algebraic geometry

Lectures delivered by Nir Avni
Notes by Akhil Mathew

Fall 2010, Harvard

Last updated 11/24/2010

Contents

Introduction

Nir Avni taught a course (Math 232a) on algebraic geometry at Harvard in Fall 2010. These are my "live-TeXed" notes from the course.

Conventions are as follows: Each lecture gets its own "chapter," and appears in the table of contents with the date. Some lectures are marked "section," which means that they were taken at a recitation session. The recitation sessions were taught by Thomas Koberda.

These notes were typeset using LaTeX 2.0. I used `vim` to take the notes. I ran the Perl script `latexmk` in the background to keep the PDF output automatically updated throughout class. The `article` class was used for the notes as a whole. The LaTeX package `xymatrix` was used to generate diagrams.

Of course, these notes are not a faithful representation of the course, either in the mathematics itself or in the quotes, jokes, and philosophical musings; in particular, the errors are my fault. By the same token, any virtues in the notes are to be credited to the lecturer and not the scribe.

Please email corrections to `amathew@college.harvard.edu`.

Lecture 1
9/1

This course will focus on polynomial equations over algebraically closed fields. Questions that interest us are:

1. When does a system of equations have a solution?
2. When do two systems have the same solutions?

The first thing to do is why this is interesting and good. In particular, why we care about *these* equations. We consider equations over fields, not general rings, because there are fewer distinct equations.

1.1 Example. The equations $x = 0$ and $x^2 = 0$ are the same over fields but not over general rings.

These sorts of things will vastly simplify things. However, we will see situations when it is necessary to solve equations over rings nonetheless.

From now on, k is an **algebraically closed field.** We fix it.

1.2 Example. Here is an example where equations over rings are useful for equations over rings. Let $f(x, y) \in k[x, y]$. The equation $f(x, y) = 0$ can be thought of as:

1. An equation in two variables x, y over the field k
2. Or, an equation in one variable over the ring $k[x]$.

The second point of view is like looking at a family of one-dimensional equations, parametrized by x, which can simplify things.

Why do we care about polynomials? We could look at equations in continuous, smooth, etc. functions instead. There are several reasons.

1.3 Example.

1. Over an alg. closed field of positive characteristic, we can't think about continuous, smooth, etc. functions; we just have the algebraic structure.
2.

1.4 Definition. **n-dimensional affine space over k** is the set k^n. We denote it by $\mathbb{A}^n_k$.

An **affine variety** $V \subset \mathbb{A}^n_k$ is the common zero locus of a family of equations, i.e. a set of polynomials $\{f_\alpha\} \subset k[x_1, \dots, x_n]$. We denote the variety corresponding to the set $\{f_\alpha\}$ by $V(\{f_\alpha\})$.

These are the main objects that we will study.

Remark. If you look at a set of equations $\{f_\alpha\}$, a point satisfies these equations if and only if the point satisfies the ideal generated by the $\{f_\alpha\}$. In particular,

$$V(\{f_\alpha\}) = V((\{f_\alpha\})).$$

However, this ideal $(\{f_\alpha\})$ is finitely generated, because the polynomial ring is noetherian, so only a finite number of the $\{f_\alpha\}$ must generate the ideal. So this variety is equal to $V(f_{\alpha_1}, \dots, f_{\alpha_n})$ for some n.

1.5 Example. What's an interesting example of an algebraic vaiety? Suppose Γ is a finitely generated group. The **deformation space** of Γ is defined to be the set of all homorphisms Γ, GL_n, i.e.

$$\mathrm{Hom}(\Gamma, \mathrm{GL}_n(\mathbb{C})).$$

This is an algebraic variety. Why? Suppose Γ is generated by $g_1, \dots, g_m$ with relations $R_1, R_2, \dots$ (infinitely many, generally). Each R_i is a word in the g_j and g_j^{-1}. For instance, a relation could be that the commutator of two of them is trivial.

We are going to pick a variety where the first n^2 coordinates say where g_1 will go, the second where g_2 will go, etc. What will constrain the possible values is precisely these relations. Let $V \subset \mathbb{A}_{\mathbb{C}}^{2mn^2} \subset (Mat_n(\mathbb{C}))^{2m}$ be defined as follows. Let the coordinates be $X_1^+, X_1^-, \dots, X_m^+, X_m^- \in Mat_n(\mathbb{C})$. We require the conditions:

1. $X_i^+ X_i^- = \mathrm{id}$.
2. An infinite list of equations $\Gamma_j(X_1^+, X_1^-, \dots, X_m^+, X_m^-)$ corresponding for each R_i.

This clearly parametrizes the morphisms $\Gamma \to \mathrm{GL}_n(\mathbb{C})$ so we have defined a structure of an affine variety. Note that we only need to use finitely many equations to define this variety in view of noetheriannness.

Let Δ be the group generated by $g_1, \dots, g_m$ with relations $\Gamma_1, \dots, \Gamma_N$. We get a $\mathrm{Hom}(\Delta, \mathrm{GL}_n(\mathbb{C})$, which is the same as $\mathrm{Hom}(\Gamma, \mathrm{GL}_n(\mathbb{C}))$ by the remark about finitely many equations when N is large. Δ is not only finitely generated, but also finitely presented. We only need to care about f.p groups for f.d. representations.

Why do we need alg. closedness?

1.6 Theorem (Hilbert Nullstellensatz–form 1 of Tarski)**.** *Let $V \subset \mathbb{A}_k^n$ be an affine variety for k any alg. closed field. Let $K \supset k$ be alg. closed. If V has a solution over K, then it has a solution over k. In fact, if you take any first-order sentence ϕ [1], using constants from k, then it is satisfied in k if and only if it is satisfied in K.*

For instance, if we have two polynomials $f_1(x, y), f_2(x, y)$, the sentence

$$\exists x \exists y f_1(x, y) = 0 \text{ and} f_2(x, y) = 0$$

is true in k if and only if it is true in K, so by this kind of reasoning the second part of the theorem implies the first. It is not true for non-alg closed fields. Indeed, $x^2 + y^2 = -1$ has no solution in $\mathbb{R}$ but does in $\mathbb{C}$.

[1] I.e., something you can write using addition, multiplication, quantifiers, and, or.

This says that every algebraic statement true for the complex numbers is true for all alg. closed fields of char. 0. Only characteristic makes a difference between alg. closed fields. This reduces char 0. to studying the complexes, which have a nice topology and whatnot.

We will use a fact from logic. If you don't like logic, there are many proofs.

1.7 Theorem. *If a countable collection of sentences has one infinite model, then it has models of each infinite cardinality.*

This follows from the compactness theorem, but we will not prove it.

Pf. of the theorem. We prove the second, general statement. Wlog, I can take k to be the smallest possible field. So k is the alg. closure of the field generated by the coefficients of ϕ. In particular, we can assume that k is countable.

Consider the following first-order language with $+, \dot{}, -, \forall, \exists,$, constants C_α for every element α of k. Let T be the following system of sentences.

1. Axioms of fields. E.g., $+$ is commutative. $\forall x, y(x + y = y + x)$. And so on.
2. Axioms of algebraic closedness. Every nontrivial equation has a solution. For instance, we consider the sentences $\forall a_0, \dots, a_n(a_n \neq 0 \implies \exists x, a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ for each n.
3. $C_\alpha C_\beta = C_{\alpha+\beta}$ and $C_{\alpha\beta} = C_\alpha C_\beta$. Also, $C_1 = 1$.

What does it mean to be a model of the system T of equations? The first two axioms say that the model is an alg. closed field; the third says that it contains a copy of k. So a model of T is an alg. closed field containing k. We have to show that Φ is satisfied in either all models of T or none.

Suppose by contradiction that $T \cup \{\phi\}$ has a model K and $T \cup \{\not\phi\}$ has a model L. Both are infinite since they are alg. closed. By the fact that I just wrote, we can assume that the cardinalities of K, L are both $\aleph_1$, the first uncountable cardinality. However, any two alg. closed fields of cardinality $\aleph_1$ are isomorphic; the only way to get one is to take the prime field, add $\aleph_1$ transcendental elements, and take the algebraic closure. So $L \simeq K$, k-isomorphically by Galois theory. (choose the isomorphism of copies of k and then extend it to $L \to K$) It can't be that a formula is satisfied in one and not the other, contradiction. ▲

1.8 Theorem (Hilbert Nullstellensatz, 2nd form)**.** *If a system of equations $\{f_\alpha\}$ has no solutions in the alg. closed field k, then there is a reason: the ideal $(\{f_\alpha\}) = 1$.*

In other words, we can write the function 1 as a combination $\sum f_\alpha g_\alpha$ for some polynomials g_α. (If we knew that, that would clearly imply that there were no roots. So the lack of roots comes with evidence.)

Proof. Let $\{f_\alpha\}$ be the system with no solution in k. Let I be the ideal generated. Consider a maximal ideal $\mathfrak{m}$ containing I. Let $K = k[x_1, \dots, x_n]/\mathfrak{m}$; this is a field containing k. In this field, the tuple $(x_1, \dots, x_n)$ modulo $\mathfrak{m}$ (i.e. the images of the variables in the field) satisfies the system $\{f_\alpha\}$ of equations; this is the same as saying that the $f_\alpha \in I$. This means the $\{f_\alpha\}$ have a solution in K containing k, but there isn't a solution in k, a contradiction by the previous form of the Nullstellensatz. ▲

In diff geo, we often need a partition of unity argument. We need to write 1 as a sum of functions, each of which vanishes somewhere. The sum $\sum f_\alpha g_\alpha = 1$ is the algebraic analog of the partition of unity.

Lecture 2
9/3

Last time, we gave two versions of Hilbert's Nullstellensatz.

Fix an alg. closed field k.

2.1 Theorem (v. 1)**.** *If a system of polynomial equations has no solution over k, then it has no solution over any bigger field.*

The second stated that if a system has no solution, then it has a good reason, *inside* k, namely the ideal generated by the system is (1).

I should put it in a box:

2.2 Theorem (v 2)**.** *If a system of equations in k has no zeros, then the ideal generated by the system is* (1)*.*

There is a third formulation of the Hilbert theorem:

2.3 Theorem (v 3)**.** *If $g(x_1, \dots, x_n) = 0$ (g a polynomial) whenever the system of polynomial equations*

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

is satisfied, then there is a power g^r of g which lies in the ideal $(f_1, \dots, f_m)$.

The prevoius version of the Nullstellensatz works with taking $g \equiv 1$; then g vanishes nowhere.

Proof. We use the second version of the Nullstellensatz. In

$$k[x_1, \dots, x_n, y]$$

the system of equations (with $X = (x_1, \dots, x_n)$)

$$f_1(X) = \dots = f_m(X) = 0, \quad (1 - yg(X)) = 0$$

has no solution. Indeed, if there were a solution, then we'd have that all the f's vanish, so g vanishes and the last equation can't be satisfied.

Therefore, by the usual Nullstellensatz, there are polynomials

$$\alpha_1(X, y) f_1(X) + \dots + \alpha_m(X, y) f_m(X) + \beta(X, y)(1 - Yg(X)) = 1 \qquad (1)$$

for polynomials $\alpha_i, \beta \in k[X, y] = k[x_1, \dots, x_n, y]$.

This holds in the ring, hence in the localization $k[X, y][1/g] = (k[x]_g)[Y]$. Now, plug in $y = 1/g$ into the equation above. What do you get? The last term dies. We get that, in the localized ring $k[X]_g$,

$$\alpha_1(X, g^{-1})f_1(X) + \cdots + \alpha_m(X, g^{-1})f_m(X)) = 1 \tag{2}$$

Now multiply by g^N for $N \gg 1$. Then we find

$$g^N = \sum \alpha_i g^N(X, g^{-1})f_i(X)$$

which holds in $k[X]_g$. But all the expressions here are polynomials in $k[X]$ for N large and the map $k[X] \to k[X]_g$ is injective, so we find the required expression for g^N.

▲

2.4 Corollary. *If two polynomials $f, g \in k[x_1, \ldots, x_n]$ satisfy that every irreducible factor of either f, g appears only once (i.e. f, g are not divisible by squares, or are squarefree) and define the same variety, then f and g differ by a constant (i.e. are scalar multiples of one another).*

In particular, the degree of f is an invariant of the variety (if it is given by one equation). This is called the **degree** of the variety. The variety is called a **hypersurface**. So hypersurfaces have a well-defined degree. In the future, we will define the degree of any algebraic variety.

Proof. Indeed, we see that f, g have the same irreducible factors by the Nullstellensatz, because f must divide a power of g, and g must divide a power of f. ▲

Apart from equations in affine space, it turns out —we will see this in the future— that equations behave more nicely if you take them in projective space. Let us recall:

2.5 Definition. Projective n-space, which we denote by $\mathbb{P}^n_k$ or $\mathbb{P}^n$, is the space of lines in k^{n+1} passing through zero. In particular, $\mathbb{P}^n$ is the quotient space of k^{n+1} by the multiplicative action of $k^* = k - \{0\}$.

2.6 Definition. The projective variety in $\mathbb{P}^n$ defined by polynomials $\{f_\alpha(x_0, \ldots, x_n)\} \subset k[x_0, \ldots, x_n]$ the set of lines in k^{n+1} passing through zero (i.e. points of $\mathbb{P}^n$) on which all the f_α vanish.

So the polynomials are required to vanish on all points of the whole line.

Remark. If a polynomial f vanishes on a line, then so do its homogeneous components of it. Indeed, we can write $f = f_0 + \cdots + f_d$ for homogeneous f_i of degree i; if f vanishes on the line, so does each f_i. So we might as well assume that the defining equations are homogeneous.

We introduce some notation. The point in $\mathbb{P}^n$ that corresponds to the line between and some point $(\alpha_0, \ldots, \alpha_n)$ is denoted by

$$[\alpha_0, \ldots, \alpha_n]$$

so that we have

$$[\alpha_0, \dots, \alpha_n] = [\lambda\alpha_0 \dots \lambda\alpha_n]$$

for all $\lambda \neq 0$.

Here is an important point. The map $(x_1, \dots, x_n) \to [1, x_1, \dots, x_n]$ a bijection of $\mathbb{A}^n$ and what we call $\mathbb{P}^n_0 = \{[\alpha_0 \dots \alpha_n] : \alpha_0 \neq 0\}$. The complement of the image is the set of all lines that lie in a codimension one subspace, i.e. the set of all $[0, \alpha_1, \dots, \alpha_n]$. In other words, this is $\mathbb{P}^{n-1}$. We have

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

More importantly, the bijection just defined preserves algebraic sets. It gives a bijection between affine varieties in $\mathbb{A}^n$ and intersections of projective varieties with $\mathbb{P}^n_0$. So, given a polynomial $f \in k[x_1, \dots, x_n]$ (of degree, say d), we want a corresponding homogeneous polynomial $\widetilde{f} \in k[x_0, \dots, x_n]$ which corresponds to the projective variety. Suppose $f(x_1, \dots, x_n) = \sum a_i X^i$ for the i's multi-indices (i.e., in $\mathbb{N}^n$). Then write

$$\widetilde{f}(x_0, \dots, x_n) = \sum a_i x_0^{d-|i|} X^i.$$

So $\widetilde{f}$ is homogeneous of degree d.

2.7 Definition. $\widetilde{f}$ is called the **homogeneization** of f.

We know that $\widetilde{f}(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$. So if we take the variety in $\mathbb{P}^n$ defined by $\widetilde{f}$ and intersect it with $\mathbb{P}^n_0$, we get the corresponding variety to f in $\mathbb{A}^n$.

The other direction is even simpler. Given a homogeneous polynomial defining a projective variety, just set $x_0 = 1$ to get the corresponding affine variety in $\mathbb{P}^n_0$.

Remark. The upshot of this is that each projective variety is covered by affine varieties in the basic open sets $\mathbb{P}^n_0$ (which can also be defined for coordiantes other than the zeroth). It goes the other way: every affine variety is a subset of a projective variety (not necessarily unique) thanks to the homogenization process above. So you can use affine vareities to study projective ones, and vice versa.

It is quite trivial that:

2.8 Proposition. *The product of two affine varieties is an affine variety.*

Proof. If you take the product of two affine spaces, you get one: $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$. If you have equations $F_1(X) = F_2(X) = \cdots = F_p(X) = 0, G_1(Y) = \cdots = G_r(Y) = 0$, then combination of those two equations in $\mathbb{A}^{n+m}$ gives the product variety. ▲

However: (dangerous bend)

$$\mathbb{P}^n \times \mathbb{P}^m \neq \mathbb{P}^{n+m}.$$

Nonetheless, the product of two projective varieties is projective, which we prove (in the case for full projective space).

§1 Segre embedding

Here is the construction, called the **Segre embedding**

If U, V are vector spaces, then the map

$$U \times V \to U \otimes V$$

$(u, v) \to u \otimes v$ (in coordinates, $\{u_i\}, \{v_j\}$ goes to the matrix $\{u_i v_j\}$) gives a map

$$\mathbb{P}(U) \times \mathbb{P}(V) \to \mathbb{P}(U \otimes V).$$

(When we write $\mathbb{P}(U)$, we mean the set of all lines through the origin in U.)

This is clear and gives a map

$$\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{mn+n+m}.$$

This is one to one. This is because each row in $\{u_i v_j\}$ which is not zero is a scalar multiple of u, each column a scalar multiple of v.

2.9 Proposition. *The image of the Segre embedding is a projective variety.*

Proof. Indeed, all the rows of the matrix $\{u_i v_j\}$ are scalar multiples of each other, so the matrix has rank one. Conversely, if the matrix a_{ij} representing a point in $U \otimes V$ (and thus a line through the origin) is of rank one, then all the rows are scalar multiples of each other, and we see that the image is precisely the set of matrices of rank one. But to say this is to say that all two-by-two minors vanish, which is an algebraic condition. ▲

Remark. The best way to define this is to use categories, and to show that this is a product in the category of projective varieties. This Segre embedding in fact gives the categorical product, but we shall not get into it here.

2.10 Example. Let's compute this for the simplest case. What is the Segre map $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$? Let us work in coordinates. In the affine charts $\mathbb{P}^1_0 \times \mathbb{P}^1_0$ (elements of the form $[1, x], [1, y]$) the image is the matrix

$$\begin{bmatrix} 1 & x \\ y & xy \end{bmatrix}.$$

So in coordinates $\mathbb{P}^3_0$, the equation of the image is that the 2-by-2 coordinate is equal to the 1-by-2 times the 2-by-1. This is a hyperboloid.

You can think of this as a family of lines, since each $\mathbb{P}^1$ is a line. The surface is then covered by the families of lines which the $\mathbb{P}^1$'s map to.

In general, when we have a system of equations, the solution set (the variety) does not determine the system. $V(\{f_\alpha\})$ does not determine $\{f_\alpha\}$. They can, of course, determine only the ideal. You might think that the solutions determine the ideal, but this is false, for some trivial reason: $x = 0$ and $x^2 = 0$ define the same set.

Up to things like that, however, that's the only obstruction.

2.11 Definition. If $X \in \mathbb{A}^n$, let $I(X)$ be the ideal of polynomials vanishing on X, i.e. $f \in k[x_1, \ldots, x_n]$ consisting of polynomials with $f|_X = 0$. This is clearly an ideal. However, it has a special property: if $f^2 \in I$, so is I.

I_X is a **radical ideal**: if a power is in I_X, then the original quantity is in it. The theorem is that this is the only obstruction, i.e. every radical ideal is obtained as the ideal of some set X.

2.12 Theorem. *The maps $I \to V(I)$ and $V \to I(V)$ between ideals and varieties are inverse bijections the set of all radical ideals in $k[x_1, \ldots, x_n]$ and the set of affine varieties in $\mathbb{A}^n$.*

Proof. This is just a restatement of the Nullstellensatz (third form). ▲

Lecture 3
9/8

We start by introducing a topology.

3.1 Definition. The **Zariski topology** on $\mathbb{A}^n$ is the topology such that the closed sets are the affine varieties (subvarieties of $\mathbb{A}^n$, that is).

Why is it a topology?

1. The empty set is closed (given by the equation $1 = 0$); the whole space is given by $0 = 0$ and is also closed.
2. We need to show that $V(I) \cup V(J)$ for I, J ideals is a variety. But this is the variety $V(IJ)$.
3. We need to show that $\bigcap V(I_\alpha)$ is a variety for ideals I_α; this is the same as $V(\bigcup I_\alpha)$ though, so is a closed set.

3.2 Example. In $\mathbb{A}^1$, a Zariski open set is either empty or is cofinite. This is because a one-variable polynomial has finitely many roots. Any infinite set is thus Zariski dense (e.g. $\mathbb{Z}$ or the unit circle in $\mathbb{C}$).

Every Zariski closed set corresponds to a subvariety, i.e. to an ideal (not unique, of course). If we have

$$V(I) \subset V(J)$$

for radical ideals I, J (recall that we can restrict to radical ideals without loss of generality) then we have

$$I \supset J$$

and conversely. The fact that $I \supset J$ implies the variety-inclusion is obvious; the reverse is the Nullstellensatz, i.e. the fact that $IV(I) = I$ for a radical ideal I.

3.3 Example. What does it mean that $V(I) = V(J_1) \cup V(J_2)$? This means that I and $J_1 J_2$ have the same radical.

The set of all ideals satisfies a chain condition, because $k[x_1, \ldots, x_n]$ is noetherian. There is no infinite (strictly) ascending sequence of ideals. As a result:

3.4 Proposition. *There is no infinite strictly descending sequence of closed subsets of $\mathbb{A}^n$. So every set of closed sets of $\mathbb{A}^n$ has a minimal element.*

This result allows you to use induction ("noetherian induction") on closed sets to prove things.

3.5 Example. We give an example of this noetherian induction business. First, a definition.

3.6 Definition. We say that an affine variety or, more generally, subset[2] $X \subset \mathbb{A}^n$, is **reducible** if it is the union of two closed[3] proper subsets. Otherwise the set is said to be **irreducible**.

In many ways, this behaves similarly to connectedness in usual general topology; connectedness is too crude in algebraic geometry because the Zariski topology is too weak.

3.7 Proposition. *A variety $V(I)$ (for I is radical) is irreducible if and only if I is prime.*

Proof. Indeed, if $V(I) = V(J_1) \cup V(J_2)$ implies that $I \supset J_1 J_2$ (since I is radical), so that I contains one of J_1, J_2. As a result, $V(I) \subset V(J_1)$ or $V(I) \subset V(J_2)$. This implies that $V(I)$ is not the union of two proper closed subsets.

Conversely, if I is not prime, then we can write $I \supset J_1 J_2$ for both J_1, J_2 not contained in I, and we have then $V(I) \subset V(J_1) \cup V(J_2)$. Neither of these contains $V(I)$ since I is radical. ▲

3.8 Theorem. *Every affine variety can be written uniquely as the union of finitely many irreducible subvarieties, none of which contains the other.*

This is really primary decomposition.

Proof. First, we prove existence.

Noetherian induction. We are looking at the set of all varieties that *can't* be decomposed in this way. Take V be a minimal element in this set, a minimal counterexample. If V is irreducible, then we are done (trivially). Otherwise, we can write $V = W_1 \cup W_2$ for smaller closed subsets; each can be decomposed as the union of finitely many irreducible subvarieties by the noetherian inductive hypothesis. Thus V itself is the union of finitely many irreducible subvarieties.

Uniqueness is left to the reader. ▲

3.9 Example. $\mathbb{A}^n$ is irreducible, because (0) is prime.

$V(xy) \subset \mathbb{A}^2$ is reducible. This is just a cross, and is the union of the x- and $y-$axes.

3.10 Theorem. *If X, Y are irreducible, then $X \times Y$ is also irreducible.*

[2]With the induced topology from the Zariski topology, of course.

[3]In the relative topology.

We will prove the result geometrically. In algebra, it actually says something. If you have prime ideals $I \subset k[x_1, \ldots, x_n]$ and $J \subset k[y_1, \ldots, y_m]$, and you look at the ideal $(I, J) \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$, then its radical $\sqrt{(I, J)}$ is prime.

Proof. Suppose $X \times Y$ is the union $V \cup U$ for both V, U both closed. We want to show that one of them is the full $X \times Y$.

For each $x \in X$, the set (the "fiber") $V_x = \{y : (x, y) \in V\}$ is a closed subset of Y. Ditto for U_x. The union $U_x \cup V_x = Y$. But Y is irreducible; this means that either $U_x = Y$ or $V_x = Y$.

Consider the set $A = \{x : U_x \supset Y\}$, or equivalently the set of x such that $(x, y) \in U$ for all $y \in Y$. We will show that this is closed. This is equivalently

$$\bigcap_{y \in Y} \{x : (x, y) \in U\}$$

so is the intersection of a bunch of fibers. But each one of the fibers is closed, so their intersection is closed. In particular, A is closed. Similarly, the set $B = \{x : V_x \supset Y\}$ is closed in X. Now by the previous paragraph, $A \cup B = X$; either $A = X$ or $B = X$ as a result. In either case, it is clear that $U = X \times Y$ or $V = X \times Y$ in the corresponding cases. This implies irreducibility of $X \times Y$. ▲

§1 Morphisms

Now we will define maps of algebraic varieties. This will become more abstract steadily.

3.11 Definition. A **morphism** from an affine variety $X \subset \mathbb{A}^n$ to $\mathbb{A}^1$ is the restriction of a polynomial $f \in k[x_1, \ldots, x_n]$ to the set X.

The set of all morphisms $X \to \mathbb{A}^1$ is denoted by $k[X]$. This is equivalently $k[x_1, \ldots, x_n]/I(X)$, because $I(X)$ is precisely the set of polynomials that vanish on X. This is also called the **coordinate ring**.

3.12 Definition. A **morphism** between the affine varieties $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ is m-tuple of morphisms $\phi_1, \ldots, \phi_m : X \to \mathbb{A}^1$ such that the image happens to lie in Y. I.e, for each x, $(\phi_1(x), \ldots, \phi_m(x)) \in Y$.

Does the fact that something is a morphism (i.e., has image lying in the subvariety Y) depend on the field? No, because of the Nullstellensatz. Any first-order statement true in one alg. closed field of given characteristic is true in any other alg. closed field of same char.

There are problems:

1. The image of a morphism of affine varieties is not necessarily an affine variety. Nonetheless, it is a boolean combination of affine varieties.

2. We want to extend this to projective spaces. We'd like to define something like $\mathbb{P}^n \to \mathbb{A}^1$. We could cover $\mathbb{P}^n$ by affine spaces $\mathbb{A}^n$ and then to say that a morphism from $\mathbb{P}^n$ is one that restricts to a morphism on each open affine piece. But why is this independent of the cover? If we had two covers $\{U_i\}, \{V_j\}$, we need to know that something that restricts to a regular fn on each U_i also restricts to one

on each V_j. But $U_i \cap V_j \subset V_j$ is not necessarily closed. Indeed, the intersection of the basic open affines $\mathbb{A}^n_0 \cap \mathbb{A}^n_j$ corresponds to the set of points $(1, x_1, \dots, x_n)$ such that $x_j \neq 0$. This is not closed.

3.13 Definition. A **quasi-affine variety** is a boolean combination of affine varieties. It is also called a **constructible set**.

We'd like to define a morphism out of a quasi-affine variety.

3.14 Definition. Let X be a constructible set. A **morphism** $\phi : X \to \mathbb{A}^1$ is a map satisfying that for each point $x \in X$, there is a relatively open set $U \subset X$ and two polynomials f, g such that g does not vanish on U and such that $\phi = f/g$ on U.

We are not saying that there exists a pair *globally*, just that there exist pairs of polynomials around each point. We now need to say why this is a more general morphism than the previous one.

3.15 Theorem. *In the case of an affine variety, the two definitions of a morphism* $X \to \mathbb{A}^1$ *agree.*

Proof. Clearly, the first definition (global, polynomials) is weaker than the second (local) one. We need to show the reverse. In particular, if in a neighborhood of every point, we can write something as a quotient of polynomials with the denominator nonvanishing, then we can write it globally as a polynomial. Fix a morphism $\phi : X \to \mathbb{A}^1$ in the sense of the second defn.

For each $x \in X$, find U_x, f_x, g_x such that U_x is a nbd of x, f_x, g_x as in the definition (i.e. $g_x \neq 0$ on U_x and $\phi = f_x/g_x$). Then $X - U_x$ is closed for each x. Find a polynomial e_x that vanishes on this set but is such that $e_x(x) \neq 0$, so e_x is not zero in $k[X]$. By replacing U_x, f_x, g_x with $U_x - V(e_x), f_x e_x, g_x e_x$, we can assume that g_x (and f_x) vanishes on $X - U_x$.

By the noetherian property, this space is quasi-compact with respect to the topology: there is no infinite descending sequence of closed subsets. So we can write $X = U_{x_1} \cup \cdots \cup U_{x_n}$. We know that $\phi = f_x/g_x$ on U_x. Alternatively, $g_x \phi = f_x$ on U_x.

But it is clear that outside U_x, it also holds: both are zero. Here's the punch line. This is what was said about arguments similar to a partition of unity. There is no common root of the g_{x_i}, so they generate the unit ideal in $k[X]$ (i.e., together with $I(X)$, they generate 1 in $k[x_1, \dots, x_n]$). So there are polynomials $h_{x_1}, \dots, h_{x_n}$ such that

$$\sum h_{x_i} g_{x_i} = 1$$

in $k[X]$. It follows that

$$\phi = \sum h_{x_i} g_{x_i} \phi = \sum f_{x_i} h_{x_i} \in k[X],$$

so ϕ is a morphism in the first, more restricted sense. ▲

Lecture 4
9/10

Last time, we defined that

> $\phi : X \to \mathbb{A}^1$ is **regular** if for any $x \in X$ there is an open neighborhood U_x and polynomials f_x, g_x with $g_x \neq 0$ on U_x and $\phi = \frac{f_x}{g_x}$ on U_x.

The use of division generalizes the naive definition of a morphism being a polynomial map. We instead require that the morphism ϕ is locally a quotient of a well-defined rational function.

Similarly, we can define:

4.1 Definition. $\phi : X \to \mathbb{A}^n$ is **regular** if and only if each of the coordinates is regular as a morphism to $\mathbb{A}^1$.

Last time, we showed that for an affine (not a quasi-affine) variety X, the morphisms out of X to $\mathbb{A}^1$ are in fact the polynomial maps. The point was to take local expressions f_x/g_x around each point (with $g_x(x) \neq 0$) and patch them together by using a partition of unity type argument, since the $\{g_x\}$ have no common root on X and consequently generate the unit ideal in $k[X]$.

4.2 Example.

1. Look at the hyperbola $V(xy-1)$. Let the map $\phi : V(xy-1) \to \mathbb{A}^1$ send $(x, y) \to x$. The image of this map ϕ is **not** an affine subvariety of $\mathbb{A}^1$; it consists of all points except zero.

   However, $\phi : V(xy-1) \to \mathbb{A}^1 - \{0\}$ is invertible with inverse $x \to (x, x^{-1})$. In particular, $V(xy-1)$ is isomorphic to the quasi-affine variety $\mathbb{A}^1 - \{0\}$.[4]

2. Consider $\psi : V(xz^2+yz+1) \to \mathbb{A}^2$ sending $(x, y, z) \to (x, y)$. What is the image? The image is the set of all (a, b) such that the polynomial

   $$az^2 + bz + 1$$

   has a root in z. Since we are in an algebraically closed field, this always has a root unless $a, b = 0$. In particular, the image is $\mathbb{A}^2 - \{(0, 0)\}$.

   Is this map invertible? The answer is no. Usually, there are two solutions to a quadratic equation. Over the open set where the discriminant is nonzero (i.e. $y^2 - 4x \neq 0$), the map is two-to-one. So ψ is not invertible. In fact, as we will show, $\mathbb{A}^2 - \{(0, 0)\}$ is **not** isomorphic to **any** affine variety.

In general, given a morphism $\phi : X \to Y$, the question of what $\phi(X)$ is is usually the question of when certain equations have solutions, which is a relative version of the question we started with (the Nullstellensatz). We start with a general discussion.

