Algebraic groups
Lecture 1

Notes by Tobias Magnusson
Lecturer: WG

September 13, 2017

Administration

Registration: A sheet of paper (for registration) was passed around. The lecturers will alternate between Rikard Bögvad and Wushi Goldring (WG).

Office hours (WG): Thursdays, 9-10.

Grading: The examination consists of homework assignments. (Approximately 1 homework assignment every 2-3 weeks.) There'll be no written exams. PhD students are also required to do a presentation at the end of the course.

Literature: Important sections of the course literature will (probably) be posted on the course web. The backbone of the course is covered in Knapp's "Lie groups, Beyond an Introduction". (In particular chapter 1 and 2.) The nature of the various recommended books is discussed in the syllabus.

Prerequisites: The only required course is Algebra III. If you have seen a bit about some of the following, you will probably find it helpful, but it's not required or expected that you have taken courses on these topics:

- Galois theory, as in the course I gave last term.
- Topological spaces, in particular the notion of connectedness, as in Alexander's course last term.
- Some algebraic geometry, as in Jonas and David's course last year
- A first course in complex analysis

I think most of you have taken some fraction of these courses, but many of you have not taken all of them and that's perfectly fine.

Introduction

The title of the course is "Algebraic Groups", but the course will focus on a special class of algebraic groups called reductive groups. These fit in the following diagram:

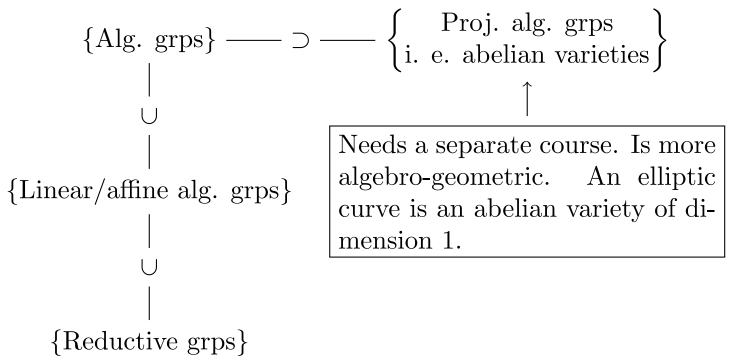

Figure 1: Reductive groups among all algebraic groups

At the core is algebraic groups, which we vaguely define as follows.

Definition 1. An algebraic group is a group given by equations, with multiplication and inversion given by equations.

By equations we mean specifically rational functions. (I. e. quotients of polynomials.) Given a group G, we can see multiplication as the map $m : G \times G \to G$ defined by $(x, y) \mapsto xy$ and inversion as the $i : G \to G$ defined $x \mapsto x^{-1}$.

Given a field k we shall often talk about the n-dimensional affine space of k, denoted by $\mathbb{A}^n(k)$, and "defined" as k^n but without the notion of addition and scalar multiplication. So for example, we've that $\mathbb{A}^n(\mathbb{R}) = \mathbb{R}^n$ but forgetting addition and scalar multiplication.

Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ and consider the following subset of $\mathbb{A}^n(k)$

$$V(f_1, \ldots, f_m) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n(k) | \forall i. \, f_i(a_1, \ldots, a_n) = 0\}.$$

It has a more natural geometric meaning when k is algebraically closed. (E. g. for $k = \mathbb{C}, \overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p}$.)

We want to look at when $V(f_1, \ldots, f_m)$ has a natural group structure. (Note that an elliptic curve is almost an algebraic according to our definition, but the point at infinity yields problems.) Recall that we get an elliptic curve if we put $f_1(x, y) = y^2 - (x^3 + ax + b)$ and look at solutions in $\mathbb{A}^2(k)$ and add the point at infinity. This is equivalent to looking at solutions of the equation $y^2 z = x^3 + axz^2 + bz^3$ in $\mathbb{P}^2(k)$. That's why an elliptic curve is an example of a projective algebraic group, but not of an affine algebraic group.

