LECTURES ON LINEAR ALGEBRAIC GROUPS

TAMÁS SZAMUELY

This is a somewhat expanded version of the notes for courses given at the Eötvös and Technical Universities of Budapest in 2006, and at Central European University in 2012 and 2017. My aim was to provide a quick introduction to the main structural results for affine algebraic groups over algebraically closed fields with full proofs but assuming only a very modest background. The necessary techniques from algebraic geometry are developed from scratch along the way. In fact, some readers may regard the text as a good example of applying the basic theory of quasi-projective varieties in a nontrivial way.

The experts should be warned at once: there is almost no theorem here that cannot be found in the standard textbooks of Borel, Humphreys or Springer. There are some differences, however, in the exposition. We do not leave the category of quasi-projective varieties for a single moment, and carry a considerably lighter baggage of algebraic geometry than the above authors. Lie algebra techniques are not used either, except at the very end. Finally, for two of the main theorems we have chosen proofs that have been somewhat out of the spotlight for no apparent reason. Thus for Borel's fixed point theorem we present Steinberg's beautiful correspondence argument which reduces the statement to a slightly enhanced version of the Lie-Kolchin theorem, and for the conjugacy of maximal tori we give Grothendieck's proof from Séminaire Chevalley.

We work over an algebraically closed base field throughout. Linear algebraic groups over more general base fields are best treated using the theory of group schemes. For this approach (and much more) we refer the reader to Milne's forthcoming book [9] and Conrad's notes [5].

I thank Philippe Gille for helpful comments and corrections. All remaining errors are mine.

Contents

Chapter 1. Basic Notions

The concept of a linear algebraic group may be introduced in two equivalent ways. One is to define it as a subgroup of some general linear group GL_n which is closed for the Zariski topology. The other, more intrinsic approach is to say that a linear algebraic group is a group object in the category of affine varieties. In this chapter we develop the foundational material necessary for making the two definitions precise, and prove their equivalence. Some basic examples are also discussed.

1. Affine varieties

Throughout these notes we shall work over an *algebraically closed* field k. We identify points of *affine n-space* $\mathbf{A}^n_k$ with

$$\{(a_1, \ldots, a_n) : a_i \in k\}.$$

Given an ideal $I \subset k[x_1, \ldots, x_n]$, set

$$V(I) := \{P = (a_1, \ldots, a_n) \in \mathbf{A}^n : f(P) = 0 \quad \text{for all } f \in I\}.$$

Definition 1.1. *$X \subset \mathbf{A}^n$ is an* affine variety *if there exists an ideal $I \subset k[x_1, \ldots, x_n]$ for which $X = V(I)$.*

The above definition is not standard; a lot of textbooks assume that I is in fact a prime ideal.

According to the Hilbert Basis Theorem there exist finitely many polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ with $I = (f_1, \ldots, f_m)$. Therefore

$$V(I) = \{P = (a_1, \ldots, a_n) \in \mathbf{A}^n : f_i(P) = 0 \quad i = 1, \ldots, m\}.$$

The following lemma is easy.

Lemma 1.2. *Let $I_1, I_2, I_\lambda\,(\lambda \in \Lambda)$ be ideals in $k[x_1, \ldots, x_n]$. Then*
- $I_1 \subseteq I_2 \Rightarrow V(I_1) \supseteq V(I_2)$;
- $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$;
- $V(\langle I_\lambda : \lambda \in \Lambda \rangle) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$.

The last two properties imply that the affine varieties may be used to define the closed subsets in a topology on X (note that $\mathbf{A}^n = V(0)$, $\emptyset = V(1)$). This topology is called the *Zariski topology* on $\mathbf{A}^n$, and affine varieties are equipped with the induced topology.

Next another easy lemma.

Lemma 1.3. *The open subsets of the shape*

$$D(f) := \{P \in \mathbf{A}^n : f(P) \neq 0\},$$

where $f \in k[x_1, \ldots, x_n]$ is a fixed polynomial, form a basis of the Zariski topology on $\mathbf{A}^n$.

Now given an affine variety $X \subset \mathbf{A}^n$, set

$$I(X) := \{f \in k[x_1, \dots, x_n] : f(P) = 0 \text{ for all } P \in X\}.$$

Now arises the natural question: which ideals $I \subset k[x_1, \dots, x_n]$ satisfy $I(V(I)) = I$? An obvious necessary condition is that $f^m \in I$ should imply $f \in I$ for all $m > 0$, i.e. I should equal its *radical* $\sqrt{I}$. Such ideals are called *radical ideals*.

The condition is in fact sufficient:

Theorem 1.4. (Hilbert Nullstellensatz) $I = \sqrt{I} \Leftrightarrow I(V(I)) = I$.

According to the Noether-Lasker theorem, given an ideal I with $I = \sqrt{I}$, there exist *prime ideals* $P_1, \dots, P_r \subset k[x_1, \dots, x_n]$ satisfying $I = P_1 \cap \dots \cap P_r$. (Recall that an ideal I is a prime ideal if $ab \in I$ implies $a \in I$ or $b \in I$.) Since in this case $V(I) = \cup V(P_i)$, it is enough to prove the theorem in the case when I is a prime ideal.

This we shall do under the following additional condition:

$(*)$ There exists a subfield $F \subset k$ with tr.deg.$(k|F) = \infty$.

(Recall that this last condition means that there exist infinite systems of elements in k that are algebraically independent over F, i.e. there is no polynomial relation with F-coefficients among them.)

The condition $(*)$ is satisfied, for instance, for $k = \mathbf{C}$. See Remark 1.6 below on how to get rid of it.

Lemma 1.5. *Let $I \subset k[x_1, \dots, x_n]$ be a prime ideal, and $F \subset k$ a subfield satisfying $(*)$. Then there exists $P \in V(I)$ such that*

$$f \in F[x_1, \dots, x_n],\ f(P) = 0 \Rightarrow f \in I.$$

Proof. Choose a system of generators $f_1, \dots, f_m$ for I. By adjoining the coefficients of the f_i to F we may assume $f_i \in F[x_1, \dots, x_n]$ for all i without destroying the assumptions. Set $I_0 := I \cap F[x_1, \dots, x_n]$. This is again a prime ideal, so $F[x_1, \dots, x_n]/I_0$ is a finitely generated F-algebra which is an integral domain. Denoting by F_0 its fraction field, we have a finitely generated field extension $F_0|F$, so $(*)$ implies the existence of an F-embedding $\phi : F_0 \hookrightarrow k$. Denote by $\bar{x}_i$ the image of x_i in F_0 and set $a_i := \phi(\bar{x}_i)$, $P = (a_1, \dots, a_n)$. By construction $f_i(P) = 0$ for all i, so $P \in V(I)$, and for $f \in F[x_1, \dots, x_n] \setminus I_0$ one has $f(\bar{x}_1, \dots, \bar{x}_n) \neq 0$, and therefore $f(P) \neq 0$. □

Proof of the Nullstellensatz assuming $(*)$*:* Pick $f \in I(V(I))$ and $F \subset k$ satisfying $(*)$ such that $f \in F[x_1, \dots, x_n]$. If $f \notin I$, then for $P \in V(I)$ as in the above lemma one has $f(P) \neq 0$, which contradicts $f \in I(V(I))$. □

Remark 1.6. Here is how to eliminate $(*)$ using mathematical logic. If k does not satisfy $(*)$, let $\Omega = k^I/\mathcal{F}$ an *ultrapower* of k which is big enough to satisfy $(*)$. According to the Łoş lemma Ω is again algebraically closed, so the Nullstellensatz holds over it. Again by the Loş lemma we conclude that it holds over k as well.

Corollary 1.7. *The rule $I \mapsto V(I)$ is an order reversing bijection between ideals in $k[x_1, \dots x_n]$ satisfying $I = \sqrt{I}$ and affine varieties in $\mathbf{A}^n$. Maximal ideals correspond to points, so in particular each maximal ideal is of the form $(x_1 - a_1, \dots, x_n - a_n)$.*

Lemma 1.8. *$I \subset k[x_1, \dots, x_n]$ is a prime ideal if and only if $V(I)$ is an irreducible closed subset in $\mathbf{A}^n$.*

Recall that Z is an irreducible closed subset if there exists no decomposition $Z = Z_1 \cup Z_2$ with the Z_i closed and different from Z.

Proof. Look at the decomposition $I = P_1 \cap \dots \cap P_r$ given by the Noether-Lasker theorem. If I is not a prime ideal, then $r > 1$, whence a nontrivial decomposition $V(I) = \cup V(P_i)$. On the other hand, if $V(I) = Z_1 \cup Z_2$ nontrivially, then by the Nullstellensatz I is the nontrivial intersection of two ideals that equal their own radical, whence r must be > 1. □

Corollary 1.9. *Each affine variety X is a finite union of irreducible varieties X_i. Those X_i which are not contained in any other X_j are uniquely determined, and are called the* irreducible components *of X.*

Proof. In view of the lemma and the Nullstellensatz, this follows from the Noether-Lasker theorem. □

Example 1.10. For $I = (x_1 x_2) \subset k[x_1, x_2]$ one has

$$V(I) = V((x_1)) \cup V((x_2)).$$

Definition 1.11. *If X is an affine variety, the quotient*

$$\mathcal{A}_X := k[x_1, \dots, x_n]/I(X)$$

is called the coordinate ring *of X.*

Note that since $I(X)$ is a radical ideal, the finitely generated k-algebra $\mathcal{A}_X$ is *reduced*, i.e. it has no nilpotent elements.

The elements of $\mathcal{A}_X$ may be viewed as functions on X with values in k; we call them *regular functions*. Among these the images of the x_i are the restrictions of the coordinate functions of $\mathbf{A}^n$ to X, whence the name. Note that X is a variety if and only if $\mathcal{A}_X$ is *reduced* (i.e. has no nilpotents).

Definition 1.12. *Given an affine variety $X \subset \mathbf{A}^n$, by a* morphism *or* regular map *$X \to \mathbf{A}^m$ we mean an m-tuple $\phi = (f_1, \dots, f_m) \in \mathcal{A}_X^m$. Given an affine variety $Y \subset \mathbf{A}^m$, by a morphism $\phi : X \to Y$ we mean a morphism $\phi : X \to \mathbf{A}^m$ with $\phi(P) := (f_1(P), \dots, f_m(P)) \in Y$ for all $P \in X$.*

Lemma 1.13. *A morphism $\phi : X \to Y$ is continuous in the Zariski topology.*

Proof. It is enough to show that the preimage of each basic open set $D(f) \subset Y$ is open. This is true, because $\phi^{-1}(D(f)) = D(f \circ \phi)$, where $f \circ \phi \in \mathcal{A}_X$ is the regular function obtained by composition. □

Definition 1.14. *Given affine varieties $X \subset \mathbf{A}^n$, $Y \subset \mathbf{A}^m$, the Cartesian product $X \times Y \subset \mathbf{A}^n \times \mathbf{A}^m \cong \mathbf{A}^{n+m}$ is called the* product *of X and Y.*

Lemma 1.15. *The product $X \times Y \subset \mathbf{A}^{n+m}$ is an affine variety.*

Proof. If $X = V(f_1, \dots, f_r)$ and $Y = V(g_1, \dots, g_s)$, then

$$X \times Y = V(f_1, \dots, f_r, g_1, \dots, g_s).$$

□

2. Affine algebraic groups

Definition 2.1. *An* affine (or linear) algebraic group *is an affine variety G equipped with morphisms $m : G \times G \to G$ ('multiplication') and $i : G \to G$ ('inverse') satisfying the group axioms.*

Examples 2.2.

(1) The additive group $\mathbf{G}_a$ of k. As a variety it is isomorphic to $\mathbf{A}^1$, and $(x, y) \to (x + y)$ is a morphism from $\mathbf{A}^1 \times \mathbf{A}^1$ to $\mathbf{A}^1$.

(2) The multiplicative group $\mathbf{G}_m$ of k. As a variety, it is isomorphic to the affine hyperbola $V(xy - 1) \subset \mathbf{A}^2$.

(3) The subgroup of n-th roots of unity $\mu_n \subset \mathbf{G}_m$ for n invertible in k. As a variety, it is isomorphic to $V(x^n - 1) \subset \mathbf{A}^1$. It is *not* irreducible, not even connected (it consists of n distinct points).

(4) The group of invertible matrices GL_n over k is also an algebraic group (note that $\mathrm{GL}_1 = \mathbf{G}_m$). To see this, identify the set $M_n(k)$ of $n \times n$ matrices over k with points of $\mathbf{A}^{n^2}$. Then

$$\mathrm{GL}_n \cong \{(A, x) \in \mathbf{A}^{n^2+1} : \det(A)x = 1\}.$$

This is a closed subset, since the determinant is a polynomial in its entries.

(5) SL_n is also an algebraic group: as a variety,

$$\mathrm{SL}_n \cong \{A \in \mathbf{A}^{n^2} : \det(A) = 1\}.$$

Similarly, we may realise $\mathrm{O}_n, \mathrm{SO}_n$, etc. as affine algebraic groups.

Proposition 2.3. *Let G be an affine algebraic group.*

(1) *All connected components of G (in the Zariski topology) are irreducible. In particular, they are finite in number.*

(2) *The component G° containg the identity element is a normal subgroup of finite index, and its cosets are exactly the components of G.*

Proof. (1) Let $G = X_1 \cup \cdots \cup X_r$ be the decomposition of G into *irrreducible* components. As the decomposition is irredundant, $X_1 \not\subset X_j$ for $j \neq 1$, and therefore $X_1 \not\subset \cup_{j\neq 1} X_j$, as it is irreducible. Therefore there exists $x \in X_1$ not contained in any other X_j. But x may be transferred to any other $g \in G$ by the *homeomorphism* $y \mapsto gx^{-1}y$. This implies that there is a single X_j passing through g. Thus the X_j are pairwise disjoint, and hence equal the connected components.
(2) Since $y \mapsto gy$ is a homeomorphism for all $g \in G$, gG° is a whole component for all g. If here $g \in G^\circ$, then $g \in G^\circ \cap gG^\circ$ implies $gG^\circ = G^\circ$ and thus $G^\circ G^\circ = G^\circ$. Similarly $(G^\circ)^{-1} = G^\circ$ and $gG^\circ g^{-1} \subset G^\circ$ for all $g \in G$, so G is a normal subgroup, and the rest is clear. □

Remark 2.4. A finite connected group must be trivial. On the other hand, we shall see shortly that any finite group can be equipped with a structure of affine algebraic group.

Now we investigate the coordinate ring of affine algebraic groups. In general, if $\phi : X \to Y$ is a morphism of affine varieties, there is an induced k-algebra homomorphism $\phi^* : \mathcal{A}_Y \to \mathcal{A}_X$ given by $\phi^*(f) = f \circ \phi$.

Proposition 2.5. (1) *Given affine varieties X and Y, denote by* $\mathrm{Mor}(X, Y)$ *the set of morphisms $X \to Y$. Then the map $\phi \to \phi^*$ induces a bijection between* $\mathrm{Mor}(X, Y)$ *and* $\mathrm{Hom}(\mathcal{A}_Y, \mathcal{A}_X)$.
(2) *If A is a finitely generated reduced k-algebra, there exists an affine variety X with $A \cong \mathcal{A}_X$.*

Proof. (1) Choose an embedding $Y \hookrightarrow \mathbf{A}^m$, and let $\bar{x}_1, \ldots, \bar{x}_m$ be the coordinate functions on Y. Then $\phi^* \mapsto (\phi^*(\bar{x}_1), \ldots, \phi^*(\bar{x}_m))$ is an inverse for $\phi \mapsto \phi^*$.
(2) There exist $n > 0$ and an ideal $I \subset k[x_1, \ldots, x_n]$ with $I = \sqrt{I}$ and $A \cong k[x_1, \ldots, x_n]/I$. The Nullstellensatz implies that $X = V(I)$ is a good choice. □

Corollary 2.6. *The maps $X \to \mathcal{A}_X$, $\phi \to \phi^*$ induce an anti-equivalence between the category of affine varieties over k and that of finitely generated reduced k-algebras.*

We say that the affine varieties X and Y are *isomorphic* if there exist $\phi \in \mathrm{Mor}(X, Y)$, $\psi \in \mathrm{Mor}(Y, X)$ with $\phi \circ \psi = \mathrm{id}_Y$, $\psi \circ \phi = \mathrm{id}_X$. The affine variety X in Proposition 2.5 is unique up to isomorphism, but its embedding in affine space is by no means unique.

Corollary 2.7. *Let X and Y be affine varieties.*
(1) *X and Y are isomorphic as k-varietes if and only if $\mathcal{A}_Y$ and $\mathcal{A}_X$ are isomorphic as k-algebras.*
(2) *X is isomorphic to a closed subvariety of Y if and only if there exists a surjective homomorphism $\mathcal{A}_Y \to \mathcal{A}_X$.*

Proof. (1) is easy. For (2), note that by Lemma 1.2 (1) $X \subset Y$ closed implies $I(X) \supset I(Y)$, so that $I(X)$ induces an ideal $\bar{I} \subset \mathcal{A}_Y$, and there is a surjection $\mathcal{A}_Y \to \mathcal{A}_Y/\bar{I} \cong \mathcal{A}_X$. Conversely, given a surjection $\phi : \mathcal{A}_Y \to \mathcal{A}_X$, setting $I = \mathrm{Ker}\,(\phi)$ and $X' = V(I)$ we obtain $\mathcal{A}_{X'} \cong \mathcal{A}_X$, whence $X \cong X'$ by (1). $\square$

Lemma 2.8. *If X and Y are affine varieties, there is a canonical isomorphism $\mathcal{A}_{X\times Y} \cong \mathcal{A}_X \otimes_k \mathcal{A}_Y$.*

Proof. Define a map $\lambda : \mathcal{A}_X \otimes \mathcal{A}_Y \to \mathcal{A}_{X\times Y}$ by $\lambda(\Sigma f_i \otimes g_i) = \Sigma(f_i g_i)$. This is a surjective map, because the coordinate functions on $X \times Y$ are in the image (to see this, set f_i or g_i to 1), and they generate $\mathcal{A}_{X\times Y}$. For injectivity, assume $\Sigma f_i g_i = 0$, We may assume the f_i are linearly independent over k, but then $g_i(P) = 0$ for all i and $P \in Y$, so that $g_i = 0$ for all i by the Nullstellensatz. Hence $\Sigma f_i \otimes g_i = 0$. $\square$

Corollary 2.9. *For an affine algebraic group G the coordinate ring $\mathcal{A}_G$ carries the following additional structure:*

multiplication $m : G\times G \to G \leftrightarrow$ comultiplication $\Delta : \mathcal{A}_G \to \mathcal{A}_G \otimes_k \mathcal{A}_G$

$$\text{unit } \{e\} \to G \leftrightarrow \text{counit } e : \mathcal{A}_G \to k$$

$$\text{inverse } i : G \to G \leftrightarrow \text{coinverse } \iota : \mathcal{A}_G \to \mathcal{A}_G$$

These are subject to the following commutative diagrams.

$$\begin{tikzcd}
G\times G\times G \arrow[r, "\mathrm{id}\times m"] \arrow[d, "m\times\mathrm{id}"'] & G\times G \arrow[d, "m"] \\
G\times G \arrow[r, "m"] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{A}_G\otimes\mathcal{A}_G\otimes\mathcal{A}_G & \mathcal{A}_G\otimes\mathcal{A}_G \arrow[l, "\mathrm{id}\otimes\Delta"'] \\
\mathcal{A}_G\otimes\mathcal{A}_G \arrow[u, "\Delta\otimes\mathrm{id}"] & \mathcal{A}_G \arrow[l, "\Delta"'] \arrow[u, "\Delta"']
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "\mathrm{id}\times e"] \arrow[d, "e\times\mathrm{id}"'] \arrow[dr, "\mathrm{id}"] & G\times G \arrow[d, "m"] \\
G\times G \arrow[r, "m"] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{A}_G & \mathcal{A}_G\otimes\mathcal{A}_G \arrow[l, "\mathrm{id}\otimes e"'] \\
\mathcal{A}_G\otimes\mathcal{A}_G \arrow[u, "e\otimes\mathrm{id}"] & \mathcal{A}_G \arrow[l, "\Delta"'] \arrow[u, "\Delta"'] \arrow[ul, "\mathrm{id}"']
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "\mathrm{id}\times i"] \arrow[d, "i\times\mathrm{id}"'] \arrow[dr, "c"] & G\times G \arrow[d, "m"] \\
G\times G \arrow[r, "m"] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{A}_G & \mathcal{A}_G\otimes\mathcal{A}_G \arrow[l, "\mathrm{id}\otimes\iota"'] \\
\mathcal{A}_G\otimes\mathcal{A}_G \arrow[u, "\iota\otimes\mathrm{id}"] & \mathcal{A}_G \arrow[l, "\Delta"'] \arrow[u, "\Delta"'] \arrow[ul, "\gamma"']
\end{tikzcd}$$

where in the last diagram c is the constant map $G \to \{e\}$ and γ the composite $A \to k \to A$.

Definition 2.10. *A k-algebra equipped with the above additional structure is called a* Hopf algebra.

Corollary 2.11. *The maps $G \to \mathcal{A}_G$, $\phi \to \phi^*$ induce an anti-equivalence between the category of affine algebraic groups over k and that of finitely generated reduced Hopf algebras.*

Examples 2.12.

(1) *The Hopf algebra structure on $\mathcal{A}_{\mathbf{G}_a} = k[x]$ is given by $\Delta(x) = x \otimes 1 + 1 \otimes x$, $e(x) = 0$, $\iota(x) = -x$.*
(2) *The Hopf algebra structure on $\mathcal{A}_{\mathbf{G}_m} = k[x, x^{-1}]$ is given by $\Delta(x) = x \otimes x$, $e(x) = 1$, $\iota(x) = x^{-1}$.*
(3) *The Hopf algebra structure on $\mathcal{A}_{\mathrm{GL}_n} = k[x_{11}, \ldots, x_{nn}, \det(x_{ij})^{-1}]$ is given by $\Delta(x_{ij}) = \Sigma_l \, x_{il} \otimes x_{lj}$, $e(x_{ij}) = \delta_{ij}$ (Kronecker delta), $\iota(x_{ij}) = y_{ij}$, where $[y_{ij}] = [x_{ij}]^{-1}$.*

Remark 2.13. Given any k-algebra R, the Hopf algebra structure on $\mathcal{A}_G$ induces a group structure on $\mathrm{Hom}(\mathcal{A}_G, R)$. (In particular, we obtain the group structure on $\mathrm{Hom}(\mathcal{A}_G, k) \cong G(k)$ using the Nullstellensatz.) Therefore an affine algebraic group may also be defined as a functor G from the category of k-algebras to the category of groups for which there exists a finitely generated reduced k-algebra A with $G \cong \mathrm{Hom}(A, \ )$ as a *set-valued* functor. Dropping the additional assumptions on A we obtain the notion of an *affine group scheme* over k.

3. Embedding in GL_n

In this section we prove:

Theorem 3.1. *Each affine algebraic group is isomorphic to a closed subgroup of* GL_n *for appropriate $n > 0$.*

Because of this theorem affine algebraic groups are also called *linear algebraic groups.*

To give an idea of the proof, we first construct a closed embedding into GL_n for a finite group G. The regular representation is faithful, hence defines an embedding $G \to \mathrm{GL}(k[G])$, where $k[G]$ is the group algebra of G viewed as a k-vector space. The image of G is finite, hence Zariski closed.

For an arbitrary affine algebraic group the coordinate ring $\mathcal{A}_G$ could play the role of $k[G]$ in the above argument, but it is not finite dimensional. The idea is to construct a finite-dimensional G-invariant subspace.

Construction 3.2. For an affine algebraic group G the map $x \mapsto xg$ is an automorphism of G as an affine variety for all $g \in G$. Thus it induces a k-algebra automorphism $\rho_g : \mathcal{A}_G \to \mathcal{A}_G$. Viewing it as a k-vector space automorphism, we obtain a homomorphism $G \to \mathrm{GL}(\mathcal{A}_G)$ given by $g \mapsto \rho_g$.

Lemma 3.3. *Let $V \subset \mathcal{A}_G$ be a k-linear subspace.*

1. *$\rho_g(V) \subset V$ for all $g \in G$ if and only if $\Delta(V) \subset V \otimes_k \mathcal{A}_G$.*
2. *If V is finite dimensional, there is a finite-dimensional k-subspace $W \subset \mathcal{A}_G$ containing V with $\rho_g(W) \subset W$ for all $g \in G$.*

Proof. (1) Assume $\Delta(V) \subset V \otimes_k \mathcal{A}_G$. Then for $f \in V$ we find $f_i \in V$, $g_i \in \mathcal{A}_G$ with $\Delta(f) = \Sigma f_i \otimes g_i$. Thus $(\rho_g f)(h) = f(hg) = \Sigma f_i(h) g_i(g)$ for all $h \in G$, hence

$$\rho_g f = \sum g_i(g) f_i, \tag{1}$$

so $\rho_g f \in V$, since $f_i \in V$ and $g_i(g) \in k$. Conversely, assume $\rho_g(V) \subset V$ for all g. Let $\{f_i : i \in I\}$ be a basis of V, and let $\{g_j : j \in J\}$ be such that $\{f_i, g_j : i \in I, j \in J\}$ is a basis of $\mathcal{A}_G$. Since $\Delta(f) = \Sigma f_i \otimes u_i + \Sigma g_j \otimes v_j$ for some $u_i, v_j \in \mathcal{A}_G$, we obtain as above $\rho_g f(h) = \Sigma f_i(h) u_i(g) + \Sigma g_j(h) v_j(g)$. By assumption here $v_j(g)$ must be 0 for all $g \in G$, thus $v_j = 0$ for all j.
(2) By writing V as a sum of 1-dimensional subspaces it is enough to consider the case dim $(V) = 1$, $V = \langle f \rangle$. Choosing f_i as in formula (1) above, the formula implies that the finite-dimensional subspace W' generated by the f_i contains the $\rho_g f$ for all $g \in G$. Thus the subspace $W := \langle \rho_g f : g \in G \rangle \subset W'$ meets the requirements. □

Remark 3.4. The lemma holds in a more general setting. Namely, one says that an affine algebraic group G acts on an affine variety X if there is a morphism $G \times X \to X$ of affine varieties satisfying the usual axioms for group actions. Each $g \in G$ then induces a k-algebra automorphism $\rho_g : \mathcal{A}_X \to \mathcal{A}_X$. The same proof as in the case $X = G$ above shows that the statements of the lemma hold for subspaces $V \subset \mathcal{A}_X$.

Proof of Theorem 3.1: Let V be the finite-dimensional k-subspace of $\mathcal{A}_G$ generated by a finite system of k-*algebra* generators of $\mathcal{A}_G$. Applying part (2) of the lemma we obtain a k-subspace W invariant under the ρ_g which still generates $\mathcal{A}_G$. Let $f_1, \ldots, f_n$ be a k-basis of W. By part (1) of the lemma we find elements $a_{ij} \in \mathcal{A}_G$ with

$$\Delta(f_i) = \Sigma_j f_j \otimes a_{ij} \text{ for all } 1 \leq i \leq n.$$

It follows that

$$\rho_g(f_i) = \Sigma_j a_{ij}(g) f_j \text{ for all } 1 \leq i \leq n,\ g \in G. \tag{2}$$

Thus $[a_{ij}(g)]$ is the matrix of ρ_g in the basis $f_1, \ldots, f_n$. Define a morphism $\Phi : G \to \mathbf{A}^{n^2}$ by $(a_{11}, \ldots, a_{nn})$. Since the matrices $[a_{ij}(g)]$ are invertible, its image lies in GL_n, and moreover it is a group homomorphism by construction. The k-algebra homomorphism $\Phi^* : \mathcal{A}_{\mathrm{GL}_n} \to \mathcal{A}_G$ (see Example 2.12 (3)) is defined by sending x_{ij} to a_{ij}. Since $f_i(g) = \Sigma_j f_j(1) a_{ij}(g)$ for all $g \in G$ by (2), we have $f_i = \Sigma_j f_j(1) a_{ij}$, and therefore Φ^* is surjective, because the f_i generate $\mathcal{A}_G$. So by Corollary

2.7 (2) and Proposition 2.5 (1) Φ embeds G as a closed subvariety in GL_n, thus as a closed subgroup. □

4. Sharpenings of the embedding theorem

Later we shall also need more refined versions of the embedding theorem. The first of these is:

Corollary 4.1. *Let G be an affine algebraic group, H a closed subgroup. Then there is a closed embedding $G \subset \mathrm{GL}(W)$ for some finite-dimensional W such that H equals the stabilizer of a subspace $W_H \subset W$.*

Proof. Let I_H be the ideal of functions vanishing on H in $\mathcal{A}_G$. In the above proof we may arrange that some of the f_i form a system of generators for I_H. Put $W_H := W \cap I_H$. Observe that

$$g \in H \Leftrightarrow hg \in H \text{ for all } h \in H \Leftrightarrow \rho_g(I_H) \subset I_H \Leftrightarrow \rho_g(W_H) \subset W_H,$$

whence the corollary. □

Next a classical trick of Chevalley which shows that the subspace W_H of the previous corollary can be chosen 1-dimensional.

Lemma 4.2. (Chevalley) *Let G be an affine algebraic group, H a closed subgroup. Then there is a morphism of algebraic groups $G \to \mathrm{GL}(V)$ for some finite-dimensional V such that H is the stabilizer of a 1-dimensional subspace L in the induced action of G on V.*

Proof. Apply Corollary 4.1 to obtain an embedding $G \subset \mathrm{GL}(V)$ such that H is the stabilizer of a subspace $V_H \subset V$. Let $d = \dim V_H$. We claim that H is the stabilizer of the 1-dimensional subspace $L := \Lambda^d(V_H)$ in $\Lambda^d(V)$ equipped with its natural G-action (which is defined by setting $g(v_1 \wedge \cdots \wedge v_d) = g(v_1) \wedge \cdots \wedge g(v_d)$ for $g \in G$). Indeed, H obviously stabilizes L. For the converse, let $g \in G$ be an element stabilizing L. We may choose a basis $e_1, \ldots, e_n$ of V in such a way that $e_1, \ldots, e_d$ is a basis of V_H and moreover $e_{m+1}, \ldots, e_{m+d}$ is a basis of gV_H. We have to show $m = 0$, for then $gV_H = V_H$ and $g \in H$. If not, then $e_1 \wedge \cdots \wedge e_d$ and $e_{m+1} \wedge \cdots \wedge e_{m+d}$ are linearly independent in $\Lambda^d(V)$. On the other hand, we must have $e_1 \wedge \cdots \wedge e_d, e_{m+1} \wedge \cdots \wedge e_{m+d} \in L$ since g stabilizes L, a contradiction. □

Based on Chevalley's lemma we can finally prove:

Proposition 4.3. *If $H \subset G$ is a closed normal subgroup, there exists a finite-dimensional vector space W and a morphism $\rho : G \to \mathrm{GL}(W)$ of algebraic groups with kernel H.*

Proof. Again start with a representation $\phi : G \to \mathrm{GL}(V)$, where H is the stabilizer of a 1-dimensional subspace $\langle v \rangle$ as in Lemma 4.2. In other words, v is a common eigenvector of the $h \in H$. Let V_H be the span of all common eigenvectors of the $h \in H$ in V. Pick $h \in H$ and a common eigenvector v of H. Then $hv = \chi(h)v$, where $\chi(h) \in k^\times$ is a constant depending on h (in fact $\chi : H \to \mathbf{G}_m$ is a character of H, but we shall not use this). Since $H \subset G$ is normal, we have

$$hgv = g(g^{-1}hg)v = g(\chi(g^{-1}hg)v) = \chi(g^{-1}hg)gv.$$

As h was arbitrary, we conclude that $gv \in V_H$. So V_H is G-invariant, and we may as well assume $V_H = V$. Thus V is the *direct* sum of the finitely many common eigenspaces $V_1, \ldots, V_n$ of H.

Let $W \subset \mathrm{End}(V)$ be the subspace of endomorphisms that leave each V_i invariant; it is the direct sum of the $\mathrm{End}(V_i)$. There is an action of G on $\mathrm{End}(V)$ by $g(\lambda) = \phi(g) \circ \lambda \circ \phi(g)^{-1}$. This action stabilizes W, because if V_i is a common eigenspace for H, then so is $\phi(g)^{-1}(V_i)$ because H is normal, and is therefore preserved by λ. We thus obtain a morphism $\rho : G \to \mathrm{GL}(W)$ of algebraic groups.

