LECTURE 1. AFFINE VARIETIES AND THE HILBERT NULLSTELLENSATZ

Contents

This course is an introduction to algebraic geometry, a field that studies the solution sets of systems of algebraic equations. Our focus will be on the language of ***schemes***, a geometric framework developed by Alexander Grothendieck in the 1960s to generalize ***algebraic varieties***. The use of schemes provides a deeper understanding of various aspects of algebraic geometry, including degenerations, deformations, and rational points of varieties.

To provide more motivation for the introduction of schemes, we'll begin by exploring algebraic varieties in the sense of Serre (1955). We'll discuss the key problems that drive the field of algebraic geometry, which will be the focus of the first few lectures. In today's lecture, we'll take a first step by introducing affine varieties in an affine space over an algebraically closed field k, and establishing the classical variety-ideal correspondence.

1. The Zariski topology on the affine space

I will approach geometry from the Descartes perspective rather than synthetically, beginning with the introduction of a background space in which geometric objects exist.

1.1. Definition (Affine space)**.** The ***n-dimensional affine space*** over k is the set k^n of n-tuples $(a_1, \ldots, a_n)$ with $a_i \in k$. Following the newly established twentieth-century tradition, we use $\mathbb{A}^n_k$, or simply $\mathbb{A}^n$, to denote n-dimensional affine space over k.

Descartes also understood that geometric figures could be represented by equations, showing how algebra shapes geometry. This is evident in the study of lines and conics, which are well understood. In a similar vein, affine geometry explores figures defined by multiple equations with more variables, resulting in structures known as affine varieties.

1.2. Definition (Zariski closed subsets of $\mathbb{A}^n$)**.** Let S be a subset of the polynomial ring $k[T_1, \ldots, T_n]$. The set of common zeros of polynomials in S is denoted by

$$\boxed{V(S) \stackrel{\text{def}}{=\!=} \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}}.$$

A subset of $\mathbb{A}^n$ of the form $V(S)$ is called a ***Zariski closed subset***, or an ***algebraic subset***, or a ***closed subvariety*** of $\mathbb{A}^n$.

1.3. Easy properties. (1) If $S \subset S'$, then $V(S') \subset V(S)$.

(2) If $\mathfrak{a}$ is the ideal generated by S, then $V(\mathfrak{a}) = V(S)$.

(3) $V((1)) = \emptyset$ and $V((0)) = \mathbb{A}^n$.

(4) If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $k[T_1, \ldots, T_n]$, then $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

(5) Suppose $(\mathfrak{a}_i)_{i \in I}$ is a family of ideals of $k[T_1, \ldots, T_n]$, then $V\left(\sum_{i \in I} \mathfrak{a}_i\right) = \bigcap_{i \in I} V(\mathfrak{a}_i)$.

For example, let me verify (4). Clearly we have $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$, Item (1) implies that $V(\mathfrak{ab}) \supset V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a})$. Doing the same with $\mathfrak{a}$ replaced by $\mathfrak{b}$ shows that

$$V(\mathfrak{ab}) \supset V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

Now suppose $P \in V(\mathfrak{ab})$, but $P \notin V(\mathfrak{a})$, then we can find $f \in \mathfrak{a}$, $f(P) \neq 0$. For any $g \in \mathfrak{b}$, since $fg \in \mathfrak{ab}$, we have $(fg)(P) = 0$. Since $f(P) \neq 0$, we must have $g(P) = 0$. Thus $P \in V(\mathfrak{b})$.

1.4. Finiteness of defining equations. Recall that the Hilbert Basis Theorem (Atiyah and Macdonald 1969, Theorem 7.5) says that any ideal of $k[T_1, \ldots, T_n]$ is finitely generated. In view of the property (2) above, it follows that any $V(S)$ is the common zero locus of a finite set of polynomials.

1.5. Definition. The properties (3) – (5) show that the family $\{V(S)\}_{S\subset k[T_1,\dots,T_n]}$ determines a topology on $\mathbb{A}^n$, in which they are closed subsets. This topology is called the ***Zariski topology***.

1.6. Definition (Principal open subsets)**.** For $f \in k[T_1,\dots,T_n]$, define

$$\boxed{D(f) = \{P \in \mathbb{A}^n \mid f(P) \neq 0\}}.$$

Then $D(f)$ is a Zariski open subset of $\mathbb{A}^n$. Zariski open subsets of $\mathbb{A}^n$ of the form $D(f)$ are called ***principal open subsets***.

1.7. Lemma. *Any Zariski open subset of $\mathbb{A}^n$ is a finite union of principal open subsets. Consequently, principal open subsets form a basis for the Zariski topology of $\mathbb{A}^n$.*

Proof. Let $U = \mathbb{A}^n \setminus V(\mathfrak{a})$ be a Zariski open subset of $\mathbb{A}^n$, where $\mathfrak{a}$ is some ideal of $k[T_1,\dots,T_n]$. By the Hilbert basis theorem, $\mathfrak{a}$ is generated by finitely many polynomials $f_1,\dots,f_r$. Thus by Property (5) above, $V(\mathfrak{a}) = \bigcap_{i=1}^r V((f_i))$, and it follows that $U = \bigcup_{i=1}^r D(f_i)$ is a finite union of principal open subsets. ∎

[1] **1.8. Definition** (Affine varieties)**.** An ***affine algebraic variety*** (resp. a ***quasi-affine algebraic variety***) over k is a closed (resp. locally closed, i.e., open in its closure) subset of $\mathbb{A}^n$ for some n with respect to the Zariski topology.

