Lectures 5–7: Ideal/variety correspondence and Hilbert's nullstellensatz

Proposition 11. *Let k be a field and $R = k[X_1, \ldots, X_n]$.*

(1) $X \subseteq k^n \Rightarrow X \subseteq \mathbb{V}(\mathbb{I}(X))$ *with equality if and only if X is a variety.*

(2) $X \subseteq Y \subseteq k^n \Rightarrow \mathbb{I}(X) \supseteq \mathbb{I}(Y)$

(3) $J \subseteq R \Rightarrow J \subseteq \mathbb{I}(\mathbb{V}(J))$. *This inclusion may be strict.*

Proof.

(1) Let $x \in X$ then $\mathbb{I}(X)$ only contains polynomials that vanish on all of X and hence on x in particular. Clearly therefore $x \in \mathbb{V}(\mathbb{I}(X))$. Now if $X = \mathbb{V}(\mathbb{I}(X))$ then X is a variety. Conversely, if $X = \mathbb{V}(J)$ for some ideal J then $J \subseteq \mathbb{I}(X)$ so $\mathbb{V}(\mathbb{I}(X)) \subseteq \mathbb{V}(J) = X$ by proposition 10 of lecture 4.

(2) Let $f \in \mathbb{I}(Y)$ then f vanishes on all of Y and hence on all of X.

(3) This proof of this follows a similar argument the first part of (1).

□

Corollary 12 (Descending chain condition on varieties)**.** *If $X_1 \supseteq X_2 \supseteq \cdots \supseteq X_n \supseteq \ldots$ is a descending chain of varieties then there is an integer N such that $X_N = X_{N+1} = \cdots$.*

Similarly, any non-empty set of varieties contains a minimal element.

Proof. Use proposition 11 on the whole chain and then apply the ascending chain condition on ideals. For the second part confer with proposition 6 of lecture 4. □

Hilbert's Nullstellensatz is a key theorem in algebraic geometry and helps us understand when we have equality in part (3). Consider the following examples in which equality does not hold.

Example 13. We consider the real field $\mathbb{R}$ and the polynomial ring $\mathbb{R}[X]$. Let $f = X^2 + 1$ and $J = (f)$ be the ideal generated by f. Clearly $J \neq \mathbb{R}[X]$, but since f has no real roots $\mathbb{V}(J) = \varnothing$. Thus $\mathbb{I}(\mathbb{V}(J)) = k[X] \neq J$.

The key property of the reals being used here is that $\mathbb{R}$ is not algebraically closed and so f does not have enough zeros.

Example 14. Consider a polynomial $f \in k[X_1, \ldots, X_n]$. For any positive integer m we know that $f(P) = 0 \Leftrightarrow f^m(P) = 0$. Thus $\mathbb{V}(f^m) = \mathbb{V}(f)$ but clearly the ideals (f^m) and (f) need not be equal.

Irreducible varieties

Definition 15 (Irreducible)**.** A variety $X \subseteq k^n$ is called *irreducible* if whenever $X = X_1 \cup X_2$ for X_i varieties then either $X_1 = X$ or $X_2 = X$. That is, we cannot decompose X into a union of strict subvarieties.

Example 16. Consider the variety $\mathbb{V}(XY) \subseteq \mathbb{C}^2$. The polynomial XY is zero if either $X = 0$ or $Y = 0$ hence $\mathbb{V}(XY)$ consists of the X-axis and the Y-axis. That is, $\mathbb{V}(XY) = \mathbb{V}(X) \cup \mathbb{V}(Y)$, hence it is *reducible*.

Proposition 17. *Let X be a variety and $\mathbb{I}(X)$ its corresponding ideal.*

(1) X is irreducible if and only if $\mathbb{I}(X)$ is a prime ideal.

(2) X can be expressed uniquely (up to permutation) as a union of irreducible varieties

$$X = X_1 \cup X_2 \cup \cdots \cup X_n$$

such that $X_i \not\subset X_j$ for all $i \neq j$.

The X_i in the decomposition are called the irreducible components *of X.*

Proof.

(1) We prove X is reducible $\Leftrightarrow \mathbb{I}(X)$ is not a prime ideal.

