9. Ideals and the Zariski Topology

Definition 9.1. *Let $X \subset \mathbb{A}^n$ be a subset.*

*The **ideal** of X, denoted $I(X)$, is simply the set of all polynomials which vanish on X.*

*Let $S \subset K[x_1, x_2, \dots, x_n]$. Then the **vanishing locus** of S, denoted $V(S)$, is*

$$\{\, p \in \mathbb{A}^n \mid f(x) = 0, \forall f \in S \,\}.$$

Lemma 9.2. *Let X, $Y \subset \mathbb{A}^n$ and I, $J \subset K[x]$ be any subsets.*

1. *$X \subset V(I(X))$.*
2. *$I \subset I(V(I))$.*
3. *If $X \subset Y$ then $I(Y) \subset I(X)$.*
4. *If $I \subset J$ then $V(J) \subset V(I)$.*
5. *If X is a closed subset then $V(I(X)) = X$.*

Proof. Easy exercise. □

Note that a similar version of (5), with ideals replacing closed subsets, does not hold. For example take the ideal $I \subset K[x]$, given as $\langle x^2 \rangle$. Then $V(I) = \{0\}$, and the ideal of functions vanishing at the origin is $\langle x \rangle$.

It is natural then to ask what is the relation between I and $I(V(I))$. Clearly if $f^n \in I$ then $f \in I(V(I))$.

Definition 9.3. *Let I be an ideal in a ring R. The **radical of** I, denoted $\sqrt{I}$, is*

$$\{\, r \in R \mid r^n \in I, \text{ some } n \,\}.$$

It is not hard to check that the radical is an ideal.

Theorem 9.4 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field and let I be an ideal.*

Then $I(V(I)) = \sqrt{I}$.

Proof. One inclusion is clear, $I(V(I)) \supset \sqrt{I}$.

Now suppose that $g \in I(V(I))$. Pick a basis $f_1, f_2, \dots, f_k$ for I. Suppose that $f_i(x) = 0$, for $1 \leq i \leq k$. Then $f(x) = 0$ for all $f \in I$ so that $x \in V(I)$. But then $g(x) = 0$. So we may apply the strong Nullstellensatz to $f_1, f_2, \dots, f_n, g$ to conclude that $g^r \in I$, some $r > 0$, that is $g \in \sqrt{I}$. □

Given any ring, a natural question is to identify the prime and maximal ideals. Now in the ring $K[x]$, there is an obvious source of maximal ideals, the ideals of the form

$$\langle x_1 - a_1, x_2 - a_2, \dots x_n - a_n \rangle,$$

where $(a_1, a_2, \dots, a_n) \in \mathbb{A}^n$. Recall we proved:

Corollary 9.5. *Let K be an algebraically closed field.*

Then every maximal ideal of $K[x]$ is of the form $m_a = \langle x_1 - a_1, x_2 - a_2, \dots x_n - a_n\rangle$, where $a_1, a_2, \dots, a_n$ are elements of K.

Note that with this formulation it is clear why we need K to be algebraically closed. Indeed $I = \langle x^2 + 1\rangle$ over $\mathbb{R}$ is in fact maximal and the vanishing locus is empty.

Another way to restate the Nullstellensatz is to observe that it establishes an inclusion reversing correspondence between ideals and closed subsets of $\mathbb{A}^n$. However this is just the tip of the iceberg.

Definition 9.6. *Let $X \subset \mathbb{A}^n$ be a closed subset.*

The ***coordinate ring of*** *X, denoted $A(X)$, is the quotient*

$$K[X]/I(X).$$

Corollary 9.7. *Let $X \subset \mathbb{A}^n$ be a closed subset over an algebraically closed field.*

There is a correspondence between the points of X and the maximal ideals of the coordinate ring $A(X)$.

