Algebraic Geometry Lecture 25 – Algebraic groups

Lee Butler

1. Introductory thingies

An algebraic group is essentially a group that is a variety, or a variety that is a group. Slightly more rigorously we have the following definition.

Def$^{\mathbf{n}}$ 1. Let k be an algebraically closed field. An algebraic group defined over k is:

- an algebraic set G over k;
- a point $e \in G(k)$;
- morphisms $m : G \times G \to G$ and $i : G \to G$ satisfying:
  1. $m(e, x) = m(x, e) = x$,
  2. $m(i(x), x) = m(x, i(x)) = e$,
  3. $m(m(x, y), z) = m(x, m(y, z))$.

We may in general write $m(x, y) = xy$ and $i(x) = x^{-1}$, as long as we remember this is notation only. I'll tend to use the inverse notation but not the other one. As G is only required to be an algebraic set it won't in general be a variety but will have several irreducible components. The irreducible component containing e is denoted G^0 and called the identity component of G. It is a normal subgroup of G of finite index.

For any $g \in G$ we can define right and left translation maps by:

$$R_g : G \to G \qquad\qquad L_g : G \to G$$
$$h \mapsto m(g, h) \qquad\qquad h \mapsto m(h, g),$$

and these are isomorphisms. Indeed,

$$R_g \circ R_{g^{-1}} = \mathrm{id}_G \qquad L_g \circ L_{g^{-1}} = \mathrm{id}_G\,.$$

To see this we just work it out:

$$\begin{aligned} R_g \circ R_{g^{-1}}(h) &= R_g\left(m(g^{-1}, h)\right) \\ &= m(g, m(g^{-1}, h)) \\ &= m(m(g, g^{-1}), h) \\ &= m(e, h) \\ &= h. \end{aligned}$$

And similarly for L_g.

The presence of an isomorphism from a variety to itself is not in itself that interesting, we can always take the identity morphism for that purpose. But given any two elements $g, h \in G$ the translation map $R_{m(h,g^{-1})}$ sends g to h, so we can transfer any property of the variety at g to h. Thus if we want to check the variety is smooth we only have to check it's smooth at a single point, which is dead handy.

2. Examples

Now for a collective nouns worth of examples. Two of the most important examples of algebraic groups in transcendence theory are (thank God) two of the simplest ones.

Example 1. The additive group on k is denoted $\mathbb{G}_a$. It is an algebraic group if one considers the affine variety $k = \mathbb{A}^1$. We have

$$\begin{aligned} m(x,y) &= x+y \\ i(x) &= -x \\ e &= 0. \end{aligned}$$

Example 2. The multiplicative group on $k^\times$ is also an algebraic group, denoted $\mathbb{G}_m$. It is the affine variety $\mathbb{A}^1 \setminus \{0\}$ with

$$\begin{aligned} m(x,y) &= xy \\ i(x) &= x^{-1} \\ e &= 1. \end{aligned}$$

I know what you're thinking — $\mathbb{A}^1 \setminus \{0\}$ isn't an affine variety at all! And verily, with our current definition of affine variety that's true. Rather than give up on $\mathbb{G}_m$, though, we simply extend our definition of affine variety a little bit. Following Shafarevich we say that an affine variety is a quasiprojective variety X that is isomorphic to a closed subset of affine space — i.e. to an affine algebraic set.

With this definition we can see that $\mathbb{A}^1 \setminus \{0\}$ is the quasiprojective variety $\{x \neq 0\} \subset \mathbb{P}^1$. Moreover it is isomorphic to the algebraic set $\{xy - 1 = 0\} \subset \mathbb{A}^2$. Thus it is an affine variety.

The algebraic groups $\mathbb{G}_a$ and $\mathbb{G}_m$ are super important, being the only irreducible one-dimensional affine algebraic groups (up to isomorphism). This shows, in some sense, that addition and multiplication are the only two intrinsic operations on a field, and that we aren't missing any.

Example 3. Another important example is the general linear group

$$\mathrm{GL}(n) = \{(x_{ij}) \in \mathbb{A}^{n^2} \mid \det(x_{ij}) \neq 0\}.$$

This appears to be a quasiprojective variety. For example, when $n = 2$ this is

$$\mathrm{GL}(2) = \mathbb{P}^3 \setminus \{x_0x_3 - x_1x_2 = 0\}.$$

But it can be made into an affine variety by adding a variable and saying

$$\mathrm{GL}(n) = \{(x_{ij}, t) \in \mathbb{A}^{n^2} \times \mathbb{A}^1 \mid t \det(x_{ij}) = 1\}.$$

Now matrix multiplication is given by polynomials in the entries; and inversion is given by a polynomials in the entries as well as division by the determinant. But with the new variable, $1/(\det(x_{ij})) = t$, so inversion is given solely by morphisms too.

