MATH 145 NOTES

ARUN DEBRAY
AUGUST 21, 2015

These notes were taken in Stanford's Math 145 class in Winter 2015, taught by Ravi Vakil. I TEXed these notes up using `vim`, and as such there may be typos; please send questions, comments, complaints, and corrections to a.debray@math.utexas.edu.

CONTENTS

1. META STUFF AND AN OVERVIEW OF ALGEBRAIC GEOMETRY: 1/5/15

"Well, sadly, we live in the real world, but if you put on your complex glasses. . . "

The thing about undergraduate algebraic geometry is that very few schools offer it, and perhaps strictly fewer should. The class has a potential to end in tears, so we'll speak carefully about where these things can go wrong.

Algebraic geometry is a grand unified theory of mathematics; well, maybe not so unified. It's very broad, and you have to know a lot to understand it very well. We'll try to make the only prerequisite Math 120, though it will also require a lot of intestinal fortitude if that's your only experience. Similarly, we'll try to actually do interesting things and motivate them, so that it's not too hand-wavy or without motivation.

Algebraic geometry, the language of varieties, still also applies to number theory and complex geometry in other ways. This deals with something called a scheme, which we'll define and discuss, but most of the cases will be for varieties.

Given that the people in the classes have vastly different backgrounds, difficult problem sets for one person will be more straightforward for others, so we'll have traditional problem sets along with maybe some other things. Perhaps we can have a source of course documents or information in which people can edit other people's documents, and people can

take (or even live-TEX!) notes for the class. This, along with problem sets and learning about some enrichment beyond the lectures, will play into the course grade.

While we're not going to follow a single book, there is a sort of canonical set of things to do, and here are some useful references to have; all of them are freely and legally available online to Stanford students.

- Miles Reed. *Undergraduate Algebraic Geometry*.
- Frances Kirwan, *Complex Algebraic Curves*.
- Fulton, *Algebraic Curves*.

The thing about algebraic geometry is that it's very hard to give a three-sentence description of it. It connects and unifies many branches of mathematics, including (commutative and noncommutative) algebra, complex (and to a certain extend, differential) geometry, number theory, topology (especially algebraic topology), and even a little mathematical logic. It's even not so much as if they were unified, but that this modern machine, whose foundation was laid in the 1950s and '60s, underlies and affects the ways that these fields are done. We'll focus on the number theory, the geometry, and the algebra in this class, since not everyone has seen a lot of topology.

A lot of this came from one man's head, Grothendieck; he died a few weeks ago. Another major player, Serre, is alive and well.

Let's talk about the central theme, more or less, in this course. Consider the Diophantine equation $x^2 + y^2 = 1$; we're looking for rational solutions, i.e. Pythagorean triples $a^2 + b^2 = c^2$. But we can't help but draw a circle (which is useful for real-valued solutions). We can even do this over $\mathbb{C}$, which gives us (as we'll see later on) a sphere with two points. We want to have an object which tracks all of these properties, that is somewhat geometric and a little arithmetic. This object is a *scheme*; it's a notion of a kind of geometric space. We've seen geometric spaces before, e.g. in finite-dimensional linear algebra, where we have subspaces and maps of subspaces. Importantly, when you learn linear algebra, the base field doesn't really matter. Another example is a manifold, which locally looks like $\mathbb{R}^n$ (we'll define it precisely later on).

Vector spaces and manifolds have dimension, but it's kind of a weird notion, especially for vector spaces over finite fields. How do we even know that dimension is an invariant (or is well-defined)? Can a manifold made by gluing together pieces of $\mathbb{R}^2$ also be obtained by gluing together pieces of $\mathbb{R}^3$? Dimension is a weird notion, and once we get the right definition (which will be weird), we will be able to define dimension in all sorts of strange but useful contexts.

Let's talk about number theory. Talking about linear equations, such as $x + y = 1$, is relatively easy; we have seen linear algebra before, and there are well-known algorithms. For quadratic equations, e.g. $x^2 + y^2 = 1$, there are lots of solutions, and we can find them. In the general case, $x^n + y^n = 1$ over $\mathbb{Q}$ is equivalent to Fermat's Last Theorem. Of course, this means it's hard! And relatively few solutions exist. The case $x^3 + y^3 = 1$ is intermediate to these; a little easier.

For the linear case, but over $\mathbb{C}$, the solution ought to be a complex line, but this topologically looks like a sphere minus a point. Conics are spheres minus two points, and in general given an n^{th}-degree equation over the complex numbers, it should look like something minus n points.

Furthermore, geometrically speaking, the second-degree case looks like the linear case: negative curvature. They look like spheres. For the cubic, it's flat, and then afterwards, in higher-degree cases, it's positively curved. Mordell's conjecture, proven by Faltings (and how he got his Fields medal in the 1980s) says that in these cases, there are few solutions (in general, there are always finitely many).

This connection between $\mathbb{Q}$ and $\mathbb{C}$ looks somewhat magical, but let's throw in finite fields, too; why not? The Weil[1] conjectures relate solutions over finite fields.

Quick recap: for any prime p and $n \in \mathbb{N}$, there's a unique field, up to isomorphism, of size p^n. This is usually denoted $\mathbb{F}_{p^n}$.

Of course, there can only be finitely many solutions over each finite field, but if one considers solutions of an equation over $\mathbb{F}_{p^n}$ for varying values of n, it comes packaged as a generating function. The conjectures claim that one can recover the behavior of the geometry of the solutions over $\mathbb{C}$ from this generating function, and vice versa. This might seem magical; this is to be expected.

Given a prime p, we can define the p-adic numbers, denoted $\mathbb{Z}_p$, as power series in p, with coefficients on $[0, p-1]$. Then, one can add, subtract, and multiply then, though not necessarily divide, and the integers sit inside them. This isn't a formal definition, but we'll fix that later. If one looks at the integers $\mathbb{Z}$, think of them as a line, geometrically. This is related to the result from complex analysis that if one knows the value of a holomorphic function in a neighborhood, one knows it on its entire domain. Then, one can recover a p-adic in a neighborhood of a prime p of $\mathbb{Z}$. This, again, is a hand-wavy overview that we will make rigorous later.

Let's talk about projective space, which can be defined over any field. For example, $\mathbb{P}^2_{\mathbb{R}}$ is the set of lines through the origin in $\mathbb{R}^3$.[2] This is something better than a set, even intuitively: it makes sense for some lines to be near other lines

[1] Weil is pronounced "veil."

[2] "I should have brought some actual, physical lines with me."

(non-horizontal lines meet the ceiling at some point $(x, y, 1)$, and points near each other should be near each other on the ceiling, too). Thus, we can think of $\mathbb{P}^2_{\mathbb{R}}$ as a topological space (and even a manifold; it's two-dimensional, which is why we have $\mathbb{P}^2$ even though it's built from $\mathbb{R}^3$).

Looking at non-horizontal lines by identifying them with their points on the ceiling, $\mathbb{P}^2_{\mathbb{R}} = \mathbb{R}^2 \cup \mathbb{P}^1_{\mathbb{R}}$, where the latter is the set of horizontal lines. We can do this more generally, too; if k is any field, $\mathbb{P}^{n-1}_k = k^{n-1} \cup \mathbb{P}^{n-2}_k$. Even if the field is different or weird, it's easiest to think of it intuitively or geometrically as $\mathbb{P}^2_{\mathbb{R}}$.

Definition. If k is a field, then *projective n-space over k*, denoted $\mathbb{P}^n_k$, is the space of lines through the origin in k^{n+1}.

We also have a hyperplane at ∞, which corresponds to our horizontal lines in $\mathbb{P}^2_{\mathbb{R}}$. These are different from the rest of our lines, because they don't have a spot on the ceiling, but thy shouldn't be that different, since rotating one's frame makes different lines horizontal. Algebraically, there's a transitive action on $\mathbb{P}^n_k$.

Definition. *Projective coordinates* on $\mathbb{P}^n_k$ is a set of equivalence classes of $(n+1)$-tuples of elements of k, not all zero, such that if $\lambda \neq 0$, then $[a_1, \ldots, a_n] \sim [\lambda a_1, \ldots, \lambda a_n]$.

So we consider points up to scalar multiplication.

We can also talk about the symmetry group of projective space. $\mathrm{GL}_{n+1}(k)$ is the set of invertible $(n+1)$-dimensional matrices, so they act on $\mathbb{P}^n_k$. However, since we care about lines, scaling everything by a constant doesn't change anything (the same line; also, the same projective coordinate). Thus, we should identify scalar multiplication, and therefore we get the *projective general linear group* $\mathrm{PGL}_{n+1}(k)$ (formally, $A \sim B$ if $A = \lambda B$ for $\lambda \neq 0$). We don't yet know why these are the symmetries, but there's geometric structure being preserved, especially in the real- and complex-valued cases. We'll get to this later in the class.

Let's talk a little more about $\mathbb{R}$ and $\mathbb{C}$. Let $p(x) = a_n x^n + \cdots + a_1 x + a_0$. How many roots are there (with multiplicity, because it's more natural to do so)? Over $\mathbb{C}$, which is algebraically closed, we get n solutions, but over $\mathbb{R}$, which isn't, we may get fewer. This suggests that it's nicer to deal with algebraically closed fields, which we'll see again and again.

We also never said that $a_n \neq 0$. This is sometimes part of the definition of "degree," but ultimately, maybe we can't. In fact (e.g. if one looks at the quadratic formula), when $a_n \to 0$, the solution goes to infinity, which ends up corresponding to a place in projective space!

Note that "the plane" is ambiguous, because it could mean k^2 or $\mathbb{P}^2$.

Let's talk about conics in $\mathbb{P}^2_{\mathbb{R}}$ and $\mathbb{R}^2$. In the latter, conics fall into different classes (hyperbola, parabola, ellipse), but it turns out that in $\mathbb{P}^2$, they can all be translated, one into another. This deals with some of the stuff at infinity again.

2. Projective Space and Fractional Linear Transformations: 1/7/15

> *"We haven't defined dimension, and we haven't defined codimension, which may be scary, but that shouldn't stop us."*

We haven't defined a variety yet, but that's OK; we will have some examples, and then can see how they fit into a definition.

Last lecture, we discussed projective space $\mathbb{P}^n$, and that its automorphisms are $\mathrm{PGL}_{n+1}(k)$. For example, $P^1_{\mathbb{C}}$ is the complex numbers plus a point at infinity, which is best visualized as a sphere. $\mathbb{P}^1_{\mathbb{F}_2}$ looks like three points, but this ignores some of the structure. Then, we defined projective coordinates; for example, on $\mathbb{P}^1_{\mathbb{C}}$, $[z, 1]$ corresponds to a $z \in \mathbb{C}$, but $[1, 0]$ corresponds to the point at infinity.

The automorphism group $\mathrm{PGL}(n+1)$ acts as matrices, e.g.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}.$$

This corresponds to the *linear fractional transformation*

$$t \longmapsto \frac{at + b}{ct + d}.$$

Why aren't these all linear? It's worth thinking about. In some sense, the linear fractional transformation can be given by writing x/y for $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$; since we can ignore scalars, everything works out.

Exercise 2.1. Prove that this group of linear fractional transformations with coefficients in k is isomorphic to $\mathrm{PGL}_2(k)$ (with function composition and matrix multiplication, respectively).

Definition. A group G acts *precisely 3-transitively* on a set X if for any distinct $p_1, p_2, p_3 \in X$ and distinct $q_1, q_2, q_3 \in X$, there is a unique $g \in G$ such that $g \cdot p_i = q_i$ for $i = 1, \ldots, 3$.

Theorem 2.2. $\mathrm{PGL}(2)$ *acts precisely* 3*-transitively on* $\mathbb{P}^1$.

Proof. It is sufficient to show that given any p_1, p_2, and p_3, we can send $p_1 \mapsto 0$, $p_2 \mapsto 1$, and $p_3 \mapsto \infty$, since then we get q_1, q_2, and q_3 in the opposite direction.

The group element we would want acts by $(ax+b)/(cx+d)$, but by plugging in p_3 and p_1, we know that $(cp_3x + p_1)/(cx+1) = p_2$, so we can just solve for c. (The trick is of course that scalar multiples can be forgotten.) □

Thus, for any pairs (p_1,p_2,p_3,p_4) and (q_1,q_2,q_3,q_4) of elements of projective space, there are transformations $(p_1,p_2,p_3,p_4) \sim (0,1,\infty,\lambda) \sim (q_1,q_2,q_3,q_4)$. This λ is called the *cross ratio* of the points.

Question. Find linear fractional transformations $f(t)$ that satisfy the following, preferably over any field.

- $f(f(f(t))) = t$.
- $f(t) \neq t$ for any t.
- $f(0) = 1$, $f(1) = \infty$, and $f(\infty) = 0$. How many are there? Can we classify them? Maybe all of the order-3 elements are conjugate (i.e. given f and g of order 3, there's an h such that $h(g(t)) = f(h(t))$, i.e. $h \circ g \circ h^{-1} = f$). This is a claim we can check.

We can ask more general questions: PGL(2) acts on $\mathbb{P}^1$ 3-transitively, but what does PGL$(n+1)$ do to $\mathbb{P}^n$?

We can make a hazy argument with dimension for $\mathbb{P}^2$: PGL(3) is eight-dimensional (which we haven't defined exactly, but ends up being as a manifold; there are nine degrees of freedom, and then we're ignoring one dimension of scalars). Given a point $x \in \mathbb{P}^2$, there are two dimensions of places it can be sent (again, as a manifold), so the subgroup fixing x has codimension 2.

Dimension is hard: it's weird in linear algebra, and gets weirder in algebraic geometry. For example, even for manifolds, we want the dimension of a manifold M to be the n of the $\mathbb{R}^n$ that it looks like locally, but how do we know that $\mathbb{R}^n$ and $\mathbb{R}^m$ aren't diffeomorphic for $m \neq n$? Algebraic topology can answer that question, but it's a bit beyond the scope of the class, and is a topological criterion, not a geometric one.

Manifolds are not vector spaces, but at each point there's a tangent space. How do we do this? Given an abstract manifold, how do we determine what an abstract tangent space means? Once we do that, we can intrinsically define what the dimension of a manifold is (since we *do* know what the dimension of a vector space is, thanks to bases and linear independence).

There was a change in point-of-view in some of this stuff in about 1900 or so; one first imagines a manifold sitting in one ambient space. But a torus could also be a square where the sides are identified (as in Figure 1). This is an intrinsic definition, which is nicer, and is more popular nowadays.

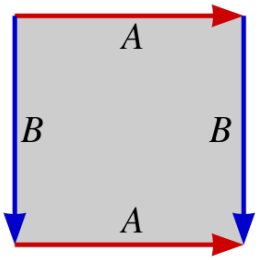


FIGURE 1. An intrinsic definition of a torus; sides with the same label or color are identified. Source: http://en.wikipedia.org/wiki/Fundamental_polygon.

Anyways, we were talking about projective space. The subset of PGL(3) fixing a point is six-dimensional (codimension 2), but we only have 8 dimensions floating around, so we can't intersect five of these and still have anything left. The best we can hope for is four points...

But that doesn't work either. What if you take all four points to be on a line? This ends up not working. Thus, we use the words "general position" to exclude these special cases, and then it does work.

Fact. Inside $\mathbb{P}^n$, this does work for $n+2$ points in general position (no 3 in a line, no 4 in a plane, etc.); they can be sent uniquely to $n+2$ points.

This is a linear algebra fact, and linear algebra is supposed to be easier, right?

For example, on $\mathbb{P}^3$, we can do this with five points in general position.

Another way to think of general position is that, when one does all of the linear algebra, a determinant is nonzero.

Conics in $\mathbb{P}^2$. Using projective coordinates $[x_0, x_1, x_2]$, we can write down equations such as $x_0^2 + x_1 x_2 = 0$. We have to be careful, though; sometimes these equations aren't homogeneous, e.g. $x_0^2 + x_1^4 = 0$. That is, this equation isn't invariant under scaling. Thus, we should only consider homogeneous ones.

Definition. A *conic* in projective space is the solution set to a homogeneous second-degree polynomial in 3 variables.

How many conics are there? That is, what dimension is the space of conics, and why? It ends up being five-dimensional, because the general form is $a_1x^2 + a_2y^2 + a_3z^2 + a_4xy + a_5xz + a_6yz$, but then we mod out by scalars, so we get $k^6 \setminus 0/k^\times \cong \mathbb{P}^5$. Thus, the space of conics is $\mathbb{P}^5$, which is cool. And this is true over every field, even finite ones.

Question. More generally, how many degree-d hypersurfaces (i.e. dimension) are there over $\mathbb{P}^n$?

This can be solved by counting monomials in the same way. We also need to define "hypersurface" (and later, "smooth"), but for the purposes of this question, this still makes sense.

This leads to other interesting questions, e.g. can one send one conic to another using an element of $\mathrm{PGL}(n)$? Or more intuitively, what kinds of conics are identical?

3. Diophantine Equations and Classifying Conics: 1/9/15

Last time, we discussed projective n-space over a field k, $\mathbb{P}^n_k$, and that its automorphism group is $\mathrm{PGL}_{n+1}(k)$. It makes sense why this ought to be true for $k = \mathbb{C}$, but for, say, $k = \mathbb{F}_{17}$, why would it be true?

When you learn about a mathematical object, you really want to know what *category* it belongs to; not just the objects, but the morphisms (or maps) that go between them. In linear algebra, you learn about vector spaces and linear maps; in differential topology, manifolds and smooth maps, and so on. This always looks the same at a distance.

To pin this down, we'll ask some questions; we know what the answers ought to be, which forces us to say what the definition has to be. Consider $\mathbb{P}^2$ with projective coordinates $[x, y, z]$; then, does a line through it (e.g. $\{z = 0\}$) look like $\mathbb{P}^1$? Yes, because we have the projective coordinates $[x, y]$ there (and similarly, if $x = 0$, we have $[y, z]$). Alternatively, we have injections $\mathbb{P}^1 \hookrightarrow \mathbb{P}^2$, e.g. $[x, y] \mapsto [x, y, 0]$. But we technically don't know what the maps are in projective spaces, though we know this ought to be true. However, $[x, y] \mapsto [x, y, 1]$ isn't linear, so it's not even well-defined (e.g. $[1, 2] \sim [2, 4]$, but they have different images). $[x, y] \mapsto [x, y, x - y]$ is well-defined and injective, corresponding to a diagonal line. Why is it a line? Well, it's a linear polynomial.

What about $[x, y] \mapsto [x^2, xy, y^2]$? The image is a conic now, not a line (specifically, the conic $ac = b^2$), and is injective. We still need to talk about what a map is, and why these are lines. Technically, the "line" is really $\mathbb{P}^1$, but this image is cut out by a linear polynomial, so it's reasonable to call it a line.

One interesting consequence is that if two different injections $i_1, i_2 : \mathbb{P}^1 \hookrightarrow \mathbb{P}^2$ have the same image, then one can compose $i_2^{-1} \circ i_1$ to get an automorphism of $\mathbb{P}^1$ distinct from the identity! This is an interesting, albeit somewhat hand-wavy, way to obtain automorphisms of $\mathbb{P}^1$, though we could just do the linear algebra to double-check.

Last lecture, we also talked about conics (degree-2 homogeneous polynomial in 3 variables). We can classify conics, but it seems reasonable to classify all ellipses to be the same, etc., so let's try to classify conics in $\mathbb{P}^2$ up to $\mathrm{PGL}(3) = \mathrm{Aut}(\mathbb{P}^2)$. For simplicity, let's do this over $\mathbb{C}$.

For example, $x^2 + y^2 = z^2$ and $x^2 + 3y^2 + 2xz - z^2 = 0$ are equivalent. There's a change of coordinates which makes this work, and Sylvester's inertial law (which is a consequence of the spectral theorem) guarantees that if the number of negative entries of a quadratic form doesn't change, then they are equivalent after a change of coordinates.

Geometrically, ellipses and circles are equivalent over $\mathbb{C}$. Cool! How about over other fields? Over $\mathbb{R}$, Sylvester's law takes a different form, so we get the classification of conics in the projective plane that we are more familiar with.

Over $\mathbb{Q}$, things get more potentially scary. Consider $x^2 + y^2 = z^2$, which gives is Pythagorean triples. This gives us a nice circle. Given a line in $\mathbb{P}^2$ that intersects $[1, 0, 1]$, does it intersect this curve somewhere else? Well, we have $y = m(x - 1)$ and $x^2 + y^2 = 1$, so $x^2 + (m^2x^2 - 2m^2x + m^2) = 1$, i.e. in general we get two roots, unless m is infinite (vertical line), in which case the root at $[1, 0, 1]$ is a double root. So we just solved a Diophantine problem. Cool.

You can do this with many related problems: pick a given solution, and then do some not-so-complicated algebra to know them all. But first you have to find a specific solution... this could be harder with, say, $x^2 + y^2 = 99z^2$. Thus, all conics with a point are $\mathbb{P}^1$, and if they don't have a point, well, that's the empty set.

Next up, how about $y^2 = x^3 + 3x^2$? How do we find solutions in $\mathbb{C}^2$? (This isn't homogeneous, so we can't do it in $\mathbb{P}^2_{\mathbb{C}}$; we would really want $y^2z = x^3 + 3x^2z$.) We have a solution, e.g. $x = 0$ and $y = 0$, or $x = 1$ and $y = \pm 2$. But the origin really is two solutions (since the curve hits the origin twice, or alternatively, a line generically meets a cubic at three points, and a line intersecting the origin only meets one other point). Thus, if $y = mx$, then $m^2x^2 = x^2 + 3x^2$, or $x = m^2 - 3$, i.e. $y = m(m^2 - 3)$, and there's another rational point at infinity (if we homogenize the equation as above).

Question. Let's end with some rhetorical questions (which we'll actually talk about next time).

- Why do a line and a degree-d curve generally intersect at d points?