It remains to show $H = \mathrm{Ker}\,(\rho)$. As W is the direct sum of the $\mathrm{End}(V_i)$ and each $h \in H$ acts on V_i by scalar multiplication, we have $\phi(h) \circ \lambda \circ \phi(h)^{-1} = \lambda$ for all $\lambda \in W$, i.e. $H \subset \mathrm{Ker}\,(\rho)$. Conversely, $g \in \mathrm{Ker}\,(\rho)$ means that $\phi(g)$ lies in the center of W, which is the direct sum of the centers of the $\mathrm{End}(V_i)$. Thus g acts on each V_i by scalar multiplication. In particular, it preserves the 1-dimensional subspace $\langle v \rangle$, i.e. it lies in H. $\square$

Chapter 2. Jordan Decomposition and Triangular Form

The embedding theorem of the last chapter enables us to apply linear algebra techniques to the study of affine algebraic groups. The first main result of this kind will be a version of Jordan decomposition which is independent of the embedding into GL_n. In the second part of the chapter we discuss three basic theorems that show that under certain assumptions one may put all elements of some matrix group simultaneously into triangular form. The strongest of these, the Lie-Kolchin theorem, concerns connected solvable subgroups of GL_n. As an application of this theorem one obtains a strong structural result for connected nilpotent groups. In the course of the chapter we also describe diagonalizable groups, i.e. commutative groups that can be embedded in GL_n as closed subgroups of the diagonal subgroup.

5. Jordan decomposition

The results of the last section allow us to apply linear algebra techniques in the study of affine algebraic groups. For instance, since k is algebraically closed, in a suitable basis each endomorphism ϕ of an n-dimensional vector space has a matrix that is in *Jordan normal form.* Recall that this means that if $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of ϕ, the matrix of ϕ is given by blocks along the diagonal that have the form

$$\begin{bmatrix} \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{bmatrix}.$$

We shall generalise this result to affine algebraic groups *independently* of the embedding into GL_n. First some definitions.

Definition 5.1. *Let V be a finite-dimensional vector space. An element $g \in \mathrm{End}(V)$ is* semisimple *(or diagonalizable) if V has a basis consisting of eigenvectors of g. The endomorphism g is* nilpotent *if $g^m = 0$ for some $m > 0$.*

Remark 5.2. Recall from linear algebra that g is semisimple if and only if its minimal polynomial has distinct roots. Consequently, if $W \subset V$ is a g-invariant subspace and g is semisimple, then so is $g|_W$ (because the minimal polynomial of $g|_W$ divides that of g). This fact will be repeatedly used in what follows.

The above statement about matrices can be restated (in a slightly weaker form) as follows:

Proposition 5.3. (Additive Jordan decomposition) *Let V be a finite-dimensional vector space, $g \in \mathrm{End}(V)$.*

There exist elements $g_s, g_n \in \mathrm{End}(V)$ with g_s semisimple, g_n nilpotent, $g = g_s + g_n$ and $g_s g_n = g_n g_s$.

Proof. In the basis yielding the Jordan form define g_s by the diagonal of the matrix. $\square$

One has the following additional properties.

Proposition 5.4.

(1) *The elements $g_s, g_n \in \mathrm{End}(V)$ of the previous proposition are uniquely determined.*
(2) *There exist polynomials $P, Q \in k[T]$ with $P(0) = Q(0) = 0$ and $g_s = P(g)$, $g_n = Q(g)$.*
(3) *If $W \subset V$ is a g-invariant subspace, it is invariant for g_s and g_n as well. Moreover, $(g|_W)_s = g_s|_W$ and $(g|_W)_n = g_n|_W$.*

Proof. (1) Let

$$\Phi(T) := \det(T \cdot \mathrm{id}_V - g) = \prod (T - \lambda_i)^{n_i}$$

the characteristic polynomial of g, and set

$$V_i := \{v \in V : (g - \lambda_i)^{n_i} v = 0\}.$$

This is a g-invariant subspace corresponding to the i-th Jordan block of g. By construction $g_s|_{V_i} = \lambda_i \mathrm{id}_{V_i}$.

Now assume $g = g'_s + g'_n$ is another Jordan decomposition. Since $gg'_s = g'_s g$, we have $g'_s(g - \lambda_i \mathrm{id}) = (g - \lambda_i \mathrm{id})g'_s$, which implies $g'_s(V_i) \subset V_i$ for all i. Since $g - g'_s = g'_n$ is nilpotent, all eigenvalues of $g'_s|_{V_i}$ are equal to λ_i, but then $g'_s|_{V_i} = \lambda_i \mathrm{id}_{V_i}$ as g'_s is semisimple (and hence so is $g'_s|_{V_i}$ – see the above remark). Thus $g_s = g'_s$.
(2) The Chinese Remainder Theorem for polynomial rings gives a direct sum decomposition

$$k[T]/(\Phi) \cong \bigoplus_i k[T]/((T - \lambda_i)^{n_i}),$$

so we find $P \in k[T]$ with $P \equiv \lambda_i \bmod (T - \lambda_i)^{n_i}$ for all i. By construction $P(g) = g_s$, and so $(T - P)(g) = g_n$. If $\Phi(0) = 0$, then 0 is an eigenvalue of g, and so $P \equiv 0 \bmod T$, i.e. $P(0) = 0$. Otherwise, adding a suitable constant multiple of Φ to P if necessary, we may assume $P(0) = 0$. Now set $Q = T - P$.
The first part of (3) immediately follows from (2). Moreover, as the characteristic polynomial of $g|_W$ divides Φ, $(g|_W)_s = P(g|_W) = g_s|_W$ is a good choice; the statement for $(g|_W)_n$ follows from this. $\square$

Definition 5.5. *An endomorphism $h \in \mathrm{End}(V)$ is* unipotent *if $h - \mathrm{id}_V$ is nilpotent (equivalently, if all eigenvalues of h are 1).*

Corollary 5.6. (Multiplicative Jordan decomposition) *Let V be a finite-dimensional vector space, $g \in \mathrm{GL}(V)$.*

(1) *There exist uniquely determined elements* $g_s, g_u \in \mathrm{GL}(V)$ *with* g_s *semisimple,* g_u *unipotent, and* $g = g_s g_u = g_u g_s$.
(2) *There exist polynomials* $P, R \in k[T]$ *with* $P(0) = R(0) = 0$ *and* $g_s = P(g)$, $g_u = R(g)$.
(3) *If* $W \subset V$ *is a* g*-invariant subspace, it is invariant for* g_s *and* g_u *as well. Moreover,* $(g|_W)_s = g_s|_W$ *and* $(g|_W)_u = g_u|_W$.

Proof. Since $g \in \mathrm{GL}(V)$, its eigenvalues are nonzero, hence so are those of the g_s defined in the above proof. Thus g_s is invertible, and $g_u = \mathrm{id}_V + g_s^{-1} g_n$ will do for (1). Then to prove (2) it is enough to see by the proposition that g_s^{-1} is a polynomial in g_s, and hence in g. This is clear, because if $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is the minimal polynomial of g_s (note that $a_0 \neq 0$), we have $-a_0^{-1} g_s^{n-1} - a_0^{-1} a_{n-1} g_s^{n-2} - \cdots - a_0^{-1} a_1 = g_s^{-1}$. Statement (3) follows from (2) as above. □

We now consider an infinite-dimensional generalisation.

Definition 5.7. Let V be a not necessarily finite dimensional vector space and fix $g \in \mathrm{GL}(V)$. Assume that V is a union of finite-dimensional g-invariant subspaces. We say that g is *semisimple (resp. locally unipotent)* if $g|_W$ is semisimple (resp. unipotent) for all finite-dimensional g-invariant subspaces W.

Note that if G is an affine algebraic group, then for all $g \in G$ the action of the 'right translation' $\rho_g \in \mathrm{GL}(\mathcal{A}_G)$ on $\mathcal{A}_G$ satisfies the finiteness condition of the definition by Lemma 3.3 (2).

Corollary 5.8. *Let* V *be a not necessarily finite-dimensional vector space,* $g \in \mathrm{GL}(V)$. *Assume that* V *is a union of finite-dimensional* g*-invariant subspaces.*

(1) *There exist uniquely determined elements* $g_s, g_u \in \mathrm{GL}(V)$ *with* g_s *semisimple,* g_u *locally unipotent, and* $g = g_s g_u = g_u g_s$.
(2) *If* $W \subset V$ *is a* g*-invariant subspace, it is invariant for* g_s *and* g_u *as well, and* $(g|_W)_s = g_s|_W$, $(g|_W)_u = g_u|_W$.

Proof. Using the third statement of the last corollary and the unicity statement of part (1) we may 'glue the $(g|_W)_s$ and $(g|_W)_u$ together' to obtain the required g_s and g_u, whence the first statement. The second one follows from part (3) of the last corollary, once we have remarked that W is also a union of finite-dimensional g-invariant subspaces. □

In the case $V = \mathcal{A}_G$ equipped with the right action of G via the $\rho_g \in \mathrm{GL}(\mathcal{A}_G)$ the corollary implies that a unique decomposition $\rho_g = (\rho_g)_s(\rho_g)_u$ exists.

Theorem 5.9. *Let* G *be an affine algebraic group.*

(1) *There exist uniquely determined* $g_s, g_u \in G$ *with* $g = g_s g_u = g_u g_s$ *and* $\rho_{g_s} = (\rho_g)_s$, $\rho_{g_u} = (\rho_g)_u$.

(2) *In the case $G = \mathrm{GL}_n$ the elements g_s and g_u are the same as those of Corollary 5.6.*
(3) *For each embedding $\phi : G \to \mathrm{GL}_n$ we have $\phi(g_s) = \phi(g)_s$ and $\phi(g_u) = \phi(g)_u$.*

Definition 5.10. *We call $g \in G$* semisimple (resp. unipotent) *if $g = g_s$ (resp. $g = g_u$).*

The following lemma already proves part (2) of the theorem.

Lemma 5.11. *Let V be a finite-dimensional vector space. An element $g \in \mathrm{GL}(V)$ is semisimple (resp. unipotent) if and only if $\rho_g \in \mathrm{GL}(\mathcal{A}_{\mathrm{GL}(V)})$ is semisimple (resp. locally unipotent).*

Proof. Recall that $\mathcal{A}_{\mathrm{GL}(V)} \cong k[\mathrm{End}(V), 1/D]$, where $D = \det(x_{ij})$ with $x_{11}, \dots, x_{nn}$ the standard basis of $\mathrm{End}(V) \cong M_n(k)$. Right multiplication by g acts not only on $\mathrm{GL}(V)$, but also on $\mathrm{End}(V) \cong \mathbf{A}^{n^2}$, whence another induced map $\rho_g \in \mathrm{GL}(\mathcal{A}_{\mathrm{End}(V)})$. Pick a function $f \in \mathcal{A}_{\mathrm{End}(V)}$. We claim that fD^{-m} is an eigenvector for ρ_g on $\mathcal{A}_{\mathrm{GL}(V)}$ for all m if and only if f is an eigenvector for ρ_g on $\mathcal{A}_{\mathrm{End}(V)} = k[\mathrm{End}(V)]$. Indeed, regarding fD^{-m} as a function on $\mathrm{GL}(V)$ we have

$$(3)\quad \rho_g(fD^{-m})(x) = f(xg)D^{-m}(x)D^{-m}(g) = D^{-m}(g)(\rho_g(f)D^{-m})(x),$$

where $D^m(g) = \det(g)^m$ for all $m \geq 0$.

Thus ρ_g is semisimple on $\mathcal{A}_{\mathrm{GL}(V)}$ if and only if it is semisimple on $\mathcal{A}_{\mathrm{End}(V)}$. The same holds with 'semisimple' replaced by 'locally unipotent'. (Indeed, note that the formula $\rho_g(D) = D(g)D$ implies that D is an eigenvector for ρ_g, so if ρ_g is unipotent, $D(g) = 1$ and (3) yields 'if'; the converse is trivial.)

By the above it is enough to prove the lemma for $\mathcal{A}_{\mathrm{GL}(V)}$ replaced by the polynomial ring $\mathcal{A}_{\mathrm{End}(V)}$. Observe that

$$\mathcal{A}_{\mathrm{End}(V)} \cong k[x_{11}, \dots, x_{nn}] \cong \mathit{Sym}(\mathrm{End}(V)^\vee),$$

where $\vee$ denotes the dual vector space and

$$\mathit{Sym}(\mathrm{End}(V)^\vee) := \bigoplus_{m=0}^{\infty} (\mathrm{End}(V)^\vee)^{\otimes m} / \langle x \otimes y - y \otimes x \rangle.$$

The action of ρ_g on $\mathrm{End}(V)^\vee$ is given by $(\rho_g f)(x) = f(xg)$, and the action on $\mathcal{A}_{\mathrm{End}(V)}$ is induced by extending this action to $\mathit{Sym}(\mathrm{End}(V)^\vee)$. If $\phi \in \mathrm{End}(V)$ is semisimple or unipotent, then so is $\phi^{\otimes m}$ for all m, so using the fact that $\mathrm{End}(V)^\vee$ is the direct summand of degree 1 in $\mathit{Sym}(\mathrm{End}(V)^\vee)$ we see that ρ_g is semisimple (resp. unipotent) on $\mathrm{End}(V)^\vee$ if and only if it is semisimple (resp. locally unipotent) on $\mathcal{A}_{\mathrm{End}(V)}$. Thus we are reduced to showing that $g \in \mathrm{GL}(V)$ is semisimple (resp. unipotent) if and only if ρ_g is semisimple (resp. unipotent) on $\mathrm{End}(V)^\vee$. This is an exercise in linear algebra left to the readers. $\square$

Proof of Theorem 5.9: Note first that part (2) of the Theorem is an immediate consequence of the above lemma in view of the unicity of the decompositions $g = g_s g_u$ and $\rho_g = (\rho_g)_s(\rho_g)_u$. Next take an embedding $\phi : G \to GL(V)$. For all $g \in G$ the diagram

$$\begin{array}{ccc} \mathcal{A}_{GL(V)} & \xrightarrow{\phi^*} & \mathcal{A}_G \\ {\scriptstyle \rho_{\phi(g)}}\big\downarrow & & \big\downarrow{\scriptstyle \rho_g} \\ \mathcal{A}_{GL(V)} & \xrightarrow{\phi^*} & \mathcal{A}_G \end{array}$$

commutes.

Now there is a unique Jordan decomposition $\phi(g) = \phi(g)_s\phi(g)_u$ in $\mathrm{GL}(V)$. We claim that it will be enough to show for (1) and (3) that $\phi(g)_s, \phi(g)_u \in \phi(G)$. Indeed, once we have proven this, we may define g_s (resp. g_u) to be the unique element in G with $\phi(g_s) = \phi(g)_s$ (resp. $\phi(g_u) = \phi(g)_u$). Since (1) holds for $G = \mathrm{GL}(V)$ by the previous lemma, the above diagram for g_s and g_u in place of g then implies that it holds for G as well. Statement (3) now follows by the unicity statement of (1) and the diagram above.

It remains to prove $\phi(g)_s, \phi(g)_u \in \phi(G)$. Setting $I := \mathrm{Ker}\,(\phi^*)$, observe that for $\bar{g} \in \mathrm{GL}(V)$

$$\bar{g} \in \phi(G) \Leftrightarrow h\bar{g} \in \phi(G) \text{ for all } h \in \phi(G) \Leftrightarrow \rho_{\bar{g}}(I) \subset I, \tag{4}$$

since I consists of the functions vanishing on G. In particular, $\rho_{\phi(g)}$ preserves I, hence so do $(\rho_{\phi(g)})_s$ and $(\rho_{\phi(g)})_u$ by Corollary 5.8 (2). On the other hand, by the lemma above $(\rho_{\phi(g)})_s = \rho_{\phi(g)_s}$ and $(\rho_{\phi(g)})_u = \rho_{\phi(g)_u}$. But then from (4) we obtain $\phi(g)_s, \phi(g)_u \in \phi(G)$, as required.□

We conclude with the following complement.

Corollary 5.12. *Let $\psi : G \to G'$ be a morphism of algebraic groups. For each $g \in G$ we have $\psi(g_s) = \psi(g)_s$ and $\psi(g_u) = \psi(g)_u$.*

Proof. Write G'' for the closure of $\mathrm{Im}\,(\psi)$ in G' (we shall prove later that $\mathrm{Im}\,(\phi) \subset G'$ is in fact closed). It suffices to treat the morphisms $\psi_1 : G \to G''$ and $\psi_2 : G'' \to G'$ separately.

As ψ_1 has dense image, the induced map $\psi_1^*(\mathcal{A}_{G''}) \to \mathcal{A}_G$ is injective, and its image identifies with a ρ_g-invariant subspace of $\mathcal{A}_G$ (ρ_g acting on $\mathcal{A}_{G''}$ via $\rho_{\psi_1(g)}$ like in the diagram above). Now apply Corollary 5.8 (2) to this subspace.

To treat ψ_2, choose an embedding $\phi : G' \to \mathrm{GL}_n$, and apply part (3) of the theorem to ϕ and $\phi \circ \psi_2$. The statement follows from the unicity of Jordan decomposition. □

6. Unipotent groups

In the next three sections we shall prove three theorems about putting elements of matrix groups simultaneously into triangular form. In terms of vector spaces this property may be formulated as follows. In an n-dimensional vector space V call a strictly increasing chain $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V$ of subspaces a *complete flag*. Then finding a basis of V in which the matrix of all elements of a subgroup $G \subset \mathrm{GL}(V)$ is upper triangular is equivalent to finding a complete flag of G-invariant subspaces in V.

We call a subgroup of an affine algebraic group *unipotent* if it consists of unipotent elements.

Proposition 6.1. (Kolchin) *For each unipotent subgroup $G \subset \mathrm{GL}(V)$ there exists a complete flag of G-invariant subspaces in V.*

The following proof uses some basic facts from representation theory (see e.g. Lang, Algebra, Chapter XVII).

Proof. By induction on the dimension n of V it will suffice to show that V has a nontrivial G-invariant subspace. Assume not. Then V is an irreducible representation of G, hence a simple n-dimensional $k[G]$-module. By Schur's lemma $D = \mathrm{End}_{k[G]}(V)$ is a division algebra over k, hence $D = k$ because k is algebraically closed (and each $\alpha \in D \setminus k$ would generate a commutative subfield of finite degree). But then by the Jacobson density theorem the natural map $k[G] \to \mathrm{End}_k(V) = \mathrm{End}_D(V)$ is surjective. In other words, the elements of G generate $\mathrm{End}_k(V)$ as a k-vector space. Each element $g \in G$ has trace n because the trace of a nilpotent matrix is 0 and $g - 1$ is nilpotent. It follows that for $g, h \in G$ $Tr(gh) = Tr(g)$, or in other words $Tr((g-1)h) = 0$. Since the $h \in G$ generate $\mathrm{End}_k(V)$, we obtain $Tr((g-1)\phi) = 0$ for all $\phi \in \mathrm{End}_k(V)$. Fixing a basis of V and applying this to those ϕ whose matrix has a single nonzero entry we see that this can only hold for $g = 1$. But g was arbitrary, so $G = 1$, in which case all subspaces are G-invariant, and we obtain a contradiction. □

Corollary 6.2. *Each unipotent subgroup $G \subset \mathrm{GL}_n$ is conjugate to a subgroup of U_n, the group of upper triangular matrices with 1's in the diagonal.*

Proof. This follows from the proposition, since all eigenvalues of a unipotent matrix are 1. □

Corollary 6.3. *A unipotent algebraic group is nilpotent, hence solvable (as an abstract group).*

Recall that a group G is nilpotent if in the chain of subgroups

$$G = G^0, G^1 = [G, G], \ldots, G^i = [G, G^{i-1}], \ldots$$

we have $G^n = \{1\}$ for some n. It is solvable if in the chain of subgroups

$$G = G^{(0)}, G^{(1)} = [G, G], \ldots, G^{(i)} = [G^{(i-1)}, G^{(i-1)}], \ldots$$

we have $G^{(n)} = \{1\}$ for some n.

Proof. A subgroup of a nilpotent group is again nilpotent, so by the previous corollary it is enough to see that the group U_n is nilpotent. This is well-known (and easy to check). □

7. Commutative groups

We begin the study of commutative linear algebraic groups with the following well-known statement.

Lemma 7.1. *For each set S of pairwise commuting endomorphisms of a finite-dimensional vector space V, there is a complete flag of S-invariant subspaces of V. If all elements of S are semisimple, there is a basis of V consisting of common eigenvectors of the elements in S.*

Proof. The lemma is easy if all elements in S act by scalar multiplications. Otherwise there is $s \in S$ that has a nontrivial eigenspace $V_\lambda \subsetneq V$. For all $t \in S$ and $v \in V_\lambda$ one has $stv = tsv = \lambda tv$, i.e. $tv \in V_\lambda$, so V_λ is S-invariant. The first statement then follows by induction on dimension. For the second, choose s and V_λ as above, and let W be the direct sum of the other eigenspaces of s. As above, both V_λ and W are stable by S, and we again conclude by induction on dimension (using Remark 5.2). □

Given an affine algebraic group G, write G_s (resp. G_u) for the set of its semisimple (resp. unipotent) elements. Note that G_u is always a closed subset, for applying the Cayley-Hamilton theorem after embedding G into some GL_n we see that all elements $g \in G_u$ satisfy equation $(g-1)^n = 0$, which implies n^2 polynomial equations for their matrix entries. The subset G_s is not closed in general.

Theorem 7.2. *Let G be a* commutative *affine algebraic group. Then the subsets G_u and G_s are closed subgroups of G, and the natural map $G_s \times G_u \to G$ is an isomorphism of algebraic groups.*

Proof. We may assume that G is a closed subgroup of some $\mathrm{GL}(V)$. The second statement of the previous lemma shows that in this case G_s is a subgroup, and its first statement implies that G_u is a subgroup as well (since a triangular unipotent matrix has 1-s in the diagonal). Now use the second statement again to write V as a direct sum of the *common* eigenspaces V_λ of the elements in G_s. Each V_λ is G-invariant (again by the calculation $stv = tsv = \lambda tv$), so applying the first statement of the lemma to each of the V_λ we find a closed embedding of G into GL_n in which all elements map to upper triangular matrices and all semisimple elements to diagonal ones. This shows in particular that $G_s \subset G$ is closed (set the off-diagonal entries of a triangular matrix to 0), and for G_u we know it already. The group homomorphism $G_s \times G_u \to G$ is injective since $G_s \cap G_u = \{1\}$, and surjective by the Jordan decomposition. It is also a morphism of affine varieties, so it remains to see that the inverse map is a morphism as well. The same argument that proves the closedness of G_s shows that the map $g \mapsto g_s$ given by Jordan decomposition is a morphism, hence so is $g \mapsto g_u = g_s^{-1}g$ and finally $g \mapsto (g_s, g_u)$. □

We now investigate commutative semisimple groups. By the above these are closed subgroups of some group D_n of diagonal matrices with invertible entries, hence they are also called *diagonalizable* groups. Another standard terminology is *groups of multiplicative type.* A diagonalizable group is called a *torus* if it is actually isomorphic to some D_n, and hence to the direct power $\mathbf{G}_m^n$.

Obviously, direct products of the form $\mathbf{G}_m^r \times \mu_{m_1} \times \dots \mu_{m_n}$ can be embedded as closed subgroups in a direct power of $\mathbf{G}_m$ and hence are diagonalizable. We now show that there are no others. For this we need the notion of the *character group.* Given a not necessarily commutative algebraic group G, a *character* of G is a morphism of algebraic groups $G \to \mathbf{G}_m$. These obviously form an abelian group, denoted by $\widehat{G}$. Moreover, the map $G \mapsto \widehat{G}$ is a contravariant functor: each morphism $G \to H$ of algebraic groups induces a group homomorphism $\widehat{H} \to \widehat{G}$ by composition.

Proposition 7.3. *If G is diagonalizable, then $\widehat{G}$ is a finitely generated abelian group having no elements of order* $\mathrm{char}\,(k)$.

The proof uses the following famous lemma.

Lemma 7.4. (Dedekind) *Let G be an abstract group, k a field and $\phi_i : G \to k^\times$ group homomorphisms for $1 \le i \le m$. Then the ϕ_i are linearly independent in the k-vector space of functions from G to k.*

Proof. Assume $\Sigma\lambda_i\phi_i = 0$ is a linear relation with $\lambda_i \in k^\times$ that is of minimal length. Then $\Sigma\lambda_i\phi_i(gh) = \Sigma\lambda_i\phi_i(g)\phi_i(h) = 0$ for all $g, h \in G$. Fixing g with $\phi_1(g) \neq \phi_i(g)$ for some i (this is always possible after a possible renumbering) and making h vary we obtain another linear relation $\Sigma\lambda_i\phi_i(g)\phi_i = 0$. On the other hand, multiplying the initial relation by $\phi_1(g)$ we obtain $\Sigma\lambda_i\phi_1(g)\phi_i = 0$. The difference of the two last relations is nontrivial and of smaller length, a contradiction. □

Next recall from Example 2.2(2) that $\mathcal{A}_{\mathbf{G}_m} \cong k[T, T^{-1}]$, with the Hopf algebra structure determined by $\Delta(T) = T \otimes T$. It follows that any character $\chi : G \to \mathbf{G}_m$ is determined by the image of T by χ^*, which should satisfy $\Delta(\chi^*(T)) = \chi^*(T) \otimes \chi^*(T)$. Thus we have proven:

Lemma 7.5. *The map $\chi \mapsto \chi^*(T)$ induces a bijection between $\widehat{G}$ and the set of elements $x \in \mathcal{A}_G$ satisfying $\Delta(x) = x \otimes x$.*

The elements $x \in \mathcal{A}_G$ with $\Delta(x) = x \otimes x$ are called *group-like elements.* The two previous lemmas imply:

Corollary 7.6. *The group-like elements are k-linearly independent in $\mathcal{A}_G$.*

Proof of Proposition 7.3: In the case $G = \mathbf{G}_m$ a group-like element in $\mathcal{A}_{\mathbf{G}_m}$ can only be T^n for some $n \in \mathbf{Z}$ (for instance, by the above corollary), so $\widehat{\mathbf{G}_m} \cong \mathbf{Z}$. Next we have $\widehat{\mathbf{G}_m^n} \cong \widehat{\mathbf{G}_m}^n \cong \mathbf{Z}^n$ and also $\mathcal{A}_{\mathbf{G}_m^n} \cong k[T, T^{-1}]^{\otimes n} \cong k[T_1, T_1^{-1}, \ldots, T_n, T_n^{-1}]$ using Lemma 2.8. If $\phi : G \to \mathbf{G}_m^n$ is a closed embedding, the induced surjection $\phi^* : k[T_1, T_1^{-1}, \ldots, T_n, T_n^{-1}] \to \mathcal{A}_G$ is a map of Hopf algebras, so in particular it sends group-like elements to group like ones. Since the elements $T_1^{m_1} \ldots T_n^{m_n}$ are group-like and span $\mathcal{A}_{\mathbf{G}_m^n}$ as a k-vector space, the $\phi^*(T_1^{m_1} \ldots T_n^{m_n})$ must span $\mathcal{A}_G$. But then by the previous corollary a group-like element in $\mathcal{A}_G$ should be one of the $\phi^*(T_1^{m_1} \ldots T_n^{m_n})$, so the natural map $\mathbf{Z}^n = \widehat{\mathbf{G}_m^n} \to \widehat{G}$ is surjective. Finally, if $\mathrm{char}\,(k) = p > 0$ and $\chi \in \widehat{G}$ has order dividing p, then $\chi^p(g) = \chi(g)^p = 1$ for all $g \in G$, but since $k^\times$ has no p-torsion, $\chi(g) = 1$ and so $\chi = 1$. □

In the course of the above proof we have also proven:

Corollary 7.7. *The group-like elements form a k-basis of $\mathcal{A}_G$.*

Now we can prove.

Theorem 7.8. *The functor $G \to \widehat{G}$ induces an anti-equivalence of categories between diagonalizable algebraic groups over k and finitely generated abelian groups having no elements of order* $\mathrm{char}\,(k)$*. Here tori correspond to free abelian groups.*

Proof. Construct a functor in the reverse direction as follows. Given a finitely generated abelian group $\widehat{G}$ as in the theorem, consider the group algebra $k[\widehat{G}]$. Equip it with a Hopf algebra structure by declaring the elements of $\widehat{G}$ to be group-like and take the associated affine group $\widetilde{G}$. This construction is contravariantly functorial and for $\widehat{G} = \mathbf{Z}^n$ gives $\widetilde{G} = \mathbf{G}_m^n$. In the general case a surjection $\mathbf{Z}^n \twoheadrightarrow \widehat{G}$ induces a closed embedding $\widetilde{G} \hookrightarrow \mathbf{G}_m^n$, so we get a diagonalizable group whose character group is $\widehat{G}$ by construction. On the other hand, if G is diagonalizable, we have an isomorphism of k-vector spaces $\mathcal{A}_G \cong k[\widehat{G}]$ by the previous corollary. It is also a Hopf algebra isomorphism as it is so for $\mathbf{G}_m^n$ and we may take Hopf algebra surjections $\mathcal{A}_{\mathbf{G}_m^n} \twoheadrightarrow \mathcal{A}_G$, $k[\mathbf{Z}^n] \twoheadrightarrow k[\widehat{G}]$ in the general case. □

Remark 7.9. The above theory is more interesting over non-algebraically closed fields. In this case the character group has an extra structure: the action of the absolute Galois group of the base field. In fact, the theorem above can be generalized as follows: the functor $G \to \widehat{G}$ realizes an anti-equivalence of categories between diagonalizable groups over a perfect field k (i.e. algebraic groups defined over k that become diagonalizable over an algebraic closure $\bar{k}$) and finitely generated abelian groups equipped with a continuous action of $\mathrm{Gal}\,(\bar{k}|k)$.

As an example, consider $k = \mathbf{R}$ and tori with character group $\mathbf{Z}$. Here $\mathrm{Gal}\,(\mathbf{C}|\mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z}$ and there are two possible actions of $\mathbf{Z}/2\mathbf{Z}$ on $\mathbf{Z}$, sending 1 to 1 and -1, respectively. The first case corresponds to $\mathbf{G}_m$ over $\mathbf{R}$ and the second case to the circle group: the affine $\mathbf{R}$-variety with equation $x^2 + y^2 = 1$ where the group structure comes from identifying the $\mathbf{R}$-points with complex numbers of absolute value 1 (this is also the group SO_2 over $\mathbf{R}$). If we now consider $\mathbf{Q}$ in place of $\mathbf{R}$, we get many different actions of $\mathrm{Gal}\,(\overline{\mathbf{Q}}|\mathbf{Q})$ on $\mathbf{Z}$ corresponding to different quadratic extensions of $\mathbf{Q}$. These correspond to tori over $\mathbf{Q}$ with equation $x^2 - ay^2 = 1$ where $a \in \mathbf{Q}^\times \setminus \mathbf{Q}^{\times 2}$.

8. The Lie-Kolchin theorem

We now come to the third main triangularisation theorem. In the special case when G is a connected solvable complex Lie group it was proven by Lie.

Theorem 8.1. (Lie-Kolchin) *Let V be a finite-dimensional k-vector space and $G \subset \mathrm{GL}(V)$ a connected solvable subgroup. Then there is a complete flag of G-invariant subspaces in V.*

Remarks 8.2.

(1) This is not really a theorem about algebraic groups, for we have not assumed that G is closed. It is just a connected subgroup equipped with the induced topology which is solvable as an abstract group. In the case when G is also closed, we shall see later (Corollary 16.6) that the commutator subgroup $[G, G]$ is closed as well (this is not true in general when G is not connected!), so all subgroups G^i in the finite commutator series of G are closed connected algebraic subgroups, by Lemma 8.3 below.

(2) The converse of the theorem also holds, even without assuming G connected: if there is a complete G-invariant flag, then G is solvable (because the group of upper triangular matrices is).

(3) However, the connectedness assumption is necessary even for closed subgroups, as the following example shows. Let $G \subset \mathrm{GL}_2(k)$ be the group of matrices with a single nonzero entry in each row and column. It is not connected but a closed subgroup, being the union of the diagonal subgroup D_2 with the closed subset A_2 of invertible matrices with zeros in the diagonal. It is also solvable, because D_2 is its identity component and $G/\mathrm{D}_2 \cong \mathbf{Z}/2\mathbf{Z}$. The only common eigenvectors for D_2 are of the form $\begin{pmatrix} a \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ a \end{pmatrix}$, but these are not eigenvectors for the matrices in A_2. Thus there is no common eigenvector for G.

