Algebraic Curves by William Fulton

Hilbert's Nullstellensatz

slideshow by
William M. Faucette

University of West Georgia

Outline

Table of Contents

Introduction

If we are given an algebraic set V, Proposition 1 from Chapter 1 gives a criterion for telling whether V is irreducible or not. What is lacking is a way to describe V in terms of a given set of polynomials which define V.

The preceding paragraph gives a beginning to this problem, but it is the Nullstellensatz, or Zeros-theorem, which tells us the exact relationship between ideals and algebraic sets.

We begin with a somewhat weaker theorem, and show how to reduce it to a purely algebraic fact. In the rest of this section we show how to deduce the main result from the weaker theorem, and give a few applications.

We assume throughout this section that k is algebraically closed.

Table of Contents

Weak Nullstellensatz

Theorem

If I is a proper ideal in $k[X_1, \dots, X_n]$, then $V(I) \neq \emptyset$.

Proof.

We may assume that I is a maximal ideal, for there is a maximal ideal J containing I, and $V(J) \subset V(I)$. So $L = k[X_1, \dots, X_n]/I$ is a field, and k may be regarded as a subfield of L.

Suppose we knew that $k = L$. Then for each i there is an $a_i \in k$ such that the I-residue of X_i is a_i, or $X_i - a_i \in I$. But $(X_1 - a_1, \dots, X_n - a_n)$ is a maximal ideal, so $I = (X_1 - a_1, \dots, X_n - a_n)$, and $V(I) = \{(a_1, \dots, a_n)\} \neq \emptyset$. □

Weak Nullstellensatz

Thus we have reduced the problem to showing:

($*$) If an algebraically closed field k is a subfield of a field L, and there is a ring homomorphism from $k[X_1, \dots, X_n]$ onto L (which is the identity on k), then $k = L$.

The algebra needed to prove this will be developed in the next two lectures; ($*$) will be proved after that.

Table of Contents

Hilbert's Nullstellensatz

Theorem

Let I be an ideal in $k[X_1, \ldots, X_n]$ (k algebraically closed). Then $I(V(I)) = \mathrm{Rad}(I)$.

In concrete terms, this says the following: if $F_1, \ldots, F_r$, and G are in $k[X_1, \ldots, X_n]$, and G vanishes wherever $F_1, \ldots, F_r$ vanish, then there is an equation $G^N = A_1F_1 + \cdots + A_rF_r$, for some $N > 0$ and some $A_i \in k[X_1, \ldots, X_n]$.

Hilbert's Nullstellensatz

Proof.

That $\mathrm{Rad}(I) \subset I(V(I))$ is easy (Problem **??**). Suppose that G is in the ideal $I(V(F_1, \ldots, F_r))$, $\quad F_i \in k[X_1, \ldots, X_n]$. Let $J = (F_1, \ldots, F_r, X_{n+1}G - 1) \subset k[X_1, \ldots, X_n, X_{n+1}]$. Then $V(J) \subset \mathbb{A}^{n+1}(k)$ is empty, since G vanishes wherever all the F_i's are zero. Applying the Weak Nullstellensatz to J, we see that $1 \in J$, so there is an equation

$$1 = \sum A_i(X_1, \ldots, X_{n+1})F_i + B(X_1, \ldots, X_{n+1})(X_{n+1}G - 1).$$

Let $Y = 1/X_{n+1}$, and multiply the equation by a high power of Y, so that an equation

$$Y^N = \sum C_i(X_1, \ldots, X_n, Y)F_i + D(X_1, \ldots, X_n, Y)(G - Y)$$

in $k[X_1, \ldots, X_n, Y]$ results. Substituting G for Y gives the required equation. □

Hilbert's Nullstellensatz

Corollary

If I is a radical ideal in $k[X_1, \ldots, X_n]$, then $I(V(I)) = I$. So there is a one-to-one correspondence between radical ideals and algebraic sets.

Hilbert's Nullstellensatz

Corollary

If I is a prime ideal, then $V(I)$ is irreducible. There is a one-to-one correspondence between prime ideals and irreducible algebraic sets. The maximal ideals correspond to points.

Hilbert's Nullstellensatz

Corollary

Let F be a nonconstant polynomial in $k[X_1, \dots, X_n]$, $F = F_1^{n_1} \dots F_r^{n_r}$ the decomposition of F into irreducible factors. Then $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components, and $I(V(F)) = (F_1 \dots F_r)$. There is a one-to-one correspondence between irreducible polynomials $F \in k[X_1, \dots, X_n]$ (up to multiplication by a nonzero element of k) and irreducible hypersurfaces in $\mathbb{A}^n(k)$.

Hilbert's Nullstellensatz

Corollary

Let I be an ideal in $k[X_1, \ldots, X_n]$. Then $V(I)$ is a finite set if and only if $k[X_1, \ldots, X_n]/I$ is a finite dimensional vector space over k. If this occurs, the number of points in $V(I)$ is at most $\dim_k(k[X_1, \ldots, X_n]/I)$.

Hilbert's Nullstellensatz

Proof.

Let $P_1, \dots, P_r \in V(I)$. Choose $F_1, \dots, F_r \in k[X_1, \dots, X_n]$ such that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$; let $\overline{F_i}$ be the I-residue of F_i. If $\sum \lambda_i \overline{F_i} = 0$, $\lambda_i \in k$, then $\sum \lambda_i F_i \in I$, so $\lambda_j = (\sum \lambda_i F_i)(P_j) = 0$. Thus the $\overline{F_i}$ are linearly independent over k, so $r \leq \dim_k (k[X_1, \dots, X_n]/I)$.

Conversely, if $V(I) = \{P_1, \dots, P_r\}$ is finite, let $P_i = (a_{i1}, \dots, a_{in})$, and define F_j by $F_j = \prod_{i=1}^r (X_j - a_{ij})$, $j = 1, \dots, n$. Then $F_j \in I(V(I))$, so $F_j^N \in I$ for some $N > 0$ (Take N large enough to work for all F_j). Taking I-residues, $\overline{F}_j^N = 0$, so $\overline{X}_j^{rN}$ is a k-linear combination of $\overline{1}$, $\overline{X}_j, \dots, \overline{X}_j^{rN-1}$. If follows by induction that $\overline{X}_j^s$ is a k-linear combination of $\overline{1}$, $\overline{X}_j, \dots, \overline{X}_j^{rN-1}$ for all s, and hence that $\{\overline{X}_1^{m_1} \cdot \dots \cdot \overline{X}_n^{m_n} \mid m_i < rN\}$ generate $k[X_1, \dots, X_n]/I$ as a vector space over k. □