Recall that the **coordinate ring** of an affine variety X (or of a quasi-affine variety, more generally) is the ring of regular maps into $\mathbb{A}^1$. This is denoted by $k[X]$. When

[4] Some authors like Shafarevich call $\mathbb{A}^1 - \{0\}$ a variety because it is isomorphic to a variety, but we don't follow this.

X is affine, this is just the quotient of the polynomial ring by a suitable radical ideal. This is an invariant of a quasi-affine variety.

Suppose there are three algebraic varieties or quasi-affine varieties $X \to Y \to Z$ with regular maps $f : X \to Y$ and $g : Y \to Z$. Then the composition $g \circ f$ is regular. The reason is that when you plug in a rational function into a rational function, you get a rational function.

Moreover, if we take $Z = \mathbb{A}^1$, we see that pulling back gives a homomorphism

$$k[Y] \to k[X]$$

sending $g : Y \to \mathbb{A}^1$ to $g \circ f$. We thus have a map

$$\mathrm{Map}(X, Y) \to \mathrm{Hom}_{k-\mathrm{alg}}(k[Y], k[X]).$$

4.3 Theorem. *If Y is an affine variety, then the map* $\mathrm{Map}(X, Y) \to \mathrm{Hom}_{k-\mathrm{alg}}(k[Y], k[X])$ *is a bijection..*

This translates geometry into algebra, in a sense: the map $X \to Y$ is determined by how it handles regular functions, and any homomorphism of the coordinate rings yields a map of varieties.

Proof. We will construct the inverse map. Given $\phi : k[Y] \to k[X]$, we want to find a regular $X \to Y$. Suppose such a map $\psi : X \to Y$ exists, that gives ϕ. Such a map is just a tuple of maps $(\psi_1, \dots, \psi_m)$ if $Y \subset \mathbb{A}^m$ that satisfy all the equations defining Y.

Then considers the projections $\pi_i : Y \to \mathbb{A}^1$ sending Y to its ith coordinate. The pull-backs $\pi_i \circ \psi = \phi(\pi_i) = \psi_i$. In particular, if ψ exists, it must happen that

$$\psi_i = \phi(\pi_i).$$

So, we **define** ψ_i to be the image $\phi(\pi_i)$. Then ψ_i is a regular function on X and $\psi = (\psi_1, \dots, \psi_m)$ is a morphism $X \to \mathbb{A}^m$. We show that the image is contained in Y.

Suppose that $g(Y_1, \dots, Y_m)$ is a polynomial that vanishes on Y. For every $y \in Y$, we get that $g(\pi_1(y), \dots, \pi_m(y)) = 0$, so that

$$g(\pi_1, \dots, \pi_m) = 0 \in k[Y].$$

In particular, by taking the image by ϕ, we see:

$$g(\psi_1, \dots, \psi_m) = 0 \in k[X]$$

which means

$$g(\psi_1(x), \dots, \psi_m(x)) = 0 \in k \quad \forall x \in X$$

so that ψ has image contained in the zero set of g. Since g was arbitrary vanishing on Y, we see that $\psi(X) \subset Y$.

We leave it to the reader to show that the map $\phi \to \psi$ is indeed the inverse to the map between morphisms of varieties and k-algebras. ▲

As an application, we show:

4.4 Proposition. $X = \mathbb{A}^2 - \{(0,0)\}$ *is not isomorphic to an affine variety.*

Proof. First, what is the ring of regular functions on the quasi-affine variety X? We use:

4.5 Proposition. *Any regular map* $\phi : X \to \mathbb{A}^1$ *extends to all of* $\mathbb{A}^2$.

Proof. This should remind you of a theorem from several complex variables. If you have a function of several complex variables on the ball of radius one in $\mathbb{C}^2$ minus the ball of radius $\frac{1}{2}$, it extends analytically to the whole ball of radius one. This is the algebraic version of that.

We next use a lemma:

4.6 Lemma. *If* $f, g \in k[X, Y]$ *are irreducible and non-collinear (one is not a multiple of another), then* $V(f, g)$ *is finite.*

If proved for irreducibles, it follows for reducibles f, g with no common factors, by taking finite unions.

Proof. If f or g depends only one on coordinate, then this is clear. Indeed, say f is a polynomial in X; let its one root be α_1. Then $V(f, g)$ is the set $\{y : g(\alpha, y) = 0\}$ which is finite since $g(\alpha, y)$ is not identically zero (or it would be divisible by $X - \alpha$).

The trick here is to consider f as a polynomial in $k(X)[Y]$. Then f is still irreducible (check).[5] Similarly, for g.

Suppose f, g were collinear in $k[X](Y)$. In particular, $f(X, Y) = \frac{\alpha(X)}{\beta(X)} g(X, Y)$ for some polynomials α, β. We find that

$$\beta(X) f(X, Y) = \alpha(X) g(X, Y).$$

In particular, f divides $\alpha(X) g(X, Y)$, so f is a polynomial only in X, contradiction.

So f, g are not collinear in $k(X)[Y]$; in particular, there are $\alpha(X, Y), \beta(X, Y) \in k[X](Y)$ such that

$$\alpha f + \beta g = 1.$$

Clearing denominators in X (only polynomials in X show up in the denominator)

$$\widetilde{\alpha(X, Y)} f(X, Y) + \widetilde{\beta(X, Y)} g(X, Y) = \gamma(X)$$

where $\widetilde{\alpha}, \widetilde{\beta} \in k[X, Y], \gamma(X) \in k[X]$. This identity actually holds in $k[X, Y]$ since all these are polynomials. Clearly γ is not the zero polynomial because it was the denominator.

If (x, y) is a common root for f, g, then $\gamma(x) = 0$. So x has only finitely many options. But we can run the same argument replacing x and y. So that y has only finitely many options as well, and we're done. ▲

[5] Gauss's lemma.

We will show that the number of zeros in $V(f, g)$ is equal to the product of $\deg f$ and $\deg g$ if counted appropriately.

Now we prove the proposition on regular functions $X = \mathbb{A}^2 - \{(0,0)\} \to \mathbb{A}^1$. Let ϕ be such a regular fn. Pick $x \in X$. There is an open set U around x and polynomials $g, h \in k[X, Y]$ such that

$$h \neq 0 \text{ on } U \quad \text{and} \quad \phi = \frac{g}{h} \text{ on } U.$$

Assume that g, h have no common factor.

Suppose h is nonconstant (otherwise ϕ trivially extends). We will show that wherever h vanishes (on $X - U$!), g vanishes too. Take $x' \in X$ arbitrary; we have a nbd U' of x' and polynomials g', h' such that

$$\phi = \frac{g'}{h'} \text{ on } U'.$$

On $U \cap U'$, we have

$$gh' = hg'.$$

But this is an equality of two polynomials, and $U \cap U'$ is open and dense (remember, $\mathbb{A}^2$ is irreducible—every open set is dense). So this means $gh' = hg'$ everywhere, i.e. in $k[X, Y]$.

Since $h'(x') \neq 0$, we get that $h(x') = 0$ would imply $g(x') = 0$. The upshot, x' being arbitrary, is that h can only vanish if g also vanishes. The previous lemma implies that $V(h) \subset V(g, h)$ is finite. This cannot be unless h is constant. (Exercise: A polynomial in two variables which is not constant has infinitely many roots.) ▲

Finally, we prove that X is not isomorphic to an affine variety. Indeed, affine varieties are the same thing as finitely reduced algebras by the proposition; since $k[X]$ is a polynomial ring in two variables, we would have that X is isomorphic to $\mathbb{A}^2$—both have the same coordinate ring. Moreover, this isomorphism $\mathbb{A}^2 - \{(0,0)\} \to \mathbb{A}^2$ would be obtained by pulling back the natural inclusion $k[X, Y] \to k[X, Y]$. This map is, however, an inclusion, which is clearly not an isomorphism. ▲

Lecture 5
9/13

Last time, we considered continuous maps

$$f : X \to \mathbb{A}^1$$

for X a quasi-affine variety. We called the map a **regular map**, or a morphism, if whenever $x \in X$, there was a nbd U_x of x and polynomials g_x, h_x such that $h \neq 0$ on U_x and $f = \frac{g_x}{h_x}$ on U_x.

We started by defining regular maps on affine varieties, then generalized to quasi-affine varieties—that led to the above definition. Now, we would like to define it for quasi-projective varieties.

Today, we shall define regular maps in more generality.

5.1 Definition. A **quasi-projective variety** is a boolean combination of projective varieties. Sometimes people require this to be locally closed (i.e. the intersection of a closed and an open); we are allowing finite unions of locally closed sets.

5.2 Example. Every affine variety is a quasi-affine variety because it is a closed set inside affine space, but affine space is an open subset of projective space.

Recall that $\mathbb{P}^n_i \subset \mathbb{P}^n$ is the set $\{[x_0 \dots x_n] : x_i \neq 0\}$, which is the ith copy of $\mathbb{A}^n$ inside $\mathbb{P}^n$.

5.3 Definition. Let $X \subset \mathbb{P}^n$ be quasi-projective. A **regular map** $\phi : X \to \mathbb{P}^m$ is a continuous map (in terms of the Zariski topology) such that for every $x \in X \cap \mathbb{P}^n_i$ with $\phi(x) \in \mathbb{P}^m_j$, the restriction

$$\phi|_{X \cap \mathbb{P}^n_i \cap \phi^{-1}(\mathbb{P}^m_j)} : X \cap \mathbb{P}^n_i \cap \phi^{-1}(\mathbb{P}^m_j) \to \mathbb{P}^m_j$$

is a regular map of quasi-affine varieties.

Practically, these maps are going to be of the form

$$[x_0 \dots x_n] \to [F_0(x) \dots F_m(x)]$$

where each F_j is homogeneous and all are of the same degree; the latter condition means that $[F_0 \dots F_m]$ is well-defined when at least one is not zero. So this map is defined outside the set of common zeros of the F_j.

5.4 Example. If V, W are finite-dimensional vector spaces over k, then there is a map

$$\mathbb{P}(V \oplus W) - \mathbb{P}(V) \to \mathbb{P}(W)$$

sending

$$[v_0 \dots v_n w_0 \dots w_m] \to [w_0 \dots w_m]$$

which is well-defined except when the w_i are all zero, i.e. outside of $\mathbb{P}(V) \subset \mathbb{P}(V \oplus W)$. This is called **projection** away from V.

For example, let V be a line and W a plane. Then $\mathbb{P}(V)$ is the point $[1 : 0 : 0] \in \mathbb{P}^2$. We would like to describe $\mathbb{P}(V \oplus W) - \mathbb{P}(V) \to \mathbb{P}(W)$ in coordinate charts. Consider the coordinate chart of $\mathbb{P}(V \oplus W) = \mathbb{P}^3$ of points $(x, y) \to [x : 1 : y]$ (this is where the second coordinate is zero). Then projection sends this to $[1 : y]$. But this goes to y in the coordinate chart of $\mathbb{P}(W)$ where the second coordinate does not vanish. So in coordinates, this is just projection $\mathbb{A}^2 \to \mathbb{A}^1$, $(x, y) \to x$.

The following is the main reason.

5.5 Theorem. *Let X be projective and $f : X \to Y$ be regular. Then $f(X) \subset Y$ is closed.*

Projectiveness is important, since this fails for affine (or quasi-projective, quasi-affine) varieties.

Remark. Over $\mathbb{C}$, $\mathbb{P}^n_{\mathbb{C}}$ is compact, so any projective variety is compact (in the classical topology). When you apply a continuous map, you get a closed set (indeed, a compact one). This is the topological version of this. In fact, this topological argument can be adapted to algebraic geometry, but then it only works in characteristic zero.

We begin with a lemma:

5.6 Lemma. *The set of linear transformations* $\operatorname{Hom}(k^n, k^m)$ *that are surjective is Zariski open.*

We endow the set of linear transformations with a structure of affine space, of course.

Proof. A matrix is onto if and only if one of the m-by-m minor which is nonzero. These minors are polynomials in the coordinates, so this set of surjective transformations is described by the nonvanishing of a few polynomials. ▲

Here is the main point to the idea of the proof of the theorem.

5.7 Proposition. *If* $Z \subset \mathbb{P}^n \times \mathbb{A}^m$ *is closed, then its (linear) projection to* $\mathbb{A}^m$ *is closed.*

Remark. It is clear what $\mathbb{P}^n \times \mathbb{A}^m$ is as a set. This can be viewed as a topological space as a subspace of $\mathbb{P}^m \times \mathbb{P}^n$ via the Segre embedding. Alternatively, we could cover $\mathbb{P}^n \times \mathbb{A}^m$ by affine spaces $\mathbb{A}^n \times \mathbb{A}^m$ and verify that we get the same topology. However, this is **not** the product topology.

5.8 Example. The locus $xy = 1$ is closed in the Zariski topology of $\mathbb{A}^2$ but not in the product topology $\mathbb{A}^1 \times \mathbb{A}^1$.

We now prove the proposition.

Proof. Now Z is defined by some homogeneous polynomials in the entries of a matrix

$$(x_i y_j)$$

where $x_i, 1 \leq i \leq n$ are coordinates for $\mathbb{P}^n$; the $y_j, 1 \leq j \leq m$ are coordinates for $\mathbb{A}^m$. The polynomials (call them $F_1(x, y), \dots, F_k(x, y)$) are homogeneous in the y_i but not necessarily in the y_j. This is because they are necessarily homogeneous in the elements of the matrix

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{bmatrix} \begin{bmatrix} 1 : y_1 : \cdots : y_m \end{bmatrix}$$

which describes the Segre embedding (with the usual embedding $\mathbb{A}^m \to \mathbb{P}^m$).

Now $p \in \mathbb{A}^m$ is not in the image of Z if and only if the polynomials

$$F_1(x, p), \dots, F_k(x, p)$$

have no zero in $\mathbb{P}^n$ (in x). By the projective version of the Nullstellensatz (which was in the homework), this means that the ideal in $k[x_0, \dots, x_n]$ generated by the $F_i(x, p)$

contains a power of each x_i. In particular, the ideal must contain all homogeneous polynomials of sufficiently large degree. And conversely.

Write $S_d = \{\deg d \text{ homogeneous poly in } x_0, \dots, x_n\}$. In particular, p is not in the image if and only if there is N such that

$$S_N \subset (F_i(x,p)).$$

I.e. each element of S_N can be written as a linear combination of the $F_i(x,p)$ with coefficients in the polynomial ring. However, S_N is a homogeneous ideal. Given that F_i is homogeneous, say of degree d_i, we can find N such that the map

$$T_N(p) : S_{N-d_1} \times \dots S_{N-d_k} \to S_N$$

sending $g_1, \dots, g_k$ to $\sum g_i F_i(x,p)$ is onto.

We have a map $p \to T_N(p)$ sending

$$p : \mathbb{A}^n \to \operatorname{Hom}(S_{N-d_1} \times \dots \times S_{N-d_k}, S_N)$$

sending p to the map $T_N(p)$ described above. This is actually a regular map; we have an explicit formula for it above in terms of polynomials. Also, we know that p is in the projection of Z if and only if all the $T_N(p)$ are not surjective.

However,

$$W_N = \{p : T_N(p) \text{ is not surjective}\}$$

is closed. Indeed, if Q is the set of matrices $S_{N-d_1} \times \dots \times S_{N-d_k} \to S_N$ which are *not surjective*, then

$$W_N = T_N^{-1}(Q)$$

while Q is closed, and T_N—being regular—is continuous. We know, however, that the projection of Z is the intersection of all the W_N; so it is closed as well. ▲

This kind of argument goes at least back to Newton with his theory of resultants. He considered the case where $n = 1$, and tried to find when two polynomials had common roots, and obtained actual formulas for when this happened. The present proposition is a vast generalization.

We now return to the task of proving the big theorem. First, a lemma.

5.9 Lemma. *Suppose X, Y quasi-projective. Let $f : X \to Y$ is regular, then the graph of f, namely $(x, f(x)) \subset X \times Y$, is closed.*

Proof. One can reduce to showing that the graph of the identity is closed. ▲

Proof of theorem 5.5. Any map $f : X \to Y$ can be factored into

$$X \to X \times Y \to Y$$

as a composition of a graph $x \to (x, f(x))$ and a projection $(x, y) \to y$. We have shown that the graph morphism is always closed for quasi-projective varieties. If X is closed in $\mathbb{P}^n$, then $X \times Y$ is closed in $\mathbb{P}^n \times Y$. So the graph of f is a closed subset of $\mathbb{P}^n \times Y$. The image via projection, which is $f(X)$, is closed in Y by the proposition. [Technically, one should note that the proposition implies that if $Z \subset \mathbb{P}^n \times Y$ is closed, so is its projection onto Y—this follows by taking an affine cover of Y and using the usual statement of the proposition.] ▲

this is to be edited.

Lecture 6
[Section] 9/13

We started by discussing some supplemental exercises.

6.1 Exercise. Prove that the following are equivalent:

1. X is noetherian.

2. Each class of closed sets of X has a minimal element.

3. Every open subset of X is quasi-compact[6]

Moreover, prove that if X is noetherian and Hausdorff, then X is finite and discrete.

Solution. The first part is a tautology.

For the last part, all open sets (being quasi-compact) are closed; thus every open subset of X is closed. If X were not finite, we could find an infinite open set U and a sequence $\{x_i\} \subset U$, and then consider $U - \{x_1\}, U - \{x_1 \cup x_2\}, \dots,$ which is a descending sequence of open (hence closed) sets that does not terminate.

6.2 Exercise. Find an irreducible $f \in \mathbb{R}[x, y]$ such that the variety $V((f)) \cap \mathbb{A}^2$ is reducible.

Solution. Consider

$$x^2(x-1)^2 + y^4$$

which consists of two points. This is a nice solution; I wish I had thought of it.

We then went on to discuss the solutions to some of the problem sets from the class, which I will not TeX up.

Lecture 7
9/15

Last time, we proved the important result that if X is projective and $f : X \to Y$ regular, then $f(X)$ is closed. The key point was that if $Z \subset \mathbb{P}^n \times \mathbb{A}^m$ is closed, then its projection to $\mathbb{A}^m$ (the second coordinate set) is closed. You might wonder what happens for nonprojective varieties. In general, the image of a closed set is not closed, but they are also not arbitrary.

Similarly, one can prove:

7.1 Proposition. *If $Z \subset \mathbb{A}^n \times \mathbb{A}^m$ is closed, its projection to $\mathbb{A}^m$ is constructible. More generally, if Z is constructible, its projection is constructible.*

[6] I.e. every open cover has a finite subcover, but the space is not required to be Hausdorff.

Recall that a **constructible** something is a boolean combination of closed sets.

So if $\phi(x, y)$ is a boolean combination of formulas of the form "$F(x, y) = 0$ ($F \in k[X, Y]$)," [7] then the formula

$$(\exists x)\phi(x, y)$$

is equivalent to a formula of the first form (i.e. a boolean combination of formulas of the form $F(x, y) = 0$), because represents the projection of a constructible set. In particular, the formula $(\exists x)\phi(x, y)$ is equivalent to a formula without quantifiers. By induction, one can show that:

7.2 Proposition. *Any formula in the theory of algebraically closed fields of fixed characteristic is equivalent to a formula without quantifiers.*

In particular, first-order logic for alg. closed fields of a fixed characteristic can represent only a combination of polynomial equations and inequations. This adds to what we showed earlier, that the same first-order sentences are true in any two alg. closed fields of a given characteristic.

7.3 Corollary. *Any regular map from an irreducible*[8] *projective variety to an affine variety is constant.*

Proof. Let X be the projective variety. We can assume the affine variety is just $\mathbb{A}^1$. In particular, it is enough to prove that any regular $X \to \mathbb{A}^1$ is constant. This is because if $Y \subset \mathbb{A}^n$, then we can show that all the coordinate maps of $X \to Y$ are constant.

So pick $f : X \to \mathbb{A}^1 \subset \mathbb{P}^1$. We get a map $f : X \to \mathbb{P}^1$ by composing with the inclusion $\mathbb{A}^1 \to \mathbb{P}^1$. The image $f(X)$ is closed by yesterday's lecture. The only closed subsets of $\mathbb{P}^1$ are the finite sets and all of $\mathbb{P}^1$; since $f(X) \subset \mathbb{A}^1 \neq \mathbb{P}^1$, we have that $f(X)$ is finite. Since X is irreducible, $f(X)$ is connected and can only consist of one point. ▲

§1 Finite morphisms

Here is an aside that could have been covered earlier. It gives a useful dictionary.

7.4 Proposition. *Let X be an affine variety. The following sets are in bijection (naturally):*

1. *The points of X.*
2. *Homomorphisms $k[X] \to k$ (of k-algebras).*
3. *Maximal ideals in $k[X]$.*

As usual, $k[X]$ is the affine coordinate ring of X, i.e. the ring of regular functions.

Proof. Given a point $x \in X$, we define the homomorphism $k[X] \to k$ sending a function f to $f(x)$. We just evaluate the functions at the point. So a point maps to a k-homomorphism.

[7] This is precisely the type of formula describing a constructible set.

[8] You need irreducibility, or you could have nonconnected varieties—for instance, two points.

A k-homomorphism (which is necessarily surjective, since it is a k-homomorphism) gives a maximal ideal, just by taking its kernel.

Finally, if $\mathfrak{m} \subset k[X]$ is a maximal ideal, then it is proper and we know (by Hilbert's theorem) that there is a solution $x \in X$ to all equations in $\mathfrak{m}$. This is a point.

We have defined from the first to the second objects, from the second to the third, and from the third to the first. We just need to check that the composition of these three is the identity. We leave this to the reader; note that a maximal ideal can correspond only to *one* point in X. ▲

7.5 Example. Consider $X = V(xy - 1) \subset \mathbb{A}^2$ and the projection $X \to \mathbb{A}^1$ sending $(x, y) \to y$. Morally, it *should* be onto, because polynomials should always have roots—the problem is that the polynomial when $y = 0$ degenerates, and the top coefficient in x goes to zero. In particular, the solution $(x, y) \in \mathbb{A}^2$ lying over $y \in \mathbb{A}^1$ goes off to infinity when $y \to 0$. In projective space, infinity will be a point. So in projective space, there is nowhere to run off to.

We want something that rules out these pathologies. Consider a variety of the form $V(a_0(y) + \cdots + a_N(y)x^N)$ where $a_N(y)$ is never zero; this means that it is constant, and we can assume that the equation is of the form

$$V(x^N + a_{N-1}x^{N-1} + \cdots + a_0(y)).$$

This is a good thing and rules out the messiness of the previous example.

We make a definition out of this:

7.6 Definition. Let $f : X \to Y$ be affine varieties with $f(X)$ dense in Y (e.g. we could restrict to $Y = \overline{f(X)}$ if this is not already true). This implies that the map $k[Y] \to k[X]$ (given by the pull-back on regular functions) is injective, because a function on Y which restricts to zero on X has a dense set of zeros on Y.

So $k[Y] \subset k[X]$ in some sense.

We say that f is **finite** if $k[X]$ is integral over $k[Y]$, so is finitely generated as a module. (Integrality means that every element in $k[X]$ satisfies a monic polynomial over $k[Y]$.)

You can extend this definition when the map $X \to Y$ is not dominant (i.e. say that $k[X]$ is a finitely generated $k[Y]$-module). However, you don't gain anything, because you just take the closure of its image. We shall not use this extended definition.

One reason it's called finite is the following.

Let $X \to Y$ be a finite morphism. In particular, the first coordinate function $x_1 : X \to \mathbb{A}^1$ satisfies a monic polynomial over $k[Y]$. This means that there is some relation

$$f_0(y) + \cdots + f_{N-1}(y)x_1^{N-1} + x_1^N = 0$$

where $f_N(y) \equiv 1$. If we fix y, there are only finitely many possibilities for x_1. Similarly, if y is fixed, there are only finitely many possibilities for $x_2, \dots$. It follows that if y is fixed, there are only finitely many possibilities for the points $(x_1, \dots, x_n)$ lying above it.

7.7 Proposition. *$f^{-1}(y)$ is finite for every $y \in Y$.*

Finite fibers does not imply finiteness; for instance, the projection from $V(xy-1) \to \mathbb{A}^1$ has finite fibers but is not finite.

7.8 Theorem. *If $f : X \to Y$ is a finite map of affine varieties, then f is onto.*

Proof. Let $y \in Y$ be a point. Then y corresponds to a maximal ideal $\mathfrak{m} \subset k[Y]$. If you take a function on Y, it evaluates to zero on y if and only if it lies in $\mathfrak{m}$.

Now $f^{-1}(y)$ corresponds to maximal ideals of $k[X]$ that contain $\mathfrak{m}$ (and so $\mathfrak{m}k[X]$).[9] To say that a fiber is empty means that $\mathfrak{m}k[X]$ is contained in no maximal ideal, so is $k[X]$. But by integrality, this is impossible by the lying over theorem in commutative algebra. ▲

7.9 Example. Take the variety $x - y^2$ and project onto the x-coordinate. We get a map $V(x - y^2) \to \mathbb{A}^1$; it is clear that this is a finite map since the y-coordinate is integral over $k[x]$ (because $y^2 = x$!). Note that the fibers $f^{-1}(x)$ are of size two for most points, but is a singleton for $x = 0$. This is not a "fibration." The different points in the fibers can "collapse" into each other, though they cannot run away to infinity.

7.10 Example. If $X \subset \mathbb{P}^n$ and is a proper closed subvariety and $p \notin \mathbb{P}^n - X$, then the projection out of X away from p gives a finite map from X into its image in $\mathbb{P}^{n-1}$. But we have to define what finiteness means for projective space. Repeating this process, we find that any projective variety admits a finite (surjective) map to some $\mathbb{P}^m$ (possibly $m = 0$). This is a nice way to think of a general variety. Another thing you get from this is the **dimension** of the variety X; we can call m the dimension. (In fact, we will give another definition of dimension, and prove that these two equivalent.)

Lecture 8
9/17

Last time, X was an affine variety; a regular $f : X \to Y$ with dense image was called **finite** if $k[X]$ is integral over $k[Y] \subset k[X]$. (The density of the image is necessary for the inclusion.) To be on the safe side, let us assume that X is an irreducible affine variety.

8.1 Definition. Maps with dense image are called **dominant**.

Note that dominant maps induce injections of the rings of regular functions.

Now we'd like to extend the definition of a finite map to a quasi-projective variety. We would like to define a map to be finite if it is locally finite in a sense, with respect to some affine cover. For this, we need to know that we can cover a quasi-projective variety by affine things.

8.2 Proposition. *If X is affine and $f \in k[X]$ is nonzero, then the open set set X_f consisting of points where $f \neq 0$ is isomorphic to an affine variety.*

This is a generalization of the idea that $\mathbb{A}^1 - \{0\}$ is isomorphic to the affine variety $V((xy - 1)) \subset \mathbb{A}^2$.

[9] Exercise in working out the correspondence.

Proof. The set X_f is the projection of the affine variety

$$\left\{(x,y) \in X \times \mathbb{A}^1 : f(x)y = 1\right\}$$

. Projection is obviously an isomorphism, since we can define the inverse $x \to (x, 1/f(x))$ on X_f. ▲

Remark. If X is affine, then the sets X_f for $f \in k[X]$ form a *basis* of the (Zariski) topology of X. So there is a basis of the topology consisting of open sets which are isomorphic to affine varieties. The reason is that any closed subset is the roots of a bunch of polynomials. Take one of these polynomials; its zero set is a bigger closed set, while its nonzero set (i.e., X_f for some f) is a small open set. We leave the details to the reader.

8.3 Proposition. *Suppose X, Y are affine varieties. Let $f : X \to Y$ be a regular map. Then $f : X \to Y$ is finite if and only if every point in Y has an open neighborhood U with $U, f^{-1}(U)$ both isomorphic to affine varieties and such that $f : f^{-1}(U) \to U$ is finite.*

Note that it is possible by the previous definitions to say what it means for a map between two constructible sets isomorphic to affine varieties to be *finite*; just pull back by the isomorphism. This result says that finiteness is a *local* condition.

For the future, we shall simply say that a constructible set is **affine** if it isomorphic to an affine variety, for convenience.

Proof. One direction is clear (take the trivial cover). The other direction is harder.

Let $k[X] = A, k[Y] = B$, and assume that there is a cover of Y by open affine[10] sets of the form $Y_{b_\alpha}, b_\alpha \in B$ such that $f^{-1}(Y_{b_\alpha})$ is affine $f^{-1}(Y_{b_\alpha}) \to Y_{b_\alpha}$ is finite. We can make this a finite cover, since Y is quasi-compact. The fact that $Y = \bigcup Y_{b_\alpha}$ implies that the $b_\alpha \in k[Y]$ generate the unit ideal, so there is an equation of the form

$$\sum a_\alpha b_\alpha = 1, \; a_\alpha \in B = k[Y].$$

Now $f^{-1}(Y_{b_\alpha})$ is the set of all points such that $b_\alpha \circ f$ does not vanish; this means that the image of b_α in $k[X]$ does not vanish. We shall just write this as b_α, following the spirit of the inclusion $k[Y] \to k[X]$.

By the construction of the previous proposition,

$$k[Y_{b_\alpha}] = k[Y]_{b_\alpha} = B_{b_\alpha}$$

and

$$k[X_{b_\alpha}] = k[X]_{b_\alpha} = A_{b_\alpha}$$

so we have interpreted in terms of localization. By assumption, we have that

$$k[Y_{b_\alpha}] \to k[X_{b_\alpha}] \quad \text{or} \quad B_{b_\alpha} \to A_\alpha$$

[10] We can reduce to this case.

is integral. In particular, there is a finite set of generators of A_{b_α} over B_{b_α}. Call this set of generators $\left\{\xi_{j,\alpha}/b_\alpha^N\right\}$ for each α.

I claim that A is a finite B-module, in fact. More particularly, we claim that the ξ_α generate A as a B-module. Take any $a \in A$. For each α, then $a \in A_{b_\alpha}$ so that a can be written in a B_{b_α}-linear combination of the $\xi_{j,\alpha}/b_\alpha^N$ in A_α. It follows that in A, $b_\alpha^{M_\alpha} a$ (for some $M_\alpha \geq N$) can be written as a B-linear combination of the ξ_α, in A, say

$$b_\alpha^{M_\alpha} a = \sum c_{j,\alpha}\xi_{j,\alpha}, \quad c_{j,\alpha} \in B.$$

Since the $\left\{b_\alpha^{M_\alpha}\right\} \subset B$ generate the unit ideal (they have no common zero since the b_α don't, or one could argue directly based on commutative algebra), it follows that a itself can be written as a B-combination of the ξ_α. This proves that the ξ_α generate B as A-module. This proves the result. ▲

8.4 Definition. Let X, Y be *quasi-projective* varieties. Then $f : X \to Y$ is **finite** if for every $y \in Y$, there is an open affine $U \subset Y$ containing y with $f^{-1}(U)$ affine and $f^{-1}(U) \to U$ finite.

We now give a useful example of a finite map. We want to prove:

8.5 Proposition. *If $X \subset \mathbb{P}^n$ is closed and $P \in \mathbb{P}^n - X$, then the projection away from P gives a finite map $X \to \mathbb{P}^{n-1}$.*

Then of course, you can iterate, if you didn't get that the projection was surjective.

Proof. Wlog, P is the point $[0\ 0\ \dots\ 0\ 1]$; projection away from P sends $[x_0 \dots x_n] \in \mathbb{P}^n - P$ to $[x_0 \dots x_{n-1}]$.

Let us start by choosing the most natural cover of $\mathbb{P}^{n-1}$ by open affines. Suppose first that X is defined by $f_1(x) = \cdots = f_n(x) = 0$. Since $P \notin X$, it can't be that the projective version of the Nullstellensatz,[11] we find that

$$x_n^M \in (f_1, \dots, f_n) + (x_1, \dots, x_{n-1}) \subset k[x_0, \dots, x_n]$$

for some power M. For every $i \leq n-1$, the set $\mathbb{P}_i^n \cap X$ (i.e., the subspace of X where the i-th coordinate is nonzero) is an affine subvariety of $\mathbb{A}^n$. Moreover, $\mathbb{P}_i^{n-1} \cap f(X)$ is affine because $f(X)$ is closed. The cover $\mathbb{P}_i^n$, $0 \leq i \leq n-1$ covers X (because $P \notin X$); the $\mathbb{P}_i^{n-1}$. It is clear that $\mathbb{P}_i^n \cap X$ is the pre-image of $\mathbb{P}_i^{n-1} \cap f(X)$ under projection.