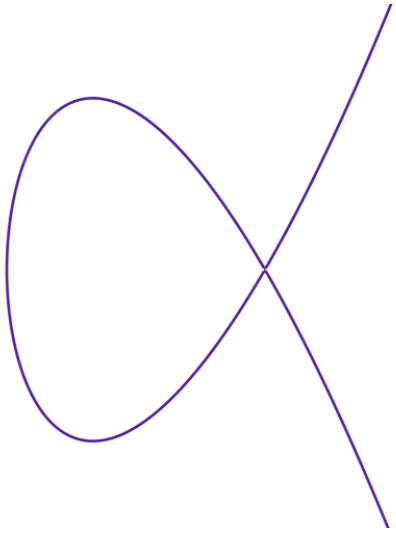


FIGURE 2. The elliptic curve $y^2 = x^3 + 3x^2$, or a depiction of it in $\mathbb{R}^2$.

- Why do a degree-d curve and a degree-e curve generally intersect at de points?
- How many conics pass through five points? Or through four points, but are tangent to a line? In the $\mathbb{P}^5$ of conics, there is a single equation corresponding to the conics tangent to a given line. What is the degree of that equation?

4. Quadratics and Cubics: 1/12/15

Proposition 4.1. *Given a set of five points in $\mathbb{P}^2$, no three of which are collinear, there is exactly one conic through all five.*

Notice that we haven't specified a field; it's easiest to think about complex numbers, and then relax assumptions where need be. We'll typically prefer algebraically closed fields, but sometimes this can also be relaxed.

Proof. Let $[x,y,z]$ be our projective coordinates; then, last time, since we showed all conics take the form of $ax^2 + byx + cy^2 + dxz + ezy + fz^2$, then there are six parameters, but they are invariant under scaling; thus, the space of conics is a $\mathbb{P}^5$.

A conic passing through a point is a linear condition, so the space of conics passing through one point is a $\mathbb{P}^4$ (formally, it's a linear equation in one variable, which kills off one degree of freedom). Then, passing through the next point is also a linear condition, so we get a $\mathbb{P}^3$ after specifying two points.

This continues in the same way, but not all linear conditions are nontrivial, so we have to check. But this is where the restriction on collinearity comes in: for a degree-2 polynomial to vanish on four non-collinear points, it must be the zero polynomial.

To look at what happens when three points are collinear, notice that since there are six parameters, there is a $\mathbb{C}^6$ of coefficients, and therefore a $(\mathbb{C}^6)^*$, the dual space, of linear conditions. Similarly, hyperplanes are dual to $\mathbb{P}^5$, so we get a $(\mathbb{P}^5)^*$.

The point is, the condition $\{ax + by + cz = 0\}$ is within a $\mathbb{P}^2 \times (\mathbb{P}^2)^*$. Each point of $\mathbb{P}^2$ gives a linear condition, but it sits in $\mathbb{P}^5$, which is much larger! Specifically, we have $\mathbb{P}^2 \hookrightarrow \mathbb{P}^5$ by $[x,y,z] \mapsto [x^2, xy, y^2, xz, yz, z^2]$. It's kind of a strange embedding, but is useful. □

$\mathbb{P}^2$ and $\mathbb{P}^5$ (over $\mathbb{C}$, at least) are both complex manifolds, as is a generic conic condition $\{ax^2 + bxy + \cdots + fz^2 = 0\}$. When we mess around with the dimensions, this latter can be seen as a six-dimensional complex manifold.

Question. How many conics pass through four points (no three collinear), and are tangent to a given line?

Playing the same game, there's a $\mathbb{P}^1$ of conics passing through the four points. Thus, it's one-dimensional, i.e. it's of the form $\lambda p(x) + q(x)$ for some quadratics p and q. This should have zero roots most of the time, but sometimes two roots, and this can be solved for (e.g. by taking the derivative, or looking at the discriminant). For example., if $p(x) = 3x^2 + 2xy + y^2$ and $q(x) = 3x^2 + 7xy$, then there are two solutions tangent to a given line. Sometimes, one may have one root, but this is in some sense an exceptional case.

The question above can be rephrased as intersecting four curves of degree 1 and one curve of degree 2, so the number should in general be the product of the degrees (which will be formalized in Bézout's theorem, eventually). Thus, there

ought to be four conics passing through three points and tangent to two given lines (in general position). This method of thinking relates to *parameter spaces*, a subclass of *moduli spaces*.

Now, here's a trick question: how about the conics that are tangent to *five* given lines? It's reasonable to think there should be $2^5 = 32$ solutions, or maybe that there are no solutions. But in general, there's one solution! (We'll look at the dual space, which will be explained.)

Recall that we had the "universal conic," the $\mathbb{P}^2 \times \mathbb{P}^5$ of conics and points on them. Similarly, we can encode the data of a conic and its tangent line, which gives us $\mathbb{P}^5 \times (\mathbb{P}^2)^*$. In $(\mathbb{P}^2)^*$, tracing the tangent lines on a conic as one moves around gives us a different variety in the dual space. We want to know the degree of this thing in the dual space with a general line in the dual space.

Points in $(\mathbb{P}^2)^*$ correspond to lines in $\mathbb{P}^2$. So what do lines in $(\mathbb{P}^2)^*$ correspond to? They will sweep out a one-dimensional variable of a line, which ends up being all of the lines through a given point. Thus, this line can be identified with that point (because the double-dual can be identified with the original space). Points on a line correspond to lines on a point.

Anyways, now we want to determine the degree of the dual to the conic, the object traced out by the tangents to it in $(\mathbb{P}^2)^*$. Translating this back into $\mathbb{P}^2$, given a random point, how often does a given line through that curve intersect the conic? Well, in general, twice, so the dual to a conic is a conic!

And since lines in $\mathbb{P}^2$ are points in $(\mathbb{P}^2)^*$, then a conic is tangent to five lines iff its dual is tangent to their duals, which are five points. Thus, there's one such dual conic, and therefore one such original conic.

There's one last thing that we should say about degree-2 curves (though there is still so much more to say). Let's consider conics in $\mathbb{P}^3$ (where $k = \mathbb{C}$, or, more generally, an algebraically closed field of characteristic not 2), called *quadric surfaces*. Then, we get conics which look somewhat like $w^2 + x^2 + y^2 + z^2 = 0$, or, in a different system of coordinates, $wx = yz$. These generally look like ellipsoids or hyperboloids.

Exercise 4.2. Each quadric surface is ruled by two dimensions of lines, so it should be given by $\mathbb{P}^1 \times \mathbb{P}^1$. Make this explicit for $wx = yz$ for $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$.

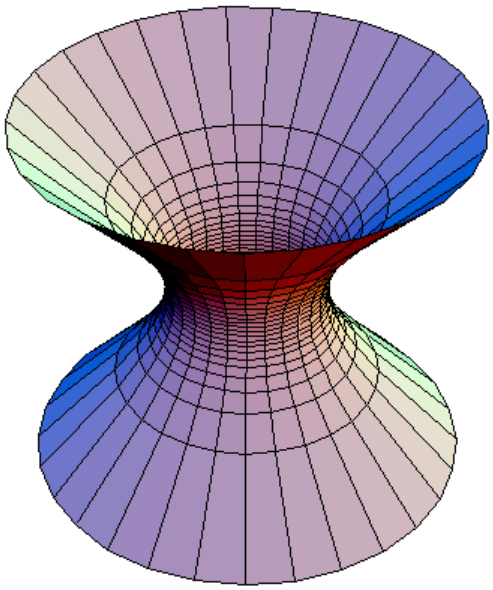


FIGURE 3. A hyperboloid of one sheet, which is an example of a quadric surface, albeit over $\mathbb{R}$. Source: http://en.wikipedia.org/wiki/Hyperboloid.

Exercise 4.3. How do these change when the base field is $\mathbb{R}$ or $\mathbb{Q}$?

For example, if $w^2 + x^2 = y^2 + z^2$, we have $[1,0,0,1]$ for $\mathbb{Q}$, or $[0,1,1,0]$, or more generally anything of the form $w = y$ and $x = z$, which specifies a line in three-space. This leads to the idea that there is a $\mathbb{P}^2$ (topologically) of directions away from a point on the surface, though something funny happens in the tangent direction.

Since we have three minutes, let's talk about cubics in the plane.

Question.

- Given a cubic $y^2 = x^3 + ax + b$, what are its rational solutions? This is harder than the quadratic case, because we can't just consider the set of lines through a point, but intuitively we can do this with two points (since a line in general intersects three points on the cubic). We can consider a point and itself (intersecting twice).
- Why is a cubic curve not $\mathbb{P}^1$? What does that even mean? Maybe it will have a different genus (well, over $\mathbb{C}$. What about other fields?), but we'll have to make that precise.

5. Cubics: 1/14/15

"In freshman calculus, we don't ask them this, because their heads would explode."

Finite fields are kind of weird: $\mathbb{P}^1_{\mathbb{F}_q}$ is just a set of $q+1$ points; unlike $\mathbb{P}^n_{\mathbb{C}}$, it's a lot harder to see what the geometry is. Assume $\mathrm{Char}(\mathbb{F}_q) \neq 2$.

But we can certainly ask questions such as, how many solutions to $x^2 + y^2 = z^2$ are there in $\mathbb{P}^2_{\mathbb{F}_q}$? One solution is $[1,0,1]$, and another is $[0,1,1]$. If q is a prime, then we can use quadratic residues to do this, and in general one can push this up to prime powers. But let's do exactly the same thing as we did over $\mathbb{Q}$: let's consider the set of lines through our first solution $[1,0,1]$, and then we can consider the slopes, which must be rational. This is an interesting point, because it gives us geometry in something that seems a little ungeometric (it's really a scheme, but we'll talk about that later), and this geometric method is in some sense a little more general than the number-theoretic one, as it works over any field.

If q is prime, we can prove that there's at least one solution to $x^2 + y^2 = \ell$ for some $\ell \in \mathbb{F}_q$ (which is useful for finding that initial solution). Half of the nonzero numbers are quadratic residues, so there are $(q-1)/2$ squares, but then we add 0, which is its own square, i.e. $(q+1)/2$ numbers in $\mathbb{F}_q$ are squares. But this is just over half, so just over half of the elements of $\mathbb{F}_q$ are of the form $k - x^2$, and just over half are of the form y^2, so there must be an overlap by the Pigeonhole Principle.

Exercise 5.1. More generally, let $p(x,y,z)$ be a conic in $\mathbb{P}^2_{\mathbb{F}_q}$, where q can be any prime power. Must p have a point?

Returning to cubics, let's consider a cubic in $\mathbb{P}^2$ which looks something like $zy^2 = x^3 + axz + bz^3$, or its affine version $y^2 = x^3 + ax + b$. At some point, we can talk about smoothness conditions on these; there's a $\mathbb{P}^9$ of cubics just by looking at the coefficients, but this includes nonsmooth and degenerate conics. Thus, there's a $\mathbb{P}^8$ of cubics passing through a given point, and a $\mathbb{P}^8$ passing through two given points, and so on, assuming general position. Given eight points in general position, we have a $\mathbb{P}^1$ of cubics, literally a 2-dimensional vector space, or, taking a basis, two cubics $p(x,y,z)$ and $q(x,y,z)$ that are linearly independent, and both vanish on the eight specified points.

We expect p and q to intersect at $3 \times 3 = 9$ points in general (which is Bézout's theorem, though we still haven't proven it yet). Thus, we get an interesting conclusion: eight points determine two linearly independent cubics (in the sense that it determines the space spanned by them), and therefore determine the nine points they intersect at! So given eight general points, there's a unique ninth point given by drawing the two cubics.

One interesting thing to think about is the $\mathbb{P}^1$ of cubics (or conics for simplicity) passing through eight (fewer for conics) points; how do they vary as one moves through $\mathbb{P}^1$? There are a few transition points, e.g. self-intersection or cusps. One kind of transition occurs 12 times, and for some reason the number 12 appears all over the place in elliptic curve theory.

Let's talk about tangents. Given a plane curve, e.g. $y^2 = x^3 + ax + b$, or more generally $f(x,y) = 0$, we can take the partial derivatives $f_x(x,y)$ and $f_y(x,y)$ to determine the direction and slope of a tangent vector. But what do we do if they're both zero? That would involve dividing zero by itself, which is a problem... so we just say that it's not smooth. There (bam!) is the definition of smoothness for plane curves. It sounds like cheating, but if you try to convince me that it's cheating, you won't succeed.

This is a nice definition in general, but it seems weird taking partials over positive characteristic; we're used to invoking things called δ and ε, but the rule $3x^5 \mapsto 15x^4$ doesn't depend on the base field (though it's a little weirder if the characteristic is 5, where $x^5 = x$ and $5x^4 = 0$). Some of these things depended on the base field being algebraically closed, but in general one can work in a suitably large finite extension.

What is a polynomial? We're used to using them as functions, but defining them as formal expressions, which is a problem over finite fields, and even over $\mathbb{R}$, how do we *a priori* know that two polynomial expressions give us different functions? In infinite fields, we can choose more points than in their degree (overdetermined, in some sense), but in finite fields it may be an issue, e.g. polynomials that vanish anywhere. This small thing will grow up to an important problem.

If R is any ring, we have to define $R[x]$ as a sequence of points in R, with certain rules for addition and multiplication. It's nice that we can evaluate it at points, but totally not what we expected.

We wanted to talk about addition on elliptic curves, but that's ok; we'll get back to it. Let's return to the mysterious fact that for cubics, a general set of eight points (but not all such sets) determines a ninth.

Given a cubic $y^2z = x^3 + axz^2 + bz^3$ in $\mathbb{P}^2$ over an algebraically closed field (or just over $\mathbb{C}$), we can turn it into a group. The curve intersects the point at infinity once (in the y-direction), and we'll call that the 0 of the group law.

But a line in general position intersects three points of the elliptic curve, since it's a cubic, so given any two points A and B on the curve, a line containing them is unique and intersects a third point $-A-B$. Reflect it across the y-axis, and the result can be called $A+B$. We'll call this addition; it's clear that it is commutative, but that's about it. Thus, any three collinear points are thought of as adding to zero.

The line through A and A is interpreted as the tangent line (since we saw that this can be thought of as a double intersection), and the negative of a point can be thought of as its reflection across the y-axis, so that the line through A and $-A$ rockets off to infinity, i.e. 0 (so $A+(-A)=0$).

Theorem 5.2. *This operation is an abelian group on the zero set of the elliptic curve.*

We basically have to show associativity; everything else has been accounted for. This will be hard, because we'll have general coordinates that may differ at different sections of the curve, and we have to do some messy algebra to show this is independent of coordinates. Is there a better way to do this? Stay tuned.

6. The Elliptic Curve Group and the Zariski Topology: 1/16/15

"If I put a gun to your head, would you be able to prove it?"

Let's begin by proving that the elliptic curve group law is associative, which is basically the only meat in the construction of the elliptic curve group law. We will assume that the curve is smooth.

We should mention exactly what we're constructing the group law on: the points of an elliptic curve in $\mathbb{P}^2_k$. In $\mathbb{C}$, this is equivalent to modding out by a lattice Λ, and the quotient group inherits the group structure from $\mathbb{C}$ (there's some stuff dealing with the Weierstrass $\wp$-function, but we won't digress into that). This is the same as the group law that we defined, but it will be nontrivial to prove that.

Proof of Theorem 5.2. Recall that given points A and B, $A+B$ is defined by taking a line joining A and B, and then reflecting the third intersection point across the y-axis (i.e. joining it with O, the point at infinity). To add three points A, B, and C, do something similar: draw out the lines, so that any two points determine a third. This is a little sketchy,[3] but it is a nice visualization as to why this ought to work. In particular, we can simplify to showing that $-(A+B)-C = -A-(B+C)$, since then adding with O will be the same.

Let's consider the cubic through the points A, B, $-A-B$, C, A, $B+C$, $-B-C$, and 0. This can be drawn in two ways (three lines through A, B, and $-A-B$; C, $A+B$, and $-(A+B)-C$; and $B+C$, $-B-C$, and O; or alternatively, A, $B+C$, and $-(A+B)-C$ and so on). Thus, since any eight points determine a ninth, $-(A+B)-C$ and $-A-(B+C)$ are the same ninth point, so they must be equal. □

There's a more algebraic (and more rigorous) way to do this, in which everything is computed with algebra and polynomials. But it takes a lot of rote computation and paper, and is a bit unpleasant. There will be special cases for multiple intersections. So right now, we have a mostly defined map $E \times E \to E$. There are little issues with adding a point to itself, which boils down to saying the right thing. For example, when we want to add (u,v) and (s,t) to get (x,y), when the two points are distinct, we get $y = (v-t)(x-u)/(u-s)$, but what if they're the same? One can write down another rule for that case, which looks more like the tangent line, as we talked about last time.

Question. Can you write down a more unified law for the algebraic formula for this group operation? Ideally, it will be a "nice" map (whatever that means).

One way to do this is to show that the tangent line is the limit of secant lines, but this also is true in an algebraic set as well.

Note that we had an assumption of continuity, allowing this to be formalized with deltas and epsilons. So what do we do more generally? One can define the group law algebraically, with two solutions to a curve in a certain way determining a third.

But it helps to have some topology on this curve. Let's quickly review what this entails: recall that in a metric space X, we have a collection of open subsets $U \subset X$, such that:

- arbitrary unions of open sets are open,
- finite intersections of open sets are open, and
- $\emptyset$ and X are both open.

Then, one defines closed sets as the complement of open sets. This can be generalized to the notion of a *topological space*: a set X and a collection of open sets $U \subset X$ satisfying these properties, so that metric spaces (and any real or complex manifolds, and a great many spaces besides) are topological spaces.

[3] No pun intended.

Maps between topological spaces are *continuous maps*, which are functions $f : X \to Y$ such that the preimage of every open subset of Y is open in X.

Anyways, we want to generalize to things other than $\mathbb{C}$, but we'll stick with algebraically closed field (including those of positive characteristic, such as $\overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$). Finite fields will still be confusing for now, but we can prove associativity by passing up to $\overline{\mathbb{F}_p}$. We had a topology on $\mathbb{C}$, and we'll want to put one on $\overline{\mathbb{F}_p}$, so that we can bring it to a given elliptic curve.

Suppose we have a curve such as $y^2 = x^3 + x^2$, which intersects itself at the origin. Let's take out the origin, which is a singularity. But what's left (over $\mathbb{C}$) is $\mathbb{P}^1$ where ∞ and 0 are thrown out, so we get $\mathbb{C} \setminus \{0\}$ (which is a multiplicative group), and it turns out the group laws coincide! Similarly, if $y^2 = x^3$, then we topologically get a sphere, so when we throw out a point, we get $\mathbb{C}$, and the group law of $(\mathbb{C}, +)$ and this elliptic curve coincide too!

This relates to something called Pappus' theorem: take two lines ℓ and m, and pick three points on each line. Then, draw all six lines between pairs of points on different lines; they intersect at three points, which the theorem says are collinear. Pascal's theorem generalizes this to any conic, and it's interesting to see how this relates to the associativity law of cubics. Let's speak more generally. Over $\mathbb{C}^n$, or even over any k^n, we can consider points $(x_1, \dots, x_n)$ as solutions

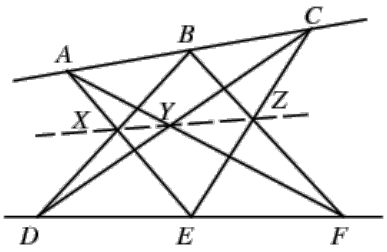


FIGURE 4. Depiction of Pappus' theorem: if A, B, and C are collinear and D, E, and F are collinear, then X, Y, and Z are collinear. Source: http://mathworld.wolfram.com/PappussHexagonTheorem.html.

to polynomials in n variables, which live in $k[x_1, \dots, x_n]$. Given polynomials $f_1, \dots \in k[x_1, \dots, x_n]$, we can define $V(f_1, \dots)$ as the points which are the zeroes of every specified polynomial. But since linear combinations of polynomials preserve their mutual zeroes, we might as well consider the ideal generated by the specified polynomials.

So the map V sends ideals of $k[x_1, \dots, x_n]$ to subsets of k^n: this is a map from algebra to geometry. We can use this to put a topology on k^n by defining the *closed* sets to be of the form $V(I)$ for some ideal $I \subset k[x_1, \dots, x_n]$. (It feels weird to start with the closed sets, but that's the way it works.) Why is this a topology?

- $\emptyset = V(1)$ and $k^n = V(0)$.
- We want to check that finite unions of closed sets are closed, so $V(f) \cup V(g) = V(fg)$ (and then by induction, this is generalized to arbitrarily large finite unions).
- To show that arbitrary intersections of closed sets are closed, we can do the same thing with sums (of ideals or of functions).

This topology on k^n is called the *Zariski topology*. One weird thing about it is that larger ideals correspond to smaller sets.

Definition. A *basis* for a topology is a collection of (nice) open sets such that every open set in the topology is a union of sets in the basis.

In a metric space, open balls are a basis for the topology, and in the Zariski topology, the complements of zero sets of a single function, $k^n \setminus V(f)$, are the basis, because every $V(I)$ is determined by its generators.

Here's a useful result which isn't particularly intuitive.

Proposition 6.1. *Every closed set on k^n is cut out by finitely many polynomial equations.*

To make sense of this, we need to describe how to break a zero set into "pieces."

Definition. A closed subset X of a topological space is *irreducible* if one cannot write $X = Y \cup Z$ for closed Y and Z, where neither Y nor Z is all of X.

This really only makes sense in weird toplogies like Zariski's. An interesting example of a closed subset is k^n, though a line or a curve is as well. It's similar to the idea of a *connected component* (maximal connected subset, i.e. can't be written as the disjoint union of two *clopen* subsets), though the two aren't the same notion.

We'll prove Proposition 6.1 by showing that every closed subset has finitely many irreducible components. This ultimately follows because for any ideal $I \subset k[x_1, \dots, x_n]$, I is finitely generated, and those generators cut out $V(I)$. This leads to the notion of a *Noetherian ring*.

