}} \leq Z(B)$.

Now let $z \in Z(B)$ be arbitrary. Consider the map

$$\varphi \colon G \to G \colon g \mapsto gzg^{-1}.$$

Then φ is constant on every left B-coset, i.e. $\varphi(gb) = \varphi(gb')$ for all $g \in G$ and all $b, b' \in B$. Therefore, φ induces a morphism (of algebraic varieties)

$$\overline{\varphi} \colon G/B \to G \colon gB \mapsto gzg^{-1}.$$

Because G/B is a projective variety and G is an affine variety, Proposition 10.2.3 implies that the map $\overline{\varphi}$ has finite image, and hence φ has finite image as well. Since G and hence also G/B is connected, this implies that φ is a constant map. Hence $z \in Z(G)$. □

Proposition 10.3.10. *Let G be a smooth connected linear algebraic group over an algebraically closed field k, and let B be a Borel subgroup of G. If B is nilpotent, then G is nilpotent.*

Proof. We prove the result by induction on $\dim(G)$. It is trivial when $\dim(G) = 0$, so assume $\dim(G) \geq 1$, which implies by Lemma 10.3.7(i) that $\dim(B) \geq 1$ as well. Since B is nilpotent, the last non-trivial term of the lower central series of B is a connected non-trivial central subgroup N of B, and hence $\dim(Z(B)) \geq 1$. By Proposition 10.3.9, this implies that $\dim(Z(G)) \geq 1$ as well. By definition, $\dim(Z(G)^\circ_{\mathrm{red}}) = \dim(Z(G))$, so we deduce that the dimension of $G/Z(G)^\circ_{\mathrm{red}}$ is strictly lower than $\dim(G)$. Notice that $Z(G)^\circ_{\mathrm{red}} \leq B$, hence $B/Z(G)^\circ_{\mathrm{red}}$ is a Borel subgroup of $G/Z(G)^\circ_{\mathrm{red}}$, which is nilpotent. By induction, $G/Z(G)^\circ_{\mathrm{red}}$ is nilpotent, and hence G is nilpotent as well. □

Chapter 11 Semisimple and reductive groups

We continue with our assumption that G is a smooth linear algebraic group over an algebraically closed field k. Our aim is to understand the structure of such a G in its full generality, but as we have seen, already our understanding of unipotent, or more generally solvable, linear algebraic groups, is limited, in the sense that there is no hope of classifying such groups.

On the other hand, we will see that when we get rid of the unipotent or solvable "part" of a linear algebraic group G, then we are left with a so-called reductive or semisimple group, respectively, and it will turn out that we have a very good understanding of such groups: we will be able to classify them. An essential ingredient of the structure of such a group will be given by its so-called root datum.

11.1 Semisimple and reductive linear algebraic groups

We first introduce the notions of reductive and semisimple groups. We begin by stating the following useful fact.

Lemma 11.1.1. *Let G be a linear algebraic group over an algebraically closed field k. Let H be a closed subgroup of G and let N be a closed normal subgroup. If H and N are solvable (resp. unipotent, resp. connected, resp. smooth), then HN is solvable (resp. unipotent, resp. connected, resp. smooth).*

Proof. In each case, use the fact that $HN/N \cong H/(H \cap N)$, and that HN is an extension of HN/N by N, together with the fact that these properties (solvable, unipotent, connected, smooth) are preserved by quotients and by extensions. In each case, this requires a different argument, and we omit the details. □

Definition 11.1.2. Let G be a smooth linear algebraic group over an algebraically closed field k.

(i) The *radical* $R(G)$ is the largest smooth closed connected solvable normal subgroup of G.

(ii) The *unipotent radical* $R_u(G)$ is the largest smooth closed connected unipotent normal subgroup of G; it coincides with $R(G)_u$, the unipotent part of $R(G)$.

(iii) We call G *semisimple* if $R(G)$ is trivial.

(iv) We call G *reductive* if $R_u(G)$ is trivial.

The following characterizations are useful.

Lemma 11.1.3. *Let G be a smooth linear algebraic group over an algebraically closed field k.*

(i) *G is semisimple if and only if G does not have non-trivial smooth closed connected commutative normal subgroups.*

(ii) *G is reductive if and only if $R(G)$ is a torus.*

(iii) *G is reductive if and only if the only non-trivial smooth closed connected commutative normal subgroups of G are tori.*

Proof. (i) Assume that G does not have non-trivial smooth closed connected commutative normal subgroups, and suppose that G is not semisimple, i.e. $R(G) \neq 1$. Notice that both $R(G)$ and $\mathcal{D}(G)$ are characteristic subgroups of G, so each group occuring in the derived series of $R(G)$ is itself a smooth closed connected normal subgroup of G. The last non-trivial term of this series is commutative, which contradicts our assumption.

(ii) Notice that $R_u(G) = R(G)_u$, so G is reductive if and only if $R(G)$ is a smooth connected solvable group with trivial unipotent part. By the structure theorem of solvable groups (Theorem 10.2.9), this is equivalent to the fact that $R(G)$ is a torus.

(iii) Assume that every non-trivial smooth closed connected commutative normal subgroup of G is a torus. Suppose that G is not reductive, i.e. $R_u(G) \neq 1$. As in the proof of (i), each group occuring in the derived series of $R_u(G)$ is itself a smooth closed connected normal subgroup of G. The last non-trivial term of this series is commutative, and by our assumption, it is a torus. This contradicts the fact that $R_u(G)$ is a non-trivial unipotent group. □

The name "semisimple" might sound mysterious at this point. Our next aim is to explain that semisimple groups are, in some sense, closely related to simple linear algebraic groups.

Definition 11.1.4. Let G be a linear algebraic k-group.

(i) We call G *simple* if it is smooth, connected, non-commutative, and has no non-trivial proper normal subgroups.

(ii) We call G *almost-simple* if it is smooth, connected, non-commutative, and has no infinite proper normal subgroups.

(iii) We say that G is the *almost-direct product* of its closed subgroups $G_1, \ldots, G_r$ if the product map

$$G_1 \times \cdots \times G_r \to G \colon (g_1, \ldots, g_r) \mapsto g_1 \cdots g_r$$

is a surjective homomorphism with finite kernel. (In particular, the subgroups G_i are normal in G, and they pairwise commute.)

