LINEAR ALGEBRAIC GROUPS: LECTURE 8

JOHN SIMANYI

1. Different Kinds of Groups

So far, we have been treating linear algebraic groups merely as groups, i.e. sets with functions

$$\begin{array}{rrcll} m: & G\times G & \to & G, & \text{(multiplication)}\\ \text{inv}: & G & \to & G, & \text{(inverse)}\\ \text{id}: & 1 & \to & G, & \text{(identity assignment)} \end{array}$$

where 1 is <u>*any*</u> one element set, obeying the usual axioms. The axioms can be written and thought of as commutative diagrams, such as the associative property:

$$\begin{tikzcd} G\times G\times G \arrow[r, "m\times 1_G"] \arrow[d, "1_G\times m"'] & G\times G \arrow[d, "m"] \\ G\times G \arrow[r, "m"] & G \end{tikzcd}$$

By replacing the category of sets by any other category $\mathcal{C}$ with finite products (binary products and the "nullary product") and a terminal object 1, we get the concept of <u>a group in $\mathcal{C}$</u>. As some basic examples:

- A group in the category of topological sets is a <u>topological group</u>.
- A group in the category of smooth manifolds is a <u>Lie group</u>.
- A group in the category of algebraic sets is called an <u>affine algebraic group</u>. Under some conditions on the field k, these are our linear algebraic groups.
- A group in the category of affine schemes, which are both more general and simpler than the above, is called an <u>affine group scheme</u>.
- Even more generally, a group in the category of schemes is a <u>group scheme</u>. We won't be needing these for this course.

Recall that a linear algebraic group is a subgroup of $GL(n)$ defined by some polynomial equations. For example, $SL(n)$ is the subgroup that requires the determinant be one, and the determinant is a polynomial function.

Definition. Given a finite dimensional vector space X over a field k, let $k[X]$ be the set of polynomial functions of the form $f : X \to k$.

Recall that a finite dimensional vector space has a basis, such as $\{e_i\}_{i=1}^n$. We can then write the space as n-tuples $(x_1, \ldots, x_n)$, where $x_i \in k$. Thus any polynomial $f : X \to k$ is really a polynomial

$$f = P(x_1, \ldots, x_n),$$

with coefficients in k.

Date: October 18, 2016.

We also have a natural generalization.

Definition. If X^n, Y^m are vector spaces over a field k, a function $f : X \to Y$ is regular if, after a choice of bases for each,

$$f(x_1, \dots, x_n) \;=\; (P_1(x_1, \dots, x_n), P_2(x_1, \dots, x_n), \dots, P_m(x_1, \dots, x_n))$$

for $P_i \in k[X]$.

2. Algebraic Geometry - an Introduction

Using the definitions above, we can begin a short discourse on algebraic geometry.

Definition. Given a finite dimensional vector space X over a field k, an algebraic set $S \subseteq X$ is one of the form

$$S \;=\; \{x \in X : P_1(x) = P_2(x) = \cdots = P_k(x) = 0\}$$

for some polynomials $P_i \in k[X]$, where by the Hilbert basis theorem finitely many is enough.

What are algebraic sets actually like? Using the duality between geometry and commutative algebra:

Definition. Let X be a vector space over a field k. If $S \subseteq X$, we define

$$I(S) \;=\; \{P \in k[X] : P(x) = 0 \text{ for all } x \in S\},$$

the ideal of S.

Similarly, given an ideal $J \in k[X]$, let

$$V(J) \;=\; \{x \in X : P(x) = 0 \text{ for all } P \in J\},$$

the variety of J.

Notice that if $S \subseteq S' \subseteq X$, then $I(S') \subseteq I(S) \subseteq k[X]$, while if $J \subseteq J' \subseteq k[X]$, then $V(J') \subseteq V(J) \subseteq X$. In other words, we have contravariant functors between posets (partially ordered sets):

$$\begin{tikzcd}
\{\text{subsets of } X\} \arrow[rr, bend left, "I"] & & \{\text{subsets of } k[X]\} \arrow[ll, bend left, "V"]
\end{tikzcd}$$

This is part of what we mean by “duality”, yet these functions I and V, as defined, need not be surjective. What do they actually give?

