18.745 Introduction to Lie Algebras September 30, 2010

Lecture 7 - Zariski Topology and Regular Elements

Prof. Victor Kac *Scribe: Daniel Ketover*

Definition 7.1. A topological space is a set X with a collection of subsets F (the closed sets) satisfying the following axioms:

1) $X \in F$ and $\emptyset \in F$
2) The union of a finite collection of closed sets is closed
3) The intersection of arbitrary collection of closed sets is closed
4) (weak separation axiom) For any two points $x, y \in X$ there exists an $S \in F$ such that $x \in S$ but $y \notin S$

A subset $O \subset X$ which is the complement in X of a set in F is called open. The axioms for a topological space can also be phrased in terms of open sets.

Definition 7.2. Let X = $\mathbb{F}^n$ where $\mathbb{F}$ is a field. We define the Zariski topology on X as follows. A set in X is closed if and only if if is the set of common zeroes of a collection (possibly infinite) of polynomials $P_\alpha(x)$ on $\mathbb{F}^n$

Exercise 7.1. Prove that the Zariski topology is indeed a topology.

Proof. We check the axioms. For 1), let $p(x) = 1$, so that $\mathbb{V}(p) = \emptyset$, so $\emptyset \in F$. If $p(x) = 0$, then $\mathbb{V}(p) = \mathbb{F}^n$, so $\mathbb{F}^n \in F$. For 2), first take two closed sets $\mathbb{V}(p_\alpha)$ with $\alpha \in I$ and $\mathbb{V}(q_\beta)$ with $\beta \in J$, and consider the family of polynomials $f_{\alpha\beta} = \{p_\alpha q_\beta \mid \alpha \in I, \beta \in J\}$. Then $\mathbb{V}(f_{\alpha\beta}) = \mathbb{V}(p_\alpha) \cup \mathbb{V}(q_\beta)$. Therefore $\mathbb{V}(p_\alpha) \cup \mathbb{V}(q_\beta)$ is closed. This can be iterated for any n-fold union. For 3) closure under arbitrary intersections is obvious. For 4), suppose $x \neq y \in \mathbb{F}^n$ and $x = (x_1, x_2, ..., x_n)$. Set $X = \mathbb{V}(p_1, p_2, ..., p_n)$ where $p_i(z) = z_i - x_i$. So $x \in X$ but y is not. □

Example 7.1. If $X = \mathbb{F}$ the closed sets in the Zariski topology are precisely the $\emptyset$, $\mathbb{F}$ and finite subsets of $\mathbb{F}$.

Notation 7.1. Given a collection of polynomials S on $\mathbb{F}^n$ we denote by $\mathbb{V}(S) \in \mathbb{F}^n$ the set of common zeroes of all polynomials in S. By definition, $\mathbb{V}(S)$ are all closed subsets in $\mathbb{F}^n$ in the Zariski topology. If S contains precisely one non-constant polynomial, then $\mathbb{V}(S)$ is called a hypersurface.

Proposition 7.1. *Suppose the field $\mathbb{F}$ is infinite and $n \geq 1$ then*

1) *The complement to a hypersurface in $\mathbb{F}^n$ is an infinite set. Consequently, the complement of $\mathbb{V}(S)$, where S contains a nonzero polynomial, is an infinite set.*
2) *Every two non-empty Zariski open subsets of $\mathbb{F}^n$ have a nonempty intersection*
3) *If a polynomial $p(x)$ vanishes on a nonempty Zariski open set then it is identically zero.*

Example 7.2. The condition that $\mathbb{F}$ be infinite is crucial. In 3), for instance, the polynomial $p(x) = x^2 + x$ on $\mathbb{F}_2$ vanishes at 1 and 0 but is not the zero polynomial.

