M4P33 Algebraic Geometry

Lectured by Prof Kevin Buzzard
Typed by David Kurniadi Angdinata

Spring 2020

Syllabus

Contents

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

$$a_1x + b_1y + c_1 = 0, \qquad \ldots, \qquad a_mx + b_my + c_m = 0.$$

  We can multiply these equations together to get

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

  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 $x = \ldots$ or $y = \ldots$ 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

$$\mathcal{F} : \left\{(x,y) \;\middle|\; x^2 - y^2 = t\right\},$$

  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

$$\left\{(x, y, t) \;\middle|\; x^2 - y^2 = t\right\}.$$

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 and 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. We already saw this in Bézout's theorem. 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. 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 $\mathbb{A}^n_k$ for affine n-space.

1.1.2 Definition and examples

Lecture 2
Thursday
16/01/20

Definition. 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

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

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
$$\{(x_1, \dots, x_n) \in \mathbb{A}^n \mid f(x_1, \dots, x_n) = 0\}, \qquad f \in k[X_1, \dots, X_n].$$
- Embeddings of $\mathbb{A}^m$ in $\mathbb{A}^n$ where $m < n$,
$$\{(x_1, \dots, x_m, 0, \dots, 0) \in \mathbb{A}^n\} = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid x_{m+1} = \cdots = x_n = 0\}.$$
More generally, the image of a linear map $\mathbb{A}^m \to \mathbb{A}^n$,
$$\{(x_1, \dots, x_n) \in \mathbb{A}^n \mid \text{some linear conditions}\}.$$

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 $\left\{x \in \mathbb{A}^1 \;\middle|\; x \neq 0\right\}$ is not an affine algebraic set. However there is an affine algebraic set which is isomorphic to $\mathbb{A}^1 \setminus \{0\}$, namely $\left\{(x,y) \in \mathbb{A}^2 \;\middle|\; xy - 1 = 0\right\}$. 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 $\mathbb{A}^m \to \mathbb{A}^n$ does not generalise to images of maps where each coordinate is given by a polynomial. For example, consider the map

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

  The image of ϕ 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 1.1. 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 $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ in $\mathbb{A}^n$. The two-point set $\{(a_1, \ldots, a_n), (b_1, \ldots, b_n)\}$ 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 $i, j \in \{1, \ldots, n\}$.

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 $(a_1, \ldots, a_{n-1}, b_n)$.

Lemma 1.2. *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

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

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

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

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 $\underline{x} \in V \cup W$. □

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

Lemma 1.3. *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

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

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 1.4. *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

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

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

Lecture 3
Friday
17/01/20

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. 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 $\{f_1, \ldots, f_m\}$ then it generates the ideal

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

Let us introduce some notation.

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

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

Lemma 1.5. *If $S \subseteq k[X_1, \ldots, X_n]$ 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 $f_1, \ldots, f_m \in S$ and $q_1, \ldots, q_m \in k[X_1, \ldots, X_n]$ 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 $f \in I$, $\underline{x} \in \mathbb{V}(I)$. □

Theorem 1.6 (Hilbert basis theorem)**.** *From commutative algebra, if k is any field, then the polynomial ring $k[X_1, \ldots, X_n]$ is Noetherian. That means that the following two equivalent conditions hold.*

- *Let I be an ideal in $k[X_1, \ldots, X_n]$. Then there exists a finite set $\{f_1, \ldots, f_m\} \subseteq k[X_1, \ldots, X_n]$ which generates I.*
- *Let $I_1 \subseteq I_2 \subseteq \ldots$ be an ascending chain of ideals in $k[X_1, \ldots, X_n]$. 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 1.7. *$\mathbb{V}(S)$ is an affine algebraic set for any set of polynomials $S \subseteq k[X_1, \ldots, X_n]$.*

Proof. Let I be the ideal in $k[X_1, \ldots, X_n]$ generated by S. By the Hilbert basis theorem, $k[X_1, \ldots, X_n]$ is Noetherian and so we can choose a finite set $\{f_1, \ldots, f_m\}$ which generates I. Then Lemma 1.5 tells us that $\mathbb{V}(S) = \mathbb{V}(I) = \mathbb{V}(f_1, \ldots, f_m)$. □

Corollary 1.8. *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 1.7. □

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

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

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

We have now defined two functions

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

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

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 1.9. *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 $J \subseteq k[X_1, \ldots, X_n]$. 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 $\underline{y} \notin \mathbb{V}(\mathbb{I}(V))$. □

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 1.10. *Let $V_1 \supseteq V_2 \supseteq \ldots$ 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 $V_1 \supseteq V_2 \supseteq \ldots$ implies that $\mathbb{I}(V_1) \subseteq \mathbb{I}(V_2) \subseteq \ldots$. Because $k[X_1, \ldots, X_n]$ is Noetherian, there exists N such that $\mathbb{I}(V_n) = \mathbb{I}(V_N)$ for all $n > N$. By Lemma 1.9, $V_n = \mathbb{V}(\mathbb{I}(V_n))$ for every n and so this proves the proposition. □

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

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

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

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

Theorem 1.11 (Hilbert's Nullstellensatz)**.** *Let I be any ideal in the polynomial ring $k[X_1, \ldots, X_n]$ over an algebraically closed field k. Then we have*

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

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 $\operatorname{rad} I$, 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 $\operatorname{rad} I = \langle X, Y \rangle \neq I$, 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.

The 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 $\mathbb{A}^n$.

Lecture 4
Monday
20/01/20

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. [1]

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

Lemma 1.12. *Suppose that $k = \mathbb{C}$, so there is a Euclidean topology on $\mathbb{A}^n_{\mathbb{C}}$. If V is a Zariski closed subset of $\mathbb{A}^n_{\mathbb{C}}$, then V is closed in the Euclidean topology, so the Euclidean topology is finer than the Zariski topology.*

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

[1] 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 1.13. *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. 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. [2]

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

Definition. 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.

[2] 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 1.14. *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. □

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

1.1.8 Prime ideals and irreducible sets

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

Lecture 5
Thursday
23/01/20

Definition. From commutative algebra, an ideal I in a ring R is a **prime ideal** if $I \neq R$ and for every $f, g \in R$, if $fg \in I$, then $f \in I$ or $g \in I$, or both.

Lemma 1.16. *An affine algebraic set $V \subseteq \mathbb{A}^n$ is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal in $k[X_1, \ldots, X_n]$.*

Proof. First suppose that V is irreducible. Suppose we have $f, g \in k[X_1, \ldots, X_n]$ such that $fg \in \mathbb{I}(V)$. Let

$$V_1 = \{\underline{x} \in V \mid f(\underline{x}) = 0\}, \qquad V_2 = \{\underline{x} \in V \mid g(\underline{x}) = 0\}.$$

For every $\underline{x} \in V$, $f(\underline{x})\, g(\underline{x}) = 0$ and hence either $f(\underline{x}) = 0$ or $g(\underline{x}) = 0$. Thus for every $\underline{x} \in V$, either $\underline{x} \in V_1$ or $\underline{x} \in V_2$. In other words, $V = V_1 \cup V_2$. Furthermore V_1 and V_2 are closed subsets of V. Hence as V is irreducible, either $V_1 = V$ or $V_2 = V$. If $V_1 = V$ then $f \in \mathbb{I}(V)$ and if $V_2 = V$ then $g \in \mathbb{I}(V)$. Now suppose that V is reducible. Then we can write it as a union $V_1 \cup V_2$ of proper closed subsets. Since V_1 is a proper closed subset of V, there exists some $f \in k[X_1, \ldots, X_n]$ vanishing on V_1 but not on all of V. Similarly there exists g vanishing on V_2 but not on all of V. Thus neither f nor g is in $\mathbb{I}(V)$, but the product fg vanishes on $V_1 \cup V_2$ and hence we have $fg \in \mathbb{I}(V)$. Thus $\mathbb{I}(V)$ is not prime. Then V is empty if and only if $\mathbb{I}(V) = k[X_1, \ldots, X_n]$, which is explicitly defined to not be a prime ideal. So it was ok to ignore this case above. □

Definition. A **hypersurface** is an affine algebraic set in $\mathbb{A}^n$ defined by one polynomial equation, that is,

$$\{\underline{x} \in \mathbb{A}^n \mid f(\underline{x}) = 0\}, \qquad f \in k[X_1, \ldots, X_n].$$

It follows from Lemma 1.16 together with Hilbert's Nullstellensatz that a hypersurface defined by a polynomial f is irreducible if and only if f is a power of an irreducible polynomial. See problem sheet 1.

Example. We can use this to prove that the circle $\left\{(x,y) \;\middle|\; x^2+y^2=1\right\}$ is irreducible, by proving that the polynomial X^2+Y^2-1 is irreducible. This is because, if $f = X^2+Y^2-1 = f_1 f_2$ then we can scale f_1 and f_2 by constants to get

$$f_1 = X + g_1(Y), \qquad f_2 = X + g_2(Y),$$

since f has degree two in X and its X^2 term has coefficient one. Since f has no X term, we must have $g_1 + g_2 = 0$. But then

$$f_1 f_2 = (X + g_1(Y))(X - g_1(Y)) = X^2 - g_1(Y)^2,$$

so $g_1(Y)^2 = -Y^2+1$, and $-Y^2+1$ is not a square. On the other hand, the hypersurface $\left\{(x,y) \;\middle|\; x^2+y^2=0\right\}$ is reducible, because X^2+Y^2 factors as $(X-iY)(X+iY)$.

It can often be convenient to rewrite the definition of irreducible spaces in terms of open sets instead of closed sets.

Lemma 1.17. *The following conditions on a topological space S are equivalent to irreducibility.*

- *S is non-empty, and every pair of non-empty open subsets $U_1, U_2 \subseteq S$ have non-empty intersection $U_1 \cap U_2$.*
- *S is non-empty, and every non-empty open subset of S is dense in S.*

Proof. Just manipulation of the topological definition. □

Corollary 1.18. *Let S be a irreducible topological space and $U \subseteq S$ a non-empty open subset. Then U is irreducible, in the subspace topology.*

Lemma 1.17 says that irreducible is a very long way from Hausdorff. The Hausdorff condition says that a space has lots of pairs of disjoint non-empty open subsets, while an irreducible space has none.

Example. We saw that $\mathbb{R}$, with the Euclidean topology, is reducible in many ways.

Corollary 1.18 implies that $\mathbb{A}^1 \setminus \{0\}$ is irreducible, in the subspace topology induced by the Zariski topology on $\mathbb{A}^1$, because it is open in $\mathbb{A}^1$. Compare this to the fact that the hyperbola H is irreducible. This lends support to the heuristic argument that the hyperbola H is irreducible, but it is not a proof. Checking that the subspace topology on $\mathbb{A}^1 \setminus \{0\}$ is the same as the Zariski topology on H would require exactly the same work as the proof that H is irreducible to prove that the Zariski topology on $H \subseteq \mathbb{A}^2$.