7. Affine Varieties and Noetherian Rings: 1/21/15

"I said it in English so you probably have no idea what I'm talking about, but I'll say it again in mathspeak in a second."

One interesting fact about cubics is that if one has a cubic with a point p where a line meets it with multiplicity 3 (a *flex line*), one can send it to a point at infinity $[0,1,0]$. This simplifies it by killing the terms in y when $z=0$ (that is, setting $z=0$ tells us about the point at infinity). In particular, this leads to a curve $yz = ?x^3 + ?x^2z + ?xz^2 + ?z^3$, but by choosing x to be a suitable multiple of z and rescaling, we have $y^2z = x^3 + ?xz + ?z^3$. In particular, in dehomogenized form, every such cubic can be transformed into $y^2 = x^3 + ax + b$, and elliptic curve.

Question.

- Geometrically, what does it mean for a point on a cubic to be a flex point?
- How many flex points are there on a smooth cubic, given that there is at least one?

For the latter question, over $\mathbb{C}$ we can think of an elliptic curve as $\mathbb{C}/\Lambda$, where Λ is a lattice, and therefore one can deduce that there are nine flex points (which are the points of order 3), but that's not immediate right now.

Another question, which may come up on a problem set: suppose we have a smooth cubic with a flex point, and let p and q be any points on a cubic. Starting with a point $\widehat{r}$, the line joining $\widehat{r}$ to p passes through the cubic once more, at $\widetilde{r}$, and the line through $\widetilde{r}$ and q intersects the cubic once more, at some r_1. Repeating with r_1 in place of $\widehat{r}$, and so forth, consider how many iterations it takes to return to $\widehat{r}$. This depends on p and q, and *a priori* on $\widehat{r}$, but actually only depends on p and q. Why?[4] Another interesting statement to prove is that for "most" points on the cubic, the recurrence time is infinite.

Suppose I have two conics; is there an automorphism of projective space that sends one to the other? Well, this seems difficult, so let's ask a *harder* question: given two conics, each with an ordered triple of points, is there an automorphism sending one to the other that sends the first point to the first point, the second to the second, and the third to the third? It turns out this is a little more approachable; we have less freedom, so there are only a few things to try, and one of them works.

We may as well show that we can send any conic to a particular conic. First, though, we'll need to restrict to smooth conics, since not everything can be sent to $xy=0$ (which isn't smooth at the origin). So now we have something like $xy+yz+xz=0$, with the points $[0,0,1]$, $[0,1,0]$, and $[1,0,0]$. This is sufficient: at this point, $\mathbb{P}^2$ can be scaled to get this from anything of the form $?xy+?yz+?xz=0$; as long as these are nonzero, this will remain smooth.

Now, let's return to the Zariski topology and other things from last time. Specifically, we talked about the Zariski topology induced by $k[x_1,\dots,x_n]$ on k^n, where the closed sets are the zero sets of polynomial equations, and the open sets are complements of closed sets. If k is algebraically closed, this is a well-behaved notion, but otherwise it can be weird, and over finite fields, it's pretty boring.

Definition. An *algebraic (sub)set* of k^n is the vanishing set $V(I)$ of an ideal of polynomials $I \subset k[x_1,\dots,x_n]$.

Thus, these are just the closed sets.

Definition. A ring A is *Noetherian* if every ideal is finitely generated.

Proposition 7.1. *A ring A is Noetherian iff every ascending chain of ideals eventually stabilizes, i.e. if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ and all if the I_n are ideals of A, then eventually $I_n = I_{n+1}$ for all sufficiently large n.*

Example 7.2. A lot of familiar rings are Noetherian.

- All *principal ideal domains* are Noetherian, e.g. $\mathbb{Z}$ and $k[x]$.
- All fields are Noetherian, which is a little silly.

Theorem 7.3 (Hilbert basis theorem)**.** *If A is Noetherian, then $A[x]$ is Noetherian as well.*

Corollary 7.4. *$k[x_1,\dots,x_n]$ is Noetherian.*

This will end up implying Proposition 6.1 from last time: this means that every ideal $I \subset k[x_1,\dots,x_n]$ is finitely generated, i.e. every closed set $V(I)$ of k^n is cut out by the generators of I, and therefore a finite number of polynomial curves.

Proposition 7.5. *Let A be a Noetherian ring and $I \subset A$ be an ideal; then, A/I is Noetherian.*

Proof sketch. It's possible to set up a correspondence between ideals of A and ideals of A/I; therefore one can take any ideal of A/I, and pass it up to an ideal of A, where it is finitely generated. Then, passing back to A/I, it remains finitely generated. □

[4] One way to think of it intuitively involves drawing lines on a torus, which sometimes are periodic and tend not to be. It may also be worth thinking of cosets in the elliptic curve group.

Proof of Proposition 7.1. Suppose A is Noetherian; then, given a chain $I_1 \subseteq I_2 \subseteq \cdots$ of ideals of A, let

$$I = \bigcup_{k=1}^{\infty} I_k,$$

which is an ideal (which is easy to check). Then, since A is Noetherian, then I is finitely generated. Thus, there are a finite number of generators $f_1, \ldots, f_{m_n} \in I_n$ for each I_n, and since all of these generators generate all of I, then $(f_1, \ldots, f_{m_n})$ certainly generates I_n. But then, if $I_{n+1} \supsetneq I_n$, then there has to be another generator f_{m_n+1}, and one can only do this finitely many times, since there are only finitely many generators. Thus, the chain stabilizes.

In the other direction, suppose A has the ascending chain condition, and suppose I is an ideal that isn't finitely generated. Thus, if S is a generating set for I, there exists an infinite sequence $s_1, s_2, \ldots$ of distinct elements from S, and therefore a chain of ideals $(s_1) \subsetneq (s_1, s_2) \subsetneq (s_1, s_2, s_3) \subsetneq \cdots$, but this is a violation of the ascending chain condition (since each containment is strict), so I cannot exist; thus, every ideal of A is finitely generated. □

The definition of Noetherian is the thing one might think of first; the ascending ideal property is often more useful in practice.

Have you ever played a game called "Chomp!"? Imagine you have a friend and a bunch of cookies in a grid, but one of them, the one to the farthest southwest is poisoned! You and the friend can make moves by eating all cookies north of and east of a given point, and the winner wins by not eating the poisoned cookie.

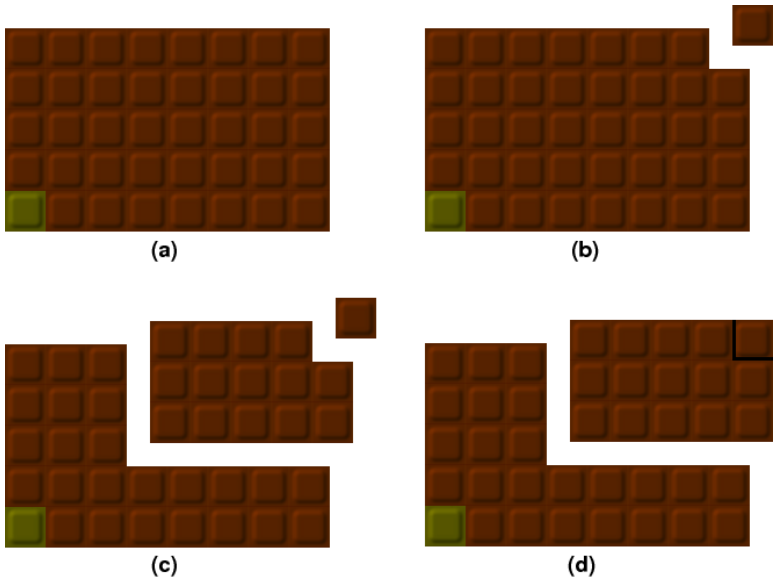


FIGURE 5. Depiction of the game Chomp, whose goal is to avoid the poisoned chocolate. Source: http://www.whydomath.org/Reading_Room_Material/ian_stewart/chocolate/chocolate.html.

Claim. The first player has a winning strategy (unless the board is 1×1).

Proof. We will give a proof without knowing what the strategy is!

Take only the cookie furthest to the northwest. Suppose this isn't a winning strategy: then, the second player wins by making some other move — but you could have won by making that move beforehand. Thus, the second player doesn't have a winning strategy, but someone has to. □

Now, we're nice to our friends, so we don't want anyone to die. Let's play with an infinite board! Then, we should think about winning strategies, etc., and can even generalize to more dimensions of cookies in the grid.

This delicious metaphor, if you think about it enough, leads to the proof to the Hilbert basis theorem.

Proof sketch of Theorem 7.3. Suppose that A is Noetherian, and let $I \subset A[x]$, which we want to be finitely generated. Then, let $I_0 = I \cap A$, I_1 be the elements of I of degree 1, I_2 be those elements of degree 2, and so on. Thus, we have a chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$.

I_0 is an ideal of A, so it's finitely generated by some coefficients $(a_{00}, a_{01}, \ldots)$. But the key is choosing in I_1 a set of generators that are the degree-1 polynomials with leading coefficients in the generating set for I_0. Using this, it's possible to finish the rest of the proof. □

Recall that we defined the notion of an irreducible component of an algebraic set, and that there are only finitely many in any closed set. It seems reasonable over $\mathbb{R}$, but over $\mathbb{C}$, who knows? But if $V(I)$ is a closed set and has infinitely many irreducible components, then each one is a distinct generator of I, and we know I is finitely generated because $k[x_1,\dots,x_n]$ is Noetherian.

Next time: localization, especially in the more general context where the ring might not be an integral domain.

8. Localization and Varieties: 1/23/15

"This follows from the Fourth Isomorphism Theorem, which is not a well-defined theorem."

Recall from last time that we defined Noetherian rings, i.e. those in which every ideal is finitely generated, or equivalently, every ascending chain of ideals is Noetherian. We proved the Hilbert basis theorem, implying if A is Noetherian then $A[x]$ is too, and the definition implies all PIDs are Noetherian. Furthermore, the ascending chain condition implies all quotients of Noetherian rings are Noetherian; thus, all finitely generated $\mathbb{Z}$-algebras and finitely generated k-algebras (when k is a field) are Noetherian, since they're of the form $A[x_1,\dots,x_n]/I$ (where $A=\mathbb{Z}$ or $A=k$).

Next, let's talk localization.[5]

Definition. If A is a ring, then a nonempty $S\subset A$ is a *multiplicative subset* of A if whenever $s_1,s_2\in S$, then $s_1s_2\in S$, and $0\notin S$.

Definition. If A is an integral domain and $S\subset A$ is a multiplicative subset, then the *localization* $S^{-1}A$ of A at S is the set of fractions a/s (well, formally ordered pairs (a,s)) for $a\in A$ and $s\in S$, under the equivalence relation that $a/s=a'/s'$ iff $as'=a's$. Using the typical rules for fraction addition and multiplication, $S^{-1}A$ is a ring.

If $S=A\setminus\{0\}$, then $S^{-1}A$ is called the *field of fractions*.

For example, if $A=\mathbb{Z}$ and $S=\mathbb{Z}\setminus\{0\}$, then we obtain $\mathbb{Q}$; if S is the set of odd numbers, we get fractions with odd denominators; if S is the set of powers of two, we get the *dyadic numbers* $a/2^n$, with $a\in\mathbb{Z}$. But if S is the set of even numbers, we just get all of $\mathbb{Q}$ again, since 3/5 is really just 6/10.

We want to be able to do this when A is more generally any commutative ring, but we have to be more careful. For example, if $A=\mathbb{Z}/6$, then $S=\{2,4\}$ is a multiplicative subset. Then, $3/2=0/4=0$, and therefore $3=0$, which is weird, but not fatal; $S^{-1}A\cong\mathbb{Z}/2$. The most important bit is that $1/1\neq 0/1$, so it's not all that weird.

We'll need to modify the definition for more general A just slightly: we'll consider $a/s=a'/s'$ iff $s''(as'-a's)=0$ for some $s''\in S$. This is necessary because otherwise, the equivalence relation isn't transitive, and addition doesn't end up working right. Specifically, if $a's=as'$ and $a's''=a''s'$, then we don't know that $as''=a''s$ unless we multiply by s' on both sides. In Math 210A, there's a more universal way of addressing this, and here, we make a definition that may look a little arbitrary; stay tuned.

One goal is to always have a map $A\to S^{-1}A$ sending $a\mapsto a/1$ (or if $1\notin S$, then pick an $s\in S$ and send $a\mapsto sa/s$, which ends up being well-defined). This is a useful thing to keep in mind.

For a more general version of the $\mathbb{Z}/6$ example, let's take a ring A and the multiplicative subset $S=\{1,f,f^2,\dots\}$ for some $f\in A$. Thus, $S^{-1}A$ is the set of a/f^i, where $a/f^i=b/f^j$ if $f^D(f^ja-f^ib)=0$. We can think of this as formally adding an element equal to $1/f$, and in fact on the homework we'll see that $S^{-1}A\cong A[x]/(xf-1)$. It looks weird, but try it in the case $\mathbb{Z}/6\to(\mathbb{Z}/6)[x]/(2x-1)$.

For one last example, what happens when $0\in S$? Then, since $0a=0b$ for all b, then everything gets killed, and localizing creates the zero ring. Oops. We know how to divide by zero, sure, but all the numbers go away.

Exercise 8.1. What is the relationship between the primes (i.e. prime ideals) of A and the primes of $S^{-1}A$? Specifically, describe the bijection between primes of A not meeting S and the primes of $S^{-1}A$. This is exactly what you think it is, and plays well with respect to sums, products, etc.[6]

This is nice to know, but once you do it once there's no need to look at the proof again; then, you can use it again.

Corollary 8.2. *If A is Noetherian and S is a multiplicative subset, then $S^{-1}A$ is also Noetherian.*

This nice result follows because of the relationship between ideals of A and ideals of $S^{-1}A$.

Varieties. Recall that we defined the vanishing set of an ideal $I\subset k[x_1,\dots,x_n]$: given an ideal I, we get its zero set $V(I)\subset k^n$. (Here, k is algebraically closed.)

Now, we want to go in the other direction: given a subset $S\subset k^n$, let $I(S)=\{f\in k[x_1,\dots,x_n]\mid f(x)=0 \text{ for all } x\in S\}$. $I(S)$ is exactly the ideal of polynomials that vanish on S. This is obviously an ideal, because two functions that vanish on a set can be added and still vanish, and similarly for the absorption property.

[5] Sometimes spelled "localisation," depending on your religion.

[6] Apparently this problem was on a Math 210A problem set last quarter, and also on a Math 210B problem set due today.

For example, if S is the x-axis, then $I(S)$ is the set of multiples of y (since k is algebraically closed and therefore infinite, then any nonzero polynomial has some point at which it doesn't vanish). Similarly, if $S = \{(n,0) \mid n \in \mathbb{Z}\}$, then since each polynomial vanishes at only finitely many points, then $I(S)$ is once again the set of multiples of y.

One interesting thing is that since k is an integral domain, then if f^2 vanishes at a point, then f must vanish at k as well.

Definition. The *radical* of an ideal I in a ring A is the ideal $\sqrt{I} = \{f \in A \mid f^n \in I \text{ for some } n > 0\}$. If $I = \sqrt{I}$, then I is said to be *radical*.

Totally radical, dude!

This is an ideal,[7] because if $g^m, h^n \in I$, then $(g+h)^{m+n} \in I$ (expand out the terms, as they'll always have either g^m or higher, or h^n or higher).

Notice that if $S \subset k^n$, then $I(S)$ is radical.

So now we have a correspondence between subsets of k^n and ideals of $k[x_1, \ldots, x_n]$ given by V and I, though not every subset is in the image of V, and not every ideal in the image of I.

Claim. If $S \subset k^n$, then $V(I(S)) = \overline{S}$, i.e. the closure in the Zariski topology.

Proof. Certainly, $V(I(S))$ is closed, since V of anything is closed. But if S is closed, then $S = V(J)$ for some J, and therefore $I(S) \supset J$ (which is a little weird, based on a definition chase), and therefore $S \subseteq V(I(S)) \subseteq V(J) = S$, i.e. (oh dear) $I(S) \supset I(V(I(S))) \supseteq I(V(J)) = I(S)$. □

But since $I(S)$ is always radical, then this bijection of algebra is really between Zariski-closed subsets and radical ideals.

We still haven't used the fact that k is algebraically closed, but we will soon.

Definition. The *nilradical* of a ring A is $\mathfrak{N} = \sqrt{0}$, i.e. the ideal of all nilpotents.

That's a `\mathfrak N`, in case you were wondering.

Lemma 8.3. *The nilradical is the intersection of all prime ideals of A.*

Proof. Let P be a prime ideal, and suppose $f \in \mathfrak{N}$; then, $f^n = 0$ for some N, and therefore $f^n \in P$, so $f \cdot f^{n-1} \in P$, and therefore one of f and f^{n-1} are (if the latter, repeat, and we'll end up at f eventually).

In the other direction, suppose $f \notin \mathfrak{N}$, and we want to find some prime ideal not containing f. Well, localization is useful: let A_f denote localization at all powers of f; then, since f is not nilpotent, then A_f is not the zero ring, as $1/1 \neq 0/1$, because $1 \cdot f^N \neq 0 \cdot f^M$ for all M, N.

Now, things get weirder: consider the set of all ideals of A_f (i.e. those ideals not containing f back in A, using the correspondence we discussed earlier); these are partially ordered by inclusion, and by Zorn's lemma, there's a maximal element, and we can prove that it's prime in A. □

Even though we're invoking the Axiom of Choice, any ring that you and I will write down will almost certainly have an explicit example, without relying on the Axiom of Choice, and certainly this is true for applications to the real world, e.g. Fermat's Last Theorem.

Localization seems like it was pulled out of a hat here, but doing something like this (or the alternative version, quotienting) is a very common way to reduce or solve problems.

Exercise 8.4. If $I \subset A$ is an ideal, then $\sqrt{I}$ the intersection of all prime ideals containing I.

9. Hilbert's Nullstellensatz: 1/26/15

"Never look at Lang."

We're now really getting to the crux of the idea of algebraic geometry: a dictionary between algebra and geometry, with geometry providing a lot of motivation for what we're doing. Here's the correspondence we know so far.

- Subsets of k^n (geometry) correspond to subsets of $k[x_1, \ldots, x_n]$ (algebra), with maps between them.
- More specifically, we have closed subsets of k^n corresponding to ideals of $k[x_1, \ldots, x_n]$, with the map V going from ideals to subsets.
- The map I going from subsets of k^n to ideals means the correspondence goes between closed subsets of k^n and radical ideals. Certainly, we get all closed subsets; do we get all radical ideals? We will soon see that we do, at least when k is algebraically closed.

Recall that a radical ideal I is such that $I = \sqrt{I}$, i.e. if $a^n \in I$ for some n, then $a \in I$. $\sqrt{I}$ is also (as will be proven on the next problem set) the intersection of all primes containing I.

[7] "I thought radical ideals were a thing of the 70s" – Boris Perkhounkov

Question. Show that a closed subset $S \subset k^n$ is irreducible iff $I(S)$ is prime.

This is on the homework, but let's look at one direction, since it illustrates the effectiveness of this dictionary. Suppose $I(S)$ is not prime; then, there exist $f, g \notin I(S)$ such that $fg \in I(S)$. Thus, $V(f)$ and $V(g)$ are subsets of S (since I and V are inclusion-reversing).

Claim. $V(I)$ is irreducible iff I has exactly one minimal prime ideal containing it.

This is intuitively true, but let's leave something left on the homework.

Returning to the question, since $fg \in I(S)$, then $S \subset V(fg) = V((f) \cap (g)) = V(f) \cup V(g)$. But $V(f)$ and $V(g)$ are closed sets that cover S, and $V(f), V(g)$ don't cover S, because $f \notin I(S)$, so f doesn't vanish on all of S (and g is the same); thus, $I(S)$ decomposes as $V(f) \cup V(g)$, and therefore is reducible.

Irreducibility feels very geometric, and primacy very algebraic, but they're instances of the same notion.

Now, we know that if $S \subset k^n$ is closed, then $V(I(S)) = S$, and if J is in the image of I, then $I(V(J)) = J$. But what's the image of I? This is a little difficult question, and leads to Hilbert's Nullstellensatz.

One way to characterize a prime ideal $\mathfrak{p}$ of a ring A is that $A/\mathfrak{p}$ is an integral domain; similarly, if $\mathfrak{m}$ is a maximal ideal, $A/\mathfrak{m}$ is a field. This is a useful characterization; for example, since fields are integral domains, all maximal ideals are prime. Additionally, $(x_1 - a_1, \dots, x_n - a_n) \subset k[x_1, \dots, x_n]$ is maximal, because the quotient is k, (the quotient map is evaluation at $(a_1, \dots, a_n)$). If k isn't algebraically closed, we may have others, e.g. $(x^2 + 1)$ if $k = \mathbb{R}$.

Theorem 9.1 (Hilbert's Nullstellensatz)**.** *Suppose k is algebraically closed. Then,*

(version 1) *If $I \subset k[x_1, \dots, x_n]$ is an ideal, then $I(V(I)) = \sqrt{I}$.*
(version 2) *If $V(I) = \emptyset$, then $I = k[x_1, \dots, x_n]$.*
(version 3) *The only maximal ideals of $k[x_1, \dots, x_n]$ are $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$.*

Proof sketch. We can see that (2) implies (3), because if we have an additional kind of maximal ideal, then it must vanish nowhere, but therefore it is $k[x_1, \dots, x_n]$, and therefore not really a maximal ideal.

Exercise 9.2. Show that if $(a_1, \dots, a_n) \in V(I)$, then $I \subseteq (x_1 - a_1, \dots, x_n - a_n)$.

This is the kind of proof where, once you unravel the definitions, it's pretty easy; furthermore, it means that (3) $\implies$ (2).

Now, why does (1) imply (2)? Every function vanishes at $\emptyset$, so if $V(I) = \emptyset$, i.e. $I(V(I)) = k[x_1, \dots, x_n]$, and therefore $I = \sqrt{k[x_1, \dots, x_n]}$ — but since $1 \in k[x_1, \dots, x_n]$, then the entire ring is a radical ideal. Thus, I is the whole ring.