($\Rightarrow$) Suppose X is reducible so $X = X_1 \cup X_2$. Since $X_i \neq X$ there is an $f_i \in \mathbb{I}(X_i) \setminus \mathbb{I}(X)$ for each i. Now clearly $f_1(P)f_2(P) = 0$ for all $P \in X$ hence $f_1 f_2 \in \mathbb{I}(X)$ but neither $f_i \in \mathbb{I}(X)$ and therefore $\mathbb{I}(X)$ is not prime.

($\Leftarrow$) Suppose $\mathbb{I}(X)$ is not prime so there are elements $f_1, f_2 \notin \mathbb{I}(X)$ such that $f_1 f_2 \in \mathbb{I}(X)$. Let $J_i = \mathbb{I}(X) + (f_i)$ for each i and let $X_i = \mathbb{V}(J_i)$. Now $X_i \subsetneq X$ for each i thus $X \supseteq X_1 \cup X_2$. To see the opposite inclusion consider $P \in X$. If $f_1(P)f_2(P) = 0$ then either $f_1(P) = 0$ or $f_2(P) = 0$ thus $P \in X_1$ or $P \in X_2$.

(2) Let $\mathcal{X}$ be the set of varieties of k^n that do not have a decomposition into a union of irreducible varieties. If $\mathcal{X} = \varnothing$ then we are done so assume that $\mathcal{X}$ is non-empty and therefore (by corollary 12) contains a minimal element $X \in \mathcal{X}$. As irreducible elements have a trivial decomposition we conclude $X = X_1 \cup X_2$ is reducible and by minimality $X_i \notin \mathcal{X}$. Therefore each X_i can be decomposed into a union of irreducible varieties and thus so can X. We conclude $\mathcal{X}$ is empty.

The uniqueness of decomposition is left as an exercise.

□

Nullstellensatz

Hilbert's Nullstellensatz is a fundamental theorem in algebraic geometry, the proof of which hinges on Zariski's lemma, which we will state but not prove. You may wish to consider exploring Zariski's lemma for your project.

Definition 18 (Finitely generated k-algebra)**.** A ring R is called a *finitely generated k-algebra* if there are elements $r_1, \ldots, r_n \in R$ such that $R = k[r_1, \ldots, r_n]$. That is, every element of R can be expressed as a sum of products of the elements r_i with coefficients from k.

Proposition 19. *If $R = k[r_1, \ldots, r_n]$ is a finitely generated k-algebra then R is isomorphic to the quotient of a polynomial ring by some ideal: $R \cong k[X_1, \ldots, X_n]/I$. Thus by proposition 7 and corollary 9 of lecture 4 each finitely generated k-algebra is Noetherian.*

Proof. Consider the homomorphism

$$\begin{array}{rcl} \varphi\colon k[X_1, \ldots, X_n] & \longrightarrow & k[r_1, \ldots, r_n] \\ X_i & \mapsto & r_i \end{array}$$

Let $I = \ker \varphi$ and apply the first isomorphism theorem (from Algebra 2). □

Theorem 20: *Zariski's Lemma*

> Let k be a field and let R be a finitely generated k-algebra. If R is a field then R is algebraic over k.

Recall. If F/K is a field extension then an element of $x \in F$ is said to be algebraic over K if there is a polynomial $f \in K[X]$ such that $f(x) = 0$. If no such polynomial exists then x is said to be transcendental.

The field F is algebraic over K if every element of F is algebraic.

Theorem 21: *Weak Nullstellensatz*

> Let k be an algebraically closed field and let $R = k[X_1, \ldots, X_n]$.
>
> (1) Every maximal ideal of R is of the form $\mathfrak{m}_P = (X_1 - r_1, \ldots, X_n - r_n) = \mathbb{I}(P)$ for some point $P = (r_1, \ldots, r_n) \in k^n$.
>
> (2) If $J \subsetneq R$ is a proper ideal then $\mathbb{V}(J) \neq \varnothing$.

Proof.

(1) Let $\mathfrak{m} \subset R = k[X_1, \ldots, X_n]$ be a maximal ideal and let $K = R/\mathfrak{m}$. Note that K is a field since $\mathfrak{m}$ is maximal. Let $\iota\colon k \hookrightarrow R$ be the natural inclusion of k into R and let $\pi\colon R \twoheadrightarrow K$ be the natural projection of R onto K. Let $\varphi = \pi \circ \iota\colon k \to K$ be the composition of these two homomorphisms. It is clear that K is a finitely generated k-algebra (simply take as generators the images $\pi(X_i) \in K$) and therefore by Zariski's lemma (20) K is algebraic over k. By assumption k is algebraically closed and therefore $K \cong k$ and φ is an isomorphism.

