Algebraic Groups

Ryan Smith

Algebraic Geometry, Fall 2008

Algebraic groups are groups which are also varieties such that the group action is compatible with the topology. In this regard they are similar to Lie groups where the manifold structure is replaced with the Zariski topology, so it's unsurprising that there are connections between algebraic groups and Lie algebras. Although there are many specializations of the definition of algebraic groups, the two most important are the cases where the underlying variety is affine (linear algebraic groups) and when the variety is complete (abelian varieties).

We shall assume throughout that the base field k is algebraicly closed, though most of the results can generalize to arbitrary subfields of a fixed algebraic closure. The trade off for generalizing to subfields is that one must check that all morphisms used during a proof are defined over the subfield.

1 Basic Properties

Definition 1.1. An algebraic group G is a variety which is also a group such that the maps $\mu : G \times G \to G$ sending $\mu(g, h) = gh$ and $\iota : G \to G$ sending $\iota(g) = g^{-1}$ given by the group operation are morphisms. A homomorphism of algebraic group is a group homomorphism which is also a morphism of varieties.

At first glance it would tempting to think of algebraic groups as topological groups with the Zariski topology, but the topology on $G \times G$ is not the product topology. Furthermore, for topological groups T_1 implies T_2 but the Zariski topology is not Hausdorff. Algebraic groups are homogeneous spaces via the group action. The set of regular points of a variety is always nonempty (in contrast with schemes), so by homogeneity all algebraic groups are regular. It follows that morphisms μ and ι are regular.

Example 1.2. For a field k, the additive group $\mathbb{G}_a$ is the affine line $\mathbb{A}^1$ with the group law $g \cdot h = g + h$. The multiplicative group $\mathbb{G}_m$ is the affine open subset $D(0) \subset \mathbb{A}^1$ where the group law is multiplication in k.

If G is any algebraic group and $S \subset G$ is any subset, then the normalizer $N(S) = \{g \in G | gSg^{-1} = S\}$ and the centralizer $Z(S) = \{g \in G | gsg^{-1} = s \quad \forall s \in S\}$ are closed subgroups of G.

Definition 1.3. For $x \in G$ the group acts smoothly on itself by right (respectively left) translation via $y \mapsto x^{-1}y$ (respectively $y \mapsto yx$). The induced homomorphisms on the coordinate ring are given by $(\lambda_x f)(y) = f(x^{-1}y)$ and $(\rho_x f)(y) = f(yx)$. Both actions define group homomorphisms $G \to \mathrm{GL}(k[G])$ which will prove important later.

Proposition 1.4 ([Spr98])**.** *1) For every algebraic group G there is a unique irreducible component G^0 containing e. It is a closed normal subgroup of finite index. 2) Every closed subgroup of finite index contains G^0.*

Proof. 1) Let X and Y be irreducible components of G containing e. The product $X \times Y \subset G \times G$ is irreducible, and $\mu(X \times Y) = XY$ is irreducible. The closure $\overline{XY}$ is again irreducible and contains X and Y, so $X = Y = \overline{XY}$. It is closed under multiplication since $X = Y$. It is also closed under taking inverses since $\iota(X) = X^{-1}$ is the image of an irreducible component and contains e. Therefore $G^0 = X$ is a closed subgroup and $e \in gG^0g^{-1}$ so $gG^0g^{-1} = G^0$. There are only finite many irreducible components of G, and G can be covered by translations of G^0 so $[G : G^0]$ is finite. Uniqueness of G^0 follows from the disjointness of cosets.

2) If $H \leq G$ has finite index, then $H^0 \leq G^0$ has finite index. But H^0 is open and closed in G^0, and G^0 is connected, so $H^0 = G^0$. □

For algebraic groups irreducibility is equivalent to connectedness since the group can be covered with disjoint translates of the identity component G^0.

