Algebraic geometry (Notes)

Anand Deopurkar

August 4, 2021

1 Affine algebraic sets

1.1 Affine space WEEK1:DONE

The objects of study in algebraic geometry are called algebraic varieties. The building blocks for general algebraic varieties are certain subsets of the affine space. Let us first recall affine space.

Let k be a field and let n be a non-negative integer. The *affine n-space over k*, denoted by $\mathbb{A}_k^n$ is the set of n-tuples $a_1, \dots, a_n$ whose entries a_i lie in k. Thus, $\mathbb{A}_k^n$ is nothing but the product k^n. The product k^n has quite a bit of extra structure—it is a k-vector space, for example—but we wish to forget it. That is the reason for choosing different notation. In particular, the zero tuple does not play a distinguished role.

1.2 Affine algebraic set WEEK1:DONE

Let $k[x_1, \dots, x_n]$ denote the ring of polynomials in variables $x_1, \dots, x_n$ and coefficients in k. An *affine algebraic subset* of the affine space $\mathbb{A}_k^n$ is the common zero locus of a set of polynomials. More precisely, a set $S \subset \mathbb{A}_k^n$ is an affine algebraic subset if there exists a set of polysomials $A \subset k[x_1, \dots, x_n]$ such that

$$S = \{a \in \mathbb{A}_k^n \mid f(a) = 0 \text{ for all } f \in A\}.$$

1.2.1 Definition (Vanishing locus) Given $A \subset k[x_1, \dots, x_n]$, the *vanishing locus of* A, denoted by $V(A)$ is the set

$$V(A) = \{a \in \mathbb{A}_k^n \mid f(a) = 0 \text{ for all } f \in A\}.$$

— Thus the affine algebraic sets are precisely the sets of the form $V(A)$ for some A.

1.2.2 Examples/non-examples

The following are affine algebraic sets

1. The empty set
2. Entire affine space
3. Single point

Proof. Done in class. □

The following are not affine algebraic sets

1. The unit cube in $\mathbb{A}^n_{\mathbb{R}}$
2. Points with rational coordinates in $\mathbb{A}^n_{\mathbb{C}}$

Proof. DIY. □

1.3 Ideals

WEEK1:DONE

Let R be a ring. Recall that a subset $I \subset R$ is an *ideal* if it is closed under addition and multiplication by elements of R. Given any subset $A \subset R$ the *ideal generated by* A, denoted by $\langle A \rangle$ is the smallest ideal containing A. This ideal consists of all elements r of R that can be written as a linear combination

$$r = a_1 r_1 + \cdots + a_m r_m,$$

where $a_i \in A$ and $r_i \in R$.

1.3.1 Proposition

Let $A \subset k[x_1, \ldots, x_n]$. Then we have $V(A) = V(\langle A \rangle)$.

Proof. Done in class. □

1.4 Noetherian rings and the Hilbert basis theorem

WEEK1:DONE

In our definition of $V(A)$, the subset A may be infinite. But it turns out that we can replace it by a finite one without changing $V(A)$. This is a consequence of the Hilbert basis theorem, which, in turn, has to do with a fundamental property of rings.

We begin with a simple observation.

1.4.1 Proposition Let R be a ring. The following are equivalent

1. Every ideal of R is finitely generated.
2. Every infinite chain of ideals
$$I_1 \subset I_2 \subset I_3 \subset \cdots$$
stabilises.

Proof. — 1

1.4.2 Definition (Noetherian ring) A ring R satisfying the equivalent conditions of Proposition 1.4.1 is called *Noetherian*.

1.4.3 Examples/non-examples The following rings are Noetherian

1. $R = \mathbb{Z}$
2. R a field.

Proof. All ideals here can be generated by 1 element. □

The ring of continuous functions on the interval is *not* Noetherian. #+begin$_{\text{proof}}$. Let I_n be the set of functions on $[0,1]$ that vanish on $[0,1/n]$. This forms an increasing chain of ideals that does not stabilise. #+end$_{\text{proof}}$

1.4.4 Proposition (Quotients of Noetherian rings) If R is Noetherian and $I \subset R$ is any ideal, then R/I is Noetherian.