Proof. One direction is clear. Given a point $x \in X$, the ideal $m_x \trianglelefteq A(X)$, the image of $m_x \trianglelefteq K[x]$, is clearly maximal. To prove the converse, suppose that $M \subset A(X)$ is maximal. Let M' be the inverse image of M in $K[x]$. By (9.5) M' is contained in a maximal ideal of the form m_a. As

$$I(X) \subset M' \subset m_a,$$

it follows that $a \in X$ so that $M \subset m_a \trianglelefteq A(X)$. But then $M = m_a$, by maximality. $\square$

In fact this correspondence is natural. To prove this, we have to reinterpret the coordinate ring. It is also necessary to investigate the Zariski topology.

Definition 9.8. *Let X be a topological space. We say that X is* ***Noetherian*** *if the set of closed subsets satisfies DCC (the descending chain condition). That is any sequence of descending closed subsets eventually stablises*

$$\dots \subset X_n \subset X_{n-1} \subset \dots \subset X_1 \subset X_0.$$

Proposition 9.9. *Any quasi-projective variety is Noetherian.*

Proof. We prove this only for an affine variety; as we will see later the general case is practically identical in execution.

Let $X \subset \mathbb{A}^n$ be a closed subset. We may as well suppose that $X = \mathbb{A}^n$. Now, by (9.2) a descending chain of closed subsets of $\mathbb{A}^n$ is the same as an ascending chain of ideals. Now apply Hilbert's basis Theorem. ☐

In other words DCC for closed subsets is the same as ACC for ideals, which is the content of Hilbert's basis Theorem.

Principle 9.10 (Noetherian Induction). *Let P be a property of topological spaces. Suppose that for every topological space X such that for every proper closed subset $Y \subset X$, $P(Y)$ holds, then $P(X)$ holds.*

Then every Noetherian topological space satisfies property P.

Proof. Suppose not. Let X be a Noetherian topological space, minimal with the property that it does not satisfy property P.

Let $Y \subset X$ be a proper closed subset. By minimality of X, Y satisfies property P. By the inductive hypothesis, X then satisfies property P, a contradiction. ☐

Definition 9.11. *Let X be a topological space. We say that X is **irreducible** if for every pair of closed subsets F_1 and F_2, such that $F_1 \cup F_2 = X$, we have either $X = F_1$ or $X = F_2$.*

Compare this definition, with the definition of connected. Clearly the definition of irreducible is stronger than connected; in practice most connected topological spaces are rarely irreducible. For example if X is irreducible (and has at least two points) then it is not Hausdorff.

Lemma 9.12. *Let X be an irreducible variety.*

Then every open subset is dense.

Proof. Let U and V be two non-empty subsets. Suppose that $U \cap V$ is empty. Let F and G be their complements. Then F and G are two proper closed subsets, whose union is X, a contradiction. ☐

Lemma 9.13. *Let X be a Noetherian topological space.*

Then X has a decomposition into closed irreducible factors

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

where X_i is not contained in X_j, unique up to re-ordering of the factors.

Proof. If X is irreducible there is nothing to prove. Otherwise we may assume that $X = A \cup B$, where A and B are proper closed subsets. By the principle of Noetherian Induction, we may assume that A and B are the finite union of closed irreducible factors. Taking the union, and discarding any redundant factors (that is any subset contained in another subset), we get existence of such a decomposition.

Now suppose that

$$X_1 \cup X_2 \cup \cdots \cup X_m = Y_1 \cup Y_2 \cup \cdots \cup Y_n.$$

Consider $X_m = X_m \cap Y_1 \cup X_m \cap Y_2 \cup \cdots \cup X_m \cap Y_n$. By irreducibility of X_m, there is an index j such that $X_m \subset Y_j$. Thus $m \leq n$ and for every i there is a j such that $X_i \subset Y_j$. By symmetry, for every j there is a k such that $Y_j \subset X_k$. In this case $X_i \subset X_k$ and so $i = k$, by assumption. Thus $X_i = Y_j$. $\square$

Proposition 9.14. *If $X \subset \mathbb{A}^n$ is an affine variety then the ring of regular functions is isomorphic to the coordinate ring.*

Proof. Let $\pi\colon K[X] \longrightarrow \mathcal{O}_X(X)$ be the map which sends a polynomial f to the obvious regular function ϕ, $\phi(x) = f(x)$. It is clear that π is a ring homomorphism, with kernel $I(X)$. It suffices, then, to prove that π is surjective.