1.1.9 Irreducible components

Just like the definition of connected components, we can define the following.

Definition. Let S be a topological space. An **irreducible component** of S is a maximal irreducible subset of S.

Unlike connected components, irreducible components need not be disjoint.

Example. The irreducible components of $\{(x,y) \mid xy = 0\}$ are the lines $x = 0$ and $y = 0$, which intersect in $\{(0,0)\}$.

More generally, the irreducible components of a hypersurface $\mathbb{V}(f)$ correspond to the irreducible factors of f. If $f = f_1^{a_1} \ldots f_m^{a_m}$, where the f_i are distinct irreducible polynomials, then the irreducible components of $\mathbb{V}(f)$ are $\mathbb{V}(f_1), \ldots, \mathbb{V}(f_m)$. Irreducible components have the following key properties.

Proposition 1.19. *Let V be an affine algebraic set. Then*

1. *the union of the irreducible components of V is all of V, and*
2. *V has only finitely many irreducible components.*

Proposition 1.19.1 matches a property of connected components. Proposition 1.19.2 does not apply to the connected components of an arbitrary topological space.

Example. $\mathbb{Z}$ or $\mathbb{Q}$ with the subspace topology from $\mathbb{R}$.

Note. Proposition 1.19.2 does imply that an affine algebraic set has only finitely many connected components for the Zariski topology, because each connected component must be a union of irreducible components.

Proposition 1.19.2 is a finiteness statement, so it is not surprising that it follows from the Noetherian property, the descending chain condition on closed subsets. The key idea in the proof is as follows. If an affine algebraic set is reducible, then we can write it as a union of proper closed subsets. If these subsets are reducible, then we can write them in turn as unions of proper closed subsets. The following lemma says that this process eventually stops. After finitely many steps, we reach irreducible sets.

Lemma 1.20. *Every affine algebraic set can be written as a union of finitely many irreducible closed subsets.*

Proof. Suppose that V is an affine algebraic set which cannot be written as a union of finitely many irreducible closed subsets. Then V must be reducible, otherwise we could write it as a union of one irreducible closed subset. So $V = V_1 \cup W_1$, with V_1 and W_1 proper closed subsets of V. Then V_1 and W_1 cannot both be unions of finitely many irreducible closed subsets, because taking the union of those decompositions would give us V as a union of finitely many irreducible closed subsets. Thus at least one of V_1 and W_1 does not satisfy Lemma 1.20. Without loss of generality, we may suppose that V_1 does not satisfy Lemma 1.20. Then V_1 must be reducible, so we can write $V_1 = V_2 \cup W_2$. We can repeat the argument. At least one of V_2 and W_2 does not satisfy Lemma 1.20, without loss of generality V_2, etc. Thus we build up a chain of closed subsets $V \supset V_1 \supset V_2 \supset \dots$ where all these sets do not satisfy Lemma 1.20, and all the inclusions are strict. This contradicts Lemma 1.10, the descending chain condition for affine algebraic sets. □

In order to prove Proposition 1.19, we want to show that the finitely many irreducible closed subsets in Lemma 1.20 are the irreducible components. There is just one wrinkle. Consider $V = \mathbb{V}(XY)$. The irreducible components are $\mathbb{V}(X)$ and $\mathbb{V}(Y)$. But we could write V as a union of finitely many irreducible closed subsets by saying

$$V = \mathbb{V}(X) \cup \mathbb{V}(Y) \cup \{(0,2)\}.$$

Thus we can always add in extra sets to a decomposition as in Lemma 1.20, where the extra sets are contained in one of the other sets in the decomposition. Of course we can always just throw away these empty sets from the list without changing the union. Let $V = V_1 \cup \dots \cup V_r$, as in Lemma 1.20. By throwing away any V_i which is contained in another V_j, we can assume that $V_i \not\subseteq V_j$ whenever $i \neq j$, and still the union of the V_j's will be V. Subject to this non-redundancy condition, there is only one way to write V as a finite union of irreducible closed subsets and we can prove the following.

Proposition 1.21. *Let V be an affine algebraic set. Write $V = V_1 \cup \dots \cup V_r$, where the V_i are irreducible closed subsets and $V_i \not\subseteq V_j$ for $i \neq j$. Then $V_1, \dots, V_r$ are precisely the irreducible components of V.*

Proof. First we show that each V_i is an irreducible component. By hypothesis, V_i is irreducible. So if V_i is not an irreducible component, it is not a maximal irreducible set and must be contained in a larger irreducible set $W \subseteq V$. But then

$$W = (V_1 \cap W) \cup \dots \cup (V_r \cap W),$$

where $V_1 \cap W, \dots, V_r \cap W$ are closed subsets of W. Because W is irreducible, we must have $W = V_j \cap W$ for some j. Thus $V_i \subseteq W \subseteq V_j$. By the condition $V_i \not\subseteq V_j$ for any $j \neq i$, we must have $i = j$ and $W = V_i$. Thus V_i is an irreducible component of V. Conversely, let C be an irreducible component of V. Then

$$C = (V_1 \cap C) \cup \dots \cup (V_r \cap C).$$

By the same argument as before, the irreducibility of C implies that $C \subseteq V_i$ for some i. Then the maximality of C implies that $C = V_i$. □

The combination of Lemma 1.20 and Proposition 1.21 proves both Proposition 1.19.1 and Proposition 1.19.2.

1.1.10 Primary decomposition of ideals

The irreducible component decomposition of an affine algebraic set can give a geometric understanding of the primary decomposition of ideals in the Noetherian ring $k[X_1, \ldots, X_n]$. However, the irreducible decomposition gives only partial information about the primary decomposition of an ideal, because ideals contain more information than affine algebraic sets. Recall that the algebraic set depends only on the radical of the ideal.

Example. Let $I = \langle X^2, XY \rangle \subseteq k[X, Y]$. Then $\mathbb{V}(I)$ is simply the line $X = 0$, which of course is irreducible. However a primary decomposition of I is

$$I = \langle X \rangle \cap \langle X^2, XY, Y^2 \rangle .$$

Here $\langle X \rangle$ is the ideal of the line $X = 0$, the unique irreducible component of $V = \mathbb{V}(I)$. The ideal $\langle X^2, XY, Y^2 \rangle$ defines the point $\{(0,0)\}$, which is contained in V so is not an irreducible component.

Thus the minimal associated primes of the primary decomposition of I corespond to the irreducible components of $\mathbb{V}(I)$, while non-minimal associated primes correspond to additional smaller sets strictly contained in the irreducible components, called **embedded components**. In scheme theory, we can think of $\mathbb{V}(I)$ as containing multiple copies of these embedded components.

Example. The ideal $I = \langle X^2, XY \rangle$ corresponds, in the world of schemes, to the line $X = 0$ with two copies of the origin.

1.2 Regular and rational maps

1.2.1 Regular functions

Lecture 6
Friday
24/01/20

So far we have only considered algebraic sets as sets, sitting individually. Now we look at functions between them. Just as one uses continuous functions for topological spaces, holomorphic functions for complex manifolds, homomorphisms for groups, etc, so algebraic geometry has its own type of functions, regular functions. Of course, these are given by polynomials.

Definition. Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set. A **regular function** on V is a function $f : V \to k$ such that there exists a polynomial $F \in k[X_1, \ldots, X_n]$ with $f(\underline{x}) = F(\underline{x})$ for all $\underline{x} \in V$.

Note. The polynomial F is not uniquely determined by the function f, since $F, G \in k[X_1, \ldots, X_n]$ determine the same regular function on V if and only if $F - G$ vanishes on V, that is if and only if $F - G \in \mathbb{I}(V)$.

Definition. The regular functions on V form a k-algebra. They can be added and multiplied by each other, and multiplied by scalars in k. This is called the **coordinate ring** of V and denoted $k[V]$.

There is a ring homomorphism $k[X_1, \ldots, X_n] \to k[V]$ which sends a polynomial F to the function $F|_V$ which it defines on V. This homomorphism is surjective and its kernel is $\mathbb{I}(V)$, so

$$k[V] \cong k[X_1, \ldots, X_n] / \mathbb{I}(V) .$$

Example. What are the coordinate rings of the following affine algebraic sets?

- The coordinate ring of $\mathbb{A}^n$ is $k[X_1, \ldots, X_n]$.
- The coordinate ring of a point is k. A regular function on a point is just a single value.
- The coordinate ring of two points $\left\{ x \in \mathbb{A}^1 \;\middle|\; x(x-1) = 0 \right\}$ is $k \times k$. A regular function on two points is determined by two scalars, namely its value on each of the two points. For any pair of values $(a, b) \in k \times k$, one can easily write down a polynomial $f \in k[X]$ such that $f(1) = a$ and $f(0) = b$. Alternatively, one can check algebraically that the map

$$\begin{array}{ccc} k \times k & \longrightarrow & k[X] / \langle X(X-1) \rangle \\ (a, b) & \longmapsto & (a-1)X + b \mod \langle X(X-1) \rangle \end{array}$$

  is a k-algebra isomorphism. This example generalises. If V is a disconnected affine algebraic set, we can write V as a union $V_1 \cup V_2$ of disjoint Zariski closed subsets, and then $k[V] = k[V_1] \times k[V_2]$. On the other hand, if V is reducible but connected, so that the sets V_1 and V_2 are not disjoint, then $k[V]$ is a proper subset of $k[V_1] \times k[V_2]$.

- The coordinate ring of two intersecting lines $\left\{(x,y) \in \mathbb{A}^2 \;\middle|\; xy = 0\right\}$ is

$$\{(f,g) \in k[X] \times k[Y] \mid f(0) = g(0)\}.$$

To prove this, one can also interpret this as

$$k[X,Y]/\langle XY\rangle \cong \left\{ a_0 + \sum_{r=1}^{m} b_r X^r + \sum_{s=1}^{n} c_s Y^s \;\middle|\; a_0, b_1, \ldots, b_m, c_1, \ldots, c_n \in k,\ m,n \in \mathbb{N} \right\}.$$

We can compare these two descriptions by observing that

$$k[X] = \left\{ a_0 + \sum_{r=1}^{m} b_r X^r \right\}, \qquad k[Y] = \left\{ a_0 + \sum_{s=1}^{n} c_s Y^s \right\},$$

and the condition that $f(0) = g(0)$ is equivalent to insisting that these two polynomials have the same constant coefficient a_0. This does not generalise to arbitrary reducible algebraic sets. We may have $V = V_1 \cup V_2$ where V_1 and V_2 are closed subsets, but

$$k[V] \neq \left\{(f,g) \in k[V_1] \times k[V_2] \;\middle|\; f|_{V_1 \cap V_2} = g|_{V_1 \cap V_2}\right\}.$$

There will be an example of this on problem sheet 2.