Lemma 8.3. *If G is a connected topological group, then the commutator subgroup $[G, G]$ is connected as well.*

Proof. Write ϕ_i for the map $G^{2i} \to G$ sending $(x_1, \ldots, x_i, y_1, \ldots y_i)$ to $[x_1, y_1] \ldots [x_i, y_i]$. Since G is connected, so is $\mathrm{Im}\,(\phi_i)$. Thus $\mathrm{Im}\,(\phi_1) \subset \mathrm{Im}\,(\phi_2) \subset \ldots$ is a chain of connected subsets and $[G, G]$ is their union, hence it is connected. □

Proof of Theorem 8.1: By induction on $\dim V$ it suffices to show that the elements of G have a common eigenvector v, for then the image of G in $\mathrm{GL}(V/\langle v\rangle)$ is still connected and solvable, and thus stabilizes a complete flag in $V/\langle v\rangle$ whose preimage in V yields a complete flag together with $\langle v\rangle$. We may also assume that V is an irreducible $k[G]$-module, i.e. there is no nontrivial G-invariant subspace in V, for if V' were one, we would find a common eigenvector by looking at the image of G in $\mathrm{GL}(V')$, again by induction on dimension.

We now use induction on the smallest i for which $G^i = \{1\}$. By Lemma 8.3 $[G, G]$ is a connected normal subgroup in G with $[G, G]^{i-1} = \{1\}$, so by induction its elements have a common eigenvector. Write W for the span of *all* common eigenvectors of $[G, G]$ in V. We claim that $W = V$. By the irreducibility of V for this it is enough to see that W is G-invariant, which follows from the normality of $[G, G]$ by the same argument as at the beginning of the proof of Proposition 4.3.

We conclude that there is a basis of V in which the matrix of each $h \in [G, G]$ is diagonal. This holds in particular for the conjugates $g^{-1}hg \in [G, G]$ with $g \in G$, and thus conjugation by g corresponds to a permutation of the finitely many common eigenvalues of the $g^{-1}hg$. In particular, each $h \in [G, G]$ has a finite conjugacy class in G. In other words, for fixed $h \in [G, G]$ the map $G \to G, g \mapsto g^{-1}hg$ has finite image. Since G is connected and the map is continuous, it must be constant. This means that $[G, G]$ is contained in the center of G.

Next observe that each $h \in [G, G]$ must act on V via multiplication by some $\lambda \in k^\times$. Indeed, if V_λ is a nontrivial eigenspace of h with eigenvalue λ, it must be G-invariant since h is central in G, but then $V_\lambda = V$ by irreducibility of V. On the other hand, h is a product of commutators, so its matrix has determinant 1. All in all, the matrix should be of the form $\omega \cdot \mathrm{id}$, where ω is a $\dim V$-th root of unity. In particular, $[G, G]$ is finite, but it is also connected, hence $[G, G] = 1$ and G is commutative. We conclude by Lemma 7.1. □

Corollary 8.4. *If G is connected and solvable, then G_u is a closed normal subgroup of G.*

Proof. By the theorem we find an embedding $G \subset \mathrm{GL}_n$ so that the elements of G map to upper triangular matrices. Then $G_u = G \cap \mathrm{U}_n$, and moreover it is the kernel of the natural morphism of algebraic groups $G \to \mathrm{D}_n$, where D_n is the subgroup of diagonal matrices. So G_u is a closed normal subgroup. □

In contrast, G_s need not be a subgroup in general. However, this is so in the nilpotent case, where much more is true.

Theorem 8.5. *Let G be a connected nilpotent affine algebraic group. Then the subsets G_u and G_s are closed normal subgroups of G, and the natural map $G_s \times G_u \to G$ is an isomorphism of algebraic groups.*

Proof. We shall prove that $G_s \subset Z(G)$, for then everything will follow as in the proof of Theorem 7.2: G_s is a subgroup as its elements commute (Lemma 7.1), so if $G \subset \mathrm{GL}(V)$ and V_λ is a common eigenspace for G_s, it is G-invariant as $G_s \subset Z(G)$, and hence by applying the Lie–Kolchin theorem to each V_λ we get an embedding $G \subset \mathrm{GL}_n$ in which G maps to the upper triangular subgroup and G_s to the diagonal subgroup. Hence $G_s \subset G$ is a closed central subgroup and the rest follows from Jordan decomposition as in the proof of Theorem 7.2.

Now assume $G_s \not\subset Z(G)$, and choose $g \in G_s$ and $h \in G$ that do not commute. Embed G into some $\mathrm{GL}(V)$, and apply the Lie-Kolchin theorem to find a complete flag of G-invariant subspaces. We find a largest subspace V_i in the flag on which g and h commute but they do not commute on the next subspace $V_{i+1} = V_i \oplus \langle v \rangle$. As g is diagonalizable, v is an eigenvector for g, i.e. $gv = \lambda v$ for some $\lambda \neq 0$. On the other hand, the G-invariance of V_{i+1} shows that there is $w \in V_i$ with $hv = \mu v + w$.

Put $h_1 := h^{-1}g^{-1}hg$. We now show that g and h_1 do not commute. Indeed, noting $g^{-1}v = \lambda^{-1}v$ and $h^{-1}v = \mu^{-1}v - \mu^{-1}h^{-1}w$ we have

$$\begin{aligned} h_1 gv &= h^{-1}g^{-1}hg^2v = \lambda^2 h^{-1}g^{-1}hv = \lambda^2 h^{-1}g^{-1}(\mu v + w) = \\ &= \lambda\mu h^{-1}v + \lambda^2 h^{-1}g^{-1}w = \lambda v - \lambda h^{-1}w + \lambda^2 h^{-1}g^{-1}w \end{aligned}$$

and

$$\begin{aligned} gh_1 v &= gh^{-1}g^{-1}hgv = \lambda gh^{-1}g^{-1}hv = \lambda gh^{-1}g^{-1}(\mu v + w) = \\ &= \mu gh^{-1}v + \lambda gh^{-1}g^{-1}w = \lambda v - gh^{-1}w + \lambda gh^{-1}g^{-1}w. \end{aligned}$$

Since g and h commute on V_i, we have $\lambda gh^{-1}g^{-1}w = \lambda h^{-1}w$, so by substracting the two equations we obtain

$$(h_1g - gh_1)v = \lambda^2 h^{-1}g^{-1}w - 2\lambda h^{-1}w + gh^{-1}w = h^{-1}g^{-1}(\lambda - g)^2 w.$$

But $gw \neq \lambda w$, for otherwise we would have $ghv = \lambda\mu v + \lambda w = hgv$, and g and h and would commute on the whole of V_{i+1}. Thus h_1 and g do not commute. Repeating the argument with h_1 in place of h and so on we obtain inductively $h_j \in G^j$ that does not commute with g (recall that $G^0 = G$ and $G^j = [G, G^{j-1}]$). But $G^j = \{1\}$ for j large enough by the nilpotence of G, a contradiction. Therefore $G_s \subset Z(G)$. □

The direct product decomposition of the theorem shows that G_s is a homomorphic image of G, hence it is connected. Thus it is a torus, and we shall see later that it is the largest torus contained as a closed subgroup in G. For this reason it is called the *maximal torus* of G.

If G is only connected and solvable, there exist several maximal tori in G (i.e. tori contained as closed subgroups and maximal with respect to this property). We shall prove in Section 25 that the maximal tori are all conjugate in G, and G is the semidirect product of G_u with a maximal torus.

9. A glimpse at Lie algebras

In order to define the Lie algebra associated with an algebraic group, we first have to discuss tangent spaces.

Let first $X = V(I) \subset \mathbf{A}^n$ be an affine variety, and $P = (a_1, \dots a_n)$ a point of X. The *tangent space* $T_P(X)$ *of* X *at* P is defined as the linear subspace of $\mathbf{A}^n$ given by the equations

$$\sum_{i=1}^{n} (\partial_{x_i} f)(P)(x_i - a_i) = 0,$$

for all $f \in I$, where the x_i are the coordinate functions on $\mathbf{A}^n$. Geometrically this is the space of lines tangent to X at P. If $I = V(f_1, \dots, f_m)$, then we may restrict to the finitely many equations coming from the f_j in the above definition, because if $\Sigma_j g_j f_j$ is a general element of I, then

$$\begin{aligned} \partial_{x_i}(\sum_j g_j f_j)(P) &= \sum_j ((\partial_{x_i} g_j)(P) f_j(P) + g_j(P)(\partial_{x_i} f_j)(P)) \\ &= \sum_j g_j(P) \partial_{x_i} f_j(P), \end{aligned}$$

and so

$$\sum_{i=1}^{n} \partial_{x_i}(\sum_j g_j f_j)(P)(x_i - a_i) = \sum_j g_j(P) \sum_{i=1}^{n} \partial_{x_i} f_j(P)(x_i - a_i) = 0.$$

A drawback of this definition is that it depends on the choice of the embedding of X into $\mathbf{A}^n$. We can make it intrinsic at follows. Let M_P be the maximal ideal in $\mathcal{A}_X$ consisting of functions vanishing at P. Denote by $T_P(X)^*$ the dual k-vector space to $T_P(X)$, and define a map $\partial_P : M_P/M_P^2 \to T_P(X)^*$ by

$$\partial_P(\bar{f}) := \text{restriction of } \sum_{i=1}^{n} (\partial_{x_i} f)(P)(x_i - a_i) \text{ to } T_P(X),$$

where f is a polynomial in $k[x_1, \dots, x_n]$ with $f(P) = 0$ that maps to $\bar{f}$ in M_P/M_P^2. The map does not depend on the choice of f, because it vanishes on elements of $I(X)$ by definition of $T_P(X)$, and it also vanishes on elements of M_P^2 by a calculation using the Leibniz rule as above.

Lemma 9.1. (Zariski) *The map* $\partial_P : M_P/M_P^2 \to T_P(X)^*$ *is an isomorphism of* k*-vector spaces.*

Proof. For surjectivity one sees that all elements of $T_P(X)^*$ can be written as a sum $\Sigma\alpha_i(x_i - a_i)$ with suitable α_i, and these linear functions are preserved by ∂_P. For injectivity, $\partial_P(\bar{f}) = 0$ means that for a representative f one has

$$\sum_{i=1}^{n}(\partial_{x_i}f)(P)(x_i - a_i) = \sum_j \alpha_j \sum_{i=1}^{n}(\partial_{x_i}g_j)(P)(x_i - a_i)$$

for some $g_1, \ldots, g_r \in I(X)$ and $\alpha_j \in k$. Replacing f by $f - \Sigma_j a_j g_j$ we may thus assume $\sum_{i=1}^{n}(\partial_{x_i}f)(P)(x_i - a_i) = 0$, i.e. f has no linear term in the $x_i - a_i$, and therefore its image in M_P lies in M_P^2. □

For the above reason one calls M_P/M_P^2 the *Zariski cotangent space* of X at P, and its dual the *Zariski tangent space*.

Let now G be an affine algebraic group, and look at the tangent space $T_1(G)$ at the unit element 1. The maximal ideal $M_1 \subset \mathcal{A}_G$ corresponding to 1 is none but the kernel of the counit map $e : \mathcal{A}_G \to k$, and $\mathcal{A}_G$ decomposes as a direct sum $\mathcal{A}_G \cong M_1 \oplus k$ via e. Given an element of $T_1(G)$, identified with a k-linear map $\phi : M_1/M_1^2 \to k$, the above decomposition allows us to view it as a map $\mathcal{A}_G \to k$ vanishing on M_1^2 and k; in fact we get a bijection between elements of $T_1(G)$ and k-linear maps $\mathcal{A}_G \to k$ with this property. Using this bijection we may introduce a *Lie bracket* on $T_1(G)$ by setting $[\phi, \psi] := (\phi\otimes\psi - \psi\otimes\phi)\circ\Delta$, where $\Delta : \mathcal{A}_G \to \mathcal{A}_G \otimes_k \mathcal{A}_G$ is the comultiplication map. This is a k-bilinear function that satisfies $[\phi, \phi] = 0$ and the *Jacobi identity*

$$[\phi, [\psi, \chi]] + [\psi, [\chi, \phi]] + [\chi, [\phi, \psi]] = 0.$$

Thus $T_1(G)$ is equipped with a *Lie algebra structure.*

Definition 9.2. *Let G be an affine algebraic group. the Lie algebra* $\mathrm{Lie}(G)$ *of G is the (Zariski) tangent space of G at 1 equipped with the above Lie algebra structure.*

Examples 9.3.

(1) $\mathrm{Lie}(\mathrm{GL}_n)$ is the Lie algebra $\mathfrak{gl}_n$ of all $n\times n$ matrices. Indeed, the tangent space of GL_n at 1 is the same as that of $\mathbf{A}^{n^2}$, namely $\mathbf{A}^{n^2}$.

(2) $\mathrm{Lie}(\mathrm{SL}_n)$ is the Lie algebra $\mathfrak{sl}_n$ of all $n \times n$ matrices of trace 0. This is because $\partial_{x_{ij}}(\det(x_{ij}) - 1)(\delta_{ij})(x_{ij} - \delta_{ij}) = \delta_{ij}(x_{ij} - 1)$ (Kronecker delta). In this way we obtain those matrices M where $M - 1$ has trace 0; translating from 1 to 0 we get $\mathfrak{sl}_n$ embedded as a vector subspace in $\mathbf{A}^{n^2}$.

A morphism $G \to G'$ of algebraic groups induces a homomorphism $\mathrm{Lie}(G) \to \mathrm{Lie}(G')$ of Lie algebras. In particular, any representation $G \to \mathrm{GL}_n$ induces a Lie algebra representation $\mathrm{Lie}(G) \to \mathfrak{gl}_n$.

Remark 9.4. The theorems of Kolchin and Lie-Kolchin have analogues (in fact, predecessors) in Lie algebra theory. *Engel's theorem* states that if $\rho : L \to \mathfrak{gl}_n$ is a Lie algebra representation such that $\rho(x)$ is a nilpotent matrix for all $x \in L$, then ρ stabilizes a complete flag in k^n. *Lie's theorem* says that a similar conclusion holds for representations of solvable Lie algebras. Here one calls a Lie algebra L solvable if the subalgebras $D^i(L)$ defined inductively by $D^0(L) = L$ and $D^i(L) = [D^{i-1}(L), D^{i-1}(L)]$ satisfy $D^i(L) = 0$ for all i large enough.

One may show that if G is solvable as a group, then $\mathrm{Lie}(G)$ is solvable as a Lie algebra (the converse also holds in characteristic 0, but not in characteristic $p > 0$!), and hence deduce Lie's theorem for $\mathrm{Lie}(G)$ from the Lie-Kolchin theorem on G°. Similarly, one may show that Kolchin's theorem for unipotent G implies that of Engel for $\mathrm{Lie}(G)$.

Chapter 3. Flag Varieties and the Borel Fixed Point Theorem

One way to rephrase the Lie-Kolchin theorem is the following: the natural action of a connected solvable subgroup of $\mathrm{GL}(V)$ on the set of complete flags in V has a fixed point. In the first part of this chapter we show that this set carries an additional structure, namely that of a projective variety. In the simplest case when $\dim V = 2$ the problem reduces to classifying lines through the origin in V which indeed correspond to points of the projective line $\mathbf{P}^1$. The higher-dimensional case is more difficult, however, and gives rise to the so-called flag varieties. With this basic example at hand one gains more insight into the main theorem of this section, the Borel fixed point theorem. It states that quite generally the action of a connected solvable group on a projective variety has a fixed point. For the proof we shall have to develop some foundational material from the theory of quasi-projective varieties.

10. Quasi-projective varieties

We identify points of *projective n-space* over our algebraically closed base field k with

$$\mathbf{P}^n(k) := (\{P = (a_0, \ldots, a_n) : a_i \in k\} \setminus \{(0, \ldots, 0)\}) \,/ \sim,$$

where $\sim$ is the equivalence relation for which $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ if and only if there exists $\lambda \in k^\times$ with $a_i = \lambda b_i$ for all i.

Definition 10.1. *Let $f_1, \ldots, f_m \in k[x_0, \ldots, x_n]$ be* homogeneous *polynomials. Define*

$$V(f_1, \ldots, f_m) := \{P \in \mathbf{P}^n(k) : \; f_i(P) = 0, \, 1 \le i \le m\}.$$

A subset of $\mathbf{P}^n(k)$ of this form is called a projective variety*. These subsets are the closed subsets of a topology on $\mathbf{P}^n$ called the Zariski topology.*

Remark 10.2. We say that a non-homogeneous polynomial vanishes at a point of $\mathbf{P}^n(k)$ if it vanishes on all of its representatives. If $X \subset \mathbf{P}^n$ is a projective closed subset, then the ideal $I(X) \subset k[x_0, \ldots, x_n]$ of polynomials vanishing on X has the following additional property: each homogeneous component of a polynomial in $I(X)$ is contained in $I(X)$. (Indeed, if $f = \Sigma f_d$ with f_d homogeneous of degree d, then $0 = f(\lambda a_0, \ldots, \lambda a_n) = \Sigma \lambda^d f_d(a_0, \ldots, a_n)$ can only hold for all $\lambda \neq 0$ if $f_d(a_0, \ldots, a_n) = 0$ for all d, because k is infinite.) Ideals in $k[x_0, \ldots, x_n]$ having this property are called *homogeneous* ideals.

There is the following analogue of the Nullstellensatz for projective varieties: if $I \subset k[x_0, \ldots, x_n]$ is a homogeneous ideal that equals its radical and does not contain the ideal $(x_0, \ldots, x_n)$, then $I(V(I)) = I$. This is not hard to derive from the affine Nullstellensatz. Note that $V(x_0, \ldots, x_n) = \emptyset$, so the additional condition is necessary.

Consider the Zariski open subsets

$$D_+(x_i) := \mathbf{P}^n \setminus V(x_i) = \{P = (x_0, \dots x_n) \in \mathbf{P}^n(k) : x_i \neq 0\}$$

for all $0 \leq i \leq n$. These form an open covering of $\mathbf{P}^n$. The points of $D_+(x_i)$ are in bijection with those of $\mathbf{A}^n$ via the maps

$$(x_0, \dots, x_n) \mapsto (\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i})$$

and

$$(t_1, \dots, t_n) \mapsto (t_1, \dots, t_{i-1}, 1, t_i \dots, t_n).$$

Here if $X = V(J)$ is a projective variety, then

$$X^{(i)} := X \cap D_+(x_i) = V(J^{(i)})$$

is an affine variety in $D_+(x_i) \cong \mathbf{A}^n$ for all i, where $J^{(i)} \subset k[t_1, \dots, t_n]$ is the ideal formed by the polynomials

$$f^{(i)}(t_1, \dots, t_n) = f(t_1, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_n)$$

for all $f \in J$. Conversely, if $X_i = V(I_i) \subset D_+(x_i)$ is an affine variety, its *projective closure* $\overline{X}_i \subset \mathbf{P}^n$ is defined as its closure in $\mathbf{P}^n$ for the Zariski topology. It can be described as $V(I)$, where I is the homogeneous ideal formed by all polynomials arising as

$$G = x_i^d g(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i})$$

for some $g \in I_i$ of degree d. One has $(\overline{X}_i)^{(i)} = X_i$, so the inclusion map $D_+(x_i) \to \mathbf{P}^n$ is a homeomorphism in the Zariski topology.

Example 10.3. For the conic $X = V(x_1x_2 - x_0^2)$ in $\mathbf{P}^2$ the subsets $X^{(1)}$ and $X^{(2)}$ are affine parabolas of equations $x_2 = x_0^2$ and $x_1 = x_0^2$, respectively, whereas $X^{(0)}$ is the affine hyperbola $x_1x_2 = 1$.

Definition 10.4. *A* quasi-projective *variety is a Zariski open subset of a projective variety.*

This is a common generalisation of affine and projective varieties (any affine variety is open in its closure). Another example of a quasi-projective variety is the complement in $\mathbf{P}^n$ of a projective variety. It need not be affine in general.

We now define products of quasi-projective varieties, beginning with the product of two projective spaces $\mathbf{P}^n$ and $\mathbf{P}^m$.

Definition 10.5. *The* Segre embedding $S^{n,m} : \mathbf{P}^n \times \mathbf{P}^m \to \mathbf{P}^N$ *(where $N := nm + n + m$) is the (set-theoretic) map defined by*

$$S^{n,m}((a_0, \dots, a_n), (b_0, \dots, b_m)) = (a_0b_0, a_0b_1, \dots, a_ib_j, \dots, a_nb_{m-1}, a_nb_m),$$

the products a_ib_j being listed in lexicographic order.

It is clear from the definition that $S^{n,m}$ is injective.

Lemma 10.6. *The image of $S^{n,m}$ is a closed subvariety of $\mathbf{P}^N$.*

Proof. To ease notation, denote the coordinate functions on $\mathbf{P}^N$ by w_{ij} ($0 \le i \le n$, $0 \le j \le m$). We claim that the closed subvariety

$$W := V(w_{ij}w_{kl} - w_{kj}w_{il} \,:\, 0 \le i,k \le n,\ 0 \le j,l \le m) \subset \mathbf{P}^N$$

is exactly the image of $S^{n,m}$. The inclusion $\mathrm{Im}\,(S^{n,m}) \subset W$ is obvious. For the converse, pick $Q = (q_{00},\dots,q_{nm}) \in W$. By permuting the coordinates if necessary we may assume $q_{00} \neq 0$. Then $Q = S^{n,m}((q_{00},\dots,q_{n0}),(q_{00},\dots,q_{0m}))$, because $q_{i0}q_{0l} = q_{00}q_{il}$ according to the equations of W. □

Remark 10.7. In the above proof we have in fact shown the equality $W \cap D_+(w_{00}) = S^{n,m}(D_+(x_0) \times D_+(x_0))$. This holds in general: $W \cap D_+(w_{ij}) = S^{n,m}(D_+(x_i) \times D_+(x_j))$. Thus W has a standard affine open covering by copies of $D_+(x_i) \times D_+(x_j) \cong \mathbf{A}^{n+m}$. The construction of the above proof also shows that the map $\mathbf{A}^n \times \mathbf{A}^m \to S^{n,m}(D_+(x_i) \times D_+(x_j))$ is a homeomorphism in the Zariski topology.

Definition 10.8. *If $X \subset \mathbf{P}^n$ and $Y \subset \mathbf{P}^m$ are quasi-projective varieties, the product $X \times Y$ is defined as $S^{n,m}(X \times Y) \subset \mathbf{P}^N$.*

Lemma 10.9. *The product $X \times Y$ is a quasi-projective variety. If X and Y are projective, then so is $X \times Y$.*

Proof. This follows from the above remark and the following easy topological statement (applied to the $D_+(x_i)$ and the $D_+(x_i)\times D_+(x_j)$): *If a topological space X has an open covering by subspaces U_i, then $Z \subset X$ is open (resp. closed) if and only if each $Z \cap U_i$ is open (resp. closed) in U_i.* □

11. Flag varieties

We now show that the set of complete flags in an n-dimensional vector space V may be endowed with the structure of a projective variety. As a first step we consider subspaces of fixed dimension d.

Recall that the exterior algebra $\Lambda(V) = \bigoplus \Lambda^d(V)$ is defined by

$$\Lambda(V) := \bigoplus_{d=0}^{\infty} V^{\otimes d}/\langle x \otimes x\rangle.$$

The image of $v_1 \otimes \cdots \otimes v_d$ in $\Lambda^d(V)$ is denoted by $v_1 \wedge \cdots \wedge v_d$. If $e_1,\dots,e_n$ is a basis of V, then the elements $e_{i_1} \wedge \cdots \wedge e_{i_d}$ form a basis of $\Lambda^d(V)$ for $i_1 < \cdots < i_d$. Thus $\Lambda^d(V)$ has dimension $\binom{n}{d}$; in particular, it has dimension 1 for $n = d$. In this case, given vectors $v_1,\dots,v_d$ with $v_i = \Sigma a_{ij}e_j$, one has $v_1 \wedge \cdots \wedge v_d = \det(a_{ij}) e_1 \wedge \cdots \wedge e_d$.

Now denote by $\mathrm{Gr}_d(V)$ the set of d-dimensional subspaces in V. The *Plücker embedding* $p_d : \mathrm{Gr}_d(V) \to \mathbf{P}(\Lambda^d(V))$ is defined by sending a dimension d subspace S to $\Lambda^d(S)$. Explicitly the map can be described as follows: if $e_1, \dots, e_n$ is a basis of V, then giving a basis $v_1, \dots, v_d$ for S is the same as giving an $n \times d$ matrix with coefficients in k. Then $p_d(S)$ is the point of $\mathbf{P}^{\binom{n}{d}-1}$ given by the $d \times d$ minors of this matrix.

Lemma 11.1. *The map p_d is injective.*

Proof. Assume S_1 and S_2 are two subspaces of dimension d in V. We may choose bases of S_1 and S_2 as follows: $e_1, \dots, e_d$ is a basis of S_1, and $e_r, \dots, e_{r+d-1}$ is a basis of S_2. Now $p_d(S_1) = p_d(S_2)$ is equivalent to $e_1 \wedge \cdots \wedge e_d = \lambda e_r \wedge \cdots \wedge e_{r+d-1}$ for some $\lambda \in k^\times$, which can only hold with $r = 1$. $\square$

Example 11.2. The simplest nontrivial case is when $n = 4$, $d = 2$. If $e_0, \dots e_3$ is a basis of V and $v_1 = \Sigma a_i e_i$, $v_2 = \Sigma b_i e_i$ generate a 2-dimensional subspace, the image $p_2(\langle v_1, v_2\rangle) \in \mathbf{P}^{\binom{4}{2}-1} = \mathbf{P}^5$ is the point $(p_{01}, p_{02}, p_{03}, p_{12}, p_{13}, p_{23})$ with $p_{ij} = a_i b_j - b_i a_j$. Denote the homogeneous coordinates on $\mathbf{P}^5$ by $x_{01}, \dots, x_{23}$ as above. One may then check that the image of p_2 is the projective hypersurface of equation $x_{01}x_{23} - x_{02}x_{13} + x_{03}x_{12} = 0$, called the *Plücker quadric.*

In general, we have:

Proposition 11.3. *The image of p_d is a closed subvariety of $\mathbf{P}^{\binom{n}{d}-1}$ for $0 \le d \le n$.*

Proof. The point of $\mathbf{P}^{\binom{n}{d}-1}$ defined by a vector $w \in \Lambda^d(V)$ is in the image of p_d if and only if w is of the form $w = \lambda v_1 \wedge \cdots \wedge v_d$ with $v_i \in V$ and $\lambda \in k^\times$. We first show that this happens if and only if the kernel V_w of the map $V \to \Lambda^{d+1}(V)$, $v \mapsto v \wedge w$ is of dimension d, and otherwise $\dim V_w < d$. Indeed, choose a basis $v_1, \dots, v_m$ of V_w, and extend it to a basis of V by adding vectors $v_{m+1}, \dots, v_n$. Then w is expressed as a linear combination of terms of the form $v_{i_1} \wedge \cdots \wedge v_{i_d}$, $i_1 < \cdots < i_d$. For each $1 \le i \le d$ we have $v_{i_1} \wedge \cdots \wedge v_{i_d} \wedge v_i = 0$ if $i = i_j$ for some j, and otherwise these are linearly independent $(d+1)$-vectors. Since $w \wedge v_i = 0$ for $1 \le i \le m$, this implies that each v_i must be one of these v_{i_j}'s. Thus $m \le d$, with equality if and only if $w = \lambda v_1 \wedge \cdots \wedge v_d$.

Now embed $\Lambda^d(V)$ in $\mathrm{Hom}_k(V, \Lambda^{d+1}(V)$ via the map $w \mapsto (v \mapsto v \wedge w)$. This induces a closed embedding $\mathbf{P}(\Lambda^d(V)) \hookrightarrow \mathbf{P}(\mathrm{Hom}_k(V, \Lambda^{d+1}(V))$. By the above observation here the points of $\mathrm{Im}\,(p_d)$ come from linear maps whose image has dimension $\le n-d$. Choosing bases, this means that the $(n-d+1) \times (n-d+1)$ minors of the matrix of the map vanish. These give rise to homogeneous polynomials on $\mathbf{P}(\mathrm{Hom}_k(V, \Lambda^{d+1}(V))$, and hence exhibit $\mathrm{Im}\,(p_d)$ as the intersection of $\mathbf{P}(\Lambda^d(V))$ with a Zariski closed subset. $\square$

The above projective variety is called a *Grassmann variety* or a *Grassmannian.*

Now we come to flag varieties. These parametrise flags in finite-dimensional vector spaces. So let V be an n-dimensional vector space, and denote by $\mathrm{Fl}(V)$ the set of complete flags in V. Define a map $p_V : \mathrm{Fl}(V) \to \mathrm{Gr}_0(V) \times \cdots \times \mathrm{Gr}_n(V)$ by sending a flag $V_0 \subset \cdots \subset V_n$ to $(p_0(V_0), \ldots, p_n(V_n))$. The map is obviously injective.

Proposition 11.4. *The image of p_V is Zariski closed, and hence p_V realises $\mathrm{Fl}(V)$ as a projective variety.*

Proof. It will be enough to show that the subset $Z_d \subset \mathrm{Gr}(V_d) \times \mathrm{Gr}(V_{d+1})$ consisting of pairs $(p_d(V_d), p_{d+1}(V_{d+1}))$ satisfying $V_d \subset V_{d+1}$ is closed. Indeed, then the image of p_V will arise as the intersection of the closed subsets $\mathrm{Gr}_0(V) \times \cdots \times \mathrm{Gr}_{d-1}(V) \times Z_d \times \mathrm{Gr}_{d+2}(V) \times \cdots \times \mathrm{Gr}_n(V)$.

Putting $w_d := p_d(V_d)$, $w_{d+1} := p_{d+1}(V_{d+1})$ it comes out from the previous proof that $V_d = V_{w_d}$ and $V_{d+1} = V_{w_{d+1}}$. Thus we are dealing with the condition $V_{w_d} \subset V_{w_{d+1}}$, which holds if and only if the kernel of the map $V \to \Lambda^{d+1}(V) \times \Lambda^{d+2}(V)$, $v \mapsto (v \wedge w_d, v \wedge w_{d+1})$ is exactly V_{w_d}. Again by the above proof, this is the same as requiring that the image has dimension $\leq n-d$, which is again a determinant condition. $\square$

We call the above projective variety the *variety of complete flags* in V.

Remark 11.5. Of course, one may also study flag varieties parametrising non-complete flags (increasing chains of subspaces of fixed dimensions). These arise from the above by projection to the product of some components of $\mathrm{Gr}_0(V) \times \cdots \times \mathrm{Gr}_n(V)$.

12. Function fields, local rings and morphisms

We next discuss rational functions and morphisms for quasi-projective varieties. *We assume everywhere that our varieties are irreducible.* This is not a serious restriction, because in our applications all varieties will be either irreducible or finite disjoint unions of irreducibles (think of algebraic groups). The definition will generalize in a straightforward manner to the latter case.

First assume X is affine. The *function field* $k(X)$ of X is the quotient field of the coordinate ring $\mathcal{A}_X$ of X, which is an integral domain by the irreducibility assumption on X. Its elements are represented by quotients of regular functions f/g. If $P \in X$ is a point, the *local ring* $\mathcal{O}_{X,P}$ is the subring of $k(X)$ consisting of functions that have a representative with $g(P) \neq 0$. It is the same as the localisation of $\mathcal{A}_X$ by the maximal ideal corresponding to P. One thinks of it as the ring of functions 'regular at P'.

Lemma 12.1. *For an affine variety X one has $\mathcal{A}_X = \bigcap_P \mathcal{O}_{X,P}$.*

Proof. To show the nontrivial inclusion, pick $f \in \cap_P \mathcal{O}_{X,P}$, and choose for each P a representation $f = f_p/g_P$ with $g_P(P) \neq 0$. The ideal $I := \langle g_P \, : \, P \in X\rangle \subset \mathcal{A}_X$ satisfies $V(I) = \emptyset$ by our assumption on f, so by the Nullstellensatz $I = \mathcal{A}_X$. In particular, there exist $P_1, \dots, P_r \in X$ with $1 = g_{P_1}h_{P_1} + \dots g_{P_r}h_{P_r}$ with some $h_{P_i} \in \mathcal{A}_X$. Thus

$$f = \sum_{i=1}^{r} f g_{P_i} h_{P_i} = \sum_{i=1}^{r} (f_{P_i}/g_{P_i}) g_{P_i} h_{P_i} = \sum_{i=1}^{r} f_{P_i} h_{P_i} \in \mathcal{A}_X.$$

□

Next we define the function field $k(X)$ for a *projective variety* X as follows. Consider the ring

$$\mathcal{R}_X := \{\frac{f}{g} \, : \, f, g \in k[x_0, \dots, x_n] \text{ homogeneous, } g \notin I(X), \deg f = \deg g\}.$$

The $f/g \in \mathcal{R}_X$ with $f \in I(X)$ form a maximal ideal $\mathcal{M}_X$, because $f/g \notin \mathcal{M}_X \Rightarrow g/f \in \mathcal{M}_X$. Therefore $k(X) := \mathcal{R}_X/\mathcal{M}_X$ is a field, the *function field* of X. Its elements, called *rational functions*, are represented by quotients of homogeneous polynomials of the same degree.

Now consider the standard affine open covering of X.