Any ideal $\mathfrak{a}$ of $k[T_1,\dots,T_n]$ determines a Zariski closed subset of $\mathbb{A}^n$. But different ideals can define the same Zariski closed set. For example, $V(f) = V(f^2)$. To each Zariski closed subset V of $\mathbb{A}^n$ we can ***canonically*** attach to it an ideal of $k[T_1,\dots,T_n]$.

1.9. Definition (The ideal associated to an affine variety)**.** Let V be a Zariski closed subset of $\mathbb{A}^n$. We define

$$\boxed{I(V) \overset{\text{def}}{=\!=} \{f \in k[T_1,\dots,T_n] \mid f(P) = 0 \text{ for all } P \in V\}}.$$

Clearly, if $V = V(\mathfrak{a})$ for an ideal $\mathfrak{a}$, then $\mathfrak{a} \subset I(V(\mathfrak{a}))$. However, as we have seen, strict inclusion is possible. On the other hand, if V is Zariski closed in $\mathbb{A}^n$, then we have $V(I(V)) = V$. Thus $I(V)$ is among the ideals that cut out V. In particular, there are many ideals of $k[T_1,\dots,T_n]$ that can define the same affine variety.

1.10. Zariski topology is noetherian. The intimate connection between ideals and Zariski closed subsets reveals a peculiar feature of the Zariski topology. Since $k[T_1,\dots,T_n]$ is a noetherian ring, any increasing chain of ideals terminates. This property has a direct consequence for Zariski closed subsets of $\mathbb{A}^n$: any decreasing chain of such subsets also terminates. To see this, consider a decreasing chain $V_1 \supset V_2 \supset V_3 \supset \cdots$. Any polynomial f vanishing on V_i automatically vanishes on V_{i+1}, so we have an increasing chain of ideals:

$$I(V_1) \subset I(V_2) \subset \cdots$$

By the Hilbert basis theorem, this chain stabilizes, meaning that

$$I(V_N) = I(V_{N+1}) = \cdots$$

for some large N. Since $V(I(V)) = V$ for any Zariski closed subset, we conclude that $V_{N+1} = V_{N+2} = \cdots$.

In point-set topology, a topological space X is called a ***noetherian space*** if any decreasing chain of closed subsets $Z_1 \supset Z_2 \supset Z_3 \supset \cdots$ eventually stabilizes, meaning that there exists N sufficiently large such that $Z_N = Z_{N+1} = \cdots$. As we have seen, the Zariski topology on $\mathbb{A}^n$ satisfies this property, so $\mathbb{A}^n$ is a noetherian topological space.

[2] **1.11. Lemma.** *Let X be a noetherian topological space. Then X is quasi-compact.*

Proof. Let $X = \bigcup_{i\in I} U_i$ be an open covering. Choose a nonempty U_{i_0}. If $X = U_{i_0}$, we're done. Otherwise, we can find U_{i_1} such that $U_{i_0} \subsetneqq U_{i_1}$. Continuing this way, we either obtain $X = U_{i_0} \cup \cdots \cup U_{i_n}$, or a strictly decreasing chain of closed subsets

$$Z_0 \supsetneqq Z_1 \supsetneqq \cdots$$

where $Z_n = X \setminus \left(U_{i_0} \cup \cdots \cup U_{i_n}\right)$. The latter contradicts the noetherian hypothesis, so the former must occur. ∎

1.12. Lemma. *If X is a noetherian topological space, and Y is a subspace of X, then Y is a noetherian topological space. In particular, Y is quasi-compact.*

Proof. Any decreasing chain of closed subsets of Y is of the form $Z_0 \cap Y \supset Z_1 \cap Y \supset \cdots$, where Z_i are closed subsets of X. This induces a decreasing chain of closed subsets in X: $Z_0 \supset Z_0 \cap Z_1 \supset \cdots$. Since X is noetherian, this chain stabilizes: $Z_0 \cap \cdots \cap Z_N = Z_0 \cap \cdots \cap Z_{N+1} = \cdots$. Intersecting with Y shows that the original chain in Y also stabilizes. ∎

1.13. Corollary. *Any quasi-affine variety in $\mathbb{A}^n$ (equipped with the induced Zariski topology) is quasi-compact.*

1.14. Definition (Irreducible topological space)**.** Let X be a topological space. If X cannot be written as the set-theoretic union of two proper nonempty closed subspaces, then we say X is an ***irreducible*** topological space.

1.15. Remarks. (i) It is vacuously true that the empty set is ***not*** an irreducible topological space.

(ii) If an affine or quasi-affine variety V in $\mathbb{A}^n$ is irreducible as a topological space (with the induced Zariski topology), we shall say the V is an ***irreducible variety***.

1.16. Proposition. *Let X be a noetherian space. Then X can be written as a union $X = X_1 \cup \cdots \cup X_r$, where each X_i is an irreducible closed subspaces of X. If we require further that for each pair $1 \leqslant i, j \leqslant r$, $i \neq j$, $X_i \not\supset X_j$, then, up to permutation, X_i is uniquely determined.*

Proof. First, we prove the existence of a decomposition into irreducible spaces. If X is already irreducible, there is nothing to prove. If X is reducible, we can write $X = Y \cup Z$ for nonempty proper closed subspaces Y and Z. If Y or Z is reducible, we can further decompose them. This process must terminate because X is noetherian, proving the existence.