- The coordinate ring of a hyperbola $\left\{(x,y) \in \mathbb{A}^2 \;\middle|\; xy - 1 = 0\right\}$ is the quotient ring $k[X,Y]/\langle XY-1\rangle$. To describe this more explicitly, note that any term of a two-variable polynomial is

$$a_{r,s}X^rY^s \equiv \begin{cases} a_{r,s}X^{r-s} & r \geq s \\ a_{r,s}Y^{s-r} & s > r \end{cases} \mod \langle XY-1\rangle.$$

Thus every coset in $k[X,Y]/\langle XY-1\rangle$ has a representative of the form

$$\sum_{i=0}^{m} a_i X^i + \sum_{j=1}^{n} a_j Y^j.$$

The polynomials of this form determine different functions on V, so we have written down exactly one representative of each coset. Furthermore, since $XY = 1$ in $k[V]$, we may relabel Y as X^{-1}. Then the multiplication rule will be what the notation leads us to expect. So we can write

$$k[V] = k\left[X, X^{-1}\right] = \left\{ \sum_{j=-n}^{m} a_j X^m \;\middle|\; a_{-n}, \ldots, a_m \in k,\ m,n \in \mathbb{N} \right\}.$$

Lemma 1.22. *An affine algebraic set V is irreducible if and only if $k[V]$ is an integral domain.*

Proof. V is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal in $k[X_1, \ldots, X_n]$. □

1.2.2 Regular maps

A regular function goes from an algebraic set V to the field k. We can also define regular maps, which go from one algebraic set V to another algebraic set W.

Definition. Let $V \subseteq \mathbb{A}^m$ and $W \subseteq \mathbb{A}^n$ be affine algebraic sets. A **regular map** $\phi : V \to W$ is a function $V \to W$ such that there exist polynomials $F_1, \ldots, F_n \in k[X_1, \ldots, X_n]$ such that $\phi(\underline{x}) = (F_1(\underline{x}), \ldots, F_n(\underline{x}))$ for all $\underline{x} \in V$. Regular maps are often called **morphisms**.

Note. In order to check that a given list of polynomials $F_1, \ldots, F_n$ defines a regular map $V \to W$, it is necessary to check that $(F_1(\underline{x}), \ldots, F_n(\underline{x})) \in W$ for every $\underline{x} \in V$. Equivalently, we need to check that the regular functions $F_1|_V, \ldots, F_n|_V \in k[V]$ satisfy the equations $g(F_1|_V, \ldots, F_n|_V) = 0$ in the coordinate ring $k[V]$, for each polynomial $g \in \mathbb{I}(W)$.

Example.

- Let $V \subseteq \mathbb{A}^m$ be an affine algebraic set. For any $n < m$, the projection defined by
$$\begin{array}{rccc} \pi & : & V & \longrightarrow & \mathbb{A}^n \\ & & (x_1, \ldots, x_m) & \longmapsto & (x_1, \ldots, x_n) \end{array}$$
is a regular map.
- A regular function on V is the same thing as a regular map $V \to \mathbb{A}^1$.
- Let $C = \left\{(x, y) \mid y^2 = x^3\right\}$. Then
$$\begin{array}{ccc} \mathbb{A}^1 & \longrightarrow & C \\ t & \longmapsto & \left(t^2, t^3\right) \end{array}$$
is a regular map.
- Consider SL_n, the set of $n \times n$ matrices with determinant one. This is an affine algebraic set in $\mathbb{A}^{n^2}$ because the determinant is a polynomial in the entries of a matrix. The map
$$\begin{array}{ccc} \mathrm{SL}_n & \longrightarrow & \mathrm{SL}_n \\ a & \longmapsto & a^{-1} \end{array}$$
is a regular map. Cramer's rule tells us how to write each entry of a^{-1} as a polynomial in the entries of a divided by $\det a$, and because we are only considering $a \in \mathrm{SL}_n$ we can drop the division by $\det a$.

A regular map $\phi : V \to W$ is a continuous function with respect to the Zariski topology. This is because, if $A \subseteq W$ is a Zariski closed subset defined by polynomials $f_1, \ldots, f_r$, then $\phi^{-1}(A)$ is the zero set
$$\phi^{-1}(A) = \{x \in V \mid (f_1 \circ \phi)(x) = 0,\ \ldots,\ (f_r \circ \phi)(x) = 0\},$$
and therefore $\phi^{-1}(A)$ is a Zariski closed subset of V. In complex analysis, holomorphic is a much stricter condition than continuous in the Euclidean topology, and similarly regular is much stricter than continuous in the Zariski topology. The following fact is very useful.

Lemma 1.23. *Let $\phi, \psi : V \to W$ be regular maps. If there exists a Zariski dense subset $A \subseteq V$ such that $\phi|_A = \psi|_A$, then $\phi = \psi$ on all of V.*

Note. If X and Y are Hausdorff topological spaces, then any continuous maps $X \to Y$ which agree on a dense set must agree everywhere. However Lemma 1.23 does not follow immediately from the fact that regular maps are continuous, because the Zariski topology is not Hausdorff, and is definitely false if we try to generalise it to all continuous maps with respect to the Zariski topology. Thus in order to prove Lemma 1.23, we have to use something special about regular maps as opposed to general continuous maps.

Proof. Write $\phi = (F_1, \ldots, F_m)$ and $\psi = (G_1, \ldots, G_m)$, where $F_1, \ldots, F_m, G_1, \ldots, G_m$ are polynomials. Then $F_i - G_i$ is also a polynomial for each i, and so
$$V' = \{\underline{x} \in V \mid \phi(\underline{x}) = \psi(\underline{x})\} = \{\underline{x} \in V \mid \forall i,\ (F_i - G_i)(\underline{x}) = 0\}$$
is a Zariski closed subset of V. But we know that V' contains A, which is Zariski dense in V. Hence $V' = V$. □

1.2.3 Isomorphisms

Lecture 7
Monday
27/01/20

Definition. A regular map $\phi : V \to W$ is an **isomorphism** if there exists a regular map $\psi : W \to V$ such that $\psi \circ \phi = \mathrm{id}_V$ and $\phi \circ \psi = \mathrm{id}_W$.

Example. If V is the parabola $\left\{(x, y) \mid y - x^2 = 0\right\}$, then the regular map given by
$$\begin{array}{rccc} \phi & : & V & \longrightarrow & \mathbb{A}^1 \\ & & (x, y) & \longmapsto & x \end{array}$$
is an isomorphism because it has an inverse given by
$$\begin{array}{rccc} \psi & : & \mathbb{A}^1 & \longrightarrow & V \\ & & x & \longmapsto & \left(x, x^2\right) \end{array}.$$

Example. On the other hand, if H is the hyperbola $\{(x,y) \mid xy = 1\}$, then the projection

$$\begin{array}{rcl} H & \longrightarrow & \mathbb{A}^1 \\ (x,y) & \longmapsto & x \end{array}$$

is not an isomorphism because it is not surjective so it cannot possibly have an inverse. This is not enough to prove that H is not isomorphic to $\mathbb{A}^1$, because maybe there is some other regular map $H \to \mathbb{A}^1$ which is an isomorphism. We will soon prove that H is not isomorphic to $\mathbb{A}^1$.

Example. Consider the affine algebraic set $W = \left\{(x,y) \;\middle|\; y^2 - x^3 = 0\right\}$. The regular map given by

$$\begin{array}{rcccl} \phi & : & \mathbb{A}^1 & \longrightarrow & W \\ & & t & \longmapsto & \left(t^2, t^3\right) \end{array}$$

is a bijection but it is not an isomorphism. Note that we should expect W not to be isomorphic to $\mathbb{A}^1$ because it has a singularity at the origin. To prove that $\phi : \mathbb{A}^1 \to W$ is not an isomorphism, consider a regular map $\psi : W \to \mathbb{A}^1$. It must be given by a polynomial $g(X,Y) \in k[X,Y]$ and so $(\psi \circ \phi)(t) = \psi\left(t^2, t^3\right)$ is a polynomial in t which can have a constant term and terms of degree two or greater, but no term of degree one. Hence we cannot find ψ such that $(\psi \circ \phi)(t) = t$.

1.2.4 Regular maps and k-algebra homomorphisms

Suppose we have a regular map $\phi : V \to W$ between affine algebraic sets. For each regular function g on W, we get a regular function $\phi^* g$ on V defined by

$$\begin{array}{rcccl} \phi^* & : & k[W] & \longrightarrow & k[V] \\ & & g & \longmapsto & g \circ \phi \end{array}.$$

We call $\phi^* g \in k[V]$ the **pull-back** of $g \in k[W]$. Thus ϕ induces a k-algebra homomorphism $\phi^* : k[W] \to k[V]$.

Note. ϕ^* goes in the opposite direction to ϕ.

If we have two regular maps $\phi : V \to W$ and $\psi : W \to Z$, then we can compose them to get $\psi \circ \phi : V \to Z$. One can easily check that the associated pull-back maps on coordinate rings satisfy

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* : k[Z] \to k[V].$$

For those who know category theory, we say that $V \mapsto k[V]$ is a contravariant functor

$$\{\text{affine algebraic sets}\} \to \{k\text{-algebras}\}.$$

In particular, this tells us that if $\phi : V \to W$ is an isomorphism with inverse $\psi : W \to V$, then $\psi^* \circ \phi^* = \mathrm{id}$ and $\phi^* \circ \psi^* = \mathrm{id}$. Thus if V and W are isomorphic affine algebraic sets, then their coordinate rings $k[V]$ and $k[W]$ are isomorphic as k-algebras.

Example. Now we can prove that the hyperbola H is not isomorphic to $\mathbb{A}^1$, because $k[H] = k\left[X, X^{-1}\right]$ is not isomorphic to $k\left[\mathbb{A}^1\right] = k[X]$. To verify that these k-algebras are not isomorphic, observe that in $k[X]$ the only invertible elements are the scalars, while $k\left[X, X^{-1}\right]$ contains non-scalar invertible elements, such as X.

Example. We can similarly prove that $\mathbb{A}^1$ is not isomorphic to the singular cubic $W = \left\{(x,y) \;\middle|\; y^2 = x^3\right\}$. We saw earlier that $k[W]$ is the ring of polynomials in one variable with no term of degree one, that is

$$k[W] = \left\{ a_0 + \sum_{r=2}^{m} a_r X^r \;\middle|\; a_0, a_2, \ldots, a_m \in k \right\}.$$

To prove that $k[W]$ is not isomorphic to $k\left[\mathbb{A}^1\right] = k[X]$, observe that $k[X]$ is a unique factorisation domain but $k[W]$ is not because $\left\langle X^2 \right\rangle^3 = \left\langle X^3 \right\rangle^2$, and X^2 and X^3 are both irreducible in $k[W]$.