Now $k[\mathbb{P}_i^n \cap X]$ is generated by $x_0/x_i, \dots, x_n/x_i$. Each x_j/x_i for $j < n$ is already contained in $k[\mathbb{P}_i^{n-1} \cap f(X)]$, however. But x_n/x_i isn't; we have to show that it is integral. Indeed, x_n/x_i satisfies a monic polynomial equation in the others thanks to the equation above. Indeed, if we can write

$$x_n^M = \sum g_i f_i + \sum_{i<n} b_i x_i \in k[x_0, \dots, x_n]$$

then we can assume that the b_i are homogeneous of degree $M-1$. When reducing modulo the coordinate ring of X and dividing by x_i^M, we find that $(x_n/x_i)^M$ is integral over the x_j/x_i.

▲

[11] An easy corollary of the affine one.

8.6 Corollary (Noether normalization theorem)**.** *Every projective variety has a finite (surjective) map to a projective space.*

Proof. Indeed, just repeat projections from a point as above, and use the previous result. ▲

We make a definition to be explored more later

8.7 Definition. Let X be an irreducible quasi-projective variety. A **rational function** on X is an equivalence class (f, U) where $f : U \to k$ is a regular function and $U \subset X$ is an open subset. Two $(f, U), (g, V)$ are considered **equivalent** if $f = g$ on $U \cap V$. Since X is irreducible, note that $U \cap V$ is dense in U, V.

Lecture 9
9/20

Last time, we ended with the definition of a rational function on a variety. If $X \subset \mathbb{P}^n$ is an irreducible quasi-projective variety, then a **rational map** $\phi : X \dashrightarrow \mathbb{A}^1$ is an equivalence class of pairs (U, f), where $U \subset X$ is open and quasi-affine subset and $f : U \to \mathbb{A}^1$ regular. Two $(U, f), (V, g)$ are considered equivalent if f, g agree on $U \cap V$. The collection of all rational functions on X is denoted

$$k(X).$$

9.1 Example. Let X be an irreducible affine variety. Then $k(X)$ is the quotient field of $k[X]$. Indeed, any fraction $f/g, f, g \in k[X]$ becomes a rational function on X (defined on $\{x : g(x) \neq 0\}$. Conversely, if you have a rational map $\phi : X \dashrightarrow \mathbb{A}^1$, we can choose a basic quasi-affine set X_f (for $f \in k[X]$; this is the set of x where $f(x) \neq 0$) on which it is regular. The regular functions on this are just $k[X]_f$, though. And this injects into the quotient field of $k[X]$.

It is clear that $k(X)$ is always a field. We can add two $(f, U), (g, V)$ by taking $f + g$ on an open quasi-affine subset of $U \cap V$. Same for multiplication. Division can be done as well; we divide (f, U) and (g, V) by writing $(f/g, U \cap V - (U \cap V)_g)$.

We now define rational functions into other places.

9.2 Definition. Let X be irreducible and quasi-projective. A **rational map** $\phi : X \dashrightarrow \mathbb{P}^n$ is an equivalence class of rational maps $X \dashrightarrow \mathbb{P}^n_i = \mathbb{A}^n \subset \mathbb{P}^n$. A **rational map** from $X \dashrightarrow \mathbb{A}^n$ is just an n-tuple of rational maps to $\mathbb{A}^1$.

The equivalence of $f : X \dashrightarrow \mathbb{P}^n_i$ and $g : X \to \mathbb{P}^i_j$ is given by saying that f, g agree on $f^{-1}(\mathbb{P}^n_j) \cap g^{-1}(\mathbb{P}^n_i)$.

In practice, you can always go to a smaller open subset of X and get a regular morphism into $\mathbb{A}^n$. When you homogeneize these polynomials, you get a rational map into $\mathbb{P}^n$.

9.3 Example. Suppose given polynomials $f_0(x), \dots, f_n(x)$ which are homogeneous of the same degree in $x = (x_0, \dots, x_m)$, which lies in some projective space $\mathbb{P}^m$. Then the map $x \to (f_0(x) : \cdots : f_n(x))$ is a rational map from $\mathbb{P}^m$ into $\mathbb{P}^n$ defined outside the common zero locus of the $\{f_i\}$.

Remark. In general, **rational functions cannot be composed.** It might be that the second function is not defined on the image of the first. Consider for instance the map

$$\mathbb{A}^1 \to \mathbb{A}^2, \quad x \to (x, 0)$$

and

$$\mathbb{A}^2 \to \mathbb{A}^1, \quad (x, y) \to 1/y.$$

There is nonetheless a special case of maps which are invertible.

9.4 Definition. A **birational isomorphism** between X, Y (irreducible quasiprojective varieties) is a rational map $\phi : X \dashrightarrow Y$ (i.e. a map of X into the projective space in which Y lives whose image is in Y) for which there is a rational map $\psi : Y \dashrightarrow X$ such that the following holds.

1. $\phi(X)$ is dense in Y and $\psi(Y)$ is dense in X. This enables us to compose the maps ψ, ϕ, because if the image of a morphism is dense, it contains an open dense subset (because the image is always constructible).

2. On open dense sets $\phi \circ \psi = 1$ and $\psi \circ \phi = 1$.

We shall in this case say that X, Y are **birational**. Birationality is an equivalence relation.

9.5 Example. 1. Every irreducible variety is birational to any of its open sets. In particular, it is birational to some affine variety, since the open affines form a basis.

2. Any plane conic C (i.e. the zero set of an irreducible quadratic equation in two variables) is birational to $\mathbb{P}^1$ (hence to $\mathbb{A}^1$). Indeed, pick any $p \in C$ and consider the projection away from p, which is defined on $C - \{p\}$. It is either constant (in which case C is contained in a line, hence is birational to a line), or it is nonconstant. If it is nonconstant, I claim that it is one-to-one.

   The point is that we are drawing through p a bunch of lines of varying slope and intersecting them with C. Each line can intersect C at most twice (since C is defined by a quadratic equation), and hence only at one point other than C. It follows that $C - \{p\} \to \mathbb{P}^1$ defined by this projection must be one-to-one and onto an open dense set. The inverse map sending a direction in $\mathbb{P}^1$ to the intersection of $C - p$ is the inverse; it is actually regular. We will give the justification in words. Given a line with a slope t through p, you can plug this into the equation for C to get a quadratic polynomial in one variable. One of the solutions is p; you can divide by $(x - p)$ to get a linear equation, and then find the other solution.

3. Suppose $k = \mathbb{C}$ and, in the previous part of this example, p had rational coordinates (in $\mathbb{Q}^2$). Suppose C is defined by a polynomial in $\mathbb{Q}[x, y]$. Then the rational maps of projection and its inverse are given by rational functions with coefficients in $\mathbb{Q}$. In particular, if you start with a rational point in $C \cap \mathbb{Q}^2$, it projects to a rational point in $\mathbb{P}^1$; if you start with a rational point in $\mathbb{P}^1$, it goes to a rational point in C.

The last part of this example shows:

9.6 Proposition. *If a conic defined over $\mathbb{Q}$ has a rational point, then it has infinitely many.*

We can actually parametrize the rational points of the conic by using the inverse.

This approach is due to the Greeks, who proved that there are infinitely many Pythagorean triples. In that case, one seeks to find the rational points on

$$x^2 + y^2 = 1.$$

One starts with the rational point $(1, 0)$ and uses it to get a parametrization for all the rational points on the circle.

As yet another example, suppose now $k = \mathbb{C}$ but we start with $p \in \mathbb{R}^2$ and C is defined by something in $\mathbb{R}[x, y]$. We get an almost bijection between $\mathbb{R}^1$ and the real points on C, i.e. $C \cap \mathbb{R}^2$. This might not be sufficient if you want all the points, but it can help compute integrals.

Call the map $\mathbb{R} \to C \cap \mathbb{R}^2$ as t.

In particular, if g is any rational function in $\mathbb{R}(X, Y)$, then

$$\int_{C\cap\mathbb{R}^2} g(x, y)dx$$

is equal to

$$\int_{\mathbb{R}} g(x(t), y(t))x'(t)dt$$

where everything here is rational. This integral can be done using partial fractions, and one gets an indefinite integral which is elementary. By contrast, this **completely fails** for higher order curves (e.g. cubics); one runs into things like elliptic functions. In fact, the general quadric will have only finitely many rational points.

Now we are very eager to know which varieties are birational to the line. More generally, we are curious when two curves or varieties are birational. There is one obvious invariant: the field of all rational functions.

9.7 Proposition. *If X, Y are birational, then $k(X), k(Y)$ are k-isomorphic.*

Proof. This is because we can compose a rational function $Y \to \mathbb{A}^1$ and pull it back to $X \to \mathbb{A}^1$, and conversely in the other direction. ▲

The converse is also true.

9.8 Proposition. *If $k(X), k(Y)$ are k-isomorphic, then X, Y are birational.*

So the question of birational equivalence classes turns into a question about finitely generated extensions of k.

Proof. Without loss of generality, X, Y are affine varieties. Suppose $X \subset \mathbb{A}^n$, for instance. We have regular functions $x_1, \dots, x_n : X \to \mathbb{A}^1$. Given an isomorphism $k(X) \simeq k(Y)$, the x_i pull back to give rational functions $\phi_1, \dots, \phi_n$ on Y. Restricting to the domain $V \subset Y$ where these are all defined, we get a regular map

$$\phi : V \to \mathbb{A}^m, \quad v \to (\phi_1(v), \dots, \phi_n(v))$$

which must have image contained in X. One similarly defines $\psi : Y \dashrightarrow X$, which is the inverse. One should check that these induce isomorphisms on open sets. ▲

We end with a definition.

9.9 Definition. For X irreducible, the **dimension of** X is the transcendence degree of $k(X)$ over k.

Lecture 10
[Section] 9/20

We discussed some of the homework, as well as some additional problems.

10.1 Exercise. Suppose $f, g : X, Y$ are regular maps between quasiprojective varieties that agree on an open dense subset. Then $f = g$.

10.2 Exercise. When are two irreducible algebraic curves homeomorphic in the Zariski topology? (Answer: Always.)

10.3 Exercise. Let $X \subset \mathbb{P}^2$ be a one-dimensional nonsingular complex variety. Then the set of regular maps $X \to \mathbb{P}^1$ are in bijection with the meromorphic functions on the complex manifold X. (This exercise should not be taken too seriously—it was more of a discussion.)

If $X \to \mathbb{P}^1$ is nonconstant, then it should be thought of as a "branched cover" of $\mathbb{P}^1$.

10.4 Exercise. The automorphism group of $\mathbb{P}^1$ is the automorphism group of the rational function field $k(x)$ because any automorphism induces an automorphism of the rational function field. This in turn is $\mathrm{PGL}_2(\mathbb{C})$. These correspond analytically to the "linear fractional transformations" of the Riemann sphere.

10.5 Exercise. Why is the intersection of affine open sets U, V affine again? It is a closed subset of the affine set $U \times V$, namely the intersection of this with the diagonal.

10.6 Exercise. The varieties $\mathbb{P}^2 - \{0\}$ and $\mathbb{P}^1 \times \mathbb{A}^1$ are not affine.

10.7 Exercise. Under what conditions is the Zariski topology on $X \times Y$ the product of the Zariski topology of X and the Zariski topology on Y? When one of them is finite.

10.8 Exercise. Suppose we have a finitely generated group Γ and an injective homomorphic map $\Gamma \to GL_n(\overline{\mathbb{Q}})$. The image will in $GL_n(K)$ for some number field K. Prove that for almost every prime, there is a finite index subgroup $\Gamma' \subset \Gamma$ such that for every nonidentity element γ in Γ', γ survives in a p-group quotient of Γ'.

Sketch. Indeed, K contains a ring of integers $\mathcal{O}_K$. We can look at the denominators of matrix entries in Γ and which primes divide those denominators; there can be finitely many of them since Γ is finitely generated. Localizing at a prime $\mathfrak{q}$ of $\mathcal{O}_K$ not among those, we can take a map

$$\Gamma \to GL_n((\mathcal{O}_K)_{\mathfrak{q}}).$$

Let's complete at $\mathfrak{q}$. We get a map

$$\Gamma \to GL_n(\hat{\mathcal{O}}_{\mathfrak{q}})$$

We have a reduction map $\hat{\mathcal{O}}_{\mathfrak{q}}/\mathfrak{q}^n$ into something of the form $(\mathbb{F}_{p^n})^m$. Taking the kernel of Γ into GL of a finite field, we can get the result. ▲

Lecture 11
9/22

Last time, we talked about rational functions and birational maps. We ended up, finally, with the most important invariant of algebraic varieties, their **dimension**. We rewrite

11.1 Definition. If X is an irreducible quasiprojective variety, then the **dimension** of X is the transcendence degree of the field of rational functions $k(X)$ over k.

We give examples of basic properties of the dimension.

11.2 Example.

1. This is a birational invariant, because birational equivalence induces isomorphisms on the fields of fractions.
2. The dimension of an irreducible variety is the dimension of any nonempty open set.
3. In particular, $\dim \mathbb{P}^n = \dim \mathbb{A}^n$. We know that the rational function field of $\mathbb{A}^n$ is the quotient field of $k[x_1, \dots, x_n]$, so $k(\mathbb{A}^n) = k(x_1, \dots, x_n)$, which has transcendence degree n. So
$$\dim \mathbb{P}^n = \dim A^n = n.$$
4. $\dim(X \times Y) = \dim X + \dim Y$. Without loss of generality, both X and Y are affine. Then if $k(X)$ is generated by n elements and $k(Y)$ by m elements, then $k(X \times Y)$ is generated by $n + m$ elements.

11.3 Proposition. $\dim X = 0$ *if and only if* X *is a point (since* X *is irreducible).*

Proof. Let's prove this. Indeed, the function field of a point is just k. Conversely, suppose $\dim X = 0$; then $k(X) = k$ since k is algebraically closed. We can assume that $X \subset \mathbb{A}^n$ for some n. Then the coordinate functions $x_1, \dots, x_n$ are all constant on X because $k(X) = k$; it thus follows that X is reduced to a point. ▲

11.4 Proposition. *If* X, Y *are irreducible and* $f : X \to Y$ *is finite (and surjective), then* $\dim X = \dim Y$*.*

Proof. Without loss of generality, X, Y are finite. This means that $k[X]$ is integral over $k[Y]$. In particular, $k(X)$ is algebraic over $k(Y)$. Therefore they have the same transcendence degree over k. ▲

In particular, the earlier definition of "dimension" was correct. The earlier definition was as follows: take X an irreducible projective variety, and find a finite projection onto $\mathbb{P}^n$ for some n. (We showed we could do this by repeated projection from a point.) Then $\dim X = n$ by the above the proposition.

Just to satisfy curiosity, we make:

11.5 Definition. For non-irreducible varieties, the **dimension** is the maximum of the dimension of all irreducible components. It is possible that the different components may have different dimensions.

X is called **of pure dimension** k if every irreducible component has dimension k.

Finally, we get to a truly nontrivial statement.

11.6 Proposition. *If Y is quasiprojective is irreducible and $X \subset Y$ is a proper closed subvariety, then* $\dim X < \dim Y$.

Proof. It is evident that $\dim X \leq \dim Y$ since the ring of regular functions on X is a quotient of the ring of regular functions on Y (at least when X, Y are affine, this does the trick, and that's all we need).

Suppose now that $d = \dim X = \dim Y$ and $X \subset Y$, $X \neq Y$. We can assume, without loss of generality, that $X, Y \subset \mathbb{A}^n$ are affine. The coordinate functions on $x_1, \dots, x_n$ become regular functions on X. These generate $k(X)$ over k, since they generate the ring of regular functions $k[X]$. In particular, d of these generate a purely transcendental extension (of degree d). Without loss of generality, we can assume that

$$x_1|_X, x_2|_X, \dots, x_d|_X \text{ are alg. independent in } k(X).$$

When restricted to Y, they still can't satisfy any algebraic identity, and these must therefore form a transcendence basis for $k(Y)$ as well.

It follows that $k(Y)/k(x_1|_Y, \dots, x_d|_Y)$ is a finite extension. Let f be a polynomial that vanishes on X but not on Y. Now f has a minimal polynomial over $k(x_1, \dots, x_d)$. It follows that f satisfies a minimal equation:

$$f^n = a_{n-1}(x_1, \dots, x_d) f^{n-1} + \dots + a_0(x_1, \dots, x_d) = 0.$$

If we restrict to points of X, we find that

$$a_0(x_1, \dots, x_d) = 0$$

as a rational function on X, which implies that $a_0 \equiv 0 \in k(x_1, \dots, x_d)$ since the $x_i, 1 \leq i \leq d$ were algebraically independent. This implies that the above polynomial was not minimal, contradiction. ▲

The next main result is that hypersurfaces have codimension one.

11.7 Proposition. *If $X \subset \mathbb{P}^n$ is an irreducible hypersurface (i.e. the zero locus of one nontrivial homogeneous polynomial), then* $\dim X = n - 1$.

Proof. Let f be the homogeneous polynomial of degree d defining X. Then $X \neq \mathbb{P}^n$, so let's assume without loss of generality that $[1, 0, \dots, 0] \notin X$. In particular,

$$f(1, 0, \dots, 0) \neq 0.$$

It follows that f contains a pure power of x_0, i.e. the monomial x^d.

Now consider the projection away from this point $[1, 0, \dots, 0]$. In many cases, we find the dimension by taking a (surjective) finite map. If we show that the projection away from this point is surjective, then we will know that it is finite (since it is finite onto its image), and that will imply that

$$\dim X = \dim \mathbb{P}^{n-1} = n - 1.$$

For any $(\alpha_1, \ldots, \alpha_n) \in k^n - (0, 0, \ldots, 0)$, the polynomial

$$t \to f(t, \alpha_1, \ldots, \alpha_n)$$

has degree d and consequently has nontrivial roots, k being algebraically closed. There is a root

$$(\xi, \alpha_1, \ldots, \alpha_n)$$

which can be considered as an element of $X \subset \mathbb{P}^n$. Its projection to $\mathbb{P}^{n-1}$ is thus $[\alpha_1, \ldots, \alpha_n]$. So the projection of X to $\mathbb{P}^{n-1}$ contains $[\alpha_1, \ldots, \alpha_n]$, hence any element of $\mathbb{P}^{n-1}$. The claim $\dim X = n - 1$ is now clear. ▲

At the end, dimension is also very much connected to counting. Dimension is some notion of size, but in the case of finite fields, the dimension corresponds to size. A variety of dimension k over a field of size p, morally, should have about p^k points rational over that field.

This result also has a converse:

11.8 Proposition. *If $X \subset \mathbb{P}^n$ is a closed subvariety that has dimension $n - 1$ and is irreducible, then X is a hypersurface.*

Proof. Let f be a polynomial in $k[x_0, \ldots, x_n]$ that vanishes on X. If there is no such polynomial, then $X = \mathbb{P}^n$. Since X is irreducible, we can assume that f is irreducible; indeed, if f was a product of two factors, then $V(f)$ would be a union of the zero loci of each factor, but X would have to lie inside one of those zero loci, since it is irreducible.

So f is irreducible and vanishes on X. Then $\dim X = \dim V(f) = n - 1$ by the previous result, and $X \subset Y$; thus from the previous result, we have that

$$X = Y.$$

So X is a hypersurface. ▲

You might think that the zero locus of two polynomials has dimension $n - 2$, and so on. But this is not true in general.

11.9 Example. Think about two parallel affine subspaces in affine space. The first equation could be $x_0 = 0$; the second could be $x_0 = 1$. Then the intersection is given by two equations but it is empty.

This doesn't happen for projective space, which is a great reason to study projective space. We start by proving a special case of this.

11.10 Proposition. *Let $X \subset \mathbb{P}^n$ be an irreducible projective variety and $H \subset \mathbb{P}^n$ is a linear hyperplane, then* $\dim(H \cap X) = \dim X - 1$ *(or $X \subset H$).*

In particular, if X is not finite, it intersects *every* hyperplane, and the intersection has the expected dimension.

Proof. Assume that $H \not\subset X$. The other case is straightforward.

We prove it by induction on n. Choose a counterexample with minimal n. Since $H \not\subset X$, we can choose a point $p \in H - X$. We can project away from p.

Let $\pi : \mathbb{P}^n - p \to \mathbb{P}^{n-1}$ be the projection away from P. Then $\pi(X)$ is a closed subvariety of $\mathbb{P}^{n-1}$. Also, $\pi(H-p)$ is a linear hyperplane.

By minimality of n, we find that either $\pi(X) \subset \pi(H-p)$ (which would imply that $X \subset H$, contradiction) or

$$\pi(X) \cap \pi(H-p) = \dim(\pi(X)) - 1 = \dim X - 1$$

since $\pi|_X : X \to \pi(X)$ is finite. But

$$\pi(X) \cap \pi(H-p) = \pi(X \cap H) = \dim X \cap H$$

since $\pi|_{X\cap H} \to \pi(X \cap H)$ is finite. So $\dim X \cap H = \dim X - 1$. ▲

It now follows from this a much stronger case.

11.11 Proposition. *If $X \subset \mathbb{P}^n$ is closed and irreducible and f is any homogeneous polynomial that does not vanish on X, then*

$$\dim X \cap V(f) = \dim X - 1.$$

Proof. We're out of time for the day ▲

Lecture 12
9/24

§1 Finishing up dimensions

Last time, we considered the question of what the intersection of a projective variety and a hyperplane looked like. Namely, we showed that if $X \subset \mathbb{P}^n$ is irreducible projective and $H \subset \mathbb{P}^n$ a hyperplane, then either $X \subset H$ or

$$\dim H \cap X = \dim X - 1$$

In particular, if you start with something of dimension five, you can't kill it by two linear equations, because adding a linear equation drops the dimension by 1.

12.1 Proposition. *If $X \subset \mathbb{P}^n$ is projective and irreducible*[12] *and $Y \subset \mathbb{P}^n$ is any hypersurface, then either $X \subset Y$ or*

$$\dim X \cap Y = \dim X - 1.$$

[12] We can make a statement for reducible varieties too.

Proof. We can prove this based on the hyperplane theorem. This is a useful trick, which will reappear. Suppose Y is described by an equation of homogeneous degree d. Let $\{F_0, \ldots, F_N\}$ be the set of all monomials of degree d in $n+1$ variables $x_0, \ldots, x_n$; it follows that N is something like $\binom{n+d+1}{n+1} - 1$. (This follows from a well-known combinatorial trick.)

Consider the so-called **Veronese embedding** $V : \mathbb{P}^n \to \mathbb{P}^N$ simply sending

$$V : [x_0, \ldots, x_n] \to [F_0(x) \ldots F_N(x)].$$

This is a regular map and its image is closed, since $\mathbb{P}^n$ is a projective variety. I claim that it is an isomorphism onto its image. Suppose you are given $F_0, \ldots, F_N$: how do you get x_0/x_1? Basically, you divide the monomial corresponding to x_0^d to that corresponding to $x_0^{d-1}x_1$.

Anyway, this map is an isomorphism. Now $V(X)$ is a projective variety in $\mathbb{P}^N$, which is still of dimension $\dim X$. Moreover, $V(X \cap Y)$ corresponds to the intersection of $V(X)$ with a hyperplane. This is because the equation defining Y was a linear combination of some monomials of degree d. Consequently $V(X \cap Y)$ has dimension $\dim X - 1$ (unless $X \subset Y$) from the case of Y itself a hyperplane, proved in the last lecture.

▲

12.2 Corollary. *Any two curves in* $\mathbb{P}^2$ *intersect.*

12.3 Corollary. $\mathbb{P}^2$ *is not isomorphic to* $\mathbb{P}^1 \times \mathbb{P}^1$.

Proof. Indeed, there are two curves in $\mathbb{P}^1 \times \mathbb{P}^1$ that do not intersect. In fact, there are whole families of pairs of curves that do not intersect. For instance, $\{x\} \times \mathbb{P}^1$ and $\{y\} \times \mathbb{P}^1$ do not intersect when $x \neq y$. ▲

Incidentally, $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ are birational, since they both contain $\mathbb{A}^2$ as a dense open subset.

Remark. The fact that $\mathbb{P}^2 \not\simeq \mathbb{P}^1 \times \mathbb{P}^1$ can also be proved using finite characteristic methods. If q is a prime power, the size of $\mathbb{P}^2(\mathbb{F}_q)$ is $q^2 + q + 1$, while the size of $(\mathbb{P}^1 \times \mathbb{P}^1)(\mathbb{F}_q)$ is $(q+1)^2$. Since this holds for any prime power, it follows—by the homework—that the varieties are not isomorphic over fields of any positive characteristic, hence over fields of characteristic zero.

§2 Fibers

One of the philosophies of modern mathematics is to pass to relative statements, i.e. to talk about families of objects. For instance, a vector space is an important 19th century concept. The relative concept, of a **vector bundle**, is an important 20th century concept.

So we don't just want to talk about varieties. We want to talk about **families of varieties**.

12.4 Definition. Let $X \to Y$ be a morphism. Then we can think of X as a family of varieties X_y, the preimage of $y \in Y$, parametrized by the points $y \in Y$.

We can try to study, for instance, how the fibers X_y change as y varies. For instance, we first started the course by determining when a variety is empty. The relative version is to study when X_y is empty. We know that when X is projective, the condition that X_y be empty is a polynomial condition on the y, because the image of X is closed.

12.5 Example. Consider $V(xy+1) \subset \mathbb{A}^2$ and projection on the x-axis to $\mathbb{A}^1$. For every point other than zero, we get a fiber consisting of one point. At zero, we get a variety containing nothing. So the dimension of a fiber can "jump."

12.6 Proposition. *Suppose $f : X \to Y$ is a surjective morphism of varieties of pure dimension* $\dim X, \dim Y$. *Then*

1. *Each fiber X_y has dimension at least* $\dim X - \dim Y$.
2. *For y in an open dense set in Y, we have* $\dim X_y = \dim X - \dim Y$.

Before proving this, we give an example:

12.7 Example. Take the union of both axes in $\mathbb{A}^2$ and project to the x-axis. This is a silly example because the total space is reducible.

12.8 Example (Blow-up of $\mathbb{A}^n$ at the origin)**.** Let $X \subset \mathbb{A}^n \times \mathbb{P}^{n-1}$ be the set of pairs (v, l) (for v a vector in $\mathbb{A}^n$ and l a line in $\mathbb{A}^n$, i.e. an element of $\mathbb{P}^{n-1}$) such that $v \in l$.

Consider the projection $X \to \mathbb{P}^{n-1}$. Over each line, the fiber is the set of vectors in this line. In particular, X is a line bundle over $\mathbb{P}^{n-1}$. The fiber dimensions over $\mathbb{P}^{n-1}$ are all one, and this is called the **tautological line bundle** over $\mathbb{P}^{n-1}$. (Note that the tautological line bundle is not trivial.)

X is in fact irreducible, but we will prove this later.

But look at the projection of the blow-up X to the second coordinate $\mathbb{A}^n$, i.e.

$$\pi : X \to \mathbb{A}^n.$$

The pre-image of 0, $\pi^{-1}(0)$, is all of $\mathbb{P}^{n-1}$, because every line passes through zero. The preimage of any other point $v \in \mathbb{A}^n$ is just the line going through 0 and v, so it is a single point. The fiber dimension thus jumps from zero to n.

Proof of the proposition. Induction on $\dim Y$. We may assume as well that $Y \subset \mathbb{A}^n, X$ are affine by taking preimages, and that Y is irreducible. Let $y \in Y$ be a point. We want to show that the fiber has at least a certain dimension. Choose a hyperplane $H \subset \mathbb{A}^n$ which does not contain Y, but passing through y. We know that

$$\dim Y \cap H = \dim Y - 1.$$

Also, $f^{-1}(Y \cap H) = X \cap f^{-1}(H)$, which is cut out of X by one equation: namely, the pull-back of the linear function defining H to X. We don't know that X is irreducible, but at least we have:

$$\dim(f^{-1}(Y \cap H)) \geq \dim X - 1.$$

Now use induction on $\dim Y$. We get to another situation where the dimension of the target is one smaller, but where the map

$$f^{-1}(Y \cap H) \to Y \cap H$$

has the same fiber at y. By induction on $\dim Y$ (the base case of Y a point is obvious), we are done for 1).

Now let us prove that there is an open dense set $U \subset Y$ on which $\dim X_y$ is constant. Again, we can assume that Y is irreducible. Assume also X is irreducible. Here we will use the fact that $f : X \to Y$ was surjective. Therefore, the map

$$k[Y] \to k[X]$$

is injective, so a map on rational functions $k(Y) \to k(X)$ makes sense. Consider

$$e = \text{tr.deg} k(X)/k(Y) = \dim X - \dim Y.$$

Now $k(X)$ is generated by the coordinate functions $x_1, \dots, x_m$; without loss of generality, $x_1, \dots, x_e$ are algebraically independent over $k(Y)$ and $x_{e+1}, \dots, x_m$ are algebraic over $k(Y)(x_1, \dots, x_e)$.

This means that there are polynomials $F_{e+1}, \dots, F_m$ in $k(Y)[T_1, \dots, T_e][S]$ which are polynomial relations between each $x_i, i > e$. Namely,

$$F_j(X_1, \dots, X_e, X_j) = 0 \quad \forall j > e.$$

By multiplying denominators, we can assume that these polynomials are actually in $k[Y][T_1, \dots, T_e][S]$. For every point of Y, substitution $Y \to y$ we get a relation between $x_1, \dots, x_e$ and x_j. Suppose that this relation is nontrivial. This means that over the fiber, the coordinaten functions $x_j, j > e$ satisfy the algebraic equations over $\{x_1, \dots, x_e\}$. In particular, $k(X_y)$ has transcendence degree at most e. So on the open subset of where these relations are nontrivial, X_y has dimension at most e—hence equal to e.

To reiterate, there is an open set $U \subset Y$, such that the polynomials $F_{j,y} = F_j(y, \cdot) \in k[T_1, \dots, T_e, S]$ show that $x_j|_{X_y}$ is algebraic over $x_1|_{X_y}, \dots, x_e|_{X_y}$, which in turn implies that the function field of the fiber is algebraic over the field generated by $x_1|_{X_y}, \dots, x_e|_{X_y}$. This means that

$$\dim X_y \leq e.$$

But we have shown earlier that

$$\dim X_y \geq e = \dim X - \dim Y.$$

▲

We are almost out of time today, so let us state the result that will imply that the blow-up is irreducible.

12.9 Proposition. *Suppose $f : X \to Y$ is surjective with Y projective, Y irreducible, and the fibers X_y are irreducible and of equal dimension. Then X is irreducible.*

12.10 Corollary. *The blow-up of $\mathbb{A}^n$ at the origin is irreducible.*

Proof. Indeed, recall that it is a line bundle over $\mathbb{P}^{n-1}$; the fibers are each isomorphic to $\mathbb{A}^1$, hence all irreducible of dimension 1. ▲

Lecture 13
9/27

§1 More fiber dimension results

Last time, we talked about fiber dimension. If $f : X \to Y$ is regular and surjective, between varieties of pure dimension $\dim X, \dim Y$, then we showed that

$$\dim f^{-1}(y) \geq \dim X - \dim Y$$

for all $y \in Y$. (We have also written $X_y = f^{-1}(y)$.) Moreover, we showed that there is an open set $U \subset Y$ such that for $y \in U$, we have in fact

$$\dim f^{-1}(y) = \dim X - \dim Y.$$

We can, actually, say more.

13.1 Corollary. *If $f : X \to Y$ is a regular morphism of projective varieties, then the sets $\left\{y \in Y : \dim f^{-1}(y) \geq k\right\}$ are closed.*

Note that we need the projectiveness because otherwise an open immersion $U \to X$ would have fibers with zero dimension on U, and dimension $-\infty$ on $X - U$.