Clearly, an almost-direct product of almost-simple linear algebraic groups is semisimple. The converse is also true:

Theorem 11.1.5. *Let G be a semisimple linear algebraic group over an algebraically closed field k. Then G is an almost-direct product of its almost-simple closed subgroups, namely the minimal closed connected infinite normal subgroups of G. (These are called the* almost-simple factors *of G.)*

Proof omitted. □

Corollary 11.1.6. *Let G be a semisimple linear algebraic group over an algebraically closed field k. Then:*

(i) *Every quotient of G is semisimple.*

(ii) *If N is a smooth connected normal subgroup of G, then N is the product of the almost-simple factors contained in N, and is centralized by the remaining ones. In particular, N is semisimple.*

(iii) *G is perfect, i.e. $\mathcal{D}(G) = G$.*

(iv) *The center of G is a finite group of multiplicative type.*

Proof. Statements (i) and (ii) are immediate from Theorem 11.1.5. To prove (iii), it suffices to observe that $\mathcal{D}(H) = H$ for any almost-simple group H, which is obvious from the definitions. (Recall that $\mathcal{D}(H)$ is smooth and connected, and hence cannot be a non-trivial finite group.) Finally, to prove (iv), observe that[1] $Z(G)^\circ_{\mathrm{red}}$ is a closed smooth connected commutative normal subgroup of G, and hence $Z(G)^\circ_{\mathrm{red}} \leq R(G) = 1$, which shows that $Z(G)$ is a finite group. □

[1]When G is an algebraic group over an algebraically closed field k, which is not necessarily smooth, then we can smoothen it as in Remark 8.5.17 to obtain a closed subgroup G_{red} of G. (In general, G_{red} need not be normal in G!)

We now show that reductive groups are, in a precise sense, not too far away from semisimple groups.

Theorem 11.1.7. *Let G be a connected reductive linear algebraic group over an algebraically closed field k. Then*

$$R(G) = Z(G)^\circ_{\mathrm{red}} \quad \textit{and} \quad G = R(G)\mathcal{D}(G).$$

Moreover, $R(G) \cap \mathcal{D}(G)$ is finite, and $\mathcal{D}(G)$ is semisimple.

Proof. We will first show that $R(G) = Z(G)^\circ_{\mathrm{red}}$. Since $Z(G)^\circ_{\mathrm{red}}$ is a closed smooth connected commutative normal subgroup of G, it is certainly contained in $R(G)$. Conversely, the fact that G is reductive implies that $R(G)$ is a torus. Notice that G acts on $R(G)$ by conjugation. By rigidity of tori (see Theorem 9.3.4), this action is trivial, i.e. $R(G) \leq Z(G)$. Since $R(G)$ is smooth and connected, this implies $R(G) \leq Z(G)^\circ_{\mathrm{red}}$ and hence $R(G) = Z(G)^\circ_{\mathrm{red}}$.

Next, notice that $R(G)\mathcal{D}(G)$ is a normal subgroup of G. Then the group $G/R(G)\mathcal{D}(G)$ is a quotient of the commutative group $G/\mathcal{D}(G)$, and a quotient of the semisimple group $G/R(G)$; hence $G/R(G)\mathcal{D}(G)$ is a commutative semisimple group, which is therefore trivial. It follows that $G = R(G)\mathcal{D}(G)$.

Our next step is to show that $R(G) \cap \mathcal{D}(G)$ is finite. Write $T = R(G) = Z(G)^\circ_{\mathrm{red}}$, and notice that T is a diagonalizable subgroup of G. Consider a finite-dimensional faithful representation $G \hookrightarrow \mathsf{GL}_V$, and use Theorem 9.2.9 to write

$$V = \bigoplus_{\chi \in X(T)} V_\chi.$$

Since T is central in G, the elements of G stabilize each V_χ; hence there is an induced monomorphism

$$\alpha \colon G \to \mathsf{GL}(V_{\chi_1}) \times \cdots \times \mathsf{GL}(V_{\chi_r}),$$

where $\chi_1, \ldots, \chi_r$ are the characters of T for which $V_\chi \neq 0$. Hence

$$\alpha(\mathcal{D}(G)) \leq \mathsf{SL}(V_{\chi_1}) \times \cdots \times \mathsf{SL}(V_{\chi_r}).$$

On the other hand, by definition of the eigenspaces V_χ,

$$\alpha(T) \leq \mathsf{Sc}(V_{\chi_1}) \times \cdots \times \mathsf{Sc}(V_{\chi_r}),$$

where $\mathsf{Sc}(V_\chi)$ denotes the group of scalar matrices of $\mathsf{GL}(V_\chi)$. Since $\mathsf{SL}(V_\chi) \cap \mathsf{Sc}(V_\chi)$ is finite for each χ, it follows that $\alpha(T \cap \mathcal{D}(G))$ is finite, and since α is a monomorphism, this implies that $T \cap \mathcal{D}(G)$ is also finite.

We finally show that $\mathcal{D}(G)$ is semisimple. Notice that the homomorphism $\mathcal{D}(G) \to G/R(G)$ is surjective, and has finite kernel $R(G) \cap \mathcal{D}(G)$. Since $G/R(G)$ is semisimple, this implies that $\mathcal{D}(G)$ is semisimple as well. $\square$

Remark 11.1.8. In what follows, we will be mainly interested in reductive groups, and not just in semisimple groups. One of the reasons is that many naturally occuring groups, such as GL_n, are reductive but not semisimple. Another reason is that the centralizer of a torus in a semisimple group is usually not semisimple, but it is reductive again, and these centralizers are important subgroups for various reasons. See, for example, Proposition 11.2.8 below.

Recall that the rank of a smooth linear algebraic group over an algebraically closed field was defined to be the dimension of a maximal torus. For reductive groups, the following related notion is sometimes more natural.

Definition 11.1.9. Let G be a connected reductive linear algebraic group over an algebraically closed field k. Then the *semisimple rank* of G is defined to be the rank of its derived group $\mathcal{D}(G)$ (which is a semisimple group by Theorem 11.1.7).

Example 11.1.10. The rank of $G = \mathsf{GL}_n$ is equal to n, but its semisimple rank is equal to the rank of $\mathcal{D}(G) = \mathsf{SL}_n$, which is $n - 1$.

11.2 The root datum of a reductive group

To each reductive linear algebraic group (over an algebraically closed field k), we will attach a combinatorial object, called the root datum, which will determine G uniquely up to isomorphism. (More precisely, it will be associated to a pair (G, T), where G is a reductive group, and T is a maximal torus of G.) Before we introduce this combinatorial object, we recall the notion of characters, we introduce cocharacters, and we define a pairing between characters and cocharacters.

Definition 11.2.1. Let T be a torus over an algebraically closed field k.

(i) A *character* of T is a morphism $\chi\colon T \to \mathbb{G}_m$.