To see why (2) implies (1), suppose $I \subset k[x_1, \dots, x_n]$, so we know $I(V(I)) \supset \sqrt{I}$. Suppose $f \in I(V(I))$; then, let's localize at f, looking at $A_f = A[y]/(yf - 1)$ ($S = \{1, f, f^2, \dots\}$). Then, $V(f) \supset V(I)$. Now, consider I as an ideal of A_f (same generating equations), but we know that we're forcing $f = 0$ whenever we're in I (since $f \in I(V(I))$, and that's exactly what it means), so this ideal has to be empty in A_f, since $1/f = y$ is not zero. This is weird, which is why it's known as Rabinowitsch's trick.[8] Thus, by part (2), the ideal $(I, yf - 1) = 0$, and therefore its vanishing polynomials are the whole ring. Since $f = 0$ in $(A/I)_f$, then $fs = 0$ for some s in the multiplicative set, i.e. $s = f^N$; thus, $f^N = 0$ in A/I, so $f \in \sqrt{I}$ (since $f^N \in I$ in A).

Now, we only have to prove one of them, and we're done! This will be an exercise. □

We've now defined *algebraic subsets* (that is, closed subsets) of n-space, corresponding to radical ideals of the polynomial ring. Then, we want to talk about maps of objects, which will be related to maps of rings. Thus, next time we'll completely describe the category of affine algebraic varieties, leading to the notion of schemes.

10. Affine Varieties: 1/28/15

"It's unnerving when Brian Conrad says you're being insane in a class."

Today we'll get to defining the category of affine varieties, and — this is the insane part — affine schemes.

Remember that last time we discussed Hilbert's Nullstellensatz, which comes in three equivalent forms for an algebraically closed field k: that for all ideals $I \subset k[x_1, \dots, x_n]$, $I(V(I)) = \sqrt{I}$; that if $V(I) = \emptyset$, then $I = k[x_1, \dots, x_n]$; and that the maximal ideals of $A = k[x_1, \dots, x_n]$ are $(x_1 - a_1, \dots, x_n - a_n)$.

Why did we do this? Really for the following reason: we have a dictionary of algebra and geometry, which is only going to get more and more connected. Algebraic subsets $S \subset k^n$ correspond (one-to-one) to radical ideals $I(S) \subset A$, and vice versa via V. Within this correspondence, prime ideals correspond to irreducible closed subsets of k^n, and maximal ideals in A correspond to points in k^n, thanks to the Nullstellensatz.

[8] It isn't well-known who Rabinowitsch was, or even how to agree on a spelling of his (her?) name. But according to Wikipedia, s/he was a pseudonym of a Russian mathematician, George Yuri Kainich. http://en.wikipedia.org/wiki/Rabinowitsch_trick.

It's sort of weird, because larger ideals correspond to smaller subsets. This is the nature of an inclusion-reversing correspondence, and it'll be possible to get used to it. There are other useful conseqeunces, e.g. $\sqrt{IJ} = \sqrt{I \cap J}$.

We almost know what affine varieties are, but we need to define the morphisms.

Definition. Let Z be a Zariski-closed subset of k^n; then, the *set of functions* on Z is the set of restrictions of polynomials in $k[x_1, \dots, x_n]$ to Z.

This sounds stupid, but it means that if $Z = V(I)$, with I radical, then this set of functions is just $k[x_1, \dots, x_n]/I$, because if $f = g$ when restricted to Z, then $f - g = 0$ on Z, i.e. $f - g \in I$. There's a little more to say here, but this is the reason the definition exists.

This is the building block that allows one to define functions between two algebraic sets, not just $Z \to k^n$.

Definition. A *map* (or *morphism*) of algebraic sets $X \hookrightarrow k^m$ to $Y \hookrightarrow k^n$ is given by maps of n polynomials in m variables, restricted to X, such that the image stays in Y.

These are the right kinds of maps because functions on Y pull back to functions on X.

It may seem like we've left projective space entirely; this is the affine story. But we'll be able to return to them eventually; just like one studies manifolds by first studying patches of $\mathbb{R}^n$, these are the ingredients we will use to create more powerful structures.

Example 10.1. Consider the hyperbola given by $uv - 1 = 0$. The ring of functions here is $k[u,v]/(uv-1)$.[9] Then, consider $xz - y^2 = 0$, and send the former to the latter by $(u,v) \mapsto (u, u^2, u^3)$. See Figure 6.

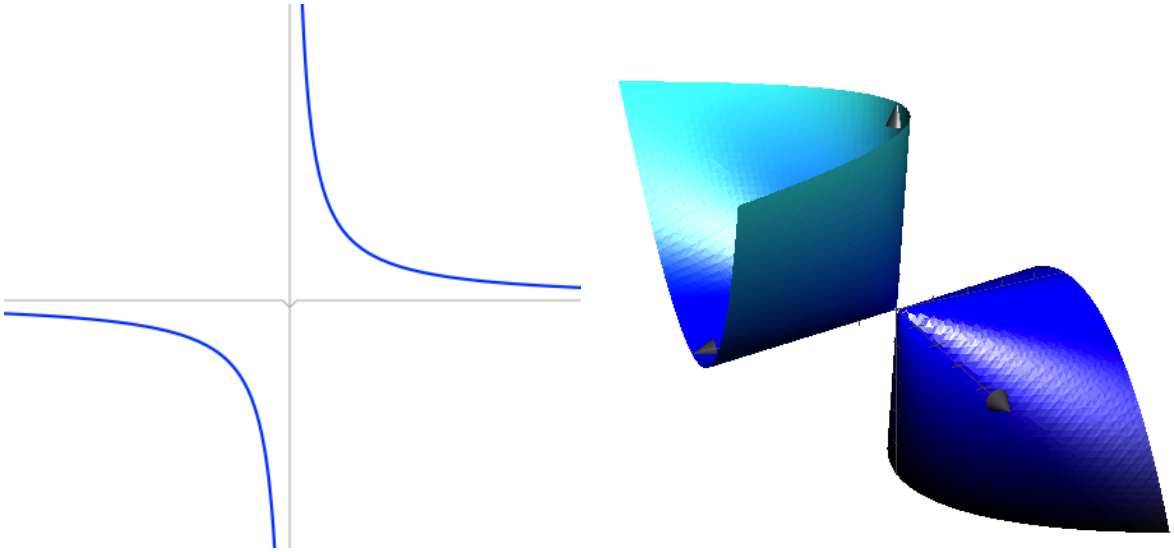


FIGURE 6. Depiction of the varieties of a polynomial map $(u,v) \mapsto (u, u^2, u^3)$.

Thus, there's an induced ring homomorphism (actually, k-algebra homomorphism) $k[x,y,z]/(xz - y^2) \to k[u,v]/(uv-1)$ given by $(x,y,z) \mapsto (u, u^2, u^3)$. Notice that this map goes in the opposite direction.

From one of these, you should be able to understand the other: every step is OK, but the whole thing can seem kind of confusing.

For a different example, suppose we send $k[x,y]/(y^2 - x^3) \to k[t]$ by $x \mapsto t^2$ and $y \mapsto t^3$. This can be recast into a map from the line to the cubic $y^2 = x^3$.

If you want more examples, just try stuff and see where it goes.

Theorem 10.2. *Suppose $I \subset k[x_1, \dots, x_m]$ and $J \subset k[y_1, \dots, y_m]$ are ideals. Then, the set of maps $V(I) \to V(J)$ is the same as maps $k[x_1, \dots, x_m]/I \leftarrow k[y_1, \dots, y_m]/J$.*

Now, we have enough to talk about a category, using fancy language that you can impress your friends with. Informally, a *category* is a collection of stuff, with some stuff that looks like maps, i.e. there's an identity map, and maps compose. Cool. For example, vector spaces with linear maps form a category.

Thus, given an algebraically closed field k, we can define the *category of affine varieties* over k, which is the set of algebraic subsets of k^n (for all possible n), with the polynomial maps given above as its morphisms.

[9] This happens to be equal to $k[u, 1/u] = k[u]_u$, which is not a coincidence.

Given a category C, one can define the *opposite category* C^{opp} by reversing all of the arrows (or functions), but keeping the objects the same.

Thus, Theorem 10.2 above tells us that the category of affine subsets of k^n is equivalent (in some categorical sense) to the opposite category to the category of rings $k[x_1,\dots,x_n]/I$ when I is radical, and, more generally (where we relax notions of generators), the category of affine varieties is the opposite category to the category of finitely generated k-algebras where 0 is radical (i.e. no nilpotents).

One important point is that we're being agnostic about generators; just as in theoretical linear algebra, one is careful to avoid questions about bases, even though people are usually brought up to think of linear functions as matrices, where a basis comes along for the ride. Thus, we'll try not to worry about generators, just as in linear algebra. The notion is that the dual (space of functions) on a vector space V is isomorphic, but not canonically, just like affine varieties and finitely generated k-algebras.

11. Affine Schemes: 1/30/15

Recall that the *algebraic (sub)sets*, or *affine varieties* of k^n are just those closed under the Zariski topology. When k is algebraically closed, the Nullstellensatz guarantees that polynomials are determined by their values (up to radical ideals), even on affine varieties, which is nice.

Given an algebraic set S, we define its ring of functions on the set to be the functions, restricted to that set, so modded out by the functions vanishing on that set: this is just $k[x_1,\dots,x_n]/I(S)$. We also defined maps from one algebraic subset $S = V(I) \subset k^m$ to another, $T = V(J) \subset k^n$, there is a bijection between maps of rings $k[x_1,\dots,x_m]/I \leftarrow k[y_1,\dots,y_n]/J$ and maps $S \to T$, reversing the direction of the arrows, and of course composition plays nicely with this correspondence. Thus, this is a *contravariant functor*, if you want to impress your friends with categorical language.

Proving this is a little weird, since there's almost nothing to say, but one still has to figure out why.

Exercise 11.1. If $k \mapsto k^3$ sends $t \mapsto (t, t^2, t^3)$, what is the map in the other direction? Prove that this is isomorphic onto its image.

The contravariant functor above is a mapping between the categories of algebraic subsets of k^n and the finitely generated, nilpotent-free k-algebras (i.e. $k[x_1,\dots,x_n]/I$ for some ideal I) with n chosen generators. This is only saying the above content. (Technically, one needs to reverse the arrows, so it's the opposite category.)

But we can define affine varieties in general; it's not as natural to embed it in space in a certain way, or to pick generators for a nilpotent-free k-algebra that may have more than one choice of generator. Thus, our contravariant functor can be more generally thought of as mapping between affine varieties and (the opposite category of) finitely generated, nilpotent-free k-algebras.

There's some notion that affine varieties are more or less the same as finitely-generated (nilpotent-free) k-algebras — so sometimes, people define affine varieties as finitely-generated, nilpotent-free k-algebras! Then, the geometric description comes from picking generators and applying the functor. It seems weird, but there's no good argument against it. There's a lot of things here which seem like tautologies, but are restatements in important ways. Later on, we'll be able to add back in nilpotents. Even now, zero divisors are allowed, so long as they aren't nilpotent.

Example 11.2. For example, $k \times k$ is a finitely generated k-algebra, where $(x_1,x_2)\cdot(y_1,y_2) = (x_1x_2, y_1y_2)$, which is generated by $(1,0)$ and $(0,1)$. Thus, we ought to be able to draw a picture of it in k^2.

On the algebra side, the goal is to find an I such that $k \times k \cong k[x,y]/I$. The relations are $xy = 0$, $x^2 = x$, $y^2 = y$, and $x + y = 1$, so $I = (xy, x^2 - x, y^2 - y, x + y - 1)$, which geometrically looks like the intersection of these curves, which is two points. More generally, if R_1, R_2 are two rings, then the geometric realization of $R_1 \times R_2$ is the union of the realizations of R_1 and R_2.[10]

Anyways, maybe it's possible to have fewer generators, since the two points are collinear. The Chinese remainder theorem shows that it's the same as $k[t]/(t(t-1)) \cong k[t]/t \times k[t]/(t-1)$. Notice how the Nullstellensatz is hidden in this: t and $t-1$ are relatively prime, so this works, but relative primeness is equivalent to $1 \in (t(t-1))$ by the Nullstellensatz.

Now, we'll do the thing we weren't supposed to do: to define affine schemes, taking this equivalence between algebra and geometry to a radical[11] level, including many more kinds of rings.

For example, what should one do for working with varieties over a field k where $k \neq \overline{k}$? One reasonable idea is to work in $\overline{k}$ anyways, so that the Nullstellensatz still holds, and then interpret the results in k^n. There's a whole theory here, with lots of words like Jacobson ring, and so forth.

The Nullstellensatz has a nice interpretation, though: in $\mathbb{R}[x]$, (x^2+1) is maximal, and $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, so (x^2+1) corresponds to the points i and $-i$, both at once: they can't be separated. This worked well enough into part of the 20th Century.

[10] Another interesting fact, which we'll get to later, is that $R_1 \otimes R_2$ corresponds to the Cartesian product of the varieties.

[11] No pun intended.

Now, though, one can generalize to any ring A. Even when $A = k[x_1, \dots, x_n]$ for an algebraically closed k, this theory is richer. According to the Nullstellenatz, maximal ideals corresponded to points, but our new definition of points is the prime ideals of A. Since maximal ideals are prime, then old points are new points too. There's nothing to prove here, since this is just a definition.

For example, on $\mathbb{Q}[x]$, there are ideals such as $(x-a)$ for $a \in \mathbb{Q}$, which correspond to points on $\mathbb{Q}$, but (x^2+1) corresponds to the points $\pm i$, glued together! And similarly, the three roots of x^3+x+1 are the three roots, glued together.

As another example, take $\mathbb{C}[x,y]$. The Nullstellensatz told us that $(x-a, y-b)$ is maximal, but (x) is prime but not maximal. This "point" is the whole y-axis. We're not quotienting or gluing the whole y-axis together, but instead, this is a *generic point*, which is on the line, but in some sense everywhere at once. It is definitely on the line, but nowhere in particular on the line.

Similarly, the ideal $(y^2 - x^3)$, which is prime (why? It's good to check), is a parabola. Or rather, it lies on that parabola, but we can't be more specific than that, and it's also a generic point. Another weird consequence of this is that the smaller points (ideals) contain the bigger points, or smaller pictures give bigger ideals. But this is just inclusion-reversing again.

And there's one more kind of prime ideal, (0). This is the smallest ideal, so it's the biggest point: it's everywhere at once, but nowhere in particular!

Finally, we can consider $\mathbb{Z}$. The prime ideals are (p) for p prime (prime numbers, that is), and (0) — which is many places at once, but also not quite everywhere.

So what happens to the ring of functions? They were given by elements of the ring back in variety-land, so here they're given by elements of A. For example, in $\mathbb{Z}$, 34 vanishes at (2) and (17); at (3), it become 34 mod $3 \equiv 1$, and at (5), it's 34 mod $5 \equiv 4$, and so on. At (0), it stays 34.

The point is, the notions of functions and vanishing are the same, but a function may take values in different places at different points. This is a little weird, but not all that weird in context of today. Vanishing at a generic point mean checking whether the ideal corresponding to the generic point contains the ideal in question. Then, vanishing creates a Zariski topology on A similar to the one on k^n.

The goal here is to build a topological object on these points, the prime ideals of A, and it will be called $\mathrm{Spec}(A)$. The Nullstellensatz has an analogue, but it's easier (that the radical of an ideal is the intersection of the prime ideals containing it). Then, given two rings A and B, a map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ can be induced by a map $A \to B$, and the reasonable way of extending it to $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ can be checked to be continuous, and therefore we have objects (there topological spaces) and morphims, describing the category of affine schemes! These make surprising things much easier.

Thus, an affine scheme is, for now, a ring, but thought of in interesting ways...

12. Regular Functions and Regular Maps: 2/2/15

Today's lecture was given by the course assistant, Donghai Pan.

Today's lecture will be the last lecture before the definition of rational functions. It will provide several definitions (regular functions and maps, coordinate rings) in the context of affine varieties.

Let k be an algebraically closed field and $X \subseteq k^n$ be algebraic.

Definition. A function $f : X \to k$ is *regular* if there is some polynomial $F \in k[x_1, \dots, x_n]$ such that for all x, $F(x) = f(x)$.

There is a difference between a regular function and a polynomial, though they are closely related.

Proposition 12.1.

(1) The regular functions form a ring $A(X)$.[12]
(2) $A(X) \cong k[x_1, \dots, x_n]/I(X)$.

The ring $A(X)$ is called the *coordinate ring* of X.

Example 12.2.

(1) Consider $p = (0, \dots, 0) \subset k^n$; then $A(p) \cong k$, with the map $k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/(x_1, \dots, x_n) \cong k$. Each function is considered to be its value at the origin.
(2) Since k^n corresponds to the zero ideal, then any regular function on k^n is just a polynomial.

But there's also some topology floating around, and it's important to think about it. There were two definitions of continuity: one for a single point (shrinking neighborhoods are sent to shrinking neighborhoods, intuitively), and one for the whole space (the preimage of every open set is open). Thus, one can make an equivalent definition of a regular function.

[12] Often, this is denoted $A[X]$, e.g. in Hartshorne, so that $A(X)$ can refer to rational functions.

Definition. $F : X \to k$ is *regular* if for any point $p \in X$, there exists an open $U \subseteq X$ and polynomials $f, g \in k[x_1, \dots, x_n]$, where $g \neq 0$, such that for all $x \in U$, $F|_U = f/g$.

These definitions are equivalent, but the proof will be postponed.

For example, on $k \setminus 0$, $1/x$ is regular, though it lives in $k[x, 1/x]$. More generally, any polynomial function with zeros at $p_1, \dots, p_n$ is invertible in any open neighborhood not containing the p_i. This relates to localization again, e.g. $1/x \in k[x]_f$ if $p_n = 0$, as $1/x = (1/f)(x - p_1) \cdots (x - p_{n-1})$.

This shows up, for example, in projective space $\mathbb{CP}^1$ (i.e. $\mathbb{P}^1_{\mathbb{C}}$). This can be given two charts as a manifold, each of which looks like $\mathbb{C}$; in one chart, the north pole is left out, and in the other chart, the south pole is. One of these is given z-coordinates (so every regular function looks like $k[z]$), and in the other, one uses $w = 1/z$, with regular functions $k[w]$.

Thus, a regular function is one that plays well with these coordinate transformations, i.e. $f(z) \mapsto f(1/w)$. But if f has any nonconstant part, $f(x) = x^n + \text{stuff}$, and therefore after changing coordinates, this becomes $1/x^n + \text{stuff}$, which isn't generally polynomial. Thus, all regular functions on $\mathbb{CP}^1$ are constant! This is an algebraic analogue to Liouville's theorem.

Given an $X \subset k^m$ and $Y \subset k^n$, what are the regular functions on $X \times Y$? Given an $f(x_1, \dots, x_m) \in A(X)$ and $g(y_1, \dots, y_n) \in A(Y)$, the polynomial definition of regular functions implies that $f(x_1, \dots, x_m) g(y_1, \dots, y_n) \in A(X \times Y)$.

Thus, it turns out that $A(X \times Y) \cong A(X) \otimes_k A(Y)$.[13] The isomorphism $f : A(X) \otimes_k A(Y) \to A(X \times Y)$ is given by

$$\sum c_i f_i(x) \otimes g_i(y) \longmapsto \sum c_i f_i(x) g_i(y).$$

This is surjective, because it hits all of the generators (which are just the monomials), since $\sum x_{i_s} \otimes 1 \mapsto x_{i_1} \cdots x_{i_\ell}$ (and similarly for any combination of y_i, or x_i and y_i). It's injective, because if the f_i are linearly independent over k, and the g_i are all linearly independent over k, then one can check that $f_1 \otimes g_1 + \cdots + f_\ell \otimes g_\ell$ is nonzero (unless $\ell = 0$, etc.), and therefore for all $x \in X$, $c_i f_i(x) = 0$, and therefore the image is nonzero (since a polynomial vanishes everywhere iff it is nonzero). Thus, injectivity requires k to be algebraically closed, but surjectivity doesn't.

A lot of things are nicer when rings are integral domains; geometrically, this relates to irreducible sets.

Question. Suppose X and Y are irreducible. Then, when is $X \times Y$ irreducible?

Definition. If $X \subset k^m$ and $Y \subset k^n$ are algebraic, then $F : X \to Y$ is *regular* if $F = (f_1, \dots, f_n)$ for regular $f_1, \dots, f_n : X \to k$.

A regular map $F : X \to Y$ is an *isomorphism* if there exists a regular $G : Y \to X$ such that $F \circ G = \mathrm{id}_Y$ and $G \circ F = \mathrm{id}_X$.

Using this definition, one can easily check that the hyperbola $xy = 1$ is isomorphic to the line $k \setminus 0$, given by $x \mapsto (x, 1/x)$, and in the other direction by projecting to the first coordinate. There's another more local characterization of regularity, which we'll say eventually.

This is interesting because $k \setminus 0$ is open in k, but $xy = 1$ is Zariski-closed in k^2! So isomorphisms are an intrinsic notion, but might not preserve how a variety sits in ambient space. Another example is that $\mathrm{GL}(n, k)$ is an open subset of $M_{n \times n}(k)$ (i.e. those with $\det(M) \neq 0$; since the determinant is a polynomial condition in the entries of a matrix, it is continuous, so the preimage of the open $k \setminus 0$ must be open). But it can also be realized as a closed subset, as $k^{n^2+1}/(\det y - 1)$. It's also possible to use regular or rational functions to prove that a conic in $\mathbb{P}^2$ looks like $\mathbb{P}^1$.

