4. Lecture 4: Elimination theory (Feb 3)

Recommended reading: Kempf §3

4.1. Statement of the result

Recall the following definitions from last time.

Definition 4.1.1. Let X be an algebraic set.

(a) We say that X is **separated** if the diagonal $\Delta \subseteq X \times X$ is a closed subset of $X \times X$.

(b) We say that X is **complete** if X is separated and for every algebraic set Y, the projection map

$$\pi_Y : X \times Y \longrightarrow Y$$

is closed.

Our goal today is to prove the following theorem.

Theorem 4.1.2. *The projective space $\mathbb{P}^n$ is complete.*

We have shown in the previous lecture that $\mathbb{P}^n$ is separated. Our goal is thus to show that for any algebraic set Y and any closed subset $Z \subseteq \mathbb{P}^n \times Y$, the image of Z in Y is closed.

Remark 4.1.3. Over $k = \mathbb{C}$, we can consider the "analytic topology" on an algebraic set X. Let us denote the resulting topological space by X^{an}. Then one can show that

$$X \text{ separated} \Leftrightarrow X^{\mathrm{an}} \text{ Hausdorff}, \qquad X \text{ complete} \Leftrightarrow X^{\mathrm{an}} \text{ compact Hausdorff}.$$

In a course of topology or differential geometry, you might have seen that $\mathbb{C}P^n = (\mathbb{P}^n)^{\mathrm{an}}$ is compact. Theorem 4.1.2 is thus an algebraic analog of this fact.

4.2. Warm-up: the resultant

Before tackling the proof of our theorem, let us deal with a special case (though at first it might not seem like a special case at all).

Let $f, g \in k[T]$ be two polynomials, $\deg(f) = n$, $\deg(g) = m$, $m, n > 0$. Write

$$f = \sum_{i=0}^{n} a_i T^i, \qquad g = \sum_{i=0}^{m} b_i T^i.$$

The **resultant** of f, g is the determinant $R(f,g)$ of the $(n+m) \times (n+m)$ matrix

$$\begin{bmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & \vdots & b_1 & b_0 & \cdots & \vdots \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & \ddots & 0 \\ a_n & \vdots & \ddots & a_0 & b_m & \vdots & \ddots & b_0 \\ 0 & a_n & \ddots & a_1 & 0 & b_m & \ddots & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n & 0 & 0 & \cdots & b_m \end{bmatrix} \tag{4.2.1}$$

Lemma 4.2.1. *Write $f = a_n \prod(T-\alpha_i)$ and $g = b_m \prod(T-\beta_j)$. We have*

$$R(f,g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j).$$

We won't need this, but only the following corollary, for which we supply an independent proof.

Corollary 4.2.2. *We have $R(f,g) = 0$ if and only if f and g have a common root.*

Proof. Since $k[T]$ is an PID, the polynomials f and g have no root in common if and only if they are coprime, i.e. if there exist polynomials $p,q \in k[T]$ such that

$$1 = pf + qg.$$

If we write $p = p_0 g + p_1$ and $q = q_0 f + q_1$ where $\deg(p_1) < m$ and $\deg(q_1) < n$, we have

$$1 = (p_0 + q_0) fg + p_1 f + q_1 g$$

Then $p_0 + q_0 = 0$, otherwise the right-hand side has degree $\geq n+m > 0$. Consequently, $1 = p_1 f + q_1 g$. In other words, we may assume that $\deg(p) < m$ and $\deg(q) < n$.

If we play the same game with the equation $h = pf + qg$ for $\deg(h) < n+m$, we obtain the following observation: For $i \geq 0$, let V_i be the space of polynomials of degree $< i$. Consider the linear map

$$\phi \colon V_m \oplus V_n \longrightarrow V_{n+m}, \qquad \phi(p,q) = pf + qg.$$

Then f and g are coprime if and only if ϕ is surjective.

The result now follows since in the bases $(T^i, 0)$ $(i = 0, \ldots, m-1)$, $(0, T^i)$ $(i = 0, \ldots, n-1)$ in the source $V_m \oplus V_n$ and T^i $(i = 0, \ldots, n+m-1)$ in the target, the matrix of ϕ is (4.2.1). Thus ϕ is surjective if and only if

$$R(f,g) = \det(\phi) \neq 0. \qquad \square$$

Remark 4.2.3. To deduce Lemma 4.2.1 from Corollary 4.2.2, fix the leading coefficients a_n and b_m, and treat the roots α_i, β_j as indeterminates (i.e., work over the polynomial ring $k[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$). The coefficients a_i $(i < n)$ and b_i $(i < m)$ are then expressed using standard symmetric polynomials in the α_i and β_i. Thus both sides of the equality in Lemma 4.2.1 are elements of this polynomial ring. By the corollary, we have $R(f,g) = 0$ if we substitute $\alpha_i = \beta_j$, which (by Nullstellensatz) implies that $(\alpha_i - \beta_j)$ divides $R(f,g)$. These linear polynomials are pairwise coprime, and hence the right-hand side divides the left-hand side. But the degrees and leading terms are the same (check by hand), so this is an equality. (N.B. The same strategy applies to the evaluation of the Vandermonde determinant.)