Lemma 1.5. *Let U and V be dense open subset of G, then $UV = G$.*

Proof. For any $x \in G$ the sets $x^{-1}U$ and V are dense and open, so $x^{-1}U \cap V \neq \varnothing$ and $x \in UV$. □

Lemma 1.6. *If $H < G$ then $\overline{H}$ is a subgroup, and if H contains a nonempty open subset of $\overline{H}$ then $H = \overline{H}$.*

Proof. If $x \in H$ then $x\overline{H}$ is closed and $\overline{H} \subseteq x\overline{H}$, so $x^{-1}\overline{H} \subseteq \overline{H}$. Therefore $H\overline{H} \subseteq \overline{H}$, from which it follows $Hx \subseteq \overline{H}$ for all $x \in \overline{H}$. It is closed under the group operation, and $(\overline{H})^{-1} = \overline{H^{-1}} = \overline{H}$, so $\overline{H}$ is a subgroup. Suppose that $\varnothing \neq U \subseteq H$ and U is open in $\overline{H}$, then H is open in $\overline{H}$ since H can be covered by translates of U. By the preceding lemma $HH = \overline{H} = H$. □

Proposition 1.7. *Let $\phi : G \to H$ be a morphism of algebraic groups. Then 1)* $\ker \phi$ *is a closed subgroup of G, 2) Im ϕ is a closed subgroup of H, and 3) $\phi(G^0) = (\phi G)^0$.*

Proof. 1) The kernel is just $\phi^{-1}\{e\}$ which is closed. 2) The continuous image of a constructible set is constructible, so $\phi(G)$ contains an open subset of its closure. 3) Clearly $e \in \phi(G)^0$ and the continuous image of connected is connected. □

2 Linear Algebraic Groups

Definition 2.1. A linear algebraic group is an algebraic group which is also an affine variety.

The general linear group GL_n is the quintessential example of a linear algebraic group since it is an affine variety with the group operation given by matrix multiplication. Closed subgroups of GL_n are also linear algebraic groups, and we will show that every linear algebraic group is isomorphic to such a subgroup. In some older literature, linear algebraic groups were actually defined to be closed subgroups of GL_n. A rational representation of an algebraic group G is a homomorphism of algebraic groups $r : G \to \mathrm{GL}(V)$ where V is a finite dimensional k-vector space.

The other classical matrix groups such as SL_n, O_n, SO_n, Sp_n, etc. are all linear algebraic groups. Elliptic curves on the other hand are examples of algebraic groups which are not linear. The variety structure of an elliptic curve is projective, and if we attempted to pass to an open affine subset the group law would no longer hold.

Let G be a linear algebraic group and define $A = k[G]$. The morphisms $\mu : G \times G \to G$ and $\iota : G \to G$ induce homomorphisms $\mu^* : A \to A \otimes_k A$ (called comultiplication) and $\iota^* : A \to A$ (called the antipode). The action of ι^* is given by $(\iota^* f)(x) = f(x^{-1})$. Since the identity element can be regarded as the inclusion morphism $e : \operatorname{Spec} k \hookrightarrow G$, it gives rise to a dual map $e^* : k[G] \to k$ via $f \mapsto f(e)$. Let $\epsilon : A \to A$ be the map $(\epsilon f)(x) = f(e)$, then group axioms give rise to a set of dual axioms which can be expressed by saying that the following diagrams commute:

$$\begin{tikzcd}
A \arrow[r, "\mu^*"] \arrow[d, "\mu^*"] & A \otimes_k A \arrow[d, "\mathrm{id} \otimes \mu^*"] \\
A \otimes_k A \arrow[r, "\mu^* \otimes \mathrm{id}"] & A \otimes_k A \otimes_k A
\end{tikzcd}
\qquad
\begin{tikzcd}
A \otimes_k A \arrow[r, "\iota \otimes \mathrm{id}"] & A \otimes_k A \arrow[d, "\mu^*"] \\
A \arrow[u, "\mu^*"] \arrow[r, "\epsilon"] \arrow[d, "\mu^*"] & A \\
A \otimes_k A \arrow[r, "\mathrm{id} \otimes \iota"] & A \otimes_k A \arrow[u, "\mu^*"]
\end{tikzcd}$$

$$\begin{tikzcd}
A & A \otimes_k A \arrow[l, "e \otimes \mathrm{id}"'] \\
A \otimes_k A \arrow[u, "\mathrm{id} \otimes e"] & A \arrow[l, "\mu^*"] \arrow[u, "\mu^*"]
\end{tikzcd}$$

