

# M4P33 Algebraic Geometry

Lectured by Prof Kevin Buzzard  
Typed by David Kurniadi Angdinata

Spring 2020

**Syllabus**

# Contents

<b>0</b>	<b>Introduction</b>	<b>3</b>
0.1	Bézout's theorem . . . . .	3
0.2	Practical information about the course . . . . .	4
<b>1</b>	<b>Affine varieties</b>	<b>5</b>
1.1	Affine algebraic sets . . . . .	5
1.1.1	Affine space . . . . .	5
1.1.2	Definition and examples . . . . .	5
1.1.3	New algebraic sets from old . . . . .	6
1.1.4	Ideals and algebraic sets . . . . .	7
1.1.5	Statement of the Nullstellensatz . . . . .	9
1.1.6	Basic facts about the Zariski topology . . . . .	9
1.1.7	Connected and irreducible sets . . . . .	10

## 0 Introduction

### 0.1 Bézout's theorem

Lecture 1  
Monday  
13/01/20

Here is an example of a theorem in algebraic geometry and an outline of a geometric method for proving it which illustrates some of the main themes in algebraic geometry.

**Theorem 0.1** (Bézout). *Let  $C$  be a plane algebraic curve  $\{(x, y) \mid f(x, y) = 0\}$  where  $f$  is a polynomial of degree  $m$ . Let  $D$  be a plane algebraic curve  $\{(x, y) \mid g(x, y) = 0\}$  where  $g$  is a polynomial of degree  $n$ . Suppose that  $C$  and  $D$  have no component in common, since if they had a component in common, then their intersection would obviously be infinite. Then  $C \cap D$  consists of  $mn$  points, provided that*

- we work over the complex numbers  $\mathbb{C}$ ,
- we work in the projective plane, which consists of the ordinary plane together with some points at infinity, and
- we count intersections with the correct multiplicities, so if the curves are tangent at a point, it counts as more than one intersection.

Consider the cases where  $C$  is a line of degree one and  $D$  has either degree one or two. The projective plane will be formally defined later in the course. We will not define intersection multiplicities in this course, but the idea is that multiple intersections resemble multiple roots of a polynomial in one variable.

*Proof.* We prove a special case, where  $C$  is the union of  $m$  lines, then use this to prove the general case of the theorem.

- First for the special case, suppose we have  $m$  lines in the plane, with equations

$$a_1x + b_1y + c_1 = 0, \quad \dots, \quad a_mx + b_my + c_m = 0.$$

We can multiply these equations together to get

$$(a_1x + b_1y + c_1) \dots (a_mx + b_my + c_m) = 0.$$

This is an equation of degree  $m$  and its solution set is the union of the lines. Each line intersects  $D$  in  $n$  points, counted with multiplicities, because we can rearrange the equation of the line into the form  $x = \dots$  or  $y = \dots$  then substitute into the equation for  $D$ . This usually gives a polynomial of degree  $n$  in one variable, and this has  $n$  roots if we count them correctly. There are also special cases to worry about where the line intersects  $D$  at infinity. Combining all the  $m$  lines, we deduce that their union intersects  $D$  in  $mn$  points.

- Now we deduce the general case from the special case. We let the curve  $C$  vary in a family of curves of degree  $m$ . What exactly we mean by varying in a family will be defined later in the course. As an example, consider the family of curves

$$\mathcal{F} : \{(x, y) \mid x^2 - y^2 = t\},$$

where  $t$  is a parameter, so for different values of  $t$  we get different curves. When the curve  $C$  varies in a family like this, the number of intersection points in  $C \cap D$  does not change, counting with multiplicity. This is the core of the proof. It requires a lot of work to justify which we will not do here. For any degree  $m$  curve  $C$ , it is possible to find a family of curves which contains both  $C$  itself and a union of  $m$  lines  $X$ . For example, if  $C$  is the hyperbola defined by the equation  $x^2 - y^2 = 1$ , then it is found in the family  $\mathcal{F}$ , with  $t = 1$ . If we let  $t = 0$  in this family, then the equation factors as  $(x - y)(x + y)$  and this defines the union of two lines in the plane. We have already proved that  $X \cap D$  has  $mn$  points, and we stated that  $X \cap D$  has the same number of points as  $C \cap D$  because  $C$  and  $X$  are in the same family. We conclude that  $C \cap D$  has  $mn$  points.

□

The idea that something stays the same everywhere, or almost everywhere, in a family of varying algebraic sets is a key theme in algebraic geometry. Note that this proof uses not just curves but also higher-dimensional algebraic sets. Instead of thinking about a family of curves such as  $\mathcal{F}$ , with coordinates  $(x, y)$  and a parameter  $t$ , we can regard  $x, y, t$  all as coordinates in three-dimensional space and consider the surface

$$\{(x, y, t) \mid x^2 - y^2 = t\}.$$

Then we use facts about this surface as part of the proof. We will not prove Bézout's theorem in this course. In particular, we will not define intersection multiplicities. But we will set up many of the tools needed to fill in the gaps in this outline proof.