Recall that there's a categorical correspondence between affine varieties, with regular maps, and finitely generated, nilpotent-free k-algebras and their k-algebra homomorphisms. Given such a k-algebra A, let G be a finite subgroup of $\mathrm{Aut}_k(A)$, such that $\mathrm{Char}(k) \nmid |G|$. Then, construct another k-algebra $A^G = \{x \in A \mid g(x) = x \text{ for all } g \in G\}$. Thus, $A^G \hookrightarrow A$, but it's merely a subring, *not* an A-module, and in fact there's an equivalence

$$\begin{array}{ccc} A^G & \longrightarrow & A \\ \uparrow\downarrow & & \uparrow\downarrow \\ X/G & \longleftarrow & X \end{array}$$

Exercise 12.3.

(1) Prove that A^G is finitely generated (so that it does correspond to a closed subset).
(2) Check that the induced red arrow is correct, and that $X \to V(A^G)$ corresponds to taking a quotient of sets.

Ideally,[14] one could check that X/G is a quotient of varieties or schemes, but we haven't defined exactly what that means yet.

[13] In case you don't know what a tensor product is, let A be a ring and M_1 and M_2 be A-modules. Then, the *tensor product* $M_1 \otimes_A M_2$ can be formed by taking the module free on the elements $M_1 \times M_2$ and quotienting by all relations of the form $(am_1, m_2) - (m_1, am_2)$ for $m_1 \in M_1$, $m_2 \in M_2$, and $a \in A$, along with $(m_1, m_2 + m_2') - (m_1, m_2) - (m_1, m_2')$, and similarly in the first coordinate. This allows elements to be written as $m_1 \otimes m_2$ such that $am_1 \otimes m_2 = m_1 \otimes am_2$, and $m_1 \otimes (m_2 + m_2') = m_1 \otimes m_2 + m_1 \otimes m_2'$, and so on. The tensor product thus has a natural A-module structure.

[14] No pun intended.

A priori, it seems like $V(A^G)$ should be larger than $V(A)$, but the trick is that A^G often needs more generators, and it doesn't follow from $k[x_1,\dots,x_n]$ being Noetherian: A^G cannot always be realized as a quotient of $k[x_1,\dots,x_n]$.

Proposition 12.4. *If $X \subseteq k^n$ is irreducible and $U \subseteq X$ is nonempty and open, then U is dense in X.*

Proof. Suppose U isn't dense in X, so that $X \setminus U$ is a nonempty proper closed subset of X, and $\overline{U}$ is a nonempty proper closed subset of X; thus, $X = (X \setminus U) \cup \overline{U}$, but X is irreducible, so this is a problem. Thus, U must be dense in X. □

This allows us to return to the question of when $X \times Y$ is irreducible. It turns out this is true whenever X and Y are, because if A and B are finitely generated integral domains, then $A \otimes B$ is still an integral domain (the finitely generated hypothesis is necessary); proving the geometric side of this fact is easier than proving this algebraic fact.

Specifically, suppose $X \times Y$ is not irreducible. Then, $X \times Y = U \cup V$, where U and V are proper, closed, and nonempty. Then, for any $y \in Y$, take the slice $X \times \{y\} = (U \cap X \times \{y\}) \cup (V \cap X \times \{y\})$; thus, one can define sets $A = \{y \in Y \mid X \times \{y\} \subset U\}$ and $B = \{y \in Y \mid X \times \{y\} \subset V\}$; then, (one can prove that) A and B are nonempty, proper closed subsets of Y whose union is Y, and therefore Y would be reducible.

13. Rational Functions: 2/4/15

Today's lecture was by Brian Conrad. All fields k will be algebraically closed today.

Let A be a reduced (that is, no nilpotents), finitely generated k-algebra, i.e. $A \simeq k[x_1,\dots,x_n]/J$, where J is a radical ideal. Then, $V(J) \subset \mathbb{A}^n$ is isomorphic to MaxSpec(A), i.e. the maximal ideals of A, using $k[x_1,\dots,x_n] \twoheadrightarrow A$.

Then, we saw that $V(J)$ is irreducible iff J is prime, or, equivalently, A is a domain. One calls the elements of A *regular functions* on J.

Now, assume A is a domain, so $V(J)$ is irreducible. We saw last time that all nonempty open $U \subset V(J)$ are dense — they're huge! For example, a typical Zariski-closed set is a line in $V(J)$, so open sets are complements of these.[15] While the Zariski topology is weird (not Hausdorff, nowhere near Euclidean, where open sets are generally small), it's still quite useful.

Given an $f \in A$, there's a function $f : V(J) \to k$ (using the polynomial representation of f, where if $f = g$ on J, then $f - g \in J$, and therefore is 0 mod J). But there's a more elegant way to see this: points in $V(J)$ are maximal ideals $\mathfrak{m}$, so $f : V(J) \to k$ sends $\mathfrak{m} \mapsto f \bmod \mathfrak{m} \in A/\mathfrak{m}$, but $A/\mathfrak{m} = k$ by the Nullstellensatz.

Exercise 13.1. If this doesn't make sense, try it in the case $J = 0$, and see what happens. Then, $k \leftarrow k[x_1,\dots,x_n]$ is naturally the constant term of

$$f(x_1,\dots,x_n) = f(c_1,\dots,c_n) + \sum_i f_i(x_i - c_i).$$

This interpretation of these functions, relating to the evaluation map at that point, is more intrinsic to A, and less dependent on the ambient coordinates the variety lives in.

Since A is a domain, one can take its fraction field Frac(A), with $f/g \in \mathrm{Frac}(A)$ for $f, g \in A$ and $g \neq 0$. These will be the rational functions.

Aside. One nice thing about the field of fractions is that if D is a domain and $S = D \setminus 0$ is multiplicative, then the natural map $D \to S^{-1}D$ is injective. In principle, one can lose some information, but in this case, just like when you learned about fractions in 3rd grade (over $\mathbb{Z}$, unless you went to a very strange elementary school), nothing is lost. Then, the *fraction field* is made by taking as many fractions as possible: $S = D \setminus 0$, so $S^{-1}D$ is denoted Frac(D).

Example 13.2. Consider 3-space $\mathbb{A}^3$, where $A = k[x,y,z]$. Then, let $f = (x-y)/xy$ and $g = (y-z)/yz$. Thus, $f, g \in \mathrm{Frac}(A)$.

Unlike 3rd grade, A might not be a UFD (though $k[x,y,z]$ is), so least common denominators might not exist.[16] There's no God-given reduced form, though there may be different expressions for the same element.

So, can we define these functions in nice ways? On $\{xy \neq 0\} = U \subset \mathbb{A}^3$, we have $f : U \to k$ sending $(x,y,z) \mapsto (x-y)/xy$, and on $\{yz \neq 0\} = U' \subset \mathbb{A}^3$, there's similarly $g : U' \to k$ sending $(x,y,z) \mapsto (y-z)/yz$. It seems reasonable to define $f + g : U \cap U' \to k$, given by $(x,y,z) \mapsto (x-z)/xz$. So really this has a bigger domain of definition, $\{xz \neq 0\}$, rather than $U \cap U' = \{xyz \neq 0\}$, which is interesting — we'll want to understand this systematically, rigorously defining rational functions and domains of definition. In general, finding the domain of definition is pretty hard; we don't know all of the ways to write it as a fraction from a given vantage point.

Definition. Choose an $f \in \mathrm{Frac}(A) = K$. Then, f is *regular* at a $p \in V(J)$ if f can be written as $f = a/b$ for $a, b \in A$ and $b(p) \neq 0$.

That is, it's regular at p if it can be written as an expression whose denominator is nonzero at p.

[15] "Doing geometry with the Zariski topology is like writing with a pencil with a two-foot radius."

[16] "Unlike everybody who now works at the University of Chicago, [Paul Sally] actually cared about education for young children…" and then later, "That whole discussion was just for the sake of telling that silly story."

Lemma 13.3. *If $f = a/b = a'/b'$, where $b(p)$, $b'(p) \neq 0$ for a $p \in V(J)$, then $a(p)/b(p) = a'(p)/b'(p)$.*

Thus, rational functions can be defined the way they ought to be: one can really write $f(p)$, and it's independent of choice of representative.

Proof. Cross-multiply: is it true that $a(p)b'(p) = a'(p)b(p)$ in k? This is $(ab')(p)$ and $(a'b)(p)$, but we know $ab' = a'b$ in A, as $a/b = a'/b'$ (since A is a domain, so cross-multiplication works). □

Thus: at a regular point, there is a well-defined value.

Remark. The locus where f is regular is open: if p is regular for f, then $p \in D(b)$, and all points of $D(b)$ are regular for f. $D(b)$ is open, and on it a/b works; there may be more regular points, though.

Sometimes, $\mathrm{Reg}(f)$ is used to denote the locus of regular points; then, this set is open. Since $b \neq 0$ in A, then $D(b) \neq \emptyset$, so there will be some regular points, and in fact a big, fat open set's worth.

Definition. The domain of f, $\mathrm{dom}(f)$, is the set of regular points of an $f \in \mathrm{Frac}(A)$, inside $V(J)$.

We've seen that this is a nonempty open set. Of course, if $f \in A$, then $\mathrm{dom}(f) = V(J)$; the beautiful thing is that the converse is true, too! This is totally non-obvious, and really awesome.

But first, let's have an example where A isn't a UFD. There's a canonical example of this.

Example 13.4. Let $A = k[x,y,z,w]/(xy - zw)$.

Exercise 13.5.

(1) Show that $(xy - zw)$ is prime, so that A is really a domain.
(2) Show that A isn't a UFD.

The idea here is that if $R = k[x,y]$, then $A = R[z,w]/(zw - r)$, and $r = xy \in R$. Then, it's a little easier, as there are fewer choices of representatives. Then, $xy = zw$ in A, and it's necessary to show that neither is a unit or a multiple of the others.

Let $f = w/x = y/z$ in $\mathrm{Frac}(A)$. Clearly, $\mathrm{dom}(f) \supset \{x \neq 0\}$, and $\mathrm{dom}(f) \supset \{z \neq 0\}$. Maybe it's even bigger than $\{x \neq 0\} \cup \{z \neq 0\}$; we still need to check points of the form $(0,\alpha,0,\beta)$. What can happen at these points? $\beta/0$ and $\alpha/0$ look kind of funny.

In general, computing exact domains of definition can be quite difficult, but here is a useful trick.[17]

Lemma 13.6. *If $f = a/b$, and if p is such that $b(p) = 0$ and $a(p) \neq 0$, then $p \notin \mathrm{dom}(f)$.*

Proof. If $p \in \mathrm{dom}(f)$, then $f = a'/b'$, where $a', b' \in A$ and $b'(p) \neq 0$. Thus, $ab' = a'b$, but evaluating at p, $a(p)b'(p) \neq 0$, but $a'(p)b(p) = 0$, which is a contradiction. □

This is the one elementary criterion; it's the cases that evaluate to 0/0 that require some real head-scratching, I mean close analysis.

Returning to the example, we now know that $(0,\alpha,0,\beta) \notin \mathrm{dom}(f)$ if $\alpha \neq 0$ or $\beta \neq 0$. In particular, if $V = \{xy = zw\} \subset \mathbb{A}^4$, then the closed set $V \setminus \mathrm{dom}(f) \supset \{(0,\alpha,0,\beta) \mid \alpha \neq 0 \text{ or } \beta \neq 0\}$.

The only mystery left is: what about the origin? Well, $V \setminus \mathrm{dom}(f)$ is closed, so fixing the "punctured line" $\alpha \neq 0$, taking its closure preserves the origin. More specifically, it's irreducible and closed in V, so the closure of the punctured line must be the whole line. In particular, $(0,0,0,0) \notin \mathrm{dom}(f)$, so $V \setminus \mathrm{dom}(f) = \{x = 0, z = 0\}$.

Next time, we'll prove that if $\mathrm{dom}(f) = V(J)$, then $f \in A$, which shows that even though the coordinate ring is a very global object, it has some important local properties.

Example 13.7. Let $f = y^2/(x-1)$ for $A = \mathbb{C}[x,y]/(x^2+y^2-1)$ or $A' = \mathbb{C}[x,y]$. Then, $A' \twoheadrightarrow A$, but there's no associated map $\mathrm{Frac}(A') \to \mathrm{Frac}(A)$ (since $1/x$ is sometimes sent to $1/0$, so to speak). For example, $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/5$, but there's no map $\mathbb{Q} \to \mathbb{F}_5$.

Exercise 13.8. Use the UFD property of $\mathbb{C}[x,y]$ to show that $\mathrm{dom}_{\mathbb{A}^2}(f) = \{x \neq 1\}$.

The interesting point is that a domain of definition can expand on a subvariety, because the two fraction fields have nothing to do with each other: on $y^2 = 1 - x^2$, f looks like $x + 1$, which is a ring element — in ambient space, it looks like a fraction, but on the subvariety $\{y^2 = 1 - x^2\}$, it is a regular function. This is no accident; we'll generalize it next time.

[17] "Famous last words: 'there must be something wrong with your example, because I can prove the lemma!' "

14. Rational Maps: 2/6/15

"I'm sure the business school would laugh if they saw us still using blackboards."

Brian Conrad gave today's lecture again, and, as usual, throughout this lecture k denotes an algebraically closed field.

Remark. If f and g are rational functions on an irreducible affine algebraic set $X = V(J) \subset \mathbb{A}^n$, and $A = k[x_1, \dots, x_n]/J$, let $U = \mathrm{dom}(f)$ and $U' = \mathrm{dom}(g)$.

Then, $f + g \in \mathrm{Frac}(A)$, and $\mathrm{dom}(f+g) \supset U \cap U'$, which is nonempty (since U and U' are dense). Sometimes, the domain is much larger, e.g. if $f = -g$.

If $p \in U \cap U'$, then $f = a/b$ with $b(p) \neq 0$ for some $a, b \in A$, and similarly $g = c/d$, where $d(p) \neq 0$. Then, by the surefire Sally method of adding fractions, $f + g = (ad + bc)/bd$, since $bd(p) \neq 0$, so $p \in \mathrm{dom}(f+g)$, and

$$(f+g)(p) = \frac{(ad+bc)(p)}{bd(p)} = \frac{a(p)}{b(p)} + \frac{c(p)}{d(p)} = f(p) + g(p),$$

and $f \cdot g$ is similar.

Proposition 14.1. *If f and g are rational functions on X and $U \subset \mathrm{dom}(f) \cap \mathrm{dom}(g)$ is nonempty, and $f|_U = g|_U$ as k-valued functions, then $f = g$.*

This is actually quite easy. And it's very useful, too; even though the domain of definition is hard to calculate in practice, it doesn't really matter, as functions are often the same. There's this rigidity to algebraic geometry, unlike continuous functions in calculus.

Note that even though $k[\underline{T}] \twoheadrightarrow A$, $k(\underline{T}) \not\twoheadrightarrow \mathrm{Frac}(A)$ (look at where the kernel can go). Thus, it's really better to think of rational functions as locally rational functions, as we've defined them.

Proof of Proposition 14.1. We can always shrink U if we want; if $f = a/b$ and $g = c/d$, then shrink U such that $U \subset \{bd \neq 0\}$, e.g. replace U with $U \cap \{bd \neq 0\}$. Since X is irreducible, the resulting set is nonempty and contained within $\mathrm{dom}(f) \cap \mathrm{dom}(g)$; now, we've made the problem easier, since U is smaller.

On U, $f(p) = a(p)/b(p) = g(p) = c(p)/d(p)$, so $ad - bc \in A$ vanishes on U. But $V(ad-bc)$ is a closed set in X containing U, which is dense, because X is irreducible. Thus, $V(ad-bc) = V(0)$ on X, and therefore $ad - bc = 0$ in A. Thus, $a/b = c/d$ in $\mathrm{Frac}(A)$. □

We use this lemma tacitly all the time; it's the reason the difficulty of computing the domain of definition is actually pretty irrelevant in practice.

Corollary 14.2. *$f \in \mathrm{Frac}(A)$ is uniquely determined by the associated function $U \to k$, for any nonempty open $U \subset \mathrm{dom}(f)$.*[18]

This is just like how polynomials, as functions, determine their coefficients, over any algebraically closed or even infinite field. We used this all the time in high school.

Now, here's the miracle from last time.

Theorem 14.3. *If $f \in \mathrm{Frac}(A) = K$ satisfies $\mathrm{dom}(f) = X$, then $f \in A$ (inside K).*

Note that algebraic closure is quite necessary. For example, if $k = \mathbb{R}$, $X = \mathbb{A}^1$, and $f = 1/(u^2+1)$, then $f \notin \mathbb{R}[u]$, true as rings or functions over $\mathbb{R}$. The proof will use the Nullstellensatz; there's a more general version for schemes, but that's beyond the scope of this class.[19]

The theorem is silly as elements of the polynomial ring; it's meaningful precisely because rational functions have no best representation as a ring element.[20]

Proof of Theorem 14.3. Consider the *ideal of denominators* $I = \{a \in A \mid af \in A \text{ inside } K\}$. The name is a little weird, e.g. $0 \in I$.

Exercise 14.4. Show that the ideal of denominators is a nonzero ideal of A (e.g. if $f = c/d$ in A and $d \neq 0$, then $d \in I \setminus 0$).

The whole content of the proof here is that we don't know that $f \in I$, $1 \in I$, or I is principal. Any of these would imply what we want.

Suppose $I \subsetneq A$, so $I \subset \mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of A. Thus, by the Nullstellensatz, $\mathfrak{m}$ corresponds to some $p \in X$, so for any expression c/d for f with $c, d \in A$ and $d \neq 0$, $d \in I$, so $d(p) = 0$. Thus, $p \notin \mathrm{dom}(f)$, which is a contradiction. □

This is totally nonconstructive, but there's nothing to construct.

---

[18] "For reduced smooth schemes, this is actually true, whatever that means."

[19] "Did you guys have fun discussing things on the blog? Not that I know what I'm talking about."

[20] "Oh, look at that! See that? That's bad colored chalk."

Remark. The ideal of denominators can be defined for all f, in which case $\mathrm{dom}(f) = X \setminus V(I)$. Thus, the proof boils down to that $V(I) \neq \emptyset$ unless $I = A$. This sounds like our good friend the Nullstellensatz, always there when we need to talk to it.

The UFD property means that even though A has many principal ideals in general, ideals of denominators are always principal. Generally, tricks like the ideal of denominators come up all the time. When there's no good unique presentation, considering the ideal of all of them (sometimes slightly adjusted) is really useful.

Theorem 14.5. *Suppose $f \in K$ satisfies $\mathrm{dom}(f) \supset X \setminus V(b) = D(b)$, i.e. f is regular wherever b is nonzero. Then, $f = a/b^n$ for some $a \in A$, $n \geq 1$.*

The point is, we would want $f = a/b$, but this is as nice as one can get, since V can't tell I from $\sqrt{I}$ in general. Also, notice that the converse is trivial.

Proof. By hypothesis, $X \setminus V(b) \subset \mathrm{dom}(f) = X \setminus V(I)$, where I is the ideal of denominators for f, so $V(b) \supset V(I)$. That is, b vanishes everywhere that I vanishes, i.e. $V(I)$. But by the Nullstellensatz, that means $b^n \in I$ for some $n \in \mathbb{N}$ (i.e. $b \in \sqrt{I}$). □

This is essentially the same argument as for Theorem 14.3, and has a very interesting consequence.

Corollary 14.6. *$A_b = A[1/b] = \{f \in K \mid \mathrm{dom}(f) \supset X \setminus V(b)\}$, i.e. the f regular whenever $b \neq 0$.*

So we have a characterization of $V(b)$ in the fraction field. Additionally, if $V(b) = V(b')$, then $A_b = A_{b'}$ within K! This is completely determined by where stuff vanishes. A_b is "intrinsic" to $V(b)$ or $D(b)$, i.e. the elements of A_b are functions on D_b. This is both extremely hard to prove with bare hands and extremely useful, as we'll see later.[21]

Just like generalizing regular functions to regular maps, one can generalize rational functions to rational maps between varieties.

Definition. Let $X \subset \mathbb{A}^n$ be an irreducible closed set with coordinate ring A and $K = \mathrm{Frac}(A)$. Then, a *rational map* $X \dashrightarrow \mathbb{A}^m$ is a map $U \to \mathbb{A}^m$ sending $u \mapsto (f_1(u), \ldots, f_m(u))$ with $f_1, \ldots, f_m \in K$ and $U \subset \bigcap_{i=1}^n \mathrm{dom}(f_i)$.[22]

Notice that rational maps are only partial functions out of X most of the time. Furthermore, two such rational functions $(f_1, \ldots, f_m)$ and $(g_1, \ldots, g_m)$ are the same if $f_i = g_i$ for all i; the open set doesn't matter.

Remark. If two rational maps $X \overset{\dashrightarrow}{\dashrightarrow} \mathbb{A}^m$ coincide on some nonempty open set, then they're the same.

Proof. The proof is exactly the same as for rational functions — or as a consequence of it: compare their components, which are rational functions. □

The notion of a rational map is extremely flexible, and it's very characteristic of algebraic geometry and large open sets (as opposed to the small open sets of differential geometry) that these are so useful.

Just as varieties correspond to coordinate rings as regular maps, varieties with *dominant* rational maps (that is, they have dense image) correspond to finitely generated fields over k, which we'll talk about next week. This leads to a definition of dimension; rational maps link the algebraic (transcedence degree) and geometric (irreducible closed sets) definitions of dimension.

15. Varieties and Sheaves: 2/9/15

"Secretly, I'm laughing here, because I hit you on the head... Now, we give these maximal ideals names. I call it $(1,1)$*, and you call it* Fred*. What's the value of the function at* Fred*?"*

Ravi Vakil is back today.

Before we get to the substance, let's think once again about the notion of an affine variety. Fix k to be an algebraically closed field.

When we fix how an affine variety sits inside k^n, it corresponds to a nilpotent-free, finitely generated k-algebra, with generators chosen, i.e. $k[x_1, \ldots, x_n]/I$. More generally, though, we want affine varieties (without an ambient embedding) to correspond to nilpotent-free, finitely generated k-algebras without generators known.