Examples

The general linear group, $\mathrm{GL}(n)$, is a reductive group. WG asked the audience:

- What is $\mathrm{GL}(n)$?
- What is $\mathrm{GL}(n, k)$?
- More generally, let R be a commutative ring with 1. What is $\mathrm{GL}(n, R)$?

Let's start with $\mathrm{GL}(n, k)$: We know that $\mathrm{GL}(n, k)$ is

$$\begin{pmatrix} \text{invertible linear transformations} \\ \text{of } k^n \end{pmatrix} \cong \begin{matrix} \text{linear automorphisms} \\ \text{of } k^n \end{matrix} \cong \begin{matrix} n \times n \text{ matrices with entries in } k \\ \text{and with } \det \neq 0 \end{matrix}$$

We know that with $\mathrm{GL}(n,k) \ni A = (a_{ij})$, $\det(A)$ is a polynomial in the n^2 variables $a_{11}, a_{12}, \ldots, a_{nn}$, so the third characterization seems useful. So, we try to consider $\mathrm{GL}(n,k)$ in $\mathbb{A}^{n^2}$. Indeed, recall that the set of $n \times n$ matrices with entries in k, denoted by $M_n(k)$, is an n^2 dimensional vector space over k.

Why aren't we done? In other words, in comparison to $V(f_1, \ldots, f_m)$, what's preventing the characterization

$$\mathrm{GL}(n,k) = \{A \in \mathbb{A}^{n^2}(k) | \det(A) \neq 0\},$$

from being an algebraic group? The problem is that $\det(A) \neq 0$ isn't an equation of the form $f_i = 0$ for all i as discussed above; it is rather an equation with $f_i \neq 0$.

Before solving this problem, let's consider a simpler example for a while. We've that the special linear group, $\mathrm{SL}(n,k)$ is defined as follows

$$\mathrm{SL}(n,k) = \{A \in M_n(k) | \det(A) = 1\} = \{A \in \mathbb{A}^{n^2}(k) | \det(A) - 1 = 0\}.$$

This clearly satisfies the first criterion of being an algebraic group. It's easy to see that matrix multiplication is given by polynomials in the entries of the matrices. Using Cramer's rule to find the inverse of a matrix, we see that the inversion map is given by rational functions, so that indeed $\mathrm{SL}(n,k)$ is an algebraic group.

But, how to make $\mathrm{GL}(n)$ an algebraic group? We use the characterization

$$\mathrm{GL}(n) \cong \{(A,t) \in \mathbb{A}^{n^2+1}(k) | (\det A)t - 1 = 0\},$$

which satisfies the criteria.

The equations have integer coeffcients, so they make sense in any field k, and even in any commutative ring R.

Warning: If R is not a field, note that that $GL(n,R)$ is not given by $\{A \in M_n(R) | \det A \neq 0\}$. Indeed the equation above 4 $(\det A)t - 1 = 0$ says that $\det A$ is invertible in R. If R is a field, then $x \in R \setminus \{0\}$ if and only if x is invertible in R. But if R is not a field, then it contains nonzero x which are not invertible. So the right condition for $GL(n,R)$ is that $\det A$ should be invertible in R.

We finally come to the question "What is $GL(n)$?" without specifying a k or an R. What we have seen is that $GL(n)$ gives us a rule: If we input a commutative ring R, the $GL(n)$ rule outputs $GL(n,R)$. One can also check that associated to every homomorphism of rings $R \to S$ we have a homomorphism of groups $\mathrm{GL}(n,R) \to \mathrm{GL}(n,S)$. If you have seen something about categories and functors, what we have seen is that $\mathrm{GL}(n)$ can be seen as a functor from the category of commutative rings to the category of groups. If you haven't heard about functors, that's OK. Just keep in mind that $GL(n)$ can be thought of as a rule which assigns a group to every commutative ring.