Example 2.2. Consider $\mathbb{G}_a$, the affine line $\mathbb{A}^1$ with the group operation given by addition in k. The comultiplication map $\mu^* : k[x] \to k[x] \otimes_k k[x] \cong k[x, y]$ acts by $\mu^*(x) = x + y$. Unsurprisingly, the antipode sends $\iota^*(x) = -x$. The additive identity is 0 so $e^*(x) = 0$.

Example 2.3. The multiplicative group $\mathbb{G}_m$ as a variety is the punctured affine line $\mathbb{A}^1 \setminus \{0\} = k^*$. The coordinate ring is $k[x, x^{-1}]$, and

$$\mu^* : k[x, x^{-1}] \to k[x, x^{-1}] \otimes_k k[x, x^{-1}] \cong k[x, x^{-1}, y, y^{-1}]$$

is given by $\mu^*(x) = xy$. The antipode is given by $\iota^*(x) = x^{-1}$ and $e^*(x) = 1$.

Proposition 2.4 ([Spr98]). *Let G be a linear algebraic group which acts on an affine variety X and let F be a finite dimensional subspace of $k[X]$. If the action of G is given by a morphism $\varphi : G \times X \to G$ then*

a) There exists a finite dimensional subspace $F \subset E \subset k[X]$ which is stable under translation for all $g \in G$.

b) F is stable under translation by all $g \in G$ if and only if $\varphi^* F \subset k[G] \otimes_k F$.

Proof. a) Without loss of generality we can assume that $F = \mathrm{Span}_k(f)$ for some $f \in k[X]$ and take sums of the 1-dimensional subspaces at the end. We can non-uniquely write $\varphi^* f = \sum_i f_i \otimes_k g_i \in k[G] \otimes_k k[X]$. Recall that for $x \in G$ and $y \in X$ left translation is given by

$(\tau_x f)(y) = \tau(x^{-1}y) = \sum_i f_i(x^{-1})g_i(y)$, so $\tau_x f = \sum_i f_i(x^{-1})g_i$. There are only finite many g_i so $E = \mathrm{Span}_k\{\tau_x f | x \in G\}$ is contained in a finite dimensional subspace.

b) If $\varphi^* F \subset k[G] \otimes_k F$ then we can take $g_i \in F$ and the subspace is stable under τ_x. If F is stable under translation extend the basis $\{f_i\}$ of F to a basis $\{f_i\} \cup \{g_j\}$ of $k[X]$. We know that $\varphi^* f = \sum_i r_i \otimes f_i + \sum_j s_j \otimes g_j$, so for $f \in F$ the translate $\tau_x f$ is of the form $\tau_x f = \sum_i r_i(x^{-1})f_i + \sum_j s_j(x^{-1})g_j \in F$. But the f_i are a basis for F, so $s_j = 0$ for all j and $\varphi^* F \subset k[G] \otimes_k F$. □

Theorem 2.5 ([Hum75]). *Let G be a linear algebraic group, then G is isomorphic to a closed subgroup of $\mathrm{GL}_n(k)$ for some n.*