Let $b_i = \pi(X_i)$ be the image of X_i under the natural projection and let $r_i = \phi^{-1}(b_i)$ for each i. Then $\pi(X_i - r_i) = 0$ and so each $(X_i - r_i) \in \ker \pi = \mathfrak{m}$. Thus $(X_1 - r_1, \ldots, X_n - r_n) \subseteq \mathfrak{m}$. Since $(X_1 - r_1, \ldots, X_n - r_n)$ is maximal we must have equality.

(2) As J is a proper ideal there is a maximal ideal $\mathfrak{m} \supseteq J$. By (1) there is a point $P = (r_1, \ldots, r_n) \in k^n$ such that $\mathfrak{m} = (X_1 - r_1, \ldots, X_n - r_n)$. Clearly $f(P) = 0$ for all $f \in \mathfrak{m}$ and therefore $f(P) = 0$ for all $f \in J$. That is, $P \in \mathbb{V}(J)$.

□

Note. As we have already established (see example 13) this theorem is completely false in the case that k is not algebraically closed. In this case it is easy to find a non-constant polynomial f, with no zeros in k, but clearly $1 \notin (f)$.

Theorem 22: *Hilbert's Nullstellensatz*

Let k be an algebraically closed field and let $R = k[X_1, \ldots, X_n]$.

If $J \subseteq R$ is an ideal then $\mathbb{I}(\mathbb{V}(J)) = \operatorname{rad} J$.

Proof. Let $J \in R = k[X_1, \ldots, X_n]$ be any ideal and let $f \in \mathbb{I}(\mathbb{V}(J))$. We already know that $\operatorname{rad} J \subseteq \mathbb{I}(\mathbb{V}(J))$ by the example 14 so we need only show that $f \in \operatorname{rad} J$. We prove this using the Weak Nullstellensatz and a clever idea known as the Rabinowitsch trick.

We introduce a new variable Y and consider the ideal $(J, fY - 1) \subseteq R[Y] = k[X_1, \ldots, X_n, Y]$. As $f \in \mathbb{I}(\mathbb{V}(J))$ we know that if all polynomials in J vanish at some point $P \in k^n$ then $f(P) = 0$ as well. Clearly therefore $(J, fY - 1) = \varnothing$, since if all polynomials in J vanish, the last polynomial takes the value -1. We can now apply the Weak Nullstellensatz and deduce that $1 \in (J, fY - 1)$. That is, for some $g_i \in R[Y]$ and some $f_i \in J$ we have

$$1 = g_0(fY - 1) + \sum_{i=1}^{t} g_i f_i$$

Now since Y is a free variable this identity continues to hold if we replace Y by some other expression, thus we may substitute $Y = 1/f$ and consider the expression over the

field $K(X_1, \ldots, X_n)$. Spelling this out we have

$$1 = \sum_{i=1}^{t} g_i(X_1, \ldots, X_n, 1/f) f_i(X_1, \ldots, X_n)$$

Notice however that the only things that can appear in the denominator of this fraction are powers of f, thus we may change to a common denominator and rewrite this as

$$1 = \frac{\sum h_i(X_1, \ldots, X_n) f_i(X_1, \ldots, X_n)}{f(X_1, \ldots, X_n)^s}$$

Finally we can multiply through by f^s and we have an expression that lives in R

$$f^s = \sum h_i(X_1, \ldots, X_n) f_i(X_1, \ldots, X_n)$$

This demonstrates that $f \in \operatorname{rad} J$ and completes the proof. □

Corollary 23. *Let k be an algebraically closed field and let $R = k[X_1, \ldots, X_n]$.*

The correspondences $\mathbb{V}$ and $\mathbb{I}$ induce bijections between radical ideals of R and varieties of k^n and bijections between prime ideals of R and irreducible varieties of k^n.

$$\begin{array}{ccc}
\{\textit{ideals } I \subseteq R\} & \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} & \{\textit{subsets } X \subseteq k^n\} \\
\cup\mathrm{I} & & \cup\mathrm{I} \\
\{\textit{radical ideals } I \subseteq R\} & \rightleftarrows & \{\textit{varieties } X \subseteq k^n\} \\
\cup\mathrm{I} & & \cup\mathrm{I} \\
\{\textit{prime ideals } I \subseteq R\} & \rightleftarrows & \{\textit{irreducible varieties } X \subseteq k^n\}
\end{array}$$

Proof. This is routine by using propositions 11 and 17 and the Nullstellensatz. □

Coordinate rings

Let $V \subseteq k^n$ be a variety and consider a polynomial function on V. This is simply the restriction of a polynomial $f \in k[X_1, \ldots, X_n]$ to the set V. Two polynomials f and $g \in k[X_1, \ldots, X_n]$ represent the same function on V whenever $f(P) - g(P) = 0$ for all $P \in V$. That is, whenever $f - g \in \mathbb{I}(V)$. This gives us the next definition.