## 0.2 Practical information about the course

The following are books.

- M Reid, Undergraduate algebraic geometry, 1988
- R Hartshorne, Algebraic geometry, 1977

During the course we will sometimes assume results from commutative algebra. Books which contain these results, and much much more, include the following.

- H Matsumura, Commutative ring theory, 1986
- M F Atiyah and I G Macdonald, Introduction to commutative algebra, 1969
- D Eisenbud, Commutative algebra: with a view toward algebraic geometry, 2011

The following is the course outline.

- Affine varieties.
  - Definition and examples.
  - Maps between varieties.
  - Translating between geometry and commutative algebra by the Nullstellensatz.
- Projective varieties.
  - Definition and examples.
  - Maps between varieties.
  - Rigidity and images of maps.
- Dimension.
  - Several different definitions, all equivalent, but useful for different purposes.
  - Calculating dimensions of examples.

What is not in the course?

- Schemes.
- Sheaves and cohomology.
- Curves, divisors, and the Riemann–Roch theorem.

# 1 Affine varieties

## 1.1 Affine algebraic sets

### 1.1.1 Affine space

Let  $k$  be an algebraically closed field. We are going to be thinking about solutions to polynomials, so everything is much simpler over algebraically closed fields. Number theorists might be interested in other fields, but you generally have to start by understanding the algebraically closed case first. In this course we will stop with the algebraically closed case too. Apart from being algebraically closed, it usually does not matter much which field we use to do algebraic geometry, except sometimes it matters whether the characteristic is zero or positive. In this course I will take care to mention results which depend on the characteristic, and sometimes we might consider only the characteristic zero case. You will not lose much if you just assume that  $k = \mathbb{C}$  throughout the course, except when it will be explicitly something else. Indeed it is often useful to think about  $k = \mathbb{C}$  because then you can use your usual geometric intuition. When I draw pictures on the whiteboard, I am usually only drawing the real solutions because it is hard to draw shapes in  $\mathbb{C}^2$ . This is cheating but it is often very useful. The real solutions are not the full picture but in many cases we can still see the important features there.

**Definition 1.1.** Algebraic geometers write  $\mathbb{A}^n$  to mean  $k^n$ , and call it **affine  $n$ -space**.

You may think of this as just a funny choice of notation, but there are at least two reasons for it.

- When we write  $k^n$ , it makes us think of a vector space, equipped with operations of addition and scalar multiplication. But  $\mathbb{A}^n$  means just a set of points, described by coordinates  $(x_1, \dots, x_n)$  with  $x_i \in k$ , without the vector space structure.
- Because it usually does not matter much what our base field  $k$  is, as long as it is algebraically closed, it is convenient to have notation which does not prominently mention  $k$ .

On occasions when it is important to specify which field  $k$  we are using, we write  $\mathbb{A}_k^n$  for affine  $n$ -space.

### 1.1.2 Definition and examples

**Definition 1.2.** An **affine algebraic set** is a subset  $V \subseteq \mathbb{A}^n$  which consists of the common zeroes of some finite set of polynomials  $f_1, \dots, f_m$  with coefficients in  $k$ . More formally, an affine algebraic set is a set of the form

$$V = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid f_1(x_1, \dots, x_n) = \dots = f_m(x_1, \dots, x_n) = 0\}, \quad f_1, \dots, f_m \in k[X_1, \dots, X_n].$$

**Example.** Examples.

- The empty set, defined by the polynomial  $f_1 = 3$ , for example.
- The whole space  $\mathbb{A}^n$ , defined by the polynomial  $f_1 = 0$ , or by the empty set of polynomials.
- Any finite subset  $\{a_1, \dots, a_n\}$  in  $\mathbb{A}^1$ , defined by the polynomial  $f_1 = (X - a_1) \dots (X - a_n)$ .
- Any single-point set  $\{(a_1, \dots, a_n)\}$  in  $\mathbb{A}^n$ , defined by the polynomials  $f_i = X_i - a_i$ . Note that this is different from the example of a finite set in  $\mathbb{A}^1$ , because that example had a single polynomial in one variable of degree  $n$ , while here we have  $n$  distinct polynomials in  $n$  variables of degree one.
- Any algebraic curve in  $\mathbb{A}^n$ , that is, a set of the form

$$\{(x_1, \dots, x_n) \in \mathbb{A}^n \mid f(x_1, \dots, x_n) = 0\}, \quad f \in k[X_1, \dots, X_n].$$