Lemma 12.2. *For each i one has $k(X^{(i)}) \cong k(X)$.*

Proof. Define maps

$$\frac{f(x_0, \dots, x_n)}{g(x_0, \dots, x_n)} \in k(X) \;\mapsto\; \frac{f(t_1, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_n)}{g(t_1, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_n)} \in k(X^{(i)})$$

and

$$\frac{f^{(i)}(t_1, \dots, t_n)}{g^{(i)}(t_1, \dots, t_n)} \in k(X^{(i)}) \;\mapsto\; x_i^{e-d} \frac{x_i^d f^{(i)}(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i})}{x_i^e g^{(i)}(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i})},$$

where $d = \deg(f^{(i)})$, $e = \deg(g^{(i)})$. The reader will check that the two maps are inverse to each other. □

As in the affine case, one defines the *local ring* $\mathcal{O}_{X,P}$ at P is the subring of $k(X)$ consisting of functions that have a representative with $g(P) \neq 0$.

Corollary 12.3. *For each i with $P \in X^{(i)}$ one has $\mathcal{O}_{X^{(i)},P} \cong \mathcal{O}_{X,P}$. Therefore $\mathcal{O}_{X^{(i)},P} \cong \mathcal{O}_{X^{(j)},P}$ for $P \in X^{(i)} \cap X^{(j)}$.*

Thus it makes sense to define the function field (resp. local ring at a point) for a quasi-projective variety as the function field (resp. local ring) of its projective closure; this agrees with the definition made for affine varieties.

We now define morphisms for quasi-projective varieties. Unfortunately the same definition as in the affine case does not work, for we shall see in Corollary 14.3 below that on an irreducible projective variety there are no nonconstant everywhere regular functions.

We proceed as follows. First, if X is a quasi-projective variety, and $U \subset X$ is an open subset, we define the *ring of regular functions on* U by

$$\mathcal{O}(U) := \bigcap_{P \in U} \mathcal{O}_{X,P},$$

the intersection being taken inside $k(X)$. Next, we define a *morphism* $\phi : X \to Y$ *of quasi-projective varieties* as a continuous map such that for all open $U \subset Y$ and all $f \in \mathcal{O}(U)$ one has $f \circ \phi \in \mathcal{O}(\phi^{-1}(U))$.

Examples 12.4.

(1) If X and Y are affine, this is the same notion as before. Indeed, it is enough to check this in the case $Y = \mathbf{A}^m$. Then if $f_1, \ldots, f_m \in \mathcal{A}_X$, then $\phi = (f_1, \ldots, f_m)$ has the above property, and conversely, if ϕ is as above, then for $U = \mathbf{A}^m$ the functions $f_i := t_i \circ \phi$ are in $\mathcal{A}_X$ and define a morphism in the old sense, where the t_i are the coordinate functions.

(2) If $X \subset \mathbf{P}^n$ is projective, and $F_1, \ldots, F_m$ are homogeneous polynomials of the same degree d with $V(F_0, \ldots, F_m) \cap X = \emptyset$, then $\phi(P) := (F_0(P), \ldots, F_m(P)) \in \mathbf{P}^m$ defines a morphism of X into $\mathbf{P}^m$. Indeed, note first that ϕ is everywhere defined by the assumption $V(F_0, \ldots, F_m) \cap X = \emptyset$. Over each $X^{(i)}$ it coincides with the map $(F_1/x_i^d, \ldots, F_m/x_i^d)$ which is given by everywhere regular functions. Thus ϕ restricts to a morphism on each affine variety $X^{(i)}$, and thus it is a morphism on X because the definition of morphisms is local (note that if a rational function is regular on an open covering, then it is regular).

(3) If X is a quasi-projective variety and $U \subset X$ is an open subset, then the inclusion map $U \to X$ is a morphism.

The following lemma will be used many times in what follows.

Lemma 12.5. *Let X be a quasi-projective variety, and $P \in X$. Then P has an open neighbourhood isomorphic (as a quasi-projective variety) to an affine variety. Hence X has an open covering by affine varieties.*

Proof. By cutting X with some $D_+(x_i)$ containing P we may assume that X is a Zariski open subset in some affine variety Y. Since a basis of the Zariski topology of Y is given by open subsets of the form $D(f)$, we only have to prove that each $D(f)$ is isomorphic to an affine variety. To prove this we reduce to the case $Y = \mathbf{A}^n$. Then $D(f)$ is isomorphic to the closed subset $V(x_{n+1}f - 1) \subset \mathbf{A}^{n+1}$ (a trick we already used in realising GL_n as an affine variety). We leave it to the readers to check that the map $(x_1, \ldots, x_n) : V(x_{n+1}f - 1) \to D(f)$ is indeed an isomorphism of quasi-projective varieties. □

13. Dimension

Once we have defined function fields, we can introduce the concept of dimension in algebraic geometry.

Definition 13.1. *The dimension* $\dim X$ *of an irreducible quasi-projective variety* X *is the transcendence degree of* $k(X)$ *over* k*. In general it is the maximum of the dimensions of the irreducible components.*

Recall that the transcendence degree means the maximal number of algebraically independent elements in $k(X)$. The definition generalises the notion of dimension for vector spaces, as $k(\mathbf{A}^n) = k(t_1, \dots, t_n)$, and so $\dim \mathbf{A}^n = n$. Similarly, $k(\mathbf{P}^n) = k(D_+(x_i)) = k(t_1, \dots, t_n)$, and therefore $\dim \mathbf{P}^n = n$.

In most of this text we shall get away with some very coarse properties of dimension.

Lemma 13.2. *If* $\phi : X \to Y$ *is a surjective morphism, then* $\dim Y \leq \dim X$*.*

Proof. We may assume that X is irreducible, and hence so is Y, being its continuous image. Then ϕ induces a homomorphism of function fields $\phi^* : k(Y) \to k(X)$ via $f \mapsto f \circ \phi$. Since ϕ^* must be an injection, the lemma follows from the definition of dimension. □

Remark 13.3. In fact, the lemma holds (with the same proof) under the weaker assumption that $\mathrm{Im}\,(\phi)$ is dense in Y. Note, however, that some restrictive assumption is needed on $\mathrm{Im}\,(\phi)$, because e.g. if ϕ is a constant map to $P \in Y$, then $\phi^*(f)$ is only defined if $f \in \mathcal{O}_{Y,P}$.

Proposition 13.4. *If* X *is irreducible, and* $Y \subset X$ *is a closed subvariety with* $Y \neq X$*, then* $\dim Y < \dim X$*.*

Proof. We may assume that Y is irreducible and moreover (by taking the projective closure and then cutting with a suitable $D_+(x_i)$) that X and Y are affine. Then $\mathcal{A}_Y \cong \mathcal{A}_X/P$ with a nonzero prime ideal P, and the proposition results from the following purely algebraic lemma. □

Lemma 13.5. *Let* A *be an integral domain which is a finitely generated* k*-algebra, and* P *a nonzero prime ideal in* A*. Then the transcendence degree of* A/P *is strictly smaller than that of* A*.*

Here the transcendence degree of an integral domain is defined as that of its quotient field.

Proof. Let $\bar{t}_1, \dots, \bar{t}_d$ be a maximal algebraically independent subset in A/P. Lift the $\bar{t}_i$ to elements $t_i \in A$. We show that for any nonzero $t_0 \in P$ the elements $t_0, t_1, \dots t_d$ are algebraically independent in A. If not, there is a polynomial $f \in k[x_0, \dots, x_d]$ with $f(t_0, \dots, t_d) = 0$. We may assume f is irreducible (because A is an integral domain) and that it is not a polynomial in x_0 only (because k is algebraically closed). It follows that reducing modulo P we obtain a nontrivial relation $f(0, \bar{t}_1, \ldots, \bar{t}_d) = 0$, a contradiction. □

Proposition 13.6. *Let $X \subset \mathbf{A}^n$ be an irreducible affine variety of dimension d, and $f \in k[x_1, \ldots, x_n]$ a polynomial vanishing at some point of X. Then each irreducible component of the intersection $X \cap V(f)$ has dimension at least $d - 1$.*

Proof. This is a form of Krull's principal ideal theorem. For the algebraic version, see e.g. Chapter 11 of Atiyah–Macdonald, Introduction to Commutative Algebra; for the geometric version, §I.7 of Mumford's Red Book of Varieties and Schemes. □

Corollary 13.7. *Let $\phi : X \to Y$ be a morphism of quasi-projective varieties with dense image. Then for each point $P \in \mathrm{Im}\,(\phi)$ the fibre $\phi^{-1}(P)$ has dimension at least $\dim X - \dim Y$.*

Proof. Up to replacing Y with an affine open subset containing P, we may assume that Y is affine and embed it as a closed subvariety in some $\mathbf{A}^m$. Choose a polynomial $f_1 \in k[x_1, \ldots, x_m]$ vanishing at P but not on the whole of Y. By Propositions 13.4 and 13.6 an irreducible component Z of $Y \cap V(f_1)$ passing through P has dimension exactly $s - 1$. Replacing Y by an affine open subset containing P and disjoint from the other components of $Y \cap V(f_1)$ we may assume $Y \cap V(f_1) = Z$. Repeating the procedure with Z and shrinking Y again, after s steps we arrive at polynomials $f_1, \ldots, f_s$ with $Y \cap V(f_1, \ldots, f_s) = \{P\}$. Then $\phi^{-1}(P) = \{Q \in X : \phi^* f_1(Q) = \cdots = \phi^* f_s(Q) = 0\}$. The corollary now follows from an inductive application of the proposition over an affine open covering of X. □

We shall see later (Proposition 16.10) that in fact the fibre dimension is exactly $\dim X - \dim Y$ over a dense open subset of Y. Our assumption that $\mathrm{Im}\,(\phi)$ is dense in Y was needed only in order to ensure (via Remark 13.3) that $\dim X - \dim Y$ is a nonnegative integer.

14. Morphisms of projective varieties

We shall now prove the following fundamental theorem.

Theorem 14.1. *Let $\phi : X \to Y$ be a morphism of quasi-projective varieties. If X is projective, then $\phi(X)$ is Zariski closed in Y.*

Here are some immediate corollaries.

Corollary 14.2. *If X is irreducible and projective, and Y is affine, then any morphism $X \to Y$ is constant.*

Proof. By embedding Y into some affine space we may assume $Y = \mathbf{A}^n$. By composing with the natural coordinate projections $\mathbf{A}^n \to \mathbf{A}^1$ we reduce to the case $n = 1$. Composing with the inclusion map $\mathbf{A}^1 \to \mathbf{P}^1$ we obtain a morphism $\widetilde{\phi} : X \to \mathbf{P}^1$ (by Example 12.4 (3) and the obvious fact that a composition of two morphisms is a morphism). By the theorem and the continuity of $\widetilde{\phi}$ the subset $\widetilde{\phi}(X) \subset \mathbf{A}^1$ is a closed and irreducible subset of $\mathbf{P}^1$, hence must be a point. $\square$

Corollary 14.3. *Any regular function on an irreducible projective variety is constant.*

Proof. This is the special case $Y = \mathbf{A}^1$ of the previous corollary. $\square$

The theorem will follow from the following statement:

Theorem 14.4. *Let X be a projective, Y a quasi-projective variety. Then the second projection $p_2 : X \times Y \to Y$ is a closed mapping, i.e. maps closed subsets to closed subsets.*

To see that Theorem 14.4 implies Theorem 14.1, one first proves

Lemma 14.5. *If Y is a quasi-projective variety, then the diagonal subvariety $\Delta(Y) \subset Y \times Y$ defined by $\{(P, P) : P \in Y\}$ is closed in $Y \times Y$.*

Proof. By covering Y with affine varieties we may assume Y is affine. Embedding Y into some $\mathbf{A}^n$ we see that $\Delta(Y) = (Y \times Y) \cap \Delta(\mathbf{A}^n)$, so it is enough to consider the case $Y = \mathbf{A}^n$ which is obvious. $\square$

Proof of Theorem 14.1. Consider the *graph* $\Gamma_\phi \subset X \times Y$ of ϕ defined by $\{(P, \phi(P)) : P \in X\}$. It is the inverse image of $\Delta(Y)$ by the morphism $(\phi, \mathrm{id}) : X \times Y \to Y \times Y$, so it is closed by Lemma 14.5 and the continuity of (ϕ, id). But $\phi(X)$ is the image of Γ_ϕ by $p_2 : X \times Y \to Y$, so we conclude by Theorem 14.4. $\square$

Remarks 14.6.

(1) The property of Lemma 14.5 is called the *separatedness* property of quasi-projective varieties, and that of Theorem 14.4 the *properness* of projective varieties. In older terminology proper varieties are also called complete.

(2) In classical parlance Theorem 14.4 is called the 'Main Theorem of Elimination Theory'. This is because (in the case when Y is affine) the equations for the image of a closed subset of $X \times Y$ in Y were found in the old times by an explicit procedure which may be regarded as a higher degree analogue of Gaussian elimination. The proof below, due to Grothendieck, will be nonconstructive but quicker.

Grothendieck's proof of Theorem 14.4 uses a form of Nakayama's Lemma:

Lemma 14.7. *Let R be a commutative ring with unit, $M \subset R$ a maximal ideal and N a finitely generated R-module. If $MN = N$, then there exists $f \in R \setminus M$ with $fn = 0$ for all $n \in N$.*

Proof. Let $n_1, \dots, n_m$ be a generating system of N. By assumption for each $1 \le i \le m$ we may find $m_{ij} \in M$ with $n_i = \Sigma_j m_{ij} n_j$. Let $[m_{ij}]$ be the $n \times n$ matrix formed by the m_{ij}, and $[n_j]$ the column vector formed by $n_1, \dots, n_m$. Then $(\mathrm{id} - [m_{ij}])[n_j] = 0$, and multiplication by the adjoint matrix yields $\det(\mathrm{id} - [m_{ij}])N = 0$ using Cramer's rule. So the element $f := \det(\mathrm{id} - [m_{ij}])$, which lies in $1 + M \subset R \setminus M$, is a suitable one. □

Proof of Theorem 14.4. First, by embedding X to some $\mathbf{P}^n$ we reduce to the case when $X = \mathbf{P}^n$. Next, by taking an open covering of Y by affine varieties (Lemma 12.5) we reduce to the case when Y is affine; denote by R its coordinate ring. Given a closed subset $Z \subset \mathbf{P}^n \times Y$, it is enough to find for all $P \in Y \setminus p_2(Z)$ some $f \in R$ with $f(P) \neq 0$ but $f(Q) = 0$ for $Q \in p_2(Z)$, because then $D(f)$ is an affine open subset containing P but disjoint from $p_2(Z)$.

Now $\mathbf{P}^n \times Y$ has an affine open covering by the $D_+(x_i) \times Y$, which have coordinate ring $R_i := R[x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots x_n/x_i]$. The intersection $Z_i := Z \cap (D_+(x_i) \times Y)$ is a closed subvariety of $D_+(x_i) \times Y$. Write $S = R[x_0, \dots, x_n]$ and $S_d \subset S$ for the R-submodule of homogeneous polynomials of degree d. Define

$$I_d := \{f \in S_d : f(x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots x_n/x_i) \in I(Z_i) \text{ for all } i\}.$$

Then $I := \oplus_d I_d$ is a homogeneous ideal in $S = \oplus_d S_d$. We show that for d large enough there is $f \in R \setminus M$ with $f S_d \subset I_d$, where M is the ideal of P in R. This will do the job, because then $f x_i^d \in I_d$ for all i, which by definition of I_d means $f \in I(Z_i)$ for all i, and hence f as a function on $\mathbf{P}^n \times Y$ vanishes on Z, i.e. f as a function on Y vanishes on $p_2(Z)$.

By the above lemma applied to S_d/I_d it will be enough to show that $S_d = I_d + MS_d$ for d large enough. Since Z_i is disjoint from $D_+(x_i) \times \{P\}$, i.e. $V(I(Z_i)) \cap V(MR_i) = \emptyset$, we have $I(Z_i) + MR_i = R_i$ by the Nullstellensatz for $D_+(x_i) \times Y$. Thus we find $f_i \in I(Z_i)$, $m_{ij} \in M$ and $g_{ij} \in R_i$ with $1 = f_i + \Sigma m_{ij} g_{ij}$. For d sufficiently large $g_{ij} x_i^d \in S_d$ for all i. It will now suffice to show that $f_i x_i^d \in I_d$ for d large enough, for then the equation $x_i^d = f_i x_i^d + \Sigma m_{ij} g_{ij} x_i^d$ will show $x_i^d \in I_d + MS_d$, and therefore for d even larger all degree d monomials in the x_i will be in $I_d + MS_d$, and these generate S_d. To find d with $f_i x_i^d \in I_d$, observe that for d large enough $f_i x_i^d \in S_d$ and it vanishes on $Z_i = Z \cap D_+(x_i)$. But then $f_i x_i^{d+1}$ vanishes on Z_i and on $V(x_i)$, so on the whole of Z, and in particular on the other Z_j as well. Hence $f_i x_i^{d+1} \in I_{d+1}$. □

15. The Borel fixed point theorem

Let G be an affine algebraic group, Y a quasi-projective variety. A (left) *action* of G on Y is a morphism of varieties $G \times Y \to Y$ satisfying the usual axioms for group actions. In particular, for each $g \in G$ the associated map $\phi_g : Y \to Y$ is an isomorphism of varieties. The *orbit* of $P \in Y$ under G is the set $\{gP : g \in G\}$. An orbit consisting of a single point is a fixed point.

One way to phrase the Lie-Kolchin theorem is to say that the natural action of a connected solvable subgroup of $\mathrm{GL}(V)$ on the projective variety $\mathrm{Fl}(V)$ of complete flags in V has a fixed point. In this section we prove the following vast generalisation.

Theorem 15.1. (Borel fixed point theorem) *An action of a connected solvable affine algebraic group G on a projective variety X has a fixed point.*

The proof below is due to Steinberg. It begins by solving the following particular case.

Proposition 15.2. *The theorem holds in the case when $G \subset \mathrm{GL}(V)$ with a finite-dimensional vector space V, and $X \subset \mathbf{P}(V)$ is a closed subset stabilised by the induced action of G on $\mathbf{P}(V)$.*

Proof. The proposition states that the elements of G have a common eigenvector whose image in $\mathbf{P}(V)$ lies in X. We prove the proposition by induction on the dimension n of V, the case $n = 1$ being obvious. If $n = 2$, then $\mathbf{P}(V) \cong \mathbf{P}^1$, so there are two cases. Either X is the whole of $\mathbf{P}(V)$ and we are done by the Lie-Kolchin theorem. Or X is a finite set of points, but since G is connected, it must fix each of these points, and we are again finished. Now assume $n > 2$. By the Lie-Kolchin theorem the elements of G have a common eigenvector $v \in V$. We may assume $v \notin X$, for otherwise we are done. Then the restriction of the map $\mathbf{P}(V) \to \mathbf{P}(V/\langle v \rangle)$ to X is a morphism, and the image $X' \subset \mathbf{P}(V/\langle v \rangle)$ of X is closed by Theorem 14.1. Thus by induction G has a fixed point P in X'. Let w be a preimage of P in V, and $W = \langle v, w \rangle$. By construction W is G-invariant and we have $X' \cap \mathbf{P}(W) \neq \emptyset$, so we are done by the case $n = 2$. □

The proof in the general case proceeds by reduction to the above proposition. We need some lemmas that are interesting in their own right. First a statement from algebraic geometry whose proof is postponed to the next section.

Lemma 15.3. *Let $\phi : X \to Y$ be a morphism of quasi-projective varieties with Zariski dense image. Then $\phi(X)$ contains a nonempty open subset of Y.*

The lemma will be used in the proof of theorem 15.1 via the following corollaries.

Corollary 15.4. *Let G be an affine algebraic group acting on a quasi-projective variety Y. Each orbit of G is open in its closure.*

Proof. Let O_P be the orbit of a point $P \in Y$ and Z its Zariski closure. Assume first G is connected. As O_P is the image of the morphism $G \to Z$ sending $g \in G$ to $gP \in Z$, the lemma implies that O_P contains an open subset $U \subset Z$. Since it is the union of the gU for all $g \in G$, it is open in Z.

In the general case let G° be the connected component of identity in G, and choose $g_1, \dots, g_n \in G$ such that G is the union of the $g_i G^\circ$. If Z° is the closure of the G°-orbit of P, then Z is the union of the isomorphic irreducible closed subsets $g_i Z^\circ$. By the lemma each $O_P \cap g_i Z^\circ$ contains an open subset $U_i \subset g_i Z^\circ$, and we conclude as before. □

Corollary 15.5. (Closed orbit lemma) *If Y is affine or projective*[1], *an orbit of minimal dimension is closed.*

Proof. Let O_P be such an orbit, Z its closure. Then Z is the union of orbits of G, because if $Q \in Z$ has an open neighbourhood U_Q containing $P' \in O_P$, then the open neighbourhood gU_Q of gQ contains gP'. By the lemma $Z \setminus O_P$ is a closed subset. It does not contain any irreducible component of Z, because Z is the union of the closures of the irreducible components of O_P which are themselves irreducible. From Proposition 13.4 applied to each irreducible component of Z we thus get that $Z \setminus O_P$ is a union of orbits of smaller dimension, and hence must be empty. □

Proof of Theorem 15.1. An orbit of G in X that has minimal dimension is closed by the above corollary, so it is also projective. Thus replacing X by this orbit we may assume there is a single G-orbit in X. Take $P \in X$, and let $G_P \subset G$ be its stabilizer. It is a closed subgroup, being the preimage of P by the morphism $g \mapsto gP$. Thus by Lemma 4.2 we find a representation of G on some finite-dimensional V with G_P stabilizing a one-dimensional subspace in V, hence fixing a point Q in the induced action of G on the projective space $\mathbf{P}(V)$. Let Y be the orbit of Q in $\mathbf{P}(V)$ and Z that of (P, Q) in $X \times \mathbf{P}(V)$ (equipped with the product action). The natural projections $Z \to X$ and $Z \to Y$ are bijective G-morphisms, so it is enough to find a fixed point in Y (which must then be the whole of Y). For this it is enough to see that Y is closed in $\mathbf{P}(V)$, for then we may conclude by Proposition 15.2 applied to the image of G in $GL(V)$ (which is again connected and solvable; it is also closed by Corollary 16.5 below, but this was not used in the proof of the proposition). Now the closedness of Y follows from that of Z by Theorem 14.4. To prove the latter fact, observe that any G-orbit in $X \times \mathbf{P}(V)$ must project onto X by the projection $X \times \mathbf{P}(V) \to X$, because X is a single G-orbit. Thus the dimension of each G-orbit in $X \times \mathbf{P}(V)$ is at least $\dim X$. But $\dim X = \dim Z$ (by Corollary 13.7

[1] This assumption is needed only to ensure that each orbit is a quasi-projective variety (by virtue of the previous corollary). The statement holds in a more general setting.

or Remark 16.4 below), hence Z is an orbit of minimal dimension, and as such closed by Corollary 15.5. □

Remark 15.6. The original proof of the theorem does not use the Lie-Kolchin theorem (and thus reproves it for connected solvable affine algebraic groups). It uses, however, some difficult results that we'll prove only later, in particular the existence of quotients by closed normal subgroups.

This proof runs as follows. Observe first that the fixed point set of any algebraic group G acting on a quasi-projective variety Y is closed. To see this, it is enough to show that each $g \in G$ has a closed fixed point set $Y_g \subset Y$. This holds because Y_g is the inverse image of the diagonal $\Delta(Y) \subset Y \times Y$ (which is closed by Lemma 14.5) by the morphism $y \mapsto (y, gy)$.

Now proceed by induction on $\dim(G)$ (or the length of a commutator series). The subgroup $[G, G]$ is closed and connected (Corollary 16.6 below) and moreover different from G, hence by induction has a fixed point in X. Let $Y \subset X$ be the set of fixed points of $[G, G]$; it is nonempty and closed in X, hence projective and also stable by G as $[G, G]$ is normal in G. We may thus assume $Y = X$, i.e. all points of X are fixed by $[G, G]$. Pick $P \in X$ whose orbit $Z \subset X$ is closed and hence projective (Corollary 15.5), and let $G_P \subset G$ be its stabilizer. Since G_P contains $[G, G]$, it is normal in G and hence G/G_P is a connected affine algebraic group by Theorem 19.4 below. But $G/G_P \cong Z$ as a quasi-projective variety (this follows from the proof of Theorem 19.3 below) and Z is projective, so this is only possible if $Z = P$ by Theorem 14.1.

Chapter 4. Homogeneous Spaces and Quotients

We now arrive at a basic question that cannot be circumvented any longer: how to put a *canonical* structure of a quasi-projective variety on the set of (left) cosets of a closed subgroup H in an affine algebraic group G? The emphasis is on the adjective ‘canonical’, for if we can show that under some additional assumption the variety thus obtained is unique up to unique isomorphism, we have the right to call it ‘the’ quotient of G by H. In the case when H is normal it turns out that G/H is affine and carries the structure of a linear algebraic group. In general, however, the quotient will only be a quasi-projective variety. This construction will use the last dose of foundational inputs from algebraic geometry that we require in this text.

At the end of the chapter we consider the more general issue of constructing the quotient of an affine variety by the action of a linear algebraic group.

16. A generic openness property

Most of this section is devoted to the following technical statement, which was already used in a weaker form in the previous section (Lemma 15.3).

Proposition 16.1. *Let $\phi : X \to Y$ be a morphism of irreducible quasi-projective varieties with Zariski dense image. Then X contains a nonempty open subset U such that $\phi|_U$ is an open mapping.*

We shall also use the proposition for *disjoint* unions of irreducible varieties; the extension of the statement is straightforward.

We start the proof with some lemmas.

Lemma 16.2. *If Y is an affine variety, the projection $p_1 : Y \times \mathbf{A}^1 \to Y$ is an open mapping.*

Proof. It will be enough to prove that $p_1(D(f))$ is open in Y for each regular function $f \in \mathcal{A}_{Y\times\mathbf{A}^1} \cong \mathcal{A}_Y[t]$. Write $f = \Sigma f_i t^i$ with $f_i \in \mathcal{A}_Y$. We contend that $p_1(D(f)) = \bigcup D(f_i)$. Indeed, if $(P, \alpha) \in Y \times \mathbf{A}^1$ with $f(P, \alpha) \neq 0$, we must have $f_i(P) \neq 0$ for some i. Conversely, if $f_i(P) \neq 0$ for some i, then the polynomial $\Sigma f_i(P)t^i \in k[t]$ is nonzero, so we find $\alpha \in k$ with $f(P, \alpha) = \Sigma f_i(P)\alpha^i \neq 0$. □

Now recall that when X and Y are affine, a morphism ϕ as in the proposition induces a homomorphism $\phi^* : \mathcal{A}_Y \to \mathcal{A}_X$ which is in fact injective (because so is the induced morphism on function fields; cf. Remark 13.3).

Lemma 16.3. *The proposition holds in the case when X and Y are affine and ϕ^* induces an isomorphism $\mathcal{A}_X \cong \mathcal{A}_Y[f]$ with some $f \in \mathcal{A}_X$.*

Proof. In the case when f is transcendental over $k(Y)$ we have $X \cong Y \times \mathbf{A}^1$, and we are done by the previous lemma. So we may assume f is algebraic over $k(Y)$. Let $F \in k(Y)[t]$ be its minimal polynomial, and let $a \in \mathcal{A}_Y$ be a common denominator of its coefficients. Replacing Y by the affine open subset $D(a)$ and X by an affine open subset of its preimage we may assume $a = 1$, i.e. $F \in \mathcal{A}_Y[t]$. Then $\mathcal{A}_X \cong \mathcal{A}_Y[t]/(F)$, because if $G \in \mathcal{A}_Y[t]$ satisfies $G(f) = 0$, we find $H, R \in \mathcal{A}_Y[t]$ with $G = HF + R$ and $\deg(R) < \deg(f)$ (observe that F is monic!), so that $R(f) = 0$ and hence $R = 0$ by minimality of $\deg(F)$. It follows that $\mathcal{A}_X$ is a free $\mathcal{A}_Y$-module of rank $d = \deg(f)$.

We now show that for the X and Y just obtained ϕ is an open mapping, i.e. for $f \in \mathcal{A}_X$ the image of the basic open set $D(f)$ by ϕ is open. Let $\Phi = t^d + f_{d-1}t^{d-1} + \cdots + f_0 \in \mathcal{A}_Y[t]$ be the characteristic polynomial of multiplication by f on the free $\mathcal{A}_Y$-module $\mathcal{A}_X$. We show that $\phi(D(f)) = \bigcup D(f_i)$. On the one hand, if P is a maximal ideal of $\mathcal{A}_X$ not containing f (this corresponds to a point of $D(f)$), then P does not contain all the f_i, for otherwise the equation $\Phi(f) = 0$ (Cayley-Hamilton theorem) would imply $f^d \in P$ and hence $f \in P$ by primeness of P, a contradiction. Conversely, if $Q \subset \mathcal{A}_Y$ is a maximal ideal coming from a point of one of the $D(f_i)$, it suffices to show that the radical R of the ideal $Q\mathcal{A}_X$ does not contain f. Indeed, by the Nullstellensatz R is the intersection of the maximal ideals containing it, so we find a maximal ideal P with $f \notin P$ and $P \cap \mathcal{A}_Y = Q$, which in turn corresponds to a point of $D(f)$ in the preimage of $D(f_i)$. To prove our claim about R, assume $f \in R$, i.e. $f^m \in Q$ for some $m > 0$. But then in the k-vector space $\mathcal{A}_X/Q \cong (\mathcal{A}_Y/Q)^d \cong k^d$ the image of f mod Q defines a nilpotent endomorphism, whereas by assumption its characteristic polynomial, which is Φ mod Q, is not of the form t^d, a contradiction. □

Proof of Proposition 16.1: Let U be an affine open subset (Lemma 12.5) of Y, and V an affine open subset of $\phi^{-1}(U)$. By the irreducibility of X the subset V is dense in $\phi^{-1}(U)$, hence so is $\phi(V)$ in U. Thus we may assume X and Y are affine by replacing them with V and U, respectively. In this case $\mathcal{A}_X$ is finitely generated as an $\mathcal{A}_Y$-algebra via the embedding $\phi^* : \mathcal{A}_Y \to \mathcal{A}_X$ (as it is already finitely generated over k), so we may write $\mathcal{A}_X = \mathcal{A}_Y[f_1, \ldots, f_n]$ for suitable f_i. Now consider the factorisation of ϕ^* into the sequence of morphisms

$$\mathcal{A}_Y \to \mathcal{A}_Y[f_1] \to \mathcal{A}_Y[f_1, f_2] \to \cdots \to \mathcal{A}_Y[f_1, \ldots, f_n] = \mathcal{A}_X. \tag{5}$$

By Proposition 2.5 each intermediate map here corresponds to a morphism of affine varieties, so we obtain a factorisation of ϕ into a composite of morphisms to which the above lemma applies. □

Remark 16.4. Using the method of the above proof it is easy to give an elementary proof of a special case of Corollary 13.7 which will be needed later: *If $\phi : X \to Y$ is a morphism of quasi-projective varieties with dense image and finite fibres, then* $\dim X = \dim Y$. Indeed, it is sufficient to examine a chain as in (5). If one of the f_i were transcendental over $\mathcal{A}_Y$, then one of the intermediate morphisms would have fibres isomorphic to $\mathbf{A}^1$ which are of course infinite.

The full statement of Proposition 16.1 will be used in the next section. Here are some other important corollaries which already follow from the weaker form (Lemma 15.3).

Corollary 16.5. *Let $\phi : G \to G'$ be a morphism of affine algebraic groups. Then $\phi(G)$ is a Zariski closed subgroup in G'.*

Proof. Let $H \subset G'$ be the Zariski closure of $\phi(G)$. We first show that it is a subgroup of G' (this is in fact true for the closure of a subgroup in any topological group). Indeed, if $x \in H$ and U is an open neighborhood of x containing $h \in \phi(G)$, then $h'U$ is an open neighbourhood of $h'x$ containing $h'h$ for all $h' \in \phi(G)$. Thus $\phi(G)H \subset H$, and continuing the argument shows that $HH \subset H$. The inclusion $H^{-1} \subset H$ is checked in a similar way.

Assume now G is connected. By Lemma 15.3 $\phi(G)$ contains a Zariski open subset U. Since the open sets $\phi(g)U$ cover $\phi(G)$ for $g \in G$, it follows that $\phi(G)$ is open and dense in H. If $h \in H$, then $h\phi(G) \cap \phi(G)$ is an intersection of dense open subsets in the irreducible variety H, hence nonempty. It follows that $h \in \phi(G)\phi(G)^{-1} \subset \phi(G)$.