(ii) The *character group* of T is the free abelian group

$$X(T) \coloneqq \{\text{characters of } T\},$$

where the group addition is given by $(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$ for all $g \in T$.

(iii) A *cocharacter* of T is a morphism $\lambda\colon \mathbb{G}_m \to T$.

(iv) The *cocharacter group* of T is the free abelian group

$$Y(T) \coloneqq \{\text{cocharacters of } T\},$$

where the group addition is given by $(\lambda_1 + \lambda_2)(g) = \lambda_1(g)\lambda_2(g)$ for all $g \in T$.

(v) We define a *pairing*

$$\langle \cdot, \cdot \rangle \colon X(T) \times Y(T) \to \mathrm{End}(\mathbb{G}_m) \cong \mathbb{Z} \colon (\chi, \lambda) \mapsto \langle \chi, \lambda \rangle \coloneqq \chi \circ \lambda.$$

Hence for all $t \in \mathbb{G}_m(R) = R^\times$, we have $\chi(\lambda(t)) = t^{\langle \chi, \lambda \rangle}$.

Example 11.2.2. Let $T = \mathbb{D}_n$ be the group of invertible diagonal n-by-n matrices. Then $X(T)$ is a free abelian group of rank n, with basis $(\chi_1, \ldots, \chi_n)$, where

$$\chi_i \colon \mathbb{D}_n \to \mathbb{G}_m \colon \mathrm{diag}(a_1, \ldots, a_n) \mapsto a_i.$$

Similarly, $Y(T)$ is a free abelian group of rank n, with basis $(\lambda_1, \ldots, \lambda_n)$, where

$$\lambda_i \colon \mathbb{G}_m \to \mathbb{D}_n \colon t \mapsto \mathrm{diag}(1, \ldots, t, \ldots, 1)$$

(where the t is on the i-th position). The pairing between $X(T)$ and $Y(T)$ is then given by

$$\langle \chi_i, \lambda_j \rangle = \delta_{ij},$$

where δ_{ij} is the Kronecker delta.

We are now ready to introduce the notion of roots in a reductive linear algebraic group. In order to define it, we recall that a linear algebraic group G acts on its Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ through its adjoint representation

$$\mathrm{Ad} \colon G \to \mathsf{GL}_{\mathfrak{g}}.$$

Definition 11.2.3. Let G be a reductive linear algebraic group over an algebraically closed field k, and let T be a maximal torus in G. By Theorem 9.2.9, the Lie algebra $\mathfrak{g}$ has a decomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\chi \in X(T) \setminus \{0\}} \mathfrak{g}_\chi,$$

where

$$\mathfrak{g}_\chi = \{v \in \mathfrak{g} \mid g.v = \chi(g)v \text{ for all } g \in T\}$$

for all $\chi \in X(T)$; in particular,

$$\mathfrak{g}_0 = \{v \in \mathfrak{g} \mid g.v = v \text{ for all } g \in T\}$$

is the subspace of elements of $\mathfrak{g}$ fixed by T.

A *root* of (G,T) is defined to be a non-zero character $\chi \in X(T) \setminus \{0\}$ for which $\mathfrak{g}_\chi \neq 0$. Notice that the set of roots is a finite subset of $X(T)$, which we will denote by $R(G,T)$.

We will illustrate this concept with several examples. Notice that the set $R(G,T)$ is a subset of $X(T)$, which is a free abelian group of finite rank (say n); hence we can view it as a subset of the Euclidean space $\mathbb{R}^n$ through the isomorphism $X(T) \cong \mathbb{Z}^n \subset \mathbb{R}^n$, which will allow us to visualize the set of roots.

Examples 11.2.4. (1) Let $G = \mathsf{GL}_2$. Then $\mathfrak{g} = \mathfrak{gl}_2 = \mathrm{Mat}_2(k)$, with $[A,B] = AB - BA$. Consider the maximal torus

$$T = \left\{ \begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix} \mid x_1 x_2 \neq 0 \right\}.$$

Then $X(T) = \mathbb{Z}\chi_1 \oplus \mathbb{Z}\chi_2$, where

$$(a\chi_1 + b\chi_2).\begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix} = x_1^a x_2^b$$

for all $a, b \in \mathbb{Z}$. By the definition of the adjoint representation, T acts on $\mathfrak{g}$ by conjugation:

$$\begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1^{-1} & \\ & x_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{x_1}{x_2} b \\ \frac{x_2}{x_1} c & d \end{pmatrix}.$$

This shows that $\mathfrak{g}$ has a decomposition

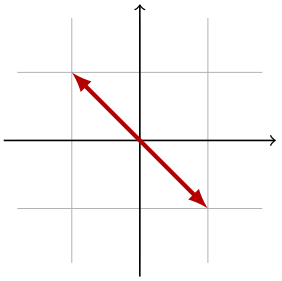
$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_{\chi_1 - \chi_2} \oplus \mathfrak{g}_{\chi_2 - \chi_1},$$

where $\dim \mathfrak{g}_0 = 2$ and $\dim \mathfrak{g}_{\chi_1-\chi_2} = \dim \mathfrak{g}_{\chi_2-\chi_1} = 1$. Hence

$$R(G,T) = \{\alpha, -\alpha\} \text{ where } \alpha = \chi_1 - \chi_2.$$

When we identify $X(T)$ with $\mathbb{Z}^2 \subset \mathbb{R}^2$, we get

$$R(G,T) = \{\pm(e_1 - e_2)\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2.$$



(2) Let $G = \mathsf{SL}_2$. Then $\mathfrak{g} = \mathfrak{sl}_2 = \{A \in \mathrm{Mat}_2(k) \mid \mathrm{tr}(A) = 0\}$. Consider the maximal torus

$$T = \left\{ \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix} \mid x \neq 0 \right\}.$$

Then $X(T) = \mathbb{Z}\chi$, where

$$(a\chi).\begin{pmatrix} x & \\ & x^{-1} \end{pmatrix} = x^a$$

for all $a \in \mathbb{Z}$. Again, T acts on $\mathfrak{g}$ by conjugation:

$$\begin{pmatrix} x & \\ & x^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} x^{-1} & \\ & x \end{pmatrix} = \begin{pmatrix} a & x^2 b \\ x^{-2} c & -a \end{pmatrix}.$$