- Embeddings of  $\mathbb{A}^m$  in  $\mathbb{A}^n$  where  $m < n$ ,

$$\{(x_1, \dots, x_m, 0, \dots, 0) \in \mathbb{A}^n\} = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid x_{m+1} = \dots = x_n = 0\}.$$

More generally, the image of a linear map  $\mathbb{A}^m \rightarrow \mathbb{A}^n$ ,

$$\{(x_1, \dots, x_n) \in \mathbb{A}^n \mid \text{some linear conditions}\}.$$

Lecture 2  
Thursday  
16/01/20

**Example.** Non-examples.

- Any infinite subset of  $\mathbb{A}^1$ , other than  $\mathbb{A}^1$  itself, such as a line segment, a line with a double point, or an infinite discrete set. This is because a one-variable polynomial with infinitely many roots must be the zero polynomial. This also tells us that  $\{x \in \mathbb{A}^1 \mid x \neq 0\}$  is not an affine algebraic set. However there is an affine algebraic set which is isomorphic to  $\mathbb{A}^1 \setminus \{0\}$ , namely  $\{(x, y) \in \mathbb{A}^2 \mid xy - 1 = 0\}$ . By looking at just the  $x$  coordinate, this set bijects to  $\mathbb{A}^1 \setminus \{0\}$ .
- A sine wave. If  $\{(x, y) \mid y = \sin x\}$  were an affine algebraic set, then  $\{(x, y) \mid y = \sin x, y = 0\}$  would also be an affine algebraic set because it is defined by imposing an extra polynomial condition, but the latter is an infinite discrete set.
- The example of the image of a linear map  $\mathbb{A}^m \rightarrow \mathbb{A}^n$  does not generalise to images of maps where each coordinate is given by a polynomial. For example, consider the map

$$\begin{aligned} \phi : \mathbb{A}^2 &\longrightarrow \mathbb{A}^2 \\ (x, y) &\longmapsto (x, xy) \end{aligned}$$

The image of  $\phi$  is  $S = \mathbb{A}^2 \setminus \{(0, y)\} \cup \{(0, 0)\}$ . To prove that  $S$  is not an affine algebraic set, consider a polynomial  $g(X, Y) \in k[X, Y]$  which vanishes on  $S$ . For each fixed  $y \in k$ , the one-variable polynomial  $g(X, y)$  vanishes at all  $x \neq 0$ . This implies that  $g(X, y)$  is the zero polynomial. Thus  $g(x, y) = 0$  for all  $(x, y) \in k^2$ , that is,  $g$  is the zero polynomial.

**Remark 1.3.** The words affine variety mean more or less the same thing as affine algebraic set but there is an ontological difference. Affine algebraic set means a subset which lives inside  $\mathbb{A}^n$  and knows how it lives inside  $\mathbb{A}^n$ , while affine variety means an object in its own right which is considered outside of  $\mathbb{A}^n$ . I will try to use these words consistently, but the difference is quite subtle and books may not always use it consistently. For the first few weeks, we will talk about affine algebraic sets only. Note that some books, such as Reid and Hartshorne, have another difference between affine varieties and affine algebraic sets. They require varieties to be irreducible, which we will define next time. Other books, such as Shafarevich, do not require varieties to be irreducible. In this course we will not require varieties to be irreducible.

### 1.1.3 New algebraic sets from old

Now we prove that the union of two affine algebraic sets is an affine algebraic set. Consider two points  $(a_1, \dots, a_n)$  and  $(b_1, \dots, b_n)$  in  $\mathbb{A}^n$ . The two-point set  $\{(a_1, \dots, a_n), (b_1, \dots, b_n)\}$  can be defined by taking the product for each possible pair of equations, one from each list, so  $(X_i - a_i)(X_j - b_j) = 0$  for all  $i, j \in \{1, \dots, n\}$ .

**Note.** It is necessary to consider all the pairs between the lists, not just the ones with  $i = j$ , because otherwise we would be allowing points like  $(a_1, \dots, a_{n-1}, b_n)$ .

**Lemma 1.4.** *If  $V, W \subseteq \mathbb{A}^n$  are affine algebraic sets, then their union  $V \cup W \subseteq \mathbb{A}^n$  is also an affine algebraic set.*

*Proof.* We have to take the product for each possible pair of defining polynomials. If

$$V = \{\underline{x} \in \mathbb{A}^n \mid f_1(\underline{x}) = \dots = f_r(\underline{x}) = 0\}, \quad W = \{\underline{x} \in \mathbb{A}^n \mid g_1(\underline{x}) = \dots = g_s(\underline{x}) = 0\},$$

then

$$V \cup W = \{\underline{x} \in \mathbb{A}^n \mid \forall 1 \leq i \leq r, \forall 1 \leq j \leq s, f_i(\underline{x})g_j(\underline{x}) = 0\}.$$