We can always express X as a finite union of irreducible closed subspaces, no one included in another, by removing any redundant components. Under this requirement, let us show that the decomposition is unique. Assume that X has two decompositions $X = X_1 \cup \cdots \cup X_r$ and $X = Y_1 \cup \cdots \cup Y_s$. Then $Y_1 = \bigcup_{j=1}^{r} (Y_1 \cap X_j)$. Since Y_1 is irreducible, either $Y_1 \cap X_j = Y_1$ or $Y_1 \cap X_j = \emptyset$. Thus, there exists i such that $Y_1 \subset X_i$. By permuting indices, we may assume $i = 1$. Reversing the roles of X_i's and Y_j's, we see $X_1 \subset Y_j$ for some j. Since $Y_1 \not\subset Y_j$ for $j \neq 1$ and $X_1 \not\subset X_j$ for $j \neq 1$, we have $X_1 = Y_1$. Continuing this way, we prove the uniqueness of the decomposition. ∎

We now explore an interesting connection between irreducibility, a topological concept, and algebra. Recall that an ideal $\mathfrak{p}$ of a commutative ring A is called a ***prime ideal*** if $fg \in \mathfrak{p}$ implies either $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$.

1.17. Proposition. *Let $V \subset \mathbb{A}^n$ be a Zariski closed subset. Then V is irreducible if and only if $I(V)$ is a prime ideal.*

Proof. Suppose first that V is reducible. Then we can write $V = V_1 \cup V_2$ for two distinct proper closed nonempty Zariski closed subsets of V. The fact that $V_1 \not\subset V_2$ implies the existence of $f \in I(V_2)$ that does not vanish on V_1. Similarly, we can find $g \in I(V_1)$ that does not vanish on V_2. Then fg vanishes on $V_1 \cup V_2$, but neither f nor g vanishes on V identically. This shows that $I(V)$ is not a prime ideal.

Conversely, if $I(V)$ is not a prime ideal, we can find $f, g \in k[T_1, \ldots, T_n]$ such that $fg \in I(V)$ but $f, g \notin I(V)$. Let $V_1 = V \cap \{f = 0\}$ and $V_2 = V \cap \{g = 0\}$. Then $V = V_1 \cup V_2$, as for any $P \in V$, either $f(P) = 0$ or $g(P) = 0$. The fact that f and g are not identically zero on V implies that $V_1 \neq V$ and $V_2 \neq V$, and neither V_1 nor V_2 is empty. This means that $V = V_1 \cup V_2$ is reducible. ∎

The results we proved above are all exercises in point-set topology. Notably, we never invoked the hypothesis that k is algebraically closed. This hypothesis will play a crucial role in the next few sections, but it was not necessary for the results we established above.

2. The Hilbert Nullstellensatz

We have seen in the previous section that different ideals can define the same variety. Hilbert's Nullstellensatz (Theorem 2.4 below) clarifies the relationship between an affine variety and its defining equations, assuming that k is algebraically closed. It states that the only reason why multiple ideals can define the same variety is simply because the polynomials $f, f^2, f^3, \ldots$ all share the same set of zeros. More formally, the Hilbert Nullstellensatz states that for two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $k[T_1, \ldots, T_n]$, $V(\mathfrak{a}) = V(\mathfrak{b})$ if and only if for any $f \in \mathfrak{a}$, there exists a natural number $r \geqslant 1$ such that $f^r \in \mathfrak{b}$.

2.1. Example (Nullstellensatz for $\mathbb{A}^1$)**.** Since $k[T]$ is a principal ideal domain, any ideal of $k[T]$ is of the form $(f(T))$ for some polynomial f, and the above assertion is particularly easy to verify. Indeed, if f and g have the same set of zeros, then we can write

$$f(T) = (T - x_1)^{e_1} \cdots (T - x_m)^{e_m},$$
$$g(T) = (T - x_1)^{d_1} \cdots (T - x_m)^{d_m}.$$

It is then clear that for any $h \in (f)$, a sufficiently high power of h falls in (g).

However, this explanation relies on the assumption that the field k is algebraically closed. For other fields, the link between "systems of equations" and "zero loci" can be more complicated. Take the polynomial $T^2 + 1$ over the real

numbers $\mathbb{R}$, for instance. This polynomial has no real roots, just like the constant polynomial 1. However, raising 1 to any power still gives 1, which is not the same as T^2+1.

In view of the discussion above, we introduce the following concept.

2.2. Definition (Radical of an ideal)**.** Let A be a commutative ring. Let $\mathfrak{a}$ be an ideal of A. Then the ***radical*** of $\mathfrak{a}$, denoted by $\sqrt{\mathfrak{a}}$, is

$$\boxed{\sqrt{\mathfrak{a}} \stackrel{\text{def}}{=\!=} \{f \in A \mid \text{there exists } m \geqslant 1,\ f^m \in \mathfrak{a}\}}.$$

The radical $\sqrt{(0)}$ of the zero ideal of A is called the ***nilradical*** of A. If $\mathfrak{a} = \sqrt{\mathfrak{a}}$, then we say $\mathfrak{a}$ is a ***radical ideal***.

2.3. Examples. (i) Let A be a commutative ring. We say A is a ***reduced ring*** if (0) is a radical ideal of A, or equivalently, if A has no nonzero nilpotent elements.

Thus, any integral domain is reduced. An ideal $\mathfrak{a}$ of A is radical if and only if $A/\mathfrak{a}$ is reduced. In particular, any prime ideal of A is radical, as is the unit ideal $(1) = A$.

(ii) If V is an affine variety in $\mathbb{A}^n$, then the ideal $I(V)$ is a radical ideal.

Using the concept of a radical ideal, the Hilbert Nullstellensatz can be stated as follows.

2.4. Theorem (Strong Nullstellensatz)**.** *Let k be an algebraically closed field. Let $\mathfrak{a}$ be an ideal of $k[T_1, \ldots, T_n]$. Then $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

I will prove Theorem 2.4 in §4.

2.5. Corollary. *The functions V and I below*

$$\left\{\begin{array}{c}\text{Radical ideals of} \\ k[T_1, \ldots, T_n]\end{array}\right\} \underset{I}{\overset{V}{\rightleftarrows}} \left\{\begin{array}{c}\text{Zariski closed} \\ \text{subsets of } \mathbb{A}^n\end{array}\right\}$$

are order reversing bijections.