Proof. For 1), We induct on n. When $n = 1$, since any nonzero polynomial has at most deg P roots, the complement of this set is infinite (since $\mathbb{F}$ is). If $n \geq 1$ then any nonzero polynomial $p(x_1, x_2, ..., x_n)$ can be written as a polynomial in one variable with coefficients polynomials in the other variables. So we can write $p(x) = p_d(x_2, x_3, ..., x_n)x_1^d + p_{d-1}(x_2, x_3, ...x_n)x_1^{d-1} + ... + p_0(x_2, x_3, ..., x_n)$ where $p_d(x_2, x_3, ...x_n)$ is a nonzero polynomial. By the inductive hypothesis, we can find $x_2^o, x_3^o, ..., x_n^o \in \mathbb{F}$ such that $p_d(x_2^o, x_3^o, ..., x_n^o) \neq 0$ Now fixing these values, $p(x) = p_d(x_2^o, x_3^o, ..., x_n^o)x_1^d + p_{d-1}(x_2^o, x_3^o, ...x_n^o)x_1^{d-1} + ... + p_0(x_2^o, x_3^o, ..., x_n^o)$ we are back in the $n = 1$ case. We can find an infinite number of values x_1^o such that $p(x) = p_d(x_2^o, x_3^o, ..., x_n^o)(x_1^o)^d + p_{d-1}(x_2^o, x_3^o, ...x_n^o)(x_1^o)^{d-1} + ... + p_0(x_2^o, x_3^o, ..., x_n^o) \neq 0$. Thus we have found an infinite number of points in $\mathbb{F}^n$ where p does not vanish. To prove the second claim of 1), just observe if S a collection of polynomials containing the nonzero polynomial $p(x)$, we have $\mathbb{V}(S)^C \supset \mathbb{V}(p)^C$ so by the first claim, we have that $\mathbb{V}(S)^C$ contains an infinite set.
2) Consider $\mathbb{V}(S_1)$ and $\mathbb{V}(S_2)$ where S_1 and S_2 are nonzero sets of polynomials. It suffices to prove that $\mathbb{V}(p_1)^C \cap \mathbb{V}(p_2)^C$ is nonempty for any fixed $p_1 \in S_1$ and $p_2 \in S_2$ nonzero polynomials. But observe that $\mathbb{V}(p_1p_2) = \mathbb{V}(p_1) \cup \mathbb{V}(p_2)$, so $\mathbb{V}(p_1p_2)^C = \mathbb{V}(p_1)^C \cap \mathbb{V}(p_2)^C$ but by 1) we know that the term on the left is infinite, hence nonempty.
3) If p vanishes on $\mathbb{V}(S)^C$ for S containing a nonzero polynomial q then p vanishes on $\mathbb{V}(q)^C$. If p were nonzero, then by 2), $\mathbb{V}(q)^C \cap \mathbb{V}(p)^C$ is nonempty. This is a contradiction, so p is identically zero.

□

Let $\mathfrak{g}$ be a finite dimensional Lie algebra of dimension d and consider the characteristic polynomial of an endomorphism **ad** a for some $a \in \mathfrak{g}$: $\det_{\mathfrak{g}}(\mathbf{ad}\ a - \lambda) = (-\lambda)^d + c_{d-1}(-\lambda)^{d-1} + ... + \det(\mathbf{ad}\ a)$.

This is a polynomial of degree d. Because $(\mathbf{ad}\ a)(a) = [a, a] = 0$, we know $\det(\mathbf{ad}\ a) = 0$ and the constant term in the polynomial vanishes.

Exercise 7.2. Show that c_j is a homogeneous polynomial on $\mathfrak{g}$ of degree $d - j$.

Proof. By "polynomial in $\mathfrak{g}$" we mean that if we fix a basis $X_1, X_2, ..., X_d$ of $\mathfrak{g}$ and write a general element $a = \sum_i a_i X_i$, then $c_k(a)$ is a polynomial in the a_i. Observe that **ad** a is a d by d matrix whose entries b_{ij} are linear combinations of the a_i. Now consider $\det_{\mathfrak{g}}(\mathbf{ad}\ a - \lambda)$. This is a polynomial in the entries of the matrix $\mathbf{ad}\ a - \lambda$. A general element in the expansion of this determinant is $b_{**}b_{**}...(b_{ii} - \lambda)...(b_{jj} - \lambda)$. In order to get a term with λ^k we have to chose k λ's and $d - k$ of the b_{**} in the expansion of this product. Therefore the coefficient of the polynomial λ^k is homogeneous of degree $d - k$ in the b_{**}, so it is also homogeneous of degree $d - k$ in the a_i since the b_{ij} are linear in the a_i. □

Definition 7.3. The smallest positive integer such that $c_r(a)$ is not the zero polynomial on $\mathfrak{g}$ is called the rank of $\mathfrak{g}$. Note $1 \leq r \leq n$. An element $a \in \mathfrak{g}$ is called regular if $c_r(a) \neq 0$. The nonzero polynomial $c_r(a)$ of degree $d - r$ is called the discriminant of $\mathfrak{g}$.

Proposition 7.2. *Let $\mathfrak{g}$ be a Lie algebra of dimension d, rank r over $\mathbb{F}$*

1) $r = d$ if and only if $\mathfrak{g}$ is nilpotent.

2) If $\mathfrak{g}$ is nilpotent, the set of regular elements is $\mathfrak{g}$.

3) If $\mathfrak{g}$ is not nilpotent, the set of regular elements is infinite if $\mathbb{F}$ is.