It isn't obvious that the dimension can be given in terms of polynomial relations on the boundary.

Proof. This can be proved by induction on the dimension of Y.

The image $f(Y)$ is always closed. So the corollary is true for $d = 0$.

Now we prove it in general. Since $f(X)$ is closed, we can assume that $Y = f(X)$. The minimal possible dimension is $\dim X - \dim Y$; the corresponding set of $y \in Y$ is just all of Y. Let us prove the theorem for anything greater than $\dim X - \dim Y$. Say $d > \dim X - \dim Y$.

There is an open set U for which $\dim f^{-1}(y) = \dim X - \dim Y$. Let $Z = Y - U$. Clearly, the only points where $\dim f^{-1}(y) \geq d$ have to lie in Z. But by noetherian induction, we can assume that the theorem is true for the map $f^{-1}(Z) \to Z$. Namely, the set of $z \in Z$ where $\dim f^{-1}(z) \geq e$ is closed for any e. Now it is easy to see that the corollary holds. ▲

Now we finish up a loose end in the last lecture.

13.2 Theorem. *Let $f : X \to Y$ be a regular map between projective varieties such that*

1. *Y irreducible projective.*

2. *The fibers $X_y = f^{-1}(y), y \in Y$ are all irreducible of the same dimension.*

Then X is irreducible.

Proof. Suppose not. Let $X = X_1 \cup X_2 \cup \cdots \cup X_n$ be the decomposition of X into irreducible components. Now $Y = \bigcup f(X_i)$, so it follows by irreducibility that one of the $f(X_i)$ is dense in Y.

Without loss of generality, the $f(X_i)$ for $i \in [1, m]$ are dense in Y, while the $f(X_i)$ for $i > m$ are contained in proper closed subvarieties. This means that $f(X_i)$ for $i \in [1, m]$ contains a dense open set. Thus, there is an open set $U \subset Y$ such that $\dim(X_i)_y, y \in U, i \in [1, m]$ is constant, say d_i. We can also shrink U such that $(X_j)_y = \emptyset$ for $j > m$.

Wlog, d_1 is maximal.

Let $y \in U$. So X_y is the union of all the $(X_i)_y, 1 \leq i \leq m$. Its dimension is thus d_1. But $(X_1)_y$ and X_y thus have the same dimension. However, X_y is irreducible, so $(X_1)_y = X_y$.

We have shown that X is equal to one of its irreducible components, namely X_1, *over a big open set.* This still isn't enough, though. Now $f(X_1)$ is closed and contains U, so $f(X_1) = Y$. Consider the map $f|_{X_1} : X_1 \to Y$. Over the open set U, we know that the dimension is d_1. By the theorem, all the fibers have dimension at least d_1. I.e.,

$$\dim(X_1)_y \geq d_1$$

for all $y \in Y$. However, we know that $\dim X_y = d_1$ for all $y \in Y$ because the fiber dimensions of X are constant. In particular, we can pull the same trick to see that for all $y \in Y$,

$$\dim(X_1)_y = \dim X_y, \quad \text{so} \quad (X_1)_y = X_y.$$

In particular, $X = X_1$ and X is irreducible. ▲

Remark. Technically, this is not enough to imply that the blow-up of $\mathbb{A}^n$ is irreducible, since the blow-up isn't projective. But the blow-up is irreducible.

§2 Another characterization of dimension

13.3 Theorem. *The dimension of X is the maximal length of a strictly increasing chain*

$$X_0 \subset X_1 \subset \dots X_d \subset X$$

of closed irreducible subvarieties.

Recall that we defined dimension in terms of the transcendence degree, not as the combinatorial dimension given in the theorem.

Proof. Whenever you have such a proper inclusion, the dimension must increase. In particular, we have

$$\dim X_0 < \dim X_1 < \cdots < \dim X_d \leq \dim X$$

whenever $X_0 \subset \cdots \subset X_d \subset X$ is a strictly increasing chain of closed subsets. We have seen this earlier.

Assume without loss of generality that X is a projective variety.

Now we need to see that there is a chain of closed subsets of length $\dim X$. This would be easy to do if X were a projective space, because we could just take linear subspaces. However, we can find a finite map $X \to \mathbb{P}^{\dim X}$ which is surjective. Then we can consider the inverse images of an increasing chain of linear subspaces in $\mathbb{P}^{\dim X}$. These preimages form a chain

$$Y_0 \subset \cdots \subset Y_{\dim X}$$

of closed subsets corresponding to a chain $L_0 \subset \cdots \subset L_{\dim X} \subset \mathbb{P}^{\dim X}$, but we should check that these are irreducible. In fact, maybe it isn't. However, we can take an irreducible component $X_{\dim X}$ of $Y_{\dim X}$ that surjects onto $L_{\dim X}$, since $L_{\dim X}$ is irreducible and the image of a projective variety is closed.

Consider now $f^{-1}(L_{\dim X-1}) = Y_{\dim X-1}$. We can find an irreducible subset of $Y_{\dim X-1}$ contained in $Y_{\dim X}$ constructed above which surjects onto $\mathbb{P}^{d-1}$. This process can be repeated to get the chain of closed sets. ▲

When you think of an affine variety, the irreducible closed subsets correspond to prime ideals. So to find the dimension, you have to look at maximal chains of prime ideals.

§3 A dimension-counting result

We now prove:

13.4 Proposition. *If $X, Y \subset \mathbb{P}^n$ are closed and irreducible, and distinct, then any irreducible component of $X \cap Y$ has dimension at least $\dim X + \dim Y - n$.*

Shafarevich has a more geometric proof. We will not prove it, rather refer to a theorem in algebra.

Proof. Use a theorem of Krull in commutative algebra that says:

13.5 Theorem (Krull)**.** *If A is noetherian and $x \in A$ is neither a zerodivisor nor a unit, then (x) has height one. In particular, if $\dim A = d$, then every prime $\mathfrak{p}$ minimal over x is contained in a chain of primes*

$$\mathfrak{p} \subset \cdots \subset \mathfrak{p}_{d-1}$$

where $\mathfrak{p}_{d-1}$ is maximal.

We start by proving this for hypersurfaces.

Suppose first $X \subset \mathbb{A}^n$ has dimension d and f is some homogeneous polynomial. We known that $X \cap V(f)$ is the subvariety corresponding to the ideal $(f) \subset k[X]$. The irreducible components of $X \cap V(f)$ correspond to the primes of $k[X]$ minimal over (f). These, however, have height one. In particular, each of these components has a decreasing sequence of irreducible subvarieties of length $d-1$, hence has dimension $d-1$.

Since $\mathbb{P}^n$ is covered by affine spaces, this proves the theorem for Y a hypersurface. The general theorem *doesn't* seem to obviously follow by induction, because in general an irreducible variety isn't an intersection of the appropriate number of hypersurfaces based on the dimension.

▲

§4 Hilbert schemes

Algebraic geometry has the special feature that the collection of lots of algebro-geometric objects is itself an algebro-geometric object. By contrast, the set of all submanifolds of a manifold is not a manifold. The dimension is too big. In algebraic geometry, many times things are different. The collection of all varieties of a given type is often a variety itself.

For instance, consider hypersurfaces in $\mathbb{P}^n$. The hypersurfaces of a given degree d can be parametrized by a projective space, since each hypersurface corresponds to a homogeneous d-dimensional polynomial determined up to scalar multiplication. The coefficients correspond to something in some big projective space.

However, many of these hypersurfaces will be reduced or reducible. For instance, we should be careful, because in considering polynomials of degree d, we also include things like x_0^d. So, strictly speaking, you get a little more.

Lecture 14
[Section] 9/27

§1 Homework

We started by discussing the homework.

14.1 Exercise. Let $X \subset \mathbb{A}^n_{\mathbb{C}}$ be a variety defined by polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. Then the $\overline{\mathbb{Q}}$-points in X are dense in X in the $\mathbb{C}$-topology.

This is an interesting problem, and I think it can be solved by using the fact that any irreducible variety is birational to a hypersurface.

§2 Grassmannians

We talked a bit about the exercise on Grassmannians and asked the question:

What is the automorphism group of the Grassmannian variety $G(k, n)$?

A linear subspace in some $\mathbb{C}^n$ is given by k independent vectors.

If we have a transitive action of a reasonable group G on X, then $X = G/G_{\mathrm{st}}$, i.e. X is the quotient of G by its stabilizer at a point. Now $\mathrm{GL}_n(\mathbb{C})$ acts transitively on the set of linear subspaces of $\mathbb{C}^n$, so it acts transitively on $G(k, n)$. In fact, the unitary group alone can be thought of acting transitively on $G(k, n)$; it acts transitively on the set of orthonormal bases.

If we pick a k-plane P and its orthogonal complement, we know that $U(n)$ acts transitively on $G(k, n)$ (the orbit of P is all of $G(k, n)$), and the stabilizer is just $U(k) \times U(n-k)$. It follows that

$$G(n, k) = U(n)/U(k) \times U(n-k).$$

One can remember the orientation and get the Grassmannian of *oriented* k-planes as well.

Anyway, we know that there is an embedding

$$G(k,n) \rightarrowtail \mathbb{P}(\wedge^k \mathbb{C}^n)$$

and we know that the automorphism group $\mathrm{PGL}_N(\mathbb{C})$ (for $N = \dim \wedge^k \mathbb{C}^n$) acting on the projective space. Some of these preserve the Grassmannian. It turns out that these are the only automorphisms of $G(k,n)$ (i.e. all of them arise from automorphisms from the underlying projective space). It is quite difficult to prove this. Joe Harris claims it's not that deep.

§3 Example

Let ω be an element of the free group on two elements. We'd like a homomorphism of F_2 into a finite group that doesn't kill ω.

To do this, note that the matrices

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

generate a free group (a subgroup of $SL_2(\mathbb{Z})$. We can consider its reduction modulo N for N large to get the required homomorphism.

Lecture 15
9/29

§1 Dimensions of intersections

Recap from last time: We proved that if $X \subset \mathbb{P}^n$ is irreducible projective and f homogeneous, then every component of $X \cap V(f)$ has dimension at least

$$\dim X - 1 = \dim X + \dim V(f) - 1.$$

We proved this using the Krull dimension of rings.

We have some corollaries.

15.1 Corollary. *Suppose X is pure-dimensional projective and $f_1, \ldots, f_m$ are homogeneous, then each irreducible component of*

$$X \cap V(f_1, \ldots, f_m)$$

has dimension at least $\dim X - m$*.*

Proof. Induction on m. The $m = 1$ case has already been proved (by Krull's theorem). ▲

Remark. The above results are also true for affine varieties. In fact, we proved it first for affine varieties, where we had the direct correspondence between spaces and functions, and where we could directly apply Krull's principal ideal theorem.

15.2 Corollary. *If X, Y are projective and pure-dimensional, then each component of $X \cap Y$ has dimension at least*

$$\dim X + \dim Y - n.$$

Proof. The sketch we started to give last time was *incorrect*. The argument we tried to give was that if Y has codimension d, then Y is defined by d equations, so the above corollary applies. But this reasoning is not true. Even locally, a variety need not be a set-theoretic complete intersection (we'll explain this someday). But fortunately, we noticed that last time before the end of class.

15.3 Example. Consider the union of two 2-dimensional planes (e.g. $V(xy) \cup V(zw) \subset \mathbb{A}^4$). This is a dimension two subvariety which cannot be cut out by two equations in any neighborhood of zero. Proof omitted.

Admittedly this is a reducible example.

Anyway, let $\Delta \subset \mathbb{P}^n \times \mathbb{P}^n$ be the diagonal $\{(x, x), x \in \mathbb{P}^n\}$. This is defined as the zero locus of the n linear equations

$$x_1 = y_1, \; x_2 = y_2, \ldots, \; x_n = y_n.$$

By the earlier corollary, every irreducible component of

$$\Delta \cap X \times Y$$

has dimension $\geq \dim X + \dim Y - n$. This, however, is isomorphic to $X \cap Y$. That completes the proof.

▲

§2 Geometric applications

We now give a geometric application of this, which will also be a good example of how, in some cases, even if you're interested in *one* object (a curve, surface, etc.), it is useful to look at the collection of *all* such objects.

Question: When will a surface in $\mathbb{P}^3$ (i.e. a hypersurface) contain lines?

Consider the collection of all surfaces of some fixed degree d in $\mathbb{P}^3$. These correspond to the *points* of $\mathbb{P}(V)$ for V the vector space of all degree d homogeneous polynomials in x, y, z, w.

$$\{\text{surfaces degree } d\} \to \mathbb{P}(V).$$

Note that this is not strictly true—it's more moral philosophy than mathematics—in that degenerate cases may occur where the polynomial is reducible. For instance, you might get something like $x^3 = 0$, which is really a degree one hyperplane.

As we said, this correspondence should really be put in quotes, because you get more than just the surfaces of degree d. However, $\mathbb{P}(V) = \mathbb{P}^N$ (for $N = \binom{d+3}{3} - 1$) is nicer. How much bigger is $\mathbb{P}^N$ than our variety, though? We can make this moral philosophy more precise.

15.4 Lemma. $\mathbb{P}^N$ *contains an open dense set of genuinely degree d hypersurfaces (i.e. corresponding to irreducible homogeneous polynomials).*

Really, it is this open set that corresponds to the degree d surfaces.

Proof. For each $i < d$, the set of polynomials that factor as a product of something of degree i and something of degree $d - i$ is the image of a product of two smaller projective spaces, namely $\mathbb{P}(\deg i) \times \mathbb{P}(\deg d - i) \to \mathbb{P}^N$. This is thus a closed subset, and since it is not the full space, its complement is an open dense set. Taking the intersection of these open dense subsets for each i, we get the open dense set. ▲

Now, we ask a question. Given a line $\ell \subset \mathbb{P}^3$, what are the surfaces that contain ℓ? In other words, I have a line and a degree d polynomial P: what are the conditions for P to vanish on this line ℓ?

If you pick $d+1$ points on this line ℓ, a degree d polynomial vanishes on ℓ iff it vanishes on the $d+1$ points. Indeed, the restriction to ℓ is a polynomial in one variable of degree d. Let us pick $d+1$ points fixed on ℓ. Then we get $d+1$ linear conditions on the polynomial for it to vanish on ℓ.

What you get is that, fixing ℓ, the space of polynomials (of degree d) vanishing on ℓ is just a linear subspace $\mathbb{P}^{N-d-1}$, since there are $d+1$ linear conditions.

Next, we note that: The collection of all lines in $\mathbb{P}^3$ is the Grassmannian $G(2,4)$ of 2-planes in four-space. This was in the homework. Consider the following geometric object:

$$Z = \{\ell, [P]\}$$

where $\ell \subset \mathbb{P}^3$ (i.e. $\ell \in G(2,4)$) and P is a polynomial ($P \in \mathbb{P}^N$) that vanishes on ℓ. Then Z is an algebraic variety. In fact:

15.5 Exercise. The condition that something belong to P is a *closed* condition. So Z is a variety.

Let us go deeper inside the structure of Z. Consider the projection

$$Z \to G(2,4)$$

and consider the fibers. The fibers are obtained by picking a line ℓ and looking at the forms P that vanish on his line. We showed above that this is just $\mathbb{P}^{N-d-1}$. We see that $Z \to G(2,4)$ is onto and the fibers are all irreducible of dimension $N - d - 1$ (indeed, projective spaces of this dimension).

Next, we need:

15.6 Proposition. $G(2,4) \subset \mathbb{P}^5$ *is irreducible of dimension four.*

Proof. This is in the homework. ▲

It follows from this fiber dimension business that

15.7 Proposition. Z *is irreducible of dimension* $N - d - 1 + 4$.

Now, let's project this onto the second coordinate. The question now becomes:

Given a surface defined by P, what are the lines containing it?

We are projecting something of dimension $N - d + 3$ onto something of dimension N (namely, $\mathbb{P}^N$). Thus:

15.8 Corollary. *If $d > 3$, the generic surface of degree d contains no lines.*

Proof. Indeed, the projection $Z \to \mathbb{P}^N$ cannot be surjective, so the image is contained in a closed subvariety of smaller dimension (since Z is projective). ▲

The question remains for smaller d.

§3 Degree three

In one of the homework, we gave an example of a cubic surface that contained many (twenty-seven) lines. It turns out that you can answer this question. We have a map

$$Z \to \mathbb{P}^N$$

but both have the same dimension. Is this map onto? Does every cubic surface contain a line? The answer is not obviously not, since both objects have the same dimension.

Well, the image is closed, while the codomain is irreducible. So if the image is not everything, the image must have smaller dimension, and all the fibers will have positive dimension (by the fiber dimension theorem).

Consequently, if we can show that there is a single cubic surface with finitely many lines (but at least one), it will follow that $Z \to \mathbb{P}^N$ cannot have all fibers of dimension 1, and $Z \to \mathbb{P}^N$ is onto. It will follow that *all* cubic surfaces have lines on them.

It turns out that there are such.

15.9 Example. Here is an affine cubic surface not containing any line. Consider $xyz = 1$ inside $\mathbb{A}^3$. It contains no line; just write the equation. Its projectivization in $\mathbb{P}^3$ is the vanishing locus of $xyz - w^3$. I claim that it contains only finitely many lines.

Indeed, it can contain only lines that lie in the complement of $\mathbb{A}^3$ in $\mathbb{P}^3$. This complement has dimension two, and we have intersected it with something of dimension two (this surface $xyz = w^3$), so the intersection of the surface with $\mathbb{P}^3 - \mathbb{A}^3$ (which has dimension one) has finitely many lines. Nonetheless, there are lines contained in the surface, for instance

$$x = w = 0.$$

We have proved:

15.10 Theorem. *Every cubic surface in $\mathbb{P}^3$ contains a line.*

As it happens, the "general" cubic contains twenty-seven lines. The cubic we constructed in the example was not generic.

§4 Differential geometry

It's a well-known secret that algebraic geometry contains infinitesimals that analysis doesn't. In algebraic geometry, you have elements so small that their *squares* are equal to zero.

Consider the ring

$$D = k[\epsilon]/(\epsilon^2),$$

which is called the **ring of dual numbers**. Then $\epsilon^2 = 0$ in D. Then ϵ functions as a derivative.

If $U \subset \mathbb{A}^n$ is open, and $p \in U$, we can define the **partial derivative** of a regular function $f \in k[U]$. Namely, we want to write

$$\frac{\partial f}{\partial x_i}(p) = \frac{f(p + \epsilon e_i) - f(p)}{\epsilon}$$

where e_i is a unit vector $(0, \dots, 1, \dots, 0)$. We are not sure how to write this, though—can we divide by ϵ?

However, the difference

$$f(p + \epsilon e_i) - f(p) \in D$$

lies in the kernel of the map $D \to k$ because this map kills ϵ. This kernel, however, just $k\epsilon \subset D$, which is isomorphic to k. So in this sense we can "divide" by ϵ. And the definition is well-defined. More generally, we can do directional derivatives.

Remark. You just get the usual (formal) derivative of polynomials and rational functions. For instance, x^n still differentiates to nx^{n-1}, and so on.

Let us set some notation.

15.11 Definition. An element $\alpha + \epsilon\beta \in D = k[\epsilon]/(\epsilon^2)$ is **infinitesimally close** to $\alpha \in k$. α is well-defined. We can define what it means for a tuple of elements in D to be **infinitesimally close** to a tuple in k.

Now that we know how to differentiate functions, let us do differential geometry.

15.12 Definition. Let X be an affine variety and $p \in X$. The **tangent space** to X at p, or $T_p(X)$, is the set of all solutions to the equation defining X in the ring $k[\epsilon]/(\epsilon^2)$ that are infinitesimally close to p.

In other words, this is the set of all vectors v such that

$$f(p + \epsilon v) = 0 \in D \quad \forall f \in I(X).$$

15.13 Proposition. *$T_p(X)$ is always a vector space. In fact, it is equal to the set of all $\{p + \epsilon v\}$ such that, for all $f \in I(X)$.*

$$\nabla f \cdot v = 0$$

for ∇f the "gradient" of f. In other words, the "directional derivative" of functions in $I(X)$ along v have to vanish.

Equivalently,

$$\sum v_i \frac{\partial f}{\partial x_i} = 0 \quad \forall f \in I(X).$$

It is enough to look at f in the generating set.

Proof. If $v \in T_p(X)$, and $f(p+\epsilon v) = 0$, then from $f(p) = 0$ it follows that the derivative of f in direction v must be zero. We have used the definition of the derivative as a "difference quotient."

Conversely, we need to show that if $\nabla f \cdot v = 0$, then $f(p + \epsilon v) = 0$ as well. This is also trivial from expanding $f(p+\epsilon v)$ via a Taylor expansion, since all the higher terms vanish. Indeed,

$$f(p + \epsilon v) - f(p) = \epsilon \nabla f \cdot v.$$

▲

Lecture 16
10/1

§1 Tangent spaces

Again, let us remind ourselves of the notation. We have $p \in X \subset \mathbb{A}^n$, where X is an affine variety defined by polynomials. We recall that we defined the **tangent space** T_pX to be the set of all $p + \epsilon v$ such that

$$f(p + \epsilon v) = 0 \in D = k[\epsilon]/(\epsilon^2), \forall f \in I(X).$$

This is equivalently the set of all v, by the Taylor expansion, where

$$D_v f(p) = \nabla f(p) \cdot v = 0, \quad \forall f \in I(X).$$

It is enough to check this for a generating set of the ideal $I(X)$.

The tangent space can be identified with a subset of $\mathbb{A}^n$.

This usually conforms to the standard notion of tangent space. For instance, $T_p\mathbb{A}^n$ is just k^n, since there are no equations.

16.1 Example. Consider the variety $X = V(xy) \subset \mathbb{A}^2$, the union of the x and y axes. Let us compute T_0X. By definition, this is the set of all points $\epsilon v = (\epsilon v_1, \epsilon v_2)$ such that

$$x(\epsilon v)y(\epsilon v) = \epsilon v_1 \epsilon v_2 = 0 \in D$$

which is a vacuous condition, so that the tangent space is just all of k^2. $T_0X = k^2$.

The example shows that it is **not** true that any tangent vector is the infinitesimal direction of a curve contained in the variety.

There are some issues with this definition. Consider any affine variety X; we can embed it in affine space. Then the question is whether the tangent space will depend on the embedding. Next, we want to define the tangent space for projective varieties. So we want to show that tangent spaces are local, because any variety is locally affine.

§2 The local ring

For this, it would be nice to have some "smallest" open set containing a point on which we could do differential calculus. But this doesn't make sense. The intersection of all open sets containing a point is just the point. Nonetheless, we can dualize this idea, and form the limit of the sets of *regular* functions over neighborhoods of a point.

16.2 Definition. Let X be any variety. The **local ring** of X at $x \in X$ is the ring of equivalence classes of pairs (U, f), where U is an open neighborhood of x and $f \in k[U]$ is regular. The equivalence relation is that $(U, f) \sim (V, g)$ if f and g agree on a smaller neighborhood of x.

The local ring is denoted $k[X]_x$.

This is very similar to the definition of rational functions on a variety. There, we looked at all open sets, but here we are only looking at open sets containing x.

If you like commutative algebra, then note that if X is affine, $k[X]_x$ is just the localization of $k[X]$ at the maximal ideal corresponding to x. Elements of $k[X]_x$ are called **germs** of regular functions at x.

There is a different between $k[X]_x$ and other rings we have studied up till now.

Remark. $k[X]_x$ is generally not finitely generated.

16.3 Example. $k[\mathbb{A}^1]_0$ is the set of all rational functions $f/g \in k(X)$ with $g(0) \neq 0$. This is not a finitely generated ring over k. Every element $X - \alpha, \alpha \neq 0$ can occur in the denominator.

We don't know how to assign a geometric object to things which are not finitely generated. But there is a way. This is why one introduces schemes into the picture.

Remark. Clearly, $k[X]_x = k[U]_x$ for any open U containing x. Note also that this is really an invariant of X, and not any embedding of X (or a neighborhood thereof) into a ring of functions.

16.4 Definition. $k[X]_x$ has a unique maximal ideal, namely the ideal of germs functions vanishing at x. We denote this by $\mathfrak{m}_x$. Any element not in this ideal can be inverted (it doesn't vanish at x), so is invertible. The residue field $k[X]_x/\mathfrak{m}_x$ is just k under evaluation at x.

In commutative algebra, this would be called a **local ring**.

§3 The local characterization of T_pX

16.5 Theorem. *Let $X \subset \mathbb{A}^n$. T_pX is isomorphic to the dual of the vector space $\mathfrak{m}_p/\mathfrak{m}_p^2$, where $\mathfrak{m}_p \subset k[X]_p$ is as above.*

In particular, we can define the **tangent space** of *any* variety now.

16.6 Definition. The **tangent space** at p of a variety X is the space

$$T_pX = (\mathfrak{m}_p/\mathfrak{m}_p^2)^\vee.$$

Clearly this is a local invariant.

Proof. To do this, we need only give a nondegenerate pairing

$$T_pX \times \mathfrak{m}_p/\mathfrak{m}_p^2 \to k.$$

So choose $f \in \mathfrak{m}_p$ and $v \in T_pX$ (i.e. $p + \epsilon v$ is a root of the polynomials of $I(X)$). We define the pairing

$$(f, v) = D_v f(p) = \nabla f(p) \cdot v.$$

If $f, g \in \mathfrak{m}_p$, then

$$(fg, v) = D_v(fg) = D_v f(p) g(p) + f(p) D_v g(p) = 0.$$

So it is indeed a pairing of $T_pX \times \mathfrak{m}_p/\mathfrak{m}_p^2$ into k. (Note that the pairing kills elements of $I(X)$.)

We now show the pairing is nondegenerate.

Let $v \in T_pX - \{0\} \subset \mathbb{A}^n$. Wlog, $p = 0$. Then there is a linear function f such that $D_v f \neq 0$. However, $f(0) = 0$, and f restricts to an element of $k[X]$, hence one of $\mathfrak{m}_p$. The pairing

$$(f, v) \neq 0$$

so the kernel on one side is trivial. Now, we need to show that for a nonzero function, there is a vector which pairs nontrivially.

Let $f \in \mathfrak{m}_p$. If $f \notin \mathfrak{m}_p^2$, we need to construct a vector $v \in T_pX$ such that $D_v f \neq 0$. Now f is a restriction of a rational function g/h on $\mathbb{A}^n$.

We will show that there is a vector v such that $D_v g(p) \neq 0$; this will be sufficient to show that there is a vector in which direction f has nonzero derivative by elementary calculus. In other words, we have reduced to the case of polynomials. Write $g = g_0 + g_1 + \dots$ where each g_i is homogeneous of degree i. Now $g_0 \equiv 0$ since $g(0) = 0$ as $g \in \mathfrak{m}_p$. Also, $g_2, g_3, \dots \in \mathfrak{m}_p^2$. So if $g \notin \mathfrak{m}_p^2$, then $g_1 \notin \mathfrak{m}_p^2$. We can assume that g is linear, i.e. $g = g_1$.

The tangent space at X was exactly all vectors v such that their pairing with q is zero for every $q \in I(X)$. Assume that g_1 pairs to zero with everything in T_pX, i.e. $g_1 \in (T_pX)^\perp$. Then this implies that g_1 is actually in the ideal $I(X) + \mathfrak{m}_p^2$ because the double dual is the same vector space when one works with finite-dimensional vector spaces. It follows that $g \in \mathfrak{m}_x^2$. ▲

Remark. I'm not sure I really got this proof; I will try and edit it later.

We are following Shafarevich, more or less.

This theorem looks a bit complicated, but it shouldn't. We are identifying a vector space with a dual of a vector space. Why don't we just identify T_pX and $\mathfrak{m}_p/\mathfrak{m}_p^2$, because they are isomorphic? The problem is that if we identify these two, we lose the *naturality*. The naturality of the above argument lets you carry out arguments in families.

16.7 Example. Let's work over $\mathbb{C}$ and consider the Riemann sphere $\mathbb{P}^1$. Topologically, it is a 2-sphere. The algebraic tangent space at each point is just $\mathbb{C}$. We can think about the differentiable tangent space at each point, which is the same, as forming a bundle. Nonetheless, it is *not* true that $T\mathbb{P}^1 \simeq \mathbb{C} \times \mathbb{P}^1$. The isomorphism $T_p\mathbb{P}^1 \to \mathbb{C}$

cannot be picked in a way coherent in p. The topological reason is that one cannot choose a nonzero tangent vector to the sphere S^2 at each point (the Euler characteristic is not zero).

§4 The derivative map

Consider $f : X \to Y$. Let $p \in X$. We can define

$$Df : T_pX \to T_{f(p)}Y$$

either using coordinates or in the following coordinate-free way. There is a map

$$k[Y]_y \to k[X]_x$$

and a map

$$\mathfrak{m}_y \to \mathfrak{m}_x$$

so the map

$$\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$$

leads by duality to the map on tangent spaces.

Assume X, Y are contained in affine spaces. In coordinates, this is the following: suppose $p + \epsilon v$ satisfies the polynomial equations of $I(X)$ (in D). Then $f(p + \epsilon v)$ satisfies the polynomial equations of Y. For, suppose $g \in I(Y)$. Then $g \circ f : X \to \mathbb{A}^1$ is equal to zero. It follows that $g \circ f$ is the zero element of $k[X]$ and consequently kills $p + \epsilon v$. This is the map $T_pX \to T_{f(p)}Y$. From the expression $p + \epsilon v \to f(p + \epsilon v)$, we can write the map in terms of a Jacobian matrix.

Of course, the derivative of the identity is the identity, and the derivative of a composite is the composite of the derivatives.

16.8 Corollary. *$V(xyz) \subset \mathbb{A}^3$ is not isomorphic to any variety in $\mathbb{A}^2$.*

Proof. Indeed, the tangent space at zero has dimension three. However, the tangent space of anything in $\mathbb{A}^2$ can have dimension at most two. ▲

Singularities can be obstructions to embedding affine varieties in smaller-dimensional affine spaces, as the above result shows.

16.9 Corollary. *There is a curve in $\mathbb{A}^n$ that cannot be embedded in $\mathbb{A}^{n-1}$.*

Proof. We find a curve whose tangent space is n-dimensional. For instance,

$$\left\{(t^{2n}, t^{2n+1}, \dots, t^{3n})\right\} \subset \mathbb{A}^n.$$

▲

16.10 Example. Let's compute the tangent space $T_p\mathbb{P}^n$. Since $\mathbb{P}^n$ is locally isomorphic to $\mathbb{A}^n$, this is just k^n. However, I don't believe the isomorphism is *canonical.*

Let $V = k^{n+1}$. We have a map $\pi : V - \{0\} \to \mathbb{P}^n$.

Koan for the weekend: The tangent space at $\mathbb{P}^n$ is naturally isomorphic to the quotient $V/\pi^{-1}(p)$.

Lecture 17
10/4

§1 A counterexample

17.1 Example (Dangerous bend)**.** The following is false. Let $f : X \to Y$ be a finite map of degree d. Then it is *not* true that

$$|X_y| \leq d$$

for all $y \in Y$. It *is* true if Y is some projective space or a *nonsingular* (or at least *normal*) variety. In general, though, it is false.

For instance, the normalization of a *nodal* cubic curve, e.g.

$$y^2 = x^3 + x^2$$

whose normalization is $\mathbb{A}^1$, traced out by

$$t \to (t^2 - 1, t(t^2 - 1)).$$

This is such that the generic fiber has size one, but not every fiber is of size one. The fiber over 0 contains two points. There are two "branches" of the nodal cubic curve at zero; the variety minus the origin is disconnected.

§2 Back to the tangent space

We go back to the tangent space to $\mathbb{P}^n$. Fix $\ell \in \mathbb{P}^n$. If V is a vector space of dimension $n+1$, we want to identify $T_\ell \mathbb{P}(V)$ (where $\mathbb{P}(V) = \mathbb{P}^n$) with V/ℓ (where ℓ is thought of as a line). Fix $p \in \ell - \{0\}$. Since there is a map $V - \{0\} \to \mathbb{P}(V)$, we get a map $T_p(V) \to T_\ell(\mathbb{P}(V))$. The kernel is just ℓ, though.