1.2.5 Rational functions

Informally, rational functions are functions on varieties defined by polynomial fractions, for example the function $x \mapsto 1/x$ on $\mathbb{A}^1$. Observe that this is not really a function $\mathbb{A}^1 \to \mathbb{A}^1$ because it is not defined at $x = 0$, but it is a genuine function on the Zariski open subset $\mathbb{A}^1 \setminus \{0\}$. These are analogues of meromorphic functions in complex analysis. Just as with regular functions and regular maps, we first define rational functions, which take values in k, then rational maps, which go into any algebraic set. We make this definition only for irreducible affine algebraic sets because, as we saw in the example of $1/x$, a rational function defines a genuine function on a Zariski open subset of V, and irreducibility guarantees that all open subsets of V are dense in V, so that a function defined on an open subset really is defined almost everywhere on V.

Definition. Let V be an irreducible affine algebraic set. The **function field** of V is the field of fractions of the coordinate ring $k[V]$. We denote this by $k(V)$.

Note. $k[V]$ is an integral domain because V is irreducible, and therefore $k[V]$ has a field of fractions.

Example. The function field of $\mathbb{A}^1$ is $k(X)$, the fraction field of the polynomial ring $k[X]$.

Definition. A **rational function** on V is an element of the function field $k(V)$. Thus a rational function can be written in the form f/g, where f and g are regular functions. There may be many different choices for f and g which define the same rational function f/g.

Definition. We say that a rational function $\phi \in k(V)$ is **regular** at a point $x \in V$ if there exist regular functions $f, g \in k[V]$ such that $\phi = f/g$ and $g(x) \neq 0$.

Thus regular points are precisely the points at which we can assign a value to $\phi(x)$. If $g(x) \neq 0$, then we can define $\phi(x) = f(x)/g(x)$.

Note. We are allowed to choose different fractions f/g representing ϕ at different points $x \in V$, in order to show that those points are regular. The value $\phi(x)$ is independent of which fraction representing ϕ we choose, as long as it has $g(x) \neq 0$.

Example. Consider the algebraic set defined by the equation $XY = ZT$ in $\mathbb{A}^4$. Let $\phi = X/Z \in k(V)$. The defining equation implies that we also have $\phi = T/Y$. Looking at the fraction X/Z shows us that ϕ is regular wherever $Z \neq 0$, and looking at the fraction T/Y shows us that ϕ is regular wherever $Y \neq 0$. On the other hand, ϕ is not regular on the closed subset $Y = Z = 0$. One can verify that there is no other fraction representing ϕ which is non-zero on this closed subset.

Lecture 8
Thursday
30/01/20

Let V be an irreducible affine algebraic set. Let $\phi \in k(V)$ be a rational function.

Definition. The set of points where ϕ is regular is called the **domain of definition** of ϕ, and denoted $\operatorname{dom}\phi$.

This is the set of points where it makes sense to assign a value to $\phi(x)$. For $x \in \operatorname{dom}\phi$, the value $\phi(x)$ is independent of which fraction f/g we choose to represent ϕ, as long as $g(x) \neq 0$.

Lemma 1.24. *The domain of definition of a rational function $\phi \in k(V)$ is a non-empty Zariski open subset of V.*

Proof. Consider the set of all possible fractions f/g with $f, g \in k[V]$ representing $\phi \in k(V)$. The set of points at which ϕ is not regular is the intersection of the Zariski closed sets $\{x \in V \mid g(x) = 0\}$ across all these fractions. Hence the set of points at which ϕ is not regular is a Zariski closed subset of V. The domain of definition is the complement of this set, and therefore is Zariski open. To show that the domain of definition is non-empty, pick a single fraction f/g representing $\phi \in k(V)$. The regular function g is not equal to zero as an element of $k[V]$, by the definition of the field of fractions, so $\{x \in V \mid g(x) = 0\}$ is a proper closed subset of V. The domain of definition contains the complement of this set, namely $\{x \in V \mid g(x) \neq 0\}$, and hence is non-empty. □

Note. Every regular function $f \in k[V]$ is also a rational function $f/1 \in k(V)$, and its domain of definition is all of V.

The converse also holds.

Lemma 1.25. *Let $\phi \in k(V)$ be a rational function whose domain of definition is equal to V. Then ϕ is a regular function on V.*

Proof. Since $\operatorname{dom}\phi = V$, for each point $x \in V$, we can choose regular functions $f_x, g_x \in k[V]$ such that $\phi = f_x/g_x$ and $g_x(x) \neq 0$. Let $I \subseteq k[V]$ denote the ideal generated by the functions g_x. Because $k[V]$ is Noetherian, we can pick finitely many of these functions $g_{x_1}, \ldots, g_{x_m}$ which still generate I. For each $x \in V$, there is some $g_x \in I$ which is non-zero at x. Hence the Zariski closed subset of V defined by $\{x \in V \mid \forall h \in I,\ h(x) = 0\}$ is empty. Then the Nullstellensatz implies that I is all of $k[V]$. In particular, $1 \in I$. Since $I = \langle g_{x_1}, \ldots, g_{x_m}\rangle$, there exist $u_1, \ldots, u_m \in k[V]$ such that $1 = u_1 g_{x_1} + \cdots + u_m g_{x_m}$ in $k[V]$. We can now calculate

$$\phi = (u_1 g_{x_1} + \cdots + u_m g_{x_m})\,\phi = u_1 g_{x_1}\frac{f_{x_1}}{g_{x_1}} + \cdots + u_m g_{x_m}\frac{f_{x_m}}{g_{x_m}} = u_1 f_{x_1} + \cdots + u_m f_{x_m}.$$

Since $u_i, f_{x_i} \in k[V]$, so is ϕ. Note that it might appear that we have only proved the above equation $\phi = u_1 f_{x_1} + \cdots + u_m f_{x_m}$ on a Zariski open subset of V, namely the intersections of the domains of definition of $f_{x_1}/g_{x_1}, \ldots, f_{x_m}/g_{x_m}$. Because V is irreducible, this open subset must be dense, but the subset where an equation of polynomials holds is closed, so it is equal to all of V. □

1.2.6 Rational maps

Let $V \subseteq \mathbb{A}^m$ and $W \subseteq \mathbb{A}^n$ be irreducible affine algebraic sets.

Definition. A **rational map** $\phi : V \dashrightarrow W$ is an n-tuple of rational functions $\phi_1, \ldots, \phi_n \in k(V)$ such that, for every point $x \in V$ where $\phi_1, \ldots, \phi_n$ are all regular, the point $(\phi_1(x), \ldots, \phi_n(x))$ is in W.

We use the broken arrow symbol instead of the usual arrow because a rational map is not a function on V in the usual set-theoretic sense. It only defines a genuine function $U \to W$, where U is the domain of definition of ϕ. This is defined as follows.

Definition. The **domain of definition** of a rational map $\phi : V \dashrightarrow W$ is the intersection of the domains of definition of the component rational functions $(\phi_1, \ldots, \phi_n)$.

The two lemmas we proved for rational functions also hold for rational maps. The domain of definition of a rational map $\phi : V \dashrightarrow W$ is a non-empty Zariski open subset of V, and if a rational map is regular everywhere then it is a regular map. In order to prove that the domain of definition of a rational map is non-empty, we have to use the fact that V is irreducible, and therefore every open subset of V is dense.

Example. An important example of a rational map is the projection from a point onto a hyperplane. Let H be a hyperplane in $\mathbb{A}^n$, that is a set defined by a single linear equation. Let p be a point in $\mathbb{A}^n \setminus H$. For simplicity, we shall assume that p is the origin and that

$$H = \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_n = 1\},$$

since we could always reduce to this case by a suitable change of coordinates. Let us write H_p for the hyperplane through p parallel to H, that is

$$H_p = \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_n = 0\}.$$

For each point $x \in \mathbb{A}^n \setminus H_p$, let L_x denote the line which passes through p and x. Since $x \notin H_p$, L_x intersects H in exactly one point. Call this point $\phi(x)$. We can write this algebraically as

$$\begin{array}{rccc} \phi & : & \mathbb{A}^n & \dashrightarrow & H \\ & & (x_1, \ldots, x_n) & \longmapsto & \left(\dfrac{x_1}{x_n}, \ldots, \dfrac{x_{n-1}}{x_n}, 1\right) \end{array},$$

and so ϕ is a rational map. This map is called the **projection from p onto H**. We have $\operatorname{dom}\phi = \mathbb{A}^n \setminus H_p$. Note that we have not proved this, because we have not proved that there is no other list of fractions which define the same rational map but have non-zero denominators at points in H_p. One can prove this. For any affine algebraic set $V \subseteq \mathbb{A}^n$ such that $V \not\subseteq H_p$, we can restrict ϕ to get a rational map $V \dashrightarrow H$. Note that p might be in V, or it might not.

Example. Let V be the circle $\{(x,y) \mid x^2+y^2=1\}$. Consider the projection from the point $p=(1,0)$ on to the line $x=0$. This is a rational map with the formula

$$\begin{array}{rccc} \pi & : & V & \dashrightarrow & \mathbb{A}^1 \\ & & (x,y) & \longmapsto & \dfrac{y}{1-x} \end{array} .$$

We can see geometrically that this projection induces a bijection between the circle, excluding p, and the line, at least for real points. If we compute the formula for the inverse map, we get

$$\begin{array}{rccc} \psi & : & \mathbb{A}^1 & \dashrightarrow & V \\ & & t & \longmapsto & \left(\dfrac{t^2-1}{t^2+1}, \dfrac{2t}{t^2+1}\right) \end{array} ,$$

a well-known parameterisation of the circle. Thus we see that the inverse is a rational map. Note that ψ is not regular at $t=\pm i$. We do not see this on the picture, which only shows the real points.

We would like to define formally what it means to say that the rational maps π and ψ are inverse to each other, taking into account that they are not true functions between the sets V and $\mathbb{A}^1$ because they are not regular everywhere. These maps are inverses in that composing them, either way round, gives the identity, if we ignore the points where the maps are not regular.

1.2.7 Birational equivalences

Lecture 9
Friday
31/01/20

In order to do this, we first define what it means to compose rational maps. But it does not always make sense to compose rational maps. In order to rigorously define composition of rational maps, we need to notice that sometimes the set of points where a composite map is undefined is everywhere and exclude that situation.

Example. Consider the rational map defined by

$$\begin{array}{rccc} \xi & : & \mathbb{A}^2 & \dashrightarrow & \mathbb{A}^1 \\ & & (x,y) & \longmapsto & \dfrac{1}{1-x^2-y^2} \end{array} .$$

This map is not regular anywhere on the circle V, and hence it does not make sense to try to define the composite map $\xi \circ \psi : \mathbb{A}^1 \dashrightarrow \mathbb{A}^1$, since it is not defined anywhere.

This problem can occur because the image of ψ is not dense in $\mathbb{A}^2$. So to rule it out this problem, we make the following definition of dominant rational maps.