Proof. We have shown that $V(I(V)) = V$ if V is a Zariski closed subset of $\mathbb{A}^n$. On the other hand, if $\mathfrak{a}$ is a radical ideal, then Nullstellensatz $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$. This completes the proof. ∎

Here is an equivalent form of Theorem 2.4 called weak Nullstellensatz.

2.6. Theorem (Weak Nullstellensatz)**.** *Let k be an algebraically closed field. Let $f_1, \ldots, f_r \in k[T_1, \ldots, T_n]$. If the system of polynomial equations*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \quad \vdots \\ f_r(x_1, \ldots, x_n) = 0 \end{cases}$$

has no solutions in $\mathbb{A}^n$, then there must exist $h_1, \ldots, h_r \in k[T_1, \ldots, T_n]$, such that

$$f_1 h_1 + \cdots + f_r h_r = 1.$$

Proof that Theorem 2.4 implies Theorem 2.6. Let $\mathfrak{a} = (f_1, \ldots, f_r)$. Then Theorem 2.6 amounts to saying that $1 \in \mathfrak{a}$. By the hypothesis $V(\mathfrak{a}) = \emptyset = V(1)$. By Theorem 2.4, some power of 1, namely 1 itself, must be in $\mathfrak{a}$, and we win. ∎

Proof that Theorem 2.6 implies Theorem 2.4. The argument described below, involving the introduction of a new
[3] variable T_0 and considering $T_0 f - 1$ instead of $f \neq 0$, is commonly known as the ***Rabinowitsch trick***.

Let $\mathfrak{a} = (f_1, \ldots, f_r)$ be an ideal in $k[T_1, \ldots, T_n]$, and assume $f \in I(V(\mathfrak{a}))$, meaning f vanishes on the variety $V(\mathfrak{a})$. Consider the polynomial $T_0 f - 1$ in the ring $k[T_0, T_1, \ldots, T_n]$. The system of equations

$$\begin{cases} f_1(x) = \cdots = f_r(x) = 0 \\ x_0 f(x) - 1 = 0 \end{cases}$$

has no solution in $\mathbb{A}^{n+1}$. According to Theorem 2.6, $f_1, \ldots, f_r, T_0 f - 1$ generate the unit ideal in $k[T_0, T_1, \ldots, T_n]$. Therefore, there exist polynomials $a_1(T_0, T), \ldots, a_{r+1}(T_0, T) \in k[T_0, T_1, \ldots, T_n]$ such that

$$a_1(T_0, T) f_1(T) + \cdots + a_r(T_0, T) f_r(T) + a_{r+1}(T_0, T)(T_0 f(T) - 1) = 1.$$

Now, by setting $T_0 = 1/f(T)$, we can clear the denominators and derive the desired result. ∎

Let us examine the weak Nullstellensatz in the special case when $n = 2$.

2.7. Example. Suppose we have two polynomials $f(T_1, T_2)$ and $g(T_1, T_2)$ without common zeros, and we want to show that f and g generate the unit ideal in $k[T_1, T_2]$. By applying a linear change of variables, we can express the polynomials as follows:

$$f(T_1, T_2) = a_d(T_2)T_1^d + a_{d-1}(T_2)T_1^{d-1} + \cdots + a_0(T_2),$$
$$g(T_1, T_2) = b_e(T_2)T_1^e + b_{e-1}(T_2)T_1^{e-1} + \cdots + b_0(T_2).$$

Viewing these polynomials as elements of $k(T_2)[T_1]$, we can find polynomials $p(T_1, T_2)$, $q(T_1, T_2)$, and $h(T_1, T_2)$ in $k(T_2)[T_1]$ such that

$$pf + qg = h.$$

By clearing the denominators, we can assume that p, q, and h are in $k[T_1, T_2]$. Since f and g have no common zeros in $\mathbb{A}^2$, it follows that h has no zeros in $\mathbb{A}^2$ either.

Specializing the variables and using the fact that k is algebraically closed, it is easy to see that the only polynomials in $k[T_1, T_2]$ without zeros in $\mathbb{A}^2$ are nonzero constant polynomials. This provides a direct proof of the weak Nullstellensatz in this simple case.

Finally, we can characterize maximal ideals of a polynomial ring.

2.8. Corollary. *If k is an algebraically closed field, then any maximal ideal of $k[T_1, \ldots, T_n]$ is of the form $(T_1 - a_1, \ldots, T_n - a_n)$ for some $(a_1, \ldots, a_n) \in \mathbb{A}^n$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of $k[T_1, \ldots, T_n]$. By Theorem 2.6, there exists a point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$, such that $f(P) = 0$ for any $f \in \mathfrak{m}$. In particular, $\mathfrak{m} \subset (T_1 - a_1, \ldots, T_n - a_n)$. We note that the latter ideal is the kernel of the surjective homomorphism

$$\mathrm{ev}_P : k[T_1, \ldots, T_n] \to k, \quad f \mapsto f(P).$$

Since $\mathfrak{m}$ is maximal, and $(T_1 - a_1, \ldots, T_n - a_n)$ is also maximal, we must have the equality. ∎

3. The coordinate ring of a variety

Let V be a Zariski closed subset of $\mathbb{A}^n$. Then each polynomial $f \in k[T_1, \ldots, T_n]$ defines a function from V into $\mathbb{A}^1$. Functions on V of this form are called ***regular functions***. Regular functions form a ring. Two polynomials define the same regular function on V if and only their difference lies in $I(V)$. Hence, the ring of all regular functions on V is naturally identified with the quotient ring $k[T_1, \ldots, T_n]/I(V)$. This leads to the following definition.