Let us check that these equations really do define  $V \cup W$ . First, suppose that  $\underline{x} \in V \cup W$ . Then either  $\underline{x} \in V$ , so  $f_i(\underline{x}) = 0$  for every  $i$ , so we can multiply by  $g_j(\underline{x})$  to get  $f_i(\underline{x})g_j(\underline{x}) = 0$  for every  $i$  and  $j$ , or  $\underline{x} \in W$ , in which case the same argument works with  $g_j$  in place of  $f_i$ . The reverse direction is a little trickier. Suppose that we have  $\underline{x} \in \mathbb{A}^n$  satisfying  $f_i(\underline{x})g_j(\underline{x}) = 0$  for all  $i$  and  $j$ . Looking just at  $f_1$ , we get

$$f_1(\underline{x})g_1(\underline{x}) = 0 \implies f_1(\underline{x}) = 0 \text{ or } g_1(\underline{x}) = 0, \quad \dots, \quad f_1(\underline{x})g_s(\underline{x}) = 0 \implies f_1(\underline{x}) = 0 \text{ or } g_s(\underline{x}) = 0.$$

Putting these all together, we get  $f_1(\underline{x}) = 0$  or  $g_j(\underline{x}) = 0$  for every  $j$ . We can do the same thing for  $f_2$  to get  $f_2(\underline{x}) = 0$  or  $g_j(\underline{x}) = 0$  for every  $j$ , and so on for each  $f_i$ . Putting all these together, we get  $f_i(\underline{x}) = 0$  for every  $i$  or  $g_j(\underline{x}) = 0$  for every  $j$ . This says precisely that  $\underline{x} \in V \cup W$ .  $\square$

It is even easier to check that the intersection of finitely many affine algebraic sets is an affine algebraic set.

**Lemma 1.5.** *If  $V, W \subseteq \mathbb{A}^n$  are affine algebraic sets, then their intersection  $V \cap W \subseteq \mathbb{A}^n$  is also an affine algebraic set.*

*Proof.* Just combine the lists of defining equations. That is, say

$$V = \{\underline{x} \in \mathbb{A}^m \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}, \quad W = \{\underline{y} \in \mathbb{A}^n \mid g_1(\underline{y}) = \cdots = g_s(\underline{y}) = 0\}.$$

Then  $V \cap W$  is simply the set where all the polynomials in both lists vanish, that is

$$V \cap W = \{\underline{x} \in \mathbb{A}^n \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = g_1(\underline{x}) = \cdots = g_s(\underline{x}) = 0\}.$$

□

Just a remark on one other way of constructing new affine algebraic sets from existing ones.

**Lemma 1.6.** *If  $V \subseteq \mathbb{A}^m$  and  $W \subseteq \mathbb{A}^n$  are affine algebraic sets, then their Cartesian product  $V \times W \subseteq \mathbb{A}^{m+n}$  is an affine algebraic set.*

*Proof.* Write

$$V = \{\underline{x} \in \mathbb{A}^m \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}, \quad W = \{\underline{y} \in \mathbb{A}^n \mid g_1(\underline{y}) = \cdots = g_s(\underline{y}) = 0\}.$$

Then

$$V \times W = \{(\underline{x}, \underline{y}) \in \mathbb{A}^{m+n} \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = g_1(\underline{y}) = \cdots = g_s(\underline{y}) = 0\}.$$

□

This looks a bit like the equations defining  $V \cap W$ , but here the  $f_i$  involve different variables from the  $g_j$ , while for  $V \cap W$  both used the same variables.

### 1.1.4 Ideals and algebraic sets

The union of infinitely many affine algebraic sets is not always an affine algebraic set. I do not mean that it is never an affine algebraic set, just that there exist counter-examples. Indeed, any subset of  $\mathbb{A}^n$  can be written as a union of single-point sets. The intersection of infinitely many affine algebraic sets always an affine algebraic set. If we try to prove this by combining the lists of defining equations, we run into a problem. In our definition of affine algebraic sets we only allowed a finite list of polynomial equations. We introduce ideals to remove this restriction.

**Definition 1.7.** Recall from commutative algebra that, if  $R$  is a ring, an **ideal** is a subset  $I \subseteq R$  with the properties that

- if  $f, g \in I$ , then  $f + g \in I$ , and
- if  $f \in I$  and  $q \in R$ , then  $qf \in I$ .

Given any subset  $S \subseteq R$ , we define the **ideal generated by  $S$**  to be the smallest ideal which contains  $S$ , and denote it by  $\langle S \rangle$ . In particular, if  $S$  is the finite set  $\{f_1, \dots, f_m\}$  then it generates the ideal

$$\langle f_1, \dots, f_m \rangle = \{q_1 f_1 + \cdots + q_m f_m \mid q_1, \dots, q_m \in R\}.$$

Let us introduce some notation.