Definition. The **image** of a rational map $\phi : V \dashrightarrow W$ is the set of points

$$\{\phi(x) \in W \mid x \in \operatorname{dom}\phi\} .$$

A rational map is **dominant** if its image is Zariski dense in W.

Example. ψ from the end of the previous lecture is dominant if we consider it as a rational map $\mathbb{A}^1 \dashrightarrow V$ but it is not dominant if we consider it as a rational map $\mathbb{A}^1 \dashrightarrow \mathbb{A}^2$. This is like surjectivity, since whether a function is surjective or not depends on what codomain you declare it to have.

Let V, W, T be irreducible affine algebraic sets. If $\phi : V \dashrightarrow W$ is a dominant rational map and $\psi : W \dashrightarrow T$ is a rational map, where ψ is not required to be dominant, then it makes sense to compose them because we know that $\operatorname{dom}\psi$ is a Zariski open subset of W, while $\operatorname{Im}\phi$ is a Zariski dense subset of W and so $\operatorname{dom}\psi \cap \operatorname{Im}\phi \neq \emptyset$. Thus there are at least some points where $\psi \circ \phi$ is defined. One can check, by writing out ψ in terms of fractions of polynomials, then substituting in fractions of polynomials representing ϕ, that $\psi \circ \phi$ is a rational map $V \dashrightarrow T$.

Definition. Rational maps $\phi : V \dashrightarrow W$ and $\psi : W \to V$ are **rational inverses** if both are dominant and $\phi \circ \psi = \mathrm{id}_W$ and $\psi \circ \phi = \mathrm{id}_V$, everywhere these composite rational maps are well-defined. A rational map $\phi : V \dashrightarrow W$ is a **birational equivalence** if it is dominant and has a rational inverse. We say that irreducible algebraic sets V and W are **birational**, or **birationally equivalent**, if there exists a birational equivalence $V \dashrightarrow W$.

Example. Our example from the previous lecture showed that the circle is birational to $\mathbb{A}^1$.

Example. Another example is the cuspidal cubic $W = \{(x,y) \mid y^2 = x^3\}$. This is also birational to $\mathbb{A}^1$, as shown by the rational maps

$$\begin{array}{rcl} W & \dashrightarrow & \mathbb{A}^1 \\ (x,y) & \longmapsto & \dfrac{y}{x} \\ \left(t^2,t^3\right) & \longmapsfrom & t \end{array}.$$

Birationally equivalent affine algebraic sets look the same almost everywhere.

Example. The cuspidal cubic is the same as the affine line everywhere except at the origin.

Example. $\mathbb{A}^1$ is not birationally equivalent to $\mathbb{A}^2$ or to an elliptic curve $\{(x,y) \mid y^2 = f(x)\}$ where f is a cubic polynomial with no repeated roots. We will prove this later in the course once we have more tools.

1.2.8 Dominant rational maps and k-field homomorphisms

If $\phi : V \dashrightarrow W$ is a dominant rational map, then we can use it to pull back rational functions from W to V, just like we earlier used regular maps to pull back regular functions. We get a k-homomorphism of fields defined by

$$\begin{array}{rcccc} \phi^* & : & k(W) & \longrightarrow & k(V) \\ & & g & \longmapsto & g \circ \phi \end{array}.$$

A **k-homomorphism** means that ϕ^* restricts to the identity on the copies of k which are contained in $k(W)$ and $k(V)$, namely the constant functions. If ϕ is a birational equivalence, then ϕ^* is a k-isomorphism of fields.

1.3 Equivalence of algebra and geometry

1.3.1 From algebra homomorphisms to regular maps

We have seen that each regular map $f : V \to W$ induces a k-algebra homomorphism $f^* : k[W] \to k[V]$, and that each dominant rational map $\phi : V \dashrightarrow W$ induces a k-field homomorphism $\phi^* : k(W) \to k(V)$. We can also carry out these constructions in the reverse direction. Starting with a k-algebra homomorphism and getting a regular map, or similarly for rational maps. Observe that if $f : V \to W$ is a regular map and $W \subseteq \mathbb{A}^n$, we can recover f from $f^* : k[W] \to k[V]$ by taking the coordinate functions $X_1, \ldots, X_n \in k[W]$ on W and pulling them back to get $f_1 = f^*(X_1), \ldots, f_n = f^*(X_n) \in k[V]$. These are precisely the regular functions on V such that $f = (f_1, \ldots, f_n)$. We generalise this procedure for any k-algebra homomorphism $\alpha : k[W] \to k[V]$. Starting from an arbitrary k-algebra homomorphism $\alpha : k[W] \to k[V]$, we define a regular map $s : V \to W$ by

$$s = (\alpha(X_1), \ldots, \alpha(X_n)).$$

Here $\alpha(X_1), \ldots, \alpha(X_n) \in k[V]$. Then $\alpha = s^* : k[W] \to k[V]$. Thus every k-algebra homomorphism $k[W] \to k[V]$ is the pull-back by some regular map $V \to W$. We conclude the following.

Proposition 1.26. *$\phi \mapsto \phi^*$ is a bijection*

$$\{\text{regular maps } V \to W\} \to \{k\text{-algebra homomorphisms } k[W] \to k[V]\}.$$

Corollary 1.27. *Affine algebraic sets V and W are isomorphic if and only if their coordinate rings $k[V]$ and $k[W]$ are isomorphic as k-algebras.*

The moral is that if we only care about affine algebraic sets up to isomorphism, then coordinate rings contain exactly the same information as algebraic sets themselves. In the language of category theory, the functor $V \to k[V]$ is fully faithful. One can do the same thing for rational maps.

Proposition 1.28. *$\phi \mapsto \phi^*$ is a bijection*

$$\{\text{dominant rational maps } V \dashrightarrow W\} \to \{k\text{-field homomorphisms } k(W) \to k(V)\}.$$

Corollary 1.29. *Irreducible affine algebraic sets V and W are birationally equivalent if and only if their function fields $k(V)$ and $k(W)$ are k-isomorphic.*

1.3.2 Dictionary between algebraic subsets and ideals

Can we do something similar with Zariski closed subsets of V, and work them out from the algebra of $k[V]$? Suppose that $V \subseteq \mathbb{A}^n$. In $\mathbb{A}^n$, the Nullstellensatz tells us that the functions $\mathbb{I}$ and $\mathbb{V}$ are bijections

$$\left\{ \text{ Zariski closed subsets of } \mathbb{A}^n \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ radical ideals in } k[X_1, \ldots, X_n] \right\}.$$

Since $\mathbb{I}$ and $\mathbb{V}$ reverse the direction of inclusions, we deduce that they restrict to bijections

$$\left\{ \text{ Zariski closed subsets of } V \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ radical ideals in } k[X_1, \ldots, X_n] \text{ containing } \mathbb{I}(V) \right\}.$$

We know that $k[V] \cong k[X_1, \ldots, X_n]/\mathbb{I}(V)$. It is a basic algebraic fact that

$$\left\{ \text{ ideals in } k[X_1, \ldots, X_n] \text{ containing } \mathbb{I}(V) \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ ideals in } k[X_1, \ldots, X_n]/\mathbb{I}(V) \right\}.$$

Under this correspondence, radical ideals on one side correspond to radical ideals on the other side and similarly for prime ideals. We conclude that the natural maps are bijections

$$\left\{ \text{ Zariski closed subsets of } V \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ radical ideals in } k[V] \right\},$$

and

$$\left\{ \text{ irreducible Zariski closed subsets of } V \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ prime ideals in } k[V] \right\}.$$

Can we describe the points of an affine algebraic set V in terms of the algebra of $k[V]$? The points of V are the smallest non-empty Zariski closed subsets. Since the bijection between Zariski closed subsets and ideals reverses direction of inclusion, they correspond to maximal ideals, so

$$\left\{ \text{ points of } V \right\} \quad \leftrightsquigarrow \quad \left\{ \text{ maximal ideals in } k[V] \right\}.$$

Lecture 10
Monday
03/02/20

Lecture 10 is a problems class.

Lecture 11
Thursday
06/02/20

1.3.3 Reduced finitely generated k-algebras

We have seen that $V \mapsto k[V]$ leads to bijections on maps between affine algebraic sets. To fully understand the relationship between affine algebraic sets and k-algebras, there is one more question to answer. Which k-algebras can occur as $k[V]$ where V is an affine algebraic set? We write down some algebraic properties which obviously hold for $A = k[V]$, the coordinate ring of an affine algebraic set V.

- A is finitely generated, because if $V \subseteq \mathbb{A}^n$ then A is generated by the coordinate functions $X_1, \ldots, X_n$.
- A is reduced, meaning that if $f \in A$ and $f^k = 0$ for some $k > 0$, then $f = 0$. This is because A is a ring of functions in the usual set-theoretic sense. If $f^k = 0$ then $f(x)^k = 0$ for all $x \in V$, so $f(x) = 0$ for all $x \in V$.

Using the Nullstellensatz, we can prove that these properties are enough to characterise the k-algebras which are coordinate rings of affine algebraic sets.

Proposition 1.30. *Let A be a finitely generated reduced k-algebra. Then there exists an affine algebraic set V such that $k[V] \cong A$.*

Proof. Pick a finite set $f_1, \ldots, f_n \in A$ which generates A as a k-algebra. We can define a homomorphism

$$\begin{array}{rccc} \alpha & : & k[X_1, \ldots, X_n] & \longrightarrow & A \\ & & (X_1, \ldots, X_n) & \longmapsto & (f_1, \ldots, f_n) \end{array}.$$

Let $I = \operatorname{Ker} \alpha$ and let $V = \mathbb{V}(I) \subseteq \mathbb{A}^n$. The homomorphism α is surjective because $f_1, \ldots, f_n$ generate A, and so $A \cong k[X_1, \ldots, X_n]/I$. Thus $k[X_1, \ldots, X_n]/I$ is a reduced k-algebra. It follows that I is a radical ideal. Hence the Nullstellensatz tells us that $I = \mathbb{I}(V)$. Thus

$$k[V] \cong k[X_1, \ldots, X_n]/\mathbb{I}(V) \cong k[X_1, \ldots, X_n]/I \cong A.$$

□

1.3.4 The notion of an affine variety

Often in mathematics, it is convenient to consider objects only up to isomorphism.

Example. One might talk about the group with seven elements, ignoring the fact that there are many different groups with seven elements because they are all isomorphic to each other, and therefore they all behave in the same ways.

Similarly, in algebraic geometry we often want to consider affine algebraic sets up to isomorphism. But affine algebraic sets are always defined in a concrete way. They are a subset of some specific affine space $\mathbb{A}^n$. It is as if we had defined all finite groups to be subgroups of a symmetric group $\mathcal{S}_n$. And we have seen that affine algebraic sets can be isomorphic even when they appear to be quite different as subsets of affine space.