3.1. Definition (Coordinate ring)**.** Let V be a Zariski closed subset of $\mathbb{A}^n$. Then the k-algebra

$$\boxed{k[V] \stackrel{\text{def}}{=\!=} k[T_1, \ldots, T_n]/I(V)}$$

is called the ***coordinate ring*** of V.

Recall the following definition.

3.2. Definition (Finite type algebra)**.** Let A be a ring. Let B be an A-algebra. We say B is ***of finite type*** over A, or B is a ***finite type A-algebra***, if there exists $n \geqslant 0$, such that the polynomial ring $A[T_1, \ldots, T_n]$ has a surjective A-algebra homomorphism onto B.

Evidently, the coordinate ring $k[V]$ of an affine variety V is a reduced, finite type k-algebra. The goal of this section is to show that we can completely recover an affine variety V from the reduced, finite type k-algebra $k[V]$.

3.3. Reconstruction the set V from $k[V]$. Assume that V is a Zariski closed subset of $\mathbb{A}^n$. Then in view of Corollary 2.5, a point P of V are in one-to-one correspondence with maximal ideals $\mathfrak{m}$ of $k[T_1, \ldots, T_n]$ such that $I(V) \subset \mathfrak{m}$. By basic algebra, these maximal ideals are also in one-to-one correspondence with the set of all maximal ideals of $k[V]$. In other words, for any $P \in V$, the ideal

$$\boxed{\mathfrak{m}_P \stackrel{\text{def}}{=\!=} \{f \in k[V] : f(P) = 0\}}$$

is a maximal ideal of $k[V]$, and all maximal ideals of $k[V]$ are of this form.

This leads to the following definition.

3.4. Definition (Maximal spectrum)**.** Let A be a ring. Then the set of all maximal ideals of A is denoted by $\mathrm{Spm}\, A$, called the ***maximal spectrum*** of A.

The preceding discussion then implies the following.

3.5. Proposition. *Let k be an algebraically closed field. Let V be an affine variety over k. Then the map*

$$\rho_V \colon V \to \operatorname{Spm} k[V], \quad \rho_V(P) = \mathfrak{m}_P$$

is a bijection. ∎

3.6. Reconstruction of the Zariski topology of V from $k[V]$. Suppose $V \subset \mathbb{A}^n$ is a Zariski closed subset. Equip $\mathbb{A}^n$ with the Zariski topology. Then V inherits a subspace topology, which we refer to as the ***Zariski topology*** of V. We now explain how to reconstruct the Zariski topology of V using $k[V]$. To do so, it suffices to give a purely algebraic way of describing the Zariski closed subsets of V. By Corollary 2.5, these the Zariski closed subsets of V are in bijective correspondence with the set of radical ideals of $k[T_1, \ldots, T_n]$ containing $I(V)$. We have the following elementary lemma in algebra:

3.7. Lemma. *Let $\alpha \colon A \to B$ be a surjective homomorphism. Suppose A and B are reduced. Then an ideal $\mathfrak{b}$ of B is radical if and only if $\alpha^{-1}(\mathfrak{b})$ is a radical ideal of A.*

Proof. Suppose $\mathfrak{b}$ is radical. If $f^r \in \alpha^{-1}(\mathfrak{b})$, then $\alpha(f)^r \in \mathfrak{b}$, and thus $\alpha(f) \in \mathfrak{b}$. This implies that $f \in \alpha^{-1}(\mathfrak{b})$, proving $\alpha^{-1}(\mathfrak{b})$ is radical.

Conversely, if $\alpha^{-1}(\mathfrak{b})$ is radical. Suppose $g^r \in \mathfrak{b}$. We can choose $f \in A$ such that $\alpha(f) = g$. Since $\alpha(f)^r \in \mathfrak{b}$, we have $f^r \in \alpha^{-1}(\mathfrak{b})$, thus $f \in \alpha^{-1}(\mathfrak{b})$. Hence $\alpha(f) \in \mathfrak{b}$. ∎

By the lemma, the ordered set of radical ideals of $k[T_1, \ldots, T_n]$ containing $I(V)$ correspond precisely to the ordered set of radical ideals of $k[V]$. Therefore, we get an order reversing bijective correspondence

(∗)
$$\left\{\begin{array}{c}\text{Radical ideals} \\ \text{of } k[V]\end{array}\right\} \underset{I}{\overset{V}{\rightleftarrows}} \left\{\begin{array}{c}\text{Zariski closed} \\ \text{subsets of } V\end{array}\right\}$$

where:

- for an ideal $\mathfrak{a}$ of $k[V]$, $V(\mathfrak{a}) = \{P \in V \mid f(P) = 0 \text{ for any } f \in \mathfrak{a}\}$, and
- for a Zariski closed subset W of V, $I(W) = \{f \in k[V] \mid f(Q) = 0 \text{ for any } Q \in W\}$.

This is analogous to Corollary 2.5, except the role of $\mathbb{A}^n$, resp. $k[T_1, \ldots, T_n]$ is subsumed by V, resp. $k[V]$. With the preceding discussions, the following theorem follows easily.

3.8. Theorem. *Let V be an affine variety with coordinate ring $k[V]$. For a Zariski closed subset W, let $I(W) = \{f \in k[V] \mid f(Q) = 0 \text{ for any } Q \in W\}$. Then*

- *For any ideal $\mathfrak{a}$ of $k[V]$, we have $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*
- *If $V(\mathfrak{a}) = \emptyset$, then $\mathfrak{a} = (1)$.*
- *Points of V are in bijective correspondence with the set of maximal ideals of $k[V]$.* ∎

Using Proposition 3.5 and the correspondence (∗), we can transport the Zariski topology of V to a topology on $\operatorname{Spm} k[V]$. Since the maximal spectrum is well-defined for any ring, we have a construction that extracts to a topological space from a ring.