Let's see this obvious fact in coordinates. So choose a coordinate x_i which is not zero. Then we have the map

$$\pi : V - \{x_i = 0\} \to \mathbb{P}_i(V).$$

The map is given by

$$\pi : [x_0 \dots x_n] \to (x_0/x_i, \dots, \widehat{x_i/x_i}, \dots x_n/x_i).$$

What is the derivative at p? What is $d\pi_p(V)$?

In fact, $d\pi_p$ is the matrix

$$\begin{bmatrix} \frac{1}{p_i} & & & \\ & \frac{1}{p_i} & & \\ \vdots & & & \\ -p_0/p_i^2 & -p_1/p_i^2 & \dots & \\ \vdots & & & \\ & & & \frac{1}{p_i}. \end{bmatrix}$$

So the map $d\pi_p$ sends $(v_0, \dots, v_n)$ into $(v_0/p_i - \frac{p_0 v_i}{p_i^2}, \dots)$. It follows that the kernel is the set of vectors $(v_0, \dots, v_n)$ such that for all j,

$$v_j p_i = p_j v_i,$$

which is precisely the line ℓ corresponding to p.

§3 A new theorem

17.2 Theorem. *Let X be irreducible. Then $\dim T_x(X) \geq \dim X$, but equality holds on an open dense set.*

Proof. It is enough to prove this for affine varieties: any irreducible variety has a dense open affine subset, and is covered by such. Note that the tangent space is a local invariant, as is the dimension (which is the transcendence degree of the function field).

Let us first prove this for a hypersurface. Then in this case $X = V(f)$, f irreducible in n variables. (So $X \subset \mathbb{A}^n$.) We have $\dim X = n - 1$. Also, $T_x(X)$ is the set of all vectors $v \in k^n$ such that

$$\{v : \nabla g(x) \cdot v = 0, \forall g \in I(X)\}$$

which is equivalently

$$\{v : \nabla f(x) \cdot v = 0\}$$

since f generates the ideal. So it is clear that $\dim T_x(X)$ is at least $n-1$ or n. In particular, it is at least $\dim X$.

Suppose it is not $\dim X$, i.e. $T_x(X)$ is the full space k^n. This is equivalent to the condition that the functional ∇f on k^n be equal to zero, which is a closed condition. In other words, this is a closed set. So it is either a proper closed set of everything. If it is not a proper closed set, then

$$\nabla f = 0$$

on the whole variety $X = V(f)$. This means that $\frac{\partial f}{\partial x_i} \in (f) \subset k[x_1, \dots, x_n]$ by the Nullstellensatz and the fact that f is prime. But these derivatives have smaller degree than f. So the partials must all be zero. In characteristic zero, this implies that f is constant. In characteristic p, we have a little more to do.

In char$k = p$, it may happen that $\frac{\partial f}{\partial x_i} \equiv 0$ (e.g. x_i^p). This implies, however, that only powers of x_i that occur in f are all multiples of p, for each i. In particular, f is a polynomial in $x_1^p, \dots, x_n^p$. I.e.

$$f(x_1, \dots, x_n) = g(x_1^p, \dots, x_n^p) = \sum_I g_I x_1^{pI_1} \dots x_n^{pI_n}.$$

But each $g_I \in k$ has a pth root in k. In particular, if we take

$$\sum_I \sqrt[p]{g_I} x_1^{I_1} \dots x_n^{I_n}$$

becomes f when raised to the power p, since the binomial coefficients are divisible by p. This is a contradiction if f was irreducible.

This proves the result for hypersurfaces. In general, we use:

17.3 Proposition. *Every irreducible variety is birational to a hypersurface.*

Assume the proposition. Then we have an arbitrary variety X, which has an open dense subset U isomorphic to an open dense subset of a hypersurface; this preserves things like dimension. We find from the version of the theorem for hypersurfaces that there is an open dense set of X (contained in U, say) for which

$$\dim T_x(X) = \dim X.$$

We still have to show inequality *everywhere*. Assume $X \subset \mathbb{A}^n$. Now consider the tangent bundle τ to X. By this, I mean

$$\tau = \{(x, v) : x \in X, v \in T_x(X)\} \subset \mathbb{A}^n \times \mathbb{A}^n.$$

The condition $v \in T_x(X)$ is equivalent to an algebraic condition of v satisfying a bunch of linear equations that depend polynomially on x. Namely, the condition is that $\nabla f(x) \cdot v = 0$ for all $f \in I(X)$ (even in some finite subset thereof). We have a map $\tau \to X$. There is a dense open set where the fiber dimensions are constant, i.e. $\dim \tau_x \equiv d$ for $d = \dim \tau - \dim X$. This dense open set must intersect the dense open set where $\dim T_x(X) = \dim X$. So the generic fiber $\dim \tau_x$ has dimension $\dim X$. We know by the fiber dimension theorem that all fibers have dimension *at least* the generic fiber. So all the fibers τ_x have at least dimension $\dim X$. But the fibers are the tangent spaces, so we are done. ▲

Proof of the proposition. This is a result in field theory. Equivalently, it states that any finitely generated field over an alg. closed field is the field of a hypersurface. (Recall that two varieties are birational iff the rational function fields are k-isomorphic.) In other words, if K/k is finitely generated, then

$$K = k(t_1, \dots, t_d, u)$$

for $\{t_1, \dots, t_d\}$ algebraically independent, and u algebraic over $k(t_1, \dots, t_d)$. (Then the corresponding hypersurface is the subset of $\mathbb{A}^{d+1}$ defined by the minimal polynomial of u.)

Let $s_1, \dots, s_m \in K$ be generators of K/k. Let $n = \text{tr.deg. } K/k$. Without loss of generality, assume $s_1, \dots, s_n$ are algebraically independent. If the algebraic extension $K/k(s_1, \dots, s_n)$ is separable, we can find one additional algebraic element generating K by the primitive element theorem in elementary field theory.[13] So we're done.

In general, this doesn't work. Consider $k(s_1, \dots, s_{n+1})/k(s_1, \dots, s_n)$. This is algebraic so it satisfies a polynomial over the field $k(s_1, \dots, s_n)$. Therefore, if one clears denominators, there is a multivariable polynomial

$$f(x_1, \dots, x_{n+1}) \in k[x_1, \dots, x_{n+1}]$$

with

$$f(s_1, \dots, s_{n+1}) = 0.$$

We can choose f irreducible. The whole point is to show that even if s_{n+1} is not separable over $s_1, \dots, s_n$, then we can switch two of them to get something better.

Two cases:

[13] A finite separable algebraic extension is generated by one element.

1. There is $i \in [1, n+1]$ such that $\frac{\partial F}{\partial x_i} \neq 0$.
2. There is no such i.

In case 1), it follows that $k(s_1, \dots, s_{n+1})/k(s_1, \dots, \hat{s}_i, \dots, s_{n+1})$ is separable (the latter hat means omit). In case 2), f is a polynomial in powers of x_j^p, so f is reducible, contradiction. Only case 1) matters thus.

The conclusion is that $k(s_1, \dots, s_{n+1})/k(s_1, \dots, \hat{s}_i, \dots, s_{n+1})$ is separable. You can continue by induction on the number of generators. You get that K is separable over $k(s_{i_1}, \dots, s_{i_n})$ for some indices $i_1, \dots, i_n$. Then it follows that K is generated by a transcendence basis and one algebraic element by the primitive element theorem. This proves the proposition. ▲

So we have our theorem. The tangent space has dimension at least that of the variety. But sometimes it can be more.

17.4 Definition. The variety X is **smooth** (or **nonsingular**) at x if $\dim T_x X = \dim X$ for all $x \in X$. X is just called **smooth** (or **nonsingular**) if it is smooth at all points.

Any irreducible variety has a dense open subset on which it is smooth.

17.5 Example. The Grassmannian $\mathrm{Gr}(k, n)$ is smooth. This is because every point has a neighborhood which is actually an affine space (as was in the homework), and affine space is smooth.

As an example of an irreducible non-smooth curve, take $y^2 = (x+1)x^2$. Then there is a "node" at the origin, so it is not smooth. Try graphing it.

Lecture 18
[Section] 10/4

§1 Some remarks

18.1 Example. Two curves in $\mathbb{P}^2$ intersect.

This is a theorem we never mentioned in class.

Proof. Let $X \subset \mathbb{P}^N$ be a projective variety and F a polynomial. Then F defines a hypersurface H_F. Then either

$$H_F \supset X$$

or

$$\dim H_F \cap X = \dim X - 1.$$

This is a theorem in Shafarevich.

In particular, X contains subvarieties of all codimensions. A surface contains a curve, a three-fold contains a surface, etc., etc. Moreover, in $\mathbb{P}^n$, any $r \leq n$ irreducible homogeneous polynomials have a common root.

So any two curves in $\mathbb{P}^2$ intersect. ▲

If X_1, X_2 are curves, then the set $X_1 \cap X_2$ is finite if X_1, X_2 are irreducible and distinct. Then for "general" curves X_1, X_2 of degrees d_1, d_2, we have

$$|X_1 \cap X_2| = d_1 d_2.$$

This is the Bezout theorem.

§2 Transversality

Let M be a compact n-manifold. Suppose $X, Y \subset M$ are closed (embedded) submanifolds of dimension i, j. Then $Z = X \cap Y$ is a closed subset of M. When is Z a submanifold? What is its dimension?[14]

We have the tangent bundles TX, TY, TM of these various manifolds. Let $z \in Z = X \cap Y$. Then we have tangent spaces:

$$T_z(X), T_z(Y), T_z(M).$$

If

$$T_z(X) + T_z(Y) = T_z(M),$$

then we say that the intersection $X \cap Y$ is **transversal** at z. If the intersection is everywhere transversal, then the intersection is always a submanifold of dimension

$$i + j - n.$$

If $i + j < n$, then transversality can *never* occur.

18.2 Example (Nontransversality)**.** $\mathrm{GL}_n(\mathbb{R})$ is a manifold; $\mathrm{SL}_n(\mathbb{R})$ is a submanifold, as is $\mathrm{O}_n(\mathbb{R})$. These are all Lie groups. They all have tangent spaces at the identity. In fact:

$$T_I(\mathrm{GL}_n(\mathbb{R})) = M_n(\mathbb{R}).$$

$$T_I(\mathrm{SL}_n(\mathbb{R})) = T_n(\mathbb{R}) \equiv \{\text{trace free matrices}\}$$

$$T_I(\mathrm{O}_n(\mathbb{R})) = \mathfrak{o}_n(\mathbb{R}) \equiv \left\{A \in M_n(\mathbb{R}) : A + A^T = 0.\right\}$$

An exercise is to show that $\mathrm{SL}_n(\mathbb{R})$ and $\mathrm{O}_n(\mathbb{R})$ don't intersect transversally. The reason is that $T_I(\mathrm{O}_n) \subset T_I(\mathrm{SL}_n)$. Their sum therefore can't $M_n(\mathbb{R})$.

Now O_n is a deformation retract of GL_n (the Gram-Schmidt process).

Intersections can be *weird*.

18.3 Exercise. Let $X \subset \mathbb{R}^2$ be a closed set. There exists an embedding $\mathbb{R} \xrightarrow{f} \mathbb{R}^3$ such that $\overline{f(\mathbb{R}) \cap \mathbb{R}^2 \times \{0\}} = X$.

Proof. Choose a countable subset $\{a_0, a_1, a_2, \dots\} \subset X$ dense. We could take f to be a curve in $\mathbb{R}^3$ with $f(0) = a_0$, $f(1) = a_1, \dots$, but such that f doesn't intersect the plane $\mathbb{R}^2 \times \{0\}$ except at the nonnegative integers. ▲

[14] Ubuntu.

§3 The homework

In the homework, we were asked to show that if $f : X \to Y$ is finite of degree d, then there is an open dense subset $V \subset Y$ such that $y \in V$ implies

$$|X_y| = |f^{-1}(y)| = d.$$

We'll talk about some related business.

Recall that if $f : X \to Y$ is a regular map of irreducible varieties with $\dim X = n, \dim Y = r$, then there is an open dense subset of y with $\dim X_y = n - r$. This was the fiber dimension theorem. One can say more, though:

18.4 Theorem. *For projective varieties, the sets $Y_k = \{y \in Y : \dim X_y \geq k\}$ are closed in Y. So the fiber dimension is semicontinuous.*

Actually, we did prove this in class. I forgot about it.

We also proved in class:

18.5 Theorem. *X, Y projective. Let $f : X \to Y$ be a morphism with Y irreducible and X_y irreducible of constant dimension for $y \in Y$. Then X is irreducible.*

So this was a review of results in class.

Lecture 19
10/6

Last time, we showed that if X is a variety and $x \in X$, then

$$T_x(X) = (\mathfrak{m}_x/\mathfrak{m}_x^2)^*.$$

So a tangent vector is a functional on the set of functions vanishing at x, but which is trivial on the functions which vanish to order two. This is close to the modern definition of the tangent space in terms of derivations.

§1 Taylor expansion

We want to talk about the local behavior around a smooth point of a variety X.

19.1 Definition. Let $x \in X$ be a smooth point.[15] A **local coordinate system** or **local parameter system** an n-tuple of functions $u_1, \ldots, u_n \in \mathfrak{m}_x$ such that the images in the linear subspace $\mathfrak{m}_x/\mathfrak{m}_x^2$ is a basis. This implies that $n = \dim X$, of course.

19.2 Proposition. *If $u_1, \ldots, u_n$ are local coordinates at x, then $u_1, \ldots, u_x$ generate $\mathfrak{m}_x$ in the local ring $k[X]_x$.*

[15] I.e., $\dim T_x(X) = \dim X$.

Proof. This follows by Nakayama's lemma. Nakayama's lemma states that a sequence of elements generates a finitely generated module M over a local ring $(R, \mathfrak{m})$ if they generate $M/\mathfrak{m}M$ over $R/\mathfrak{m}$.

So apply Nakayama to the module $\mathfrak{m}_x$ over $k[X]_x$. (Recall that $k[X]_x$ is local with maximal ideal $\mathfrak{m}_x$, since every element which doesn't vanish at x is invertible.) Then the result follows. ▲

19.3 Proposition. *Suppose $u_1, \dots, u_n$ are local coordinates, then for every $k \in \mathbb{Z}_{>0}$, the monomials of degree r are a basis for $\mathfrak{m}_x^r/\mathfrak{m}_x^{r+1}$.*

Proof.

1. Spanning. This follows because the monomials in the u_i generate $\mathfrak{m}_x^r$ by the above result.

2. Independence. Note that if $u_1, \dots, u_n$ are local coordinates and $\{a_{ij}\}$ an invertible matrix over k, then

$$\left\{ \sum_j a_{ij} u_j \right\}$$

is a family of local coordinates as well. So suppose F is a degree r homogeneous polynomial in n variables. Suppose

$$F(u_1, \dots, u_n) \in \mathfrak{m}_x^{r+1};$$

we show $F = 0$, which will prove the claim. Suppose $F \neq 0$. After applying a linear transformation, we may assume that the monomial x_1^r appears in the polynomial. Then we have

$$F(x_1, \dots, x_n) = x_1^r + \text{terms of lower order in } x_1.$$

But any element of $\mathfrak{m}_x^{r+1}$ is a homogeneous polynomial of degree r with coefficients in the maximal ideal $\mathfrak{m}_x$. Anyway, from $F(u_1, \dots, u_n) \in \mathfrak{m}_x^{r+1}$ we find that

$$u_1^r = \mu u_1^r \mod (u_2, \dots, u_n)$$

for $\mu \in \mathfrak{m}_x$, because the other coefficients of $x_1^i, i < r$ involve things in $(u_2, \dots, u_n)$. We find that

$$(1 - \mu) u_1^r \in (u_2, \dots, u_n),$$

so

$$u_1^r \in (u_2, \dots, u_n)$$

as $1 - \mu$ is a unit. It follows that $V(u_1, \dots, u_n) = V(u_2, \dots, u_n)$. This is a contradiction since the second thing has to have dimension at least one by dimension theory. The first thing $V(u_1, \dots, u_n)$ is just $\{x\}$ as the $\{u_i\}$ generate $\mathfrak{m}_x$.

▲

Remark. I am not sure, but I *suspect* this proof works the same for any regular local ring. I believe in that case one has to show that there is a *coefficient field* contained in the ring, which is the hard part of the proof of the Cohen structure theorem.

What do we get from this theorem?

We see that for any $f \in k[X]_x$ and any r, there is a *unique* degree r (nonhomogeneous) polynomial $g_r(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ such that

$$f \equiv g_r(u_1, \dots, u_n) \mod \mathfrak{m}_x^{r+1}.$$

The reason is that we can approximate f up to first order by a constant. This difference, which is in $\mathfrak{m}_x$, can be approximated up to second order by a linear term; one repeats by induction.

By uniqueness, we see that the g_r's are compatible, i.e.

$$g_r \equiv g_{r+1} \mod (x_1, \dots, x_n)^{r+1}.$$

By this compatibility, there is a limit to this process. The limit of the g_r is actually a formal power series, so it lies in formal power series ring $k[[x_1, \dots, x_n]]$.

19.4 Definition. The limit of the g_r is called the **Taylor series** of f. It lies in the formal power series ring.

A rephrasing of the above arguments shows:

19.5 Theorem. *The completion of $k[X]_x$ with respect to $\mathfrak{m}_x$ is the formal power series ring $k[[x_1, \dots, x_n]]$.*

Proof. This means that $k[X]_x/\mathfrak{m}_x^r \simeq k[[x_1, \dots, x_n]]/(x_1, \dots, x_n)^r$, the isomorphisms being compatible with the quotient maps. This is what we have shown above via the system of coordinates $\{u_i\}$. ▲

Someone asked, so we recall:

19.6 Definition. Let A be a ring, $I \subset A$ an ideal. The **I-adic topology** on A is the topological ring whose basis at zero is given by the powers I^j. The **I-adic completion** of A is the completion of A with respect to this topology, i.e.

$$\hat{A} = \varprojlim A/I^j.$$

In other words, equivalence classes of Cauchy sequences.

19.7 Example. The completion of the polynomial ring $k[x_1, \dots, x_n]$ with respect to the ideal $(x_1, \dots, x_n)$ is the formal power series ring.

19.8 Proposition. *In $k[X]_x$, we have $\bigcap \mathfrak{m}_x^r = (0)$. In particular, the map $k[X]_x \to \widehat{k[X]_x}$ is an injection.*

Proof. This follows from the Krull intersection theorem in commutative algebra as $k[X]_x$ is a noetherian local ring. ▲

§2 Applications

Taylor series in analysis are useful because we can plug in values and compute things. In our case, infinite series need not have any sense of convergence. However, we can use the fact that $k[X]_x$ is contained in its completion, a power series ring, to deduce properties of it.

19.9 Example. $k[[x_0, \ldots, x_n]]$ is a domain. It follows that $k[X]_x$ is a domain for any smooth point x. The local ring at a smooth point is a domain. Geometrically, this means that:

19.10 Corollary. *If x is smooth, there is only one component of X passing through x.*

19.11 Corollary. *If X is smooth and connected, then it is irreducible.*

Proof. Exercise. The idea is that the intersection of any two irreducible components is a nonsmooth point. ▲

Remark. There are many ways to say that something is locally invariant of X. One natural invariant is $k[X]_x$, the local ring; but this remembers too much. If you have a smooth connected complex variety, then any two points have neighborhoods in the complex topology which are isomorphic as complex manifolds. This is not true algebraically. The local rings are generally not isomorphic; they remember more than the analytic topology. But the *completions* at a smooth point are isomorphic. The completion forgets quite a lot of the other parts of the variety.

In the next lecture, we want to do the same thing as in this lecture for a harder algebraic property, namely *unique factorization.* We will prove that the power series ring is a UFD, and from that deduce the same for $k[X]_x$.

19.12 Theorem. *The local ring at a smooth point is a UFD.*

Lecture 20
10/8

Last time, we defined a topology on the local ring $k[X]_x$ of a variety X. This topology was the $\mathfrak{m}_x$-adic topology for $\mathfrak{m}_x$ the maximal ideal. We showed that if x is smooth, the completion $\widehat{k[X]_x}$ is isomorphic to the polynomial ring $k[T_1, \ldots, T_n]$ for $n = \dim X$. We want to use this to get information about the local ring.

The goal for the next few lectures is to show that $k[X]_x$ is a UFD if x is a smooth point. We showed earlier that it is a domain. We will deduce it from:

20.1 Theorem. *The completion $k[[T_1, \ldots, T_n]]$ is a UFD.*

Next, we will show that if you have a local ring whose completion is a UFD, then the ring itself is a UFD.

§1 The division and preparation theorems

We start with

20.2 Definition. If $(A, \mathfrak{m})$ is a local ring and $f \in A[[T]]$, then we say that f is has **order** m if $f = \sum a_i T^i$ where

$$a_0, \dots, a_{m-1} \in \mathfrak{m}$$

but

$$a_m \notin \mathfrak{m}.$$

It is the order of vanishing of the reduction of f over the field $A/\mathfrak{m}$.

20.3 Theorem (Weierstrass division theorem)**.** *Let $(A, \mathfrak{m})$ be local and complete. If $g, h \in A[[T]]$ where h has order m, then there are unique elements $q, r \in A[[T]]$ such that*

1. *$g = qh + r$.*
2. *r is a polynomial of degree $\leq m - 1$.*

So it is a division algorithm in power series rings over a local ring.

Proof. First, if the order of h is zero, i.e. if the constant coefficient in h is not in $\mathfrak{m}$, then h is a unit in $A[[T]]$. This proves the theorem in the case $m = 0$. The reason for this fact is that if

$$h = h_0 + h_1 T + \dots, \quad h_0 \notin \mathfrak{m},$$

then one simply successively solves the equations

$$(h_0 + h_1 T = \dots)(x_0 + x_1 T + \dots) = 1.$$

Each equation, as one can check, is solvable as g_0 is invertible. For instance $x_0 = \frac{1}{h_0}$ and $x_1 = \frac{-x_0 h_1}{h_0}$.

In general, say h is of order m. Then we can write h as a polynomial of degree $\leq m - 1$ plus T^m times something with an invertible element in the constant term. So we can write

$$h = \beta(T) + T^m \gamma$$

for $\beta(T) \in \mathfrak{m}[T]$ and $\gamma \in A[[T]]$ invertible. Inverting yields that $\gamma^{-1} h = \gamma^{-1}\beta + T^m$. So up to a unit in $A[[T]]$, we can write

$$\gamma^{-1} h = T^m + \alpha, \quad \alpha = \beta\gamma^{-1} \in \mathfrak{m}[[T]].$$

We want to solve the equation $g = qh + r$. We will do this by successive approximation, analogous in a sense to the Banach fixed point theorem. Since h is up to units $T^m + \alpha$, we can just assume that $h = T^m + \alpha$. So we want to solve:

$$g = (T^m + \alpha) q + r.$$

Start with any set q_0, r_0 of polynomials. Define by induction q_i, r_i via:

$$g - \alpha q_{i-1} = r_i + T^m q_i$$

where r_i has degree $\leq m-1$ and q_i is unconstrained. We have to show that this pair of sequence converges. One gets from these equations that

$$\alpha(q_{i+1} - q_i) = (r_i - r_{i+1}) + T^m(q_i - q_{i+1}).$$

But $\alpha \in \mathfrak{m}$. If we start with any q_0, we find that the $r_i \equiv r_{i+1}$ modulo a high power $\mathfrak{m}^i$. Ditto for $q_i - q_{i+1}$ when i is large. It follows that we can define

$$q_\infty = \lim q_i, \quad r_\infty = \lim r_i.$$

We then have

$$g - \alpha q_\infty = r_\infty + T^m q_\infty,$$

so the pair (r_∞, q_∞) solves the equation we wanted. ▲

As a corollary, we get:

20.4 Theorem (Weierstrass preparation lemma)**.** *Let $(A, \mathfrak{m})$ be a complete local ring. Then any element $h \in A[[T]]$ of order m can be written as $h = ug$ where u is a unit and g is a monic polynomial of degree m.*

In particular, the principal ideals in $A[[T]]$ come from ideals in the polynomial ring.

Proof. This follows from the division theorem. Let $h \in A[[T]]$ be of order m. By the division theorem, we can divide T^m by h. We can write

$$T^m = qh + r, \quad \deg r \leq m-1.$$

If we reduce this modulo $A/\mathfrak{m}$, we find that r maps to zero and so is a polynomial in $\mathfrak{m}[T]$; furthermore, q is invertible in $A/\mathfrak{m}[[T]]$. The reason is that q when reduced mod $\mathfrak{m}$ has only nonzero terms of degree $\geq m$.

As a result, the intial coefficient of q is a unit, so we can write

$$h = q^{-1}(T^m - r).$$

This completes the proof. ▲

Remark. We actually find that the polynomial in the preparation theorem has the form

$$T^m + a_1 T^{m-1} + \cdots + a_0, \quad \forall a_i \in \mathfrak{m}.$$

This is the algebraic counterpart of the several complex variables theorem. We are going to apply this to the power series rings now.

§2 Power series rings are UFDs

Proof of theorem 1. We will now prove the first theorem, namely that if k is a field, then $k[[T_1, \ldots, T_n]]$ is a UFD. The proof runs by induction on n. When $n = 0$, this is immediate.

We will now assume the result for $n - 1$ and then prove it for n. Recall the **Gauss lemma**:

20.5 Theorem. *If A is a UFD, $A[T]$ is a UFD.*

Thus the inductive hypothesis with Gauss's lemma implies that $k[[T_1, \ldots, T_{n-1}]][T_n]$ is a UFD. But every element in the whole power series ring $k[[T_1, \ldots, T_n]]$ is a unit times an element in $k[[T_1, \ldots, T_{n-1}]][T_n]$ by the preparation theorem. So every element in $k[[T_1, \ldots, T_n]]$ can be written uniquely as a product of irreducible elements in $k[[T_1, \ldots, T_{n-1}]][T_n]$ and a unit.

Dangerous bend. Someone pointed out that technically, the preparation lemma does not apply to elements of infinite order (which may exist if the maximal ideal is not zero). This point will be clarified in the future. It is simple.

We now only have to check that an irreducible element in $k[[T_1, \ldots, T_{n-1}]][T_n]$ is irreducible in $k[[T_1, \ldots, T_n]]$. This also follows from the preparation theorem, and we leave it to the reader. ▲

§3 The downward UFD theorem

20.6 Theorem. *Let $(R, \mathfrak{m})$ be a noetherian local ring. If the completion $\hat{R}$ is a UFD, then R is a UFD.*

Remark. I initially asked whether we need to require that $R \to \hat{R}$ is injective, but this is automatic as R is a noetherian local ring.

Proof. R is a topological ring with the $\mathfrak{m}$-adic topology, where a basis at zero is given by $\{\mathfrak{m}^n\}$. We shall prove:

20.7 Lemma. *Any ideal I in R is closed with respect to this topology.*

Proof. If we have an ideal $I \subset R$, then R/I is a local ring as well with maximal ideal $\mathfrak{m}/I$. The map $R \to R/I$ is continuous. So it is sufficient to do this in the case of $I = 0$. However, the Krull intersection theorem implies that

$$\bigcap \mathfrak{m}^n = (0).$$

Now each $\mathfrak{m}^n$ is open, so it is closed (recall that an open subgroup of a topological group is closed); the intersection is also closed. ▲

We now prove a special case of a more general result in commutative algebra.

20.8 Lemma. *If $I \subset R$ is an ideal, then $I\hat{R} \cap R = I$.*

Proof. One inclusion $\supset$ is clear.

For the other inclusion, suppose $x \in I\hat{R} \cap R$. Suppose I is generated by $(a_1, \dots, a_n)$. We find that we can write

$$x = \sum a_i \alpha_i, \quad \alpha_i \in \hat{R}.$$

We are using the convention of Roman letters for R and Greek letters for $\hat{R}$. We must show that $x \in I$ in fact. The idea is to approximate.

The $\alpha_i \in \hat{R}$. For every n, there is $x_i^n \in R$ such that $\beta_i^n = x_i^n - \alpha_i \in \hat{\mathfrak{m}}^n$. It follows that

$$x = \sum a_i x_i^n + \sum a_i \beta_i^n.$$

The first term is in I, while the second is in $I\hat{\mathfrak{m}}^n \cap R$. The second element is thus in $\hat{\mathfrak{m}}^n \cap R$. In particular, by a result in commutative algebra, it lies in $\mathfrak{m}^n$. It follows in particular that

$$x \in \bigcap (I + \mathfrak{m}^n).$$

But I is closed, so this means $x \in I$. ▲

We're out of time so will finish the result later.

▲

Lecture 21
10/13

§1 Correction

OK. So, let's start with a correction. Last time, we stated:

We proved the **Weierstrass preparation theorem** for the power series ring. We said that:

21.1 Theorem. *If k is a field, and $f \in k[[T_1, \dots, T_n]]$ is such that f has order m in T_n, i.e.*

$$f = \sum f_i(T_1, \dots, T_{n-1}) T_n^i, \quad f_0, \dots, f_{m-1} \in \mathfrak{m}_{k[[T_1, \dots, T_{n-1}]]}, f_m \notin \mathfrak{m}_{k[[T_1, \dots, T_{n-1}]]},$$

then f can be written as a product of a monic "polynomial," i.e. something in $k[[T_1, \dots, T_{n-1}]][T_n]$ with coefficients in the maximal ideal,[16] *and a unit.*

The condition that the coefficients of T_n not all be nonunits is equivalent to saying that f doesn't vanish on the T_n-axis. Also, technically we proved the theorem more generally for power series rings over a complete local ring.

21.2 Corollary. *$k[[T_1, \dots, T_n]]$ is a UFD.*

This is what we have to touch up from last time.

[16]Except for the first coefficient, which is one.

Proof. Let f be a power series. After a *linear change of variables*, we can assume that the preparation theorem applies to f, i.e. that f doesn't vanish on the T_n-axis. So we can write f as a polynomial over $k[[T_1, \dots, T_{n-1}]]$ times a unit. But $k[[T_1, \dots, T_{n-1}]]$ is a UFD, so the Gauss lemma implies that f can be factored uniquely into primes in the UFD $k[[T_1, \dots, T_{n-1}]][T_n]$. One has to check that these primes remain primes in the power series ring. ▲

Remark. The Weierstrass preparation theorem is also true with *convergent power series* if $k = \mathbb{C}$. The proof is the same. One has to check that when you run the proof with a convergent power series at the start, you get a convergent power series at the end.

21.3 Corollary (of the holomorphic Weierstrass preparation theorem)**.** *We find that the vanishing locus of a holomorphic function in* $\mathbb{C}^n$ *at* 0 *is locally (in the metric topology) a finite branched cover of an open ball in* $\mathbb{C}^{n-1}$*.*

The reason is that if f is holomorphic in a neighborhood of zero in $\mathbb{C}^n$, then we can write up to units at zero (which don't matter for the *local* nature of the analytic variety at zero)

$$f = z_n^k + g_1 z^{k-1} + \dots + g_k.$$

So the roots of f correspond to points in a small neighborhood of zero in $\mathbb{C}^{n-1}$ with multiplicities (generally, k of them).

This is a side remark and won't be used in the course.

§2 The local ring

Anyway, we were in the middle of showing last time that the *local ring* at a *smooth point* of a variety is a UFD. This is going to follow from:

21.4 Theorem. *If the completion* $\hat{R}$ *of a noetherian local ring* R *is a UFD, then so is* R*.*

Proof. We begun this last time, but did not finish. Last time, we were only able to prove a few lemmas. One of them was that if $I \subset R$ is an ideal,

$$I\hat{R} \cap R = I.$$

This follows from the fact that ideals are *closed* in the adic topology.

We need to prove that if $a, b \in R$ do not have common factors, and $a \mid bc$, then $a \mid c$. After that one can run the usual proof: we see from this that every irreducible element is *prime*. Since R is noetherian, any element is a product of irreducibles. So every element is a product of primes, necessarily uniquely (up to units).