Example. The line $\mathbb{A}^1$ is isomorphic to the parabola $\mathbb{V}\left(Y - X^2\right) \subseteq \mathbb{A}^2$.

Thus it is useful to use different terminology. We talk about affine algebraic sets when we mean subsets of $\mathbb{A}^n$, and we talk about **affine varieties** when we mean an affine algebraic set up to isomorphism, forgetting its embedding into $\mathbb{A}^n$. Proposition 1.30 is more naturally stated in terms of affine varieties rather than affine algebraic sets. In the proof we had to choose a generating set for A, for which there is no distinguished choice. Different choices of generating set would lead to isomorphic affine algebraic sets, but embedded differently into affine space. So it is better to say that each finitely generated reduced k-algebra A is the coordinate ring of some affine variety V, with no distinguished choice of embedding into $\mathbb{A}^n$. I mentioned this philosophy about affine varieties before, and I will mention it again after we have defined quasi-projective varieties. For those who know some fancy categorical language, we can sum up all the results on the equivalence between affine geometric objects and their coordinate rings by saying that $V \mapsto k[V]$ is an equivalence of categories

$$\{\text{affine varieties over } k\} \to \{\text{reduced finitely generated } k\text{-algebras}\}^{\text{op}},$$

where the superscript op indicates that the directions of morphisms are reversed. Let A be a reduced finitely generated k-algebra and V an affine variety such that $A \cong k[V]$. How can we work out the geometry of V from the algebra of A? If we choose an embedding of V into $\mathbb{A}^n$, then we get an isomorphism $k[X_1, \ldots, X_n]/\mathbb{I}(V) \to A$. We conclude that

$$\begin{aligned}
\left\{ \text{ Zariski closed subsets of } V \right\} &\quad \leftrightsquigarrow \quad \left\{ \text{ radical ideals in } A \right\}, \\
\left\{ \text{ irreducible Zariski closed subsets of } V \right\} &\quad \leftrightsquigarrow \quad \left\{ \text{ prime ideals in } A \right\}, \\
\left\{ \text{ points of } V \right\} &\quad \leftrightsquigarrow \quad \left\{ \text{ maximal ideals in } A \right\}.
\end{aligned}$$

1.3.5 The weak and strong Nullstellensatz

Now we aim to prove Hilbert's Nullstellensatz. There are many different proofs, all of which require some difficult algebra. We will roughly follow the method in Shafarevich appendix A, which incorporates the hard algebra into one statement which we can quote, and then do the rest as geometrically as possible. Recall the statement of Hilbert's Nullstellensatz, Theorem 1.11, also called the strong Nullstellensatz. In order to prove this, we will first prove a weaker version, which is called the weak Nullstellensatz, then use that to deduce the strong Nullstellensatz.

Theorem 1.31 (Weak Nullstellensatz)**.** *Let I be an ideal in the polynomial ring $k[X_1, \ldots, X_n]$ over an algebraically closed field k. If $\mathbb{V}(I) = \emptyset$, then $I = k[X_1, \ldots, X_n]$.*

This is a statement about the existence of solutions to polynomial equations, so it is necessary to require k to be algebraically closed.

Example. To show that it fails when k is not algebraically closed, consider the ideal $\left\langle X^2 + Y^2 + 1 \right\rangle$ in $\mathbb{R}[X, Y]$. This ideal is not the full polynomial ring, but there are no real solutions to the equation $x^2 + y^2 + 1 = 0$.

Note. The strong Nullstellensatz easily implies the weak Nullstellensatz. If $\mathbb{V}(I) = \emptyset$ then the strong Nullstellensatz tells us that $\operatorname{rad} I = \mathbb{I}(\emptyset) = k[X_1, \ldots, X_n]$. In particular, $1 \in \operatorname{rad} I$ but then $1 \in I$ so $I = k[X_1, \ldots, X_n]$.

Proof of Theorem 1.11. We use a method called the Rabinowitsch trick, introducing an extra variable. Let I be an ideal in $k[X_1,\dots,X_n]$ and let $V=\mathbb{V}(I)\subseteq\mathbb{A}^n$. It is easy to see that $\operatorname{rad} I\subseteq\mathbb{I}(V)$. Thus we have to prove that $\mathbb{I}(V)\subseteq\operatorname{rad} I$. Let $f\in\mathbb{I}(V)$. Define a new polynomial g with an extra variable Y by

$$g(X_1,\dots,X_n,Y)=f(X_1,\dots,X_n)\cdot Y-1.$$

Let J be the ideal in $k[X_1,\dots,X_n,Y]$ generated by I and g, and consider the affine algebraic set $W=\mathbb{V}(J)\subseteq\mathbb{A}^{n+1}$. Every point $(x_1,\dots,x_n,y)\in W$ satisfies $f(x_1,\dots,x_n)\neq 0$, in order for there to exist some y such that $f(x_1,\dots,x_n)\,y-1=0$. This is generalising the fact that the hyperbola projects down to $\mathbb{A}^1\setminus\{0\}$. Since $I\subseteq J$, points $(x_1,\dots,x_n,y)$ of W also satisfy $(x_1,\dots,x_n)\in V$. Therefore, if $\pi:\mathbb{A}^{n+1}\to\mathbb{A}^n$ is the projection map, forgetting the extra Y coordinate, then

$$\pi(W)\subseteq\{(x_1,\dots,x_n)\in V\mid f(x_1,\dots,x_n)\neq 0\}.$$

Since $f\in\mathbb{I}(V)$, the set on the right is empty. Thus $\pi(W)=\emptyset$. This implies that W itself is empty. Therefore, by the weak Nullstellensatz, $J=k[X_1,\dots,X_n,Y]$. In particular, $1\in J$ and thus $1=a+bg$ for some $a\in I\cdot k[X_1,\dots,X_n,Y]$ and $b\in k[X_1,\dots,X_n,Y]$. Expanding out a and b as sums over powers of Y,

$$a=\sum_{j\geq 0}a_jY^j,\qquad b=\sum_{j\geq 0}b_jY^j,\qquad a_j\in I,\qquad b_j\in k[X_1,\dots,X_n].$$

The equation $1=a+bg$ can be expanded and rearranged to give

$$1=a_0-b_0+\sum_{j\geq 1}(a_j+b_{j-1}f-b_j)\,Y^j.$$

Looking at the terms of degree zero in Y gives $b_0=a_0-1\in I-1$, then terms of degree one in Y gives $b_1=a_1+b_0f\in I-f$, using $a_1\in I$ and $b_0\in I-1$. Continuing by induction on j, these imply that

$$b_j=a_j+b_{j-1}f\in I-f^j,\qquad j\geq 0,$$

where $I-f^j$ means the coset $\{t-f^j\mid t\in I\}$. But b is a polynomial, so $b_j=0$ once j gets large enough. Thus for some j, we get $0\in I-f^j$, that is $f^j\in I$. This proves that $f\in\operatorname{rad} I$. □

Lecture 12
Friday
07/02/20

We can restate the weak Nullstellensatz in elementary terms as, if $f_1,\dots,f_m\in k[X_1,\dots,X_n]$ are a finite set of polynomials, and the ideal I which they generate is not the whole polynomial ring, then there exists a common solution $(x_1,\dots,x_n)\in k^n$ to the equations

$$f_1(x_1,\dots,x_n)=0,\qquad,\dots,\qquad f_m(x_1,\dots,x_n)=0.$$

We prove this in two steps.

Step 1. There exists a larger field K containing k such that these equations have a common solution in K^n.

Step 2. If the equations have a common solution in K^n, then they also have a common solution in k^n.

1.3.6 Finding a solution in a bigger field

The proof of step 1 is fairly short, and relies on Zorn's lemma.

Lemma 1.32. *Let $f_1,\dots,f_m$ be polynomials in $k[X_1,\dots,X_n]$, such that the ideal $I=\langle f_1,\dots,f_m\rangle$ is not equal to $k[X_1,\dots,X_n]$. Then there exists a field K which is a finitely generated extension of k such that the equations $f_1=\dots=f_m=0$ have a common solution $(x_1,\dots,x_n)\in K^n$.*

Because $I\neq k[X_1,\dots,X_n]$, we can use Zorn's lemma to show that I is contained in some maximal ideal $M\subseteq k[X_1,\dots,X_n]$. This is a natural way to start. We are trying to show that $\mathbb{V}(I)$ has a point, and last time we saw that points in $\mathbb{V}(I)$ correspond to maximal ideals in $k[X_1,\dots,X_n]$ containing I. We cannot just quote the correspondence from the previous lecture because we used the Nullstellensatz in proving that correspondence, but this justifies why obtaining a maximal ideal is a good first step.

Proof. Let $K=k[X_1,\dots,X_n]/M$. Let $x_1,\dots,x_n$ denote the images of $X_1,\dots,X_n$ in K. Then K is a field because M is a maximal ideal, and it is finitely generated as an extension of k because it is generated by $x_1,\dots,x_n$. Since $f_j(X_1,\dots,X_n)\in I\subseteq M$, we get that $f_j(x_1,\dots,x_n)=0$ in K for each j. Thus $(x_1,\dots,x_n)$ is the required common solution to $f_1,\dots,f_m$ in K^n. □

1.3.7 Shrinking the field required

Before proving step 2, we begin by quoting an algebraic result.

Lemma 1.33. *Let k be an algebraically closed field and let K be a finitely generated extension field of k. Then there exist $t_1, \ldots, t_d, u \in K$ such that*

- $K = k(t_1, \ldots, t_d, u)$,
- *$t_1, \ldots, t_d$ are algebraically independent over k, that is there is no non-zero polynomial in d variables with coefficients in k whose value at $(t_1, \ldots, t_d)$ is zero, and*
- *u is algebraic over $k(t_1, \ldots, t_d)$, that is there exists a non-zero polynomial in one variable with coefficients in the field $k(t_1, \ldots, t_d)$ which is zero at u.*

Proof. This follows from the primitive element theorem in field theory. For a full proof, see Proposition A.7 in the appendix of Shafarevich basic algebraic geometry. □

Lemma 1.33 has a nice geometric interpretation. Every finitely generated extension of k is isomorphic to the field of fractions of a hypersurface. We need to use the Nullstellensatz to prove this geometric interpretation, so that is postponed until after we have finished the proof of the Nullstellensatz.

Theorem 1.34. *Let k be an algebraically closed field and let K be a finitely generated extension field of k. Let $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Suppose there exists a common solution $(x_1, \ldots, x_n) \in K^n$ to the equations $f_1 = \cdots = f_m = 0$. Then there exists a common solution $(y_1, \ldots, y_n) \in k^n$ to the equations $f_1 = \cdots = f_m = 0$.*

Proof. Write $K = k(t_1, \ldots, t_d, u)$ as in Lemma 1.33. Let $K' = k(t_1, \ldots, t_d)$. Because $t_1, \ldots, t_d$ are algebraically independent, we can identify K' with $k(T_1, \ldots, T_d)$, the field of fractions of the polynomial ring $k[T_1, \ldots, T_d]$. This will allow us to substitute a vector $\underline{z} \in k^d$ into an element $\alpha \in K'$ and get out an element $\alpha(\underline{z}) \in k$, as long as the denominator of α does not vanish at $\underline{z}$. We use two facts about the finite algebraic extension K/K'.

