CLASS 21, APRIL 10TH: HILBERT-NULLSTELLENSATZ THEOREM

Recall last time we ended with this result:

Corollary 1. *$X \subseteq V(I(X))$ with equality if and only if X is a variety, i.e. $X = V(I)$. Similarly, $J \subseteq I(V(J))$ for any ideal J.*

The if and only if part of this corollary is actually the inspiration to define a variety this way; it is precisely the the collection of subsets X for which $X = V(I(X))$. Note the following example demonstrates that it is not always the case:

Example 21.1. Consider $\langle x^n \rangle \subseteq \langle x \rangle \subseteq K[x]$. By Proposition 20.7, we have that $V(x^n) \supseteq V(x)$. On the other hand, both sets are just the point $0 \in K$! Thus $V(x^n) = V(x)$.

Similarly, if we take $X = \mathbb{Z} \subseteq \mathbb{C}$, then the set of functions in $\mathbb{C}[x]$ which vanish at $\mathbb{Z}$ are precisely the zero function. Thus $I(\mathbb{Z}) = 0$. But $V(I(\mathbb{Z})) = \mathbb{C} \neq \mathbb{Z}$! So of course $\mathbb{Z} \subseteq \mathbb{C}$ is not an algebraic variety.

This brings up the following question: what are the set of ideals for which $I(V(J)) = J$? This was resolved by Hilbert:

Theorem 21.2 (Hilbert-Nullstellensatz)**.** *Assume K is an algebraically closed field. If $J \subsetneq K[x_1, \ldots, x_n]$ is an ideal, then $V(J) \neq \emptyset$. Furthermore, $I(V(J)) = \sqrt{J}$.*

Recall the statement that

$$\sqrt{J} = \bigcap_{J \subseteq \mathfrak{p} \text{ prime}} \mathfrak{p}$$

The Nullstellensatz gives an even stronger result: we can take the intersection to be only over maximal ideals containing J!

$$\sqrt{J} = \bigcap_{J \subseteq \mathfrak{m} \text{ maximal}} \mathfrak{m}$$

To see this, note that $V(J)$ is in bijection with the set of maximal ideals containing J, via $a = (a_1, \ldots, a_n) \longleftrightarrow \langle x_1 - a_1, \ldots, x_n - a_n \rangle = \mathfrak{m}_a$. Note $\mathfrak{m}_a$ is precisely the set of functions vanishing at a. Applying I asks what polynomials vanish at each of these points? Well that is exactly the intersection of the polynomials vanishing at each point!

This also extends to non-algebraically closed fields K by Corollary 20.2 from last time, and to quotients of such rings by the ideal correspondence.

Of course, it should be noted that this can not be pushed to arbitrary rings (in general rings with this property are called **Jacobson Rings**). Considerations for a local ring provide counterexamples to this statement more broadly:

Example 21.3. If $R = K[x, y]_{\langle x,y \rangle}$, then the ideal $\langle x^2+y^2-1 \rangle$ is prime (unless $char(K) = 2$). However, it is not equal to the intersection of maximal ideals, since there is only 1: $\langle x, y \rangle$.

Proof. (of Theorem 21.2) For the first statement, notice that $J \subseteq \mathfrak{m}$ for some maximal ideal. Thus

$$V(J) \supseteq V(\mathfrak{m}) = V(\langle x_1 - a_1, \ldots, x_n - a_n \rangle) = (a_1, \ldots, a_n)$$

The second statement is far more interesting. It is easy to see that $I(V(J)) \supseteq \sqrt{J}$, since $f(a_1, \ldots, a_n) = 0$ if and only if $f^n(a_1, \ldots, a_n) = 0$. Suppose $f \in I(V(J))$. That is to say the $f(P) = 0$ for every $P \in V(J)$.

Fix such an $f \in I(V(J))$ and construct an auxiliary polynomial ring $S' = K[x_1, \ldots, x_n, y]$ and consider the ideal $J' = J \cdot S' + \langle fy - 1 \rangle$. If we consider $V(J')$, it necessarily is empty! This is because if $(a_1, \ldots, a_n, b) \in V(J')$, then we have $g(a_1, \ldots, a_n) = 0$ for every $g \in J \subseteq J'$. This is to say $(a_1, \ldots, a_n) \in V(J)$, which implies $f(a_1, \ldots, a_n) = 0$ since $f \in I(V(J))$. However, this yields $f(a)b - 1 = -1 \neq 0$. This contradicts the choice of our point.

By the first part of the Theorem, we have that this implies $J' = K[x_1, \ldots, x_n, y]$. This is to say

$$1 = \sum_i g_i h_i + g_0(fy - 1) \qquad \text{for some } g_i \in K[x_1, \ldots, x_n, y],\ h_i \in J$$

Multiplying this by some sufficiently high power of f, enough to dominate the appearances of y, we get

$$f^m = \sum_i G_i H_i + G_0(fy - 1) \qquad \text{for some } G_i \in K[x_1, \ldots, x_n, fy],\ H_i \in J$$

But since this is a relationship between polynomials, we can set the 'variable' $fy = 1$. Doing so verifies that $f^m \in J$, as desired. □

A corollary is that V and I induce bijections between radical ideals and varieties:

$$\{J = \sqrt{J} \subseteq K[x_1, \ldots, x_n]\} \longleftrightarrow \{X = V(J) \subseteq K^n\}$$

As we have noted previously, prime ideals are themselves radical. Therefore, we can also naturally detect what prime ideals represent under this correspondence.

Definition 21.4. A variety $X \subseteq K^n$ is called **irreducible** if X cannot be expressed as a union of 2 proper subvarieties:

$$X \neq X_1 \cup X_2 \quad \text{where } X_1 \neq X \neq X_2$$

Otherwise, X is called **reducible**.

This is exactly the geometric analog of being prime. We will pick up with the proof of the following statement next time:

Proposition 21.5. *X is irreducible if and only if $I(X)$ is prime:*

$$\mathit{Spec}(K[x_1, \ldots, x_n]) = \{J \subseteq K[x_1, \ldots, x_n] \textit{ prime}\} \longleftrightarrow \{V = V(J) \subseteq K^n \textit{ irreducible}\}$$

Example 21.6. If we consider the ideal $J = \langle xy \rangle$ in $K[x, y]$, geometrically we get a union of the lines $x = 0$ and $y = 0$ in K^2. Therefore we anticipate that $V(J)$ is reducible. Indeed, it is easy to check that $V(J) = V(x) \cup V(y)$.

So we can already see that the variety associate to a non-prime ideal can be reducible, facilitating Proposition 21.5's plausibility.