This shows that $\mathfrak{g}$ has a decomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_{2\chi} \oplus \mathfrak{g}_{-2\chi},$$

where $\dim \mathfrak{g}_0 = 1$ and $\dim \mathfrak{g}_{2\chi} = \dim \mathfrak{g}_{-2\chi} = 1$. Hence

$$R(G,T) = \{\alpha, -\alpha\} \text{ where } \alpha = 2\chi.$$

When we identify $X(T)$ with $\mathbb{Z}^1 \subset \mathbb{R}^1$, we get

$$R(G,T) = \{\pm 2e_1\} \subset \mathbb{Z}^1 \subset \mathbb{R}^1.$$

(3) Let $G = \mathsf{PGL}_2 = \mathsf{GL}_2/\mathbb{G}_m$. Then $\mathfrak{g} = \mathfrak{gl}_2/\mathfrak{sc}_2$. Consider the maximal torus

$$T = \left\{ \begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix} \mid x_1 x_2 \neq 0 \right\} \ / \ \mathbb{G}_m.$$

Then $X(T) = \mathbb{Z}\chi$, where

$$(a\chi).\begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix} = \left(\frac{x_1}{x_2}\right)^a$$

for all $a \in \mathbb{Z}$. We compute the action of T on $\mathfrak{g}$ by conjugation:

$$\begin{pmatrix} x_1 & \\ & x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1^{-1} & \\ & x_2^{-1} \end{pmatrix} = \begin{pmatrix} a & \frac{x_1}{x_2} b \\ \frac{x_2}{x_1} c & d \end{pmatrix}.$$

This shows that $\mathfrak{g}$ has a decomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_{\chi} \oplus \mathfrak{g}_{-\chi},$$

where $\dim \mathfrak{g}_0 = 1$ and $\dim \mathfrak{g}_\chi = \dim \mathfrak{g}_{-\chi} = 1$. Hence

$$R(G,T) = \{\alpha, -\alpha\} \text{ where } \alpha = \chi.$$

When we identify $X(T)$ with $\mathbb{Z}^1 \subset \mathbb{R}^1$, we get

$$R(G,T) = \{\pm e_1\} \subset \mathbb{Z}^1 \subset \mathbb{R}^1.$$

(4) Let $G = \mathsf{GL}_n$. Then $\mathfrak{g} = \mathfrak{gl}_n = \mathrm{Mat}_n(k)$. Consider the maximal torus

$$T = \left\{ \begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix} \mid x_1 \cdots x_n \neq 0 \right\}.$$

Then $X(T) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_n$, where

$$(a_1\chi_1 + \cdots + a_n\chi_n).\begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix} = x_1^{a_1} \cdots x_n^{a_n}$$

for all $a_1, \ldots, a_n \in \mathbb{Z}$. We compute the action of T on $\mathfrak{g}$ by conjugation:

$$\begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1^{-1} & & \\ & \ddots & \\ & & x_n^{-1} \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & \frac{x_1}{x_n}a_{1n} \\ \vdots & \ddots & \vdots \\ \frac{x_n}{x_1}a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

(i.e. the matrix with as (i,j)-th entry $\frac{x_i}{x_j}a_{ij}$). This shows that $\mathfrak{g}$ has a decomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{i \neq j} \mathfrak{g}_{\chi_i - \chi_j}.$$

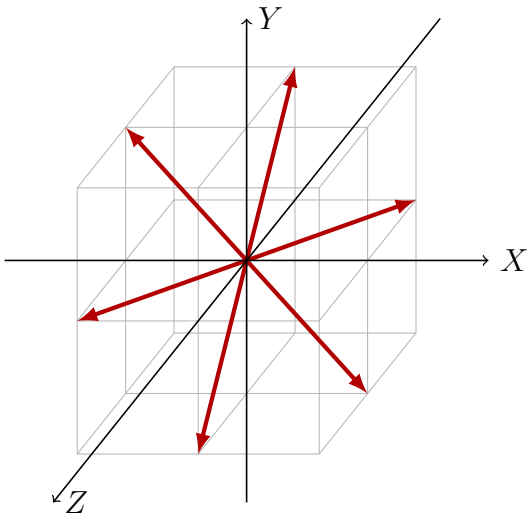
Notice that $\dim \mathfrak{g}_0 = n$ and $\dim \mathfrak{g}_{\chi_i - \chi_j} = 1$ for all $i \neq j$. Hence

$$R(G,T) = \{\chi_i - \chi_j \mid 1 \leq i, j \leq n, i \neq j\}.$$

When we identify $X(T)$ with $\mathbb{Z}^n \subset \mathbb{R}^n$, we get

$$R(G,T) = \{\pm(e_i - e_j) \mid 1 \leq i < j \leq n\} \subset \mathbb{Z}^n \subset \mathbb{R}^n.$$

For example, for $n = 3$, we get the following configuration:



Although the set of roots (which we will call a root system) already provides a lot of information about the group (it will determine the *type* of the algebraic group), we will need another piece of data to complete the picture. This is captured by the following definition. Notice that this definition is purely combinatorial and does not involve any reference to linear algebraic groups whatsoever.

Definition 11.2.5. A *root datum* is a quadruple

$$\Psi = (X, R, X^\vee, R^\vee),$$

where

- X and $X^\vee$ are free $\mathbb{Z}$-modules of finite rank, equipped with a bilinear pairing $\langle \cdot, \cdot \rangle \colon X \times X^\vee \to \mathbb{Z}$;
- R and $R^\vee$ are finite subsets of X and $X^\vee$, respectively, equipped with a bijection $\alpha \leftrightarrow \alpha^\vee$, such that:

  (i) $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in R$;

  (ii) $s_\alpha(R) \subseteq R$ for all $\alpha \in R$, where

  $$s_\alpha \colon X \to X \colon x \mapsto x - \langle x, \alpha^\vee \rangle \alpha;$$

  (iii) the *Weyl group*

  $$W(\Psi) \coloneqq \langle s_\alpha \mid \alpha \in R \rangle \leq \mathrm{Aut}(X)$$

  is a finite group.

A root datum is called *reduced* if $\alpha \in R$ implies $2\alpha \notin R$, or equivalently, if the only multiples of $\alpha \in R$ again contained in R are α and $-\alpha$.

To get a feeling for these objects, we will show a few properties of the maps s_α; they show that, in some sense, the s_α are (abstract) reflections.

Proposition 11.2.6. *Let $\Psi = (X, R, X^\vee, R^\vee)$ be a root datum, and $\alpha \in R$. Then:*

(i) $s_\alpha(\alpha) = -\alpha$;

(ii) $s_\alpha^2 = \mathrm{id}_X$;

(iii) $s_\alpha(x) = x$ *for all* x *such that* $\langle x, \alpha^\vee \rangle = 0$;

(iv) *If* $q \in \mathbb{Q}$ *is such that* $q\alpha \in R$, *then* $(q\alpha)^\vee = \frac{1}{q}\alpha^\vee$. *In particular,* $(-\alpha)^\vee = -\alpha^\vee$, *and hence* $s_\alpha = s_{-\alpha}$.