One could simply take the category of such k-algebras with arrows reversed, but that's somehow unsatisfying. It's also not satisfying to just embed in k^n; similarly, one wouldn't define all vector spaces in terms of bases.

However, we know the dictionary between the two: given an affine variety, its functions form the corresponding k-algebra, and given a nilpotent-free, finitely generated k-algebra A, its maximal ideals, $\mathrm{mSpec}(A)$, is the set of points of an affine variety (though, there's a little more information contained here: the points and the functions). Then, one

[21] "That's a very ungrammatical phrase, but it's in quotes, so I can say anything I want."

[22] "Don't ask me how to do that in LaTeX."

can get a subring of functions out of it. mSpec sends maximal ideals to points, and a ring element f to $f \bmod \mathfrak{m}$ (which is a function). The ring of functions is always nilpotent-free, because if $f^2 = 0$, then $f(x)^2 = 0$ at each x, and therefore $f(x) = 0$ for each x (since k lacks nilpotents).

Thus, one can define an affine variety as a set of points X with a subring of functions whose set of maximal ideals is given by X. Then, maps between varieties are formalized as pullbacks of these nice maps.

For example, $y^2 = x^3$ in k^2 is an affine variety corresponding to, of course, $k[x,y]/(y^2 - x^3)$. One can describe the correspondence between them independent of the embedding into k or the generators of the k-algebra.

However, $J = (x+y)^2$ isn't an affine variety, since we don't have all the functions needed. This has to do with it not being radical.

One can apply this to define the cotangent space in a coordinate-free way near a point.

Definition. Let R be a ring and $\mathfrak{m}$ be a maximal ideal of R, so that $k = R/\mathfrak{m}$ is a field. Then, $\mathfrak{m}$ is a R-module, and so $\mathfrak{m}/\mathfrak{m}^2$ is an $R/\mathfrak{m}$-module, i.e. a k-vector space. $\mathfrak{m}/\mathfrak{m}^2$ is called the *cotangent space* at the point $\mathfrak{m}$.

This is somewhat irrelevant to the rest of today's lecture, but the point is that lots of interesting things can be defined in a coordinate-free way, and without a whole lot of work. Try calculating the cotangent space of $\mathbb{Z}$, which sort of relates to schemes or smoothness.

Another goal for today is to discuss varieties more generally; we've already seen affine varieties and projective hypersurfaces, and hopefully we can unify them somehow. First, though, let's review rational functions. Let R be a ring and $S^{-1}R$ be a localization, where $S = R \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p}$.[23] For now, R will be a finitely generated, nilpotent-free k-algebra and an integral domain, and $\mathfrak{p} = \mathfrak{m}$ will be maximal. Thus, R has a fraction field $K(R)$, and $R \hookrightarrow K(R)$.

Given an irreducible affine variety X whose ring of functions is R, and an $S \subset X$, one has $R \subset \mathrm{Reg}(S) \subset K(R)$ (that is, $\mathrm{Reg}(S)$ is the functions regular at S: at each point p, each regular function has a representation a/b with $b(p) \neq 0$). This is inclusion-reversing: if $S \subset T \subset X$, then $\mathrm{Reg}(T) \subset \mathrm{Reg}(S)$.

It's also true that $\mathrm{Reg}(\emptyset) = K(R)$, and if $\mathfrak{m} \subset R$ is maximal, then $\mathrm{Reg}(\mathfrak{m}) = R_{\mathfrak{m}} = (R \setminus \mathfrak{m})^{-1}R$.

Definition. A ring is *local* if it has a unique maximal ideal.

Then, $R_{\mathfrak{m}}$ is local (localized rings are local, which is good linguistically): its sole maximal ideal is $\mathfrak{m}R_{\mathfrak{m}}$, because $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} \cong k$ is a field.

Exercise 15.1. Finish this proof, i.e. show that $R_{\mathfrak{m}}$ has no other maximal ideals.

Now, the next question: what are the functions that are regular everywhere? We proved that they're exactly R, and the key thing is the *ideal of denominators*.

Exercise 15.2. Show that $\mathrm{Reg}(D(f)) = R_f$.

This is pretty reasonable intuitively, and uses the ideal of denominators again.

Sheaves. We're going to define something we probably shouldn't do in an undergraduate class again, the notion of a sheaf. Well, that is, we'll give a bunch of examples today, and then define it on Wednesday.

The idea is that on an affine variety, a lot of the information is contained in the functions on the space, not just on the whole space, but on open sets of it. This is also true of complex projective varieties (since, e.g. on $\mathbb{P}^1_{\mathbb{C}}$, there aren't very many interesting ones by Liouville's theorem). A *sheaf* will be the gadget used to understand all functions on all open sets of something.

Consider a topological space X.[24] For each open set U, there's a ring $C(U)$ of $\mathbb{R}$-valued, continuous functions on U; if $V \subset U$, then restriction of functions gives a map $\mathrm{res}_{U,V} : C(U) \to C(V)$.

If $W \subset V \subset U$, then restriction composes: $\mathrm{res}_{V,W} \circ \mathrm{res}_{U,V} = \mathrm{res}_{U,W}$. It's also true that if one has several continuous functions on different open sets that agree on all of the intersections, there's a way to glue them together into a single function.

One can do the same thing with differentiable $\mathbb{R}$-valued functions, or $C^\infty(\mathbb{R})$-functions, or holomorphic ($\mathbb{C}$-valued, of course) functions; the same axioms work.

16. From Rational Functions to Rational Maps: 2/11/15

"Awkwardly, $\mathbb{C}$ is not $\mathbb{Q}$."

[23] We've been using maximal ideal here, but in scheme-land, it works just as well with prime ideals.

[24] "An example of a topological space is this blackboard. We'll take the usual topology on the blackboard..."

Recall that a rational map $V \dashrightarrow k^n$ (the notation because it's a partially defined map) is a tuple of rational functions $\mathbf{x} \mapsto (f_1(\mathbf{x}), \dots, f_n(\mathbf{x}))$. This will be defined on some open set within V, though there are issues with this characterization that lead us to want to define this more intrinsically for general varieties.

Then, one can define a rational map $V \dashrightarrow W$ by choosing $W \hookrightarrow k^n$ and then writing a map $V \dashrightarrow k^n$ and taking the pullback, which is adequate, but maybe not as intrinsic as one would like.

In terms of rings, a map $V \to W$ induces a map in the other direction on rings of rational functions $k(V) \leftarrow k(W)$.[25] Thus, we can also map $\mathcal{O}(W)$ to the field of rational functions $\mathrm{Frac}(\mathcal{O}(V))$ (which is sometimes denoted $K(V)$, which I'm sure isn't confusing in the slightest).

Example 16.1. Consider the circle $x^2 + y^2 = 1$ (over $\mathbb{C}$, though nothing except intuition changes over a more general k), where there's a nice near-bijection between lines through a given point and elements on the circle. Thus, there's a rational map between the circle $\mathbb{C}[x,y]/(x^2+y^2-1)$ and the line, given by $\mathbb{C}[t]$, and a map

$$t \mapsto \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right),$$

which isn't defined everywhere, but is a rational map! The same is true of the reverse map $(x,y) \mapsto y/(x-1)$; once again, it's a rational function.

Since each rational function is defined on a dense (equivalently, nonempty!) open set (the intersection of the domains of definition of their components, which is nonempty because they're all dense), then one can compose rational maps.

Definition. Let X and Y be irreducible varieties; then, $f : X \dashrightarrow Y$ is *dominant* if the image is dense.

The circle mapping to the line is dominant; the line mapping onto the plane given by the circle isn't dominant (since the image is just the circle).

But the point is, we can compose dominant maps, so there's a category again! It's not the same as the category of varieties with regular maps. This is linguistic, not a theorem. This category has for objects irreducible varieties over an algebraically closed k, and morphisms dominant rational maps.

When is a rational map an isomorphism? Once again, it requires an inverse in the other direction, so that their composition is the identity. Then, the trick is that everything is only mostly defined, but if two rational functions agree on an open set, then they're equivalent.

Definition. An isomorphism in this category is called *birational*. Then, a *rational variety* is any variety birational to k^n.

Why does this particular class get its own name? This is because on a rational variety, one can solve Diophantine equations, in the same way that we did: mapping from the variety to k^n, where finding points is easy, and then mapping back. For example, we had $w^2 + x^2 = y^2 + z^2$ is a rational variety, and therefore finding solutions is relatively easy (as on the problem set); it's birational to k^3, plus some special cases.

Next question: $x^n + y^n = 1$. Wait, maybe this is a little too ambitious. We have a particular solution $(1,0)$, but the issue is that this is birational to something with $\binom{n-1}{2}$ holes and some number of missing points, so this isn't birationally equivalent to a sphere (though it's OK for $n = 3$). This is a nifty relation between geometry and arithmetic, and illustrates why Fermat's Last Theorem was so difficult.

Theorem 16.2. *The following are equivalent.*

(1) $f : V \dashrightarrow W$ is a dominant rational map.

(2) There's an induced map $\mathrm{Frac}(\mathcal{O}(V)) \leftarrow \mathrm{Frac}(\mathcal{O}(W))$.

One interesting fact is that the degree of a field extension $k \hookrightarrow L$ is the topological degree of the map: a given point has five preimages when one adjoins some roots. For example, $y^2 = x^3 - x$ is a degree-two extension of the rational functions $k(x)$, and is a double cover. This relates to the fact that a generic point has two preimages.

Claim. The topological shape of $x^n + y^n = 1$ isn't birationally equivalent to the line if $n > 2$.

This is interesting, because you can prove it yourself: if there are rational functions f, g such that $f(t)^n + g(t)^n = 1$, and then clearing denominators there are polynomials $F(t)^n + G(t)^n = H(t)^n$.[26] This doesn't work, because the only maps that work here are constant (where $k = \mathbb{C}$), which is worth working through. It illustrates algebraic, arithmetic, and topological connections.

Another useful consequence is that not all curves are birational to each other.

With two minutes left, let's talk about a sheaf of rings on a topological space.

[25] This isn't the best notation for the ring of regular functions, since one might think this is a field; alternative notations include $\Gamma(V)$ or $\mathcal{O}(V)$.

[26] This doesn't prove Fermat's Last Theorem; it just says any solutions that would exist aren't very nicely parameterized.

Definition. A *sheaf of rings* on a topological space X is an association of a ring $\Gamma(U)$ to each open set U, with restriction maps $\mathrm{res}_{U,V} : \Gamma(U) \to \Gamma(V)$ whenever $U \supseteq V$, such that $\mathrm{res}_{V,W} \circ \mathrm{res}_{U,V} = \mathrm{res}_{U,W}$. An element of $\Gamma(U)$ is often called a *section* over U. Furthermore, we require that if two sections agree on each element of a cover, then they agree on U, and the "gluability axiom" requires that if two sections agree on all triple intersections of open sets, then they are identical.

17. Varieties and Pre-Varieties: 2/13/15

"It smells like the Nullstellensatz."

Recall that an affine variety over an algebraically closed field k is a set of points (with the Zariski topology) and a ring of algebraic functions (i.e. restrictions of polynomials), and maps from one to another are continuous maps $X \to Y$ between the point sets, such that the pullback of nice (i.e. regular) functions on Y consists of regular functions on X.

Today we'll want to generalize this. Consider $\mathbb{P}^1$ with the usual topology; there simply won't be enough functions (e.g. on $\mathbb{P}^1_{\mathbb{C}}$, all holomorphic functions are constant), so $\mathbb{P}^1$ isn't an affine variety. However, if S denotes the south pole and N the north pole, then $\mathbb{P}^1 \setminus S$ and $\mathbb{P}^1 \setminus k$ are both copies of k, which is an affine variety! Thus, we don't have very many functions globally on $\mathbb{P}^1$, but we have more open sets, and functions on those open sets.

Geometrically, $\mathbb{P}^1$ is the union of the two affine lines $[u, 1]$ and $[1, v]$, which are open sets that cover it. A function on $\mathbb{P}^1$ is given by functions on each of these that glue, i.e. agree on the overlap. But this makes a lot of sense: we need a polynomial $f(u)$ and a polynomial $g(v)$, but since $u = 1/v$, then on the overlap, $f(u) = g(1/v)$, so we just get constant functions. This is an interesting way to think about Liouville's theorem.

Thus, we need to keep track of lots of open sets and functions on those sets. The tool to do this is a sheaf.

Definition. If X is an irreducible affine variety, then $\mathcal{O}_X$, its *sheaf of regular functions*, is given by assigning to every open $U \subset X$ the ring of functions $\mathrm{Reg}(U) = \{x \in \mathrm{Frac}(A) \mid x \text{ is regular on all of } U\}$.

Eventually, we will relax the requirement that X is irreducible.

This really is a sheaf; restriction was already a map $\mathrm{Reg}(V) \to \mathrm{Reg}(W)$, and composes, and since these are functions, we care about their value, so the gluing axiom is satified, too, even though the fractional representation of a regular function may not glue. There's also the identity axiom, which is easy because this is a sheaf of a ring of functions, so there's little work to do.

Note that this setup can be generalized considerably; with a little more work, relatives of this construction with different kinds of functions give you schemes (more than just affine schemes!), manifolds, measurable spaces, and so on.

Now, we have a sheaf! We want to talk about how functions pull back, which is geometric, so let's see the algebraic side of things. Let $X = \mathrm{mSpec}(R)$ and $Y = \mathrm{mSpec}(S)$ be irreducible (for now), so a map of affine varieties $X \to Y$ induces a ring map $\phi : S \to R$. Suppose a $p \in X$ goes to a $q \in Y$; then, p is a maximal ideal, so $p = \phi^{-1}(q)$.

If $\eta \in S$ is regular at q, then $\eta = f/g$, where $g(q) \neq 0$. Then, the pullback to p is $\phi(f)(p)/\phi(g)(p)$. The value at the pullback is the same, because that's what pulling back does; this is a little too simple to believe the first time.

Definition. An *irreducible prevariety* (over an algebraically closed field k) is an irreducible topological space X with a sheaf of functions $\mathcal{O}_X$, such that every point $p \in X$ has an open neighborhood U such that the sheaf at U is $\mathrm{mSpec}(A)$ for a nilpotent-free domain finitely generated over a field k.

A map of irreducible prevarieties is a continuous map $\pi : X \to Y$ such that for any open $U \subset Y$, the pullback π^* of regular functions on U are regular functions on $\pi^{-1}(U)$.

This solves the $\mathbb{P}^1$ problem from before. Also, any irreducible affine variety X and its ring of functions R will do; on any open $D(f) \subset X$, for $f \in R$, the corresponding ring of functions is the localization R_f. Topological localization and algebraic localization are really the same! Topologously, the open sets and regular functions are the same; R_f is really associated with $D(f)$. Moreover, every $U \subset X$ is an irreducible prevariety.

Finally, a map of affine varieties is a map of irreducible prevarieties, since the maps of functions are the same; if one thinks about it more sheafily, there's a way to think of this more flashily by using sheaves, but when one unravels the definition, it's the same thing, really.

Exercise 17.1. Prove that these two ways of stating this are the same, and that a map of affine varieties is a map of irreducible prevarieties.

Finally, as noted, $\mathbb{P}^1$ is an irreducible prevariety, since it is covered by two copies of k, just as $\mathbb{P}^1_{\mathbb{R}}$ and $\mathbb{P}^1_{\mathbb{C}}$ are covered as manifolds.

Now, let's get rid of the irreducibility condition.

Definition. Let R be a nilpotent-free finitely generated k-algebra, where k is algebraically closed. Then, an element of $\mathrm{Frac}(R)$ is *regular* at a $p \in \mathrm{mSpec}(R)$ if it can be written as a/b, where $b(p) \neq 0$.

In English (well, more or less), this is a function on $D(b)$, where there's some b such that $p \in D(b)$. This looks familiar, but the point is, we want to be able to define the sheaf without using $\mathrm{Frac}(R)$.

The sheaf of regular functions $\mathscr{O}(U)$ at an open $U \subset X$, where X may be reducible, is given by defining functions only in a neighborhood of p (since X isn't irreducible, then the field of functions isn't an integral domain, so we can't use it), i.e. $f/g \in R_{\mathfrak{m}}$, where $\mathfrak{m}$ is a maximal ideal of R contained within U, where $g(p) \neq 0$ (and $g \neq 0$ in a neighborhood of p).

Using this sheaf, one can take the same sheafy definition to get prevarieties in the case where X may be reducible.

This is a little confusing, so let's have some more examples.

Example 17.2. Here's an example of a prevariety that you probably won't like. Recall that we made $\mathbb{P}^1$ into a prevariety by taking two copies of k and gluing them with $v = 1/u$, so the localized functions are $k[u]_u = k[u, 1/u]$ (or $k[v, 1/v]$).

Instead, let's just glue on $v = u$. Then, the result looks mostly like k, but now has two copies of the origin! This is not something we want. It recalls the notion of manifolds, where this can happen, but there, the condition to prevent it is the Hausdorff condition. However, the Zariski topology is very non-Hausdorff, so we'll need a better definition.

This journey from local to global happens over and over again: it's how varieties and manifolds (and any kind of geometric space, e.g. complex singular spaces) are defined; and even schemes! A scheme is given by patching together affine schemes, with maps of schemes given by taking pullbacks.

18. Presheaves, Sheaves, and Affine Schemes: 2/18/15

Today's lecture was given by Donghai Pan.

Let $k = \overline{k}$ be an algebraically closed field and $X \subseteq \mathbb{A}^n_k$ be an affine irreducible variety; then, we have its coordinate ring $A(X)$ and $k(X)$, its ring of rational functions.

Recall some stuff Brian Conrad did a few weeks ago.

(1) The rational functions $f \in k(X)$ which are regular everywhere are in $A(X)$.
(2) The rational functions that are regular on $D(f)$ lie in A_f.
(3) The rational functions that are regular around $\mathfrak{p}$ can be identified with $A_{\mathfrak{p}}$.

These will be the starting point for the notion of an affine scheme.

In the language of sheaves, $A_{\mathfrak{p}}$ is a *germ* and A_f is a *stalk*: the germ is defined as the direct limit of a bunch of stalks. There's also an association from open sets to commutative rings, and there's a way to restrict from larger opens to smaller opens.

Definition. Let $\mathscr{C}$ be a category. Then, a *terminal object* in $\mathscr{C}$ is an object $O \in \mathscr{C}$ such that for any object $A \in \mathscr{C}$, there is a unique $\mathscr{C}$-morphism $A \to O$.

If a terminal object exists, it is unique up to isomorphism; not all categories have a terminal object, but all of the ones we'll think about, and most reasonable categories, do. For example, any set with one element is terminal in the category of sets, and the trivial (abelian) group, ring, or R-module is also a terminal object.

Definition. Let X be a topological space and $\mathscr{C}$ be a category with a terminal object O. Then, a *presheaf* $\mathscr{F}$ in the category $\mathscr{C}$ consists of the following:

(1) for each open $U \subseteq X$, there is an object $\mathscr{F}(U)$ in $\mathscr{C}$, and
(2) for U, V open in X with $V \subseteq U$, there is a *restriction map* $\mathrm{res}_{U,V} : \mathscr{F}(U) \to \mathscr{F}(V)$, which is a $\mathscr{C}$-morphism,

subject to the following restrictions.[27]

(1) $\mathscr{F}(\emptyset) = O$.
(2) For any open U, $\mathrm{res}_{U,U} = \mathrm{id}_U$.
(3) If $W \subseteq U \subseteq V$ as open subsets of X, then $\mathrm{res}_{U,W} = \mathrm{res}_{V,W} \circ \mathrm{res}_{U,V}$.

Common choices for $\mathscr{C}$ include sets, abelian groups, and (as in the example from above) commutative rings. Also, $\mathrm{res}_{U,V}(s)$ is sometimes denoted $s|_V$ if U is understood from context.

It is possible to define a category $\mathscr{T}(X)$ on the open subsets of X, where there is a unique arrow $U \to V$ iff there is an inclusion $U \subseteq V$. Then, the axioms of a presheaf are equivalent to stating that $\mathscr{F}$ is a contravariant functor $\mathscr{F} : \mathscr{T}(X) \to \mathscr{C}$. This means that the notion of elements in objects of $\mathscr{C}$ is important (though in classical algebraic geometry, $\mathscr{C}$ is always some kind of rings, modules, etc., and abelian categories can always be realized as some kind of enriched sets, but this is somewhat beyond the scope of our course).

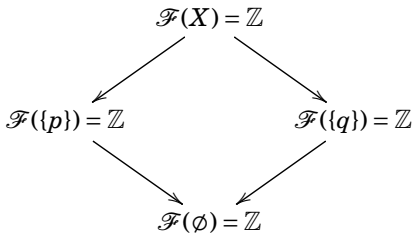
Definition. If X is a topological space and $\mathscr{F}$ is a $\mathscr{C}$-valued presheaf on X, then $\mathscr{F}$ is a *sheaf* if it satisfies the following two additional axioms.

[27] No pun intended.

- For any open $U \subseteq X$ and $s, t \in \mathscr{F}(U)$, if $\{U_i\}_{i\in I}$ is a (possibly infinite) cover of U such that $\mathrm{res}_{U,U_i}(s) = \mathrm{res}_{U,U_i}(t)$ for all i, then $s = t$ in $\mathscr{F}(U)$.
- If $U \subseteq X$ is open and $\{U_i \to U\}_{i\in I}$ is an open covering, then suppose that for each $i \in I$, there's an $s_i \in \mathscr{F}(U_i)$ such that for all i and j, $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$; then, there's some $s \in \mathscr{F}(U)$ such that $s|_{U_i} = s_i$.

The first example is the sheaf of continuous functions on a topological space X, which is a sheaf of rings; here, the key is that continuous functions satisfy the gluing axioms nicely. If X is a variety, then regular functions on open subsets of X form a sheaf, which is also a sheaf of rings.

Let $X = \{p, q\}$ be the two-point space with the *discrete topology* (i.e., every set is open). Define a presheaf $\mathscr{F}$ by letting $\mathscr{F}(U) = \mathbb{Z}$ for each open $U \subseteq X$, where the restriction map is the identity. That is, we can summarize it in the following diagram.