3.9. Definition (Zariski topology on $\operatorname{Spm} A$)**.** Let A be a ring. Then a ***Zariski closed subset*** of $\operatorname{Spm} A$ is a set of the form

$$V(\mathfrak{a}) = \{\mathfrak{m} \in \operatorname{Spm} A \mid \mathfrak{a} \subset \mathfrak{m}\}.$$

One checks that

- $V((0)) = \operatorname{Spm} A$, $V((1)) = \emptyset$,
- if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of A, then $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$,
- if $(\mathfrak{a}_i)_{i \in I}$ is a collection of ideals, then $V(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} V(\mathfrak{a}_i)$.

Thus Zariski closed subsets of $\operatorname{Spm} A$ determine a topology in which they are closed sets. This topology is called the ***Zariski topology*** of $\operatorname{Spm} A$.

3.10. Proposition. *Let k be an algebraically closed field. Let V be an affine variety over k, equipped with the Zariski topology. Equip $\operatorname{Spm} k[V]$ also with its Zariski topology. Then the map $\rho_V \colon V \to \operatorname{Spm} k[V]$ described in Proposition 3.5 is a homeomorphism.* ∎

3.11. Remark. Let k be an algebraically closed field. Suppose A and B are finite type k-algebras, and $\alpha\colon A \to B$ is a ring homomorphism. Then for any maximal ideal $\mathfrak{m}$ of B, the inverse image $\mathfrak{n} = \alpha^{-1}(\mathfrak{m})$ is a prime ideal of A. It is in fact a maximal ideal as well, because the map $A/\mathfrak{n} \to B/\mathfrak{m} \simeq k$ is an injective map, and both spaces are k-vector spaces. This forces $A/\mathfrak{n}$ to be isomorphic to k as well. This argument also carries to non-algebraically closed field, but we will need Zariski's version of Nullstellensatz (Theorem 4.1 below) to see it.

Finally, to show *an affine variety is completely determined by its coordinate ring*, we shall need a category in which affine varieties are objects.

3.12. Definition (Morphism of affine varieties, provisional version)**.** Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be Zariski closed subsets. A map $\varphi\colon V \to W$ is called a ***morphism***, if there exist polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that [4]

$$\varphi(P) = (f_1(P), \ldots, f_m(P)) \quad \text{for all } P \in V.$$

Thus, affine varieties over k and morphisms between them form a category. The set of morphisms from an affine variety V to another affine variety W is denoted by $\mathrm{Mor}(V, W)$.

Now that we have the notion of morphisms, the assignment $V \mapsto k[V]$ determines a contravariant functor from the category of affine varieties to the category of k-algebras. For a variety V, $k[V]$ can be identified with the set of all morphisms from V to $\mathbb{A}^1$, and its k-algebra structure is the same as the multiplication and addition of these functions. If $\varphi\colon V \to W$ is a morphism of affine varieties, it induces a map

$$\varphi^{\#}\colon k[W] \to k[V], \quad g \mapsto g \circ \varphi.$$

This induced map $\varphi^{\#}$ is, naturally, a ring homomorphism.

As a consequence of the Nullstellensatz, We can now establish the following theorem linking algebra and geometry over an algebraically closed field.

3.13. Theorem. *Let k be an algebraically closed field. The functor $V \mapsto k[V]$ is a contravariant equivalence from the category of affine varieties to the category of reduced, finite type k-algebras. In other words, the following are true:*

(1) *For any reduced, finite type k-algebra A, there exists an affine variety V such that $k[V] \simeq A$.*
(2) *Let V and W be two affine varieties, then*

$$\varphi \mapsto \varphi^{\#}\colon \mathrm{Mor}(V, W) \to \mathrm{Hom}_k(k[W], k[V]).$$

is bijective.

Proof. Since A is of finite type, there is a surjective homomorphism

$$\alpha\colon k[T_1, \ldots, T_n] \to A.$$

Let $\mathfrak{a}$ be the kernel of α. Since A is reduced, $\mathfrak{a}$ is a radical ideal. By Theorem 2.4, $\mathfrak{a} = I(V(\mathfrak{a}))$. Therefore $A \simeq k[V(\mathfrak{a})]$. This proves (1).

For the injectivity in (2), we use the following remark: if $\varphi\colon V \to W$ is a morphism, then the following diagram is commutative

$$\begin{array}{ccc} V & \xrightarrow{\quad\varphi\quad} & W \\ \downarrow{\scriptstyle \rho_V} & & \downarrow{\scriptstyle \rho_W} \\ \operatorname{Spm} k[V] & \xrightarrow{\mathfrak{m} \mapsto (\varphi^{\#})^{-1}\mathfrak{m}} & \operatorname{Spm} k[W]. \end{array}$$

Here, ρ_V and ρ_W are described in Proposition 3.5. The verification is rather routine and is left to the reader. From the commutativity we see that for any $\varphi, \psi \in \mathrm{Mor}(V, W)$, $\varphi^{\#} = \psi^{\#}$ implies $\varphi = \psi$.