Proof. Notice that (i) and (iii) are obvious from the definitions. We will now show (ii). So let $x \in X$ be arbitrary; then

$$s_\alpha(s_\alpha(x)) = s_\alpha\big(x - \langle x, \alpha^\vee \rangle \alpha\big) = s_\alpha(x) - \langle x, \alpha^\vee \rangle s_\alpha(\alpha) \\ = x - \langle x, \alpha^\vee \rangle \alpha + \langle x, \alpha^\vee \rangle \alpha = x.$$

The last statement (iv) is more involved, and we will omit its proof. □

Our next goal is to attach a root datum to a given reductive linear algebraic group (together with a given maximal torus). We begin with a lemma.

Lemma 11.2.7. *Let G be a reductive linear algebraic group over an algebraically closed field k, and let T be a maximal torus in G. Then the action of the group $W(G,T) = N_G(T)/C_G(T)$ on $X(T)$ stabilizes the set $R(G,T)$ of roots.*

Proof. It follows from Theorem 9.3.2 that $W(G,T)$ acts on the set

$$M = \{\chi \in X(T) \mid \mathfrak{g}_\chi \neq 0\} = R(G,T) \cup \{0\}.$$

Since the elements of $N_G(T)$ stabilize the space $\mathfrak{g}_0$ of fixed vectors, we conclude that there is an induced action of $W(G,T)$ on $R(G,T)$. □

The following result will define the coroots.

Proposition 11.2.8. *Let G be a reductive linear algebraic group over an algebraically closed field k, and let T be a maximal torus in G. Let $X(T)$*

be the character group of T, let $Y(T)$ be the cocharacter group of T, and let $R = R(G,T) \subset X(T)$ be the set of roots. For each $\alpha \in R$, we let

$$T_\alpha \coloneqq \ker(\alpha)^\circ_{\mathrm{red}}, \quad G_\alpha \coloneqq C_G(T_\alpha).$$

Then $W(G_\alpha, T)$ contains a unique non-trivial element s_α, and there is a unique element $\alpha^\vee \in Y(T)$ such that

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha$$

for all $x \in X(T)$. Moreover, $\langle \alpha, \alpha^\vee \rangle = 2$.

Proof. We omit the proof. The crucial point is that G_α is a reductive group of semisimple rank 1 (see Definition 11.1.9). Since every semisimple group of rank 1 is isomorphic to either SL_2 or PGL_2, the other statements can then be shown by looking at each of these two cases separately. □

The cocharacter $\alpha^\vee$ is called the *coroot* of α, and the set of all coroots is denoted by $R^\vee(G,T)$.

To each root α, we can associate a so-called *root group* U_α:

Proposition 11.2.9. *Let G be a reductive linear algebraic group over an algebraically closed field k, let T be a maximal torus in G, and let $\alpha \in R(G,T)$ be a root. Then:*

(i) *There is a unique subgroup U_α of G isomorphic to $\mathbb{G}_a$, such that for each isomorphism $u_\alpha \colon \mathbb{G}_a \to U_\alpha$, we have*

$$t \cdot u_\alpha(x) \cdot t^{-1} = u_\alpha\big(\alpha(t)x\big),$$

for all $t \in T(k)$ and all $x \in k = \mathbb{G}_a(k)$.

(ii) *The group U_α is the unique subgroup of G normalized by T with Lie algebra $\mathfrak{g}_\alpha$.*

(iii) *Let $T_\alpha \coloneqq \ker(\alpha)^\circ_{\mathrm{red}}$ and $G_\alpha \coloneqq C_G(T_\alpha)$ as before. Then $G_\alpha = \langle T, U_\alpha, U_{-\alpha} \rangle$.*

Proof omitted. □

We have assembled all the necessary facts to prove that we can associate a root datum to any reductive group.

Theorem 11.2.10. *Let G be a reductive linear algebraic group over an algebraically closed field k, and let T be a maximal torus in G. Then*

$$\Psi(G,T) \coloneqq \big(X(T), R(G,T), Y(T), R^\vee(G,T)\big)$$

is a reduced root datum.

Proof. We already know that $X(T)$ and $Y(T)$ are free modules of equal rank, equipped with a pairing $\langle \cdot, \cdot \rangle$ (see Definition 11.2.1(v)), and that $R = R(G,T)$ and hence also $R^\vee = R^\vee(G,T)$ are finite. The fact that $\langle \alpha, \alpha^\vee \rangle = 2$ holds for each root α is contained in Proposition 11.2.8. The same proposition also shows that $s_\alpha \in W(G_\alpha, T) \leq W(G,T)$; since $W(G,T)$ stabilizes the set R by Lemma 11.2.7, this shows that $s_\alpha(R) \subseteq R$. Moreover, the fact that $W(G,T)$ is a finite group (see Theorem 9.3.2) shows that the group $\langle s_\alpha \mid \alpha \in R \rangle$ is also finite. (In fact, it coincides with $W(G,T)$, but it requires more effort to show this.) The fact that the root datum is always reduced, is somewhat more delicate, and we will omit its proof. □

Before we give examples, we mention the fundamental fact that a reductive linear algebraic group over an algebraically closed field k is completely determined by its root datum and the field k only.

Theorem 11.2.11. (i) *Let G be a reductive linear algebraic group over an algebraically closed field k, and let T and T' be two maximal tori in G. Then $\Psi(G,T)$ and $\Psi(G,T')$ are isomorphic.*

(ii) *Let k be an algebraically closed field. Each reduced root datum arises from a reductive linear algebraic group over k.*

(iii) *Let G and G' be two reductive linear algebraic groups over the same algebraically closed field k, and let T and T' be maximal tori in G and G', respectively. Assume that $\Psi(G,T)$ and $\Psi(G',T')$ are isomorphic root data. Then G and G' are isomorphic. More precisely, there is an isomorphism from G to G' mapping T to T'.*

Proof omitted. □

We now come to examples.