In the general case write G as a finite union of cosets g_iG°, where $g_1, \dots, g_n \in G$ and G° is the connected component of identity as in Proposition 2.3. By the connected case $\phi(G^\circ)$ is closed in G'. Hence so is $\phi(G)$ which is the finite union of the $\phi(g_iG^\circ) = \phi(g_i)\phi(G^\circ)$. □

Corollary 16.6. *Let G be a connected affine algebraic group. Then $[G, G]$ is closed and connected.*

Proof. Let $\phi_i : G^{2i} \to G$ be the morphisms considered in the proof of Lemma 8.3. The union of the $\mathrm{Im}\,(\phi_i)$ equals $[G, G]$. The closures Z_i of the $\mathrm{Im}\,(\phi_i)$ are irreducible closed subsets in G whose union H is the closure of $[G, G]$; it is again irreducible. The chain $Z_1 \subset Z_2 \subset \cdots$ must stabilize for dimension reasons, so we find n such that $Z_n = H$. Lemma 15.3 applied to $\phi_n : G^n \to H$ shows that $\mathrm{Im}\,(\phi_n)$ contains an open subset $U \subset H$. Given $h \in H$, we have $U \cap hU \neq \emptyset$ as H is irreducible. So $h \in UU^{-1} \subset \mathrm{Im}\,(\phi_n)\mathrm{Im}\,(\phi_n)$. This shows $H = [G, G]$. □

We close this section by two statements needed later that are proven by a method similar to that of Proposition 16.1. The first of these is:

Proposition 16.7. *Let $\phi : X \to Y$ be an* injective *morphism of irreducible quasi-projective varieties with Zariski dense image. If the induced field extension $k(X)|\phi^*k(Y)$ is separable, then in fact $k(X) = \phi^*k(Y)$.*

Using the arguments of the proof of Proposition 16.1, we see that the proposition is a consequence of the following lemma.

Lemma 16.8. *Assume that* $\phi : X \to Y$ *is a morphism of irreducible affine varieties and* ϕ^* *induces an isomorphism* $\mathcal{A}_X \cong \mathcal{A}_Y[f]$ *with* f *separable over* $k(Y)$*. Then there is an open subset* $V \subset Y$ *such that each point of* V *has exactly* $[k(X) : \phi^* k(Y)]$ *preimages in* X*.*

Proof. As in the proof of Lemma 16.3 we may assume $\mathcal{A}_X \cong \mathcal{A}_Y[t]/(F)$, where $F \in \mathcal{A}_Y[t]$ is the minimal polynomial of f over $k(Y)[t]$. The degree of F equals that of the field extension $\phi(X)|\phi^* k(Y)$; let us denote it by d. As F is a separable polynomial, its derivative F' is prime to F in the ring $k(Y)[t]$. Hence we find polynomials $A, B \in k(Y)[t]$ satisfying $AF + BF' = 1$. Multiplying with a common denominator in $g \in \mathcal{A}_Y$ of the coefficients of A and B we obtain polynomials $C = gA, D = gB \in \mathcal{A}_Y[t]$ with $CF + DF' = g$. We claim that $V = D(g)$ is a good choice. Assume Q is a maximal ideal in $\mathcal{A}_Y$ with $g \notin Q$. The image $\bar{F}$ of F in $(\mathcal{A}_Y/Q)[t] \cong k[t]$ has d distinct roots in k, for reducing $CF + DF' = g \bmod Q$ we obtain $\bar{C}\bar{F} + \bar{D}\bar{F}' \neq 0$, so $\bar{F}(\alpha) = 0$ implies $\bar{F}'(\alpha) \neq 0$. Thus $\bar{F}$ is a product of d distinct linear factors, and therefore by the Chinese Remainder Theorem $\mathcal{A}_X/Q\mathcal{A}_X \cong k[t]/(\bar{F}) \cong k^d$. In particular, this ring is reduced, so the ideal $Q\mathcal{A}_X$ equals its radical. Now the preimages of the point of $D(g)$ defined by Q correspond to the maximal ideals $P_1, \dots, P_r \subset \mathcal{A}_X$ containing the radical ideal $Q\mathcal{A}_X$, so by the Nullstellensatz $Q\mathcal{A}_X = \cap P_i$ and by the Chinese Remainder Theorem $\mathcal{A}_X/Q\mathcal{A}_X \cong \oplus(\mathcal{A}_X/P_i) \cong k^r$. Thus $r = d$, as required. □

Remarks 16.9.

(1) An analysis of the above proof shows that when the polynomial F is not necessarily separable, at least one obtains that each point of Y has at most $d = [k(X) : \phi^* k(Y)]$ preimages in X.

(2) In the jargon of algebraic geometry the lemma claims that the morphism ϕ is *étale* over an open subset of Y, or in other words it is *generically étale.* Similarly, in the proof of Lemma 16.3 we have first proven that ϕ is *generically faithfully flat*, and then that a finite flat morphism is an open mapping. Generic faithful flatness is a key property in the theory of group schemes that is used for the construction of quotients in a more general setting than ours.

The second statement we prove by the method of of Proposition 16.1 will not be used until Section 26.

Proposition 16.10. *Let* $\phi : X \to Y$ *be a morphism of irreducible quasi-projective varieties with Zariski dense image. There exists a dense open subset* $U \subset Y$ *such that for each* $P \in U$ *the fibre* $\phi^{-1}(P)$ *has dimension* $\dim X - \dim Y$*.*

Recall (Corollary 13.7) that each irreducible component of a nonempty fibre has dimension at least $\dim X - \dim Y$.

Proof. As in the proof of Proposition 16.1 we reduce to the case when X and Y are affine and $\mathcal{A}_X \cong \mathcal{A}_Y[f_1, \ldots, f_n]$. We may assume that $f_1, \ldots, f_r$ are algebraically independent over $k(Y)$, and $f_{r+1}, \ldots, f_n$ are algebraic over $k(Y)(f_1, \ldots, f_r)$. Here we must have $r = \dim X - \dim Y$, because the extension $k(X)|k(Y)(f_1, \ldots, f_r)$ is finite. On the other hand, Corollary 2.6 implies that ϕ factors as $X \to Z \to Y$, where Z is the variety with coordinate ring $\mathcal{A}_Y[f_1, \ldots, f_r]$. From the proof of Lemma 16.3 we see that the map $X \to Z$ has finite fibres, whereas the fibres of $Z \to Y$ have dimension r, since $Z \cong Y \times \mathbf{A}^r$ by construction. □

Corollary 16.11. *Given a morphism $\phi : G \to G'$ of connected algebraic groups, we have* $\dim G = \dim \mathrm{Im}\,(\phi) + \dim \mathrm{Ker}\,(\phi)$.

Proof. Using Corollary 16.5 we see that $\mathrm{Im}\,(\phi)$ is a connected algebraic group. Since ϕ is a morphism of algebraic groups, each fibre $\phi^{-1}(g)$ for $g \in \mathrm{Im}\,(\phi)$ is a coset of $\mathrm{Ker}\,(\phi)$, hence isomorphic to $\mathrm{Ker}\,(\phi)$ as a closed subvariety of G. In particular, they all have the same dimension, and the corollary follows from the proposition. □

17. Homogeneous spaces

As a first step towards the construction of quotients we study *homogeneous spaces.*

Definition 17.1. A (left) homogeneous space for an algebraic group G is a quasi-projective variety on which G acts *transitively* (on the left).

If $H \subset G$ is a closed subgroup, then clearly any reasonable definition of the quotient G/H should include the fact that G/H is a homogeneous space for G.

Lemma 17.2. *The irreducible components of a homogeneous space are the same as its connected components. They are all isomorphic as quasi-projective varieties.*

Proof. Same proof as in the special case of G as a homogeneous space under itself (Proposition 2.3 (1).) □

Lemma 17.3. *Let G be an algebraic group, X and Y homogeneous spaces under G, and $\phi : X \to Y$ a morphism compatible with the action on G. Then ϕ is an open mapping.*

Proof. Assume first X and Y are connected. By Proposition 16.1 there exists $U \subset X$ such that $\phi|_U$ is open. Then for all $g \in G$ the restriction $\phi|_{gU}$ must be open as well, because $x \mapsto gx$ is a homeomorphism of X onto itself. But the gU for all $g \in G$ form an open covering of X, whence the lemma.

In the general case ϕ must map each connected component of X in a connected component of Y and we may apply the above argument componentwise (after restricting to the stabilizer of the component). $\square$

The following result will be the key step in the construction of the quotient of an affine algebraic group by a closed subgroup.

Proposition 17.4. *Let G be an affine algebraic group, and $H \subset G$ a closed subgroup. There exists a homogeneous space X for G together with a point P in X such that H is the stabilizer of P and the fibres of the natural surjection $\rho : G \to X$ given by $g \mapsto gP$ are exactly the left cosets gH of H.*

Proof. By Lemma 4.2 there is a morphism of algebraic groups $G \to \mathrm{GL}(V)$ such that H is the stabilizer of a 1-dimensional subspace $\langle v \rangle$ in V. Let X be the orbit of $P = \langle v \rangle$ in the projective space $\mathbf{P}(V)$. By Corollary 15.4 X is open in its Zariski closure, hence it is a quasi-projective variety and therefore a homogeneous space for G. It manifestly satisfies the other requirements of the proposition. $\square$

The problem with the above construction is that it is not canonically attached to the pair $H \subset G$. In the next two sections we carry out the extra work needed for making it canonical.

18. Smoothness of homogeneous spaces

We now bring into play an important local property of varieties. Recall that the tangent space of a point P on an affine variety X was defined in Section 9. Using Lemma 9.1 the definition immediately extends to arbitrary quasi-projective varieties.

Definition 18.1. *On an irreducible quasi-projective variety a point $P \in X$ is a* smooth point *if $\dim T_P(X) = \dim X$, otherwise it is a* singular point*. The variety is smooth if all of its points are smooth, otherwise it is singular.*

The definition obviously extends to finite disjoint unions of irreducible varieties, so in particular to algebraic groups and their homogeneous spaces.

Proposition 18.2. *A homogeneous space under an algebraic group G is a smooth variety. In particular, G itself is smooth.*

Proof. For a homogeneous space X the map $x \mapsto gx$ is an isomorphism of X with itself for each $g \in G$. On the other hand, an isomorphism takes smooth points to smooth points (this follows e.g. from Lemma 9.1 and the fact that the isomorphism preserves the maximal ideals of the points). So taking the transitivity of the G-action on X and Lemma 17.2 into account the proposition follows from the lemma below. $\square$

Lemma 18.3. *An irreducible quasi-projective variety has a smooth point. These form a dense open subset.*

Proof. The proof consists of two steps.
Step 1. The lemma is true for an affine hypersurface $V(f) \subset \mathbf{A}^n$ defined by an irreducible polynomial $f \in k[x_1, \dots, x_n]$ with $\partial_{x_n} f \neq 0$.[2] Indeed, we find $P \in V(f)$ with $\partial_{x_n} f(P) \neq 0$, for otherwise by the Nullstellensatz the irreducible polynomial f would divide some power $(\partial_{x_n} f)^m$, hence $\partial_{x_n} f$, which is impossible. Then $T_P(V(f))$ is defined by a single nonzero linear equation and hence has dimension $n-1$, just like $V(f)$. This proves Step 1, and moreover shows that all points of the open subset $D(\partial_{x_n} f) \subset V(f)$ are smooth.
Step 2. An irreducible variety X contains an open subset U isomorphic to an open subset $V \subset V(f)$ for suitable f as above. This will prove the lemma, for irreducibility of $V(f)$ implies $V \cap D(\partial_{x_n} f) \neq \emptyset$. To prove Step 2 we may assume, by intersecting with some $D_+(x_i)$, that X is an open subset of some affine variety $\bar{X} \subset \mathbf{A}^m$, and then that $X = \bar{X}$. By a general theorem in algebra we find algebraically independent elements $x_1, \dots, x_{n-1} \in k(X)$ so that $k(X) = k(x_1, \dots, x_{n-1}, x_n)$ with x_n satisfying an irreducible polynomial $f \in k[x_1, \dots, x_{n-1}, x]$ with $\partial_x f \neq 0$. In particular, $k(X) \cong k(V(f))$. Choosing an open $U \subset X$ such that all x_i are regular on X we obtain a morphism $U \to V(f)$ defined by $(x_1, \dots, x_n)$. In the same way, the restrictions of the coordinate functions $y_1, \dots, y_m$ of $\mathbf{A}^m$ to X define a morphism $V \to X$ for suitable $V \subset V(f)$. The reader will check that these maps are inverse to each other whenever both are defined, so after possibly shrinking U and V we are done. ☐

Remark 18.4. In the language of algebraic geometry, in Step 2 of the above proof we have shown that X is *birational* to the affine hypersurface $V(f)$.

Finally, we need for later use the following fact.

Lemma 18.5. *If P is a smooth point on a variety X, then the local ring $\mathcal{O}_{X,P}$ is a unique factorisation domain.*

Proof. Recall that we have identified $T_P(X)$ with the dual k-vector space of M_P/M_P^2, where M_P is the maximal ideal of $\mathcal{O}_{X,P}$. It follows that P is a smooth point if and only if $\dim_k M_P/M_P^2 = \dim X = \dim \mathcal{O}_{X,P}$. In commutative algebra a local ring with this property is called a *regular local ring*, and it is quite generally true that these rings are UFD's (see e.g. Matsumura, Commutative ring theory, Theorem 20.3). There is also a direct proof of the special case we need which goes back to Zariski. It proceeds by comparing $\mathcal{O}_{X,P}$ with its completion

[2] This condition is automatic in characteristic 0, but not in characteristic $p > 0$: think of the polynomial $x_1^p + \dots + x_n^p$.

which is a power series ring, hence a UFD; one shows that the UFD property 'descends' from the completion to $\mathcal{O}_{X,P}$. □

The lemma will be used through the following corollary.

Corollary 18.6. *Let f be a rational function on a quasi-projective variety X which is not regular at a smooth point $Q \in X$. Then there is a point $P \in X$ where $1/f$ is regular and $(1/f)(P) = 0$.*

Proof. By replacing X with an affine open subset containing Q we may assume X is affine, and may choose a representation $f = g/h$ with $g, h \in \mathcal{A}_X$. Since $\mathcal{O}_{X,Q}$ is a UFD which is a localisation of $\mathcal{A}_X$, in $\mathcal{O}_{X,Q}$ we may write $g = up_1^{a_1} \dots p_r^{a_r}$ and $h = vq_1^{b_1} \dots q_s^{b_s}$ with p_i, q_j irreducible elements of $\mathcal{O}_{X,Q}$ lying in $\mathcal{A}_X$ and u, v units in $\mathcal{O}_{X,Q}$; moreover, h is not a unit since $f \notin \mathcal{O}_{X,Q}$. By unique factorisation we may assume that there is no equality $p_i = wq_j$ with w a unit in $\mathcal{O}_{X,Q}$. Now if we find P with $g(P) \neq 0$ but $h(P) = 0$, we are done. Otherwise $h(P) = 0$ implies $g(P) = 0$ for all P, i.e. $g \in I(V(h))$. By the Nullstellensatz we thus have $g^m \in (h)$ for some $m > 0$, i.e. h divides g^m in $\mathcal{A}_X$, and hence in the local ring $\mathcal{O}_{X,Q}$ as well. This contradicts our assumptions that h is not a unit and there is no equation of the form $p_i = wq_j$. □

Remarks 18.7.

(1) The corollary is false in general. Consider the function y/x on the affine plane curve $y^2 = x^3$. It is not regular at the singular point $(0, 0)$, but x/y does not vanish anywhere on the curve.
(2) If $\dim X = 1$, one may choose $P = Q$ in the corollary. Indeed, in this case the local ring $\mathcal{O}_{X,Q}$ is a *discrete valuation ring*, and such rings always contain either f or $1/f$ for an f in their fraction field. However, for $\dim X > 1$ the ring $\mathcal{O}_{X,Q}$ does not have this property, so the corollary does not hold with $P = Q$.

19. Quotients of affine groups

We now turn to the canonical construction of quotients.

Let G be an affine algebraic group, and $H \subset G$ a closed subgroup. Consider pairs (X, ρ) consisting of a quasi-projective variety X and a morphism $G \to X$ that is constant on the left cosets of H.

Definition 19.1. *The pair (X, ρ) is the quotient of G by H if for any other pair (X', ρ') as above there is a morphism $\phi : X \to X'$ with $\phi \circ \rho = \rho'$.*

By general abstract nonsense a quotient (X, ρ) is unique up to unique isomorphism. We'll use the following criterion:

Lemma 19.2. *Assume that (X, ρ) is a pair as above such that*

(1) *each fibre of ρ is a left coset of H in G;*

(2) *for each open set $U \subset X$ the map ρ^* induces an isomorphism of $\mathcal{O}(U)$ with the ring of those $f \in \mathcal{O}(\rho^{-1}(U))$ that satisfy $f(hP) = f(P)$ for all $h \in H$ and $P \in \rho^{-1}(U)$;*

(3) *X is a homogeneous space of G and $\rho : G \to X$ is a morphism of homogeneous spaces of G.*

Then (X, ρ) is the quotient of G by H.

Proof. Assume given $\rho' : G \to X'$ constant on the left cosets of H. For $P \in X$ define $\phi(P) := \rho'(g)$, where $g \in G$ is such that $\rho(g) = P$. The map ϕ is well-defined by property (1). It is also continuous, because ρ' is continuous and ρ is open by property (3) and Lemma 17.3. Finally ϕ is a morphism of quasi-projective varieties by property (2). □

Theorem 19.3. *Let G be an affine algebraic group, $H \subset G$ a closed subgroup. Then the quotient of G by H exists. Moreover, it is a homogeneous space for G such that H is the stabilizer of a point.*

Proof. Let (X, ρ) be the pair constructed in Proposition 17.4. To show that it is a quotient it remains to check property (2) of Lemma 19.2. It is enough to check this property for a connected affine open subset $U \subset X$. Pick $f \in \mathcal{O}(\rho^{-1}(U))$ constant on the left cosets of H, and consider the composite map $\rho^{-1}(U) \xrightarrow{(\rho,f)} U \times \mathbf{A}^1 \to U$, where the last map is the natural projection. Note that $\rho^{-1}(U)$ is a finite disjoint union of connected open sets, each one dense in a component of G. Let Z be the closure of $\mathrm{Im}\,(\rho, f)$ in $U \times \mathbf{A}^1$; it is an affine variety. Let $V \subset Z$ be a dense open subset contained in $\mathrm{Im}\,(\rho, f)$ (which exists by Lemma 15.3); it is quasi-projective. We may view the projection $V \to \mathbf{A}^1$ as a regular function $\bar{f}$ on V; it satisfies $\bar{f} \circ (\rho, f) = f$. We have to show that $\bar{f} = p^*g$ for some $g \in \mathcal{O}(U)$, for then $f = \rho^*g$. Since f is constant on H-orbits, the projection $p : V \to U$ is injective, and it has dense image. This implies that we must have $\dim V = \dim U$. Hence the induced field extension $[k(V) : p^*k(U)]$ is finite; moreover, it is separable.[3] Hence by Proposition 16.7 the map $p^* : k(U) \to k(V)$ is an isomorphism, so $\bar{f} = p^*g$ for some $g \in k(U)$. It remains to see that g is regular on U. For this we use Corollary 18.6 (with U in place of X and g in place of f), which applies by virtue of Proposition 18.2. It shows that if g is not regular, then $1/g$ vanishes somewhere on U, but then $1/f = \rho^*(1/g)$ should vanish somewhere on $\rho^{-1}(U)$, a contradiction. □

Similarly, one proves starting from Proposition 4.3:

[3]Separability is automatic in characteristic 0. It also holds in characteristic $p > 0$, though it is not obvious to prove; one has to study the induced morphism on tangent spaces, and use the differential criterion of separability. We omit the details of the argument, which uses the explicit form of X as constructed in Proposition 17.4.

Theorem 19.4. *In the previous theorem assume moreover that H is normal. Then G/H is an affine algebraic group, and $\rho : G \to G/H$ is a morphism of algebraic groups.*

Proof. By Proposition 4.3 there is a morphism of algebraic groups $\rho : G \to \mathrm{GL}(W)$ with $H = \mathrm{Ker}\,(\rho)$. By Corollary 16.5 $\mathrm{Im}\,(\rho)$ is a closed subgroup of $\mathrm{GL}(W)$. The same argument as above shows that the pair $(\mathrm{Im}\,(\rho), \rho)$ satisfies the assumptions of Lemma 19.2. □

The theorem allows us to give other classical examples of linear algebraic groups.

Example 19.5. If G is an affine algebraic group, then $G/Z(G)$ is also an affine algebraic group by the theorem. For example, in the case $G = \mathrm{GL}_n$ we obtain the projective general linear group PGL_n, and for $G = \mathrm{SL}_n$ the projective special linear group PSL_n.

20. Quotients of varieties by group actions

In the remainder of this chapter, whose results will not be used later, we consider a more general situation. Suppose G is an affine algebraic group, and X is an affine variety on which G acts as an algebraic group. We would like to know whether a quotient Y of X by the action of G exists as an affine variety.

The following easy example shows that in general one cannot expect the set of G-orbits to carry the structure of a variety over k.

Example 20.1. Consider the natural action of $\mathbf{G}_m$ on $\mathbf{A}^1$ given by $(\lambda, x) \mapsto \lambda x$. It has two orbits: one closed, namely $\{0\}$, and one open, namely $\mathbf{A}^1 \setminus \{0\}$. But this open orbit can never be a fibre of a morphism of $\mathbf{A}^1 \to Y$ with some variety Y because it is not closed in $\mathbf{A}^1$. (In fact, the right category in which the quotient $\mathbf{A}^1/\mathbf{G}_m$ makes sense is that of algebraic stacks.)

Fortunately, for a large class of groups G there exists a quotient parametrizing *closed* orbits of G on X. Moreover, the quotient will satisfy the following universal property generalizing Definition 19.1.

Definition 20.2. (Mumford) Let G be an affine algebraic group acting on a quasi-projective k-variety X. Consider pairs (Y, ρ) consisting of a quasi-projective variety Y and a morphism $\rho : G \to Y$ constant on the orbits of G. The pair (Y, ρ) is a *categorical quotient* of X by G if for every other such pair (Y', ρ') there is a unique morphism $\phi : Y \to Y'$ with $\rho' = \phi \circ \rho$.

A good class of groups G for which the categorical quotient exists is that of groups satisfying the following property.

Definition 20.3. An affine algebraic group G is *geometrically reductive* if for every finite-dimensional representation $G \mapsto \mathrm{GL}(V)$ and each fixed vector $v_0 \in V^G$ there exists a homogeneous G-invariant polynomial f on V such that $f(v_0) \neq 0$.

In the case when f has degree 1, it is an element of the dual space $V^\vee$; in general it is an element of some symmetric power $Sym^d(V^\vee)$ (see the proof of Lemma 5.11).

In fact, we can say a bit more about the polynomial f.

Lemma 20.4. *Let $G \to GL(V)$ and v_0 be as in the above definition.*

(1) *If* $\operatorname{char}(k) = 0$, *one can find f as in the definition with* $\deg(f) = 1$.
(2) *If* $\operatorname{char}(k) = p > 0$, *one can find f as in the definition with* $\deg(f) = p^r$ *for an integer $r \geq 0$.*

Proof. Pick f of degree d as in Definition 20.3, and for $\lambda \in k$ consider the affine linear map $v \mapsto \lambda v + v_0$ on V. Substituting in f we may develop following λ as

$$f(\lambda v + v_0) = \sum_{i=0}^{d} \lambda^i f_i(v)$$

with homogeneous polynomials f_i of degree i. Since v_0 and f are G-invariant, so are the f_i. Substituting $v = v_0$ gives

$$(\lambda + 1)^d f(v_0) = f(\lambda v_0 + v_0) = \sum_{i=0}^{d} \lambda^i f_i(v_0),$$

so by comparing coefficients of λ^i we get

$$\binom{d}{i} f(v_0) = f_i(v_0).$$

In characteristic 0 the binomial coefficients are nonzero, whence $f_1(v_0) \neq 0$. In characteristic $p > 0$ write $d = p^r s$ with $(s, p) = 1$. Then $\binom{d}{p^r}$ is not divisible by p, and so $f_{p^r}(v_0) \neq 0$. □

Remark 20.5.

(1) If $\deg(f) = 1$ works for all v_0, one says that G is *linearly reductive.* In this case it is not hard to show that every finite-dimensional representation $G \mapsto \mathrm{GL}(V)$ is completely reducible (i.e. each G-invariant subspace has a G-invariant complement).
(2) In characteristic $p > 0$ one can show that GL_n is geometrically reductive but not linearly reductive. In fact, a theorem of Nagata says that in characteristic $p > 0$ the only connected linearly reductive groups are tori.
(3) Geometrically reductive groups are exactly the reductive groups of Definition 23.9 below. That reductive groups are geometrically reductive can be proven using some Lie algebra theory in

characteristic 0 and is a difficult theorem of Haboush in characteristic $p > 0$ (formerly a conjecture by Mumford). The converse is not hard to show in characteristic 0; see Remark 20.9 below for the general case.

We can now state:

Theorem 20.6. *Let G be a geometrically reductive affine algebraic group acting on an affine variety X. A categorical quotient $\rho : X \to Y$ of X by G exists. Moreover, Y is an affine variety and each fibre of ρ contains exactly one (nonempty) closed G-orbit on X.*

Remark 20.7. We thus see that the points of Y correspond bijectively to the closed G-orbits on X. Moreover, the theorem implies that in the case when all G-orbits on X are closed, the fibres of ρ are exactly the G-orbits. A categorical quotient with this property is called a *geometric quotient.*

The following theorem contains the key algebraic ingredient in the proof of the theorem above. First some terminology: an action of a group G on a k-algebra A is *locally finite* if every finite-dimensional k-subspace of A is contained in a finite-dimensional G-invariant subspace. By Remark 3.4 this is the case for the G-action on $\mathcal{A}_X$ coming from the action of an affine group G on an affine variety X.

Theorem 20.8. (Hilbert, Nagata) *Let A be a finitely generated k-algebra equipped with a locally finite action of a geometrically reductive group G. Then A^G is also a finitely generated k-algebra.*

Remarks 20.9.

(1) The subalgebra A^G may not be finitely generated in general, even when A is the coordinate ring of an affine variety on which an affine group G acts. Indeed, there is a famous example of Nagata exhibiting an action of a direct power $\mathbf{G}_a^r$ of the additive group on some affine space $\mathbf{A}^n$ such that $k[x_1, \dots, x_n]^{\mathbf{G}_a^r}$ is not a finitely generated k-algebra.

(2) One can show that if A^G is finitely generated for all A, then G is reductive. The idea is that if G is not reductive (i.e. has a nontrivial connected unipotent normal subgroup), one can construct an A with A^G not finitely generated by performing a fibre product construction starting from Nagata's example. Together with Theorem 20.8, this shows that geometrically reductive groups are reductive.

21. Proof of the Hilbert-Nagata theorem

We start the proof of Theorem 20.8 with the following lemma.

Lemma 21.1. *Let A be a k-algebra equipped with a locally finite action of a geometrically reductive group G. If $I \subset A$ is a G-invariant* *ideal, then the the natural map $A^G \to (A/I)^G$ induces an* integral *ring extension $A^G/I^G \subset (A/I)^G$.*

Recall that a ring extension $A \subset B$ is integral if for every $b \in B$ satisfies a monic polynomial equation over A; this is equivalent to the A-algebra $A[b] \subset B$ being finitely generated as an A-module.

Proof. Pick an element $\bar{a} \in (A/I)^G$ and lift it to $a \in A$. Since the action of G on A is locally finite, the G-orbit of a spans a finite-dimensional G-invariant subspace $V \subset A$. Moreover, by the choice of a we have $\sigma(a) - a \in I \cap V$ for all $\sigma \in V$, so there is a direct sum decomposition $V = \langle a \rangle \oplus (I \cap V)$. It also follows that the linear form $\lambda \in V^\vee$ which is 0 on $I \cap V$ and 1 on a is G-invariant. Therefore by geometric reductivity there is some $f \in Sym^d(V^{\vee\vee})^G = Sym^d(V)^G$ with $f(\lambda) = 1$. Choose a k-basis $v_2, \dots, v_n$ of $I \cap V$. We may view the vectors $a = v_1, v_2, \dots, v_n$ as coordinate functions on $V^\vee$, so that λ becomes the point with coordinates $(1, 0, \dots, 0)$. The relation $f(\lambda) = 1$ then means that f as a homogeneous polynomial in the v_i defines an element of A^G of the form $v_1^d +$ terms lying in I. But then f maps to $\bar{a}^d$ in A/I, which implies $\bar{a}^d \in A^G/I^G$. In particular $\bar{a}$ is integral over A^G/I^G. □

Corollary 21.2. *In the situation of the lemma assume moreover that $(A/I)^G$ is a finitely generated k-algebra. Then so is A^G/I^G.*

Proof. Let $a_1, \dots, a_n$ be a system of generators of the k-algebra $(A/I)^G$. By the lemma, each a_i satisfies a monic polynomial equation f_i over A^G/I^G; let $A_0 \subset A^G/I^G$ be the k-subalgebra generated by the finitely many coefficients of the f_i. This is a Noetherian ring, and A^G/I^G is an A_0-submodule of the finitely generated A_0-module $(A/I)^G$. Hence it is also a finitely generated A_0-module, and therefore a finitely generated k-algebra. □

The following corollary will serve in the proof of Theorem 20.6.

Corollary 21.3. *For G and A as in the lemma, let $I_1, I_2 \subset A$ be G-invariant ideals. If $a \in (I_1 + I_2)^G$, then $a^d \in I_1^G + I_2^G$ for some $d > 0$.*

In particular, if moreover $I_1 + I_2 = A$, we find $f_1 \in I_1^G$, $f_2 \in I_2^G$ with $f_1 + f_2 = 1$.

Proof. Only the first statement requires a proof. Write $a = a_1 + a_2$ with $a_i \in I_i$ $(i = 1, 2)$. Note that for $\sigma \in G$ we have

$$\sigma(a_1) - a_1 = a_2 - \sigma(a_2) \in I_1 \cap I_2,$$

so if we write $\bar{A} := A/I_1 \cap I_2$ and $\bar{a}_i := a_i \bmod I_1 \cap I_2$, we conclude that $\bar{a}_i \in \bar{A}^G$. By the (proof of the) lemma applied to the ideal $I_1 \cap I_2 \subset A$, we therefore find $d > 0$ with $\bar{a}_i^d \in I_i^G/(I_1 \cap I_2)^G$ for $i = 1, 2$, i.e. $a_i^d \in I_i^G + (I_1 \cap I_2)^G \subset I_i^G$. According to Lemma 20.4, in characteristic 0 we may take $d = 1$ and hence $a = a_1 + a_2 \in I_1^G + I_2^G$; in characteristic $p > 0$ we may take $d = p^r$ and $a^{p^r} = (a_1 + a_2)^{p^r} = a_1^{p^r} + a_2^{p^r} \in I_1^G + I_2^G$. □

Proof of Theorem 20.8. The proof is in several steps.

Step 1: We may assume that $(A/I)^G$ is finitely generated for every nonzero G-invariant ideal $I \subset A$. This is the principle of Noetherian induction. Assume A^G is not finitely generated, and consider the set of G-invariant ideals $J \subset A$ such that $(A/J)^G$ is not finitely generated, partially ordered with respect to inclusion. As A is Noetherian, this set has (possibly several) maximal elements; let $\bar{J}$ be such an element. Then $\bar{A} := A/\bar{J}$ has the property above, and if we obtain a contradiction for $\bar{A}$, we get a contradiction for A as well.

Step 2: We may assume that A^G has no zero-divisors. Assume $f \in A^G$ is a zero-divisor, and set $I := \mathrm{Ann}(f) = \{a \in A : af = 0\}$. The ideals fA and I are G-invariant, so by Step 1 the k-algebras $(A/fA)^G$ and $(A/I)^G$ are finitely generated. Hence so are the k-subalgebras $\bar{A}_1 := A^G/(fA \cap A^G)$ and $\bar{A}_2 := A^G/I^G$ by Corollary 21.2. Thus there is a finitely generated k-subalgebra $B \subset A^G$ mapping surjectively onto both $\bar{A}_1$ and $\bar{A}_2$. On the other hand, by Lemma 21.1 the finitely generated k-algebra $(A/I)^G$ is integral over $\bar{A}_2$ and hence over B. Thus it is a finitely generated B-module, and we find a finitely generated B-submodule $B[c_1, \dots, c_n] \subset A$ mapping surjectively onto $(A/I)^G$. Here for all $\sigma \in G$ we have $\sigma(c_j) = c_j + i_j$ for some $i_j \in I$, so since $I = \mathrm{Ann}(f)$ and $f \in A^G$, we get $fc_j \in A^G$ for all j. We contend that $A^G = B[fc_1, \dots, fc_n]$, which will imply the finite generation of A^G over k. Since B surjects onto $\bar{A}_1$, for each $a \in A^G$ we find $b \in B$ so that the element $a - b$ is G-invariant and moreover $a - b = fc$ with some $c \in A$. The image of f in A/I is G-invariant and a non-zerodivisor (again since $I = \mathrm{Ann}(f)$), whence the image of c in A/I must also be G-invariant. This shows $c \in B[c_1, \dots, c_n]$, as required.