1. Let us first show that under the above assumptions (a, b have no common factors in R), then they have none in $\hat{R}$. Suppose otherwise, say $a = \alpha\gamma, b = \beta\gamma$ where the Greek letters indicate elements of $\hat{R}$; we may as well assume that α, β have no common factor. We find

$$\alpha b = \beta a.$$

Now we want to get something like this but for approximations in R. For each n, choose $x_n, y_n \in R$ that approximate α, β up to $\hat{\mathfrak{m}}^n$. Then

$$x_n b - y_n a = -(\alpha - x_n)b + (\beta - y_n)a \in \hat{\mathfrak{m}}^n.$$

Consequently, $x_n b - y_n a \in R \cap (a,b)\hat{\mathfrak{m}}^n$. By the lemma, this is equal to $(a,b)\mathfrak{m}^n \subset R$. As a result, we can write

$$x_n b - y_n a = -ae_n + bf_n, \quad e_n, f_n \in \mathfrak{m}^n.$$

So if we modify x_n, y_n by e_n, f_n, we still get approximations of order n of α, β. Writing $x'_n = x_n + e_n, y'_n = y_n + f_n$, we also find

$$x'_n b - y'_n a = 0.$$

So the equation in the completion has given us a corresponding equation in the original ring. Since $a = \alpha\gamma, b = \beta\gamma$, we find ($R$ being a domain):

$$x'_n \beta = y'_n \alpha.$$

Since the completion is a UFD, we find that $\alpha \mid x'_n$. For every n, we have a very good approximation of α, and α divides it. If k is such that $\alpha \in \hat{\mathfrak{m}}^k - \hat{\mathfrak{m}}^{k+1}$ and $n > k+1$, then it cannot be that $x'_n/\alpha \in \hat{\mathfrak{m}}$ or x'_n couldn't approximate α; they'd have different "valuations" at $\hat{\mathfrak{m}}$. It must follow that α, x'_n are associates.

But $\alpha \mid a$ in $\hat{R}$. So $x'_n \mid a$ in $\hat{R}$. In particular, $a \in \hat{R}x'_n \cap R = Rx'_n$; thus

$$x'_n \mid a \quad \text{in } R.$$

Let say $dx'_n = a, d \in R$. In the equation $x'_n b = y'_n a$, we find that $x'_n b = y'_n d x'_n$. In particular, $b = y'_n d$. However, it follows that d is a common factor of a, b in R. Thus d is a unit. So actually x'_n, a are associates. In other words, $(x_n) = (\alpha) = a$. In particular, this means that γ is invertible. And we're done. But this was confusing.

2. Anyway, now let $a, b \in R$ have no common factor, and $a \mid bc$. Then a, b have no common factor in $\hat{R}$. We know that $a \mid bc$ in $\hat{R}$, so $a \mid c$ in $\hat{R}$. It follows that $c \in \hat{R}a \cap R = Ra$. Thus $a \mid c$ in R. That's the end of the proof.

▲

§3 Local complete intersections

This was really a ton of commutative algebra, but it has a good reason. It answers a basic question. Say you have a bunch of equations. One of the basic questions is, *How many equations do you need to define a variety?* If you have a variety V inside some affine space $\mathbb{A}^n$, what is the minimal number of equations in $k[x_1, \ldots, x_n]$ that will cut out V? We have seen that we need at least the codimension. In some cases, you can get by with *just* the codimension, but not in general. Smoothness answers the question in some cases.

Smooth varieties are *local set-theoretic intersections*, as we will see. We are going to run out of time today, but anyway:

21.5 Theorem. *Suppose $x \in X$ is smooth for X a variety. Let $Y \subset X$ be irreducible and of codimension 1. Then there is an affine neighborhood U of $x \in X$ and $f \in k[U]$ such that $I(U \cap Y) = (f) \subset k[U]$. As a result, $Y \cap U = V(f) \cap X$.*

So locally codimension 1 subvarieties are cut out by one equation. But the result actually says more: it says something about the *ideals*.

Proof. Wlog, X is affine. Y is a closed set, so there is a function $f \in k[X]$ that vanishes on Y. We get an element $f \in k[X]_x$, which can be factored into primes:

$$f = f_1 \dots f_k \in k[X]_x.$$

By replacing X by a smaller neighborhood U of x, we can assume the f_i are regular in $k[U]$. Then $Y \cap U$ is still irreducible, so since

$$Y \subset \bigcup V(f_i) \cap X,$$

some f_i must vanish on Y. We can replace f by that f_i which vanishes on Y.

We can assume, therefore, that f is a regular function vanishing on Y which gives a prime element in $k[X]_x$. Suppose $V(f) \supset Y$ can be written as $V(f) = Y \cup Y'$. Then there are two options $x \in Y'$ and $x \notin Y'$. In the latter case, Y is defined by the ideal (f) outside of Y'. Shrinking U to throw out Y', we get on that open set $V(f) = Y$.

In the former case of $x \in Y'$, then we have two closed components passing through Y. We have functions $g, h \in k[X]$ such that $gh = 0$ on $V(f)$ but g does not vanish on Y and h does not vanish on Y'. The first means by the Nullstellensatz that $f \mid (gh)^n$ for some n, the division being in $k[U]$. This holds in the local ring $k[X]_x$ consequently. Since the localization is a UFD, we must have that $f \mid g$ or $f \mid h$. This is a contradiction, since then we would have that (by shrinking U), $f \mid g$ or $f \mid h$ in $k[U]$, which contradicts what we have assumed about g, h not vanishing on all of $V(f)$.

In any case, we almost get what we wanted. We have shown that Y can be cut out near x by one equation: f. We still have to show that f is actually the ideal. Suppose g vanishes on Y; then $f \mid g^n$ for some n by Hilbert. Therefore f divides g in some shrinking of U by the same localization argument and the fact that f is prime in $k[X]_x$. ▲

Lecture 22
10/15

§1 Recap and vista

Let us recall what we were doing. The aim is to show that better the codimension and number of equations you need to define a variety. We had one inequality that whenever you add an equation, the dimension can drop at most by one. In general, this is all you can say, but in the presence of smoothness, things become nicer.

Last time, we showed that:

22.1 Theorem. *If X is smooth at x and Y is a codimension 1 irreducible subvariety, then Y has a local equation near x.*

This means that there is an open affine U containing x such that the ideal of $Y \cap U$ in $k[U]$ is generated by one element $f \in k[U]$. This is a generalization of a theorem we already saw when $X = \mathbb{A}^n$.

I think this follows from the fact that a ring is a UFD only if (and if) every prime ideal of height one is principal. In fact, this is essentially the idea of the proof we gave.

We sketched the proof hastily last time, so let's sketch it hastily again.

Proof. Shrink X and assume that it is affine. Take any polynomial $f \in k[X]$ which vanishes on Y. This f gives you an element in the local ring $k[X]_x$. We can decompose it into primes in $k[X]_x$, say $f = f_1 \dots f_k$. Since there are finitely many of them, we can assume that this factorization happens in some neighborhood U, which is affine. So each $f_i \in k[U]$ and $f = \prod f_i \in k[U]$. Since f vanishes on all of Y, irreducibility implies that one of the f_i vanishes on Y. We might as well replace f with this f_i.

We can thus assume that the f we initially chose gives an irreducible element in the local ring. Then $V(f) \supset Y$; the question is whether $V(f) = Y$ at least in a neighborhood of x. We can split $V(f) = Y \cup Y'$ for components Y, Y'; suppose $Y' \neq \emptyset$. If Y' doesn't pass through x, then $V(f)$ is locally Y and we got it.

If Y' passes through x, then we could take a function g which vanishes on Y and not on Y', and we could take a function h which vanishes on Y' and not on Y. Then gh vanishes on $V(f)$ but g, h are not multiples of f. This is a contradiction.

We showed earlier, moreover, that f doesn't just cut out Y, but is a *local equation* for Y. So if g vanishes on Y, then $f \mid g^n$ for some n, and therefore $f \mid g$—locally, at least. To be precise, $I(Y)$ is finitely generated by $g_1, \dots, g_k$. Each one of these vanishes on Y. By the Nullstellensatz, we have $f \mid g_i^n$ for each i. In the local ring $f \mid g_i$ for each i. So shrinking to a smaller open neighborhood, we can assume that $f \mid g_i$ in $k[U]$ itself. And in this neighborhood,

$$I(Y) = (g_1, \dots, g_k) = (f).$$

▲

Here is a nice corollary.

22.2 Corollary. *If X is smooth everywhere, and $X \dashrightarrow \mathbb{P}^n$ is a rational map. Then ϕ can be defined outside a codimension two subvariety.*

Proof. Near any point x, ϕ is given by a tuple of rational functions, so

$$\phi(y) = [\phi_0(y) \dots \phi_n(y)].$$

A priori they are quotients, but by clearing denominators we can assume each ϕ_i is actually regular. As written here, this map ϕ is not defined if and only if each ϕ_i is zero. It is not defined therefore in the common zero locus $V(\phi_0, \dots, \phi_n)$. However, we want to extend the definition of ϕ.

For every x, choose an affine neighborhood U_x of x and functions $\phi_0, \dots, \phi_n \in k[U_x]$ representing ϕ on U_x, and furthermore such that these *have no common divisor in the local ring*. The way we can do this is first to pick polynomials $\phi_0, \dots, \phi_n$, then go to the local ring $k[X]_x$ and pull out a common factor. Pulling out the common factor may mean we have to go to a smaller affine neighborhood.

Fix $x \in X$. If the procedure above gives functions $\phi_0, \dots, \phi_n$ that don't simultaneously vanish at x, then we have a neighborhood of x in which ϕ is regular. Suppose the procedure at x gives functions that do simultaneously vanish at x. Now I claim that the common zero locus of $\phi_0, \dots, \phi_n$ cannot be of codimension one in U_x. If otherwise, then it would be principal in a smaller neighborhood of U_x. It would have a defining equation. But this contradicts the lack of a common factor.

So we have shown that each $x \in X$ has a neighborhood U_x on which ϕ can be defined except in codimension ≥ 2. Covering X by finitely many such of them, we get the corollary. ▲

22.3 Corollary. *Let X, Y be smooth projective curves that are birational.*[17] *Then they are isomorphic.*

Proof. Indeed, this follows from the previous result, and the fact that $1-2$ is negative. ▲

Remark. Of course, this is not true without the projectivity hypothesis.

§2 Smooth subvarieties of smooth varieties

We have a very nice result for systems of local coordinates.

22.4 Theorem. *Suppose that X is smooth at x and $\phi_1, \dots, \phi_n \in \mathfrak{m}_x \subset k[X]_x$ are local coordinates at x. For every m, the vanishing locus $Y = V(\phi_1, \dots, \phi_m)$ is smooth at x and has dimension $n-m$. Moreover, the $\phi_{m+1}|_Y, \dots, \phi_n|_Y$ form a system of local coordinates at $x \in Y$. Furthermore, the ideal of Y is generated locally by $\phi_1, \dots, \phi_m$.*

Proof. Induction on m. Let us first do $m = 1$.

So Y is the vanishing locus of ϕ_1, and is thus of codimension one, since ϕ_1 is not trivial. Moreover, $I(Y)$ is locally generated by a single function f by previous results. It follows that $f \mid \phi_1$, say $\phi_1 g$. This implies that $\nabla\phi_1(x) = g(x)\nabla f(x)$ by the product rule. Since $\nabla\phi_1(x)$ is nonzero, as ϕ_1 is a local coordinate, we have that $g(x) \neq 0$. In particular g is invertible in some open neighborhood, and the ideals generated by f, ϕ_1 are the same in some open neighborhood. Restrict to this open neighborhood; then Y has ideal generated by ϕ_1 on that neighborhood.

Now $\nabla\phi_1(x)$ vanishes on $T_x(Y)$ because the tangent space of Y is defined as the common vanishing locus of the gradients of generators. In particular, $T_x(Y)$ is the kernel of $\nabla\phi_1(x) : T_x(X) \to k$. It follows that the dimension of $T_x(Y)$ is one less than the dimension of $T_x(X)$. So we find that $\dim T_x(Y) = n-1$ and Y is smooth at x. Since $\phi_1, \phi_2, \dots, \phi_n$ are local coordinates on X, their gradients are linearly independent, and it follows that the last $n-1$ must be local coordinates on Y.

The general m follows by induction since the hypotheses and conclusions are similar. ▲

Now I claim that any smooth inclusion of varieties looks like this.

[17] A field-theoretic question.

22.5 Theorem. *Let $Y \subset X$ be irreducible varieties. Suppose $x \in Y$ is smooth in both X, Y. Then there is a system of local coordinates $\phi_1, \dots, \phi_n$ at $x \in X$ such that $Y = V(\phi_1, \dots, \phi_m)$ near x.*

In particular, the $\phi_i|_{i \leq m}$ locally generate the ideal of Y, and the other ϕ_i are local coordinates.

Proof. Let $m = \dim X - \dim Y$. Now we want $\phi_1, \dots, \phi_m$ to vanish on Y. We have an inclusion $T_x(Y) \subset T_x(X)$ which by smoothness has codimension m by smoothness. It is cut out by equations of the form

$$\nabla f(x)(v) = 0, \quad v \in T_x(X)$$

for $f \in I(Y)$. We can thus choose $\phi_1, \dots, \phi_m$ in this ideal such that the gradients $\nabla \phi_i, 1 \leq i \leq m$ are linearly independent as functionals on the tangent space; this is precisely the statement that they cut out the tangent space $T_x(Y)$. It follows that the $\phi_1, \dots, \phi_m \in \mathfrak{m}_x$, which have gradients linearly independent on $T_x(X)$, are linearly independent in $\mathfrak{m}_x/\mathfrak{m}_x^2$ by the nondegenerate pairing $\mathfrak{m}_x/\mathfrak{m}_x^2 \times T_x(X) \to k$.

So we can extend these to a basis $\phi_1, \dots, \phi_n \in \mathfrak{m}_x/\mathfrak{m}_x^2$. We have thus just built a system of local coordinates. What we now need to show is that Y is in fact the vanishing locus of these, at least locally. Let's look at

$$Y' = V(\phi_1, \dots, \phi_m);$$

by the previous theorem, Y' is smooth at x and has dimension $n - m$. Moreover, $Y' \supset Y$.

Remember now that if a point is smooth, there is only one irreducible component passing through it. So in some open neighborhood of x, Y' is irreducible; it also has the same dimension as Y and consequently is locally equal to Y. Since $Y = Y'$, the previous result says that the $\phi_j|_{j \geq m+1}$ form local coordinates. ▲

Remark. If X is smooth and $Y \subset X$ is smooth, then Y is a local complete intersection. I think this is the fancy way of stating the above result.

§3 Beginning Bezout

We are now done talking about smoothness. We want to talk about the Bezout theorem.

In the simplest form: If you have two projective curves of degree d, e in $\mathbb{P}^2$, they intersect (we know this). Morally, they intersect in de points. Morally means that they do "generically"; less generically it is $\leq de$ points, and if you count them with multiplicities we do get equality. At least, we can state a higher dimension analog of this. For this we will need to define the degree of something which is not a hypersurface. So far we have defined the degree of a hypersurface (the degree of the polynomial cutting it out).

We start with:

22.6 Definition. Let $f : X \to Y$ is a dominant map between two irreducible varieties of the same dimension.[18] The **degree** of f is $\deg f = [k(X) : k(Y)]$.

[18] This is **not necessarily birational.**

Note that dominance induces a map $k(Y) \to k(X)$. Note also that the transcendence degrees of $k(Y), k(X)$ are the same, so the degree is finite.

22.7 Example. The map $x \to x^2$, $\mathbb{A}^1 \to \mathbb{A}^1$ satisfies the above but is not birational.

Lecture 23
10/18

§1 Intersections

We are dealing with the most important question for equations: namely, how many solutions there are. Let us say you have two varieties X, Y, and we consider the intersection $X \cap Y$. One measure of the size is given by the **dimension**. We have showed earlier that the codimension of $X \cap Y$ is at most the codimension of X plus the codimension of Y (if the varieties do intersect). In particular, if the varieties do intersect,

$$\dim X + \dim Y - n.$$

We also know that the varieties will always intersect if they are projective varieties.

In general, we can say much more. We start with a definition of "nice" intersection.

23.1 Definition. Let Z be a smooth variety. Let $X_1, \dots, X_n \subset Z$ subvarieties. We say that $X_1, \dots, X_n$ intersect **transversely** at a point $x \in X_1 \cap \dots \cap X_n$ if all these varieties X_i are smooth at x and, in addition, the tangent spaces at x are in "general position:"

$$\operatorname{codim}(\bigcap T_x X_i) = \sum \operatorname{codim} T_x(X_i).$$

(Here "codimension" is with respect to $T_x(Z)$.)

23.2 Proposition. *Let $X_1, \dots, X_n$ intersect transversely at $x \in Z$. Then $\bigcap X_i$ is smooth at x and has codimension $\sum \operatorname{codim}(X_i)$ near x.*

Proof. This follows because $\operatorname{codim}_x(\bigcap X_i) \leq \sum \operatorname{codim}_x(X_i)$ by standard dimension theory and $\operatorname{codim}(T_x(\bigcap X_i)) = \sum \operatorname{codim} T_x(X_i) = \sum \operatorname{codim}_x(X_i)$ by transversality and smoothness. Also, necessarily $\operatorname{codim}_x(\bigcap X_i) \geq \operatorname{codim} T_x(\bigcap X_i)$ by basic properties of tangent spaces: the tangent space is always bigger than the variety. ▲

§2 The degree

23.3 Definition. Let $X \subset \mathbb{P}^n$ be an irreducible projective variety of dimension d. The **degree of** X is the number of points of the intersection of X with a generic $n-d$-dimensional plane in $\mathbb{P}^n$.

When X is reducible, we define $\deg X$ to be the sum of the degrees of the irreducible components.

We should clarify what "generic" means. It means the following: there is an open dense set of $n-d$ planes (which is a Grassmannian variety[19]) in $\mathbb{P}^n$ for which the

[19]Defined in the homework—we have seen that the Grassmannian is irreducible, and indeed it is smooth, as it is locally isomorphic to some affine space.

intersection with X has a fixed number of points. That number is the "generic" size. This claim, however, is nontrivial. So $\deg X$ is uniquely determined once we grant this claim.

Remark. If X was a d-dimensional plane, then this is linear algebra: the generic $n-d$-dimensional plane intersects X at one point. So the degree of a plane is one.

More generally, what we are aiming towards is Bezout's theorem:

23.4 Theorem. *If $X, Y \subset \mathbb{P}^n$ intersect transversally, then*

$$\deg X \cap Y = \deg X \deg Y.$$

In particular, when X, Y have complementary dimension, then $X \cap Y$ is just a finite set, and the degree is just the size. So $X \cap Y$ has $\deg X \deg Y$ points. For instance, two generic conics in $\mathbb{P}^2$ intersect at four points.

The purpose of this class is to prove the mysterious "claim" above about genericness being well-defined, i.e. that as λ ranges over an open dense subset of the Grassmannian, then $|\lambda \cap X|$ is constant.

We start with a review of an old definition:

23.5 Definition. Let X, Y be irreducible of the same dimension. Let $f : X \to Y$ be dominant. Then the **degree** of f is the degree of the field extension

$$k(Y) \to k(X).$$

The equality of the dimensions assures that this is finite.

We want to connect this idea of degree to the size of the fiber.

23.6 Theorem. *Suppose Y is affine, and $Z \subset Y \times \mathbb{P}^1$ is closed; let $f : Z \to Y$ be the projection. Suppose $\dim Y = \dim Z$ and both are irreducible. Suppose $y_0 \in Y$ is a smooth point, and for every $z \in f^{-1}(y_0)$, $z \in Z$ is smooth. Moreover, assume that $Df : T_z Z \to T_{y_0} Y$ is an isomorphism for each $z \in f^{-1}(y_0)$.*

Then $|f^{-1}(y_0)| = \deg f$.

These "y_0's" are called *regular values.* In analysis, Sard's theorem says that there are lots of regular values. The set of irregular values has measure zero.

Generically, it is **not necessarily true** that this condition is satisfied.

23.7 Example. Let $k = \overline{\mathbb{F}_p}$. Take $Y = \mathbb{A}^1$, $Z = \{(x^p, x)\} \subset \mathbb{A}^2 \subset \mathbb{A}^1 \times \mathbb{P}^1$. Then Z is closed in $\mathbb{A}^1 \times \mathbb{P}^1$. Now $k(Y) = k(x)$. The projection from $Y \to Z$ is not an isomorphism on the function fields, though, as it is the purely inseparable inclusion $k(x) \to k(x^{1/p})$. However, the fibers of a point in Y are each of size one.

This counterexample is fundamentally a characteristic p thing though, because in characteristic zero you have Sard's theorem. This shows that there are lots of regular values in the case $k = \mathbb{C}$. This implies that there are lots of regular values over any algebraically closed field of characteristic zero.

Let us now prove the theorem.

Proof. Everything here is local on Y, so we can assume that Y is affine, for instance.

First, let us show that $f^{-1}(y_0) \subset \{y_0\} \times \mathbb{P}^1$ is finite. It's obviously a closed subset of $\mathbb{P}^1$, so it is either $\mathbb{P}^1$ or a finite set. But $\mathbb{P}^1$ has a nonzero tangent vector pointing in the $\mathbb{P}^1$ direction. The fact that $Df : T_z(Z) \to T_{y_0}(Y)$ is an isomorphism implies that there cannot be any nonzero tangent vectors pointing purely in the $\mathbb{P}^1$ direction. So $f^{-1}(y_0)$ is finite.

Z has codimension one in $Y \times \mathbb{P}^1$. We can assume that Y is smooth, by shrinking Y further. So $Y \times \mathbb{P}^1$ is smooth. Z is thus defined by a single equation in $Y \times \mathbb{P}^1$ locally—in a neighborhood of each element of Z. (More on this in the next paragraph.) For now, put homogeneous coordinates $[\xi, \eta]$ on $\mathbb{P}^1$. We can assume $(y_0, \infty) = (y_0, [1, 0]) \notin Z$; otherwise choose different homogeneous coordinates. Shrinking Y, we can thus assume that $Z \subset Y \times \mathbb{A}^1$.

So first, we have shrunk Y such that $Z \subset Y \times \mathbb{A}^1$. We want to say that Y can be shrunk Y even further so that Z is defined by one equation. Let P be some element vanishing on Z. We know that $k[Y]_y$ is a UFD, hence $k[Y]_y[t]$ is a UFD. We can decompose P into a product $\prod P_i$ where each P_i is irreducible in $k[Y]_y[t]$. It follows by irreducibility that Z must be defined by one of the P_i by the usual argument if we shrink Y. (Sketch.)

Anyway, Z is defined by a single equation $F(y, t) = 0$. So the equation is something like

$$F(y, t) = a_d(y)t^d + \cdots + a_0(y), \quad a_d \not\equiv 0,$$

with d minimal. This implies that the degree of f is exactly d.

I claim that $a_d(y_0) \neq 0$. Otherwise, (y_0, ∞) would be a solution of this equation (or rather its projectivization). (Geometrically, the idea is that when the leading coefficient of a polynomial vanishes, one of the roots flies off to ∞.) We find that $|f^{-1}(y_0)| \leq d$ since a one-variable polynomial of degree d, namely $F(y_0, t)$, can have at most d roots.

Now we have to use the assumption that the value is regular to show that there are actually d roots. Let $z = (y_0, t_0) \in Z$. We know two things. We know that z is smooth and the derivative is onto. The former means that the tangent space is of the right dimension. I.e. as F defines Z, we have that $\nabla F|_z \neq 0$. Furthermore the differential DF of the projection is onto, so the last coordinate of ∇F, which is to say $\frac{\partial F}{\partial t}$, is nonzero. Since we have this at all preimages, this implies that the one-variable polynomial $F(y_0, \cdot)$ has no multiple roots. There are thus precisely d roots in t. ▲

Remark. What's important here is that the derivative $\frac{\partial F}{\partial t}$ does not vanish. However, $\frac{\partial F}{\partial t}$ is a polynomial of smaller degree than F, so if it vanishes on the zero locus of F, it must be identically zero. This can happen only in characteristic p. This is why generically the above conditions are satisfied in characteristic zero.

Lecture 24
[Section] 10/18

There's an alternative perspective on number three on the problem set in Shafarevich, on *differential forms*.

24.1 Exercise. Let $X \subset \mathbb{A}^n$ be an affine variety. A derivation of X is the same thing as a *vector field* $X \to k^n$ which maps each $x \in X$ into $T_x X$.

One can similarly define a *differential.* Given X and the coordinate ring $k[X]$, one can think of the module of *differentials* as the $k[X]$-module Ω which is generated by symbols $df, f \in k[X]$ modulo the standard relations of differentials.

If you are interested in doing extra reading, there is a very interesting paper related to problem 1 (the determination of a tangent space to a group-homomorphism variety) by Goldman, *The symplectic nature of surface groups.* Goldman shows that any representation variety of a *surface group* (i.e. the fundamental group of an orientable group) in a semisimple Lie group has a natural symplectic structure having to do with Poincaré duality. It's pretty easy to read, and about twenty pages long. The paper will give you an introduction to the algebraic side of the field of Teichmuller theory.

§1 A little Teichmuller theory

Consider a surface Σ_2 of genus two. This is a very concrete thing, which can be drawn explicitly; it is a nice, smooth manifold. It is also a complex manifold: it has a complex structure. There are charts on this curve which map to $\mathbb{C}$ and transition functions which are holomorphic.

How can you explicitly find a complex structure on this? We can think of it by starting with the Riemann sphere S^2, which has a complex structure on it, and choosing six points $a_1, \dots, a_6$. If you choose paths between those points, cut open, and double across them, and glue two copies of these together, you get Σ_2 with a natural map to the sphere S^2. The map $\Sigma_2 \to S^2$ gives a complex structure (it makes Σ^2 a branched cover). This is not the only way, though.

The **Teichmuller space** $T(\Sigma)$ of a surface Σ is given by equivalence classes of complex structures on Σ. This depends on the genus of Σ.

How does this relate to representations of the fundamental group? First, note that the covering space of a complex manifold is a complex manifold. If we have a surface Σ with a complex structure, there is a complex structure on its universal covering space Σ'. The universal covering space is homeomorphic to hyperbolic space though, because of the classification of simply connected surfaces.

24.2 Theorem. *A simply-connected Riemann surface is biholomorphic to the Riemann sphere, the complex plane, or hyperbolic space.*

So if Σ is a surface of positive genus, then its cover can't be S^2. The group of holomorphic isomorphisms of $\mathbb{C}$ is isomorphic to the affine group, which is solvable. However, the fundamental group injects into the group of holomorphic isomorphisms, and the fundamental group is not solvable if $g > 0$, the genus is positive. So if Σ is a surface of positive genus, then the covering is hyperbolic space.

The isometry group of hyperbolic space can be checked to be $\mathrm{PSL}_2(\mathbb{R})$. It follows that to give a complex structure on a surface is the same thing as giving a homomorphism $\pi_1(\Sigma) \to \mathrm{PSL}_2(\mathbb{R})$. So the representation variety of Σ in $\mathrm{PSL}_2(\mathbb{R})$ is now the set of complex structures on a surface Σ. Well, almost. First, we have to switch from the representation variety to the *character variety.* Second, we have to look at reasonable homomorphisms only.

24.3 Theorem. *There is a component of the character variety which is biholomorphic to the Teichmuller space $T(\Sigma)$.*

This is supposed to be a loose sketch. Anyhow, this is how character varieties relate to topology.

Lecture 25
10/20

§1 Recap

Let us recall from last time that we had the following scenario.

$Z \subset Y \times \mathbb{P}^1$ was a closed codimension-one subvariety for Y an irreducible variety. $\pi : Z \to Y$ was the projection. We were interested in the size of the fibers of π. If $y \in Y$ is a "regular value," which meant that

1. y was smooth in Y.
2. Every preimage of y was smooth in Z
3. For each $z \in Z$, the map $D\pi : T_z(Z) \to T_y(Y)$ was an isomorphism of vector spaces.

Remark. This is a very good example of something called an **étale map.**

Then, we showed that

$$\boxed{|\pi^{-1}(y) = \deg \pi}.$$

We saw, moreover, that if you drop the assumption on $d\pi$ but keep the assumption on the smoothness, then either $|f^{-1}(y)|$ is infinite or $\left|f^{-1}(y)\right| \leq \deg \pi$. This was seen in the proof.

Remark. One important fact that we shall need is that the result is true if $\mathbb{P}^1$ is replaced by $\mathbb{P}^n$. This can be proved by induction on n.

§2 Intersections

Now we want to understand the intersections of a variety X of dimension d with linear subspaces of complementary dimension $n-d$. It is very useful that we have a parametrization of all of them. Let $\mathrm{Gr} = \mathrm{Gr}(n-d+1, n+1)$ be the Grassmannian. This variety parametrizes the d-dimensional planes in $\mathbb{P}^n$ (or $d+1$-dimensional planes in k^{n+1}).

Let $\Omega = \{(\Lambda, p) \in \mathrm{Gr} \times \mathbb{P}^n : p \in \Lambda\}$. This is the **"tautological"** plane bundle consisting of pairs of a point and a plane where the point is in the plane. Consider $Z = \mathrm{Gr} \times X \cap \Omega$. If Ω is the universal plane, then Z is the universal plane over X.

In particular, if $\pi_p : Z \to \mathrm{Gr}$ is the projection, then $\pi_p^{-1}(\Lambda) = X \cap \Lambda$. So these "universal" guys Z, Ω will be handy. Let us now say some more about Ω.

We have a projection

$$\pi_p : \Omega \to \mathrm{Gr}$$

which is onto, and whose fibers are projective $n-d$-planes. These fibers are all irreducible of the same dimension and the Grassmannian is irreducible. By a result proved earlier, we see that:

25.1 Proposition. *Ω is irreducible of dimension $d(n-d+1)+n-d$.*

Proof. Indeed, in the homework it was shown that the Grassmannian has dimension $d(n-d+1)$, and the fibers have dimension $n-d$. ▲

This is not that important. The next thing is important.

Moreover, Ω is homogeneous under an action of a certain group. Namely, $\mathrm{GL}_{n+1}(k)$ acts transitively on Ω by the natural action of this group on Ω. This action is given by isomorphisms of varieties (as one can easily check). Now there is at least one smooth point in Ω since the singular locus has proper codimension. Since Ω is homogeneous, all points look the same, and in particular must all be nonsingular:

We have now proved:

25.2 Proposition. *Ω is smooth.*

We now consider the other projection

$$\pi_2 : Z \to X.$$

This map is onto, because each point of X is contained in some $n-d$-plane. Let us consider $\pi_2^{-1}(x)$ for a given x. This is the set of all $n-d$-planes that pass through x. Alternatively, it is the set of all $n-d$ planes in a vector space of smaller dimension, i.e.

$$\mathrm{Gr}(n-d, n).$$

So all the fibers of π_2 are irreducible and have dimension $d(n-d)$ by the computation of the dimension of the Grassmannian.

By the usual result, we conclude:

25.3 Proposition. *Z is irreducible and of dimension $(n-d)d+d=(n-d+1)d$.*

This, however, is just the dimension of the Grassmannian. Let us now look at $\pi_1 : Z \to \mathrm{Gr}$; the two varieties have the same dimension. I claim that it is in fact onto. This states that every $n-d$-plane intersects X, which is true. In protective space, every two varieties of complementary dimension intersect.

So after these discussions, we find ourselves in a setting where we can apply the theorem (or more precisely, the modification with $\mathbb{P}^n$ replacing $\mathbb{P}^1$) from last time.

25.4 Proposition. *If a plane Λ intersects X transversely, then $|X \cap \Lambda| = \deg \pi_1$. (Here $\pi_1 : Z \to \mathrm{Gr}$ is the map above.)*

Proof. We need to check that if Λ intersects X transversely, then near Λ, the conditions of the theorem apply.

25.5 Lemma. *Under these hypotheses, Ω intersects $\Lambda \times \mathbb{P}^n$ transversely.*

We postpone the proof.