Proof. — 2

1.4.5 Theorem If R is Noetherian, then so is $R[x]$

- Proof Assume R is Noetherian, and let $I \subset R[x]$ be an ideal. We must show that I is finitely generated. The basic idea is to use the division algorithm, while keeping track of the ideals formed by the leading coefficients.

  For every non-negative integer m, define
$$J_m = \{\text{Leading coeff}(f) \mid f \in I, f \neq 0, \quad \deg(f) \leq m\} \cup \{0\}$$
  We make the following claims.

  1. J_m is an ideal of R.
  2. $J_m \subset J_{m+1}$.

DIY.

Since R is Noetherian, the chain $J_1 \subset J_2 \subset \cdots$ stabilises; say $J_m = J_{m+1} = \cdots$. Let S_i be a finite set of generators for J_i, and for $a \in S_i$, let $p_a \in I$ be a non-zero element of degree at most i whose leading coefficient is a. We claim that the (finite) set $\{p_a \mid a \in S_1 \cup \cdots \cup S_m\}$ generates I.

Proof. Let $G = \{p_a \mid a \in S_1 \cup \cdots \cup S_m\}$. By construction, this is a subset of I, so the ideal it generates is contained in I. We remains to prove that every $f \in I$ is a linear combination of elements of G. It will be convenient to set $S_n = S_m$ for all $n \geq m$.

We induct on the degree of f (leaving the base case to you). Suppose the degree of f is n and the statement is true for elements of degree less than n. By construction, the leading coefficient of f is an R-linear combination of elements of S_n, say

$$\mathrm{LC}(f) = \sum c_i s_i.$$

Let n_i be the degree of p_{s_i}; then by construction $n_i \leq n$. Consider the linear combination $g = \sum c_i p_{s_i} x^{n-n_i}$. See that g lies in I, has degree n, the same leading coefficient as f, and is an $R[x]$-linear combination of elements of G. So $f - g \in I$ has lower degree. By inductive hypothesis, $f - g$ is an $R[x]$-linear combination of elements of G, and hence so is f. $\square$

1.4.6 Corollary (Hilbert basis theorem) $k[x_1, \ldots, x_n]$ is Noetherian.

Proof. Induct on n. $\square$

1.4.7 Corollary Every affine algebraic subset of $\mathbb{A}^n_k$ is the vanishing set of a finite set of polynomials.

Proof. Done in class. $\square$

1.5 The Zariski topology

WEEK2

The notion of affine algebraic sets allows us to define a topology on $\mathbb{A}^n_k$. Recall that we can specify a topology on a set by specifying what the open subsets are, or equivalently, what the closed subsets are. In our case, it is more convenient to do the latter. The collection of closed subsets must satisfy the following properties.

1. The empty set and the entire set are closed.
2. Arbitrary intersections of closed sets are closed.
3. Finite unions of closed sets are closed.

   We define the *Zariski topology* on $\mathbb{A}^n_k$ by setting the closed subsets to be the affine algebraic sets, namely, the sets of the form $V(A)$ for some $A \subset k[x_1, \ldots, x_n]$.

1.5.1 Proposition The collection of affine algebraic subsets satisfies the three conditions above.

Proof. — (1)

1.5.2 Proposition The Zariski topology on $\mathbb{A}^1_k$ is the *finite complement topology.* The only closed sets are the finite sets (or the whole space). In other words, the only open sets are the complements of finite sets (or the empty set).

Proof. We saw that the subsets $V(A) \subset \mathbb{A}^1_k$ are either the whole $\mathbb{A}^1_k$ or finite sets. $\square$

1.5.3 Comparison between Zariski and Euclidean topology over $\mathbb{C}$. Every Zariski closed (open) subset of $\mathbb{A}^n_{\mathbb{C}}$ is also closed (open) in the usual Euclidean topology. The converse is not true.