Since we are here, let us define the discriminant.

Definition 4.2.4. The **discriminant** of a polynomial $f = \sum_{i=0}^n a_i T^i \in k[T]$ of degree $n \geq 0$ is

$$\Delta(f) = (-1)^{n(n-1)/2} a_n^{-1} R(f, f')$$

where $f' = df/dT$ is the formal derivative of f.

Thus $\Delta(f) = 0$ if and only if f has a multiple root. For a quadratic $f = aT^2 + bT + c$, we have the familiar $\Delta(f) = b^2 - 4ac$, and for $f = T^3 + aT + b$ we have

$$\Delta(f) = -4a^3 - 27b^2$$

familiar from the theory of elliptic curves.

4.3. Proof of Theorem 4.1.2: Elimination theory

Theorem 4.3.1. *The projective space $\mathbb{P}^n$ is complete.*

Proof. We have already shown that $\mathbb{P}^n$ is separated (the diagonal being the preimage of the linear subspace $W_{ij} = W_{ij}$ under the Segre embedding $\mathbb{P}^n \times \mathbb{P}^n \to \mathbb{P}^N$, $N+1 = (n+1)^2$. It remains to show that for every algebraic set, the projection map $\mathbb{P}^n \times Y \to Y$ is closed.

Let Y be an algebraic set and let $Z \subseteq \mathbb{P}^n \times Y$ be a closed subset. Then $\pi_Y(Z) \subseteq Y$ is closed if and only if for every affine open $U \subseteq Y$, the subset $\pi_Y(Z) \cap U = \pi_U(Z \cap (\mathbb{P}^n \times U))$ is closed. It therefore suffices to treat the case $Y \subseteq \mathbb{A}^m$ closed. But then Z is closed in $\mathbb{P}^n \times \mathbb{A}^m$, and $\pi_Y(Z)$ is closed in Y if and only if it is closed in $\mathbb{A}^n$. We have now reduced to the case $Y = \mathbb{A}^n$.

Let $T_0, \ldots, T_n$ be the homogeneous coordinates on $\mathbb{P}^n$ and let $x_0, \ldots, x_m$ be the coordinates on $\mathbb{A}^n$. Write $P = k[T_0, \ldots, T_n] = \bigoplus_{d \geq 0} P_d$ and $B = k[x_0, \ldots, x_n]$. Consider the graded polynomial ring

$$A = B \otimes_k P = k[x_0, \ldots, x_m][T_0, \ldots, T_n], \qquad A_d = B \otimes_k P_d.$$

A homogeneous ideal $I \subseteq A$ defines a $k^\times$-invariant closed subset of $(\mathbb{A}^{n+1} \setminus 0) \times \mathbb{A}^m$ and hence a closed subset of $Z \subseteq \mathbb{P}^n \times \mathbb{A}^m$. Every closed subset of $\mathbb{P}^n \times \mathbb{A}^m$ is of this form (easy proof omitted).

Let thus $I \subseteq A$ be the radical homogeneous ideal corresponding to our closed subset $Z \subseteq \mathbb{P}^n \times \mathbb{A}^m$, and write $I = (f_1, \ldots, f_r)$ where $f_i \in A_{d_i} = B \otimes_k P_{d_i}$. Then the image $\pi_{\mathbb{A}^n}(Z)$ is the set of all $(x_1, \ldots, x_m) \in k^n$ for which the system

$$f_i(x_1, \ldots, x_m, T_0, \ldots, T_n) = 0, \qquad i = 1, \ldots, r$$

has a nonzero solution $(t_0, \ldots, t_n) \in k^{n+1}$. Effectively, we wish to eliminate the variables $T_0, \ldots, T_n$ from this system. For this we need:

Claim. *Let $f_1, \ldots, f_r \in P = k[T_0, \ldots, T_n]$ be homogeneous, $f_i \in P_{d_i}$. Then the system $f_i = 0$ has no nonzero solution in k^{n+1} if and only if for some $d \geq 0$, every $f \in P_d$ can be written as*

$$f = \sum_{i=1}^r h_i f_i, \qquad h_i \in P_{d-d_i}.$$

(In other words, if $I_d = P_d$ for some $d \geq 0$. If this holds for d, then it also holds for all $d' > d$, so we can rephrase the condition as: $I_d = P_d$ for $d \gg 0$.)