Proof. Let $f_1, \ldots, f_n$ be generators for $k[G]$ as an algebra. They generate a finite dimensional vector space over k, $E = \mathrm{Span}_k\{f_1, \ldots, f_n\}$. By the previous proposition, E is contained in a finite dimensional vector space F which is stable under translation. The f_i can be extended to a basis of E, so without loss of generality assume that the f_i are a basis for F. G acts on E by right translation, so there is a morphism $\varphi : G \times E \to E$. Since the f_i form a basis for E we have $\varphi^* f_i = \sum_j m_{ij} \otimes_k f_j$ for some $m_{ij} \in k[G]$. Acting by translation gives $(\rho_x f_i)(y) = f_i(yx) = \sum_j m_{ij}(x) f_j(y)$ so $\rho_x f_i = \sum_j m_{ij}(x) f_j$. Thus the matrix representation of $\rho_x|_E$ with respect to the basis $\{f_i\}_{i\in I}$ is $(m_{ij}(x))_{i,j}$. Let $\psi : G \to \mathrm{GL}_n(k)$ be this map, then ψ is a morphism of algebraic groups. The image of any algebraic group is closed, so it remains to show that G is an isomorphism onto its image. Since $f_i(x) = f_i(ex) = \sum_j m_{ij} f_j(e)$ we can write $f_i = \sum_j f_j(e) m_{ij}$, so the m_{ij} generate $k[G]$ and ψ is injective. Let T_{ij} be the standard basis for $k[\mathrm{GL}_n]$, so they can also be viewed as a basis of $\mathrm{Im}\ (G)$ and $\psi^*(T_{ij}) = m_{ij}$ which generate $k[G]$. Therefore ψ induces an isomorphism on coordinate rings and ψ is an isomorphism. □

We now specialize to the case where G is abelian.

Definition 2.6. If G is an abelian linear algebraic group a character of G is a homomorphism of algebraic groups $\chi : G \to \mathbb{G}_m$ (which isomorphic as a group to k^*). The set of characters of G is itself an abelian group denoted $X^*(G)$. Characters of G are regular functions on G, so $X^*(G) \subset k[G]$. A cocharacter is a homomorphism of algebraic groups $\lambda : \mathbb{G}_m \to G$, but the set of cocharacters of G is not a group when G is nonabelian.

Since every linear algebraic group can be realized as a closed subgroup of GL_n, the structure of linear algebraic groups can be naturally described in the language of linear algebra.

Definition 2.7. A linear algebraic group G is diagonalizable if it is isomorphic to a closed subgroup of the diagonal matrices D_n for some n. G is called an algebraic torus if it is isomorphic to D_n for some n.

Example 2.8. Consider the case where $G = D_n$. Let $\chi_i \in X^*(D_n)$ be the character which projects onto the ith diagonal entry, then any $x \in D_n$ can be written $x = \mathrm{diag}(\chi_1(x), \ldots, \chi_n(x))$. The coordinate ring is $k[D_n] = k[\chi_1, \ldots, \chi_n, \chi_1^{-1}, \ldots, \chi_n^{-1}]$, which has a basis of terms of the form $\chi_1^{a_1} \ldots \chi_n^{a_n}$ where $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. The sum of two such terms is not a multiplicative homomorphism so every character is of the form $\chi_1^{a_1} \ldots \chi_n^{a_n}$. Hence $X^*(D_n) \cong \mathbb{Z}^n$.

Theorem 2.9 ([Spr98])**.** *For an abelian linear algebraic group the following conditions are equivalent: 1) G is diagonalizable, 2) $X^*(G)$ is finitely generated abelian group whose elements form a k-basis of $k[G]$, and 3) Any rational representation decomposes as a sum of 1-dimensional representations.*