BREAK

On affine space

Someone asked a good question during the break: "What kind of object is affine space?" Some good intuition comes from the topological spaces $\mathbb{A}^n(\mathbb{R}) \cong \mathbb{R}^n$ and $\mathbb{A}^n(\mathbb{C}) \cong \mathbb{C}^n$. For more general fields, we will gain a better understanding of $\mathbb{A}^n(k)$ and $\mathbb{A}^n(R)$ when we discuss the Zariski topology later in the course. Historically, the Zariski topology was the first attempt to make sense of topology over fields (and later general rings) different from $\mathbb{R}, \mathbb{C}$. Finally, in an analogous manner to $GL(n)$, we can view affine space $\mathbb{A}^n$ as a functor, i.e. as a rule which assigns $\mathbb{A}^n(R)$ to every commutative ring R.

Some more examples of algebraic groups

One way to get examples is through bilinear forms.

Definition 2. Let V be a vector space over k. A bilinear form is a map $B : V \times V \to k$ that is linear in both arguments. In other

$$B(a_1u_1 + a_2u_2, v) = a_1B(u_1, v) + a_2B(u_2, v),$$

for all $a_1, a_2 \in k$ and all $u_1, u_2, v \in V$, and

$$B(u, a_1 v_1 + a_2 v_2) = a_1 B(u, v_1) + a_2 B(u, v_2),$$

for all $a_1, a_2 \in k$ and all $u, v_1, v_2 \in V$.

Two special types of bilinear forms are especially interesting.

Definition 3. A bilinear form B is called symmetric if for all $u, v \in V$ it holds that

$$B(u, v) = B(v, u).$$

It's called alternating if for all $u \in V$ it holds that

$$B(u, u) = 0.$$

By expanding $B(u + v, u + v) = 0$, we see that $B(u, v) = -B(v, u)$, so an alternating bilinear form is skew-symmetric. Over a field of characteristic $\neq 2$, the conditions $B(u, v) = -B(v, u)$ and $B(u, u) = 0$ for all u, v are equivalent, but over a field of characteristic 2, the condition $B(u, v) = -B(v, u)$ is vacuous (because $2B(u, v) = 0$).

If $\{e_i\}$ is a basis of V, then B can be represented as a matrix

$$A = (a_{ij}) \text{ with } a_{ij} = B(e_i, e_j).$$

If $u, v \in V$ are represented by x, y in this basis, then

$$B(u, v) = {}^t x A y.$$

In the homework you will be asked to show that, if $\{f_i\}$ is another basis and $X e_i = f_i$ (so that X is the change-of-basis matrix) then the matrix of B in the new basis $\{f_i\}$ is ${}^t X A X$.

A symmetric bilinear form is represented by a symmetric matrix, and an alternating bilinear form is represented by a skew-symmetric matrix.

Algebraic groups through bilinear forms

Let B be a bilinear form. Let

$$\mathrm{GL}(V) = \text{linear automorphisms of } V$$

Set

$$\mathrm{G}(B)(k) = \mathrm{G}(B, k) = \{A \in \mathrm{GL}(V) | B(u, v) = B(Au, Av)\}.$$

In otherwords $\mathrm{G}(B, k)$ consists of the matrices that "preserve" the bilinear form.

Exercise: Show that the above is a group.

By the above homework problem on change of basis,

$$\mathrm{G}(B, k) = \{A \in \mathrm{GL}(V) | {}^t A X A = X, \text{ where } X \text{ is the matrix of } B \text{ in some basis}\}$$

This shows that $\mathrm{G}(B, k)$ is given by equations in the entries of A. Thus $\mathrm{G}(B, k)$ is an algebraic group.

On notation: WG typically writes ${}^t A$ for the transpose of A. This is because the inverse of the transpose looks nicer typographically with this notation, namely ${}^t A^{-1}$.