For now, let's ignore the condition that $\mathscr{F}(\emptyset) = 0$, and think about gluing. The empty set can be covered by anything, especially by the empty cover $\{U_i \to U\}_{i\in\emptyset}$. This means that, since there's nothing to check, then any two elements in $\mathscr{F}(\emptyset)$ must be the same! This is the reason that one require $\mathscr{F}(\emptyset)$ to be the terminal object, which in any concrete case we'll use is a single-element set (group, ring, module, etc.).

Awesome, so let's replace $\mathbb{Z}$ with 0, and $\mathbb{Z} \to 0$ is the zero map. So now, if $1 \in \mathscr{F}(\{p\})$ and $2 \in \mathscr{F}(\{q\})$, then they glue to 0, sure, but there's no way to lift to $\mathscr{F}(X)$, since these two are a cover.

Exercise 18.1. However, if one replaces $\mathscr{F}(X)$ with $\mathbb{Z} \oplus \mathbb{Z}$, the result is a sheaf, called a *constant sheaf*. Prove this; what are the restriction maps?

It's also important to talk about morphisms of sheaves, but we won't need that today.

Affine Schemes. Now, we can talk about arbitrary rings. Let A be a commutative ring with identity (no Noetherian condition exists here).

Definition. The *spectrum* of A, denoted $\mathrm{Spec}(A)$, is the set of prime ideals of A.

$\mathrm{Spec}(A)$ has a topology on it, again called the *Zariski topology*, in which the closed sets are those of the following form: for an ideal $\mathfrak{a} \subseteq A$, one gets the closed set $V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p}\}$.

It's important to check that this is really a topology, but just as in the affine case,

$$\bigcap_{i\in I} V(\mathfrak{a}_i) = V\left(\sum_{i\in I} \mathfrak{a}_i\right),$$

since $\mathfrak{p} \supseteq \mathfrak{a}_i$ for all i iff $\mathfrak{p}$ contains the ideal generated by the $\mathfrak{a}_i$. Similarly, we also have that:

- $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$.
- If $V(\mathfrak{a}) \supseteq V(\mathfrak{b})$, then $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$.

These can be thought of as a more general version of the Nullstellensatz.

Now, it's possible to define a presheaf on the topological space $X = \mathrm{Spec}(A)$: for each open $U \subseteq X$, associate the ring of functions $f : U \to \prod_{\mathfrak{p}\in U} A_{\mathfrak{p}}$, with the condition that for each $\mathfrak{q} \in U$, there exits an open $V \subset U$ with $\mathfrak{q} \in V$ and some $a, g \in A$ such that $g(\mathfrak{p}) \neq 0$ for any $\mathfrak{p} \in V$ and f can be expressed as a/g in V.

This is a little weird, but it encompasses the same notion as regular or rational functions at a point, but in the more general case than affine varieties. And checking that it is in fact a presheaf is a little strange, but makes sense; this relates to the ways that regular functions could be restricted that we talked about last week.

To check that it is a sheaf, the idea to check not that $s = t$, but $s - t = 0$; the idea is that if s can be written as $0/g$ anywhere locally, then $s = 0$ in some open set, and therefore $s = 0$ everywhere.

This is an interesting difference between presheaves and sheaves: presheaves are only defined on open sets, but sheaves have stalks, and the gluing axiom is really more global.

19. Morphisms of Varieties and Projective Varieties: 2/20/15

"It's exactly the same picture, but there are blobs here, so I feel like I'm doing geometry."

One consequence of talking about maps of varieties will be to unify the projective notions from the first few weeks of class with the more general things we're discussing now.

We started with just irreducible (affine) varieties X. Then, the regular functions on an open $U \subseteq X$ correspond to sections of the structure sheaf $\mathcal{O}$ on U, and are also those elements of $\mathrm{Frac}(R)$ that are regular at all points of U. Additionally, on $\mathrm{mSpec}(R)$, we just get R back, which is just the argument with the ideal of denominators.

Sections of $\mathcal{O}$ on U are the regular functions, i.e. the $\overline{k}$-valued functions on U. But near any point $p \in U$, one can write these as $f = g/h$ for $h \neq 0$ in a neighborhood $V \subseteq U$ containing p.

Suppose we have a regular function b on $\mathrm{mSpec}(R)$, not just an element of R (though we'll get there). Is $b \in R$? In other words, is the map $R \to \mathrm{Reg}(\mathrm{mSpec}(R))$ injective? Is it surjective?

For injectivity, suppose $r_1, r_2 \in R$, and suppose $r_1 = r_2$ as regular functions. Then, are they equal in R? This is actually kind of trivial, because it's equivalent to asking whether the zero function corresponds to the $0 \in R$, which is true. Functions are determined by their values (since R is nilpotent-free), which is untrue when one generalizes to schemes.

Why is it surjective? Let r be a regular function on $X = \mathrm{mSpec}(R)$. *A priori*, this seems kind of ugly, because there are an infinite number of points to check on. But we can make this easier to deal with by covering X with sets of the form $D(h)$, where $r = a/h$ on that set. (This implicitly requires a little clearing of denominators: r may not look like a/h everywhere, but it does somewhere, and since they're a basis, one can find a g such that $D(g) \subset D(h)$, and then write $r = ag/gh$.)

So now the question is, what's the union of these $D(f_i)$? Consider $I = (f_{\mathfrak{p}})_{\mathfrak{p} \in \mathrm{mSpec}(R)}$. Then, $I \subsetneq \mathfrak{m}$ for any maximal ideal $\mathfrak{m}$, so that means $I = R$, and in particular, $1 \in I$, so it's a finite sum of $r_i f_i$; in fact, one can use a finite number of such i, by compactness. In other words, $R = I = (f_i)$, so $X = \bigcup D(f_i)$ for a finite number of i.

So now, we have finitely many distinguished subsets, and therefore $\bigoplus_{i=1}^{n} R_{f_i}$, and they agree on the overlaps, i.e. $a_i/f_i = a_j/f_j$ on $D(f_i, f_j)$. Then, $(f_1, \ldots, f_n) = 1$, or $r_1 f_1 + \cdots + r_n f_n = 1$. Next question: why can this be used to find something in R? This is a somewhat rhetorical question, but once it's done, we'll really know what varieties are.

This felt a little like a black box, maybe a bit confusing, but it's the only such black box in the class.

Morphisms of Varieties. First, we'll recall the notion of a map of varieties.

Definition. Let X and Y be varieties. Then, a *morphism of varieties* $\pi : X \to Y$ is a continuous map such that for every $U \subset Y$, every regular function on U pulls back to a regular function on $\pi(U)$.

Consider a map $X = \mathrm{mSpec}(A) \to Y = \mathrm{mSpec}(B)$. This map was induced from $\phi : B \to A$. We want to prove this is a map of varieties more generally, but notice: we want to prove things on arbitrary open sets, so we want to prove it for $D(f)$, where we know exactly what the regular functions are, and then use the fact that sets of the form $D(f)$ cover the whole space. But this is pretty nice, because on $D(f)$, we can write all regular functions as a/f for some $a \in R$, and this pulls back to $\phi(a)/\phi(f)$, so we're good.

However, can we go in the other direction? Given a morphism of varieties $X \to Y$, is it a map of affine varieties? It induces a map of varieties, but why is it the same map? Consider a $p \in X$; then, there are two maps. In each case, how does one tell where p goes? In the new case, it'll go to q_{new}, and in the old case to q_{old}.

Given a maximal ideal of A, which is equivalent to a map $A \to \overline{k}$, one can get a maximal ideal of B by precomposing. Then, consider all functions on $\mathrm{mSpec}(B)$ whose pullback vanishes at p. This is the maximal ideal q_{old}, because that's just what the old map does.

It's also q_{new}, because it can be recognized as the functions whose pullbacks vanish at p (and there can't be anything else, since it's a maximal ideal). Thus, this is q_{old} again (but this is a little weird to understand; try tracing back to exactly how everything was defined).

Example 19.1. Consider the conic $x^2 + y^2 = z^2$ in $\mathbb{P}^2$.

First of all, $\mathbb{P}^2$ is a variety, because it's covered by two open sets, $z \neq 0$, corresponding to the ring $k[x/z, y/z]$, and when $y \neq 0$, we get $k[x/y, z/y]$ (and there's a further one, where $x \neq 0$, in the same way). Let $a = x/z$, $b = y/z$, $c = x/y$, and $d = z/y$. Then, we want to identify $\mathrm{mSpec}\, k[a,b]_b$ and $\mathrm{mSpec}\, k[c,d]_d$. But this is equivalent to identifying the rings. But $c = a/b$ and $d = 1/b$, and $a = c/d$ and $b = 1/d$, so these glue together nicely. Then, adding the third open, $\mathbb{P}^2$ becomes a variety.

The conic $x^2 + y^2 = z^2$ can be realized on these three affine spaces. When $z \neq 0$, it's the max-spec of $k[a,b]/(a^2 + b^2 - 1)$; when $y \neq 0$, its coordinate ring is $k[c,d]/(c^2 + 1 = d^2)$, and similarly for the third open. Thus, this is a variety with a sheaf of rings.

When $z \neq 0$, then $b \neq 0$, so it's possible to localize $k[a,b]/(a^2 + b^2 - 1)$ at b, and similarly $k[c,d]/(c^2 + 1 = d^2)$ can be localized at d. Then, the goal is to show these are isomorphic (which is the statement of gluing), and the isomorphism is given by $a = c/d$, $b = 1/d$, etc.

Thus, we can rigorously define the notion of a *projective variety*: since $\mathbb{P}^n$ is a variety, then one can use homogeneous equations to cut out a subset of $\mathbb{P}^n$, which can be patched into a bunch of affines just like the above example.

Exercise 19.2.

(1) Show that $x^2+y^2=z^2$ in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$ as varieties.
(2) Show that $xy-zw=0$ in $\mathbb{P}^3$ is isomorphic to $\mathbb{P}^1\times\mathbb{P}^1$ as varieties.

Now, we have the tools to say what "isomorphic" means, independent of field or such; it's the real deal.

20. Products and Projective Varieties: 2/23/15

"There's no eraser in here... there must have been a philosophy class in here before."

If X and Y are prevarieties, one can defined their *product* $X\times Y$; for example, given varieties corresponding to $k[x_1,\dots,x_m]/(f_1,\dots,f_r)$ and $k[y_1,\dots,y_n]/(g_1,\dots,g_s)$. Then, the product is given by taking all the variables and all the relations: it's the MaxSpec of $k[x_1,\dots,x_m,y_1,\dots,y_n]/(f_1,\dots,f_r,g_1,\dots,g_s)$.

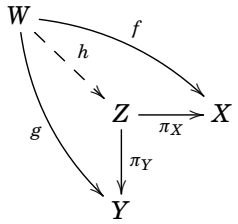
This is cool, but it's not clearly well-defined. What if a variety has two different presentations given by patching together affines in different ways, or by different generators and relations? Maybe we can prove some independence result, but it will be a mess.

There's a more elegant way to do this.

Definition. Let X and Y be objects in a category $\mathscr{C}$. Then, $Z\in\mathscr{C}$ is a *product* for X and Y, denoted $Z=X\times Y$, if there are maps $\pi_Y: Z\to Y$ and $\pi_X: Z\to X$ if for all objects W of $\mathscr{C}$ with maps $f: W\to X$ and $g: W\to Y$, there is a unique map $h: W\to Z$ such that $\pi_X\circ h=f$ and $\pi_Y\circ h=g$.

Products may not exist in a given category (e.g. fields, since $\mathbb{Q}\times\mathbb{Q}$ is not a field), but if they do, they are the familiar products wherever you've seen them: sets, groups, rings, topological spaces, manifolds, vector spaces, modules, and now varieties. The maps π_X and π_Y should be thought of as coming with the product object.

Traditionally, one can draw a diagram here, and the commutativity of the diagram encapsulates the definition of the product: let X, Y, Z, and W be as above. Then, the definition requires that there's a unique h such that the following diagram commutes.



Remember products of sets? Your grandfather may have told you, sitting on his front porch, that if A and B are sets, then $A\times B$ is the set of ordered pairs (a,b) for $a\in A$ and $b\in B$. But maybe down in Louisiana they defined them as the set AB of $\binom{a}{b}$ with $a\in A$ and $b\in B$. But the point of the more abstract definition is that there are maps $A\times B\leftrightarrows AB$, and they're unique. This means they must compose as the identity, since $\pi_X\circ h=f$ and so on, and therefore they're inverses of each other. In particular, if Z and W are both products of X and Y, then *they are uniquely isomorphic*.

Exercise 20.1. Check that the product we defined on affine varieties satisfies the categorical definition.

Note that this is not the product as topological spaces! For example, if $X=k$ and $Y=k$, the topology on $\mathbb{A}^2$ is not that on $\mathbb{A}^1\times\mathbb{A}^1$ (since there are more curves to be closed in the Zariski topology).

Now, we can return to $\mathbb{P}^1\times\mathbb{P}^1$, with coordinates $[u,1]$ and $[1,v]$ (two copies of $\mathbb{A}^1$ for the first coordinate) and $[s,1]$ and $[1,t]$ (two more copies of $\mathbb{A}^1$ for the second coordinate). Then, for $wz-xy=0$, send $(u,s)\mapsto(us,u,s,1)$, $(u,t)\mapsto(u,ut,1,t)$ (so that they agree on the overlap), and so on: on each of these open sets, one can check that they agree on the overlaps, and that these are continuous bijections with continuous inverses, which is a little less fun to think about.

Products are useful for structures like manifolds and varieties where there may be more than one way to think about an abstract objects: there are many ways to cover manifolds with charts and atlases, so proving that products exist and are unique is extremely messy. But the categorical definition makes it more abstract and a little weirder, but much slicker.

Projective Varieties. One interesting aspect of products is that since there is a map $\mathrm{id}: X\to X$, and there are maps $\pi_{1,2}: X\times X\rightrightarrows X$ (specified as part of the product), then the universal property of a product says that there must be a unique map $X\to X\times X$. This is called the *diagonal map*. It usually isn't that weird (e.g. in sets, groups, rings, or topological spaces, this sends $x\mapsto(x,x)$). This is a nice example of something that comes for free with the more abstract definition.

Definition. A prevariety X is a *variety* if the diagonal map $X \to X \times X$ has closed image.

This is a weird analogue of the Hausdorff condition, akin to a condition on a *premanifold* (like a manifold, but not Hausdorff) that turns it into a manifold.

So you believed you knew what products were, but were lied to; it turns out, you were lied to about projective varieties, too: the definition already given involved choice of the covering affine sets. This is a useful way to think about it, but it's not as nice as a definition.

We want to be able to do this in a reasonably choice-free way, e.g. starting with $k[x_0,\dots,x_n]$ and a bunch of homogeneous polynomials that describe how it's cut out of projective space. We'll want a projective prevariety to be a prevariety, i.e. a set with a topology and a sheaf of functions.

It's a little weird to think of how, e.g. $\mathbb{P}^2$ sits in $\mathbb{R}^3$, but the set of points is just what we wanted before: $(n+1)$-tuples of points in k on which an ideal of homogeneous polynomials vanishes; then, the topology is given by closed sets, the vanishing sets of ideals I of homogeneous polynomials.

One annoying thing is that the traditional Nullstellensatz is false for stupid reasons in projective space; there exists a proper ideal I such that $V(I) = \emptyset$. This has exactly one exception: $I = (x_1,\dots,x_n)$. This is therefore sometimes called the *irrelevant ideal*.

Exercise 20.2. Prove that there is no other ideal J such that $J \subsetneq k[x_0,\dots,x_n]$, but $V(J) = \emptyset$.

Now, the sheaf: take regular (or algebraic) functions similarly to before, the functions which locally are degree-0 quotients of homogeneous polynomials (i.e. f/g where $\deg(f) = \deg(g)$), which are defined on open sets, which give rise to the sheaf.

For example, consider the map $\mathbb{P}^1 \times \mathbb{P}^1 \to \{wz - yx = 0\} \subset \mathbb{P}^3$ sending $[\ell, m] \times [n, p] \mapsto [\ell n, \ell p, mn, mp]$.

Schemes. Now, we have a few minutes left, so let's define schemes.

We know already an affine scheme is a topological space $X = \mathrm{Spec}(R)$, whose points are prime ideals, and with the Zariski topology. Then, the sheaf of functions is given again by the ring of functions f/g where $g \neq 0$, since $\{g \neq 0\}$ is open.

Then, the same Hausdorff-like condition (called *separatedness*) applies to schemes just like varieties.

21. Varieties in Action: 2/25/15

Today, we'll try to do mostly examples, first for varieties (and morphisms between them), and then maybe for schemes too. With time, we may cover a bit of dimension theory. Though we're talking about varieties today, we're not going to rely on separatedness, so this all works for prevarieties as well.

Given the field k, which can also be thought of as the variety $\mathbb{A}^1$, whose ring is $k[v]$, then we can build $\mathbb{P}^1$ by gluing it with another copy of $\mathbb{A}^1$ with ring of functions $k[u]$, such that they agree on the intersection (not the north and south poles).

To glue them, we need to glue the topological space, but more interestingly also the sheaves of functions. We'll send $u \mapsto 1/v$ and $v \mapsto 1/u$, which creates a bijection of sets, between the set of everything but the poles and itself, and also leads to gluing on the sheaves: we get $k[u]_u = k[u, 1/u] \cong k[v, 1/v]$ (which is isomorphic through $u = 1/v$, albeit in a silly way). This defines the entire variety: the points, the rings, the topology, and even the sheaf of functions. This is exactly the information we want.

But what about an open set, e.g. all of $\mathbb{P}^1$, which isn't covered by one of the affines? The whole point of the sheaf is that different maps can be glued together, so it ends up working out. All we needed to do to make them glue was to describe an isomorphism of the rings.

But there's an even more obvious isomorphism: what if we instead glued along the isomorphism $u = v$? This is a prevariety, but the result isn't $\mathbb{P}^1$. Since they're glued everywhere except at the origin, the result is a copy of $\mathbb{A}^1$, except with two copies of the origin. This is noticeably non-Hausdorff.

One quick way to check that this isn't $\mathbb{P}^1$ is that on $\mathbb{P}^1$, there are no non-constant regular functions, but here, $3u + 1 = 3v + 1$ is a nonconstant function.

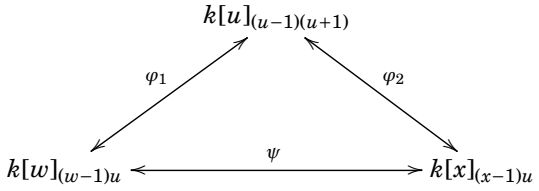
Thus, one can ask what sorts of gluings are possible. This means asking what the isomorphisms $k[u] \xrightarrow{\sim} k[u]$ are, i.e. its automorphisms. More generally, if R is any such ring (not necessarily $k[u, 1/u]$), what do its automorphisms look like?

Within $k[u, 1/u]$, the only units are λu^a, $\lambda \in k$ and $a \in \mathbb{Z}$. Scaling λ doesn't do much, so to get constants, there are only two choices, $a = 1$ and $a = -1$.

Now, we can go back and make rigorous something from very early on in the quarter: that $\mathrm{Aut}(\mathbb{P}^1)$ is the group of fractional linear transformations. Now, we actually know what automorphisms of varieties are, so we can check if fractional linear transformations satisfy the definition.

For example, consider $f : u \mapsto (u+1)/(u-1)$. How does this boil down on the affines? We want $k[u] \leftrightarrow k[w]$ and $k[v] \leftrightarrow k[x]$. f is defined on everything except 1, so it creates an isomorphism $k[u]_{u-1} \leftarrow k[w]_{w-1}$, given by $w \mapsto (u+1)/(u-1)$. Then, it's important to check that this is invertible; this ends up being its own inverse. The map on the other affine sending $k[x] \to k[v]$, hits everything except -1 (where would have the point at infinity gone?), and the map in the other direction hits everything except 1. Thus, we have maps $k[v]_{v+1} \leftrightarrows k[x]_{x-1}$.

Finally, we need to check that the map is the same on the overlaps. The intersection is $k[u]_{(u-1)(u+1)}$, and so we already have φ_1 and φ_2 as isomorphisms in the following diagram, so ψ is an isomorphsim, and the diagram commutes.



In summary, to check whether two varieties are isomorphic, check on the affines, at which point it just boils down to investigating a bunch of ring maps. There's some sheafiness here, but it's not fundamental to understanding everything.

Using this strategy, one can prove all fractional linear transformations are automorphsims of $\mathbb{P}^1$. How can we prove that all automorphisms are fractional linear? It's sufficient to show that if $\phi \in \mathrm{Aut}(\mathbb{P}^1)$, then $\phi \in \mathrm{PGL}(2)$, since we established the equivalence of PGL(2) and fractional linear transformations. And it's possible to reduce further: no matter what $\phi(0)$, $\phi(1)$, and $\phi(\infty)$ are, since PGL(2) is 3-transitive, then there's an α sending them to 0, 1, and ∞ respectively, so their composition is a $\beta \in \mathrm{PGL}(2)$ sending $0 \mapsto 0$, $1 \mapsto 1$, and $\infty \mapsto \infty$, so $\beta = \mathrm{id}$, and therefore $\phi = \alpha^{-1}$. (There's more work here, but this is the general idea.)

In particular, since $\infty \mapsto \infty$, we can restrict to $\mathbb{P}^1 \setminus \infty = \mathbb{A}^1$. Thus, it's equivalent to a map $k[u] \leftarrow k[u]$, and it's invertible, so $u \mapsto au + b$. But $0 \mapsto 0$ and $1 \mapsto 1$, so $a = 1$ and $b = 0$. This is the complete proof.

Thinking About Schemes. We know how to think about varieties, with their well-behaved rings of functions, but what about more general rings?