Proof. 1) $r = d$ means that $\det(\mathbf{ad}\ a - \lambda) = (-\lambda)^d$ for all a. This is true if and only if all the eigenvalues of $\mathbf{ad}\ a$ are 0, which happens if and only if $\mathbf{ad}\ a$ is nilpotent for all a. By Engel's theorem, this is equivalent to $\mathfrak{g}$ being nilpotent.
2) If $\mathfrak{g}$ is nilpotent, we know $\det(\mathbf{ad}\ a - \lambda) = (-\lambda)^d$ and $c_r = c_d = 1$, which does not vanish anywhere, so all elements are regular.
3) If $\mathfrak{g}$ is not nilpotent, the set of regular elements is by definition $\mathbb{V}(c_r)^C$, which is the complement of a hypersurface, defined by a homogeneous polynomial of degree $d - r > 0$ by Ex 7.2. By part 1 of the previous theorem the complement of a hypersurface is an infinite set if $\mathbb{F}$ is. □

Example 7.3. For $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{F})$, the rank is n and we will find its discriminant. Also, the set of regular elements consists of all matrices with distinct eigenvalues.

Exercise 7.3. 1) Show that the Jordan decomposition of $\mathbf{ad}\ a$ is given by $\mathbf{ad}\ a = (\mathbf{ad}\ a_s) + (\mathbf{ad}\ a_n)$ in $\mathfrak{gl}_n$
2) If $\lambda_1, ..., \lambda_n$ are eigenvalues of a_s then $\lambda_i - \lambda_j$ are eigenvalues of $\mathbf{ad}\ a_s$
3) $\mathbf{ad}\ a_s$ has the same eigenvalues as $\mathbf{ad}\ a$.

Proof. For 2), If $\lambda_1, ..., \lambda_n$ are eigenvalues of a_s observe that if E_{ij} is the matrix with 1 in the ij slot and zero elsewhere, then $[a_s, E_{ij}] = (a_{sii} - a_{sjj})E_{ij}$ so $\mathbf{ad}\ a_s$ is diagonalizable since the E_{ij} form a basis of $\mathfrak{gl}_n(\mathbb{F})$. The eigenvalues are thus $\lambda_i - \lambda_j$. As for 1), we already showed that $\mathbf{ad}\ a_s$ is diagonalizable, also $\mathbf{ad}\ a_n$ is nilpotent because a_n is. Finally, $\mathbf{ad}\ a_s$ and $\mathbf{ad}\ a_n$ commute: $[\mathbf{ad}\ a_s, \mathbf{ad}\ a_n]v = [a_s, [a_n, v]] - [a_n, [a_s, v]] = -[[a_s, a_n], v] = 0$ (since $[a_s, a_n] = 0$). Thus by uniqueness of Jordan form, $\mathbf{ad}\ a = \mathbf{ad}\ a_s + \mathbf{ad}\ a_n$. As for 3), we know from Jordan canonical form that the semisimple part of an operator and the operator itself have the same eigenvalues – and since $\mathbf{ad}\ a_s$ is the semisimple part of the operator $\mathbf{ad}\ a$, the claim follows. □

Exercise 7.4. Deduce the statement of example 1.3 by showing that the rank of $\mathfrak{gl}_n$ is n and that the discriminant is given by $c_n(a) = \prod_{i \neq j}(\lambda_i - \lambda_j)$. Also compute $c_2(a)$ for $\mathfrak{gl}_2(\mathbb{F})$ in terms of the matrix coefficients of a.

Proof. We must compute $\det(\mathbf{ad}\ a - \lambda)$. This is equal to $\det(\mathbf{ad}\ a_s - \lambda) = \prod_{i,j}(\lambda_i - \lambda_j - \lambda)$. Note when $i = j$, we can pull out the $(-\lambda)$, so we have $\prod_{i,j}(\lambda_i - \lambda_j - \lambda) = (-\lambda)^n \prod_{i \neq j}(\lambda_i - \lambda_j - \lambda)$. Thus we see that the rank of $\mathfrak{gl}_n(\mathbb{F}^n) = n$, and the discriminant is $\prod_{i \neq j}(\lambda_i - \lambda_j)$. An element in $\mathfrak{gl}_n$ is therefore regular if and only if all its eigenvalues are distinct. Finally we compute the discriminant c_2 for $\mathfrak{gl}_2(\mathbb{F})$: $\prod_{i \neq j}(\lambda_i - \lambda_j) = (\lambda_1 - \lambda_2)(\lambda_2 - \lambda_1) = -(\lambda_1 + \lambda_2)^2 + 4\lambda_1\lambda_2$. If we write a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the discriminant is $-(a + d)^2 + 4(ad - bc)$. This a clearly a homogeneous polynomial of degree $n^2 - n = 2^2 - 2 = 2$. □