We know that Λ is transversal to X. (We can write this as $\Lambda \pitchfork X$.) We see that this implies that $\{\Lambda\} \times \Lambda \subset \mathrm{Gr} \times \mathbb{P}^n$ is transversal to $\mathrm{Gr} \times X$. This implies that the three varieties $\Omega, \mathrm{Gr} \times X, \Lambda \times \mathbb{P}^n$ intersect transversely by the next lemma, whose proof is omitted.

25.6 Lemma. *A, B, C intersect transversely if and only if $A \pitchfork B$ and $(A \cap B) \pitchfork C$.*

This means that $\Omega \pitchfork \mathrm{Gr} \times X$. However, this intersection must be smooth by transversality, and this intersection is Z. So Z is smooth. Also, $Z \pitchfork \{\Lambda\} \times \mathbb{P}^n$. This is the same as saying that Z has no tangent vectors pointing directly in the $\mathbb{P}^n$ direction. In particular, it states that $d\pi_1$ is an isomorphism.

We can now apply the theorem. It states that the size of the preimage of π_1, which is the number of intersections of Λ with X, is equal to $\pi_1^{-1}(X)$. ▲

We next need to show that there is at least one (and in fact a dense open subset) plane intersects X transversely. This is done by dimension considerations. The set of all planes that are tangent to X at some point is too small. This is easy, and we leave it to the reader.

Thus, this actually proves that the definition of degree is well-defined. In particular, there is an open dense subset of planes that intersect X in the same number of points. For every other plane, we have seen that $|\Lambda \cap X|$ is $\leq \deg \pi_1$ or ∞.

We should prove the lemma now, but I'm far too confused to see what's going on.

Lecture 26
10/22

Mainly, we are heading towards the proof of Bezout's theorem. Last time, we proved a special case.

§1 Recap

Last time, we looked at a projective variety X of dimension d, and we looked at the *universal* $n-d$ plane $\Omega = \{(\Lambda, v) \in \mathrm{Gr}(n-d+1, n+1) : v \in \Lambda\}$. We defined

$$Z = \Omega \cap \mathrm{Gr} \times X$$

. This had a first projection $\pi : Z \to \mathrm{Gr}$, and the fiber over the plane Λ was the intersection of X and Λ. We computed that $Z, \mathrm{Gr} = \mathrm{Gr}(n-d+1)$ had the same dimension, and that the projection

$$\pi : Z \twoheadrightarrow \mathrm{Gr}$$

was onto. In particular, there is a degree.

26.1 Definition. The **degree** of X is defined as $\deg \pi$.

The claim is that the generic $n-d$-plane intersects X with $\deg X$ points. The claim was that, in particular, if $\Lambda \pitchfork X$, then

$$|X \cap \Lambda| = \deg X.$$

We proved this modulo the following lemma:

26.2 Lemma. $\Omega \pitchfork \{\Lambda\} \times \mathbb{P}^n$ *for all* $\Lambda \in \mathrm{Gr}$.

Proof. Choose a basis $e_0, \ldots, e_n \in k^{n+1}$. Without loss of generality, $\Lambda = \mathrm{span}(e_0, \ldots, e_{n-d+1})$. Or, we can replace $(n-d+1, n)$ with $(d+1, n+1)$ for simplicity to make the notation easier. So we can then assume

$$\Lambda = \mathrm{span}(e_0, \ldots, e_d).$$

Then, as in the homework, locally Gr is identified with transformations $\mathrm{Hom}(k^{d+1}, k^{n-d})$ in the following way. A linear map $T : k^{d+1} \to k^{n-d}$ is identified with the $d+1$-space of points $(v, Tv), v \in k^{d+1}$. This parametrization is near Λ. This set of $d+1$-planes is such that the projection onto $\mathrm{span}(e_0, \ldots, e_d)$ is an isomorphism.

Near Λ, Ω is identified with pairs T, v where $v \in \mathbb{P}^d$ via

$$(T, v) \xrightarrow{f} (T(\{e_1, \ldots, e_d\}), (v, Tv)) \in \mathrm{Gr} \times \mathbb{P}^n.$$

The reason is that Ω consists of linear spaces and points in that linear space. The $T\{e_1, \ldots, e_d\}$ is the linear space. The (v, Tv) is the point in that linear space. (This gives another proof of nonsingularity.)

The tangent space at the point corresponding to T, e_0 is the image of the tangent space at (T, e_0). We need to describe the image of the tangent map. In other words, if we called it f, we want the image of Df. To find this, we start by perturbing (T, v) to $(T + \epsilon S, v + \epsilon u)$ (where $\epsilon \in k[\epsilon]/(\epsilon^2)$). Here $u \in \mathrm{span}\{e_1, \ldots, e_d\}$. We then look at the image of this via f and remember that $\epsilon^2 = 0$. In other words,

$$df|_{T,v}(Y, u) = \frac{f((T, v) + \epsilon(Y, u)) - f(T, v)}{\epsilon}.$$

The first coordinate is just going to be Y. On the second part, we get

$$\frac{((I|T + \epsilon Y)(v + \epsilon u) - (I|T)(v)}{\epsilon}$$

where $(I|X)$ denotes the matrix $v \to (v, Xv)$. When this is simplified, we find that this is $(0|Y)v + (I|T)u$. To compute the tangent space at $\Lambda \times \mathbb{P}^n$ at (Λ, v), this is just $\mathrm{span}\{e_1, \ldots, e_n\}$. Meaning, it is $\{0\} \times \mathrm{span}\{e_1, \ldots, e_n\}$.

This needs some editing and fixing—I'm only partially following.

The intersection is as follows. If

$$(Y, (0|Y)v + (I|T)u) \in 0 \times \mathrm{span}\{e_1, \ldots, e_d\}$$

then $Y = 0$. This consists of all vectors $(0, (I|T)u)$, which is d-dimensional. So you can compute that it is the correct codimension. In particular, it is $\dim \mathrm{Gr} \times \mathbb{P}^n - \dim \Omega - \dim \{\Lambda\} \times \mathbb{P}^n = d$. ▲

Back to the main story about intersections. We *still* don't know that there is a single plane that meets the projective variety X in $\deg X$ points. We know that if there is one which intersects transversally, then we have one.

So we need:

26.3 Lemma. *The set of all $n-d$-planes that nontransversely intersect X has proper codimension.*

Proof. For each point, you look at all planes that don't intersect X transversely. Then you show that it has codimension greater than d. Then you go over all points and use a fiber dimension argument.

We leave this to you. ▲

§2 Bezout theorem

We now prove the result.

26.4 Theorem (Bezout)**.** *Let $X, Y \subset \mathbb{P}^n$ be irreducible projective varieties and suppose $X \cap Y$ is transverse in an open dense set of points. Then*

$$\deg X \cap Y = \deg X \deg Y.$$

Proof. The **main point** is the following. If $\dim X + \dim Y = n$, then this hypotheses mean that $X \pitchfork Y$. In this case,

$$|X \cap Y| = \deg X \deg Y.$$

Let us first prove this statement. It is going to be a simple proof. We will define a variety and compute its dimension in two ways. It's a nice geometric construction that appears in other branches of mathematics.

26.5 Definition. If $X, Y \subset \mathbb{P}(V)$ for V an $n+1$-dimensional vector space, then the **join** of X, Y is the set $J(X,Y) \subset \mathbb{P}(V \times V)$ consisting of all lines passing through $X \times \{0\}$ and $\{0\} \times Y$.

So we take X, Y, and put them in complementary subspaces. Then we take all lines passing through a point in X and a point in Y. Let us state this differently.

Stated differently, let $C(X), C(Y) \subset V$ be the *affine cones* on X, Y. This means that $C(X), C(Y)$ are the vanishing loci of the homogeneous polynomials defining X, Y, but considered as zero loci in the affine space. Consider $C(X) \times C(Y) \subset V \times V$; this is invariant under scalar multiplication. The projectivization is the join.

Even more straightforwardly, you look at the polynomials defining X in variables $x_0, \dots, x_n$; you look at the polynomials defining Y in variables $y_0, \dots, y_n$. Then you look at these polynomials in $k[x_0, \dots, x_n, y_0, \dots, y_n$ as cutting out a zero locus in $\mathbb{P}^{2n+1}$.

In geometric combinatorics, you also have this notion when you take the join of simplicial complexes.

Anyway, back to the proof. Let's compute $\deg J(X,Y)$ in two ways.

1. $J(X,Y)$ has dimension $\dim X + \dim Y + 1$. This means that the codimension in $\mathbb{P}^{2n+1} = \mathbb{P}(V \oplus V)$ is n. We have to intersect this with an n-dimensional plane. Namely, we consider the *diagonal* $\Delta \subset \mathbb{P}(V \times V)$.

   What is $\Delta \cap J(X,Y)$? Well, it is easy to see (e.g. from the last description) that it is isomorphic to $X \cap Y$. I claim, moreover, that $\Delta \pitchfork J(X,Y)$. But we know that $X \pitchfork Y$, which implies by a dimension check that $C(X) \pitchfork C(Y)$ except at zero. However, if $C(X) \pitchfork C(Y)$, then the affinization $\Delta \pitchfork C(X) \times C(Y)$ except at zero. However, at projectivization, we throw away zero. We find

   $$\Delta \pitchfork J(X,Y).$$

   This shows that $\deg J(X,Y) = |X \cap Y|$.

2. Here is the second condition. Let Λ_X be a $n-d$-dimensional plane intersecting X transversely. Similarly, let Λ_Y intersect Y transversely. Let $\Lambda^* = J(\Lambda_X, \Lambda_Y)$. Then $\dim \Lambda^*$ has dimension $2n+1-\dim X - \dim Y = n+1$. This is *not* the intersect we want to intersect with. Anyhow, consider

   $$\Lambda^* \cap J(X,Y);$$

   this is the following. A point in the join gives a point in X and a point in Y (unless it lies in X or in Y). Then a point in $\Lambda^* \cap J(X,Y)$ should have the x-component in Λ_X and y-component in Λ_Y.

   So this intersection consists of all lines passing through a point in $X \cap \Lambda_X$ and a point in $Y \cap \Lambda_Y$. More generally, I claim that

   $$J(X,Y) \cap J(Z,W) = J(X \cap Z, Y \cap W).$$

   This is now easy to see.

   So we intersected $J(X,Y)$ with an $n+1$-dimensional space. We got the space of all lines passing through $X \cap \Lambda_X$ and $Y \cap \Lambda_Y$. If we choose a generic hyperplane, it will intersect this set of lines in precisely

   $$|X \cap \Lambda_X||Y \cap \Lambda_Y| = \deg X \deg Y$$

   points. So $J(X,Y)$ has degree $\deg X \deg Y$ points. This completes the proof.

We have now proved the special case of Bezout's theorem when the varieties are of complementary dimension. In general, fix X, Y, and let $Z = X \cap Y$. Then $\mathrm{codim} Z = \mathrm{codim} X + \mathrm{codim} Y := c$. Find a c-dimensional plane that intersects Z transversally. Now, if you look at everything that happens only in this plane, we reduce to the previous case. If this plane intersects only at points where X, Y intersects transversally, then X, Y, and the plane all intersect transversally. We find a plane Λ where $X \cap \Lambda, Y \cap \Lambda$ can be used to replace X, Y. Now we can use the previous version of Bezout's theorem to conclude that

$$\deg Z = |Z \cap \Lambda| = \deg X \cap \Lambda \deg Y \cap \Lambda.$$

But if $\Lambda \pitchfork X, Y$, then $\deg X = \deg X \cap \Lambda$. The reason is simply that to compute the degree, you just take the size of the intersection with an appropriate codimension subspace.[20] ▲

Lecture 27
10/25

Today, we will deviate a little from the generality of algebraically closed fields, and focus on $\mathbb{C}$. We want to talk about things that we can prove using the topology of $\mathbb{C}$.

§1 A topological proof of Bezout (over $\mathbb{C}$)

We will use singular cohomology. Cohomology is actually a theory of intersections, thanks to the cup product.

We start by computing the *homology.*

27.1 Lemma. *$H_k(\mathbb{CP}^n) = 0$ if k is odd or $k > 2n$. In even degrees between 0 and $2n$, we have $H_k(\mathbb{CP}^n) = \mathbb{Z}$.*

Proof. The way you prove this lemma is to note how $\mathbb{CP}^n$ is built. $\mathbb{CP}^n$ is built as $S^{2n} \cup S^{2n-2} \cup S^{2n-4} \cup \dots$. So to build it, you start with a point and add strata of dimension two greater. When you use cellular homology, this is what you get. ▲

If $X \subset \mathbb{CP}^n$ is a smooth subvariety of (algebraic) dimension k, then it is an oriented $2k$-dimensional manifold (with a preferred orientation). The orientation is as follows. Choose complex local coordinates $z_1, \dots, z_k$ of X. We can write $z_j = x_j + iy_j$. The orientation is given by

$$dx_1 \wedge dy_1 \wedge dx_2 \wedge dy_2 \wedge \cdots \wedge \cdots \wedge dx_k \wedge dy_k.$$

You have to check that any complex change of coordinates preserves the orientation. But the derivative of a holomorphic map has positive determinant, because it is just a composite of rescaling and rotation. This proves the claim.

So this orientation in $H_{2k}(X)$ gives by the push-forward $H_{2k}(X) \to H_{2k}(\mathbb{CP}^n)$ an element $[X] \in H_{2k}(\mathbb{CP}^n)$. Note that $[\mathbb{CP}^k]$ is a generator of $H_{2k}(\mathbb{CP}^n)$, by cellular homology.

In general, if X has algebraic dimension k, the class $[X] \in H_{2k}(\mathbb{CP}^n)$ is given by some multiple d_X of the class of $[\mathbb{CP}^k]$.

27.2 Proposition. *$d_X = \deg X$.*

We will prove something more:

More generally, suppose $X, Y \subset \mathbb{CP}^n$ have dimensions a, b. Suppose that $X \pitchfork Y$. Then the Poincaré dual $PD([X])$ of $[X]$ is in $H^{2n-2a}(\mathbb{CP}^n)$. Similarly $PD([Y]) \in H^{2n-2b}(\mathbb{CP}^n)$, and $PD([X \cap Y]) \in H^{4n-2a-2b}(\mathbb{CP}^n)$.

Then:

[20] To compute $\deg X \cap \Lambda$, just choose a plane of codim$X$ dimension containing X intersecting X transversely.

27.3 Proposition. $PD([X \cap Y]) = PD([X]) \cup PD([Y])$.

In particular,

$$PD([X \cap Y]) = d_X d_Y PD([\mathbb{CP}^a]) \cup PD(\mathbb{CP}^b) = d_X d_Y PD([\mathbb{CP}^a \cap \mathbb{CP}^b]).$$

Here the copies of $\mathbb{CP}^a, \mathbb{CP}^b$ are chosen to be transversal. Their intersection is a projective space $\mathbb{CP}^{n-a-b}$, and it follows by Poincaré duality again that

$$\boxed{d_X d_Y = d_X d_Y}$$

This is Bezout's theorem.

§2 A computation

We have the **Segre embedding** $S : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{nm+n+m}$. Let us compute the degree of the image.

The image is the (projectivized) set of all $n+1$-by-$m+1$ matrices of rank 1. The question is if you take a general $m+n$ plane and intersect it with this set of all matrices, how many will have rank one?

Let $h \in H^2(\mathbb{CP}^{nm+m+n})$ be the generator. It is the Poincaré dual of a hyperplane by the (unproved) results of the previous section. Let us compute its pull-back $S^*(h) \in H^2(\mathbb{CP}^n \times \mathbb{CP}^m)$. (Cohomology is nice here because it is contravariant.)

By Kunneth, the second cohomology of $\mathbb{CP}^n \times \mathbb{CP}^m$ is

$$H^2(\mathbb{CP}^n) \otimes H^0(\mathbb{CP}^m) \oplus H^0(\mathbb{CP}^n) \otimes H^2(\mathbb{CP}^m)$$

since the cohomology in degree one vanishes. So we need to compute a piece of $S^*(h)$ in $\mathbb{CP}^n$ and $S^*(h)$ in $\mathbb{CP}^m$.

$S^*(h)$ is the restriction of h to the copy of $\mathbb{CP}^n \times \mathbb{CP}^m$. The projection of $S^*(h)$ to $H^2(\mathbb{CP}^n)$ is again given by a restriction. The Kunneth theorem states that the projection of $S^*(h)$ to $H^2(\mathbb{CP}^n) = H^2(\mathbb{CP}^n) \times H^0(\mathbb{CP}^m)$ is given by first restricting h to $\mathbb{CP}^n \times \mathbb{CP}^m$ and then restricting further to $\mathbb{CP}^n \times *$ for $* \in \mathbb{CP}^m$ a point.

However, $S(\mathbb{CP}^n \times *)$ is just a linear embedding of $\mathbb{CP}^n$ in $\mathbb{CP}^{n+m+nm}$. So $S^*(h) \in H^2(\mathbb{CP}^n \times \mathbb{CP}^m) = H^2(\mathbb{CP}^n) \oplus H^2(\mathbb{CP}^m)$ is obtained by restricting h to the two planes. We can write

$$S^* h = (h_{\mathbb{P}^n}, h_{\mathbb{P}^m})$$

where $h_{\mathbb{P}^n} \in H^2(\mathbb{CP}^n)$ is the Poincaré dual of a hyperplane in $\mathbb{P}^n$.

Now let us compute the degree. $S(\mathbb{P}^n \times \mathbb{P}^m)$ is $n+m$-dimensional. We need to intersect this variety with a plane of complementary dimension $nm+n+m-(m+n)$ or dimension mn. This we can do in cohomology.

$$\deg S(\mathbb{P}^n \times \mathbb{P}^m) = PD([S(\mathbb{P}^n \times \mathbb{P}^m)]) \cup PD([\mathbb{CP}^{nm}]).$$

However, $[\mathbb{CP}^{nm}]$ is the cup product of h with itself $n+m$ times with itself. When we pull back by S, we get

$$< [\mathbb{P}^n \times \mathbb{P}^m], S^*(h)^{\cup(n+m)} >_{\mathbb{P}^n \times \mathbb{P}^m} .$$

Here $S^*(h)$ is a sum of two elements $h_{\mathbb{P}^n}, h_{\mathbb{P}^m}$. When we cup product them to the $n+m$, we get

$$(h_{\mathbb{P}^n} + h_{\mathbb{P}^m})^{n+m} = \binom{m+n}{n} h^n_{\mathbb{P}^n} h^m_{\mathbb{P}^m}.$$

So when we take the pairing, we find that:

27.4 Proposition. *The degree of the Segre embedding is* $\binom{m+n}{n}$.

§3 Example

Here is another example that computes the degree. Consider the Segre embedding

$$\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3.$$

Take a curve C in $\mathbb{P}^1 \times \mathbb{P}^1$. It has actually two degrees—the degree in which it's homogeneous in the first part, and in the second part. Say it is homogeneous of bidegree a, b. What is the degree of $S(C) \subset \mathbb{P}^3$?

We'll do this algebraically. We need to intersect C with something. Choose the tangent plane to the Segre embedding at another point. Let $p = [1\ 0\ 0\ 0] \in S(\mathbb{P}^1 \times \mathbb{P}^1)$. Near this point, we can use affine coordinates (y, z, w) where the curve has the equation $w = yz$. The tangent space at the point $(0,0,0) = [1000]$ is just $w = 0$. But this is because $\nabla(w - yz)_{(0,0,0)} = (0,0,1)$.

Let T be the tangent space. So the intersection $T \cap S(\mathbb{P}^1 \times \mathbb{P}^1)$ consists of two lines. These lines are of the form $S(\mathbb{P}^1 \times *), S(* \times \mathbb{P}^1)$. In particular, for each point, you get a pair of lines; as you go over all the points in the Segre embedding, you get a family of pairs of lines.

Choose $p \notin C$ such that the intersection of $T_p(S(\mathbb{P}^n \times \mathbb{P}^m)) \cap S(\mathbb{P}^n \times \mathbb{P}^m)$ consists of two lines such that one of them is horizontal (i.e. depends only on the first coordinate) and intersects the curve in a points, and the other is vertical and intersects the curve in b points. Then $T_p(S(\mathbb{P}^1 \times \mathbb{P}^1)) \cap S(C)$ is transverse and has $a+b$ points. So the degree is $a+b$.

Reference: Griffiths and Harris, Principles of Algebraic Geometry.

Lecture 28
10/27

We shall now talk about differential forms.

§1 Differential forms

Let X be a smooth variety. Given $f \in k[X]$ and $x \in X$, we can consider

28.1 Definition. $df|_x$ is the linear function (∇f) from the tangent space at x, $T_x(X)$, into the affine line k, which is the derivative of f. This does not depend on the representative in the polynomial ring used. So $df|_x \in (T_x(X))^*$.

We can say it another way. Since $T_x(X)^* = \mathfrak{m}_x/\mathfrak{m}_x^2$, then df is the image of $f - f(x)$ in $\mathfrak{m}/\mathfrak{m}_x^2$.

28.2 Definition. A **regular differential 1-form** on a smooth variety X is a function $\omega : X \to \bigcup T_x(X)^*$ s.t. for any $x \in X$, there is a (Zariski) neighborhood U containing x and a regular functions $f_i, g_i \in k[U]$ s.t.

$$\omega|_U = \sum_i f_i dg_i.$$

It's not clear even what the regular forms on $\mathbb{A}^1$ are.

28.3 Proposition. *Let X be nonsingular of dim n, and suppose that $u_1, \ldots, u_n$ are regular fns on X which are loc. coordinates at every point (i.e. $\nabla u_i(x)$ linearly independent).*[21]

Then any regular differential 1-form ω on X can be written uniquely as

$$\omega = \sum f_i du_i, \quad f_i \in k[X].$$

This is a global representation of ω.

I.e. the 1-forms are a free rank n module over $k[X]$.

28.4 Definition. The 1-forms on X is called $\Omega^1(X)$.

Remark. Not agreeing with Shafarevich's notation here.

Proof. Since du_i is a basis at each x of $T_x(X)^*$, we can always get such a representation locally via some f_i (not necessarily regular a priori). We can piece them together because the du_i are linearly independent. Uniqueness is also obvious.

We need to show that if $\omega = \sum f_i du_i$ is regular, the f_i are regular. It's enough to assume $X \subset \mathbb{A}^n$ affine for this. Letting t_k be the coordinate fns, we have $\omega = \sum g_k dt_k$ in some smaller nbd for g_k regular. Now from this transfer the dt_k into the du_i as these form a basis, in a regular fashion. Or something like that. ▲

Remark. Two reasons these notes are so short: I'm reducing note-taking to save my hands, and there was a fire alarm.

28.5 Definition. The same can be done for higher rank. A **differential r-form** is a fn $X \to \cup \wedge^r T_x(X)^*$ such that locally it is of the form $\sum f_i dg_{i_1} \wedge \cdots \wedge dg_{i_k}$. We denote this space by $\Omega^r(X)$.

The above proposition, with almost the same proof.

28.6 Proposition. *If X has local coordinates $u_1, \ldots, u_n$ everywhere, $\Omega^r(X)$ is $k[X]$-free on $du_{i_1} \wedge \cdots \wedge du_{i_r}, i_1 < \cdots < i_r$. The rank is thus $\binom{n}{r}$.*

[21] Always this can be done locally—if something is loc. coordinates at x, they will be loc. coordinates in a nbd.

Lecture 29
10/29

Lecture 30
11/1

Last time, we were talking about differential p-forms. I did not livetex that part of the lecture.

§1 More on differential forms

We said last time

30.1 Proposition. *If X, Y smooth projective, $\phi : X \dashrightarrow Y$ a dominant rational map, $\omega \in \Omega^r(Y)$, then the pullback $\phi^*(\omega)$ can be extended to $\Omega^r(X)$.*

Proof. Follows from:

1. Locus of indeterminancy of a rational map is codimension ≥ 2 (because X smooth, Y projective).
2. $\phi^*\omega$ is locally a map to a map to $\mathbb{A}^n$. The problems of ω not being defined are in codimension one; these are the "poles" of the various components. Thus $\phi^*\omega$ can be extended to all of X, since the set where it isn't defined is codimension ≥ 2. (Recall what we said about functions $\mathbb{A}^2 - (0,0) \to k$ being extendable to $\mathbb{A}^2$.)

▲

We used:

30.2 Lemma. *If X is smooth (or even just normal), $f : X \dashrightarrow \mathbb{A}^1$ rational and regular on $X - Z$ for* codim$Z \geq 2$, *then f extends to X.*

30.3 Corollary. *$\Omega^r(X)$ is a birational invariant of a smooth projective variety.*

Here is a big theorem:

30.4 Theorem. *If X is proj and smooth, then*

$$\dim_k \Omega^{\dim X}(X) < \infty.$$

(More generally, we *don't* have to restrict to top forms. This follows more generally from the hard theorem that push-forwards of a coherent sheaf by a proper morphism are coherent, or that cohomology of a coherent sheaf on $\mathbb{P}^n_k$ is finite-dimensional.)

30.5 Definition. The **genus** of X (smooth proj. variety) is $\dim_k \Omega^{\dim X}(X)$. It is a birational invariant.

30.6 Example. The genus of $\mathbb{P}^1$ is zero (no nontrivial 1-forms).

30.7 Example. The genus of a smooth projective cubic $y^2 = x^3 + Ax + B$ is ≥ 1 because of the global nonzero differential dx/y. The genus is actually one.

We will slowly prove this hard theorem. We work more generally in the context of line bundles. $\Omega^{\dim X}$ is a **line bundle**. I.e., locally a free module of rank one over the regular functions. This is too abstract, though, you can't do anything with it.

30.8 Definition. In general, a **line bundle** on X is given by

1. A cover of X by open sets U_i
2. For each i, j a regular fn $f_{ij} \in k[U_i \cap U_j]$. These satisfy

$$f_{i,i} = 1, \quad f_{i,j} f_{j,k} = f_{i,k} \in k[U_i \cap U_j \cap U_k] \text{ (cocyclecondition).}$$

   These are the *changes of coordinates* between U_i and U_j.

30.9 Example. The top forms on a smooth variety are a line bundle. Locally, they are just a function times some $dx_1 \wedge \cdots \wedge dx_d$ where $x_1 \ldots x_d$ are local coordinates. The change of coordinates are defined by Jacobians of different local coordinates $x_1 \ldots x_d, x'_1 \ldots x'_d$.

Suppose X irr. In order to get a more compact presentation of a line bundle, fix i and define $g_\alpha = f_{\alpha,i}$, a rational fn on U_α. This is called a **Cartier divisor**.

30.10 Definition. A **Cartier divisor** is a tuple $(\{U_\alpha\}, \{g_\alpha\})$ consisting of a cover U_α together with rational functions $g_\alpha \in k(U_\alpha)$ such that g_α / g_β is a unit in $k[U_\alpha \cap U_\beta]$.

Now we have to talk about poles and zeros. I.e., **divisors** (in a new way). First,

30.11 Definition. A **Weil divisor** on an irr variety X is a formal sum $\sum c_i Z_i, c_i \in \mathbb{Z}$ where the Z_i are irreducible subvarieties of codimension one.

Lecture 31
11/3

Again, we are trying to prove that the space of global differential forms on a smooth projective variety is finite-dimensional. This turns out to be isomorphic to the question of how many rational functions exist that have specified poles and zeros. This we will show is finite, by induction.

31.1 Definition. X a variety. A **Weil divisor** is a formal finite integer combination of irreducible closed subvarieties of codimension one. So the free abelian grp on these subvarieties. The set of divisors is denoted $\mathrm{Div}(X)$; it is a group.

31.2 Definition. A Weil divisor $D = \sum d_i [C_i]$ (the C_i subvarieties, d_i integers) is called **effective** if $d_i \geq 0$.

31.3 Definition. Assume that X is smooth. Let $f \in k(X)$ and $C \subset X$ closed irreducible of codimension 1. Pick $x \in C$. Now $k[X]_x$ is factorial. In a neighborhood of this point, f is equal to a product of functions $\prod f_i^{k_i}$ where the $f_i \in k[X]_x$ irreducible, $k_i \in \mathbb{Z}$. Also, near x, C is defined by a single irreducible element F_C of $k[X]_x$.

We define the C-**multiplicity** of f at x to be k_i if F_C is associated to some f_i and 0 otherwise. Call this $v_C^x(f)$.

31.4 Lemma. *This does not depend on x.*

Proof. You find a neighborhood of x in C where the multiplicities are the same. Thus the multiplicity is locally constant, hence constant. ▲

As a result, we can simply write $v_C(f)$. We thus have a notion of *multiplicity* along a subvariety.

Remark. For any f, there is a nbhd U_x such that if C is any codimension one subvariety that intersects U_x, then $v_C(f) \neq 0$ if and only if C is one of finitely many subvarieties. It follows that, for any f, there are **finitely many** C with $v_C(f) \neq 0$.

31.5 Definition. The **divisor** of $f \in k(X)$ is $\mathrm{Div}(f) = \sum v_C(f)[C]$.

31.6 Definition. A divisor is **principal** if it is $\mathrm{Div}(f)$ for some f.

Remark. $\mathrm{Div}(fg) = \mathrm{Div}(f) + \mathrm{Div}(g)$ as the same is true for multiplicities.

31.7 Lemma. *(X smooth)* $\mathrm{Div}(f)$ *is effective iff f is regular.*

(On a projective variety, this means f constant.)

Proof. If f regular, obviously $\mathrm{Div}(f) \geq 0$. The other side is also clear. If $\mathrm{Div}(f) \geq 0$, then for each x, we can write in the quotient field of the local ring $k[X]_x$ $f = \prod f_i^{k_i}$ where the $f_i \in k[X]_x$ irred, $k_i \in \mathbb{Z}$. Effectivity means that all $k_i \geq 0$. So $f \in k[X]_x$. x being arbitrary, f is everywhere regular. ▲

31.8 Definition. The **class group** of X is $\mathrm{Cl}(X) = \mathrm{Div}(X)/\text{principal divisors}$.

31.9 Example. Let's compute $\mathrm{Cl}(\mathbb{P}^n)$. A divisor is given by a sum of codim one subvarieties, i.e. of hypersurfaces. Recall that hypersurfaces are *precisely* codimension one subvarieties of $\mathbb{P}^n$. So X is defined by the vanishing of some homogeneous $F(x_1, \dots, x_n) = 0$, say of degree d. This doesn't say that X is principal as F is not a rational function on $\mathbb{P}^n$. Now F/x_1^d *is* a rational function of degree d. So X is in the same equivalence class as d times the hyperplane $\{x : x_1 = 0\}$. Thus this hyperplane generates $\mathrm{Cl}(\mathbb{P}^n)$. We also get a map $\mathrm{Div}(\mathbb{P}^n) \to \mathbb{Z}$ taking a generator to its degree, which factors through $\mathrm{Cl}(\mathbb{P}^n)$. So

$$\mathrm{Cl}(\mathbb{P}^n) = \mathbb{Z}.$$

Similarly, $\mathrm{Cl}(\mathbb{P}^n \times \mathbb{P}^m) = \mathbb{Z} \oplus \mathbb{Z}$ since one can attach two degrees to a hypersurface.

Remark. Often, the class group can be given the structure of a finite-dimensional algebraic variety times some discrete set.

Remark. You can do this more generally for $X \subset \mathbb{P}^n$ to get a map $\text{Div}(X) \to \mathbb{Z}$ sending C to $\deg C$. The total degree of a divisor of a rational function on $\mathbb{P}^n$ is zero. This map really depends on the embedding of X in $\mathbb{P}^n$, as this will affect the degree.

Assume X is smooth. Then **Weil divisors** and **Cartier divisors** turn out to be equivalent. Let $D = \sum a_i[C_i]$ be a Weil divisor. If U open, we can restrict D to U—$\sum a_i[C_i \cap U]$. For $x \in X$, there is a small enough neighborhood U_x such that everything is given by a local equation f. That is, $D|_{U_x}$ is principal, thus the divisor of some $f \in k(U_x)$. We can put these f's together to get a Cartier divisor, since the quotients of any two will be a unit, as any two will define the same Weil divisor on the intersection of the open sets. So we get a map from Weil divisors to Cartier divisors. You can go the other way around as well.