Theorem. *If $J \subseteq k[X]$, then $V(J)$ is an algebraic set. If $S \subseteq X$, then $I(S)$ is an ideal:*

- *If $P, Q \in I$, then $aP + bQ \subseteq I$ for all $a, b \in k$.*
- *If $P \in I$ and $R \in k[X]$, then $PR \in I$.*

Moreover, it is a radical ideal:

- *If $P^n \in I$, then $P \in I$.*

The proof of the theorem is fairly obvious, and this result gives us contravariant functors

$$\begin{tikzcd} \{\text{algebraic sets in } X\} \arrow[r, bend left, "I"] & \{\text{radical ideals of } k[X]\} \arrow[l, bend left, "V"] \end{tikzcd}$$

It would be even nicer if these were actually inverses, so $V(I(S)) = S$ for any algebraic set $S \in X$, and $I(V(J)) = J$ for any ideal $J \in k[X]$. Under a particular condition, this is true.

Theorem (Hilbert's Nullstellensatz)**.** *If k is algebraically closed, then I and V are inverses.*

Recall that being algebraically closed means every nonconstant polynomial over k has a root. The proof is moderately difficult, and easy to find in books, so we will skip it here.

Unfortunately, some pretty interesting fields, such as $\mathbb{R}$ and $\mathbb{F}_q$, are not algebraically closed, although they can be interesting in a geometric manner (think of the Fano plane). However, $\mathbb{C}$ is closed , and every field (including finite ones) has an algebraic closure by field extensions.

Example 1. Consider the ideal J generated by the polynomial $P(x, y) = x^2 + y^2 - 1$ in $k[\mathbb{R}^2]$, which is the smallest ideal containing $P(x, y)$. Then

$$V(J) \;=\; \left\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0\right\},$$

which is the unit cirlce, an algebraic set. On the other hand, the ideal J' generated by $P'(x, y) = x^2 + y^2 + 1$ is $V(J) = \emptyset$, since $x^2 + y^2 + 1$ can never be zero. However, $V\left(k\left[\mathbb{R}^2\right]\right) = \emptyset$ as well, so the functor V is not one-to-one.

This is one problem that needs to be overcome; another is that we would like to describe algebraic sets intrinsically, not as subspaces dependent on some ambient vector space. For example, our unit circle is the same in the plane as it is in 3-space. To get a more intrinsic approach to algebra sets, we will characterize the algebras of functions on these sets. To do this, we begin with

Definition. If $S \subseteq X$ is an algebraic set, we define the <u>algebra of regular functions on S</u> to be

$$k[S] \;=\; \left\{f : S \to k : f = P\big|_S, \text{ where } P \in k[X]\right\}.$$

Note that $k[S]$ is a commutative algebra. In particular, for $f, g \in k[S]$,

(1) $af + bg \in k[S]$ for all $a, b \in k$.
(2) $fg \in k[S]$.

Theorem. *If $S \subseteq X$ is an algebraic set,*

$$k[S] \;=\; k[X]/I(S).$$

Proof. Every $f \in k[S]$ is the restriction of some $P \in k[X]$. But $P\big|_S = Q\big|_S$ if and only if $P - Q = 0$ on S, so $P - Q \in I(S)$. □

In this manner, we only get a particular type of commutative algebra.

Definition. A commutative algebra A over an algebraically closed field k is called an affine algebra if it is isomorphic to $k[S]$ for some algebraic set S.

We can characterize affine algebras in a nice way:

Theorem. *A commutative algebra A over an algebraically closed field k is affine if and only if:*

1. *It is finitely generated: there exist $x_1, \ldots, x_n \in A$ such that every element of A can be written as $P(x_1, \ldots, x_n)$ for some polynomial with coefficients in k.*
2. *If $x \in A$ is nilpotent (meaning $x^m = 0$ for some m), then $x = 0$.*

As an example of something that is *not* an affine algebra, let $\mathbb{C}[z]$ be the algebra of complex polynomials in one variable z and consider the ideal generated by z^2, which we will write as $J = \left\langle z^2 \right\rangle$. This is not a radical ideal, as

$$z^2 \in J, \qquad \text{but} \qquad z \notin J.$$

In this case,

$$\mathbb{C}\left[z\right]/J \;=\; \left\{az + b : a, b \in \mathbb{C}\right\},$$

the algebra of first order Taylor series in $\mathbb{C}$. Notice that there are plenty of nilpotents here - namely, anything with z as a factor, since $z \neq 0 \bmod J$ but $z^2 = 0 \bmod J$.

Our intrinsic description of algebraic sets will be in terms of the polynomial functions on them, and we will simply decree that they are affine algebras.