The claim is almost obvious: having no nonzero solutions means that $V(f_1, \ldots, f_r) \subseteq \{0\} = V(T_0, \ldots, T_n)$. Applying $\mathcal{I}(-)$ translates this to $I = (T_0, \ldots, T_n) \subseteq \sqrt{(f_1, \ldots, f_r)}$, i.e. $T_i^N \in I$ for large enough N. But this means that $I_d = P_d$ for $d \gg 0$ (more precisely, $d > N(n+1)$ will do).

Let us rephrase the condition from the claim: the system $f_i = 0$ has a nonzero solution if and only if for every $d \geq 0$, the map

$$\phi_d \colon \bigoplus_{i=1}^r P_{d-d_i} \longrightarrow P_d, \qquad \phi(h_1, \ldots, h_r) = \sum_{i=1}^r h_i f_i$$

is not surjective. Note that this is a map between finite-dimensional vector spaces over k, corresponding to a big rectangular matrix, say of size $a_d \times b_d$ (the exact values of $a_d = \sum \dim(P_{d_i})$ and $b_d = \dim(P_d)$ are unimportant). Its non-surjectivity can thus be detected by the vanishing of all minors of size $b_d \times b_d$.

Now come back to our initial problem: our $f_1, \ldots, f_n$ depend on the parameters $x_1, \ldots, x_m$. We consider the map between free modules of finite rank (a_d and b_d) over the polynomial ring $B = k[x_1, \ldots, x_m]$:

$$\phi_d \colon \bigoplus_{i=1}^r B \otimes_k P_{d-d_i} \longrightarrow B \otimes_k P_d, \qquad \phi_d(h_1, \ldots, h_r) = \sum_{i=1}^r h_i f_i.$$

By the claim, the image $\pi_{\mathbb{A}^n}(Z)$ is the set of points $(x_1,\dots,x_m)$ at which ϕ_d. By the previous discussion, it is cut out by the ideal generated by the $b_d \times b_d$ minors of the corresponding matrix (now, treated as elements of $k[x_1,\dots,x_m]$) and is therefore closed. □

Corollary 4.3.2. *Every projective algebraic set is complete.*

Remark 4.3.3. Consider the case $n=1$ and $Z \subseteq \mathbb{P}^1 \times Y$ cut out by a pair of functions $f=g=0$ where

$$f=\sum_{i=0}^{n} a_i T_0^{n-i}T_1^i, \qquad g=\sum_{i=0}^{m} b_i T_0^{m-i}T_1^i$$

for $a_0,\dots,a_n,b_1,\dots,b_m \in \mathcal{O}(Y)$ and $a_n,b_m \in \mathcal{O}(Y)^\times$. Then the proofs of Corollary 4.2.2 and of Theorem 4.1.2 give the same description of the image of Z in Y as the vanishing set $V(R)$ of the resultant $R=R(f(1,T),g(1,T)) \in \mathcal{O}(Y)$ (we substituted $T_0=1$ to de-homogenize the polynomials).

4.4. Chevalley's theorem

What can we say about the image of a morphism $Y \to X$ between algebraic sets? If Y is complete and X is separated, then the image is closed. In general, the image is a constructible subset.

Definition 4.4.1. Let X be an algebraic set. A subset $W \subseteq X$ is **constructible** if it is the union of a finite number of locally closed subsets of X.

Importantly, constructible subsets of X form a Boolean algebra (closed under intersection, union, and complement).

Remark 4.4.2. A word of warning: While every locally closed subset of an algebraic set is an algebraic set, not every constructible subset is an algebraic set. For example, the subset

$$\{(0,0)\} \cup D(X) \subseteq \mathbb{A}^2$$

(where the coordinates are X,Y) is constructible but not locally closed, and it does not have any obvious structure of an algebraic set.

Theorem 4.4.3 (Chevalley)**.** *Let $f\colon Y \to X$ be a morphism between algebraic sets and let $W \subseteq Y$ be a constructible subset. Then $f(W)$ is a constructible subset of X.*

Proof. We proved last semester that if $A \to B$ is a morphism of finite type between Noetherian rings, then the image of

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

is constructible. This implies the result if X and Y are affine and $W=Y$. The general case is deduced from this by passing to affine open covers (details omitted). □