Step 3: We may assume that A is a polynomial ring and the G-action preserves the homogeneous components of A. Let $a_1, \dots, a_n$ be generators of A over k. Since the action of G is locally finite, we find a G-invariant subspace $V \subset G$ containing the a_i. Changing the a_i if necessary, we may assume that they form a k-basis of V. For $\sigma \in G$ we have $\sigma(a_i) = \Sigma_j \alpha_{ij\sigma} a_j$ with some $\alpha_{ij\sigma} \in k$. Now define a G-action on the polynomial ring $S := k[x_1, \dots, x_n]$ via $\sigma(x_i) = \Sigma_j \alpha_{ij\sigma} x_j$ and a G-homomorphism $\phi : S \to A$ induced by $\phi(x_i) := a_i$. The kernel I of ϕ is a G-invariant ideal in S, and we have a G-isomorphism $A \cong S/I$. If S^G is a finitely generated k-algebra, so is $C := S^G/I^G$. So it will suffice to show that A^G is a finitely generated C-module. For this, notice first that both of these rings are integral domains by Step 2, and the fraction field L of A^G is a finite extension of C. Indeed, $L|K$ is an algebraic extension since A^G is integral over C by Lemma 21.1. On the other hand, L is finitely generated over K. This is obvious if A is a domain, for then L is a subfield of its fraction field which is finitely generated over k. Otherwise localize A by the set T of its non-zerodivisors. Every maximal ideal M of A_T consists of zero-divisors, so $A^G \cap M = 0$. Hence the natural inclusion $A^G \subset A_T$ induces an inclusion of fields $L \subset A_T/M$. But A_T/M is the fraction field of $A/A \cap M$, and as such finitely generated over k.

Finally, since C is a finitely generated k-algebra and $L|K$ is a finite extension, a theorem from commutative algebra says that the integral closure $\widetilde{C}$ of C in L is a finitely generated C-module. As A^G is integral over C, it is a C-submodule of $\widetilde{C}$, and hence also finitely generated because C is Noetherian.

Step 4: The case where A is a polynomial ring and the G-action preserves the homogeneous components of A. Denote by $A_d \subset A$ the homogeneous component of degree d and by A_+ the direct sum of the A_d for $d > 0$. We contend that $A_+^G = A^G \cap A_+$ is a finitely generated ideal in A^G. We may assume $A_+^G \neq 0$ (otherwise we are done), and pick a homogeneous $f \in A_+^G$. By Step 1 the k-algebra $(A/fA)^G$ is finitely generated, hence so is $A^G/(fA)^G$ by Corollary 21.2. But $(fA)^G = fA^G$ since f is a G-invariant non-zerodivisor (same argument as in Step 2), so A^G/fA^G is finitely generated over k. In particular, it is Noetherian and therefore the image of A_+^G in A^G/fA^G is finitely generated. Hence so is A_+^G (add f to a system of lifts of generators).

Let $f = f_1, \dots, f_r$ be a system of homogeneous generators of A_+^G, and set $d_i := \deg(f_i)$. For $d > \max d_i$ we have

$$A_d^G = \bigoplus_i A_{d-d_i}^G f_i.$$

It follows that A^G is generated as a k-algebra by the f_i and the A_r^G for $r \leq \max d_i$. But each A_r is a finite-dimensional k-vector space and we are done. □

22. Construction of categorical quotients

Now we can prove Theorem 20.6. As already remarked, if G and X are as in the theorem, the induced action of G on $\mathcal{A}_X$ is locally finite, hence $\mathcal{A}_X^G$ is finitely generated as a k-algebra by Theorem 20.8. Now fix an affine variety Y with $\mathcal{A}_Y \cong \mathcal{A}_X^G$ and consider the morphism $\rho : X \to Y$ corresponding to the inclusion $\mathcal{A}_X^G \to \mathcal{A}_X$ via Proposition 2.5.[4] Note that ρ is constant on the orbits of G.

Lemma 22.1.

(1) *If $Z \subset X$ is a G-invariant closed subvariety, then $\rho(X) \subset Y$ is also closed.*

[4]Since we are using the elementary Proposition 2.5, we have to choose objects and morphisms in an isomorphism class. This ambiguity disappears when one works with affine schemes instead.

(2) *If $W \subset X$ is another G-invariant closed subvariety with $Z \cap W = \emptyset$, then $\rho(Z) \cap \rho(W) = \emptyset$.*

Proof. For (1), pick an arbitrary $Q \in Y \setminus \rho(Z)$. Then $W := \rho^{-1}(Q)$ is a G-invariant closed subset with $Z \cap W = \emptyset$. Applying Corollary 21.3 to the ideals of Z and W in $\mathcal{A}_X$, we find $f, g \in \mathcal{A}_X^G$ with $f + g = 1$ and $f|_Z = 0$, $g|_W = 0$. Viewing f as a regular function on Y, it satisfies $f|_{\rho(Z)} = 0$ and $f(Q) = 1$. This implies that Q cannot be in the closure of $\rho(Z)$, and therefore $\rho(Z)$ is closed.

The same argument for an arbitrary G-invariant W shows that there is $f \in \mathcal{A}_Y$ with $f|_{\rho(Z)} = 0$ and $f|_{\rho(W)} = 1$, whence statement (2). □

Proof of Theorem 20.6. Let $\rho : X \to Y$ be the above morphism, and consider another morphism $\rho' : X \to Y'$ that is constant on the G-orbits. We have to show that ρ' factors through ρ. This is very easy if Y' is affine: in that case ρ' corresponds to a morphism $\mathcal{A}_{Y'} \to \mathcal{A}_X$ whose image must lie in $\mathcal{A}_X^G \cong \mathcal{A}_Y$ as ρ' is constant on G-orbits.

In the general case we use an affine open covering $\{U_i'\}$ of Y', and set $V_i := \rho'^{-1}(U_i')$. This is a G-stable open subset in X, so its complement Z_i is a G-stable closed subset. Lemma 22.1 (1) then implies that $U_i := Y \setminus \rho(Z_i)$ is open in Y, and an iterated application of Lemma 22.1 (2) shows that the U_i form an open covering of Y. Given a basic affine open set $D(f) \subset U_i$, the function $\rho^* f$ is an element of $\mathcal{A}_X^G$ that does not vanish on Z_i. Thus the restriction of ρ' to $D(\rho^* f)$ induces a ring homomorphism $\mathcal{A}_{U_i'} \to \mathcal{A}_{D(\rho^* f)} = A_{\rho^* f}$ with image in $(A_{\rho^* f})^G$, again since ρ' is constant on G-orbits. But we have $(A_{\rho^* f})^G \cong (A^G)_f = \mathcal{A}_{D(f)}$, whence a morphism $D(f) \to U_i'$ compatible with $\rho'|_{D(\rho^* f)}$. One checks that for another basic open set $D(g) \subset U_i$ the morphisms thus obtained coincide on $D(f) \cap D(g) = D(fg)$, and similarly for basic opens contained in the intersections $U_i \cap U_j$. We thus obtain the required map by patching.

Finally, by the Closed Orbit Lemma (Corollary 15.5) for each $Q \in Y$ the fibre $\rho^{-1}(Q)$ contains a closed G-orbit Z. That there is only one such Z follows from Lemma 22.1 (2). □

Example 22.2. Consider GL_n acting on the space $M_n(k)$ of $n \times n$ matrices via conjugation, and define the geometric structure on $M_n(k)$ by identifying its elements with points of the affine space $\mathbf{A}_k^{n^2}$.

For each $A \in M_n(k)$ consider its characteristic polynomial $f_A(t) = t^n + (-1)^{n-1} a_{n-1} t^{n-1} + \cdots + (-1) a_1 t + a_0$. The map $\rho : M_n(k) \to \mathbf{A}_k^n$ sending A to $(a_{n-1}, \ldots, a_0)$ is a morphism of affine varieties constant on GL_n-orbits. We claim that $(\mathbf{A}^n, \rho)$ is the categorical quotient of $M_n(k)$ by the above action of GL_n. Assume first $\rho' : M_n(k) \to Y$ is a morphism of affine varieties constant on GL_n-orbits. For a point of $\mathbf{A}_k^n$ corresponding to a polynomial f let D be a diagonal matrix with characteristic polynomial f, and set $\phi(f) := \rho'(D)$. This does not depend on the choice of D since D is determined up to permutation of its diagonal entries, and such a permutation is conjugation by an element of GL_n. On the other hand, the coefficients of f are the elementary symmetric polynomials in the entries of D, so since ρ' is given by symmetric polynomials in the entries of D (again by permutation invariance), it factors through ρ by the fundamental theorem of symmetric polynomials. The case of general Y reduces to the affine case by taking an affine open cover and using the defining property of categorical quotients (for not necessarily affine varieties).

One can check that the closed orbit in each fibre of ρ is that of diagonalizable matrices. But for non-separable f there exist non-diagonalizable matrices with characteristic polynomial f, so the fibre of ρ over f contains several orbits.

Chapter 5. Borel Subgroups and Maximal Tori

We can now harvest the fruits of our labours in the previous two chapters, and prove the remaining general structural results for affine algebraic groups. These concern *Borel subgroups*, i.e. maximal closed connected solvable subgroups, and *maximal tori*, i.e. tori embedded as closed subgroups that are maximal with respect to this property. The main theorems state that in a connected group all Borel subgroups (resp. maximal tori) are conjugate.

23. Borel subgroups and parabolic subgroups

In the remaining part of these notes, G will always denote a *connected* affine algebraic group.

Definition 23.1. *A* Borel subgroup *is a maximal connected solvable closed subgroup in* G*.*

Here 'maximal' means a maximal element in the set of connected closed solvable subgroups partially ordered by inclusion. Such elements exist by dimension reasons.

Theorem 23.2. *Any two Borel subgroups of* G *are conjugate.*

For the proof we need a key lemma.

Lemma 23.3. *If* $H \subset G$ *is a closed subgroup such that* G/H *is a projective variety and* B *is a Borel subgroup in* G*, then* H *contains a conjugate of* B*.*

Proof. There is a natural left action of G on the projective variety G/H given by $(g, g'H) \mapsto gg'H$. Restricting to B we get a left action on G/H to which the Borel fixed point theorem (Theorem 15.1) applies. It yields $g \in G$ with $BgH = gH$. In particular $Bg \subset gH$, so that $g^{-1}Bg \subset H$. □

Proof of Theorem 23.2. Embed G in some $\mathrm{GL}(V)$ and consider the action of G on the projective variety $\mathrm{Fl}(V)$ of complete flags of V (cp. Proposition 11.4). Pick a point $F \in \mathrm{Fl}(V)$ whose orbit under the action of G has minimal dimension; it is a closed orbit by Corollary 15.5. Denote by H the stabilizer of F. If B is a Borel subgroup in G, then H contains a conjugate gBg^{-1} of B by Lemma 23.3. But B is connected, so gBg^{-1} is contained in the connected component H° of H. But H° is connected and solvable (since it stabilizes a complete flag), so we must have $gBg^{-1} = H^\circ$ by maximality of B. This shows that H° is a Borel subgroup and all Borel subgroups are conjugate to H°. □

It is worth isolating the key property of the above subgroup H in a definition.

Definition 23.4. *A* parabolic *subgroup is a closed subgroup $P \subset G$ with G/P a projective variety.*

Proposition 23.5. *A Borel subgroup is parabolic.*

Proof. Given a Borel subgroup $B \subset G$, choose an embedding $G \subset \mathrm{GL}(V)$ such that B is the stabilizer of a 1-dimensional subspace $V_1 \subset V$ (Lemma 4.2). Applying the Lie-Kolchin theorem to V/V_1 we see that B stabilizes a complete flag $\overline{F}$ in V/V_1, so it is *exactly* the stabilizer of the preimage F of $\overline{F}$ in V viewed as a point of $\mathrm{Fl}(V)$. Now let $H \subset G$ be a subgroup as in the previous proof. Then $B = g^{-1}H^\circ g$ for some $g \in G$. For $H^g := g^{-1}Hg$ there is thus a natural surjection of quasi-projective varieties $G/B \to G/H^g$ whose fibres are finite since B has finite index in H^g. But then $\dim G/B = \dim G/H^g$ by Corollary 13.7 or Remark 16.4, so G/B, identified with the G-orbit of F in $\mathrm{Fl}(V)$, is also an orbit of minimal dimension. Therefore G/B is projective by Corollary 15.5. □

Corollary 23.6. *A closed subgroup $P \subset G$ is parabolic if and only if it contains a Borel subgroup.*

Proof. Since a conjugate of a Borel subgroup is again a Borel subgroup, the 'only if' part follows from Lemma 23.3. For the 'if' part let P is a closed subgroup containing a Borel subgroup B, inducing a natural surjective morphism $G/B \to G/P$. Embed G/P into some $\mathbf{P}^n$ as a quasi-projective variety. By Theorem 14.1 the composite map $G/B \to G/P \to \mathbf{P}^n$ has closed image as G/B is projective, but the image is G/P, which is thus projective as well. □

Observe that the corollary characterizes Borel subgroups by a geometric and not a group-theoretic property: they are the minimal parabolic subgroups. Another formulation is that the Borel subgroups are exactly the solvable parabolic subgroups.

Examples 23.7.

(1) In the case $G = \mathrm{GL}_n$ the Borel subgroups are the conjugates of the subgroup T_n of upper triangular matrices (by the Lie-Kolchin theorem). The quotient $\mathrm{GL}_n/\mathrm{T}_n$ is the variety of complete flags constructed in Section 10. For this reason for general G and B the projective variety G/B is often called a *(generalised) flag variety*. Examples of non-solvable parabolic subgroups in GL_n are given by stabilizers of non-complete flags (cp. Remark 11.5).

(2) In the case $G = \mathrm{SL}_n$ the Borel subgroups are the conjugates of the subgroup $\mathrm{SL}_n \cap \mathrm{T}_n$ of upper triangular matrices of determinant 1, again by the Lie-Kolchin theorem.

(3) It can be shown using the theory of quadratic forms that the Borel subgroups in SO_n are the stabilizers of those flags of subspaces $V_0 \subset V_1 \subset \cdots \subset k^n$ that are maximal with respect to

the property that the restriction of the quadratic form to each V_i is trivial (these flags have length $[n/2]$).

Here is an important consequence.

Corollary 23.8. *The identity component $R(G)$ of the intersection of the Borel subgroups in G is the largest closed connected solvable normal subgroup in G.*

Proof. By Theorem 23.2 $R(G)$ is a normal subgroup; it is also closed, connected and solvable by construction. On the other hand, a closed connected solvable normal subgroup N must be contained in a Borel subgroup by the definition of Borel subgroups, hence in all of them by Theorem 23.2 and the normality of N. By connectedness it is then contained in $R(G)$. $\square$

Definition 23.9. *The subgroup $R(G)$ of the last corollary is called the* radical *of G. The group G is* semisimple *if $R(G) = \{1\}$, and it is* reductive *if $R(G)$ is a torus.*

Example 23.10. The group GL_n is reductive. To see this, observe that the group T_n of upper triangular matrices is a Borel subgroup, and so is its transpose L_n of lower triangular matrices. Their intersection is the diagonal subgroup D_n, so $R(G)$ is diagonalizable and hence a torus. In fact, the radical of GL_n is $Z(\mathrm{GL}_n) \cong \mathbf{G}_m$ by an easy lemma from linear algebra: a diagonal matrix not of the form $\lambda \cdot Id$ has a conjugate which is not diagonal.

By Example 23.7 (2) every Borel subgroup of SL_n is of the form $B \cap \mathrm{SL}_n$ for a Borel subgroup of GL_n, and hence $R(\mathrm{SL}_n) \subset R(\mathrm{GL}_n) \cong \mathbf{G}_m$. Now a matrix of the form $\lambda \cdot Id$ lies in SL_n if and only if $\lambda \in \mu_n$, and therefore $R(\mathrm{SL}_n)$ identifies with a subgroup of μ_n. Since $R(\mathrm{SL}_n)$ is connected, it must be trivial, and so SL_n is semisimple.

Finally, we use the theory of Borel subgroups to establish some basic properties of low-dimensional groups.

Proposition 23.11. *A connected affine algebraic group G of dimension ≤ 2 is solvable.*

The proof uses a lemma.

Lemma 23.12. *Let G be a connected affine algebraic group, and $B \subset G$ a Borel subgroup. If B is nilpotent, then $G = B$.*

Proof. We use induction on the dimension of B. If $\dim B = 0$, then $G = G/B$ is at the same time projective, affine and connected, hence it must be a point. For $\dim B > 0$ the identity component Z° of the center $Z(B)$ is nontrivial. Indeed, since B is nilpotent by assumption, there is a largest i for which the element B^i of the upper central series is nontrivial. This B^i is closed and connected (same argument as for Corollary 16.6) and by definition it is contained in $Z(B)$.

Now given $z \in Z^\circ$, the inner automorphism $g \mapsto zgz^{-1}$ of G is trivial on B, hence induces a morphism of varieties $G/B \to G$. Such a map is constant, because G is affine connected and G/B is projective, so z is central in G. Thus $Z^\circ \subset Z(G)$, and hence Z° is normal in G. The quotient B/Z° is a Borel subgroup in G/Z°, because it is connected, solvable and $(G/Z^\circ)/(B/Z^\circ) \cong G/B$ is projective. By the inductive assumption $G/Z^\circ = B/Z^\circ$, so $G = B$. □

Proof of Proposition 23.11. Let B be a Borel subgroup. If $B = G$, we are done. If $B \neq G$, then $\dim B \leq 1$, so there are two cases. Either $B_u \neq \{1\}$, in which case it is a nontrivial closed subgroup in B by Corollary 8.4, and hence $B = B_u$ by dimension reasons. Otherwise $B_u = 1$, and therefore B is a torus (embed it in $\mathrm{T}_n \subset \mathrm{GL}_n$ using the Lie-Kolchin theorem, and observe that the composite map $B \to \mathrm{T}_n \to \mathrm{D}_n$ is injective, where D_n is the diagonal subgroup). In either case B is nilpotent, which contradicts the proposition. □

Corollary 23.13. *If* $\dim G = 1$*, then* G *is commutative.*

Proof. In any case G is solvable, so its closed commutator subgroup $[G, G]$ cannot equal G. Hence $[G, G]$=1 by dimension reasons. □

Remark 23.14. In fact, one can say more: a connected affine algebraic group of dimension 1 is isomorphic either to $\mathbf{G}_m$ or to $\mathbf{G}_a$. Part of this theorem is easily proven: by dimension reasons we must have $G = G_s$ or $G = G_u$. In the first case G is a torus, and thus must be $\mathbf{G}_m$ by dimension reasons. It then remains to be shown that in the second case G is isomorphic to $\mathbf{G}_a$. In characteristic 0 we shall prove this later (see Remark 25.4 (1) below). The positive characteristic case is much more difficult, however: either one has to develop some analogue of the logarithm in positive characteristic (see Humphreys or Springer), or one has to use some facts about automorphisms of algebraic curves (see Borel).

24. Interlude on 1-cocycles

In this section we collect some very basic facts from the cohomology of groups that will be used in the next section. All groups are abstract groups.

If G is a group, by a *G-module* we mean an abelian group A equipped with a (left) action by G. It is equivalent to giving a left module over the group ring $\mathbf{Z}[G]$.

Definition 24.1. *A* 1-cocycle *of G with values in A is a map $\phi : G \to A$ (of sets) satisfying $\phi(\sigma\tau) = \phi(\sigma) + \sigma\phi(\tau)$ for all $\sigma, \tau \in G$. These form an abelian group $Z^1(G, A)$ under the natural addition. A map $\phi : G \to A$ is a* 1-coboundary *if it is of the form $\phi(\sigma) = a - \sigma(a)$ for a fixed $a \in A$. These form a subgroup $B^1(G, A) \subset Z^1(G, A)$, and* *the quotient* $H^1(G,A) := Z^1(G,A)/B^1(G,A)$ *is the* first cohomology group of G *with values in* A.

We shall be interested in 1-cocycles because of the following basic example.

Example 24.2. Assume given an extension $1 \to A \to E \xrightarrow{p} G \to 1$ of G by the abelian group A, i.e. a surjective homomorphism $p: E \to G$ with kernel A. In this situation we can give A the structure of a G-module by $\sigma(a) := \tilde{\sigma} a \tilde{\sigma}^{-1}$, where $\tilde{\sigma} \in E$ is any element with $p(\tilde{\sigma}) = \sigma$. Since A is abelian and normal in G, this action is well defined.

A *section* of p is a homomorphism $s : G \to E$ with $p \circ s = \mathrm{id}_G$. Giving a section is equivalent to giving a subgroup $H \subset E$ that is mapped isomorphically onto G by p (set $H = s(G)$).

Now given two sections $s_1, s_2 : G \to E$, the map $\sigma \mapsto s_1(\sigma)s_2(\sigma)^{-1}$ has values in A by definition. Moreover, it is a 1-cocycle because of the calculation

$$\begin{aligned} s_1(\sigma\tau)s_2(\sigma\tau)^{-1} &= s_1(\sigma)s_1(\tau)s_2(\tau)^{-1}s_2(\sigma)^{-1} \\ &= s_1(\sigma)s_2(\sigma)^{-1}(s_2(\sigma)s_1(\tau)s_2(\tau)^{-1}s_2(\sigma)^{-1}) \\ &= s_1(\sigma)s_2(\sigma)^{-1}\sigma(s_1(\tau)s_2(\tau)^{-1}), \end{aligned}$$

where we have used that $p(s_2(\sigma)) = \sigma$.

Assume now that this cocycle is a 1-coboundary, i.e. there is an $a \in A$ with $s_1(\sigma)s_2(\sigma)^{-1} = a\sigma(a)^{-1}$. By the equality $\sigma(a) = s_2(\sigma)as_2(\sigma)^{-1}$ this holds if and only if $s_1(\sigma) = as_2(\sigma)a^{-1}$, so that $s_1s_2^{-1}$ is a 1-coboundary if and only if the s_i are conjugate. It follows that under the assumption $H^1(G,A)$=0 any two sections are conjugate.

We finally derive sufficient conditions for the vanishing of $H^1(G,A)$.

Lemma 24.3. *If G is a finite group of order n, then $nH^1(G,A) = 0$ for all G-modules A.*

Proof. Let ϕ be a 1-coycle with values in A. Fix $\tau \in G$ and consider the map $\phi^\tau : \sigma \mapsto \phi(\sigma\tau) - \phi(\tau)$. By the cocycle relation $\phi(\sigma\tau) - \phi(\tau) - \phi(\sigma) = \sigma\phi(\tau) - \phi(\tau)$, so ϕ^τ differs from ϕ by a 1-coboundary. Therefore it is a 1-cocycle cohomologous to ϕ. Now for all $\sigma \in G$

$$\sum_{\tau \in G} \phi^\tau(\sigma) = \sum_{\tau \in G} \phi(\sigma\tau) - \sum_{\tau \in G} \phi(\tau) = 0,$$

i.e. the sum of the ϕ^τ over all $\tau \in G$ is 0. But this sum is cohomologous to $n\phi$, which proves the lemma. □

Corollary 24.4. *Let G be a finite group of order n, and A a G-module that is either*

- *a* $\mathbf{Q}$*-vector space; or*
- *a group of finite exponent prime to n.*

Then $H^1(G,A) = 0$.

Proof. By definition of 1-cohomology for each $m > 0$ the multiplication by m map on A induces multiplication by m on $H^1(G, A)$. In the case of a $\mathbf{Q}$-vector space this map is an isomorphism on A and hence on $H^1(G, A)$, but for $m = n$ it is the zero map by the lemma, whence the statement in this case. In the second case we obtain that $H^1(G, A)$ is annihilated both by n and the exponent of A which is prime to n, so it is trivial again. □

25. Maximal tori

A *maximal torus* in a connected algebraic group G is a torus of maximal dimension contained as a closed subgroup in G. Such a torus exists by dimension reasons.

Example 25.1. In GL_n the maximal tori are the conjugates of the diagonal subgroup D_n. In SL_n they are the conjugates of of the subgroup $\mathrm{D}_n \cap \mathrm{SL}_n$, which is the kernel of the determinant map on D_n. Both of these facts follow from the Lie-Kolchin theorem. Thus for GL_n the maximal tori have dimension n, and for SL_n they have dimension $n-1$.

However, it is not *a priori* clear in general that a maximal torus is a nontrivial subgroup. In any case, it must be contained in a Borel subgroup since it is connected and solvable, so to prove nontriviality it suffices to discuss the case when G is solvable. Recall from Corollary 8.4 (and its proof) that in this case we have a commutative diagram with exact rows and injective vertical maps

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_u & \longrightarrow & G & & & & \\ & & \big\downarrow & & \big\downarrow & & & & \\ 1 & \longrightarrow & \mathrm{U}_n & \longrightarrow & \mathrm{T}_n & \longrightarrow & \mathrm{D}_n & \longrightarrow & 1 \end{array}$$

where $G_u \subset G$ is the closed subgroup of unipotent elements. Now that we have constructed quotients, we can deduce that the quotient G/G_u embeds as a closed subgroup into D_n. Hence it is a torus, because G is connected and hence so is G/G_u.

Theorem 25.2. *Let G be a connected solvable affine algebraic group. There exists a torus T contained as a closed subgroup in G that maps isomorphically onto G/G_u via the natural projection $G \to G/G_u$.*

The proof below is that of Grothendieck ([2], exposé on 10/12/1956), which contains several improvements with respect to Borel's original proof. It uses two lemmas.

Lemma 25.3. *Let G be a commutative unipotent algebraic group. If k is of characteristic 0, then G as an abelian group is isomorphic to a $\mathbf{Q}$-vector space. In characteristic $p > 0$ its elements have p-power order.*

Proof. The group U_n of unipotent matrices in GL_n has a composition series $N_1 \supset N_2 \supset \dots$ obtained as follows: first we set a_{12} to 0, then a_{23}, and so on until $a_{n-1,n}$, then $a_{1,3}$, and so on; each successive quotient is isomorphic to $\mathbf{G}_a$. From this one infers in characteristic $p > 0$ that each element of U_n itself has p-power order. Assume now we are in characteristic 0. Note first that a closed subgroup $G \subset \mathrm{U}_n$ must be connected, for G/G° is a finite unipotent group (by Proposition 2.3 and Corollary 5.12) and hence must be trivial (a nontrivial element would have an eigenvalue that is a root of unity different from 1). Now one sees that either $N_i \cap G = N_{i+1} \cap G$ or $(N_i \cap G)/(N_{i+1} \cap G) \cong \mathbf{G}_a$. Indeed, each $N_i \cap G$ is closed in U_n, hence connected. Therefore so are their quotients, but the only closed connected subgroups of the 1-dimensional group $\mathbf{G}_a$ are the trivial subgroup or $\mathbf{G}_a$ itself. We thus obtain that G as an abstract group has a chain of normal subgroups with the successive quotients $\mathbf{Q}$-vector spaces. If moreover G is commutative, it is a $\mathbf{Q}$-vector space, because an abelian group that is an extension of $\mathbf{Q}$-vector spaces is itself a $\mathbf{Q}$-vector space. □

Remarks 25.4.

(1) In characteristic 0 the above proof shows that a unipotent group of dimension 1 must be isomorphic to $\mathbf{G}_a$ and that an arbitrary unipotent group of dimension n is isomorphic to $\mathbf{A}^n$ as a variety. In characteristic $p > 0$ the first fact still holds but is much more difficult to prove (as mentioned earlier), but if one accepts this fact, the second one follows by a similar argument.

(2) In characteristic 0 one can in fact show that a commutative unipotent group is isomorphic to a direct power of $\mathbf{G}_a$. This isomorphism is realised using the formal exponential and logarithm series (which are polynomials for nilpotent, resp. unipotent elements).

Lemma 25.5. *Let $s \in G$ be a semisimple element, $Z \subset G$ its centralizer, and $U \subset G$ a closed normal unipotent subgroup. Then the image of the composite map $Z \to G \to G/U$ is exactly the centralizer of the image of s in G/U.*

Proof. We first reduce to the case when U is commutative using induction on the length of the commutator series of the unipotent (hence solvable) group U. (Note that its terms are closed characteristic subgroups in U, hence normal subgroups in G.) Let $U^{(n)}$ be the smallest nontrivial term. It is commutative, so we may assume the lemma holds for it. The statement for U then follows from the inductive hypothesis applied to $G/U^{(n)}$.

So assume U is commutative, and let $S \subset G$ be the closure of the subgroup generated by s. It is a closed commutative subgroup, hence its subset S_s of semisimple elements is a closed subgroup by Theorem 7.2. But then we must have $S_s = S$ by construction, whence S is diagonalizable by Lemma 7.1. By Theorem 7.8 it is thus a product of a torus and a finite abelian group, therefore it is the Zariski closure of the union of its n-torsion subgroups S_n for $n > 0$ (because so is $\mathbf{G}_m$). Let Z_n be the centralizer of S_n; it is a closed subset because the commutation relation with each $s \in S_n$ gives equations for the entries of the matrices in Z_n. Thus the intersection of the Z_n is Z, it is therefore enough to prove the statement for S_n in place of s and Z_n in place of Z.

Let g be an element whose mod U image commutes with the mod U image of S_n. This means that for each $\sigma \in S_n$ there is a unique $\phi(\sigma) \in U$ with $\sigma g \sigma^{-1} = g\phi(\sigma)$. The map $\sigma \mapsto \phi(\sigma)$ is a 1-cocycle of S_n with values in the abelian group U (endowed with the S_n-action given by conjugation), because

$$\phi(\sigma\tau) = g^{-1}\sigma\tau g\tau^{-1}\sigma^{-1} = (g^{-1}\sigma g\sigma^{-1})\sigma(g^{-1}\tau g\tau^{-1})\sigma^{-1} = \phi(\sigma)\sigma\phi(\tau)\sigma^{-1}.$$

Now Lemma 25.3 says that in characteristic 0 U as an abelian group is a $\mathbf{Q}$-vector space, and in characteristic $p > 0$ its elements have p-power order. Thus Corollary 24.4 shows that $H^1(S_n, U) = 0$ (noting that in characteristic $p > 0$ S has no p-torsion). It follows that $\phi(\sigma) = u(\sigma u \sigma^{-1})^{-1}$ for some $u \in U$, so that $\sigma g u \sigma^{-1} = gu$ for all $\sigma \in S_n$, i.e. $gu \in Z_n$, and moreover gu is in the same mod U coset as g. This proves the lemma. □

Proof of Theorem 25.2. Assume first that each $s \in G_s$ centralizes the elements of G_u. If G_u is commutative, then G is a central extension of the torus G/G_u by G_u, hence it is nilpotent and we are done by Theorem 8.5. Otherwise we again use induction on the length of the commutator series of G_u. If $G_u^{(n)}$ is the smallest nontrivial term, it is commutative and by induction there is a torus $T \subset G/G_u^{(n)}$ mapping isomorphically onto G/G_u. The preimage of T in G is a central extension of T by $G_u^{(n)}$. Hence it is nilpotent and isomorphic to $T \times G_u^{(n)}$, again by Theorem 8.5. This concludes the proof in this case.

Assume now there is an element $s \in G_s$ that does not commute with all elements of G_u; in particular, its centralizer Z is not the whole of G. We then use induction on $\dim(G)$, the case of dimension 0 being trivial. The subgroup Z is closed in G (same argument as in the previous proof) and it is also solvable, being a subgroup of G. As G/G_u is commutative, the natural map $Z \to G/G_u$ is surjective by the above lemma. Hence so is the map $Z^\circ \to G/G_u$ for the identity component $Z^\circ \subset Z$, because G/G_u is connected. Applying the inductive hypothesis to Z° we obtain the result, because $Z_u^\circ = G_u \cap Z^\circ$. □

Corollary 25.6. *A torus T as in the theorem is a maximal torus and G is a semidirect product of G_u by T.*

Proof. Since $T \cap G_u = \{1\}$, this follows from Jordan decomposition. □

Theorem 25.7. *Any two maximal tori in a connected affine algebraic group are conjugate.*

Proof. By the remarks at the beginning of this section and the conjugacy of Borel subgroups we may assume G is solvable. Then by the previous theorem it is the semidirect product of a maximal torus T by G_u. We first show that we may assume that G_u is commutative. This is done by a similar induction as in Lemma 25.5: let S be another maximal torus, and let $U^{(n)}$ be the smallest nontrivial term of the commutator series of G_u. By induction applied to $G/U^{(n)}$ we obtain an element $g \in G$ with $gSg^{-1} \subset TU^{(n)}$. But $U^{(n)}$ is commutative and $TU^{(n)}$ is the semidirect product of T with $U^{(n)}$, so if we know the theorem in the commutative case, we may conjugate gSg^{-1} into T.