Proof. It suffices to prove that $V(A)$ is closed in the usual topology. We have $V(A) = \cap_{f \in A} V(f)$, so it suffices to show that $V(f)$ is closed. But $V(f) = f^{-1}(0)$ is closed, because it is the pre-image of a closed set under a continuous function. $\square$

1.5.4 Proposition (Polynomials are continuous) Let f be a polynomial function on $\mathbb{A}^n_k$, viewed as a map $f\colon \mathbb{A}^n_k \to \mathbb{A}^1_k$. Then f is continuous in the Zariski topology.

Proof. We check that pre-images of closed sets are closed. The only closed sets of $\mathbb{A}^1_k$ is the whole space and finite sets. The pre-image of $\mathbb{A}^1_k$ is $\mathbb{A}^n_k$, which is closed. Since finite unions of closed sets are closed, it suffices to check that the pre-image of a point $a \in \mathbb{A}^1_k$ is closed. But the pre-image of a under f is just $V(f - a)$, which is closed by definition. $\square$

— The Zariski topology has very few open sets, and as a result has terrible separation properties. It is not even Hausdorff (except in very small examples). Nevertheless, we will see that it is extremely useful. For one, it makes sense over every field!

1.6 The Nullstellensatz WEEK2

We associated a set $V(A)$ to a subset A of the polynomial ring $k[x_1, \ldots, x_n]$. If we think of A as a system of equations $\{f = 0 \mid f \in A\}$, then $V(A)$ is the set of solutions. We can also define a reverse operation. The Nullstellensatz says that if k is algebraically closed, then these two operations are mutually inverse. That is, the data of a system of equations is equivalent to the data of its set of solutions. This pleasant fact allows us go back and forth between algebra (equations) and geometry (the solution set).

We start with a straightforward definition.

1.6.1 Definition (Ideal vanishing on a set) Let $S \subset \mathbb{A}^n_k$ be a set. The *ideal vanishing on* S, denoted by $I(S)$, is the set

$$I(S) = \{f \in k[x_1, \dots, x_n] \mid f(a) = 0 \text{ for all } a \in S\}$$

— Recall that an ideal $I \subset k[x_1, \dots, x_n]$ is *radical* if it has the property that whenever $f^n \in I$ for some $n > 1$, then $f \in I$.

1.6.2 Proposition The set $I(S)$ is a radical ideal of $k[x_1, \dots, x_n]$.

Proof. We leave it to you to check that $I(S)$ is an ideal. To see that it is radical, see that if f^n vanishes on S, then so does f. □

1.6.3 Proposition (Easy properties of radical ideals)

1. $I \subset R$ is radical if and only if R/I has no (non-zero) nilpotents.

2. All prime ideals are radical. In particular, all maximal ideals are radical.

Proof. Consider $f \in R$ and its image $\overline{f} \in R/I$. Then $\overline{f}$ is a nilpotent of R/I if and only if $f^n \in I$ and $\overline{f} = 0$ in R/I if and only if $f \in I$. From this, the result follows. If I is prime, then R/I is an integral domain, so it has no nilpotents (it does not even have zero divisors). □

1.6.4 Proposition (Radical of an ideal) Let I be an ideal, and set $\sqrt{I} = \{f \mid f^n \in I \text{ for some } n > 0\}$. Then $\sqrt{I}$ is a radical ideal.

Proof. — (2)

1.6.5 Definition (Radical of an ideal) The ideal $\sqrt{I}$ is called the radical of I.

1.6.6 Proposition (V is unchanged by radicals) We have $V(I) = V(\sqrt{I})$.

Proof. — (3)

— We now state a string of important theorems, all called the "Nullstellensatz", starting with the most comprehensive one.

1.6.7 Theorem Let k be an algebraically closed field. Then we have a bijection

$$\text{Radical ideals of } k[x_1, \dots, x_n] \leftrightarrow \text{Zariski closed subsets of } \mathbb{A}^n_k$$

where the map from the left to the right is $I \mapsto V(I)$ and the map from the right to the left is $S \mapsto I(S)$. The correspondence is inclusion reversing.

1.6.8 Theorem Let k be an algebraically closed field and $I \subset k[x_1, \dots, x_n]$ an ideal. If $V(I) = \emptyset$, then $I = (1)$.