Fact 1. There exists a minimal polynomial $p(U) \in K'[U]$ for u. That is, $p(u) = 0$, p has leading coefficient one, and p divides every other polynomial $q(U) \in K'[U]$ such that $q(u) = 0$.

Fact 2. Every element of K can be written in the form $a(u)$ for some polynomial $a(U) \in K'[U]$.

The idea of the proof is to consider the almost hypersurface

$$H = \left\{(z_1, \ldots, z_d, s) \in k^{d+1} \;\middle|\; p(z_1, \ldots, z_d, s) = 0\right\}.$$

The almost is because p is not a polynomial in $k[T_1, \ldots, T_d, U]$ but rather may have denominators, so we have to ignore the places where these denominators vanish. Then we construct a rational map $\phi : H \dashrightarrow \mathbb{V}(f_1, \ldots, f_m)$. The domain of definition of ϕ is an open subset of an almost hypersurface, and we can easily check that this is non-empty. Then a point in the image of ϕ gives us a point in $\mathbb{V}(f_1, \ldots, f_m)$, as desired. In particular, we apply fact 2 to $x_1, \ldots, x_n \in K$, our common solution to $f_1 = \cdots = f_m = 0$, so we can write $x_i = a_i(u)$ where $a_i(U) \in K'[U]$. In the informal outline, these $a_i \in k(T_1, \ldots, T_d)[U]$ define a rational map $\phi : H \dashrightarrow \mathbb{A}^n$. Next we check that the image of this rational map is contained in $\mathbb{V}(f_1, \ldots, f_m)$. We know that $(x_1, \ldots, x_n)$ is a common solution to the polynomials $f_1, \ldots, f_m$. Hence

$$f_j(a_1(u), \ldots, a_n(u)) = 0 \in K, \qquad j = 1, \ldots, m.$$

In other words, the single-variable polynomial $f_j(a_1(U), \ldots, a_n(U)) \in K'[U]$ has u as a root. Therefore, fact 1 tells us that this polynomial is divisible by $p(U)$. Thus there exist polynomials $q_1, \ldots, q_m \in K'[U]$ such that

$$f_j(a_1(U), \ldots, a_n(U)) = q_j(U)\, p(U) \in K'[U], \qquad j = 1, \ldots, m. \tag{1}$$

Now, if $(z_1, \ldots, z_d, s) \in k^{d+1}$ satisfies $p(z_1, \ldots, z_d, s) = 0$, then (1) implies that

$$f_j(a_1(z_1, \ldots, z_d, s), \ldots, a_n(z_1, \ldots, z_d, s)) = 0, \qquad j = 1, \ldots, m,$$

so long as all the denominators involved are non-zero. Thus we just have to find $(z_1, \ldots, z_d, s)$ where all these denominators will be non-zero. So consider the polynomials

$$p(U), a_i(U), q_j(U) \in K'[U].$$

Their coefficients are elements of the field K' which we are identifying with the field of fractions $k(T_1, \ldots, T_d)$. Let $\sigma \in k[T_1, \ldots, T_d]$ denote the product of the denominators of all these fractions. Because the denominator of a fraction is never zero, σ is not the zero polynomial in $k[T_1, \ldots, T_d]$. Therefore, there exists $(s_1, \ldots, s_d) \in k^d$ such that $\sigma(s_1, \ldots, s_d) \neq 0$. Then the denominators of the coefficients of p, a_i, q_j do not vanish at $s_1, \ldots, s_d$, so we can substitute $(s_1, \ldots, s_d)$ into each of these coefficients, as elements of K', and get out values in k. Thus we get new polynomials

$$\widetilde{p}(U), \widetilde{a_i}(U), \widetilde{q_j}(U) \in k[U].$$

The leading coefficient of $\widetilde{p}(U)$ is one, which is unchanged by this process. So $\widetilde{p}(U)$ has the same degree as $p(U)$. In particular $\widetilde{p}(U)$ is not a constant polynomial. Hence as k is algebraically closed, there exists $s \in k$ such that $\widetilde{p}(s) = 0$. Let $y_i = \widetilde{a_i}(s) \in k$. Then (1) tells us that

$$f_j(y_1, \ldots, y_n) = \widetilde{q_j}(s)\,\widetilde{p}(s), \qquad j = 1, \ldots, m.$$

But we chose s such that $\widetilde{p}(s) = 0$, and so we conclude that $(y_1, \ldots, y_n) \in k^n$ is a common solution to $f_1 = \cdots = f_m = 0$. □

Combining Lemma 1.33 and Theorem 1.34 proves the weak Nullstellensatz.

1.3.8 Hypersurfaces and birational equivalence

Now we prove the geometrical interpretation of Lemma 1.33.

Proposition 1.35. *Let K be a finitely generated extension of k. Then there exists an irreducible hypersurface $H \subseteq \mathbb{A}^{d+1}$ for some d such that K is isomorphic to the field of functions $k(H)$.*

Corollary 1.36. *Let $V \subseteq \mathbb{A}^n$ be an irreducible affine algebraic set. Then there exists an irreducible hypersurface $H \subseteq \mathbb{A}^{d+1}$ for some d such that V is birationally equivalent to H.*

Corollary 1.36 tells us that, even if V is a complicated algebraic set defined by many equations, provided we only care about properties of V which are preserved by birational equivalence, we can replace V by a simpler set defined by just one equation, that is a hypersurface.

Note. It is not true that every irreducible affine algebraic set is isomorphic to a hypersurface.

Proof of Proposition 1.35. Write $K = k(t_1, \ldots, t_d, u)$ as in Lemma 1.33, and let $K' = k(t_1, \ldots, t_d)$. Because u is algebraic over K', let $p(U) \in K'[U]$ be the minimal polynomial of u over K'. Each coefficient of $p(U)$ is a fraction whose numerator and denominator are polynomials in $t_1, \ldots, t_d$. We can multiply up by a suitable element of $k[t_1, \ldots, t_d]$ to clear the denominators, and also replace $t_1, \ldots, t_d$ by indeterminates $T_1, \ldots, T_d$ to get a polynomial $g \in k[T_1, \ldots, T_d, U]$ such that $g(t_1, \ldots, t_d, u) = 0$ in the field K. Assuming we multiplied up by a lowest common denominator for the coefficients of p, g is irreducible. Let H be the hypersurface in $\mathbb{A}^{d+1}$ defined by the polynomial g. Because g is irreducible, it generates a radical ideal in $k[X_1, \ldots, X_n]$ and so the strong Nullstellensatz implies that $\mathbb{I}(H) = \langle g \rangle$. Thus the coordinate ring is given by

$$k[H] = k[T_1, \ldots, T_d, U] / \langle g \rangle.$$

There is a k-algebra homomorphism

$$\begin{array}{rccc} \alpha & : & k[T_1, \ldots, T_d, U] & \longrightarrow & K \\ & & (T_1, \ldots, T_d, U) & \longmapsto & (t_1, \ldots, t_d, u) \end{array}.$$

A little algebra, using Gauss' lemma, shows that the kernel of α is generated by g, so α induces an injection $k[H] \hookrightarrow K$. Furthermore, the image of α generates K as a field, so α induces an isomorphism from the fraction field of $k[H]$ to K. The fraction field of $k[H]$ is the function field $k(H)$. Thus we have shown that $k(H) \cong k(V)$. By Corollary 1.29, this implies that V is birationally equivalent to H. □

Proof of Corollary 1.36. Apply Proposition 1.35 to the function field $K = k(V)$. □

2 Projective varieties

2.1 Projective algebraic sets

2.1.1 Projective space

Lecture 13
Monday
10/02/20

Projective space consists of affine space together with points at infinity, one for each direction. The purpose for adding extra points is that it avoids special cases where a point disappears to infinity.

Example. A pair of parallel lines do not intersect in affine space but they do intersect at a point at infinity in projective space.

Definition. Projective n-space, $\mathbb{P}^n$, is the set of lines through the origin in $\mathbb{A}^{n+1}$.

A convenient way to label points in $\mathbb{P}^n$ is via homogeneous coordinates. These are just coordinates in $k^{n+1} \setminus \{(0,\dots,0)\}$. Any sequence of coordinates $\underline{x} \in k^{n+1} \setminus \{(0,\dots,0)\}$ represents the unique line through the origin and $\underline{x}$ in $\mathbb{A}^{n+1}$. Two sequences of homogeneous coordinates $(x_0,\dots,x_n)$ and $(y_0,\dots,y_n)$ represent the same point in $\mathbb{P}^n$ if and only if there exists $\lambda \in k \setminus \{0\}$ such that $(x_0,\dots,x_n) = (\lambda y_0,\dots,\lambda y_n)$. Thus projective n-space is the quotient of $k^{n+1} \setminus \{(0,\dots,0)\}$ by the equivalence relation

$$(x_0,\dots,x_n) \sim (\lambda x_0,\dots,\lambda x_n)\,, \qquad \lambda \in k \setminus \{0\}\,.$$

We call a representative for an equivalence class the **homogeneous coordinates** of that point in $\mathbb{P}^n$, and there are many choices for each point, by scaling by λ. To avoid confusion between homogeneous coordinates for $\mathbb{P}^n$ and ordinary coordinates for $\mathbb{A}^n$, we usually write homogeneous coordinates as $[x_0 : \cdots : x_n]$. Observe that we can embed

$$\begin{array}{ccc} \mathbb{A}^n & \longrightarrow & \mathbb{P}^n \\ (x_1,\dots,x_n) & \longmapsto & [1 : x_1 : \cdots : x_n] \end{array}\,.$$

Any other homogeneous coordinates where the first coordinate is non-zero can be re-scaled to have first coordinate one. So we are left with the points with first coordinate equal to zero. These are the **points at infinity**. A point $[0 : x_1 : \cdots : x_n]$ can be seen as a point in $\mathbb{P}^{n-1}$, by just dropping the initial zero. Thus

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}.$$

Similarly, we can embed $\mathbb{A}^1$ by the map $x \mapsto [1 : x]$, and then the point at infinity is $[0 : 1]$, so

$$\mathbb{P}^1 = \mathbb{A}^1 \cup \{[0 : 1]\}\,.$$

Over the complex numbers, $\mathbb{P}^1_{\mathbb{C}}$ is also called the **Riemann sphere**. Thinking about projective space as affine space plus points at infinity can be useful if we want to make use of our geometric intuition about affine space or the algebraic tools we have developed for working with affine algebraic sets. On the other hand, thinking about projective space in terms of homogeneous coordinates emphasises that all points of projective space look the same. We can only distinguish points at infinity from points in affine space after choosing a convention for how we embed $\mathbb{A}^n$ into $\mathbb{P}^n$.