Examples 11.2.12. (1) Let $G = \mathsf{SL}_2$, and let T be as in Example 11.2.4(2). Then

$$\begin{aligned} X = X(T) &= \mathbb{Z}\chi && \text{with } \chi.\left(\begin{smallmatrix} x & \\ & x^{-1} \end{smallmatrix}\right) = x; \\ X^\vee = Y(T) &= \mathbb{Z}\lambda && \text{with } \lambda.t = \left(\begin{smallmatrix} t & \\ & t^{-1} \end{smallmatrix}\right); \\ R = R(G,T) &= \{\alpha, -\alpha\} && \text{with } \alpha = 2\chi; \\ R^\vee = R^\vee(G,T) &= \{\alpha^\vee, -\alpha^\vee\} && \text{with } \alpha^\vee = \lambda. \end{aligned}$$

Observe that $(\alpha \circ \alpha^\vee)(t) = (2\chi \circ \lambda)(t) = t^2$, so indeed $\langle \alpha, \alpha^\vee \rangle = 2$. We have $W(G,T) = W(\Psi) = \langle s_\alpha, s_{-\alpha} \rangle = \langle s_\alpha \rangle = \{1, s_\alpha\}$. Hence we can write

$$\Psi(\mathsf{SL}_2, T) \cong \big(\mathbb{Z}, \{-2, 2\}, \mathbb{Z}, \{-1, 1\}\big),$$

with $\langle x, y\rangle = xy$, and where $2 \overset{\vee}{\leftrightarrow} 1$ and $-2 \overset{\vee}{\leftrightarrow} -1$.
Notice that $\ker(\alpha)$ is a group of order 2; hence $T_\alpha = \ker(\alpha)^\circ_{\mathrm{red}} = 1$, and in particular $G_\alpha = G$. The unique non-trivial element s_α of $W(G_\alpha, T)$ is the image of $n_\alpha \coloneqq \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in N_G(T) \setminus C_G(T)$ in $W(G, T)$.
We claim that the root group U_α is given by

$$U_\alpha = \left\{ \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \;\middle|\; x \in k \right\}.$$

Consider the isomorphism

$$u_\alpha \colon \mathbb{G}_a \to U_\alpha \colon x \mapsto \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}.$$

(This is of course not the only isomorphism from $\mathbb{G}_a \to U_\alpha$, but the choice is irrelevant.) We check that the condition from Proposition 11.2.9 is satisfied. So let $t = \left(\begin{smallmatrix} s & \\ & s^{-1} \end{smallmatrix}\right)$ be arbitrary; then indeed

$$\begin{aligned} t \cdot u_\alpha(x) \cdot t^{-1} &= \begin{pmatrix} s & \\ & s^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} s^{-1} & \\ & s \end{pmatrix} = \begin{pmatrix} 1 & s^2 x \\ & 1 \end{pmatrix} \\ &= u_\alpha\big(s^2 x\big) = u_\alpha\big(\alpha(t) x\big) \end{aligned}$$

for all $x \in k$. Similarly, it can be checked that

$$U_{-\alpha} = \left\{ \begin{pmatrix} 1 & \\ x & 1 \end{pmatrix} \;\middle|\; x \in k \right\}.$$

Notice that $G = \langle T, U_\alpha, U_{-\alpha}\rangle$ by Proposition 11.2.9(ii); in fact, $G = \langle U_\alpha, U_{-\alpha}\rangle$ in this case.

(2) Let $G = \mathsf{PGL}_2$, and let T be as in Example 11.2.4(3). In this case, $\alpha = \chi$ and $\alpha^\vee = 2\lambda$, and we get

$$\Psi(\mathsf{PGL}_2, T) \cong \big(\mathbb{Z}, \{-1, 1\}, \mathbb{Z}, \{-2, 2\}\big),$$

with $\langle x, y\rangle = xy$, and where $1 \overset{\vee}{\leftrightarrow} 2$ and $-1 \overset{\vee}{\leftrightarrow} -2$.
Observe that the root systems of PGL_2 and SL_2 are isomorphic, but their root data are not.

(3) Let $G = \mathbb{G}_m$; then G is a torus, so we let $T = G$. Observe that G has no roots in this case. (The group G is reductive of rank 1, but has semisimple rank 0.) We have

$$\Psi(\mathbb{G}_m, T) \cong \big(\mathbb{Z}, \emptyset, \mathbb{Z}, \emptyset\big).$$

(4) Let $G = \mathsf{GL}_n$, and let T be as in Example 11.2.4(4). Define the characters χ_i and the cocharacters λ_i as in Example 11.2.2. Let

$$R = \{\alpha_{ij} \mid i \neq j\}, \quad \alpha_{ij} \coloneqq \chi_i - \chi_j;$$
$$R^\vee = \{\alpha_{ij}^\vee \mid i \neq j\}, \quad \alpha_{ij}^\vee \coloneqq \lambda_i - \lambda_j.$$

Notice that $\langle \alpha, \alpha^\vee \rangle = 2$ for every $\alpha \in R$. It is not too hard to check that

$$s_{\alpha_{ij}}(\chi_k) = \begin{cases} \chi_j & \text{if } k = i; \\ \chi_i & \text{if } k = j; \\ \chi_k & \text{if } k \neq i, j. \end{cases}$$

Hence $s_{\alpha_{ij}}$ acts on the basis $\{\chi_1, \ldots, \chi_n\}$ of X as the transposition (ij) on the set $\{1, \ldots, n\}$. This implies that

$$W = \langle s_\alpha \mid \alpha \in R \rangle \cong \mathrm{Sym}_n .$$

Observe that the groups $G_\alpha = C_G(T_\alpha)$ are isomorphic to $\mathsf{GL}_2 \times \mathbb{G}_m^{n-2}$; they have rank n but semisimple rank 1.
We now describe the root groups of G (w.r.t. T). For each $i \neq j$ and each $x \in k$, we write $E_{ij}(x)$ for the matrix with 1's on the diagonal, with x on position (i, j), and with 0's everywhere else. Let

$$U_{ij} \coloneqq \{E_{ij}(x) \mid x \in k\} .$$

Then it is quickly verified that U_{ij} is the root group corresponding to $U_{\alpha_{ij}}$, for each $i \neq j$. Notice that all the root groups U_{ij} with $i < j$ are upper triangular, while all the root groups U_{ij} with $i > j$ are lower triangular.

11.3 Classification of the root data

In this section, we want to present the classification of root data, mostly without proofs. To begin, we distinguish a few degenerate cases.

Definition 11.3.1. Let $\Psi = (X, R, X^\vee, R^\vee)$ be a root datum.

(i) We call Ψ a *toral* root datum if $R = R^\vee = \emptyset$.

(ii) We call Ψ a *semisimple* root datum if R generates a finite index subgroup of X.