Proof. Suppose that G is diagonalizable. The inclusion into D_n induces a surjection $k[D_n] \twoheadrightarrow k[G]$. Any character of D_n restricts to a character of G, so in particular the restrictions spans $k[G]$. Thus $X^*(D_n) \twoheadrightarrow X^*(G)$, but $X^*(D_n) \cong \mathbb{Z}^n$. Now suppose that $X^*(G)$ is finitely generated abelian group and $X^*(G)$ span $k[G]$. Let $\phi : G \to \mathrm{GL}_n(k)$ be a rational representation, and let $\psi_{ij}(x)$ be the (i,j)th component of $\phi(x)$. Because $X^*(G)$ span $k[G]$, each component function can be written as $\psi_{ij} = \sum_{\chi \in X^*(G)} c_{i,j,\chi}\chi$. Hence by rearranging terms we can write

$$\phi(x) = \sum_{i,j} \psi_{ij} e_{ij} = \sum_{i,j} \sum_{\chi \in X^*(G)} c_{i,j,\chi}\chi(x) e_{ij} = \sum_{\chi \in X^*(G)} \chi(x) A_\chi \text{ for some } A_\chi \in M_n(k)$$

with only finitely many of the A_χ nonzero. Representations are homomorphisms, so $\phi(xy) = \phi(x)\phi(y)$ gives an orthogonality relation $A_\chi A_\psi = \delta_{\chi,\psi} A_\chi$. Since $\phi(e) = I$ and $\chi(e) = 1$ for all χ, we have $\sum_{\chi \in X^*(G)} A_\chi = I$. For each nonzero A_χ define a 1-dimensional subspace $V_\chi = \mathrm{Im}\ (A_\chi)$. If $v \in V_\psi$ then

$$\phi(x)v = \sum_{\chi \in X^*(G)} \chi(x) A_\chi v = \psi(x) A_\psi v \in V_\psi$$

Therefore

$$V = \bigoplus_{A_\chi \neq 0} A_\chi$$

gives an explicit decomposition into 1-dimensional representations. The last implication is automatic when G is viewed as a closed subgroup of GL_n. ☐

To prove further a further results for algebraic tori we first must take a slight detour by starting with a coordinate ring and trying construct a suitable linear algebraic group. Let M be a finitely generated abelian group and $k[M]$ the group algebra. There is a canonical basis for the group algebra given by $\{e_m | m \in M\}$. If M_1 and M_2 are both finitely generated abelian groups, then $k[M_1 \oplus M_2] \cong k[M_1] \otimes_k k[M_2]$. We can define a comultiplication $\Delta : k[M] \to k[M] \otimes_k k[M]$ to be the diagonal map $\Delta(e_m) = e_m \otimes_k e_m$. The antipode $\iota : k[M] \to k[M]$ is defined to be $\iota(e_m) = e_{-m}$, and $e : k[M] \to k$ is simply $e(e_m) = 1$ for all $m \in M$. For reasons which will become clear, we assume that M has no p-torsion when $p = \mathrm{char}\ k > 0$.

Proposition 2.10 ([Spr98])**.** *1) The group algebra $k[M]$ is an affine algebra. There exists a diagonalizable linear algebraic group $\mathcal{G}(M)$ such that $k[\mathcal{G}(M)] = k[M]$ and (Δ, ι, e) as defined above are the induced maps on $k[\mathcal{G}(M)]$. 2) There is a canonical isomorphism $M \cong X^*(\mathcal{G}(M))$. 3) If G is diagonalizable then $\mathcal{G}(X^*(G)) \cong G$.*

Proof. By the fundamental theorem of finitely generated abelian groups it suffices to reduce to the case where M is cyclic. If M is infinite then $k[M] \cong k[T, T^{-1}]$ which is an integral domain. If M is cyclic of order n, then $k[M] \cong k[T]/(T^n - 1)$. Since $p \nmid n$ this is a reduced algebra. For 2), recall that by definition $k[M]$ is the ring of regular functions on $\mathcal{G}(M)$, so in particular $k[M]$ contains the characters of $\mathcal{G}(M)$. Each e_m defines a character on $\mathcal{G}(M)$ and they form a basis for $X^*(\mathcal{G}(M)) \subset k[M]$. But as seen before, a linear combination of the e_m is no longer a character, so every character is actually equal to e_m for some $m \in M$. Hence $M \cong X^*(\mathcal{G}(M))$. A nearly identical argument proves 3) □

