PCMI 2008 Undergraduate Summer School

Lecture 2: The Nullstellensatz and the Noetherian property.

David Perkinson

Reed College
Portland, OR

Summer 2008

Correspondence

Algebra		Geometry
ideals of R	$\longleftrightarrow$	subsets of $\mathbb{A}^n$
I	$\rightarrow$	$Z(I)$
$I(X)$	$\leftarrow$	X

HW: $I(Z(J)) \supseteq J$ $\quad$ $Z(I(X)) \supseteq X$

$Z(I(Z(J))) = Z(J)$ $\quad$ $I(Z(I(X))) = I(X)$

Theorem (Hilbert's Nullstellensatz)

If k is algebraically closed and $J \subseteq R$ is an ideal, then

$$I(Z(J)) = rad(J).$$

Corollary

If k is algebraically closed and $J \subseteq R$ is a radical ideal, then

$$I(Z(J)) = J.$$

Better correspondence

Algebra		Geometry
radical ideals	$\longleftrightarrow$	algebraic sets
I	$\rightarrow$	$Z(I)$
$I(X)$	$\leftarrow$	X

Corollary (of the Nullstellensatz)

If k is algebraically closed, then the above correspondence is one-to-one.

Proof.

$Z(I(X)) = X$ and $I(Z(J)) = \text{rad}(J) = J$. □

The Hilbert basis theorem.

Every proper algebraic set is the intersection of a finite number of hypersurfaces.

hypersurface: $Z(f)$ for a nonconstant $f \in R$.

Noetherian rings

Definition

An arbitrary ring B is Noetherian if every ideal of B is finitely generated.

Example

A PID is Noetherian, e.g., $k[x]$.

Theorem (Hilbert basis theorem)

$R = k[x_1, \ldots, x_n]$ is Noetherian.

Previous version

$$I \subset R \quad \Rightarrow \quad I = (f_1, \ldots, f_s) \quad \Rightarrow \quad Z(I) = \cap_{i=1}^{s} Z(f_i).$$

Theorem (Hilbert basis theorem)

If B is a Noetherian ring, then so is $B[x_1, \ldots, x_n]$.

Proof.

- $B[x_1, \ldots, x_n] = B[x_1, \ldots, x_{n-1}][x_n]$. So $n = 1$ suffices.
- Let $I \subset B[x]$ be an ideal.
- f_1 a nonzero element of least degree in I.
- For $i > 1$, let f_i an element of least degree in $I \setminus (f_1, \ldots, f_{i-1})$ if possible.
- Let a_i be the leading coefficient of f_i, and $J = (a_1, a_2, \ldots)$.
- B Noetherian implies $J = (a_1, \ldots, a_m)$ for some m.
- $I = (f_1, \ldots, f_m)$. If not, there is an f_{m+1}. Subtract off its leading term using elements of $(f_1, \ldots, f_m)$. Contradiction.

$\square$

Irreducible algebraic sets

Definition

An algebraic set is reducible if it is the union of two proper algebraic subsets. Otherwise, it is irreducible.

Proposition

An algebraic set X is irreducible if and only if $I(X)$ is prime.

Irreducible decomposition

Theorem

If X is an algebraic set, then there are unique irreducibles, $X_1, \ldots, X_m$ such that $X_i \not\subseteq X_j$ for $i \neq j$ and

$$X = X_1 \cup \cdots \cup X_m.$$

The X_i are the irreducible components of X.

Proof of decomposition theorem

Lemma

Every nonempty collection $\mathcal{I}$ of ideals in a Noetherian ring has a maximal element.

Corollary

Every collection of algebraic sets in $\mathbb{A}^n$ has a minimal element.

Proof of decomposition theorem

Consider the bad guys:

$$\mathcal{B} = \{\text{alg. sets in } \mathbb{A}^n\text{, not unions of a finite number of irreds.}\}$$

Now choose a minimal criminal.

Algebraic varieties

The central object of study in algebraic geometry:

Definition

An irreducible algebraic set is called an algebraic variety.