Definition 24 (Coordinate ring)**.** Let $V \subseteq k^n$ be a variety. The *coordinate ring* $k[V]$ is defined to be

$$k[V] = \{f \colon V \to k \mid f \text{ is a polynomial}\} \cong k[X_1, \ldots, X_n]/\mathbb{I}(V)$$

Each ideal of $k[V]$ corresponds to an ideal J of $k[X_1, \ldots, X_n]$ containing $\mathbb{I}(V)$. Thus $\mathbb{V}(J) \subseteq V$ by proposition 11. Conversely if $X \subseteq V$ then $\mathbb{I}(X) \supseteq \mathbb{I}(V)$ and thus $\mathbb{I}(X)$ corresponds to an ideal of $k[V]$. Therefore the correspondences $\mathbb{I}$ and $\mathbb{V}$ restrict to the coordinate ring and variety.

$$\{\text{ideals } I \subseteq k[V]\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \{\text{subsets } X \subseteq V\}$$

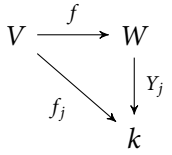
Recall. Let $V \subseteq k^n$ and $W \subseteq k^m$ be varieties. Let $X_1, \ldots, X_n$ be the coordinates of k^n and $Y_1, \ldots, Y_m$ be the coordinates of k^m.

A morphism of varieties $f: V \to W$ is simply a map between the varieties that may be realised by polynomial functions:

$$f(P) = (f_1(P), \ldots, f_m(P)) \in W \subseteq k^m \quad \text{for all } P \in V$$

where each $f_i \in k[X_1, \ldots, X_n]$.

Definition 25 (Coordinate function)**.** The function $f_j = Y_j \circ f$ is called the jth *coordinate function*.



Proposition 26. *A general function $f: V \to W$ is a morphism of varieties if and only if each coordinate function is an element of the coordinate ring $k[V]$.*

Proof. The proof of this proposition is left as an exercise. □

Theorem 27:

Let $V \subseteq k^n$ and $W \subseteq k^m$ be varieties.

(1) A morphism of varieties $f: V \to W$ induces a ring homomorphism $f^*: k[W] \to k[V]$ between the coordinate rings but in the opposite direction. Where f^* is simply the composition of maps: $f^*(g) = g \circ f$ for all $g \in k[W]$. Moreover, the map f^* restricts to the identity map on k.

(2) Conversely any ring homomorphism $\Phi: k[W] \to k[V]$ that restricts to the identity map on k is uniquely determined by a map of varieties $f: V \to W$.

(3) If $f: V \to W$ and $g: W \to U$ are morphisms of varieties then $(g \circ f)^* = f^* \circ g^*$.

Note. Recall that coordinate rings are actually finitely generated k-algebras. Ring homomorphisms that restrict to the identity map on k such as those described in this theorem are known as k-algebra homomorphisms.

Proof.

(1) Clearly the composition of polynomial maps is a polynomial map and so by proposition 26 $f^*(g) \in k[V]$. And obviously if we pre-compose a constant map with any other map, it remains a constant function. Thus, $f^*(a) = a$ for any $a \in k$. Finally it is plain to see that $f^*(g_1 + g_2) = (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f = f^*(g_1) + f^*(g_2)$ and similarly, $f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$.

(2, 3) This is left as an exercise.

□

Corollary 28. *There is a bijection (duality)*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{morphisms of varieties} \\ f\colon V \to W \end{array} \right\} & \longrightarrow & \left\{ \begin{array}{c} k\textit{-algebra homomorphisms} \\ \Phi\colon k[W] \to k[V] \end{array} \right\} \\ f & \mapsto & f^* \end{array}$$

such that f is an isomorphism if and only if f^* is an isomorphism.