So assume henceforth that G_u is commutative. As in the proof of Lemma 25.5 we may write S as the Zariski closure of an increasing chain of finite subgroups S_n. For each $n > 0$ put

$$C_n := \{u \in G_u : uS_nu^{-1} \subset T\}.$$

This is a decreasing chain of closed subsets of G_u whose intersection C_∞ is the set of $u \in G_u$ with $uSu^{-1} \subset T$. The chain must stabilize for dimension reasons, i.e. $C_n = C_\infty$ for n large enough. Thus to prove the theorem it is enough to show that $C_n \neq \emptyset$ for all n. Put $G_n := S_nG_u$; it is a semidirect product. The intersection $T_n := T \cap G_n$ maps isomorphically onto G_n/G_u by construction, so G_n is also the semidirect product of G_u by T_n. But $H^1(S_n, G_u) = 0$ as in the proof of Lemma 25.5, so S_n and T_n are conjugate, i.e. $C_n \neq \emptyset$. $\square$

Remark 25.8. For solvable G the above proof did not use the fact that S is actually a torus; the argument works more generally for any commutative subgroup $S \subset G$ consisting of semisimple elements. Indeed, the closure $\overline{S}$ of such a subgroup is always diagonalizable by the same argument as in the proof of Lemma 25.5, so the above argument works for $\overline{S}$, and we obtain that some conjugate of $\overline{S}$ (hence of S) lies in T. In particular, we may choose S to be the cyclic subgroup generated by a semisimple element, and obtain: *In a connected solvable group each semisimple element is contained in a maximal torus.*

The theorem also yields characterisations of nilpotent algebraic groups.

Corollary 25.9. *The following are equivalent for a connected affine algebraic group G.*

(1) *G is nilpotent.*
(2) *All maximal tori are contained in the center of G.*
(3) *G has a unique maximal torus.*

Proof. By Lemma 23.12 we may assume that G is solvable. Then we have seen (1) $\Rightarrow$ (2) in the proof of Theorem 8.5, and (2) $\Rightarrow$ (3) follows from the above theorem. To show (3) $\Rightarrow$ (1), observe first that by the theorem the unique maximal torus T is stable by conjugation, hence so is its n-torsion subgroup T_n for each n. But T_n is finite, so each $t \in T_n$ has finite conjugacy class. As in the proof of the Lie-Kolchin theorem, the connectedness of G implies that T_n is contained in the center $Z(G)$ of G. Hence $T \subset Z(G)$, because T is the closure of the union of the T_n and $Z(G)$ is closed. But since $G_u \subset G$ is also a closed normal subgroup (Corollary 8.4), we have $G \cong G_u \times T$, and therefore G is nilpotent by Corollary 6.3. $\square$

Finally, we use the conjugacy of maximal tori to define a fundamental invariant of a connected affine algebraic group G.

Definition 25.10. *Let T be a maximal torus in G, $N_G(T)$ its normalizer in G and $Z_G(T)$ its centralizer. The quotient $W(G,T) := N_G(T)/Z_G(T)$ is the* Weyl group *of G.*

By the conjugacy of maximal tori the isomorphism class of $W(G,T)$ does not depend on T, hence it is indeed an invariant of G.

Proposition 25.11. *Given any torus S contained as a closed subgroup in G we have an equality of identity components $N_G(S)^\circ = Z_G(S)^\circ$. In particular, the Weyl group $W(G,T)$ is finite.*

The proof is based on the following very useful lemma.

Lemma 25.12. (Rigidity Lemma) *Let S and T be diagonalizable groups, V a connected variety, and $\phi : V \times S \to T$ a morphism of varieties. If the morphism $\phi_P : S \to T$ given by $s \mapsto \phi(P,s)$ is a morphism of algebraic groups for each $P \in V$, then the map $P \mapsto \phi_P$ is constant.*

Proof. If $s \in S$ is a fixed element of finite order m, the morphism $\phi_s : P \mapsto \phi(P,s)$ has finite image, because T has only finitely many elements of order dividing m. Hence ϕ_s is constant, because V is connected. In other words, we have $\phi_P(s) = \phi_{P'}(s)$ for all $P, P' \in V$. We now use again a trick seen in the proof of Lemma 25.5: S is the Zariski closure of the subgroup of finite order elements, so by continuity $\phi_P = \phi_{P'}$ on the whole of S. $\square$

Proof of Proposition 25.11. The first statement implies the second since the identity component has finite index in any group. To prove the first statement it is enough to show $N_G(S)^\circ \subset Z_G(S)$ as the inclusion $Z_G(S)^\circ \subset N_G(S)^\circ$ is obvious. In other words, we have to see that the homomorphism $s \to nsn^{-1}$ is the identity for each $n \in N_G(S)^\circ$. This follows from Lemma 25.12 applied with $V = N_G(S)^\circ$, $S = T$ and $\phi(n,s) = nsn^{-1}$ since $\phi(1,s)$ is the identity. $\square$

Remark 25.13. Note also that $W(G,T)$ identifies with a (finite) subgroup of $\mathrm{Aut}(T)$ in a natural way. Indeed, every element $n \in N_G(T)$

induces an inner automorphism of T which is trivial if and only if $n \in Z_G(T)$.

26. The union of all Borel subgroups

In this section we prove the following theorem of Borel.

Theorem 26.1. *Each element of a connected affine algebraic group is contained in a Borel subgroup.*

In view of Theorem 23.2 an equivalent phrasing of the theorem is that if B is a Borel subgroup in a connected group G, then the union of the conjugates gBg^{-1} for all $g \in G$ is the whole of G. In particular:

Corollary 26.2. *If a Borel subgroup B is normal in G, then $B = G$.*

Unfortunately, it is not obvious at all to construct 'by hand' a connected solvable subgroup containing a given element of G. The problem is with the semisimple elements. Still, for those contained in a (maximal) torus one may proceed as follows. If T is a maximal torus, the only maximal torus in the identity component of the centralizer $Z_G(T)$ is T (by Theorem 25.7), hence $Z_G(T)^\circ$ is nilpotent by Corollary 25.9. Thus $Z_G(T)^\circ$ is a connected solvable subgroup containing T. (Note that once we have proven Theorem 26.1, we'll be able to invoke Remark 25.8 and conclude that in fact every semisimple element of G is contained in a maximal torus. But we are not allowed to use this fact for the moment.)

The main point in the proof Theorem 26.1 will be that the union of the conjugates of $Z_G(T)^\circ$ is already dense in G; the rest will then follow rather easily. We begin with the following general lemma.

Lemma 26.3. *Let G be a connected algebraic group, and H a closed connected subgroup. Denote by X the union of all conjugates gHg^{-1} in G.*

1. *If H is parabolic, then X is a Zariski closed subset.*
2. *Assume that H contains an element whose natural left action on G/H has finitely many fixed points. Then X is dense in G.*

Proof. We may view X as the image of the composite morphism $p_2 \circ \phi : G \times G \to G$, where $\phi : G \times H \to G \times G$ is given by $\phi(g, h) = (g, ghg^{-1})$, and $p_2 : G \times G \to G$ is the second projection. Let Y be the image of $\mathrm{Im}\,(\phi)$ by the quotient map $\pi : G \times G \to G \times G/(H \times \{1\}) \cong (G/H) \times G$. Since π is an open surjective mapping (Lemma 17.3) and $\mathrm{Im}\,(\phi)$ is closed in $G \times G$ (Corollary 16.5), we get that Y is closed in $(G/H) \times G$. On the other hand, its image by the second projection $\bar{p}_2 : (G/H) \times G \to G$ is still X by construction. Hence if H is parabolic, X must be closed by Theorem 14.4.

We prove (2) by a dimension count. By Proposition 13.4 it suffices to show that the dimension of the Zariski closure $\overline{X}$ equals that of G. The assumption in (2) means that there is an element $h \in H$ over which the fibre of $\bar{p}_2$ is finite, i.e. of dimension 0. Hence by Corollary 13.7 we must have $\dim Y = \dim \overline{X}$. On the other hand, the first projection $\bar{p}_1 : (G/H) \times G \to G/H$ maps Y onto G/H, and the fibre over a coset gH is isomorphic to gHg^{-1}, so it is of dimension $\dim H$. Thus from Proposition 16.10 we obtain $\dim Y = \dim H + \dim G/H = \dim G$, as required. □

The following proposition verifies condition (2) of the lemma for the identity component of the centralizer of a maximal torus.

Proposition 26.4. *Let T be a maximal torus in G, and $C = Z_G(T)$ its centralizer. There is an element $t \in T$ whose natural left action on G/C° has finitely many fixed points.*

In fact, we shall show in the next section that $C = C^\circ$, but the proof will use Theorem 26.1, so we are not allowed to use this. Before proving the proposition let us first show how it implies Theorem 26.1.

Proof of Theorem 26.1. Applying statement (2) of Lemma 26.3 to the subgroup C° of the proposition we see that its conjugates are dense in G. As remarked at the beginning of this section, C° is nilpotent. Hence it is solvable, and as such is contained in a Borel subgroup B. The union of the conjugates of B is therefore dense in G, and it remains to apply statement (1) of Lemma 26.3 to B. □

It remains to prove the proposition. We need the following elementary lemma.

Lemma 26.5. *If T is a torus embedded as a closed subgroup in a connected group G, there is an element $t \in T$ with $Z_G(T) = Z_G(t)$.*

The proof will in fact show that the t having the required property form a dense open subset in T.

Proof. Choose a closed embedding of G into some GL_n. Up to composing with an inner automorphism of GL_n, we may assume using Lemma 7.1 that the elements of T map to diagonal matrices. A calculation shows that in GL_n the centralizer of a diagonal matrix $\mathrm{diag}\,(d_i)$ consists of those matrices $[c_{ij}]$ where $c_{ij} = 0$ if $d_i \neq d_j$ and c_{ij} is arbitrary otherwise. It follows that we may choose t as any diagonal matrix $\mathrm{diag}\,(t_i)$ where $t_i \neq t_j$ for all $i \neq j$, unless $s_i = s_j$ for all $s = \mathrm{diag}\,(s_i) \in T$. □

Proof of Proposition 26.4. By the previous lemma we find $t \in T$ with $C = Z_G(t)$. Now observe that the class $gC^\circ \in G/C^\circ$ is a fixed point for t if and only if $g^{-1}tg \in C^\circ$. But $g^{-1}tg$ is a semisimple element (by Corollary 5.12), so $g^{-1}tg \in T$, as T is the semisimple part of the nilpotent group C° (by the remarks at the beginning of this section and Theorem 8.5). Hence $T \subset Z_G(g^{-1}tg)^\circ = g^{-1}Z_G(t)^\circ g = g^{-1}C^\circ g$, so that $gTg^{-1} \subset C^\circ$. Since T is the only maximal torus in C°, this forces

$gTg^{-1} = T$, i.e. $g \in N_G(T)$. But $N_G(T)^\circ = C^\circ$ by Proposition 25.11 (and its proof), which leaves finitely many possibilities for gC°. □

Finally, we record that, as noted above, Theorem 26.1 together with Remark 25.8 yields:

Corollary 26.6. *In a connected affine algebraic group each semisimple element is contained in a maximal torus.*

27. Connectedness of centralizers

We now turn to the proof of the following theorem.

Theorem 27.1. *For a torus S contained as a closed subgroup in a connected algebraic group G the centralizer $Z_G(S)$ is connected.*

The first reduction is:

Lemma 27.2. *If the theorem holds for connected solvable groups, it holds for arbitrary connected groups.*

Proof. We shall prove that given G and S as in the theorem, for $z \in Z_G(S)$ there is a Borel subgroup B containing both z and S. Since $Z_B(S)^\circ \subset Z_G(S)^\circ$ and by the solvable case z is contained in $Z_B(S)^\circ = Z_B(S)$, the theorem will follow for G. Choose a Borel subgroup B_0 containing z. Then $B = gB_0g^{-1}$ will be a good choice provided $zg \subset gB_0$ and $sg \subset gB_0$ for all $s \in S$. This is equivalent to saying that the coset gB_0 is a common fixed point under the natural left actions of z and S on the projective variety G/B_0. Consider the subset $X \subset G/B_0$ of fixed points under the action of z. This is a nonempty subset of G/B_0 (as $z \in B_0$), and it is closed, being the preimage of the graph of the multiplication-by-z map by the diagonal morphism $G/B_0 \to (G/B_0) \times (G/B_0)$. Thus it is a projective variety. Since z centralizes S, the natural left action of S on G/B_0 preserves X, so it has a fixed point in X by the Borel fixed point theorem. □

The key lemma is the following one.

Lemma 27.3. *Let G be a connected algebraic group, $U \subset G$ a connected commutative normal unipotent subgroup and $s \in G$ a semisimple element. Then $Z_G(s) \cap U$ is connected.*

Proof. Consider the map $\gamma_s : U \to U$ given by $u \mapsto usu^{-1}s^{-1}$. Since U is commutative and normal, this is a group homomorphism, and its kernel C equals $Z_G(s) \cap U$. Observe now that $C \cap \gamma_s(U) = \{1\}$. Indeed, assume $u \in C$ and $v \in U$ are such that $u = \gamma_s(v)$, or in other words $us = vsv^{-1}$. Here s is semisimple, u is unipotent and commutes with s, so this must be the Jordan decomposition of vsv^{-1}. But vsv^{-1} is also semisimple (by Corollary 5.12), which forces $u = 1$.

By the above property the multiplication map $m : C \times \gamma_s(U) \to U$ is injective. But here $\dim C + \dim \gamma_s(U) = \dim U$ by Corollary

16.10, so by the same corollary the image of the multiplication map $C^\circ \times \gamma_s(U) \to U$ must be the whole of U. Therefore there exists a projection of U onto C° which must map C isomorphically onto C° since $C \cap \gamma_s(U) = \{1\}$. The connectedness of C follows. □

The following lemma is much simpler.

Lemma 27.4. *Let $1 \to G' \to G \xrightarrow{\phi} G'' \to 1$ be an exact sequence of algebraic groups. If G' and G'' are connected, then so is G.*

Proof. By assumption, G° surjects onto G'', so for each $g \in G$ we find $g^\circ \in G^\circ$ with $\phi(g) = \phi(g^\circ)$. But then $g^\circ g^{-1} \in G' \subset G^\circ$, so $g \in G^\circ$. □

Corollary 27.5. *If G is a connected solvable group, then its unipotent subgroup G_u is connected as well.*

Proof. Since G/G_u is diagonalizable, hence in particular commutative, G_u must contain $[G, G]$, which is connected by Lemma 8.3. The quotient $G_u/[G, G]$ is the unipotent subgroup of the commutative group $G^{\mathrm{ab}} := G/[G, G]$ (by Corollary 5.12), so it is connected, being a direct factor of G^{ab} in view of Theorem 7.2. The corollary now follows from the lemma. □

Proof of Theorem 27.1. Using Lemma 26.5 it will suffice to prove that the centralizer of a semisimple element $s \in G$ is connected. Moreover, by Lemma 27.2 we may assume G is solvable. Then G_u is a closed normal subgroup in G, and moreover connected by the previous corollary. We use induction on the length of the commutator series of G_u, the case $G_u = \{1\}$ being obvious. Let U be the smallest nontrivial term in the series; it is closed, commutative and normal in G. It is also connected by an iterated application of Lemma 8.3, so Lemma 27.3 applies and yields the connectedness of $Z_G(s) \cap U$. On the other hand, the image of $Z_G(s)$ in G/U is exactly the centralizer of s mod U in G/U according to Lemma 25.5, so it is connected by the inductive assumption. The connectedness of $Z_G(s)$ now follows from lemma 27.4. □

.

28. The normalizer of a Borel subgroup

We now prove the last important structural result concerning Borel subgroups, which is due to Chevalley. Its proof will use all the major results proven earlier in this chapter.

Theorem 28.1. *Let B be a Borel subgroup in a connecetd affine algebraic group G. Then $N_G(B) = B$, i.e. B equals its own normalizer.*

For the proof we need the following proposition which is interesting in its own right.

Proposition 28.2. *Let S be a torus contained as a closed subgroup in G, and B a Borel subgroup of G. Then $Z_G(S) \cap B$ is a Borel subgroup in $Z_G(S)$.*

Note that the centralizer $Z_G(S)$ is a connected affine algebraic group by Theorem 27.1.

Proof. We have $Z_G(S) \cap B = Z_B(S)$, so it is connected by (the solvable case of) Theorem 27.1. It is also solvable, so by Corollary 23.6 it is enough to see that it is parabolic in $Z_G(S)$. The composite map $Z_G(S) \to G \to G/B$ factors through $Z_G(S)/(Z_G(S) \cap B)$, and maps it isomorphically onto the image of $Z_G(S)$ in G/B. We show that this image is a closed subset of the projective variety G/B. In any case, it is the same as the image of the subgroup $Y = Z_G(S)B$ in G/B, so since the projection $G \to G/B$ is surjective and open (Lemma 17.3), it is enough to show that Y is closed in G. It is certainly connected (being the image of the multiplication map $Z_G(S) \times B \to G$), hence so is its Zariski closure $\overline{Y}$.

Pick now $\bar{y} \in \overline{Y}$; we show that it lies in Y. To do so, we shall find $b \in B$ such that $\bar{y}b^{-1}$ centralizes S. In any case, we know that $\bar{y}^{-1}S\bar{y} \subset B$, because the elements of Y have this property by definition, hence so does $\bar{y}$ by continuity. Now write $T = B/B_u$ (where $B_u \subset B$ is the unipotent subgroup), and apply Lemma 25.12 to the map $\overline{Y} \times S \to T$ sending a pair (y, s) to the image of $y^{-1}sy$ in T. It says that for each y and s the image of $y^{-1}sy$ in T equals that of s. In particular, $\bar{y}^{-1}S\bar{y} \subset SB_u$. But S and $\bar{y}^{-1}S\bar{y}$ are maximal tori in the connected solvable group SB_u, so by Theorem 25.7 we have $\bar{y}^{-1}S\bar{y} = b^{-1}Sb$ for some $b \in B_u$. But then $\bar{y}b^{-1} \in Z_G(S)$, as required. □

Proof of Theorem 28.1. We use induction on the dimension of G, the case of dimension 1 being trivial by Corollary 23.13. Fix a maximal torus $T \subset B$ and an element $x \in N_G(B)$. We shall show that $x \in B$. Conjugation by x maps T onto another maximal torus in B which is of the form yTy^{-1} for some $y \in B$ by Theorem 25.7. Hence up to replacing x by $y^{-1}x$ (which is allowed) we may assume that $xTx^{-1} = T$. Now consider the endomorphism $\rho_x : T \to T$ given by $t \mapsto xtx^{-1}t^{-1}$. We distinguish two cases.

Case 1: ρ_x is not surjective. Then $\mathrm{Im}\,(\rho_x)$ is a proper closed subgroup of T, whence it follows (for example by a dimension count using Corollary 16.11) that the identity component S of $\mathrm{Ker}\,(\rho_x)$ is a nontrivial torus. By construction, x lies in the centralizer $Z_G(S)$ of S. On the other hand, $B \cap Z_G(S)$ is a Borel subgroup in the connected group $Z_G(S)$ by the proposition above, and since $x \in N_G(B)$, it normalizes $B \cap Z_G(S)$. Thus if $Z_G(S) \neq G$, the inductive hypothesis applies to $Z_G(S)$ and shows that $x \in B$. Otherwise S is central in G and hence it is a normal subgroup. But then we may conclude by applying the inductive hypothesis to G/S (which has lower dimension by Corollary 16.11).

Case 2: ρ_x is surjective. This assumption implies that T is contained in the commutator subgroup $[N_G(B), N_G(B)]$. We now use the always handy Lemma 4.2 to find a finite-dimensional vector space V and a morphism $G \to \mathrm{GL}(V)$ such that the stabilizer of a 1-dimensional subspace $L \subset V$ is exactly $N_G(B)$. The action of $N_G(B)$ on L is given by a morphism $N_G(B) \to \mathrm{GL}(L) \cong \mathbf{G}_m$. Since $\mathbf{G}_m$ is commutative and semisimple, it follows that both $[N_G(B), N_G(B)]$ and the unipotent part B_u of B act trivially on L. But $T \subset [N_G(B), N_G(B)]$ and $B = TB_u$ (Theorem 25.2), so B acts trivially on L. Therefore if $v \in L$, the map $G \to V$ given by $g \mapsto gv$ factors through G/B. But this is a morphism of the irreducible projective variety G/B into V viewed an as affine space, so it is constant by Corollary 14.2. In particular, the whole of G stabilizes L, so $G = N_G(B)$, i.e. B is normal in G. But then $G = B$ by Corollary 26.2, and the statement to be proven is obvious. □

Corollary 28.3. *The map $g \mapsto gBg^{-1}$ induces a bijection between the points of the flag variety G/B and the set $\mathcal{B}$ of Borel subgroups in G.*

Proof. The map certainly factors through G/B and it is surjective by Theorem 23.2. Theorem 28.1 now says that its kernel is exactly B. □

Because of the corollary above the set $\mathcal{B}$ carries the structure of a projective variety. It is called the *variety of Borel subgroups* in G. The natural left action of G on G/B corresponds to the conjugation action of G on $\mathcal{B}$.

The study of this variety as a homogeneous space for G is extremely important. For instance, one has the following difficult theorem, which is one form of the *Bruhat decomposition*:

Theorem 28.4. *Let T be a maximal torus in B. In the natural left action of B on G/B each B-orbit contains a unique fixed point by the action of T.*

A further study of the B-orbits reveals that each of them is locally closed in G/B (i.e. each point has an open neighbourhood on which the trace of the orbit is closed), and moreover isomorphic to some affine space. In this way one obtains a *cellular decomposition* of G/B.

29. The Borel subgroups containing a given maximal torus

Suppose now $T \subset G$ is a maximal torus. We may restrict the G-action on the variety $\mathcal{B}$ of Borel subgroups to $N_G(T)$. This action stabilizes the subset $\mathcal{B}^T \subset \mathcal{B}$ of Borel subgroups containing T. We shall shortly see that this subset is finite.

Lemma 29.1. *The centralizer $Z_G(T)$ acts trivially on $\mathcal{B}^T$. Consequently, the action of $N_G(T)$ on $\mathcal{B}^T$ induces an action of the Weyl group $W = W(G,T)$.*

Proof. The subgroup $Z_G(T)$ is connected by Theorem 27.1 and nilpotent by Theorem 8.5 (since T is central in B). Therefore it is contained in a Borel subgroup $B \in \mathcal{B}^T$. If $B' = gBg^{-1}$ is another Borel subgroup containing T, then T and gTg^{-1} are maximal tori in B', and as such are conjugate. This means that $T = hgTg^{-1}h^{-1}$ for some $h \in B'$, and hence $hg \in N_G(T)$. But $N_G(T) \subset N_G(Z_G(T))$, because if $n \in N_G(T)$, $t \in T$, then $ntn^{-1} \in T$, so if moreover $z \in Z_G(T)$, we have $zntn^{-1} = ntn^{-1}z$, whence $n^{-1}znt = tn^{-1}zn$, i.e. $n^{-1}zn \in Z_G(T)$. So finally

$$Z_G(T) = hgZ_G(T)g^{-1}h^{-1} \subset h(gBg^{-1})h^{-1} \subset B',$$

i.e. $Z_G(T)$ fixes B'. □

Proposition 29.2. *The action of the Weyl group W on $\mathcal{B}^T$ is simply transitive. Consequently, $\mathcal{B}^T$ is finite of cardinality equal to the order of W.*

Proof. For transitivity, let $B, B' = gBg^{-1} \in \mathcal{B}^T$. As above, we have $hg \in N_G(T)$ for some $h \in B'$, so B is mapped to B' by the class of hg in W. For simple transitivity, assume $n \in N_G(T)$ satisfies $nBn^{-1} = B$. Since $N_G(B) = B$, we have $n \in B$, and therefore $n \in N_B(T)$. But B is a connected solvable group and $T \subset B$ is a maximal torus, and hence the composite map $T \hookrightarrow B \to B/B_u$ is an isomorphism. If now $n \in N_B(T)$ and $t \in T$, then the elements $ntn^{-1}, t \in T$ have the same image in the commutative group B/B_u, so we must have $ntn^{-1} = t$, i.e. $n \in Z_G(T)$. □

We now use a geometric method to give a lower bound for the order of W. Consider the following situation. Let V be a finite-dimensional vector space equipped with a linear action of $\mathbf{G}_m$. There is an induced action of $\mathbf{G}_m$ on the associated projective space $\mathbf{P}(V)$ where a fixed point of $\mathbf{G}_m$ corresponds to a common eigenvector of $\mathbf{G}_m$ in V.

Lemma 29.3. *Assume $\mathbf{G}_m$ acts on $\mathbf{P}(V)$ as above. If P is not a fixed point, the Zariski closure of its $\mathbf{G}_m$-orbit in $\mathbf{P}(V)$ contains two fixed points.*

Proof. Consider the morphism $\phi_P : \mathbf{G}_m \to \mathbf{P}(V)$ given by $\alpha \mapsto \alpha P$. Considering $\mathbf{G}_m$ as an open subset of $\mathbf{P}^1$, a general fact from algebraic geometry says that ϕ_P extends to a morphism $\bar{\phi}_P : \mathbf{P}^1 \to \mathbf{P}(V)$. Its image is closed by Theorem 14.1, hence it is the closure of the orbit of P. The complement $\bar{\phi}_P(\mathbf{P}^1) \setminus \phi_P(\mathbf{G}_m)$ consists of at most two points, $\bar{\phi}_P(0)$ and $\bar{\phi}_P(\infty)$. Since $\bar{\phi}_P(\mathbf{P}^1) \setminus \phi_P(\mathbf{G}_m)$ is a union of $\mathbf{G}_m$-orbits and $\mathbf{G}_m$ is connected, these must be fixed points.

It remains to see that $\bar{\phi}_P(0) \neq \bar{\phi}_P(\infty)$. For this we give an explicit construction of $\bar{\phi}_P$. As $\mathbf{G}_m$ is commutative, there is a basis $v_1, \dots, v_n$ of V consisting of common eigenvectors of $\mathbf{G}_m$. The action of $\mathbf{G}_m$ on each v_i is given by a character of $\mathbf{G}_m$; since $\widehat{\mathbf{G}_m} = \mathbf{Z}$, the action is of the form $\alpha \mapsto \alpha^{m_i} v_i$ for an integer $m_i \in \mathbf{Z}$. We may order the m_i so that m_1 is maximal and m_n is minimal.

Choosing a preimage $v \in V$ of P, we have $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ with some $\lambda_i \in k$, so P has homogeneous coordinates $(\lambda_1, \dots, \lambda_n)$. We may assume $\lambda_i \neq 0$ for all i; otherwise we replace V by the subspace generated by the v_i for which $\lambda_i \neq 0$. By the above, the map $\phi_P : \mathbf{G}_m \to \mathbf{P}(V)$ is given by $\alpha \mapsto (\alpha^{m_1}\lambda_1, \dots, \alpha^{m_n}\lambda_n)$. Here we are free to multiply the coordinates by a fixed $\lambda \in k^\times$; in particular, $\alpha \mapsto (\alpha^{m_1 - m_n}\lambda_1, \dots, \alpha^{m_n - m_n}\lambda_n)$ defines the same map. But this makes sense also for $\alpha = 0$, so we have an extension of ϕ_P to a morphism $\mathbf{A}^1 \to \mathbf{P}(V)$. Similarly, $\alpha \mapsto (\alpha^{m_1 - m_1}\lambda_1, \dots, \alpha^{m_n - m_1}\lambda_n)$ gives an extension to a morphism $\mathbf{P}^1 \setminus \{0\} \to \mathbf{P}(V)$. Putting the two maps together gives the required map $\bar{\phi}_P$. Now $\bar{\phi}_P(0) = \bar{\phi}_P(\infty)$ would mean that all the m_i are equal, but then v would be a common eigenvector of $\mathbf{G}_m$, which it is not by assumption. $\square$

Proposition 29.4. *If moreover $X \subset \mathbf{P}(V)$ is an irreducible projective variety of positive dimension stable by the action of $\mathbf{G}_m$, then it contains at least two fixed points.*

If $\dim X \geq 2$, it contains at least three fixed points.

Proof. If X is pointwise fixed by $\mathbf{G}_m$, there is nothing to prove. Otherwise we may take the closure of the orbit of some $P \in X$ not fixed by $\mathbf{G}_m$ and apply the lemma to get the first statement.

For the second statement let again $P \in X$ be a point not fixed by $\mathbf{G}_m$, coming from $v \in V$. As in the previous proof, choose a basis $v_1, \dots, v_n$ of V, with $\mathbf{G}_m$ acting on v_i via $\alpha \mapsto \alpha^{m_i} v_i$. Again we may assume m_1 is maximal among the m_i, and set $W := \langle v_2, \dots, v_n \rangle$; note that this is a $\mathbf{G}_m$-invariant subspace. Then $v \notin W$ and hence $X \not\subset \mathbf{P}(W)$. The intersection $X \cap \mathbf{P}(W)$ has finitely many irreducible components permuted by $\mathbf{G}_m$; as $\mathbf{G}_m$ is connected, each component must be stable by $\mathbf{G}_m$. Moreover, each component must be of dimension ≥ 1 by (the projective version of) Theorem 13.6 and hence it contains at least two fixed points by the first part. On the other hand, by the construction of the previous proof one of the fixed points in the closure of the orbit of P, namely $\bar{\phi}_P(\infty)$, has a v_1-component and hence lies outside $\mathbf{P}(W)$. $\square$

Now we generalize the above statements to torus actions. The key lemma is the following.

Lemma 29.5. *Let T be an algebraic torus acting linearly on a finite-dimensional vector space V. There is a cocharacter $\lambda : \mathbf{G}_m \to T$ such* *that the action of T on $\mathbf{P}(V)$ has the same fixed points as the induced action of $\mathbf{G}_m$ obtained by composition with λ.*

Proof. Again V has a basis consisting of common eigenvectors v_i of T, with T acting on v_i via a character χ_i of T. for $\lambda : \mathbf{G}_m \to T$ the composite $\chi_i \circ \lambda$ is a character of $\mathbf{G}_m$, hence of the form $\alpha \mapsto \alpha^{m_i}$. Since the pairing $\mathrm{Hom}(\mathbf{G}_m, T) \times \mathrm{Hom}(T, \mathbf{G}_m) \to \mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m) \cong \mathbf{Z}$ can be identified with the pairing $\mathrm{Hom}(\mathbf{Z}^r, \mathbf{Z}) \times \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}^r) \to \mathbf{Z}$ via Theorem 7.8, it is a perfect pairing of free abelian groups. Therefore we may choose λ so that the m_i corresponding to different χ_i are different. Then the eigenspaces of V for the action of T and its composite with λ are the same. □

Corollary 29.6. *Proposition 29.4 holds more generally for the action of an algebraic torus T on $\mathbf{P}(V)$.*

We now apply the corollary in a concrete situation.

Corollary 29.7. *Let G be a connected nonsolvable algebraic group, $B \subset G$ a Borel subgroup, and $T \subset G$ a maximal torus with associated Weyl group W.*

Then W has order ≥ 2, with equality if and only if $\dim G/B = 1$.

Proof. As in the construction of quotients, identify G/B with the orbit of a suitable point in a projective space $\mathbf{P}(V)$, where $\mathbf{P}(V)$ carries a G-action. By Corollary 29.6, the restriction of the natural left G-action on G/B to T has at least two fixed points, with equality if and only if $\dim G/B = 1$. This means that T is contained in at least two Borel subgroups, or equivalently that W has order ≥ 2, by Proposition 29.2. □

As an application, we obtain (part of) a structure theorem for certain semisimple groups. First some terminology: the *rank* of a connected linear algebraic group G is the dimension of a maximal torus. The *semisimple rank* of G is the rank of $G/R(G)$.

Proposition 29.8. *Let G be a connected linear algebraic group of semisimple rank 1. There exists a surjective morphism $\rho : G \to \mathrm{PGL}_2(k)$ with $\mathrm{Ker}\,(\rho)^\circ = R(G)$. In particular, the kernel is finite for semisimple G.*

The proof will use two basic facts from the theory of algebraic curves. First, if X is a smooth irreducible quasi-projective curve, every morphism $U \to \mathbf{P}^n$ from an open subset $U \subset X$ to projective space extends to a morphism $X \to \mathbf{P}^n$. For a proof see e.g. [7], §1.6. Consequently, if two irreducible projective curves have isomorphic open subsets, they are isomorphic.

Second, the automorphism group of $\mathbf{P}^1$ as a projective variety is isomorphic to $\mathrm{PGL}_2(k)$. For an elementary proof, see [11], §I.1.