The reason for this terminology can easily be guessed:

Proposition 11.3.2. *Let G be a reductive linear algebraic group over an algebraically closed field k, let T be a maximal torus in G, and let $\Psi = \Psi(G,T)$ be the corresponding root datum. Then*

(i) *Ψ is toral if and only if G is a torus;*

(ii) *Ψ is semisimple if and only if G is semisimple.*

Proof. We omit the proof. The key ingredient is the fact that the center of G coincides with the intersection $\bigcap_{\alpha \in R} \ker(\alpha)$. □

From now on, we focus on semisimple root data. The set of roots R already contains a lot of structure on its own, although it is not sufficient to recover the algebraic group uniquely up to isomorphism (as we have seen in the examples SL_2 vs. PGL_2). This additional structure of the set R is known as a root system.

Definition 11.3.3. (i) Let V be a finite-dimensional vector space over $\mathbb{Q}$. A subset R of V is called a *root system* in V, if:

(a) R is finite, spans V (as a vector space), and does not contain 0;

(b) For each $\alpha \in R$, there is a (unique) reflection s_α with vector α stabilizing the set R;

(c) For all $\alpha, \beta \in R$, the element $s_\alpha(\beta) - \beta$ is an integer multiple of α.

If in addition

(d) For each $\alpha \in R$, the only multiple of α which lies again in R is $-\alpha$,

then the root system is called *reduced*.

(ii) The *rank* of the root system is defined to be the dimension of V.

(iii) If $(V_1, R_1), \ldots, (V_n, R_n)$ are root systems, then the *direct sum* of these root systems is the root system $(V_1 \oplus \cdots \oplus V_n, R_1 \sqcup \cdots \sqcup R_n)$.

(iv) A root system is called *indecomposable* or *irreducible* if it cannot be written as the direct sum of root systems of lower rank.

Proposition 11.3.4. *Let $\Psi = (X, R, X^\vee, R^\vee)$ be a semisimple root datum. Then R is a root system in the $\mathbb{Q}$-vector space $X \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Proof. Notice that $0 \notin R$ because $\langle \alpha, \alpha^\vee \rangle = 2$ for all $\alpha \in R$. Moreover, for all $\alpha, \beta \in R$, we have $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$ because $\alpha^\vee \in X^\vee$, which shows that $s_\alpha(\beta) - \beta$ is an integer multiple of α. The fact that Ψ is a semisimple root system implies that R spans V as a vector space. The other facts are clear. □

Remark 11.3.5. As we already pointed out, the converse is more delicate, and there is *no unique* root datum that one can associate to a given root system. Instead, the following is true: if (V, R) is a root system (where V is a finite-dimensional $\mathbb{Q}$-vector space), then for any choice of a lattice X in V lying between the root lattice P and the weight lattice Q of (V, R), there is a unique semisimple root datum $\Psi = (X, R, X^\vee, R^\vee)$ w.r.t. the root system (V, R) and this choice of X. Since P has finite index in Q, there is only a finite number of choices for X and hence a finite number of root data associated to the given root system (V, R).

We have seen in Theorem 11.2.11 that the root datum of a reductive linear algebraic group over an algebraically closed field uniquely determines the group up to isomorphism. The root system does not determine the group uniquely, but it almost does.

Theorem 11.3.6. *Let G and G' be two reductive linear algebraic groups over the same algebraically closed field k, and let T and T' be maximal tori in G and G', respectively. Assume that $\Psi(G, T)$ and $\Psi(G', T')$ are root data with isomorphic root systems. Then G and G' are isogenous. More precisely, there is an isogeny from G to G' mapping T to T'.*

Proof omitted. □

The root systems have been classified, and this will associate a certain *type* to each reductive linear algebraic group. In order to describe the different root systems, we will need the notion of a base.

Definition 11.3.7. Let R be a root system in the $\mathbb{Q}$-vector space V. A subset $S \subset R$ is called a *base* for R if it is a basis for V, and if each root $\beta \in R$ can be written as $\beta = \sum_{\alpha \in S} m_\alpha \, \alpha$, where the m_α are integers of the same sign, i.e. either all $m_\alpha \geq 0$ or all $m_\alpha \leq 0$. Once a base has been fixed, we refer to the elements of the base as the *simple roots*.

It is a non-trivial fact that every root system has a base, but we will take this for granted.

Example 11.3.8. Consider the root system associated to $G = \mathsf{GL}_n$ as in Example 11.2.4(4), i.e.

$$R = \{e_i - e_j \mid 1 \leq i, j \leq n, i \neq j\}.$$

Then

$$S = \{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n\}$$

is a base for R. (Recall that V is the $\mathbb{Q}$-space spanned by R, which is the hyperplane $x_1 + x_2 + \cdots + x_n = 0$ inside $\mathbb{Q}^n$.)

The following fact greatly reduces the possibilities for a root system.

Proposition 11.3.9. *Let R be a root system in the $\mathbb{Q}$-vector space V, and let S be a base for R. Then:*

(i) *For any two distinct $\alpha, \beta \in S$, the angle between α and β is either $\pi/2$, $2\pi/3$, $3\pi/4$ or $5\pi/6$. Moreover,*

  (a) *If $\angle(\alpha, \beta) = 2\pi/3$, then $|\alpha| = |\beta|$;*

  (b) *If $\angle(\alpha, \beta) = 3\pi/4$, then $|\alpha|/|\beta| = \sqrt{2}$ or $1/\sqrt{2}$;*

  (c) *If $\angle(\alpha, \beta) = 5\pi/6$, then $|\alpha|/|\beta| = \sqrt{3}$ or $1/\sqrt{3}$.*

(ii) *The root system is completely determined, up to isomorphism, by the set S of simple roots, the length of each of the simple roots, and the angles between any two distinct simple roots.*

Proof omitted. □

The previous proposition will allow us to associate a diagram to each root system which encodes the necessary information to recover the root system completely.