1.6.9 Theorem Let k be an algebraically closed field. Then all the maximal ideals of $k[x_1, \dots, x_n]$ are of the form $\langle x_1 - a_1, \dots, x_2 - a_n \rangle$ for some $(a_1, \dots, a_n) \in \mathbb{A}^n_k$.

— Theorem 1.6.8 says that we have a dichotomy: either a system of equations $f_i = 0$ has a solution, or there exist polynomials g_i such that

$$\sum f_i g_i = 1.$$

1.6.10 Theorem Let k be an algebraically closed field and $I \subset k[x_1, \dots, x_n]$ an ideal. If f is identically zero on $V(I)$, then $f^n \in I$ for some n.

1.7 Proof of the Nullstellensatz

WEEK2

The proof of Theorem 1.6.7 actually goes via the proofs of the subsequent theorems. We use the following result from algebra, whose proof we skip.

1.7.1 Theorem Let K be any field and let L be a finitely generated K-algebra. If L is a field, then it must be a finite extension of K.

Proof. See `https://web.ma.utexas.edu/users/allcock/expos/nullstellensatz3.pdf` □

1.7.2 Proof of Theorem 1.6.9 Let $m \subset k[x_1, \dots, x_n]$ be a maximal ideal. Taking $K = k$ and $L = k[x_1, \dots, x_n]/m$ in Theorem 1.7.1, and using that k is algebraically closed, we get that the natural map $k \to k[x_1, \dots, x_n]/m$ is an isomorphism. Let $a_i \in k$ be the pre-image of x_i under this isomorphism. Then we have $m = (x_1 - a_1, \dots, x_n - a_n)$.

Explain this and prove the last statement. — (4)

1.7.3 Proof of Theorem 1.6.8 Suppose I is not the unit ideal. We show that $V(I)$ is non-empty. To do so, we use that every proper ideal is contained in a maximal ideal.

Finish the proof. — (5)

1.7.4 Proof of Theorem 1.6.10 We consider the system $g = 0$ for $g \in I$ and $f \neq 0$. Notice that the last one is not an equation, but there is a trick that allows us to convert it into an equation. Let y be a new variable, and consider the polynomial ring $k[x_1, \dots, x_n, y]$. In the bigger ring, consider the system of equations $g = 0$ for $g \in I$ and $yf - 1 = 0$. By our assumption, this system of equations has no solutions.

Explain this and finish the proof using Theorem 1.6.8. — (6)

1.7.5 Proof of Theorem 1.6.7. We show that the maps $I \to V(I)$ and $S \to I(S)$ are mutual inverses. That is, we show that $I(V(I)) = I$ if I is a radical ideal, and $V(I(S)) = S$ if S is a Zariski closed subset of $\mathbb{A}^n_k$.

Let us first show that for any ideal I, we have $I(V(I)) = \sqrt{I}$. Suppose $f \in \sqrt{I}$, then $f^n \in I$ for some $n > 0$. But then f^n is identically zero on $V(I)$, and hence so is f; that is, $f \in I(V(I))$. It remains to show that $I(V(I)) \subset \sqrt{I}$. Let $f \in I(V(I))$. Then f is identically zero on $V(I)$. By 1.6.10, there is some n such that $f^n \in I$, and hence $f \in \sqrt{I}$.

Let us now show that $V(I(S)) = S$. Since S is Zariski closed, we know that $S = V(J)$ for some ideal J. So $I(S) = I(V(J)) = \sqrt{J}$. But we know that $V(J) = V(\sqrt{J})$, and hence $V(I(S)) = S$. The proof of Theorem 1.6.7 is then complete.

1.8 Affine and quasi-affine varieties WEEK2

An *affine variety* is a subset of the affine space that is closed in the Zariski topology. A *quasi-affine variety* is a subset of the affine space that is locally closed in the Zariski topology. (A locally closed subset of a topological space is a set that can be expressed as an intersection of an open set and a closed set).

2 Regular functions and maps

Throughout this section, k is an algebraically closed field.

2.1 Regular functions WEEK3

Let $S \subset \mathbb{A}^n$ be a set and let $f\colon S \to k$ be a function. Let a be a point of S.