Corollary 2.11. *Let G be diagonalizable, then then following are equivalent: 1) G is a torus, 2) G is connected, 3) $X^*(G)$ is a free abelian group.*

Proof. The group of characters $X^*(G)$ is finitely generated, so $X^*(G) \cong \mathbb{Z}^n \oplus M$ for a finite abelian group M. By the previous proposition $G \cong D_n \times \mathcal{G}(M)$ and $\mathcal{G}(M)$ is finite. D_n is connected but $\mathcal{G}(M)$ has the discrete topology since it's finite, so G is connected if and only if $X^*(G)$ is torsion free. □

3 Abelian Varieties

Definition 3.1. An abelian variety is a connected algebraic group which is a complete variety. In particular, any projective algebraic group is an abelian variety.

The study of abelian varieties is a vast subject and beyond the scope of this work, however some justification is required to avoid awkward questions over the choice of terminology.

Theorem 3.2 ([Mil08])**.** *Let $\alpha : V \times W \to U$ be a regular morphism where V is complete and $V \times W$ is irreducible. If there exist points $v_0 \in V$, $w_0 \in W$ and $u_0 \in U$ such that $\alpha(V \times \{w_0\}) = \alpha(\{v_0\} \times W) = \{u_0\}$ then $\alpha(U \times W) = \{u_0\}$.*

Proof. Let $\pi : V \times W \to W$ be the projection map; since V is complete π is closed. Recall that every regular map from a connected, complete variety to an affine variety is trivial. Let U_0 be an open affine neighborhood of u_0 and define $Z = \pi(\alpha^{-1}(U \setminus U_0)) \subset W$. Z is closed and $w \notin Z$ if and only if $\alpha(V \times \{w\}) \subset U_0$. If $w \in W \setminus Z$ then $V \times \{w\}$ is complete (since it is isomorphic to V) and $\alpha(V \times \{w\}) = \alpha(u_0, w) = \{u_0\}$. The point $w_0 \notin Z$ so $W \setminus Z \neq \varnothing$. But then $V \times (W \setminus Z)$ is a nonempty open subset of $V \times W$. Hence α is constant on a dense open subset and must be constant on all of $V \times W$. □

Corollary 3.3. *If $\alpha : A \to B$ is a regular map of abelian varieties then α is the composition of a homomorphism and a translation.*

Proof. Let e_A and e_B be the identity elements of A and B respectively. $\alpha(e_A) = b$ for some $b \in B$, so by composing with the translation $g \mapsto gb^{-1}$ we can assume that $\alpha(e_A) = e_B$. Define $\varphi : A \times A \to B$ to measure the failure of α to be a homomorphism by $\varphi(a, a') = \alpha(aa')\alpha(a)^{-1}\alpha(a')^{-1}$. Clearly φ is regular and $\varphi(A \times \{e_A\}) = \varphi(\{e_A\} \times A) = e_B$, which implies by the previous theorem that $\varphi(A \times A) = e_B$ and α is a homomorphism. □

Corollary 3.4. *Abelian varieties are abelian.*

Proof. A group G is abelian if and only if the map $\iota(g) = g^{-1}$ is a homomorphism. The inverse map is a regular map for an algebraic group and $\iota(e) = e$, so ι is a homomorphism. □

In the special case where $k = \mathbb{C}$ it can be shown that all abelian varieties are actually projective.

References

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[Hum75] James E. Humphreys. *Linear Algebraic Groups*. Springer, first edition, 1975.

[Mil08] J.S. Milne. Abelian varieties, 2008.

[Spr94] T.A. Springer. *Algebraic Geometry IV*, volume 55 of *Encyclopdia of Mathematical Science*. Springer-Verlag, 1994.

[Spr98] T.A. Springer. *Linear Algebraic Groups*. Birkhauser, second edition, 1998.