**Definition 1.8.** For any set  $S \subseteq k[X_1, \dots, X_n]$ , let

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

**Lemma 1.9.** *If  $S \subseteq k[X_1, \dots, X_n]$  generates the ideal  $I$ , then  $\mathbb{V}(S) = \mathbb{V}(I)$ .*

*Proof.* We have  $S \subseteq I$  and so it is easy to see that  $\mathbb{V}(I) \subseteq \mathbb{V}(S)$ . Suppose that  $\underline{x} \in \mathbb{V}(S)$ , and  $f \in \mathbb{V}(I)$ . Then there are  $f_1, \dots, f_m \in S$  and  $q_1, \dots, q_m \in k[X_1, \dots, X_n]$  such that  $f = q_1 f_1 + \cdots + q_m f_m$ . Since  $f_1(\underline{x}) = \cdots = f_m(\underline{x}) = 0$ , it follows that  $f(\underline{x}) = 0$ . Since this holds for every  $f \in I$ ,  $\underline{x} \in \mathbb{V}(I)$ . □

Lecture 3  
Friday  
17/01/20

**Theorem 1.10** (Hilbert basis theorem). *From commutative algebra, if  $k$  is any field, then the polynomial ring  $k[X_1, \dots, X_n]$  is Noetherian. That means that the following two equivalent conditions hold.*

- *Let  $I$  be an ideal in  $k[X_1, \dots, X_n]$ . Then there exists a finite set  $\{f_1, \dots, f_m\} \subseteq k[X_1, \dots, X_n]$  which generates  $I$ .*
- *Let  $I_1 \subseteq I_2 \subseteq \dots$  be an ascending chain of ideals in  $k[X_1, \dots, X_n]$ . Then there is some  $N$  such that  $I_n = I_N$  for every  $n > N$ .*

Using the Hilbert basis theorem, we can deduce that the restriction to finite lists of polynomials in the definition of affine algebraic sets is unnecessary.

**Corollary 1.11.**  $\mathbb{V}(S)$  is an affine algebraic set for any set of polynomials  $S \subseteq k[X_1, \dots, X_n]$ .

*Proof.* Let  $I$  be the ideal in  $k[X_1, \dots, X_n]$  generated by  $S$ . By the Hilbert basis theorem,  $k[X_1, \dots, X_n]$  is Noetherian and so we can choose a finite set  $\{f_1, \dots, f_m\}$  which generates  $I$ . Then Lemma 1.9 tells us that  $\mathbb{V}(S) = \mathbb{V}(I) = \mathbb{V}(f_1, \dots, f_m)$ .  $\square$

**Corollary 1.12.** *The intersection of finitely many affine algebraic sets is an affine algebraic set.*

*Proof.* Combine the lists of defining polynomials for all the algebraic sets, and apply Corollary 1.11.  $\square$

We can also go in the other direction, from affine algebraic sets to ideals. Say  $V_n = \mathbb{V}(I_n)$ . Does  $V_1 \supseteq V_2$  imply that  $I_1 \subseteq I_2$ ? No. The problem is that there is more than one ideal defining the same algebraic set.

**Example.** Let  $I_1 = \langle X \rangle$  and  $I_2 = \langle X^2 \rangle$  in  $k[X]$ . We have  $\mathbb{V}(I_1) = \{0\} = \mathbb{V}(I_2)$ .

However, there is a natural choice we can make for one ideal canonically associated with an affine algebraic set, the set of all polynomials which vanish on that set.

**Definition 1.13.** Formally, if  $A$  is any subset of  $\mathbb{A}^n$ , usually  $A$  will be an affine algebraic set, we define

$$\mathbb{I}(A) = \{f \in k[X_1, \dots, X_n] \mid \forall \underline{x} \in A, f(\underline{x}) = 0\}.$$

**Note.**  $\mathbb{I}(A)$  is an ideal in  $k[X_1, \dots, X_n]$ .

We have now defined two functions

$$\mathbb{V} : \{\text{ideals in } k[X_1, \dots, X_n]\} \rightarrow \{\text{affine algebraic sets in } \mathbb{A}^n\},$$

$$\mathbb{I} : \{\text{affine algebraic sets in } \mathbb{A}^n\} \rightarrow \{\text{ideals in } k[X_1, \dots, X_n]\}.$$

These functions are not inverses of each other. The example of  $\langle X \rangle$  and  $\langle X^2 \rangle$  shows that  $\mathbb{I}(\mathbb{V}(\langle X^2 \rangle)) = \langle X \rangle \neq \langle X^2 \rangle$ . But composing  $\mathbb{V}$  and  $\mathbb{I}$  in the other order gives the identity.