One important algebraic group formed with bilinear forms is the symplectic group. Let B be alternating and non-degenerate. By definition a bilinear form B is non-degenerate if $B(u, v) = 0$ for all v implies $u = 0$. Equivalently, a bilinear form is non-degenerate if the determinant of its matrix is nonzero in some (equivalently every) basis.

A standard choice of skew-symmetric matrix is:

$$J = \begin{pmatrix} 0_n & -I_n \\ I_n & 0_n \end{pmatrix}.$$

Exercise: If B is non-degenerate and alternating on V, then $\dim(V)$ is even.

Definition 4. With B as above, the symplectic group (of B), denoted by $Sp(B)$, is defined as

$$Sp(B) = \{A \in \mathrm{GL}(V) | B(Au, Av) = B(u, v)\} = \{A \in \mathrm{GL}(V) | {}^t AJA = J\}.$$

We also denote it by $Sp(J)$, $Sp(2n, k)$, or $Sp_{2n}(k)$.

We will see later that the symplectic group is another example of a reductive group. Note that if $n = 1$, then $Sp(J) = Sp(2, k) = \mathrm{SL}(2, k)$, but this isn't so when $n > 1$.

Let B be symmetric. In the same way as above, we get the orthogonal group of B.

Definition 5. With B as above, the orthogonal group of B is defined as $\mathrm{G}(B)$.

Consider the following example. Let $k = \mathbb{R}$, and $V = \mathbb{R}^n$. Let $B(u, v)$ be the standard inner product. So that

$$B((u_1, \ldots, u_n), (v_1, \ldots, v_n)) = \sum_{i=1}^{n} u_i v_i.$$

In the standard basis $\{e_i\}_{i=1}^n$, with $e_i = (0, \ldots 0, 1, 0, \ldots, 0)$ and the 1 is in the ith position, B has the matrix I_n, whence

$$\mathrm{G}(B) = \{A \in \mathrm{GL}_n(\mathbb{R}) | {}^t AA = I_n\} = O(n),$$

which might be familiar.

If instead we consider the symmetric bilinear form B with matrix

$$I_{pq} = \begin{pmatrix} 1 & & & & & \\ & \overset{p}{\ddots} & & & 0 & \\ & & 1 & & & \\ & & & -1 & & \\ & 0 & & & \overset{q}{\ddots} & \\ & & & & & -1 \end{pmatrix},$$

where $p + q = n$. Then

$$\mathrm{G}(B) = \{A \in \mathrm{GL}(n, k) | {}^t AI_{pq}A = I_{pq}\} =: O(p, q).$$

Exercise: Show that $O(p, q)$ is a group.

Note that $O(p, q) \not\cong O(n)$, and in fact $\{p, q\} \neq \{p', q'\}$ implies that $O(p, q) \not\cong O(p', q')$.

The fact that we got many non-isomorphic orthogonal groups for a fixed value of $n = p + q$ is related to the fact that we took $k = \mathbb{R}$, a non-algebraically closed field. Since many things are easier to study in an algebraically closed setting, it makes sense that it should be easier to study algebraic groups over algebraically closed fields too.

Endword

In the first part of the course we will study the structure theory of reductive groups over algebraically closed fields. (This is analogous in a finite group setting with the Sylow theorems.) This will lead to the classification of reductive groups over an algebraically closed field. (This is analogous in a finite group setting with the classification of finite simple groups, but the classification of reductive groups turns out to be much simpler. In fact, the reductive classification served as a blueprint for the finite simple groups classification)

A consequence of the classification is that every simple algebraic group is one of the following Cartan-Killing types:

	classical				exceptional				
Type	A_n	B_n	C_n	D_n	G_2	F_4	E_6	E_7	E_8
	$\mathrm{SL}(n+1,k)$	$\mathrm{SO}(2n+1)$	$S_p(2n)$	$\mathrm{SO}(2n)$					

Figure 2: The Cartan-Killing classification.

So there are four infinite families and five exceptional cases. We have gotten some initial idea of the four infinite families by looking at the groups associated to bilinear forms.