Lecture 32
11/8

Last time, we talked about the canonical divisor and differentials.

32.1 Proposition. *If D is a divisor on a smooth X, and $x_1, \dots, x_n \in X$, then D is linearly equivalent to another divisor that passes through no x_i.*

(Weil and Cartier divisors are equivalent.)

Proof. Wlog, D a prime divisor, and X is affine. (Given a finite set of pts, there is an affine containing all of them.)

Induct on n.

Suppose $n = 1$. Say D passes through x_1. By smoothness, there is a local equation f for D near x_1. Then $E = D - \text{Div}(f)$ doesn't pass through x_1. E does the job.

Now let $n > 1$. Still assume D a prime divisor. By induction, we can assume that $x_1, \dots, x_{n-1} \notin \text{supp}D$ and $x_n \in \text{supp}D$. Choose a loc equation f of D near x_n. Locally, $f = a/b$ for $b(x_n) \neq 0$ and $a(x_n) = 0$, $a, b \in k[X]$. By multiplying f by a suitable regular function, assume that f is regular on X and still is a local equation near x_n. If we change D by $\text{Div}(f)$, it might happen that x_1 might become a zero or pole. So we need to be trickier.

By induction, $x_i \notin \text{supp}D$. Choose $g_i \in k[X]$ s.t. $g_i(D) = 0$ and $g_i(x_j) = 0$, $j \neq i$, but $g_i(x_i) \neq 0$. We are going to change D by the divisor of

$$h = f + \sum \alpha_i g_i^2, \quad \alpha_i \in k$$

where the α_i are taken so that $h(x_i) \neq 0$, $i < n$. Let $E = D - \text{Div}(h)$. Now D did not pass through $x_i, i < n$; thus E does not. Near x_n, f is a local equation and the g_i's are squared, so h is a local equation for D. So E doesn't pass through x_n. ▲

This says that

$$k(X) \to \prod_{C \subset X \text{ codim } 1} \mathbb{Z}$$

has image *dense* in the Tychonov topology.

32.2 Definition. Suppose $f : X \to Y$ regular. Let $D \subset Y$ a divisor. There is an equiv $E \sim D$ s.t. $f(X) \not\subset \text{supp}E$. Then we can pull back E to X. This leads to a map from the class group of Y to the class group of X.

32.3 Definition. Suppose D a div on X (smooth). The **linear system** corresponding to this divisor is the set of all rational functions $f \in k(X)$ such that

$$\text{Div}(f) + D \geq 0 \text{ or } f = 0.$$

This is denoted $\mathcal{L}(D)$—the Riemann-Roch space.

32.4 Example. $X = \mathbb{P}^1$, $D = n[\infty]$. So we are looking at rational functions that have a pole at most of order n at infinity, and no pole anywhere else. So that is, polynomials of degree $\leq n$.

32.5 Example. Let K be the canonical class on X. Then $\mathcal{L}(K)$ is the space of global top forms. Or $\Omega^n(X), n = \dim X$.

32.6 Proposition. *$\mathcal{L}(D)$ depends (up to isomorphism) only on the class of D.*

32.7 Theorem. *If X a smooth (irred) projective curve and D any divisor, then $\mathcal{L}(D)$ finite-dimensional.*

Proof. Enough to prove this for effective divisors $D \geq 0$. If $D \leq E$, then $\mathcal{L}(E) \supset \mathcal{L}(D)$. Now prove this by induction.

1. For the zero divisor, clear—no nonconstant regular fns.
2. Say $D = m[x] + \dots$. Choose a local coordinate t near x. If $f \in \mathcal{L}(D)$. Then ft^m is regular at x. Define $\mathcal{L}(D) \to k$ sending $f \to (ft^m)(x)$. The kernel of this map is $\mathcal{L}((m-1)[x] + \dots)$. So we have an exact sequence

$$\mathcal{L}((m-1)[x] + \dots) \to \mathcal{L}(D) \to k$$

which implies that $\mathcal{L}(D)$ is f.d.

▲

Remark. We showed in fact that $\dim \mathcal{L}(D) \leq \deg D + 1$ for an effective divisor.

Remark. This is the beginning of cohomology.

Question. What is the cokernel of $\mathcal{L}(D - [x]) \to \mathcal{L}(D)$? This is related to cohomology. There is a long exact sequence

$$0 \to \mathcal{L}(D - [x]) \to \mathcal{L}(D) \to k \to H^1(\mathcal{L}(D - [x]) \to H^1(\mathcal{L}(D)) \to 0.$$

The H^1 are f.d. as well. From this, one can show that

$$\dim \mathcal{L}(D) \geq \chi(0) + \deg D$$

where $\chi(0)$ is the *Euler characteristic* of the trivial bundle.

Lecture 33
11/10

§1 A Weil divisor which isn't a Cartier divisor

We are going back to an example done earlier of a Weil divisor on a cone which isn't locally principal. We can define the cone by $V(xy - z^2)$. Let us consider the divisor Y given by the line $y = 0$. Set-theoretically this is the x-axis. Now the divisor of y is some *multiple* of $[Y]$. In fact, we find that $\mathrm{Div}(y) = 2[Y]$. But Y is nontrivial, and is not a Cartier divisor. That is, there no function that generates the ideal of vanishing of Y locally. We omit the details.

We *will* show that $[Y]$ generates the class group.

33.1 Proposition. $[Y]$ *generates the class group of the cone. In particular, the cone has as class group* $\mathbb{Z}/2$*.*

This will follow from the next result as $\mathrm{Cl}(V(xy-z^2)-Y) = 0$. Indeed, this variety has as ring of regular functions

$$(k[x, y, z]/(xy - z^2))_y = k[y, z]_y.$$

Indeed the cone minus a line is the product of a line and a line minus a point. That has trivial class group.

33.2 Proposition. *If* X *is smooth in codimension one and irreducible and* $Y \subset X$ *is a proper irred., codim one, subvariety, then there is a map* $\mathrm{Cl}(X) \to \mathrm{Cl}(X - Y)$ *(coming from* $[T] \to [T - T \cap Y]$*) whose kernel is generated by* $[Y]$*.*

That is, there is an exact sequence

$$\mathbb{Z} \to \mathrm{Cl}(X) \to \mathrm{Cl}(X - Y) \to 0.$$

If Y has codim ≥ 2, the restriction map is an isomorphism in fact.

33.3 Example. $\mathrm{Cl}(\mathbb{A}^2 - \mathbb{A}^1)$ is trivial. $\mathrm{Cl}(\mathbb{P}^2 - V) = \mathbb{Z}/d\mathbb{Z}$ for d the degree of V.

33.4 Theorem. *If the singular locus has codimension* ≥ 2*,* $\mathrm{Cl}(X \times \mathbb{A}^1) = \mathrm{Cl}(X)$*.*

Proof. Wlog, X smooth. There is a map $\mathrm{Div}(X) \to \mathrm{Div}(X \times \mathbb{A}^1)$ sending a prime divisor D to $D \times \mathbb{A}^1$. This is the *pull-back* under projection. There is a map

$$\mathrm{Cl}(X) \to \mathrm{Cl}(X \times \mathbb{A}^1).$$

Injectivity: We must show that if $D \times \mathbb{A}^1 = \mathrm{Div}(f)$ for $f \in k(X \times \mathbb{A}^1) = k(X)(t)$, then D is principal itself. I claim now that $f \in k(X)$ itself. This will give us the claim. Suppose not. Then $f = \frac{g(t)}{h(t)}$ where g, h are relatively prime polynomials in $k(X)[t]$. If $h \notin K$, then its divisor $\mathrm{Div}(h)$ will have points an open set on X. We can take the open dense set of X where all the coefficients of h are defined and nonzero. Over this open set, $\mathrm{Div}(h)$ will have some root in t. Thus $\mathrm{Div}(h)$ must have things that are not of the form $D \times \mathbb{A}^1$ because any such $D \subset X$ is non-dense. This is a contradiction.

Surjectivity: We want to show that any divisor is equivalent to a divisor that does not dominate X. Let E be a prime divisor on $X \times \mathbb{A}^1$. Choose $U \subset X$ such that E is defined by a single equation f on $U \times \mathbb{A}^1$. We can think about this as a rational function on $U \times \mathbb{A}^1$ and then $E - \mathrm{Div}(f)$ has support lying in $(X - U) \times \mathbb{A}^1$. This must then come from something in $\mathrm{Div}(X)$. (Indeed, choose some x, and find a local equation in $k[X]_x[t]$—this is a UFD, so there is a local equation in this ring.) ▲

Lecture 34
11/12

We started to talk about the linear space attached to a divisor. Let us start talking about irreducible smooth projective *curves*. Given a div D, then $\mathcal{L}(D)$ is the set of all rational functions such that

$$\mathrm{Div}(f) + D \geq 0.$$

(And also $0 \in \mathcal{L}(D)$.)

So when D has a positive coefficient at a point, then f can have a pole of at most that order at the point.

We showed

$$\dim \mathcal{L}(D) < \infty,$$

in fact, if D is effective, then

$$\dim \mathcal{L}(D) \leq \deg D + 1.$$

For instance, if $X = \mathbb{P}^1$, then any divisor is linearly equivalent to $n[\infty]$ for some $n \in \mathbb{Z}$ and $\mathcal{L}(D)$ is a space of polynomials of degree $\leq n$, of dimension $n+1$. This characterizes the projective line.

34.1 Proposition. *Let X be a smooth proj curve and $\dim \mathcal{L}([x]) = 2$ for $x \in X$ a point. Then $X \sim \mathbb{P}^1$.*

Proof. There is a nonconstant rational function f with a pole of degree ≤ 1 at x and no other poles. There can't not be a pole or f would be constant. So $v_x(f) = 1$. Now f becomes a map $f : X \dashrightarrow \mathbb{P}^1$ which extends to $f : X \to \mathbb{P}^1$ regular. The image is onto. So this means that ∞ is a regular value of $f : X \to \mathbb{P}^1$. So $\deg f = |f^{-1}(\infty) = 1$, so f is birational and hence an isomorphism. ▲

34.2 Example. A nonsingular cubic. $X \subset \mathbb{P}^2$ is a nonsingular cubic, say $y^2 = x^3 + Ax + B$ projectivized.

Claim: if $x, y \in X$ are different points, then the divisors $[x], [y]$ are not equivalent. If $[x] - [y] = \mathrm{Div}(f)$, then f would have a simple pole and a simple zero, and then X would be $\mathbb{P}^1$, but X has a nontrivial differential form, so this is silly.

Claim: every divisor of degree one is equivalent to some $[x]$.

Proof. Use the pt $x_0 = [0, 1, 0]$ at "infinity." The tangent line to x_0 intersects X with multiplicity three. So $3[x_0]$ is principal. Take $x, y \in X$. Consider the line through x, y

intersects X in a third point z by Bezout. Then if F the eqn of this line, G the eqn of the line at ∞, we get

$$\mathrm{Div}\frac{F}{G} = [x] + [y] + [z] - 3[x_0].$$

So

$$([x] - [x_0]) + ([y] - [x_0]) \sim [x_0] - [z]$$

And using this, we can reduce any divisor down piece by piece. (I have not written down the rest.) This trick is specific to cubic curves. Anyway, in total, one can get a bijection

$$\mathrm{Cl}(X) = \mathbb{Z} \times X.$$

. Here this means that X is also a group, and we get the **group law** on an **elliptic curve.** Moreover, we find that the part of the class group of degree zero is X, so is a variety. This is true in much more generality.

▲

Lecture 35 11/15

Last time, talked about nonsingular cubic. Showed that any divisor on this takes the form $[X] + n[X_0]$ for X_0 fixed. Let us compute $\mathcal{L}(D)$ for some D. We show that if $D > 0$:

$$\dim \mathcal{L}(D) = \deg D.$$

Enough to prove for $X = n[X_0]+[X]$. For $n = 0$, we know that there are only constants that have poles only at $[X]$ of rank one, or X would be $\mathbb{P}^1$. So $n = 0$ is good. It follows that $\dim \mathcal{L}(D) \leq \deg D$ by induction. Must prove that each time the degree raised, a new fn appears. I.e. for each n, there is a rational f whose order at x_0 is n and whose order at X is ≤ 1. Then degree clearly goes up by one.

Let us now check $n = 1$. Let f be a linear form vanishing at X, X_0, y. Let g be nonzero linear frm vanishing at y at not at X, X_0. Then g/f is rat'nl and in $\mathcal{L}([X] + [X_0])$.

Let F have a triple pole at X_0 (tangent line at infinity) and G be linear form not vanishing at X_0. Then G/F has a triple pole at X_0, nowhere else. If want fn with double pole, take same F, and take G to be a fn vanishing simply on X_0. Then G/F will do. Products of these will give fns with arbitrary poles on X_0 and nowhere else.

35.1 Lemma. *Let X be smooth proj curve, choose n pts $x_1, \ldots, x_n \in X$. Let R be the ring of rat'nl fns regular at those pts. Then R is PID, with n max'l ideals.*

Proof. Choose loc coordinates $t_i \in k(X)$ at x_i. Then $\mathrm{Div}(t_i) = [x_i] + D_i$, $x_i \notin D_i$. We can move the support outside the other x_i. There is a fn f_i such that $x_j \notin f_i D_i, \forall j$. Then $f_i t_i$ is loc coordinate at x_i that doesn't vanish at the others. So the (t_i) generate max'l ideals in this ring, and they are the only ones. (Any $f = t_1^{a_1} \ldots t_n^{a_n} u$ where u has no zeros at these pts and is thus invertible.) ▲

35.2 Proposition. *Let X be smooth proj curve, let $f \in k(X)$ be nonconstant. Denote $Z = \mathrm{Div}_\infty(f)$ (only poles of f). Then* $\deg f = \deg D$. *Also, $\exists c$ such that for any t,*

$$\dim \mathcal{L}(tZ) \geq t \deg Z - c.$$

So bound below growth of $\mathcal{L}$ for specific divisors.

Proof. $m = \deg Z$, $n = \deg f, S = \mathrm{supp} Z, n_P = v_P(f)$. $\exists f_1, \dots, f_m \in k(X)$ with poles of order $\leq n_P$ for each $P \in S$ and for every $g \in k(X)$ s.t. the same,

$$v_P(g) \geq -n_P, \forall P \in S,$$

there is a k-linear combination s.t. $g - \sum \lambda_i f_i$ regular at all $P \in S$, $\lambda_i \in k$. **The claim is that the f_i are lin indep over $k(f)$. If there were a dependence the poles would get screwed up.**

It is clear that the dim of vector spc $V \subset k(X)$ spanned by the f_i is $\deg Z$. (This is the set of fns $g \in k(X)$ s.t. $\forall p \in S$, we have $v_P(g) \geq v_P(f)$.) Consequently $\deg Z \leq [k(X) : k(f)]$.

Let $g_1, \dots, g_n$ be basis for $k(X)/k(f)$ as vec spc. Wlog the g_i integral over $k(f)$. So each g_i satisfies an eqn

$$g_i^M + a_1(f) g_i^{M-1} + \cdots + a_M(f) = 0, \quad a_i \in k[X].$$

So only g_i poles in S. There is c s.t. $\mathrm{Div}(g) + cZ \geq 0$. For any t, $\mathcal{L}((t+c)Z)$ contains $g_i, g_i f, \dots, g_i f^t$ for all i. These elements are linearly indep over k. We find

$$\dim((t+c)Z) \geq n(t+1).$$

This can grow at most $m(t+c)+1$ or so because of the bound on the degree, whence $n \leq m = \deg Z$. ▲

Lecture 36
11/17

36.1 Theorem (Riemann inequality)**.** *$\exists c$ s.t.*

$$\dim \mathcal{L}(D) \geq \deg D - c \quad \forall D$$

Proof. Know the opposite ineq. Know this inequality for certain divisors. Let D be a div and let f, Z, c as in last result. Change D to equiv div s.t. zeros D contained in Z. Then $\exists T$ s.t. $0 \leq TZ - D$. Then $\dim \mathcal{L}(TZ) \leq \deg(TZ - D) + \dim \mathcal{L}(D)$ by exact seqs. When T large get the result. ▲

This is some result on sublinear fns on groups with partial orders.

36.2 Definition. We know that there is a constant c as in the thm. The **minimal** g s.t. $\dim \mathcal{L}(D) \geq \deg D + 1 - g$ is called the **genus** of the curve.

We also defined the genus as the dimension of the linear system associated to the canonical class. All two defs are equal by Riemann-Roch.

Lecture 37
11/19

Last time we proved the **Riemann inequality.** For a smooth projective curve X, we can find a constant c such that for any D,

$$\dim \mathcal{L}(D) \geq \deg D + 1 - c.$$

We define the **genus** to be the minimal such c.

37.1 Definition. The **defect** of a divisor D, $\delta(D)$, is the difference

$$\deg D - \dim \mathcal{L}(D) + 1.$$

We showed that:

1. If Z is the divisor of zeros of a rational fn f, then the defect $\delta(tZ) \geq c$ for all c
2. If $D \leq D'$, then
$$\delta(D') \geq \delta(D).$$
3. If $D \sim D'$, then $\delta(D) = \delta(D')$
4. For any divisor D, there is an n such that $nZ \geq D'$ where $D' \sim D$.

37.2 Corollary. *If D actually achieves the maximum, i.e. $\delta(D)$ is the genus, and $D' \geq D$, then D' achieves the maximum (i.e. $\delta(D') = g$). In particular, we know $\mathcal{L}(D') = \deg D' + 1 - g$.*

So large enough out, the defect is the genus.

37.3 Corollary. *There is N such that if D is a divisor of deg $\geq n$, then*

$$\delta(D) = g.$$

Proof. Suppose $D_0 = g$. Let $N = \deg D_0 + g + 1$. If $\deg D \geq N$, then $\deg(D - D_0) > g$. In particular, from the Riemann inequality

$$\dim \mathcal{L}(D - D_0) > 1.$$

Choose $f \in \mathcal{L}(D - D_0)$. This means that $\mathrm{Div}(f) + D - D_0 \geq 0$. Equivalently $\mathrm{Div}(f) + D \geq D_0$. By the corollary, $\delta(\mathrm{Div}(f) + D) \geq g$, so it is g. But δ doesn't depend on the linear equivalence class. ▲

§1 Eqns over finite fields

We start by doing alg geo over non-alg closed flds.

Let $\mathbb{F}_q$ be a finite field of size $q = p^r$ where p prime. Denote $k = \overline{\mathbb{F}_q}$. Suppose $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$. We can look at the variety they generate. Look at

$$A_0 = \mathbb{F}_q[x_0, \ldots, x_n]/(f_1, \ldots, f_m).$$

Let $A = A_0 \otimes_{\mathbb{F}_q} k$ be the coordinate ring of $X = V(f_1, \ldots, f_m)$. I think we all know that things called *schemes* exist. We won't define them though.

So X contains points corresponding to either

1. Maximal ideals in A
2. k-homomorphisms $A \to k$.

For A_0 these notions are different: a maximal ideal in A need not correspond to a homomorphism $A_0 \to \mathbb{F}_q$. We will call the max'l ideals in A the **closed schematic points** of $X = \mathrm{Spec} A_0$. We will call the $\mathbb{F}_q$ morphisms $A_0 \to k$ **geometric pts.** The geometric pts correspond to the usual points of the variety $V(f_1, \ldots, f_m) \subset k^{n+1}$. More generally if F is a field we can consider F-valued points.

Yet the two notions are not too different. Given a homomorphism, we get a max'l ideal by taking the kernel. The map from

$$\{\text{geometricpts}\} \to \{\text{closedpts}\}$$

is injective.

37.4 Definition. The **schematic points** of X_0 is denoted $|X_0|$. The set of F-valued points A_0 (i.e. morphisms $A_0 \to F$) is denoted by $X_0(F)$.

We want to count $X_0(\mathbb{F}_{p^n})$.

37.5 Proposition. *The map* $X_0(k) \to |X_0|$ *is onto and the fibers are orbits of* $\mathrm{Gal}(k/\mathbb{F}_q)$.

Proof. Clearly there is an action of the Galois group on $X_0(k)$ (postcomposition $A_0 \to k \to k$). If we have a max'l $\mathfrak{m} \subset A_0$, then $A_0/\mathfrak{m}$ is finite ext. of $\mathbb{F}_q$. In particular is contained in k. It is nonunique and the nonuniqueness is *exactly* the orbit of Galois grp. If we have two isomorphic subfields given by images of two homomorphisms $A_0 \to k$, then we can move them into each other via the Galois grp. So the maximal ideal determines the homomorphism $A_0 \to k$ up to Galois conjugation. ▲

So counting geometric and schematic points are kind of similar.

37.6 Definition. If $x \in |X_0|$ is a closed schematic pt, denote by $\kappa(x)$ the field A_0/x. (x is a max'l ideal.) This is a finite ext of $\mathbb{F}_q$. The degree $[\kappa(x) : \mathbb{F}_q]$ is called the degree of x.

A schematic pt x corresponds to $\deg x$ geometric pts. This is because the action of the Galois group $G(k/\mathbb{F}_q)$ on the fiber factors through $G(\kappa(x)/\mathbb{F}_q)$. We are using the fact that $\kappa(x)$ is automatically normal since we are dealing with finite fields.

Now we need to redo the course for non-algebraically closed fields. But it is the same. You can talk about projective spaces in the same way, and they are covered by affine pieces. (You can think of them as homogeneous ideals in a suitable graded ring, or by gluing affine pieces.)

Lecture 38
11/22

(This is the second-to-last lecture.)

Irreducibility is not preserved when you change your base field. You should very suspicious about when you change to a non-alg-closed fld. We will talk about the Weil conjectures.

We looked at curves over $\mathbb{F}_q$, a finite fld. X_0 defined by eqns over $\mathbb{F}_q$, X variety defined by the same eqns but in $\overline{\mathbb{F}_q}$. Alg. geo. is about solving eqns. Namely, given F, we look at $X_0(F)$. To X_0, attach a ring $A_0 = \mathbb{F}_q[x_0, \ldots, x_n]/(f_1, \ldots, f_m)$; then $X_0(F)$ is equal to $\mathrm{Hom}_{\mathbb{F}_q}(A_0, F)$. This is interesting even if $F \neq \overline{\mathbb{F}_q}$. Each homomorphism gives a kernel, which may be maximal or simply prime. So in the more sophisticated version of alg geo, you consider *all prime ideals,* and not just max'l ones. But we're not there. When we say "schematic points," we mean **max'l** points. In our case, will look at curves.

38.1 Example. $X_0 = \mathbb{A}^1$, then $A_0 = \mathbb{F}_q[x]$. The points are the schematic points (max'l ideals) and (0).

For a closed schematic pt, we defined the *degree* of x as $[\kappa(x) : \mathbb{F}_q]$ where $\kappa(x) = A_0/(x)$.

From now on, work only with curves.

38.2 Definition. A **Weil divisor** on X_0 is a $\mathbb{Z}$-combination of closed schematic points. The **degree** of a divisor $\sum n_i[x_i]$ is $\sum n_i \deg x_i$. This is because x_i represents $\deg x_i$ geometric points. (We need nonsingularity to define it.)

Whenever f is a rational fn in the old sense defined over $\mathbb{F}_q$, its zeros and poles are stable under Galois conjugates, so gives a divisor on X_0. We can get a **class group** of X_0.

Let X_0 be a curve, X the base-change to $\overline{\mathbb{F}_{||}}$.

38.3 Proposition. *Suppose X irred, proj., smooth. For any n, the level n class group (divisors of deg n) $\mathrm{Cl}^n(X_0)$, is finite.*

Proof. Suppose first $n \gg 0$. Choose a div $D \in \mathrm{Div}^n(X)$. Gives a divisor D on X. If n big, Riemann inequality implies $\exists$ a section of $\mathcal{L}(D)$. Also a f.d. subspace of $\overline{\mathbb{F}_q}(X)$. I claim that the eqns defining it are eqns over $\mathbb{F}_{||}$. Indeed, $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is topologically generated by a Frobenius σ. Then σ defines an $\mathbb{F}_{||}$-linear automorphism on $k(X)$. Indeed, we just raise every coefficient to the qth power. Now $\mathcal{L}(D)$ is invariant under σ, since D is, so is defined by $\mathbb{F}_{||}$-linear equations. By linear algebra, $\mathcal{L}(D)$ contains a basis consisting of Frobenius fixed pts. Changing D to $D + \mathrm{Div}(f)$, we may assume $D \geq 0$. Then it's clear. There are only finitely many pts on the curve whose degree is at most n, as those pts would have to be contained in the set of solns to the eqn over $\mathbb{F}_{q^n}$. So $\mathrm{Cl}^n(X_0) < \infty$ for n large. But these are all cosets of same grp, there is a homomorphism $\mathrm{Cl}(X_0) \twoheadrightarrow \mathbb{Z}$ (at least if $\mathbb{F}_q$-ratn'l pt exists, otherwise slightly different argument), so done. ▲

OK. So goal. Start with X_0, count $|X_0(\mathbb{F}_{q^n})$. These numbers can be put in a generating fn, consider:

$$\sum_{n=1}^{\infty} |X_0(\mathbb{F}_{q^n})| t^n = \sum_n \sum_{d|n} |\{x \in |X_0|, \deg x = d\}| t^n/d.$$

Each schematic pt gives a degree. Now switch the sums:

$$\sum_d |\{x \in |X_0| : \deg x = d\}|/d \sum_{k=1}^{\infty} t^{kd} = \sum_{x \in |X_0|} \frac{\deg x t^{\deg x}}{1 - t^{\deg x}}$$

Here we can write each term as $-t\frac{d}{dt}\log(1 - t^{\deg x})$. We find in total:

$$-t\frac{d}{dt}\log\left(\prod_{x \in |X_0|}(1 - t^{\deg x})\right)$$

38.4 Definition. This fn $\prod_{x\in|X_0|}\left(\prod_{x\in|X_0|}(1 - t^{\deg x})^{-1}\right)$ is the **zeta function** of X_0.

This is equivalently

$$\prod_x (1 + t^{\deg x} + t^{2\deg x} + \dots)$$

which can be multiplied out as in the Euler formula. This is

$$\sum_{D \in \mathrm{Div}_{\geq 0}(X_0)} t^{\deg D}.$$

Now, group them according to classes.

$$\sum_{E \in \mathrm{Cl}_{\geq 0}(X_0)} \sum_{D \sim E, D \geq 0} t^{\deg D}$$

Here's a claim. We want to know what all the divisors ≥ 0 are in a given divisor class.

38.5 Proposition. *Let $D \geq 0$ be a divisor. $\exists$ a bijection between the set of all divisors $D' \sim D$ and $D' \geq 0$ and $\mathbb{P}(\mathcal{L}(D))$.*

Proof. If you have $\phi \in \mathcal{L}(D)$, nonzero, then send it to the divisor $\mathrm{Div}(\phi) + D$. By definition, this is a nonnegative divisor. It depends on ϕ up to multiplication by constant. And conversely. Hence the bijection. ▲

So we have a sum here. Let's write this as

$$\sum_{n=0}^{\infty} \sum_{E \in \mathrm{Cl}^n(X_0)} |\mathbb{P}(\mathcal{L}(E))| t^{\deg E}$$

We split this into

$$\sum_{n=0}^{N} + \sum_{N+1}^{\infty}$$

where $N \gg 0$. Forget about the first sum; it's a polynomial. Look at the second sum. We know that $\mathrm{Cl}^n(X_0)$ has the same size as $\mathrm{Cl}^0(X_0)$ if X_0 has a $\mathbb{F}_q$-point. Also if D large, then

$$\dim \mathcal{L}(D) = \deg D + 1 - g$$

by Riemann inequality. So we find that the second sum is

$$\sum_{n \geq N} |\mathrm{Cl}^0(X_0)| q^{n+1-g-1} t^n / (q-1)$$

by counting the size of a projective space. This is a **rational function**. It is of the form polynomial$/((1-t)(1-qt))$.

If a generating fn is a rational fn, then the coefficients satisfy a linear recursion. So this is big.

Lecture 39
11/24

Recall that last time, given a smooth proj curve X_0 over $\mathbb{F}_q$, we defined

$$Z(t) = \prod_{x \in X_0} (1 - t^{\deg x})^{-1}$$

the product over all closed schematic pts. We know that the thing we are interested in is

$$\sum |X_0(\mathbb{F}_{q^n})| t^n = t \frac{d}{dt} \log Z(t).$$

Recall that $Z(t) = f(t)/((1-t)(1-qt))$ as we saw last time. We know that $Z(0) = 1$. So we can write $f(t) = \prod(1 - \lambda_i t)$. When we write this out, we find an expression for $|X_0(\mathbb{F}_{q^n})|$ in terms of n, by equating coefficients. In particular, the upshot is that

$$\boxed{|X_0(\mathbb{F}_{q^n})| = q^n + 1 - \sum^N \lambda_i^n.}$$

How large can N be? It's all the roots of the polynomial.

To advance further, we need:

39.1 Theorem (Riemann-Roch)**.** *For any divisor D, we have*

$$\dim \mathcal{L}(D) - \dim \mathcal{L}(K - D) = \deg D + 1 - g.$$

39.2 Corollary. $\deg K = 2g - 2$.

Proof. Take $D = K$. ▲

39.3 Corollary. *If* $\deg D > 2g - 2$*, then* $\dim \mathcal{L}(D) = \deg D + 1 - g$.

Proof. When a divisor is negative, its $\mathcal{L}$ is zero. ▲

39.4 Corollary. *We can take* $N \le 2g$*.*

39.5 Theorem.

$$Z(1/qt) = (qt^2)^{g-1} Z(t).$$

This is a type of palindromic symmetry.

Proof. We know

$$Z(t) = \sum_{D \in \mathrm{Div}, D \ge 0} |\mathbb{P}(\mathcal{L}(D))| t^{\deg D}$$

We split this into two sums where the first sum is small and the second large. This is

$$\sum_{0 \le D \le g-1} \frac{q^{\dim \mathcal{L}(D)} - 1}{q-1} t^{\deg D} + \sum_{g-1 < \deg D < 2g-2} \frac{q^{\dim \mathcal{L}(D)} t^{\deg D} - q^{\deg D + 1 - g}}{q-1} + \sum_{g-1 < \deg D \le 2g-2} \frac{q^{\deg D + 1 - g} - 1}{q-1} t^{\deg D}$$

Replace D in the first summand by $K - D$ and do some more tricks. The basic trick is for $0 \le \deg D \le g-1$ is to use $q^{\deg D} - 1$, for $g \le D \le 2g-2$, to use an incorrect formula, and then for the rest, add and subtract some terms that cancel. ▲

39.6 Corollary. *The roots of the numerator* $f(t)$ *of the zeta functions come in reciprocal pairs* $\lambda, \widetilde{\lambda}$ *with* $\lambda\widetilde{\lambda} = q$*.*

The big result is:

39.7 Theorem (Weil)**.** *The absolute values of the roots of* f *are* $\sqrt{q}$*.*

39.8 Corollary. $|X_0(\mathbb{F}_{q^n})| = q^n + O(q^{n/2})$*.*

This is true (Lang-Weil) for arbitrary geometrically integral varieties, not necessarily curves, not even projective. That is, we have

$$|V(\mathbb{F}_{q^n})| = q^{n \dim V} + O(q^{n \dim V - 1/2}).$$

Namely, you start with V, project it $\mathbb{P}^{\dim V - 1}$; the fibers will then be curves. Over a smaller set, the fibers might be bigger. Forget about the bad points; then just focus on the curves.

For a smooth proj V_0 (with the base-change V to $\overline{\mathbb{F}_q}$), we have $|V(\mathbb{F}_{q^n})| = \sum_{i=0}^{2g} \sum \lambda_{i,j}^n$ where $\lambda_{i,j}$ has absolute value $\sqrt{q}$. So these behave like the traces of powers of a matrix. These are the **Weil conjectures: proved by Dwork, Grothendieck, and Deligne.**