**Lemma 1.14.** *If  $V$  is an affine algebraic set, then  $\mathbb{V}(\mathbb{I}(V)) = V$ .*

*Proof.* It is clear that  $V \subseteq \mathbb{V}(\mathbb{I}(V))$ , and this works when  $V$  is any subset of  $\mathbb{A}^n$ , not necessarily algebraic. For the reverse inclusion, we have to use the hypothesis that  $V$  is an affine algebraic set. By the definition of affine algebraic sets,  $V = \mathbb{V}(J)$  for some ideal  $J \subseteq k[X_1, \dots, X_n]$ . Suppose that  $\underline{y} \notin V$ . We shall show that  $\underline{y} \notin \mathbb{V}(\mathbb{I}(V))$ . Because  $\underline{y} \notin V = \mathbb{V}(J)$ , there exists  $f \in J$  such that  $f(\underline{y}) \neq 0$ . By definition,  $J \subseteq \mathbb{I}(V)$  and so  $f \in \mathbb{I}(V)$ . Hence  $f(\underline{y}) \neq 0$  tells us that  $\underline{y} \notin \mathbb{V}(\mathbb{I}(V))$ .  $\square$

What is the geometric interpretation of the Hilbert basis theorem?

**Note.** It is clear that  $\mathbb{V}$  and  $\mathbb{I}$  reverse the direction of inclusions, so if  $I_1 \subseteq I_2$ , then  $\mathbb{V}(I_2) \subseteq \mathbb{V}(I_1)$ .

Hence the ascending chain condition for ideals translates into the descending chain condition for affine algebraic sets. The following statement is the translation into affine algebraic sets of the Hilbert basis theorem.

**Lemma 1.15.** *Let  $V_1 \supseteq V_2 \supseteq \dots$  be a descending chain of affine algebraic sets in  $\mathbb{A}^n$ . Then there exists  $N$  such that  $V_n = V_N$  for all  $n > N$ .*

*Proof.* The fact that  $V_1 \supseteq V_2 \supseteq \dots$  implies that  $\mathbb{I}(V_1) \subseteq \mathbb{I}(V_2) \subseteq \dots$ . Because  $k[X_1, \dots, X_n]$  is Noetherian, there exists  $N$  such that  $\mathbb{I}(V_n) = \mathbb{I}(V_N)$  for all  $n > N$ . By Lemma 1.14,  $V_n = \mathbb{V}(\mathbb{I}(V_n))$  for every  $n$  and so this proves the proposition.  $\square$



### 1.1.5 Statement of the Nullstellensatz

When does  $\mathbb{I}(\mathbb{V}(I)) = I$ ? It turns out that the only reason that this can fail is where elements of the ideal  $I$  have  $n$ -th roots which are not in  $I$ , just as with the example of  $I = \langle X^2 \rangle$  where  $X^2 \in I$  has a square root  $X$  which is not in  $I$ . To state this precisely, we need to recall the definition of the radical of an ideal from commutative algebra.

**Definition 1.16.** Let  $I$  be an ideal in a ring  $R$ . The **radical** of  $I$  is

$$\text{rad } I = \sqrt{I} = \{f \in R \mid \exists n > 0, f^n \in I\}.$$

We say that  $I$  is a **radical ideal** if  $\text{rad } I = I$ .

**Note.** If  $I$  is any ideal, then  $\text{rad } I$  is always a radical ideal.

**Theorem 1.17** (Hilbert's Nullstellensatz). *Let  $I$  be any ideal in the polynomial ring  $k[X_1, \dots, X_n]$  over an algebraically closed field  $k$ . Then*

$$\mathbb{I}(\mathbb{V}(I)) = \text{rad } I.$$

This is a substantial theorem, fundamental to algebraic geometry. We will prove it in a few lectures' time, not because we need to develop more theory, just because I would like to introduce some more concepts first which will allow us to do more with examples.

**Note.** To calculate  $\text{rad } I$ , we need to add in  $n$ -th roots of all elements of  $I$ , not just the generators.

**Example.** If  $I = \langle X, Y^2 - X \rangle \subseteq k[X, Y]$ , then we can rewrite this as  $I = \langle X, Y^2 \rangle$  and so  $\text{rad } I = \langle X, Y \rangle \neq I$ , even though neither of the original generators of  $I$  had any non-trivial  $n$ -th roots.

### 1.1.6 Basic facts about the Zariski topology

We have seen that affine algebraic sets in  $\mathbb{A}^n$  satisfy the following conditions.

- $\mathbb{A}^n$  and  $\emptyset$  are affine algebraic sets.
- A finite union of affine algebraic sets is an affine algebraic set.
- An arbitrary intersection of affine algebraic sets is an affine algebraic set.