2.1.1 Definition (Regular function) We say that f is *regular* (or *algebraic*) *at* a if there exists a Zariski open set $U \subset \mathbb{A}^n$ and polynomials $p, q \in k[x_1, \dots, x_n]$ with $q(a) \neq 0$ such that

$$f \equiv p/q \text{ on } S \cap U.$$

We say that f is *regular* if it is regular at all points of S.

In other words, f is regular at a point a if locally around a (in the Zariski topology), f can be expessed as a ratio of two polynomials. Although the definition of a regular function makes sense for $S \subset \mathbb{A}^n$, we use it only in the context of quasi-affine varieties.

2.1.2 Example

1. A constant function is regular.

2. Every polynomial function is regular.

3. Sums and products of regular functions are regular. So, the set of regular functions forms a ring. This ring contains a copy of k, namely the constant functions.

2.1.3 Definition (Ring of regular functions) We denote the ring of regular functions on S by $k[S]$.

2.1.4 Proposition (Local nature of regularity) Let f be a function on S, and let $\{U_i\}$ be an open cover of S. If the restriction of f to each U_i is regular, then f is regular.

Proof. — (1)

2.2 Regular functions on an affine variety

WEEK3

It turns out that regular functions on closed subsets of $\mathbb{A}^n$ are just the polynomial functions! So, not only is there a global algebraic expression, we don't even need denominators.

2.2.1 Proposition Let $X \subset \mathbb{A}^n$ be a Zariski closed subset. Let f be a regular function on X. Then there exists a polynomial $P \in k[x_1, \dots, x_n]$ such that $P(x) = f(x)$ for all $x \in X$.

Proof. By definition, we know that for every $x \in X$, there is a Zariski open set $U \subset X$ and polynomials p, q such that $f = p/q$ on U. The set U and the polynomials p, q may depend on x, so let us denote them by U_x, p_x, and q_x. We need to combine all of these p's and q's and construct a single polynomial P that agrees with f for all x.

This is done by a "partition of unity" argument. First, let us do some preparation. We know that $p_x/q_x = f$ on U_x, but we know nothing about p_x and q_x on the complement of U_x. Our first step is a small trick due to which we may assume that both p_x and q_x are identically zero on the complement of U_x.

Since $U_x \subset X$ is open, its complement is closed. By the definition of the Zariski topology, this means that
$$X \setminus U_x = X \cap V(A),$$
for some $A \subset k[x_1, \dots, x_n]$. Since $x \in U_x$, at least one of the polynomials in A must be non-zero at x. Let g be such a polynomial, and set $U'_x = X \cap \{g \neq 0\}$. Then $U'_x \subset U_x$ is a possibly smaller open set containing x. Set $p'_x = p_x \cdot g$ and $q'_x = q_x \cdot g$. Then we have $f = p'_x/q'_x$ on U'_x, and we also have $p'_x \equiv q'_x \equiv 0$ on $X \setminus U'_x$. So, we may assume from the beginning that both p_x and q_x are identically zero on the complement of U_x..

Now comes the crux of the argument. Suppose $X = V(I)$. Consider the set of "denominators" $\{q_x \mid x \in X\}$. Note that the system of equations

$$g = 0 \text{ for all } g \in I \text{ and } q_x = 0 \text{ for all } x \in X$$

has no solution!

Why is this true? — (2)

By the Nullstellensatz, this means that the ideal $I + \langle q_x \mid q \in X \rangle$ is the unit ideal. That is, we can write

$$1 = g + r_1 q_{x_1} + \cdots + r_m q_{x_m}$$

for some polynomials $r_1, \ldots, r_m$. Take $P = r_1 p_{x_1} + \cdots + r_m p_{x_m}$. Then $f = P$ on all of X.

Check the last equality. — (3)

□

—- Let $X \subset \mathbb{A}^n$ be any subset. We have a ring homomorphism

$$\pi \colon k[x_1, \ldots, x_n] \to k[X],$$

where a polynomial f is sent to the regular function it defines on X.