Finally we shall show $\varphi \mapsto \varphi^{\#}$ is surjective. Since V and W are affine varieties, there exist surjective homomorphisms $k[T_1, \ldots, T_n] \to V$ and $k[T'_1, \ldots, T'_m] \to W$ for some n and m. By the universal property of the polynomial algebra, any solid diagram below can be completed by a dotted arrow making the diagram commutative:

$$\begin{array}{ccc} k[T'_1, \ldots, T'_m] & \overset{\alpha}{\dashrightarrow} & k[T_1, \ldots, T_n] \\ \downarrow & & \downarrow \\ k[W] & \xrightarrow{\quad\beta\quad} & k[V] \end{array}$$

Let $f_j = \alpha(T'_j)$. Then $\varphi = (f_1, \ldots, f_m)$ defines a morphism from V to W that induces the given homomorphism β. ∎

4. Proof of the Nullstellensatz

Proof of Theorem 2.6. Let $\mathfrak{a}$ be any ideal of $k[x_1, \ldots, x_n]$. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{a}$. To show $V(\mathfrak{a})$ is nonempty, it suffices to show that $V(\mathfrak{m})$ is nonempty. Consider the field $K = k[x_1, \ldots, x_n]/\mathfrak{m}$ and the following composition

$$k \hookrightarrow k[T_1, \ldots, T_n] \twoheadrightarrow K.$$
$$\iota$$

It suffices to show this composed map ι is an isomorphism. Indeed, once proving that ι is an isomorphism of fields, the image a_i of T_i can be identified with some number in k, and any element f in $\mathfrak{m}$ will satisfy $f(a_1, \ldots, a_n) = 0$, and $(a_1, \ldots, a_n)$ will be an element of $V(\mathfrak{m})$. Since K is by definition finite type over k, and since k is algebraically closed, Theorem 4.1 below then implies ι is indeed an isomorphism. ∎

4.1. Theorem (Zariski's Nullstellensatz)**.** *Let k be a field. Let K be a finite type k-algebra that is also a field. Then is K is a finite extension of k.*

The proof of Theorem 4.1 will exploit the notion of integral dependence in commutative algebra.

4.2. Definition (Integral dependence)**.** Let A be a subring of B. An element b of B is said to be ***integral*** over A if there is a monic polynomial f in $A[T]$ such that $f(b) = 0$.

For the proof of Theorem 4.1, we only need a half of the following simple lemma.

4.3. Lemma. *Let B be an integral domain, A a subring of B. Suppose that B is integral over A. Then A is a field if and only if B is a field.*

Proof. Suppose A is a field. Let $b \in B$, but $b \notin A$. Let us show that b^{-1} exists in B. Since B is integral over A, b satisfies a relation

$$b^e + a_{e-1}b^{e-1} + \cdots + a_0 = 0$$

where $a_i \in A$, $a_0 \neq 0$. Thus

$$b \cdot \left[-a_0^{-1}\left(a_{e-1}b^{e-1} + \cdots + a_1\right)\right] = 1$$

and b is invertible.

Conversely, suppose B is a field. Then for each $a \in A$, its inverse a^{-1} is in B. Since B is integral over A, a^{-1} satisfies an integral relation

$$a^{-d} + a_{d-1}a^{-(d-1)} + \cdots + a_0 = 0.$$

Multiply both sides by a^{d-1} yields

$$a^{-1} = -[a_{d-1} + a_{d-2}a + \cdots + a_0 a^{d-1}] \in A.$$

This completes the proof. ∎

[5] **Proof of Theorem 4.1.** We prove by induction on the number of elements generating K as a k-algebra. The base case is $K = k(x)$. If x is algebraic over k, then there is nothing to prove. If x is transcendental, $k(x)$ won't be of finite type. This handles the base case.

Consider the general case. Let us assume that $x, x_1, \ldots, x_n$ are generators of K as a finite type k-algebra. If all these elements are algebraic over k, then there is nothing to prove. Otherwise, let us assume x is transcendental over k, and we will derive a contradiction.

Since K is a field containing $k(x)$, and since K is finite type over k, it is also of finite type over the rational function field $k(x)$. Note that although $k(x)$ is not of finite type over k while K is, so far we have not obtained a contradiction since a finite type k-algebra may have a non-finite type k-subalgebra.

At any event, K is generated, as a $k(x)$-algebra, by $x_1, \ldots, x_n$. By the inductive hypothesis, applied now with base field $k(x)$, we know $x_1, \ldots, x_n$ are algebraic over $k(x)$. Therefore, there exist $f_i(T) \in k(x)[T]$, such that $f_i(x_i) = 0$. By clearing the denominators, we may assume $f_i(T) \in k[x, T]$. Thus we can write

$$f_i(T) = a_0^{(i)}(x) + a_1^{(i)}(x)T + \cdots + a_{d_i}^{(i)}(x)T^{d_i}, \quad a_j^{(i)}(x) \in k[x]$$

Define $g(x) = \prod_{i=1}^n a_{d_i}^{(i)}(x)$, and set $A = k[x][g^{-1}]$. Then through $f_i(x_i) = 0$ we find $x_1, \ldots, x_n$ are integral over A. In other words, K is integral over A. By Lemma 4.3 below, we see A is a field as well. This is absurd, since there are infinitely many irreducible polynomials in $k[x]$. ∎

To give yet another formulation of the Nullstellensatz, let us recall the following lemma, known as the "dumb Nullstellensatz".

4.4. Lemma (Scheinnullstellensatz)**.** *Let A be a commutative ring. Let $\mathfrak{a}$ be an ideal of A. Then*

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \text{ prime ideal} \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p}.$$

Proof. This follows from Atiyah and Macdonald 1969, Proposition 1.8. ∎

4.5. Definition (Jacobson ring)**.** A ring A is a ***Jacobson ring***, if for any ideal $\mathfrak{a}$ of A, we have

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{m} \text{ maximal ideal} \\ \mathfrak{a} \subset \mathfrak{m}}} \mathfrak{m}.$$

4.6. Theorem (Hilbert Nullstellensatz)**.** *Let k be a field (not assumed to be algebraically closed). Let A be a finite type k-algebra. Then A is a Jacobson ring.*

Proof. It suffices to show that for any finite type k-algebra A, the nilradical of A equals the Jacobson radical of A. It is clear the Jacobson radical contains the nilradical, since maximal ideals are prime. To complete the proof, we shall prove the following. Let $a \in A$, such that a is not nilpotent, then a is not in the Jacobson radical.