These are precisely the conditions satisfied by the closed sets in a topological space. Therefore, we can define a topological space in which the underlying set is  $\mathbb{A}^n$  and closed sets are the affine algebraic sets. This is called the **Zariski topology**. This is a very different topology from the ones you are used to in analysis. In particular, it is a very long way from being Hausdorff. For any affine algebraic set  $V \subseteq \mathbb{A}^n$ , we define the **Zariski topology** on  $V$  to be the subspace topology on  $V$  induced by the Zariski topology on  $\mathbb{A}^n$ . Thus, a subset of  $V$  is Zariski closed in  $V$  if and only if it is Zariski closed in  $\mathbb{A}^n$ . Thus for closed sets it does not matter whether we say Zariski closed in  $V$  or Zariski closed in  $\mathbb{A}^n$ .

**Example.** The Zariski topology on  $\mathbb{A}^1$  is the same as the cofinite topology. Prove that the Zariski topology on  $\mathbb{A}^1$  is not Hausdorff. <sup>1</sup>

Thus we see that the Zariski topology has much fewer closed sets, or much fewer open sets, than for example the Euclidean topology.

**Lemma 1.18.** *Suppose that  $k = \mathbb{C}$ , so there is a Euclidean topology on  $\mathbb{A}_{\mathbb{C}}^n$ . If  $V$  is a Zariski closed subset of  $\mathbb{A}_{\mathbb{C}}^n$ , then  $V$  is closed in the Euclidean topology, so the Euclidean topology is finer than the Zariski topology.*

*Proof.* Let  $f \in \mathbb{C}[X_1, \dots, X_n]$  be a polynomial. It is a continuous function  $\mathbb{A}_{\mathbb{C}}^n \rightarrow \mathbb{C}$  for the Euclidean topology. Since  $\{0\}$  is a closed subset of  $\mathbb{C}$ ,  $\mathbb{V}(f) = f^{-1}(0)$  is a closed subset of  $\mathbb{A}_{\mathbb{C}}^n$  in the Euclidean topology. We conclude by noting that intersections of closed sets are closed.  $\square$

<sup>1</sup>Exercise

On the other hand, for open sets Zariski open in  $V$  does not mean the same thing as Zariski open in  $\mathbb{A}^n$ . A Zariski open subset of  $V$  need not be Zariski open in  $\mathbb{A}^n$ .

**Example.** Let  $V$  be the  $x$ -axis in  $\mathbb{A}^2$ . Then  $V \setminus \{0\}$  is open in  $V$ , but not open in  $\mathbb{A}^2$ .

The open subsets of the Zariski topology are all very big. This is made precise, for  $\mathbb{A}^1$ , by the following lemma.

**Lemma 1.19.** *Prove that every pair  $U_1$  and  $U_2$  of non-empty open sets in  $\mathbb{A}^1$  has a non-empty intersection  $U_1 \cap U_2$ .*

Hence the Zariski topology on  $\mathbb{A}^1$  is not Hausdorff. A subset of  $\mathbb{A}^1$  is dense in the Zariski topology if and only if it is infinite. At the moment, the Zariski topology is likely to seem very strange. It might also seem like, what is the point of such a strange topology? We will not use it in a very deep way, it is just a convenient language to be able to talk about open and closed sets. It does get used more seriously in the theory of schemes.

### 1.1.7 Connected and irreducible sets

Recall the definition of a connected topological space.

**Definition 1.20.** A topological space  $S$  is **connected** if it is not possible to write it as the union of two disjoint non-empty open sets. This is equivalent to, it is not possible to write  $S$  as the union of two disjoint non-empty closed sets.

It is possible to talk about connectedness in the Zariski topology.

**Example.** A finite set of points of size greater than one is not connected in the Zariski topology, since every subset is closed.

Consider the following affine algebraic sets in  $\mathbb{A}^2$ . Do they have one or two pieces? Do they have one or two pieces? I have deliberately not specified what I mean by pieces. There are multiple sensible interpretations, so there is not always a unique correct answer.

- The union of two disjoint lines  $\mathbb{V}(X(X-1))$ .
- The union of two intersecting lines  $\mathbb{V}(XY)$ .
- The hyperbola  $\mathbb{V}(XY-1)$ .

**Example.** The union of two disjoint lines  $\mathbb{V}(X(X-1))$  is not connected, since it unambiguously has two pieces, the two lines  $\mathbb{V}(X)$  and  $\mathbb{V}(X-1)$ , and each line is a non-empty closed subset.

But there is a more refined notion for the Zariski topology.

**Example.** The set  $\mathbb{V}(XY)$  has more than one answer. The two axes form two pieces. It is a union of two lines, intersecting at the origin, joining them into one piece. Describe the Zariski closed subsets.<sup>2</sup>

The following notion gives us a way of formally understanding the example described.