Example 4. What about a group that isn't algebraic? Let G be the subgroup of $\mathbb{R} \times \mathbb{R}^\times$ given by

$$H = \{(x, e^x) \mid x \in \mathbb{R}\}.$$

This is a group and a curve in $\mathbb{R}^2$, but isn't a variety. For suppose that there were a polynomial $P \in \mathbb{R}[X, Y]$ such that $P(x, e^x) = 0$ at all $x \in \mathbb{R}$. Then e^x would be an algebraic function, which it isn't. In fact, suppose P has degree d, then $P(x, e^x)$ is a Pfaffian function of order 1 and degree $(1, d)$, so by Khovanskiĭ's theorem it can have at most $2d(d+1)$ zeros.

Actually that's not true, I just wanted to use the word Pfaffian function in a talk. Khovanskiĭ's theorem says the space of zeros of $P(x, e^x)$ can have at most $2d(d+1)$ connected components, so it doesn't prohibit the function being zero everywhere. To prove e^x is transcendental we suppose it is algebraic of degree d. Note that $d > 1$ since if $d = 1$ then e^x is a polynomial, which it isn't. So there is a polynomial $P(x, y) \in \mathbb{C}[x, y]$ of degree d with $P(x, e^x) = 0$. In particular we may write

$$p_0(x) + p_1(x)e^x + p_2(x)e^{2x} + \ldots + p_d(x)e^{dx} = 0.$$

Pulling out a factor of e^x this is

$$e^x Q(x, e^x) + p_0(x) = 0$$

where $\deg Q, \leqslant d - 1$, $\deg p_0 \leqslant d$. If we differentiate the above identity $d + 1$ times we get

$$e^x R(x, e^x) = 0$$

for some polynomial R of degree $\leqslant d - 1$. But $e^x \neq 0$ for any x so in fact we have $R(x, e^x) = 0$. Thus e^x has degree $< d$, a contradiction.

3. More examples

While it may not seem particularly obvious, the most important example of an affine algebraic group from the list above is the general linear group. This is because it turns out that every affine algebraic group is isomorphic to a subgroup of $\mathrm{GL}(n)$ for some n. Because of this, affine algebraic groups are called linear algebraic groups. Projective algebraic groups also exist, though, and they are called abelian varieties. The two types of algebraic group are inexorably linked by the following theorem.

Theorem (Chevalley)**.** *Let G be an algebraic group defined over k. There exists a maximal connected affine subgroup H of G. This subgroup is defined over k and is a normal subgroup of G. Moreover, the quotient G/H has a natural structure as an abelian variety.*

Before we prove anything to do with algebraic groups we have a few more examples.

Example 5. The special linear group is given by

$$\mathrm{SL}(n) = \{(x_{ij}) \in \mathrm{GL}(n) \mid \det(x_{ij}) = 1\}.$$

This is the affine variety defined by $\det(x_{ij}) - 1 = 0$. Since it is defined by a single equation it is a hypersurface in $\mathbb{A}^{n^2}$.

Example 6. The symplectic group is defined by

$$\mathrm{Sp}(2n) = \{(x_{ij}) \in \mathrm{GL}(2n) \mid (x_{ij})^T E (x_{ij}) = E\},$$

where E is the $2n \times 2n$ matrix $E = \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}$, with

$$J = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & & \iddots & 0 \\ \vdots & \iddots & & \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Example 7. Now an example of a subgroup of $\mathrm{GL}(n)$ that isn't a linear algebraic group. Consider the subgroup of $\mathrm{SL}(2)$ over $\mathbb{C}$ given by

$$G = \left\{ A_n := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

One can check that $A_n A_m = A_{n+m}$, so G is a group. But it isn't an affine variety. For suppose there was $f \in \mathbb{C}[x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}]$ that vanished on G. Set

$$\tilde{f}(t) = f(1, t, 0, 1) = f(A_t).$$

So $\tilde{f} \in \mathbb{C}[t]$ has infinitely many roots, one at each $t \in \mathbb{Z}$, and hence $\tilde{f} = 0$. So f vanishes on

$$G' = \left\{ A_c := \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \mid c \in \mathbb{C} \right\}.$$

So any function vanishing on G vanishes on $G' \supsetneq G$, thus G is not closed and hence not an algebraic set.