Let ϕ be a regular function on X. By definition there is an open cover U_i of X and rational functions f_i/g_i such that ϕ is locally given by f_i/g_i. As X is Noetherian, we may assume that each U_i is irreducible. We may assume that $U_i = U_{h_i}$ for some regular function h_i, as such subsets form a base for the topology. Replacing f_i by $f_i h_i$ and g_i by $g_i h_i$ we may assume that f_i and g_i vanish outside of U_i. There are two cases; $U_i \cap U_j$ is non-empty or empty.

Suppose that $U_i \cap U_j$ is non-empty. As U_i is irreducible it follows that $U_i \cap U_j$ is a dense subset of U_i. Now $f_i/g_i = f_j/g_j$ as functions on $U_i \cap U_j$ and so $f_i g_j = f_j g_i$ as functions on $U_i \cap U_j$. As these functions are continuous, $f_i g_j = f_i g_j$ on U_i. Suppose that $U_i \cap U_j$ is empty. Then the identity $f_i g_j = f_j g_i$ holds on U_i as both sides are zero.

By assumption, the common zero locus of $\{g_i\}$ is empty. Thus, by the Nullstellensatz, there are polynomials $h_1, h_2, \dots, h_n$ such that

$$1 = \sum_i g_i h_i.$$

Set $f = \sum_i f_i h_i$. I claim that the function

$$x \longrightarrow f(x),$$

is the regular function ϕ. It is enough to check this on U_j, for every j. We have

$$\begin{aligned} f g_j &= \left(\sum_i f_i g_j\right) h_i \\ &= \sum_i (f_i g_j) h_i \\ &= \sum_i (f_j g_i) h_i \\ &= f_j \sum_i g_i h_i = f_j. \end{aligned}$$

□

Note that this result implies that the working definition of a morphism between affine varieties is correct. Indeed, simply projecting onto the jth factor, it is clear that if the map is given as

$$(x_1, x_2, \dots, x_m) \longrightarrow (f_1(x), f_2(x), \dots, f_n(x)),$$

then each $f_j(x)$ is a regular function. By (9.14), it follows that $f_j(x)$ is given by a polynomial.

Definition-Lemma 9.15. *Let X be an affine variety and let $p \in X$.*

Then the stalk of the structure sheaf of X at p, $\mathcal{O}_{X,p}$ is equal to the localisation of $A(X)$ at the maximal ideal m_p of $p \in X$.

Proof. There is an obvious ring homomorphism

$$A(X) \longrightarrow \mathcal{O}_{X,p},$$

which just sends a polynomial f to the equivalence class (f, X). Suppose that $f \notin m$. Then $p \in U_f \subset X$ and $(1/f, U_f)$ represents the inverse of (f, X) in the ring $\mathcal{O}_{X,p}$. By the universal property of the localisation there is a ring homomorphism

$$A(X)_m \longrightarrow \mathcal{O}_{X,p},$$

which is clearly injective. Now suppose that we have an element (σ, U) of $\mathcal{O}_{X,p}$. Since sets of the form U_f form a basis for the topology, we may assume that $U = U_g$. But then $\sigma = f/g^n \in A(X)_g \subset A(X)_m$, for some f and n. □

Lemma 9.16. *There is a contravariant functor A from the category of affine varieties over K to the category of commutative rings. Given an affine variety X we associate the ring $\mathcal{O}_X(X)$. Given a morphism $f\colon X \longrightarrow Y$ of affine varieties, $A(f)\colon \mathcal{O}_Y(Y) \longrightarrow \mathcal{O}_X(X)$, which sends a regular function ϕ to the regular function $A(f)(\phi) = \phi \circ f$.*

It is interesting to describe the image of this functor. Clearly the ring $A(X)$ is an algebra over K (which is to say that it contains K, so that we can multiply by elements of K). Further the ring $A(X)$ is a quotient of the polynomial ring, so that it is a finitely generated algebra over K. Also since the ideal $I(X)$ is radical, the ring $A(X)$ does not have any nilpotents.