2.2.2 Proposition (Ring of regular functions of an affine) Let $X \subset \mathbb{A}^n$ be a closed subset. Then the ring homomorphism $\pi \colon k[x_1, \ldots, x_n] \to k[X]$ induces an isomorphism

$$k[x_1, \ldots, x_n]/I(X) \xrightarrow{\sim} k[X].$$

Proof. The map π is surjective by Proposition 2.2.1 and its kernel is $I(X)$ by definition. The result follows by the isomorphism theorems. □

2.3 Regular maps

WEEK3

Regular functions play the same role in algebraic geometry as continuous functions in topology or smooth functions in differential geometry.

Consider $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ and a function $f \colon X \to Y$. Write f in coordinates as

$$f = (f_1, \ldots, f_m).$$

2.3.1 Definition (Regular map) We say that f is *regular at a point* $a \in X$ if all its coordinate functions $f_1, \ldots, f_m$ are regular at a. If f is regular at all points of X, then we say that it is *regular*.

2.3.2 Example (Maps to $\mathbb{A}^1$) A regular map to $\mathbb{A}^1$ is the same as a regular function.

2.3.3 Example (An isomorphism) Let $U = \mathbb{A}^1 \setminus \{0\}$ and $V = V(xy - 1) \subset \mathbb{A}^2$. We have a regular function $\phi\colon V \to U$ given by $\phi(x, y) = x$. We have a regular function $\psi\colon U \to V$ given by $\psi(t) = (t, 1/t)$. These functions are mutual inverses, and hence we have a (bi-regular) isomorphism $U \cong V$.

2.4 Proposition (Elementary properties of regular maps) WEEK3

1. The identity map is regular.
2. The composition of two regular maps is regular.
3. Regular maps are continuous (in the Zariski topology).

Proof. The identity map is given by $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n)$; each coordinate is a polynomial, and hence regular. The statement for composition is true because the composition of fractions of polynomials is also a fraction of polynomials. The third statement is left as homework. $\square$

2.5 Proposition (Regular maps preserve regular functions) WEEK3

Let $\phi\colon X \to Y$ be a regular map. If f is a regular function on Y, then $f \circ \phi$ is a regular function on X.

Proof. View a regular function as a regular map to $\mathbb{A}^1$. Then this becomes a special case of composition of regular maps. $\square$

—

As a result, we get a k-algebra homomorphism $k[Y] \to k[X]$, often denoted by ϕ^*:

$$\phi^*(f) = f \circ \phi.$$

We thus get a (contravariant) functor from the category of (quasi-affine) varieties to k-algebras. On objects, it maps X to $k[X]$. On morphisms, it maps $\phi\colon X \to Y$ to $\phi^*\colon Y \to X$. It is easy to check that this recipe respects composition. That is, if we have maps $\phi\colon X \to Y$ and $\psi\colon Y \to Z$, and if we let $\psi \circ \phi\colon X \to Z$ be the composite, then

$$(\psi \circ \phi)^* = \phi^* \circ \psi^*.$$

2.6 Corollary (Isomorphic varieties have isomorphic rings of functions) WEEK3

If $\phi\colon X \to Y$ is an isomorphism of varieties, then $\phi^*\colon k[Y] \to k[X]$ is an isomorphism of k-algebras.

Proof. Let $\psi\colon Y \to X$ be the inverse of ϕ. Then $\psi^*\colon k[X] \to k[Y]$ is the inverse of ϕ^*. □

2.7 Proposition (For affines, map between rings induces map between spaces) WEEK3

Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be Zariski closed, and let $f\colon k[Y] \to k[X]$ be a homomorphism of k-algebras. Then there is a unique (regular) map $\phi\colon X \to Y$ such that $f = \phi^*$.

Proof. We know that $k[X] = k[x_1, \ldots, x_n]/I(X)$ and $k[Y] = k[y_1, \ldots, y_m]/I(Y)$. Let $\phi_i = f(y_i) \in k[X]$. Consider $\phi\colon X \to \mathbb{A}^m$ given by $\phi = (\phi_1, \ldots, \phi_m)$. Then ϕ sends X to Y and is the unique map satisfying the required properties. □

Prove the last statement. — (6)

PDF Version