Consider the A-algebra $A[a^{-1}]$. Since a is not nilpotent, $A[a^{-1}]$ is nonzero, hence must contain some maximal ideal $\mathfrak{m}$. Let $\mathfrak{n}$ be the inverse image of $\mathfrak{m}$ under the map $A \to A[a^{-1}]$. Then we know $a \notin \mathfrak{n}$. It suffices to show $\mathfrak{n}$ is a maximal ideal.

We have following commutative diagram

$$\begin{array}{ccccc} k & \hookrightarrow & A & \longrightarrow & A[a^{-1}] \\ & \searrow & \downarrow & & \downarrow \\ & & A/\mathfrak{n} & \longrightarrow & A[a^{-1}]/\mathfrak{m} \end{array} .$$

By Theorem 4.1, $A[a^{-1}]/\mathfrak{m}$ is a finite extension of k. Since $\mathfrak{n}$ is always a prime ideal, $A/\mathfrak{n}$ is an integral domain that is also a finite dimension k-algebra. This forces $A/\mathfrak{n}$ to be a field, i.e., $\mathfrak{n}$ is a maximal ideal. ∎

Notes

1. Many authors, such as Mumford 1988 and Hartshorne 1977, define affine varieties as irreducible (Definition 1.14) Zariski closed subsets of $\mathbb{A}^n$. They call Zariski closed subsets "algebraic sets". We (following Serre 1955) shall not adopt their practice.

2. Following Bourbaki, a topological space is ***quasi-compact*** if any of its open covering admits a finite subcovering. A ***compact*** topological space is a quasi-compact topological space which is also separated (in the sense that the Hausdorff axiom T2 holds). At least in algebraic geometry, this choice of terminology is not bad, because it reminds us that quasi-compactness of Zariski topology is quite different from the compactness of, say spheres, that we built our intuition on. The proper analogue of compactness in algebraic geometry is the ***properness***, which we will introduce later.

3. Rabinowitsch's paper titled *Zum Hilbertschen Nullstellensatz* was published in Math. Ann. in 1929. The identity of J. L. Rabinowitsch has sparked considerable discussion on the MathOverflow thread #416577. The condensed version is as follows: According to Bruce Palka's *Editor's Endnotes* in the American Mathematical Monthly 111, No. 5 (May, 2004), p. 460, this Rabinowitsch is in fact G. Y. Rainich, who changed his surname from "Rabinovich" upon immigrating to the United States. However, this claim has been refuted as an embellished version of a different anecdote about Rainich. Ultimately, consensus seems to be that Rabinowitsch is not Rainich but rather a Russian mathematician who had some interaction with E. Noether in the 1920s. He is known for translating Courant's *Differential and Integral Calculus* into Russian, and was remembered as an exceptional lecturer.

4. It's worth noting that the definition of morphisms of affine varieties in Definition 3.12 is quite simplistic. To draw a comparison, consider the concept of differentiable maps between closed submanifolds of Euclidean spaces. There are two approaches to defining such maps.

- The first is the "global" approach: a differentiable map from $M \subset \mathbb{R}^n$ to $N \subset \mathbb{R}^m$ is simply a differentiable map from $\mathbb{R}^n$ to $\mathbb{R}^m$ that maps M into N. This direct definition aligns with our approach for defining morphisms of affine varieties.
- There's also a "local" definition, which turns out to be equivalent: a differentiable map φ from M to N is a map such that for each point $P \in M$, there exists a neighborhood U of P in $\mathbb{R}^n$ and a differentiable map $\widetilde{\varphi}\colon U \to \mathbb{R}^m$ such that φ restricted to $U \cap M$ equals $\widetilde{\varphi}$ restricted to $U \cap M$. This local definition is typically favored by

those familiar with differentiable manifolds. The equivalence between the two definitions is established using the partition of unity technique.

Similarly, we can adopt a more local definition of morphisms of affine varieties, which will be more suitable for broader contexts and deeper discussions. We will revisit this point in Lecture 2.

5. The proof of Theorem 4.1 we presented is unclear in its origin. Fulton uses this proof in his book *Algebraic curves*, §1.10. In contrast, the more common proof relies on Emmy Noether's normalization lemma (cf. Atiyah and Macdonald 1969, Chapter 5, Exercise 16). This lemma implies that if K is a finite type k-algebra and a field, then it is integral over $k[T_1, \ldots, T_n]$, which by Lemma 4.3 must be a field, forcing $n = 0$ and making K a finite extension of k. Fulton's proof avoids Noether normalization altogether.

References

Atiyah, M. F. and I. G. Macdonald (1969), *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., pp. ix+128 (cit. on pp. 1, 9, 10).

Fulton, William (1989), *Algebraic curves*, Advanced Book Classics, An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, pp. xxii+226 (cit. on p. 10).

Hartshorne, Robin (1977), *Algebraic geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, pp. xvi+496 (cit. on p. 9).

Mumford, David (1988), *The red book of varieties and schemes*, vol. 1358, Lecture Notes in Mathematics, Springer-Verlag, Berlin, pp. vi+309 (cit. on p. 9).

Serre, Jean-Pierre (1955), *Faisceaux algébriques cohérents*, Ann. of Math. (2), vol. 61, pp. 197–278 (cit. on pp. 1, 9).

E-mail address: zhangdingxin13@gmail.com