Definition 9.17. *Let R be a ring. A non-zero element r of R is said to be* ***nilpotent*** *if there is a positive integer n such that $r^n = 0$.*

Clearly if a ring has a nilpotent element, then it is not an integral domain.

Theorem 9.18. *The functor A is an equivalence of categories between the category of affine varieties over K and the category of finitely generated algebras over K, without nilpotents.*

Proof. First we show that A is essentially surjective. Suppose we are given a finitely generated algebra A over K. Pick generators $\xi_1, \xi_2, \dots, \xi_n$ of A. Define a ring homomorphism

$$\pi \colon K[x_1, x_2, \dots, x_n] \longrightarrow A,$$

simply by sending x_i to ξ_i. It is easy to check that π is an algebra homomorphism. Let I be the kernel of π. Then I is radical, as A has no nilpotents. Let $X = V(I)$. Then the coordinate ring of X is isomorphic to A, by construction. Thus A is essentially surjective.

To prove the rest, it suffices to prove that if X and Y are two affine varieties then A defines a bijection between

$$\operatorname{Hom}(X, Y) \qquad \text{and} \qquad \operatorname{Hom}(\mathcal{O}_Y(Y), \mathcal{O}_X(X)).$$

To prove this, we may as well fix embeddings $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$. In this case A naturally defines a map between

$$\operatorname{Hom}(X, Y) \qquad \text{and} \qquad \operatorname{Hom}(A(Y), A(X)),$$

which we continue to refer to as A. It suffices to prove that there is a map

$$B \colon \operatorname{Hom}(A(Y), A(X)) \longrightarrow \operatorname{Hom}(X, Y),$$

which is inverse to the map

$$A \colon \operatorname{Hom}(X, Y) \longrightarrow \operatorname{Hom}(A(Y), A(X)).$$

Suppose we are given a ring homomorphism $\alpha \colon A(Y) \longrightarrow A(X)$. Define a map

$$B(\alpha) \colon X \longrightarrow Y,$$

as follows. Let $y_1, y_2, \dots, y_n$ be coordinates on $Y \subset \mathbb{A}^n$. Let $f_1, f_2, \dots, f_n$ be polynomials on $\mathbb{A}^n$, defined by $\alpha(y_i) = f_i$. Then define $B(\alpha)$ by the rule

$$(x_1, x_2, \dots, x_m) \longrightarrow (f_1, f_2, \dots, f_n).$$

Clearly this is a morphism. We check that the image lies in Y. Suppose that $p \in X$. We check that $q = (f_1(p), f_2(p), \dots, f_n(p)) \in Y$. Pick $g \in I(Y)$. Then

$$\begin{aligned} g(q) &= g(f_1(p), f_2(p), \dots f_n(p)) \\ &= g(\alpha(y_1)(p), \alpha(y_2)(p), \dots, \alpha(y_n)(p)) \\ &= \alpha(g)(p) \\ &= 0. \end{aligned}$$

Thus $q \in Y$ and we have defined the map B.

We now check that B is the inverse of A. Suppose that we are given a morphism $f \colon X \longrightarrow Y$. Let $\alpha = A(f)$. Suppose that f is given by $(f_1, f_2, \dots, f_n)$. Then $\alpha(y_i) = y_i \circ f = f_i$. It follows easily that $B(\alpha) = f$. Now suppose that $\alpha \colon A(Y) \longrightarrow A(X)$ is an algebra homomorphism. Then $B(\alpha)$ is given by $(f_1, f_2, \dots, f_n)$ where $f_i\alpha(y_i)$. In this case $A(f)(y_i) = f_i$. As $y_1, y_2, \dots, y_n$ are generators of $A(Y)$, we have $\alpha = A(B(\alpha))$. $\square$

(9.18) raises an interesting question. Can we enlarge the category of affine varieties so that we get every finitely generated algebra over K and not just those without nilpotents. In fact why stop there? Can we find a class of geometric objects, such that the space of functions on these objects, gives us any ring whatsoever (not nec. finitely generated, not nec. over K). Amazingly the answer is yes, but to do this we need the theory of schemes.