Example. We could have used $[x_1 : \cdots : x_n : 1]$ instead.

Throughout this lecture we will use the convention above.

2.1.2 Definition and examples

A projective algebraic set is a subset of projective space defined by the vanishing of a finite list of polynomials. What does it mean for a polynomial to vanish at a point in projective space? Because a single point in $\mathbb{P}^n$ can be represented by many different homogeneous coordinates, it does not make sense to evaluate a polynomial in $k[X_0,\dots,X_n]$ at a point of $\mathbb{P}^n$. We have to restrict attention to homogeneous polynomials.

Definition. A polynomial $f \in k[X_0,\dots,X_n]$ is **homogeneous** if every term of f has the same degree.

Example. $X_0^3 + X_0^2X_1 + 3X_2^3 - X_0X_1X_2$ is homogeneous of degree three while $X_0X_1 - X_2$ is not homogeneous because it has a term of degree two and a term of degree one.

If $[x_0 : \cdots : x_n]$ and $[y_0 : \cdots : y_n]$ represent the same point $p \in \mathbb{P}^n$, then

$$(x_0,\dots,x_n) = \lambda\,(y_0,\dots,y_n)\,, \qquad \lambda \in k \setminus \{0\}\,.$$

Hence if $f \in k[X_0, \ldots, X_n]$ is a homogeneous polynomial of degree d, then

$$f(x_0, \ldots, x_n) = \lambda^d f(y_0, \ldots, y_n).$$

Thus the actual value of f at p is not well-defined, but it is well-defined to ask whether or not f is zero at p.

Definition. A **projective algebraic set** is a set of the form

$$\{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid f_1(x_0, \ldots, x_n) = \cdots = f_m(x_0, \ldots, x_n) = 0\},$$

for some finite list of homogeneous polynomials $f_1, \ldots, f_m \in k[X_0, \ldots, X_n]$.

By definition, a projective algebraic set is the vanishing of finitely many homogeneous polynomials. We can use the Hilbert basis theorem to show that the vanishing set of an infinite collection of homogeneous polynomials is a projective algebraic set. This is similar to the analogous result for affine algebraic sets, but a little trickier due to the word homogeneous.

Example. An example of a projective algebraic set is

$$V' = \left\{[w : x : y] \in \mathbb{P}^2 \;\middle|\; wx - y^2 = 0\right\}.$$

What is $V = V' \cap \mathbb{A}^2$, using the embedding $\mathbb{A}^2 \to \mathbb{P}^2$ which we considered before? To find this, we just substitute $w = 1$ into the equation for V', so

$$V = \left\{(x, y) \in \mathbb{A}^2 \;\middle|\; x - y^2 = 0\right\},$$

that is an affine parabola. The polynomial $X - Y^2$ is not homogeneous. Therefore consider instead the homogeneous polynomial $WX - Y^2$. When $W = 1$, this restricts to $X - Y^2$. That takes care of the points of V' where $w \neq 0$, since we can scale the homogeneous coordinates of such a point to get $w = 1$. But V' contains extra points where $w = 0$. We can also work out the intersection of V' with the $\mathbb{P}^1$ at infinity. Substituting $w = 0$ into the equation $wx - y^2 = 0$ for V' gives also $y = 0$. There is only one point of $\mathbb{P}^2$ with $w = y = 0$, the point $[0 : 1 : 0]$, since any other value for x could be scaled to one. So we get

$$V' = V \cup \{[0 : 1 : 0]\}.$$

Thus geometrically, V' consists of the parabola V together with a point at infinity in the direction $(1, 0)$, that is along the x-axis. Informally, the two arms of the parabola close up at infinity.

We would like to reverse this process, and go from an affine algebraic set to a projective algebraic set.

Example. Consider the affine hyperbola

$$H = \left\{(x, y) \in \mathbb{A}^2 \;\middle|\; xy - 1 = 0\right\}.$$

We need to turn the polynomial $XY - 1$ into a homogeneous polynomial, using a new variable W in $k[W, X, Y]$, which restricts to $XY - 1$ when $W = 1$. To do this, note that the highest degree term in $XY - 1$ has degree two. We multiply each term by an appropriate power of W to get all terms of degree two, so we have to replace the constant one by W^2. Thus we get $XY - W^2 = 0$. Thus we consider

$$H' = \left\{[w : x : y] \in \mathbb{P}^2 \;\middle|\; xy - w^2 = 0\right\}.$$

Again, when $w \neq 0$, we can scale to get $w = 1$, so we can substitute that in and see that we just get back H'. When $w = 0$, the equation becomes $xy = 0$, so we now get two points at infinity. Either $x = 0$, giving the point $[0 : 0 : 1] \in \mathbb{P}^2$, or $y = 0$, giving the point $[0 : 1 : 0] \in \mathbb{P}^2$. Thus

$$H' = H \cup \{[0 : 0 : 1], [0 : 1 : 0]\}.$$

Geometrically, H' consists of H together with points at infinity along the x-axis and y-axis. These axes are the asymptotes of H.

Compare the two above examples, where V' had equation $wx - y^2$, and H' had equation $xy - w^2$. These equations differ only by relabelling the coordinates. Thus V' and H' are isomorphic. We have not yet defined isomorphism of projective algebraic sets, but just relabelling the coordinates should certainly be an isomorphism. From the point of view of projective geometry, the only difference between the hyperbola and the parabola is that the parabola has one point at infinity while the hyperbola has two points at infinity. It turns out that V' and H' are also isomorphic to the projective line $\mathbb{P}^1$. We will need to define isomorphism of projective algebraic sets before we can prove this.

2.1.3 Homogenisation

The process we went through above to obtain V' from V and H' from H can be generalised.

Definition. For any polynomial $f \in k[X_1, \ldots, X_n]$, we define the **homogenisation** of f to be the polynomial in $\overline{f} \in k[X_0, \ldots, X_n]$ obtained by the following procedure. Let d be the maximum degree of terms of f. Then multiply each term of f by X_0^{d-e}, where e is the degree of this term in f.

Example. If

$$f(X_1, X_2, X_3) = X_1^3 + 4X_1X_2X_3 - X_1^2 - X_2^2 + 5X_3 + 8,$$

then the homogenisation is

$$\overline{f}(X_0, X_1, X_2, X_3) = X_1^3 + 4X_1X_2X_3 - X_1^2X_0 - X_2^2X_0 + 5X_3X_0^2 + 8X_0^3.$$

Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set. Let $W \subseteq \mathbb{P}^n$ be the set defined by the homogenisations of all polynomials in $\mathbb{I}(V)$. Then W is the smallest projective algebraic set containing V. This is not entirely obvious, because we have defined it using infinitely many homogeneous polynomials. We will prove this in the next lecture. When we substitute $x_0 = 1$ into the polynomials defining W, we just get back $\mathbb{I}(V)$, so

$$W \cap \{[1 : x_1 : \cdots : x_n]\} = V.$$

This proves that every affine algebraic set V is of the form $W \cap \mathbb{A}^n$ for some projective algebraic set W. We call W the **projective closure** of V. When defining the projective closure, it is not enough to just take the homogenisations of some finite list of polynomials which define V. You must take all of $\mathbb{I}(V)$. The standard example of this below shows that if we just use homogenisations of a generating set, instead of all of $\mathbb{I}(V)$, we still get a projective algebraic set V' such that $V' \cap \mathbb{A}^n = V$, but it might not be the smallest such set.

Example. Here is a more complex example, the twisted cubic curve. Let

$$C = \left\{(t, t^2, t^3) \in \mathbb{A}^3\right\} = \mathbb{V}\left(Y - X^2, Z - XY\right) \subseteq \mathbb{A}^3.$$

Parametrically, we can write this as

$$C = \left\{\left[1 : t : t^3 : t^3\right] \in \mathbb{P}^3\right\}.$$

Homogenising the parametric description, we might expect the projective closure to be

$$C' = \left\{\left[s^3 : s^2t : st^2 : t^3\right] \in \mathbb{P}^3\right\} = C \cup \{[0 : 0 : 0 : 1]\}.$$

One can check that C' is a projective algebraic set. But if we homogenise the two defining polynomials $Y - X^2$ and $Z - XY$, we get the projective algebraic set

$$C'' = \left\{[w : x : y : z] \in \mathbb{P}^3 \;\middle|\; wy - x^2 = wz - xy = 0\right\}.$$

It is still true that we can reverse this by just setting $w = 1$, so $C'' \cap \mathbb{A}^3 = C$. But what happens at infinity? Substituting in $w = 0$, one can check that

$$C'' = C \cup \left\{[0 : x : y : z] \in \mathbb{P}^3 \;\middle|\; -x^2 = -xy = 0\right\} = C \cup \left\{[0 : 0 : y : z] \in \mathbb{P}^3\right\}.$$

Thus the intersection of C'' with the plane at infinity is a copy of $\mathbb{P}^1$. Thus $C'' \neq C'$. It contains an extra line at infinity. This is not what we should expect, if C'' were the projective closure of C, since the dimension of the intersection with the plane at infinity should be smaller than the dimension of the initial affine algebraic set, speaking informally. If we homogenised all polynomials in $\mathbb{I}(C)$ and not just the two generators, then you can calculate that the projective closure of C is in fact

$$C' = \left\{[w : x : y : z] \in \mathbb{P}^3 \;\middle|\; wy - x^2 = wz - xy = xz - y^2 = 0\right\} = C \cup \{[0 : 0 : 0 : 1]\}.$$

The three polynomials $Y - X^2, Z - XY, XZ - Y^2$ are a generating set for $\mathbb{I}(C)$ and their homogenisations define C'. The extra polynomial involves only x, y, z and is in the ideal generated by $Y - X^2$ and $Z - XY$. I am not giving a procedure to find the projective closure of a given affine algebraic set. I just assert that this happens to work in this case. There is an algorithm but you would not want to have to use it by hand.

2.1.4 Zariski topology on projective space

We can define the Zariski topology on $\mathbb{P}^n$ by saying that the closed subsets are the projective algebraic sets. Observe that $\mathbb{A}^n$ is embedded as a Zariski open subset in $\mathbb{P}^n$, because the complement $\mathbb{P}^n \setminus \mathbb{A}^n$ is described by the homogeneous polynomial equaiton $X_0 = 0$. The existence of projective closures shows that the Zariski topology on $\mathbb{A}^n$ is the same as the subspace topology coming from the Zariski topology on $\mathbb{A}^n \subseteq \mathbb{P}^n$. The terminology projective closure is justified by noting that the smallest projective algebraic set containing $V \subseteq \mathbb{A}^n$ which we just described is the same as the closure of V in the Zariski topology on $\mathbb{P}^n$.