Definition 11.3.10. Let R be a root system in the $\mathbb{Q}$-vector space V, and let S be a base for R. The *Dynkin diagram* of R is a graph with vertex set S, and where the edges can be either single, double or triple edges, depending on the following rule:

(a) When $\angle(\alpha, \beta) = \pi/2$, there is no edge between α and β;

(b) When $\angle(\alpha, \beta) = 2\pi/3$, there is a single edge between α and β;

(c) When $\angle(\alpha, \beta) = 3\pi/4$, there is a double edge between α and β;

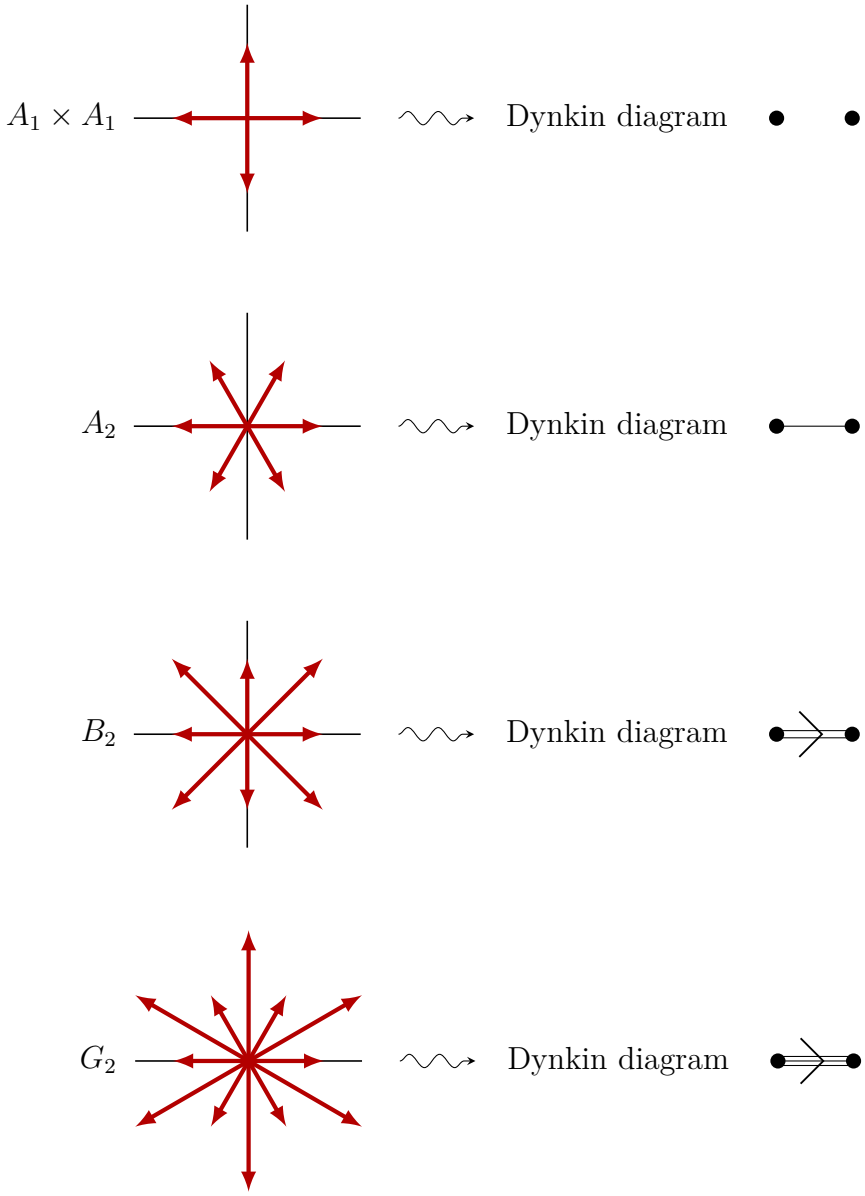
(d) When $\angle(\alpha, \beta) = 5\pi/6$, there is a triple edge between α and β.

Moreover, for each double or triple edge, we put an arrow pointing from the longest root towards the shortest root.

Remark 11.3.11. The Dynkin diagram of a root system R is a connected graph if and only if R is an irreducible root system.

It turns out that there are exactly four different reduced root systems of rank 2.

Proposition 11.3.12. *Let R be a root system of rank 2. Then R is one of the following:*

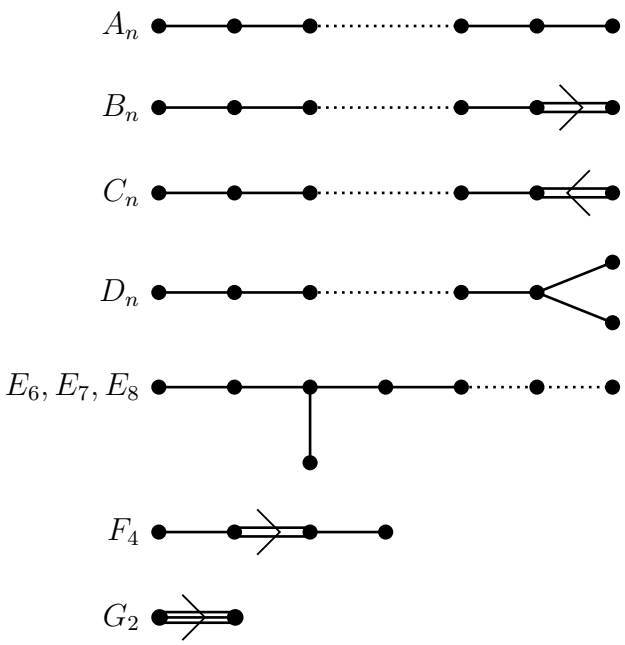


Proof omitted. □

We will now describe all irreducible root systems.

Theorem 11.3.13. *Let R be an irreducible root system of arbitrary rank.*

Then the Dynkin diagram of R is exactly one of the following.



Proof omitted. □

We can now reformulate our main result.

Theorem 11.3.14. *Let G be an almost simple linear algebraic group over an algebraically closed field k. Then up to isogeny, G is uniquely determined by the field k and the root system R of G (w.r.t. an arbitrary maximal torus in G). Its type is one of A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4 or G_2.*

Proof. Since G is almost simple, the root datum of G is semisimple, reduced, and irreducible. The result now follows from Theorem 11.3.6 and Theorem 11.3.13. □

Bibliography

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[CGP15] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, second edition, 2015.

[CP16] Brian Conrad and Gopal Prasad. *Classification of pseudo-reductive groups*, volume 191 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2016.

[Hum75] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits.

[McG10] Kevin McGerty. Algebraic groups. Personal lecture notes, 2010.

[Mil12a] James S. Milne. Basic theory of affine group schemes, 2012. Available at `www.jmilne.org/math`.

[Mil12b] James S. Milne. Lie algebras, algebraic groups, and lie groups, 2012. Available at `www.jmilne.org/math`.

[Mil12c] James S. Milne. Reductive groups, 2012. Available at `www.jmilne.org/math`.

[Mil17] James S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[MT11] Gunter Malle and Donna Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011.

[Spr09] Tonny A. Springer. *Linear algebraic groups*. Modern Birkhäuser Classics. Birkhäuser Boston Inc., Boston, MA, second edition, 2009.

[Sza12] Tamás Szamuely. Lectures on linear algebraic groups. `http://www.renyi.hu/~szamuely/lectures.html`, 2012.

[Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.