**Definition 1.21.** A topological space  $S$  is **reducible** if it is empty, or there exist closed sets  $S_1, S_2 \subseteq S$  such that  $S = S_1 \cup S_2$ , and neither  $S_1$  nor  $S_2$  is equal to  $S$ . A topological space  $S$  is **irreducible** if it is non-empty and it is not possible to write it as the union  $S_1 \cup S_2$  of two closed sets, unless at least one of  $S_1$  and  $S_2$  is equal to  $S$  itself. Compared to the second definition of connected, we no longer require  $S_1$  and  $S_2$  to be disjoint.

This is not a very useful notion for the topological spaces we consider in analysis.

**Example.** Considering the real line with the Euclidean topology, we can write it as a union of proper closed subsets,

$$\mathbb{R} = \{x \in \mathbb{R} \mid x \leq 0\} \cup \{x \in \mathbb{R} \mid x \geq 0\}.$$

These subsets are not disjoint because they intersect at zero. Of course, there are many other ways to write  $\mathbb{R}$  as a union of proper closed subsets in the usual topology. The same is true for any other Hausdorff space.

---

<sup>2</sup>Exercise

**Example.** The drawing of  $\mathbb{V}(XY - 1)$  in  $\mathbb{R}^2$  is misleading. It looks like it has two pieces, but, as mentioned before, we are missing a lot by only looking at real solutions. For algebraic geometry, we need to look at complex solutions, and then over  $\mathbb{C}$  it unambiguously has one piece. One way to visualise this is to note that, if we project down to the  $x$  coordinate,  $\mathbb{V}(XY - 1)$  looks like the set  $\mathbb{A}^1 \setminus \{0\}$ . This is not a formal statement. We have not yet defined a notion of isomorphism of affine algebraic sets, and even if we had,  $\mathbb{A}^1 \setminus \{0\}$  is not an affine algebraic set. In a few weeks we will develop technology to make this into a rigorous statement. But for now we use it as a heuristic. Then  $\mathbb{R} \setminus \{0\}$  unambiguously has two pieces, but  $\mathbb{C} \setminus \{0\}$  is connected in the usual analytic topology on  $\mathbb{C}$  and unambiguously has one piece. So the hyperbola, over an algebraically closed field, should have only one piece.

We prove below in the lecture that  $\mathbb{V}(XY - 1)$  is irreducible, and also connected.

**Lemma 1.22.** *The hyperbola  $H = \mathbb{V}(XY - 1)$  is irreducible.*

*Proof.* We need to describe the Zariski closed subsets of  $H$ . So let  $V \subseteq H$  be a proper Zariski closed subset. Since  $V \neq H$  there must be some polynomial  $f \in k[X, Y]$  which vanishes on  $V$  but does not vanish on all of  $H$ . Because  $V \subseteq H$  and  $y = 1/x$  on  $H$ , we have  $f(x, y) = f(x, 1/x)$  when  $(x, y) \in V$ . Now  $f(X, 1/X)$  is almost a polynomial in the single variable  $X$ , except that it may contain negative powers of  $X$ , so

$$f\left(X, \frac{1}{X}\right) = \sum_{n \in \mathbb{Z}} a_n X^n.$$

We can multiply up by  $X^m$  where  $-m$  is the lowest exponent of  $X$  which appears in this expression. Then  $X^m f(X, 1/X)$  is a polynomial in  $X$ , which vanishes on  $V$ . Furthermore  $f(X, 1/X)$  is not identically zero because  $f$  does not vanish identically on  $H$ . Hence  $X^m f(X, 1/X)$  is a non-zero single-variable polynomial, therefore it has only finitely many roots. The roots of  $X^m f(X, 1/X) = 0$  are the possible  $x$  coordinates for points in  $V$ . For each value of  $x$ , there is at most one possible  $y$  such that  $(x, y) \in V$  because  $y = 1/x$  on  $V$ . Therefore  $V$  is finite. Thus we have shown that all proper Zariski closed subsets of  $H$  are finite. In particular, if  $V_1$  and  $V_2$  are two proper Zariski closed subsets of  $H$ , they are both finite and so their union is finite. Hence  $V_1 \cup V_2 \neq H$  so  $H$  is irreducible.  $\square$

Thus the Zariski topology on  $H$  is the cofinite topology. Here is a bonus fact about connected sets in the Zariski topology which I did not mention in the lecture. The proof is surprisingly hard.

**Theorem 1.23.** *Over  $\mathbb{C}$ , an affine algebraic set is connected in the Zariski topology if and only if it is connected in the Euclidean topology.*

If  $V$  is an affine algebraic set, what condition on the ideal  $\mathbb{I}(V)$  is equivalent to  $V$  being irreducible?