Proof. Let T be a maximal torus in G. We first prove that there are exactly two Borel subgroups containing T. Indeed, since $R(G)$ is contained in every Borel subgroup of G, the Borel subgroups of G and $\bar{G} := G/R(G)$ correspond bijectively. Moreover, by the theory of maximal tori in connected solvable groups, if a Borel subgroup B contains T, then $\bar{T} := T/T \cap R(G)$ is a maximal torus in $B/B \cap R(G)$, and as such is isomorphic to $\mathbf{G}_m$ by assumption. Thus the Borel subgroups of G containing T correspond bijectively to those of $\bar{G}$ containing $\bar{T}$, and their number equals the order of $\bar{W} := W(\bar{G}, \bar{T})$ by Proposition 29.2. Now $\bar{G}$ is not solvable (otherwise G would be solvable too and we would have $G = R(G)$), hence $\bar{W}$ has order at least 2 by Corollary 29.7. On the other hand, $\bar{W}$ is a subgroup of $\mathrm{Aut}(\bar{T}) = \mathrm{Aut}(\mathbf{G}_m) = \mathbf{Z}/2\mathbf{Z}$ by Remark 25.13 so it indeed has order 2.

Applying Corollary 29.7 again, we obtain $\dim G/B = 1$ for a Borel subgroup B. As in the previous proof we embed G/B in some projective space $\mathbf{P}(V)$ equipped with a G-action. The action of T on G/B has two fixed points; in particular it is nontrivial. Therefore by choosing a suitable cocharacter $\mathbf{G}_m \to T$ we can define a $\mathbf{G}_m$-action on $\mathbf{P}(V)$ such that G/B contains a nontrivial $\mathbf{G}_m$-orbit. In other word, there is a nonconstant morphism $\phi : \mathbf{G}_m \to G/B$ that extends to a morphism $\bar{\phi} : \mathbf{P}^1 \to \mathbf{P}(V)$ as in the proof of Lemma 29.3. As the image of $\bar{\phi}$ is the closure of $\mathrm{Im}\,(\phi)$ by Theorem 14.1, it is contained in the closed subvariety G/B, hence it is equal to G/B by dimension reasons. But G/B is a smooth projective curve, and therefore $\bar{\phi}$ must be an isomorphism by the first fact recalled above. We obtain an isomorphism $G/B \cong \mathbf{P}^1$.

Finally, the natural action of G on G/B induces a homomorphism of algebraic groups $\rho : G \to \mathrm{Aut}(\mathbf{P}^1) \cong \mathrm{PGL}_2(k)$. Its kernel is the intersection of all Borel subgroups in G, whence $\mathrm{Ker}\,(\rho)^\circ = R(G)$ as required. As remarked before, $G/R(G)$ is not solvable and therefore must be of dimension ≥ 3 by Proposition 23.11. Therefore ρ must be surjective for dimension reasons (using that $\mathrm{Im}\,(\rho) \subset \mathrm{PGL}_2(k)$ is closed). □

We shall need the following more precise statement in the case of reductive G.

Proposition 29.9. *Let G be a reductive group of semisimple rank 1. Then the kernel of the morphism $\rho : G \to \mathrm{PGL}_2(k)$ above is of multiplicative type.*

Proof. Fix a maximal torus $T \subset G$. By the previous proof there are exactly two Borel subgroups B^+, B^- containing T. We may assume that the morphism ρ is constructed using the action of G on G/B^+. We show that $\mathrm{Ker}\,(\rho) \subset T$, which implies the statement. As $\mathrm{Ker}\,(\rho)$ is the intersection of all Borel subgroups of G, it will suffice to show $B^+ \cap B^- = T$.

The group $\mathrm{PGL}_2(k)$ has dimension 3, and Borel subgroups $B \subset \mathrm{PGL}_2(k)$ are conjugate to the image of the upper triangular subgroup of $\mathrm{GL}_2(k)$. Hence they are of dimension 2, with unipotent part of dimension 1. On the other hand, the unipotent part $B_u^+ \subset B^+$ is nontrivial (otherwise B^+ would be a torus, which would contradict Lemma 23.12 for our noncommutative G). Since $\mathrm{Ker}\,(\rho)^\circ = R(G)$ by the previous proposition and $R(G)_u = 1$ by assumption, it follows that $\rho(B_u^+) \subset \mathrm{PGL}_2(k)$ is the unipotent part of a Borel subgroup in $\mathrm{PGL}_2(k)$ and moreover the map $\rho : B_u^+ \to \rho(B_u^+)$ has finite kernel. In particular, B_u^+ has dimension 1, and as such is isomorphic to $\mathbf{G}_a$ by Remark 23.14. Therefore the conjugation action of T on B_u^+ (coming from the conjugation action on B^+ which must preserve unipotents) is via a character $T \to \mathbf{G}_m$. Similarly, T acts on B_u^-, and hence the above $\mathbf{G}_m$-action on B_u^+ preserves $B_u^+ \cap B_u^-$. In other words, $B_u^+ \cap B_u^-$ is a $\mathbf{G}_m$-stable proper closed subgroup of $\mathbf{G}_a$, and hence must be trivial. But then $B^+ \cap B^- = T(B_u^+ \cap B^-) = T(B_u^+ \cap B_u^-) = T$, as claimed. $\square$

Remark 29.10. In Chapter 21 of [9] it is shown that actually the *scheme-theoretic kernel* of ρ is of multiplicative type, which is a somewhat more difficult result.

Remark 29.11. An *isogeny* $\widetilde{G} \to G$ of algebraic groups is a surjective morphism with finite kernel; it is a *multiplicative isogeny* if moreover the kernel is of multiplicative type (=diagonalizable). We call G simply connected if every multiplicative isogeny $\widetilde{G} \to G$ is an isomorphism. If G is a *semisimple* linear algebraic group, it can be shown that there exists a multiplicative isogeny $\pi : G^{\mathrm{sc}} \to G$ such that G^{sc} is semisimple simply connected and moreover for every multiplicative isogeny $\rho : \widetilde{G} \to G$ there exists $\lambda : G^{\mathrm{sc}} \to \widetilde{G}$ with $\pi = \rho \circ \lambda$.

For $G = \mathrm{PGL}_2(k)$ we have $G^{\mathrm{sc}} = \mathrm{SL}_2(k)$ with π the natural projection. Thus Proposition 29.9 implies that *every semisimple group of rank 1 is isomorphic to* $\mathrm{SL}_2(k)$ *or* $\mathrm{PGL}_2(k)$.

The proof of these results is not very hard, but requires inputs from algebraic geometry beyond the scope of these notes. See e.g. §20 of [9] from where we borrowed the terminology 'multiplicative isogeny'.

Chapter 6. Reductive Groups and Root Data: A Brief Introduction

In the classification of reductive groups one associates with each group an object of combinatorial nature called its root datum. It determines the group up to isomorphism, and hence the classification is reduced to a purely combinatorial problem. In this chapter we quickly explain the construction the root datum but do not discuss the classification itself. Our main goal is to clarify how the general structure theory of the previous chapter is exploited during the construction of the root datum.

30. Structural results for reductive groups

Before beginning the study of roots we collect together some consequences of the general structure theory for reductive groups. Throughout the whole section G denotes a reductive (in particular connected) linear algebraic group.

Proposition 30.1. *We have an equality $R(G) = Z(G)^\circ$.*

Proof. As $Z(G)^\circ$ is connected, commutative and normal, it is contained in $R(G)$ by its very definition. Also, since $R(G)$ is a normal subgroup of the connected group G, we have $G = N_G(R(G)) = N_G(R(G))^\circ$. But G is reductive, hence $R(G)$ is a torus, and therefore $N_G(R(G))^\circ = Z_G(R(G))^\circ$ by (the proof of) Proposition 25.11. This proves the inclusion $R(G) = Z(G)^\circ$. □

Proposition 30.2. *The intersection $[G, G] \cap R(G)$ is finite.*

Proof. Embed G in some $GL(V)$. Since $R(G)$ is a torus, its image in $GL(V)$ is diagonalizable, so we may decompose V as a direct sum $V = V_1 \oplus \cdots \oplus V_r$ of common eigenspaces of $R(G)$. As $R(G)$ is central in G, each V_i is a G-invariant subspace. If $g \in [G, G]$, it restricts to an element of determinant 1 in $\mathrm{GL}(V_i)$. If $g \in R(G)$, it restricts to an element of the form $\lambda_i \cdot \mathrm{id}_{V_i}$. Hence for $g \in [G, G] \cap R(G)$ there are finitely many possibilities for $g|_{V_i}$ for each $i = 1, \ldots, r$. □

Corollary 30.3. *The commutator subgroup $[G, G]$ is semisimple.*

Proof. By definition, every Borel subgroup of $[G, G]$ is contained in a Borel subgroup of G. Taking their intersection, we obtain

$$R([G, G]) \subset (R(G) \cap [G, G])^\circ = \{1\}$$

by the proposition. □

Remark 30.4. It can be shown that every semisimple group is *perfect*, i.e. it equals its commutator subgroup. In the case of SL_n $(n > 1)$ and its quotients this is a classical fact proven by matrix computations; see e.g. Lang, Algebra, Chapter XIII. We shall only use this case in what follows.

It follows that if G is reductive, then $G/R(G)[G,G]$ is both abelian (as a quotient of $G/[G,G]$) and perfect (as a quotient of the semisimple group $G/R(G)$). Therefore $G = R(G)[G,G]$, and thus by Proposition 30.2 the composite map $[G,G] \to G \to G/R(G)$ is surjective with finite kernel contained in $Z(G)$. Therefore the natural projection $G \to G/R(G)$ is 'almost split'.

Finally, we record the following consequence of the general results concerning centralizers of tori.

Proposition 30.5. *If G is a reductive group and $S \subset G$ is a torus, then $Z_G(S)$ is also reductive. If T is a maximal torus, then $Z_G(T) = T$.*

Proof. By Theorem 27.1 $Z_G(S)$ is connected. Moreover, every Borel subgroup of $Z_G(S)$ is contained in a Borel subgroup of G, so by Proposition 28.2 the Borel subgroups of $Z_G(S)$ are exactly the subgroups of the form $Z_G(S) \cap B$ for a Borel subgroup $B \subset G$. Taking identity components of intersections we obtain $R(Z_G(S)) \subset R(G)$. Therefore if $R(G)$ is a torus, so is $R(Z_G(S))$. Finally, if $T \subset G$ is a maximal torus, it is also a maximal torus in $Z_G(T)$ and it is central by definition. Hence $Z_G(T)$ is nilpotent by Corollary 25.9, but its radical must be a torus. It follows that $Z_G(T) = T$. □

31. The concept of a root datum

Here is the basic definition.

Definition 31.1. (Demazure) A *root datum* $\Psi = (X, X^\vee, R, R^\vee)$ consists of:

- a pair $(X, X^\vee)$ of *lattices* (i.e. finitely generated free abelian groups) that are dual to each other via a perfect bilinear pairing $\langle\ ,\ \rangle : X \times X^\vee \to \mathbf{Z}$;
- a finite subset $R \subset X$ together with a map $\alpha \mapsto \alpha^\vee$ onto a finite subset $R^\vee \subset X^\vee$.

For each $\alpha \in R$ the following axioms are imposed.

(RD1) $\langle \alpha, \alpha^\vee \rangle = 2$.

(RD2) $s_\alpha(R) \subset R$, $s_{\alpha^\vee}(R^\vee) \subset R^\vee$, where

$$s_\alpha(x) := x - \langle x, \alpha^\vee \rangle \alpha, \quad s_{\alpha^\vee}(y) := y - \langle \alpha, y \rangle \alpha^\vee$$

for $x \in X$, $y \in X^\vee$.

The root datum is *reduced* if moreover

(RD3) If $\alpha \in R$ and $c \in \mathbf{Q}$, then $c\alpha \in R$ if and only if $c = \pm 1$.

The elements of R (resp. $R^\vee$) are called *roots* (resp. *coroots*). An easy calculation using axioms (RD1) and (RD2) shows that all s_α satisfy $s_\alpha \circ s_\alpha = \mathrm{id}$ and $s_\alpha(\alpha) = -\alpha$. In particular, the s_α are automorphisms of order 2 of X.

Definition 31.2. *The* (abstract) Weyl group $W(\Psi)$ *of* Ψ *is the subgroup of* $\mathrm{Aut}_{\mathbf{Z}}(X)$ *generated by the* s_α.

Remarks 31.3.

(1) It is not hard to check that the subgroup of $\mathrm{Aut}_{\mathbf{Z}}(X^\vee)$ generated by the $s_{\alpha^\vee}$ is canonically isomorphic to $W(\Psi)$ (this is not surprising in view of Lemma 31.4 below). Thus the definition of $W(\Psi)$ is symmetric.

(2) By axiom (RD2) the Weyl group $W(\Psi)$ acts on the set R of roots. It can be shown by linear algebra calculations starting from the axioms that this action is faithful, and hence $W(\Psi)$ is finite (as so is R). We omit this direct argument here, but in the case of root data coming from reductive groups these facts will follow from Theorem 33.3 below.

We shall need the following important property.

Lemma 31.4. *If* $\alpha, \beta \in R$ *are such that* $\langle x, \alpha^\vee\rangle = \langle x, \beta^\vee\rangle$ *for all* $x \in X$, *then* $\alpha = \beta$. *Consequently, the map* $\alpha \mapsto \alpha^\vee$ *is a bijection.*

Proof. Using the formulas

$$s_\alpha(\alpha) = -\alpha, \quad s_\alpha(\beta) = \beta - 2\alpha, \quad s_\beta(\alpha) = \alpha - 2\beta$$

we compute

$$s_\beta s_\alpha(\alpha) = 2\beta - \alpha = \alpha + 2(\beta - \alpha), \quad s_\beta s_\alpha(\beta - \alpha) = s_\beta(\beta - \alpha) = \beta - \alpha,$$

whence for all $n > 0$

$$(s_\beta s_\alpha)^n(\alpha) = \alpha + 2n(\beta - \alpha).$$

But these elements are in R by axiom (RD2) and R is finite. This is only possible if $\alpha = \beta$. □

In the next two sections we shall associate with each connected affine algebraic group G and maximal torus $T \subset G$ a reduced root datum $\Psi(G, T)$ whose abstract Weyl group is isomorphic to the Weyl group $W(G, T)$. The lattices X and $X^\vee$ will be defined as the group of *characters*

$$X^*(T) = \mathrm{Hom}(T, \mathbf{G}_m)$$

and *cocharacters*

$$X_*(T) = \mathrm{Hom}(\mathbf{G}_m, T)$$

for a maximal torus $T \subset G$. Note there is a natural duality pairing

$$X_*(T) \times X^*(T) \to \mathbf{Z}$$

obtained from the composition of characters and cocharacters and using $\mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m) \cong \mathbf{Z}$. By Theorem 25.2 different T give rise to isomorphic pairs of lattices.

The roots are also easy to define. They come from the *adjoint representation*

$$\mathrm{Ad} : G \to \mathrm{Aut}(\mathrm{Lie(G)})$$

which sends $g \in G$ to the automorphism of $\mathrm{Lie}(G)$ induced by the inner automorphism $x \mapsto gxg^{-1}$. In fact, every automorphism of the algebraic group G induces an automorphism of the tangent space at 1. It can be checked that Ad preserves the Lie algebra structure but in fact for our purpose here it is enough to consider it as a representation of G on the underlying vector space L of $\mathrm{Lie}(G)$.

The maximal torus T maps via Ad to a commutative subgroup of semisimple elements in $\mathrm{GL}(L)$, so it is diagonalizable: there is a basis of L consisting of simultaneous eigenvectors of T. If v is such a basis element, we have $tv = \chi(t)v$ for a constant $\chi(t) \in k^\times$; in fact $t \mapsto \chi(t)$ defines a character $\chi \in X^*(T)$.

Definition 31.5. The *roots* of (G, T) are the finitely many *nontrivial* characters of T arising in this way.

Note that if G is reductive, the roots of G can be identified with those of the semisimple group $G/R(G)$ because $R(G)$ is a central torus in G by Proposition 30.1.

The remaining task is the definition of the coroots in a way that they satisfy the axioms above. This we carry out in two steps.

32. Construction of the root datum: rank 1 case

We first construct the root datum in the key special case of semisimple groups of rank 1. By Remark 29.11 we know that these are isomorphic to SL_2 or PGL_2.

Example 32.1. In SL_2, a maximal torus is given by the diagonal subgroup of matrices of the form $T = \mathrm{diag}(t, t^{-1})$ with $t \in k^\times$. Its character group is isomorphic to $\mathbf{Z}$, generated by the character $\chi : \mathrm{diag}(t, t^{-1}) \mapsto t$.

The Lie algebra is that of 2×2 matrices of trace 0. The conjugation action is given by

$$\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} a & t^2 b \\ t^{-2} c & -a \end{bmatrix}.$$

Therefore matrices with $a = c = 0$ form an eigenspace on which T acts with character χ^2, and matrices with $a = b = 0$ form an eigenspace on which T acts with character χ^{-2}. In other words, after the identification $X^*(T) = \mathbf{Z}$ the roots are $2, -2$. The corresponding coroots are $1, -1$, i.e. the cocharacters $t \mapsto \mathrm{diag}(t, t^{-1})$, $t \mapsto \mathrm{diag}(t^{-1}, t)$.

Example 32.2. For $G = \mathrm{PGL}_2$ the maximal torus is the image of the diagonal subgroup of GL_2; it is isomorphic to $\mathbf{G}_m^2/\mathbf{G}_m$, with $\mathbf{G}_m$ embedded diagonally. If $\chi_1 : (t_1, t_2) \mapsto t_1$ and $\chi_1 : (t_1, t_2) \mapsto t_2$ are the standard generators of $\widehat{\mathbf{G}_m^2}$, we may identify a generator $\widehat{\mathbf{G}_m^2/\mathbf{G}_m} \cong \mathbf{Z}$ with the character $\chi := \chi_1 \chi_2^{-1}$ trivial on the diagonal image of $\mathbf{G}_m$.

The Lie algebra of $G = \mathrm{PGL}_2$ is that of 2×2 matrices modulo scalar matrices, and the conjugation action is induced by

$$\begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{bmatrix} = \begin{bmatrix} a & t_1 t_2^{-1} b \\ t_1^{-1} t_2 c & d \end{bmatrix}.$$

Therefore, after the identification $\widehat{\mathbf{G}_m^2/\mathbf{G}_m} \cong \mathbf{Z}$ sending χ to 1, the roots become $1, -1$ and the coroots $2, -2$.

Construction 32.3. If now G is a reductive group of semisimple rank 1, then $[G,G]$ is semisimple of rank 1 surjecting onto $G/R(G)$ by Remark 30.4. By Remark 29.11, the kernel of this surjection is trivial or isomorphic to μ_2; the latter case arises only when $[G,G] \cong \mathrm{SL}_2(k)$ and $G/R(G) \cong \mathrm{PGL}_2(k)$. The two explicit examples above then show that in both cases a root α of $G/R(G)$ induces a root of $[G,G]$, whence a coroot $\alpha^\vee$ of $[G,G]$ yielding a coroot of G via the composition $\mathbf{G}_m \to T \cap [G,G] \to T$. The pair $(\alpha, \alpha^\vee)$ attached to G still satisfies the axioms for root data.

Finally, if G is semisimple of rank 1 and $T \subset G$ is a maximal torus, then we have seen during the proof of Proposition 29.8 that the Weyl group $W(G,T)$ has order 2. If now G is reductive of semisimple rank one, then $R(G)$ is a central torus with $T/R(G) \cong \mathbf{G}_m$, so the same holds for $W(G,T) = W(G/R(G), T/R(G))$. It permutes the two roots of (G,T).

33. Construction of the root datum: general case

We now construct the root datum associated with an arbitrary reductive group G and maximal torus $T \subset G$.

Construction 33.1. Let $\alpha : T \to \mathbf{G}_m$ be a root. Put $S_\alpha := \mathrm{Ker}\,(\alpha)^\circ$ and $G_\alpha := Z_G(S_\alpha)$. Since T centralizes S_α, it is contained in G_α and hence it is one of its maximal tori. Moreover, S_α is central in G_α by construction, and so by the conjugacy of Borel subgroups it is contained in the radical $R(G_\alpha)$. It follows that T/S_α is a maximal torus in the semisimple group $G_\alpha/R(G_\alpha)$. This group is of rank 1 because S_α is of codimension 1 in T. Furthermore, G_α is reductive by Proposition 30.5, hence the theory of the previous section applies to G_α and furnishes a coroot $\alpha^\vee \in X_*(T)$.

Put $X = X^*(T)$, $X^\vee = X_*(T)$ and denote by R and $R^\vee$ the set of roots and coroots, respectively. Note that $W(G,T)$ acts on X and $X^\vee$ via its conjugation action on T, and also that $W(G_\alpha, T) \subset W(G,T)$ because $N_{G_\alpha}(T) \subset N_G(T)$ and $Z_G(T) \subset Z_G(S_\alpha) = G_\alpha$. Recall that $W(G_\alpha, T)$ has order 2.

Lemma 33.2. *Let w_α be the nontrivial element of $W(G_\alpha, T)$ viewed as an element of $W(G,T)$. Its action on X is given by*

$$w_\alpha(x) := x - \langle x, \alpha^\vee \rangle \alpha \tag{6}$$

so that the lattice automorphism of X induced by w_α is given by the element s_α defined in (RD2).

Similarly, the lattice automorphism of $X^\vee$ induced by w_α is given by the element $s_{\alpha^\vee}$.

Proof. Consider a $\mathbf{Z}$-basis $\beta_1, \dots, \beta_r$ of the free $\mathbf{Z}$-module $X^*(S_\alpha)$. Together with α they yield a basis of the $\mathbf{Q}$-vector space $V = X \otimes_{\mathbf{Z}} \mathbf{Q}$. By definition, w_α induces the endomorphism of V sending α to $-\alpha$ and fixing the β_i (because $S_\alpha \subset Z(G_\alpha)$). But s_α also sends α to $-\alpha$ by its defining formula. To see that it also fixes the β_i, identify $V^\vee := X^\vee \otimes_{\mathbf{Z}} \mathbf{Q}$ with $\mathrm{Hom}_{\mathbf{Q}}(V, \mathbf{Q})$, and denote by $W \subset V$ the subspace generated by the β_i. By construction the element $\alpha^\vee$ is in the image of the map $\mathrm{Hom}_{\mathbf{Q}}(V/W, \mathbf{Q}) \to \mathrm{Hom}_{\mathbf{Q}}(V, \mathbf{Q})$. Indeed, the map $\phi : T \cap [G,G] \to T$ involved in the construction of $\alpha^\vee$ in the previous section yields an 'almost splitting' of the projection $T \to T/S_\alpha$ in G_α and it is ϕ that induces the projection $V \to V/W$ splitting the inclusion $\langle \alpha \rangle \subset V$ by Remark 30.4. Thus $\langle \beta_i, \alpha^\vee \rangle = 0$ for all i, and therefore w_α and s_α coincide on V and hence also on X. The proof of the second statement is similar. □

In the proof below we shall need the following observations. Consider the finite-dimensional $\mathbf{R}$-vector space $V := X \otimes_{\mathbf{Z}} \mathbf{R}$, and fix a positive definite inner product $[\ ,\ ]$ on it. Since $W(G,T)$ is finite, the formula

$$(x, y) := \sum_{w \in W(G,T)} [wx, wy]$$

again defines a positive definite inner product on V that is moreover $W(G,T)$-invariant. In particular, the elements w_α considered in the above lemma are orthogonal linear transformations of the inner product space $(V, (\ ,\ ))$. Moreover, formula (6) shows that they are *reflections*: they fix the hyperplane $H_\alpha \subset V$ of equation $\langle x, \alpha^\vee \rangle = 0$ and satisfy $w_\alpha(\alpha) = -\alpha$. For $y \in H_\alpha$ the calculation $(\alpha, y) = (w_\alpha \alpha, w_\alpha y) = -(\alpha, y)$ shows that we have an *orthogonal* direct sum decomposition $V = \langle \alpha \rangle \oplus H_\alpha$ with respect to $(\ ,\ )$, and then we may compute

$$w_\alpha(x) = x - 2(\alpha, \alpha)^{-1}(x, \alpha)\alpha \tag{7}$$

for general $x \in V$. Comparing with formula (6) shows the relation $\langle x, \alpha^\vee \rangle = 2(\alpha, \alpha)^{-1}(x, \alpha)$.

Theorem 33.3. *The system $\Psi = (X, X^\vee, R, R^\vee)$ is a reduced root datum, and $W(G,T) = W(\Psi)$ as subgroups of $\mathrm{Aut}_{\mathbf{Z}}(X)$.*

Recall here that sending $x \in N_G(T)$ to the map $t \mapsto xtx^{-1}$ identifies $W(G,T) = N_G(T)/Z_G(T)$ with a subgroup of the automorphism group of the torus T, and the latter identifies with $\mathrm{Aut}_{\mathbf{Z}}(X)$ via Theorem 7.8.

Proof. Axiom (RD1) follows from the construction of $\alpha^\vee$ in the previous section, and so does (RD3) because $G_{c\alpha} = G_\alpha$ for all $c \in \mathbf{Q}^\times$. Axiom (RD2) follows from Lemma 33.2 because $W(G,T)$ acts on T by conjugation and hence permutes the roots and coroots by definition of the adjoint representation.

To show the equality of Weyl groups, it suffices to see by definition of $W(\Psi)$ that the elements $w_\alpha \in W(G,T)$ considered in Lemma 33.2 generate $W(G,T)$. This we do by induction on $\dim G$. Consider an arbitrary $w \in W(G,T)$, and represent it by $x \in N_G(T)$. The map $\psi_w : t \mapsto xtx^{-1}t^{-1}$ is an endomorphism of the torus T; it depends only on w.

Assume first ψ_w is not surjective. Then $T_w := \mathrm{Ker}\,(\psi_w)^\circ \subset T$ is a nontrivial subtorus. Denote by Z_w its centralizer in G and note that $Z_w \supset T$. Moreover, Z_w is reductive by Proposition 30.5. If $Z_w = G$, then T_w is a nontrivial central subtorus of T and as such carries a trivial action of $W(G,T)$. Thus we may apply induction to $T/T_w \subset G/T_w$ and conclude. Otherwise $Z_w \subset G$ is a proper closed subgroup and $w \in W(Z_w,T) \subset W(G,T)$, so we again conclude by induction.

Suppose now ψ_w is surjective. The induced endomorphism $y \mapsto wy - y$ of the character group $X = \widehat{T}$ must then be injective. After tensoring by $\mathbf{R}$ we obtain an automorphism of the finite-dimensional $\mathbf{R}$-vector space $V = X \otimes_{\mathbf{Z}} \mathbf{R}$. If $\alpha_0 \in R$ is a root, we thus find $y \in V$ with $wy - y = \alpha$. Using the above $W(G,T)$-invariant scalar product, we compute

$$(y,y) = (wy,wy) = (y+\alpha_0, y+\alpha_0) = (y,y) + 2(y,\alpha_0) + (\alpha_0,\alpha_0)$$

whence $2(\alpha_0,\alpha_0)^{-1}(y,\alpha_0) = -1$. But then $w_{\alpha_0}(y) = y + \alpha_0 = wy$ by formula (7), so that $w_{\alpha_0}^{-1}w$ has a fixed vector in V. It follows that $\psi_{w_{\alpha_0}^{-1}w}$ cannot be surjective, hence by the previous case $w_{\alpha_0}^{-1}w$ is in the subgroup generated by all the w_α's. This concludes the proof. □

We can now state the main structural results concerning reductive groups. First, note that there is an obvious notion of isomorphism between root data $\Psi_1 = (X_1, X_1^\vee, R_1, R_1^\vee)$ and $\Psi_2 = (X_2, X_2^\vee, R_2, R_2^\vee)$: it is a pair of isomorphisms $X_1 \cong X_2$, $X_1^\vee \cong X_2^\vee$ compatible with the duality pairings, and preserving roots and coroots.

Theorem 33.4. *Let G, G' be reductive groups and $T \subset G'$, $T \subset G'$ maximal tori. Each isomorphism $\lambda_\Psi : \Psi(G,T) \xrightarrow{\sim} \Psi(G',T')$ of root data arises from a unique isomorphism $\lambda : G \xrightarrow{\sim} G'$ mapping T onto T'. Moreover, λ is uniquely determined up to an inner automorphism of G.*

Theorem 33.5. *For each reduced root datum Ψ there exists a reductive group G and a maximal torus $T \subset G$ with $\Psi = \Psi(G,T)$.*

The proofs of these theorems are long and rather technical. They can be found in Chapters 9 and 10 of [12].

The theorems reduce the classification of reductive groups to that of root data, which is fairly classical. More precisely, it is classical in the important case where the set of roots R spans the $\mathbf{R}$-vector space $V := X \otimes_{\mathbf{Z}} \mathbf{R}$; it can be shown that these are the root data arising from semisimple groups. Under this assumption the pair (V,R) is classically called a *root system* which means that it satisfies the following axioms:

(RS1) The $\alpha \in R$ generate V, and $0 \notin R$;
(RS2) For each $\alpha \in R$ there exists $\alpha^\vee$ in the dual vector space V^* such that $\langle \alpha, \alpha^\vee \rangle = 2$ and (with the above notation) $s_\alpha(R) \subset R$;
(RS3) For each $\alpha \in R$ the function $\alpha^\vee$ satisfies $\alpha^\vee(R) \subset \mathbf{Z}$.[5]

Conversely, it is not hard to show that each root system (V,R) gives rise to a root datum $\Psi = (X, X^\vee, R, R^\vee)$ where R generates $X \otimes_{\mathbf{Z}} \mathbf{R}$.

Root systems have first arisen in the theory of complex semisimple Lie algebras, and their classification has been known for more than a hundred years. One first decomposes them into a finite direct sum of irreducible root systems (the notion of a direct sum of root systems being the obvious one) and then classifies the irreducibles by means of a finite graph, the Dynkin diagram. One obtains three infinite families traditionally labelled A_n, B_n and D_n (one diagram for each $n \geq 1$), and five exceptional diagrams denoted by G_2, F_4, E_6, E_7 and E_8, respectively. The connection with Lie algebras is not surprising, since it is known (see e.g. [8], §13) that in characteristic 0 the correspondence $G \mapsto \mathrm{Lie}\,(G)$ induces an equivalence between the category of semisimple algebraic groups and that of semisimple Lie algebras. It is more surprising that there is no difference in the classification of semisimple groups in positive characteristic. (For the classification of root systems and semisimple Lie algebras, see e.g. the first chapters of [1].) The proof of Theorem 33.5 for arbitrary reductive groups proceeds by reduction to the semisimple case.

[5]In the works following the conventions of Bourbaki, one imposes instead of (RS2) and (RS3) the existence of order 2 automorphisms s_α of V that preserve R and have the property that for all $\alpha, \beta \in R$ there is $m \in \mathbf{Z}$ with $s_\alpha(\beta) - \beta = m\alpha$. The two definitions are equivalent.

References and Sources

(1) R. Carter, *Affine Lie Algebras*, Cambridge University Press, 2006.
(2) *Séminaire Chevalley*, année 1956-58: Groupes de Lie algébriques. Reprinted as *Classification des groupes algébriques semisimples*, Springer-Verlag, 2005.
(3) A. Borel, Groupes algébriques linéaires, *Ann. of Math.* **64** (1956), 20–82.
(4) A. Borel, *Linear Algebraic Groups*, 2nd edition, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, 1991.
(5) B. Conrad, Algebraic Groups I-II, lecture notes available from the website `www.ams.org/open-math-notes`.
(6) I. Dolgachev, *Lectures on Invariant Theory*, London Mathematical Society Lecture Note Series, vol. 296, Cambridge University Press, 2003.
(7) R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.
(8) J. E. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, vol. 21, Springer-Verlag, 1975.
(9) J. S. Milne, *Algebraic Groups*, book to be published in 2017, preliminary version available at `http://www.jmilne.org.`
(10) D. Mumford, J. Fogarty, F. Kirwan, *Geometric Invariant Theory,* 3rd ed., Ergebnisse der Mathematik, vol. 34, Springer-Verlag, 1994.
(11) I. R. Shafarevich, *Basic Algebraic Geometry I-II*, Springer-Verlag, 1994.
(12) T. A. Springer, *Linear Algebraic Groups*, 2nd edition, Progress in Mathematics, vol. 9, Birkhäuser-Verlag, 1998.
(13) R. Steinberg, On theorems of Lie-Kolchin, Borel, and Lang, in *Contributions to Algebra*, Academic Press, 1977, 349–354.
(14) R. Steinberg, *Conjugacy Classes in Algebraic Groups*, Lecture Notes in Mathematics, vol. 366, Springer-Verlag, Berlin, 1974.
(15) W. C. Waterhouse, *Introduction to Affine Group Schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, 1979.