- $\mathbb{Z}/6$ isn't nilpotent. Its prime ideals are (2) and (3), so the Zariski topology is pretty discrete. 4 is a function, defined on points as 0 mod 2 and 1 mod 3. This ends up relating to the Chinese remainder theorem.
- Consider $k[x]/(x^2)$. Geometrically, this sits within the affine line $\mathbb{A}^1$, at a single point, but we have more than that; we have an x such that $x \neq 0$, but $x^2 \neq 0$. The functions are things like $3+4x$, but they're not just determined by their values on the single point.
- Let X and Y be varieties on $k^n = \mathbb{A}^n$; then, let I and J be their vanishing ideals. Usually, one would take $\sqrt{I \cup J}$ to calculate their intersection, but now, we don't have to worry about radicals. For example, if $X = \{x = 0\}$ and $Y = \{x = y^2\}$, then the result is just $k[x]/(x^2)$. Geometrically, the intersection is a point again, but the nilpotence provides information about the direction of the tangent line at that point (i.e. along the y-axis), since the only thing left is the degree-one y-term, which is the directional derivative there.

This is most of the weirdness that happens when one goes from varieties to schemes: nilpotents keep track of infinitesimal information, and generic points are weird, but there's not too much to say about them. If you're still worried, pick an example and work it out; there's somehow nothing to worry about, and the world becomes much bigger seemingly for free.

The last caveat is that functions aren't determined by their values, but that's true of finite fields as well, so that's not so odd.

22. Dimension: 2/27/15

To make sense of dimension, there's a little bit of a question. Geometric objects tend to have dimension associated with them. For example, $\mathbb{A}^2_{\mathbb{C}} = \mathbb{C}^2$ should have dimension 2 or 4 (as a complex or real manifold, respectively), but intuitively, it ought to have two dimensions. But then, what about $\mathbb{A}^2_{\mathbb{F}_p}$? This has only p^2 points, so it's zero-dimensional if one thinks about dimension on the old-fashioned way — and $\mathbb{A}^1_{\mathbb{F}_{p^2}}$ has the same number of points, but maybe it ought to be one-dimensional.

Though we've been thinking mostly about algebraically closed fields, the definition of dimension that we'll get to works more generally too. However, we've only really defined varieties over an algebraically closed field, so we'll stay there. Furthermore, we'll stick with irreducible varieties, because it's not worth our time asking what the dimension of a line union a plane is.

Given an irreducible variety X over an algebraically closed field k, there's a function field $K(X)$, which is finitely generated over k (since this is true on each affine that's part of a cover).

This leads to the notion of transcendence degree. Consider the ring of functions on $y^2 = x^3 - x$. It can be given by $k[x,y]$, but there are algebraic (i.e. polynomial) relations between them, so in some sense only one is really necessary to create the extension.

The reason this all works so nicely is that algebraic independence and dimension of function fields or varieties will work exactly like linear independence for the dimension of vector spaces.

Definition.

- If K/k is a field extension, then $x_1,\dots,x_n \in K$ are *algebraically independent* if there is no polynomial relation over k among them (i.e. a nontrivial function $f(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$ that is equal to 0).
- Let K/k be a (finitely generated) field extension. Then, the *transcendence degree* of K, denoted $\mathrm{trdeg}(K)$, is the size of any maximal set of algebraically independent elements (called a *transcendence basis*) of K.
- The *dimension* of an algebraic variety X is $\dim(X) = \mathrm{trdeg}(K(X))$.

Intuitively, just as in a vector space, this corresponds to degrees of freedom of movement.

Definition. A field extension E/F is *algebraic* if every element $e \in E$ satisfies some algebraic relation over F, i.e. there exists a monic $f \in F[x]$ such that $f(e) = 0$. An element that isn't algebraic is called *transcendental*, and a field extension of the form $k(x_1,\dots,x_n)/k$ is called *transcendent* (or sometimes also *transcendental*).

Be careful; some of these similar-sounding words mean different things. Also, a field extension is algebraic iff it has transcendence degree zero.

Notice that intrinsically, transcendental elements look the same, so $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$.

Let K/k be a field extension; then, it's possible to introduce an equivalence relation on subfields of K that contain k; specifically, if $E, E' \hookrightarrow K$ are extensions of k, then $E \sim E'$ if their compositum EE' is algebraic over E and over E'. What this really means is that everything in E is algebraic over E' and vice versa, or equivalently that E and E' are both algebraic over $E \cap E'$.

For example, let $X = \mathrm{mSpec}(k[x,y,z]/(y^2 - x^3 - x))$. Then, $k(X)$ contains as subextensions $k(x)$ and $k(y)$, which are equivalent under this relation, since their intersection is $k(y^2) = k(x^3 - x)$ (and they both have transcendence degree 0), but $k(x,z)$ isn't equivalent to them.

We want this to really be an equivalence relation; as usual, everything is clear except transitivity. Recall that if K'/K is algebraic and K/k is algebraic, then K'/k is algebraic (since adding finitely many algebraic elements twice is still adding finitely many). Thus, transitivity of the equivalence relation follows.

This motivates a redefinition of transcendence basis.

Definition. If E/F is a field extension, then $x_1,\dots,x_n$ is a *transcendence basis* if $x_1,\dots,x_n$ are algebraically independent and $F(x_1,\dots,x_n) \sim E$.

This will be useful for establishing that dimension is well-defined, c.f. the following proposition.

Proposition 22.1. *Any two transcendence bases of a field extension E/F are the same size.*

Proof. Let $x_1,\dots,x_m$ and $y_1,\dots,y_n$ be transcendence bases for E/F. Then, $F(x_1,\dots,x_m) \sim E \sim F(y_1,\dots,y_n)$, and in particular, each is algebraic over the other. Just like in linear algebra, the goal is to substitute elements of $y_1,\dots,y_n$ for elements of $x_1,\dots,x_m$.

Without loss of generality, assume $m < n$. Then, we can toss in y_1; since $F(x_1,\dots,x_m) \sim E$, then $F(x_1,\dots,x_m) \sim F(x_1,\dots,x_m,y_1)$, but since $x_1,\dots,x_m$ is a transcendence basis, then there's a polynomial relation for y_1 in terms of some of the x_i. Without loss of generality, assume x_m is one of them; thus, $E \sim F(x_1,\dots,x_m,y_1) \sim F(x_1,\dots,x_{m-1},y_1)$.

In the same way, toss in y_2, which means we can throw out another x_i, and so on, until we run out of elements y_j. But then, there are still some y_j left, so $F(x_1,\dots,x_m) \sim F(y_1,\dots,y_m) \sim F(y_1,\dots,y_n)$, so the remaining $y_{m+1},\dots,y_n$ are algebraic over the first m. □

The similarity between this idea and linear-algebraic dimension of vector spaces is captured in a notion called a *matroid*, which allows one to abstract these proofs and generalize them. The idea is to capture notions of independence, objects, and subobjects.

Now, we have a definition of dimension. Let's test it.

- $\dim(\mathbb{A}^n_k) = n$, because $k[x_1,\dots,x_n] \hookrightarrow k(x_1,\dots,x_n)$ have no relations.
- $\dim(\mathbb{P}^n_k) = n$ as well, because on an irreducible variety, dimension is local, so one can compute it on any affine subvariety.
- Suppose X is given by $k[x_1,\dots,x_n]/(f(x_1,\dots,x_n))$. Then, $\dim(X) = n-1$, because there's one polynomial relation between the x_i, given by f. The same applies to a homogeneous polynomial in projective space, since one can just pass to affine space and check.

Another tool used to analyze dimension is the Noether normalization theorem. Suppose $X \subset \mathbb{A}^n$; then, the goal is to find a $d < n$, so that $\mathbb{A}^d = \mathrm{mSpec}\, k[x_1, \dots, x_d]$ and $X = \mathrm{mSpec}\, k[x_1, \dots, x_d, y_1, \dots, y_{n-d}]/I$, where I encompasses some algebraic relations expressing that the y_i are algebraic over the x_i.

In summary, if $\dim(X) = d$, it should be possible to directly express X with d transcendental generators (and some algebraic ones); based on those sets of coordinates, it's possible to express every variety as some sort of hypersurface.

One way to think of it is, if things aren't working, then give it a hit (and here Prof. Vakil hit the blackboard), and things might pop down a dimension and work a little better.

23. Smoothness and Dimension: 3/2/15

Recall that if X is an irreducible variety, its dimension is $\mathrm{trdeg} K(X)$, the transcendence degree of the field of regular functions. But there's a different, equivalent notion called *Krull dimension*, which can be generalized considerably.

In $\mathbb{A}^2_{\mathbb{C}}$, we know what all the Zariski-closed sets are: points, curves, and the whole space. In $\mathbb{A}^3_{\mathbb{C}}$, there are points, curves, surfaces, and the whole space. Every irreducible set is contained in something of one dimension bigger. Thus, say that something has dimension zero if it has no irreducible (strict) subvarieties; then, dimension 1 means its only irreducible subvarieties have dimension zero, and so forth. That is, the dimension of a variety is the length of the longest chain (under strict inclusion) of irreducible closed subsets, not including the variety itself.

This is actually reasonably geometric, but it will become a little stranger once it's translated into algebra.

Definition. If R is a ring and $\mathfrak{p}$ is a prime ideal of R, the *Krull dimension* of $\mathrm{mSpec}(R/\mathfrak{p})$ is the supremum of the length of all chains $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ (i.e. the length of this chain is n).

Topologically, this creates a dimension on the topological space $\mathrm{Spec}(R)$, but it was originally developed as a completely algebraic notion, that happened to correspond to the "right thing."

Theorem 23.1. *If X is a variety, the Krull dimension of X and the transcendence degree dimension agree.*

We won't need to prove this, but one way to think about it is that all maximal ideals of $k[x_1, \dots, x_n]$ has residue field k (when k is algebraically closed), which is the Nullstellensatz. This is because maximal ideals have Krull dimension 0, so they have transcendence degree 0!

Now, let's calculate $\dim(\mathbb{Z})$. All prime ideals are of the form (0) or (p) for a prime p. If p and q are distinct primes, then $p \notin (q)$ and vice versa, so the longest chain is $(0) \subsetneq (1)$. Thus, $\dim(\mathbb{Z}) = 1$.

What about $\mathbb{Z}[i]$? Not all prime ideals lift from $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. For example, $\mathbb{Z}[i]/(5) = \mathbb{Z}[x]/(x^2 - 1, 5) = ((\mathbb{Z}/5)[x]/(x-2)) \times ((\mathbb{Z}/5)[x]/(x+2))$, but $x^2 + 1$ doesn't factor mod 3, so $(\mathbb{Z}/3)[x]/(x^2+1) = \mathbb{F}_9$, which is a field, rather than a product. But mod 2, $\mathbb{F}_2[x]/(x^2+1) = \mathbb{F}_2[x]/((x+1)^2) = \mathbb{F}_2[t]/t^2$. This feels like a branched double cover, but in arithmetic! That is, it seems like $\mathrm{Spec}(\mathbb{Z}[i])$ is a branched double cover of $\mathrm{Spec}(\mathbb{Z})$ — and it's probably not a coincidence that each covering point is either a field extension of order 2 (at (2) or (3 mod 4)), or a product of two field extensions of order 1, at (1 mod 4). This gets weird topologically, because it's branched at exactly one point.

There's a correspondence between Galois theory and that of covering spaces, and in fact one can use this to understand the algebraic topology of $\mathrm{Spec}(\mathbb{Z})$! For example, these correspondences can be used to show that there are no nontrivial connected covering spaces, and therefore the universal cover is itself. Thus, $\pi_1(\mathrm{Spec}(\mathbb{Z}))$ is trivial — $\mathrm{Spec}(\mathbb{Z})$ is simply connected. The correspondence is beautiful: topology turns into Galois theory, and vice versa.

Returning to varieties, let $\pi : X \to Y$ be a dominant (i.e. with dense image) map of irreducible algebraic varieties, i.e. $K(X)/K(Y)$ is a field extension.

Exercise 23.2. Suppose $\pi : X \to Y$ is a map of irreducible algebraic varieties and $\dim(X) < \dim(Y)$. Then, show that π is not dominant.

Solution. If this were dominant, then $K(X)/K(Y)$ would be a field extension with a smaller transcendence degree, which cannot happen. □

If $\dim(X) = \dim(Y)$, then $K(X)/K(Y)$ is of transcendence degree zero, so it's algebraic! Thus, we can talk about its degree (since all of these are finitely generated, then this extension is even finite algebraic).

Definition. Let X and Y be irreducible algebraic varieties of the same dimension. Then, the *degree* of a dominant map $\pi : X \to Y$ is $\deg(K(X)/K(Y))$ (as a field extension).

In other words, a dominant map $X \to Y$ corresponds to an injective map $K(Y) \hookrightarrow K(X)$.

We can also talk about the codimension of a subvariety within another (which is the difference in their two dimensions). If f is a function, what possible codimensions exist for spaces $V(f)$? Clearly, if $f = 0$, we get a codimension 0 surface. If $V(f)$ is irreducible, then it's possible to show that it must have codimension 1! This can be proven geometrically or algebraically (thanks to something called Krull's principal ideal theorem). This was a little hand-wavy, but makes some intuitive sense, and can be made properly rigorous.

Claim. In $\mathbb{P}^5$, any five homogeneous equations of positive degree have a common, nontrivial solution.

Proof. Let's look at $\mathbb{A}^6$ instead. Here, since the equations are homogeneous, the solution space includes 0. Then, it must be at least one-dimensional, if it is nonempty (by calculating the solution space of the first equation, then the second in the first, and so on). But we have a solution, the origin! So the solution space is at least one-dimensional, so a solution remains when we pass to projective space. □

Smoothness. We've already discussed smoothness here and there, implicitly. It's yet another thing Brian Conrad put the brakes on in a graduate-level class, so let's talk about it.

We have, at least implicitly, the notion of the *Zariski tangent space* on a variety (or more generally, a scheme). If X is affine and $p \in X$, then it corresponds to a maximal $\mathfrak{m}$ within a ring R. Then, $\mathfrak{m}$ is an R-module, so $\mathfrak{m}/\mathfrak{m}^2$ is an $R/\mathfrak{m}$-module, i.e. a k-vector space. This is kind of weird, but has the right naturality properties to be the cotangent space; thus, take its dual to obtain the tangent space.

This *a priori* seems like it would depend on coordinates, but when we localize, taking $R_{\mathfrak{m}}$ and its maximal ideal $\mathfrak{n} = \mathfrak{m}R_{\mathfrak{m}}$, the result looks exactly the same: $\mathfrak{n}/\mathfrak{n}^2 = \mathfrak{m}/\mathfrak{m}^2$.

Well, what are the elements of this, actually? We have sets of open sets U and functions f on U, where $(f,U) \sim (g,V)$ if there's a neighborhood W of p such that $W \subset U,V$ and $f|_W = g|_W$. In other words, one takes the direct limit as the open neighborhoods get smaller and smaller, leading to the germs of functions at p, in some sense the local functions. This is a local ring, called $\mathcal{O}_p$, and its unique maximal ideal is the functions vanishing at p (since if you're not in that, it's possible to invert near p).

But this is also looks exactly like the definition of the tangent space to a manifold. A manifold, of course, is a ringed space, and the tangents are germs of functions near a point p! So this is actually the same notion, and the direct limit and the sheaf was hiding there the whole time. This leads to forms in algebraic geometry.

So consider the following, uh, Math 51 problem: the surfaces $x + y + x^4y^7 = 0$ and $z + (yxz)^{95} + x^4 = 0$ intersect at the origin. What's the tangent to this curve at the origin?

Instead of taking lots of derivatives and kvetching, we know $\mathfrak{m} = (x,y,z)$, and $\mathfrak{m}/\mathfrak{m}^2 = \alpha x + \beta y + \gamma z$ for some α, β, and γ. But we can restrict the curves to $\mathfrak{m}/\mathfrak{m}^2$: in particular, anything in $\mathfrak{m}^2$ dies, including *any higher powers*. This equation reduces to the much nicer $x + y = 0$ and $z = 0$, and the linearization is exactly what they would get anyways. If the linearization becomes $0 = 0$, then there is no nice tangent space (wrong dimension), which means it's not smooth. But it's always true that $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \le \dim(X)$.

Exercise 23.3. Check that the integers are a smooth curve.

This is all really just calculus. Or maybe calculus is really just algebraic and differential geometry, which is why these definitions seem to be the right ones.

24. The Tangent and Cotangent Spaces: 3/6/15

Today's lecture was given by Donghai Pan.

Assume k is an algebraically closed field and $f(x,y) \in k[x,y]$. Then, if $f \in (x,y)$, then $f(x,y) = \alpha x + \beta y + \cdots$. Assume at least one of α and β are nonzero; then, the curve corresponding to $k[x,y]/(f)$ is smooth at the origin (in the sense of taking partial derivatives, as well as the sense of algebraic geometry), and the tangent line is given by $0 = \alpha x + \beta y$. Another way of saying this is that the tangent vector has the form $t(\beta, -\alpha)$ for $t \in k$.

Last time, we defined the cotangent vector space: if $\mathfrak{n}$ denotes the maximal ideal $(0,0)/(f)$, then this is just $\mathfrak{n}/\mathfrak{n}^2$. That is, $\mathfrak{n}/\mathfrak{n}^2 = (\mathfrak{m}/(f))/(\mathfrak{m}/(f))^2$ (where $\mathfrak{m} = (0,0)$), but this is just $\mathfrak{m}/(\mathfrak{m}^2 + (f))$ (the sum of modules given by taking sums of generators of $\mathfrak{m}$ and of (f)). This can be viewed as the quotient space of $\mathfrak{m}/\mathfrak{m}^2$ by (f_1), where f_1 denotes the linear term of f. But this is therefore $\{(u,v) \mid \alpha u + \beta v = 0\}$.

Since this is the cotangent space, the elements ought to be linear functionals, and the action is $\alpha(1,0) = 1$ and $\alpha(0,1) = 0$ (and then, since we need the sum to be zero, this defines how β acts). This means that we really get the linear functionals we were looking for, so this is in fact the cotangent space.

The next question is, how does the tangent vector come out of this? Recall that inside the ring $k[x,\varepsilon]/(\varepsilon^2)$, the map $x \mapsto x + \varepsilon$ sends an $f(x) \in k[x]$ to $f(x) + f'(x) \cdot \varepsilon$. Since this space contains information about the derivative of f, it's used to define tangent vectors, on varieties as well as on schemes.

The map $k[x,y]/(f) \to k[\varepsilon]/(\varepsilon^2)$ should be thought of as sending a point into the scheme $k[\varepsilon]/(\varepsilon^2)$ (it's not nilpotent, so it's not a variety!) that only has one maximal ideal (one point), but with some "fuzziness" which defines its direction.

Assume the preimage of (ε) is $(x,y)/(f)$, i.e. the point of $k[\varepsilon]/(\varepsilon^2)$ is sent to the origin. We could put this anywhere, so the origin isn't a bad choice, and it can be thought of as localizing at the origin. Then, $x \mapsto x_0 + x_1 \cdot \varepsilon$ and $y \mapsto y_0 + y_1 \cdot \varepsilon$, with $f(x,y) = 0 \pmod{\varepsilon^2}$. But since the constant term is 0, then $x_0 = y_0 = 0$, so $\alpha \cdot x_1\varepsilon + \beta \cdot y_1\varepsilon = 0$ implies $\alpha x_1 + \beta y_1 = 0$. Thus, this seems like a reasonable notion of tangent direction.

Another way to look at this is that if A is a local ring, then $\mathrm{Spec}(k[\varepsilon]/(\varepsilon^2)) \to \mathrm{Spec}(A)$ gives all of the tangent vectors of $\mathrm{Spec}(A)$ at the unique maximal ideal $\mathfrak{m}_A$ of A. The idea is, once we compute the corresponding map of rings, we get the tangent space. But it seems like the key is not the global scheme, but some local data near it, so one can replace $k[x,y]$ with $k[x,y]_{(f)}$.

Smoothness. Related to this is the notion of smoothness.

Definition. Let A be a Noetherian local ring (e.g. $k[x]_{(x)}$), with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. Then, A is *regular* (or is a *regular local ring*) if $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim A$ (the latter as the Krull dimension).

If A is a finitely generated k-algebra, then one can use the transcendence degree dimension, but the Krull dimension is more general.

The intuition is that regularity should be like a manifold: the dimension of a manifold, a property that can be determined locally (after all, it's the dimension of the tangent space), is a global property. A regular ring has the same property.

Example 24.1.

- If k is a field, then it's zero-dimensional as a finitely generated k-algebra (i.e. over itself), and (0) is a maximal ideal, and $\dim_k((0)/(0)) = 0$, so k is regular.
- More interestingly, $k[x]_{(x)}$ has two primes, $(0) \subseteq (x)$, and it's regular and one-dimensional.
- $\mathbb{Z}_{(p)}$ is similar, with $(0) \subseteq (p)$.

Let p be prime; then, one can take the field extension $\mathbb{F}_p[x]/(x^p - a)$ such that a doesn't have a root in $\mathbb{F}_p$. This is a somewhat funny thing, and will illustrate that regularity and smoothness aren't the same thing; they are intuitively similar for manifolds, and are indeed the same for perfect or algebraically closed fields, it's not always the case. In other words, regular schemes and smooth schemes are not the same things.

Definition. Let k be an algebraically closed field and $X \subseteq \mathbb{A}^n_k$ be an irreducible r-dimensional variety; then, an $x \in X$ is a *non-singular point* if the Jacobian matrix $\left[\frac{\partial f_i}{\partial x_j}\right]_{m \times n}$ has rank $n - r$ at x.

Proposition 24.2 (Jacobian criterion)**.** *Let k be algebraically closed and $X \subseteq \mathbb{A}^n_k$ be an irreducible variety. Then, X is* non-singular *at an $x \in X$ if $\mathcal{O}_x$ is a regular local ring.*

Proof. Let $I(X) = \mathfrak{b} \subseteq k[x_1, \dots, x_n]$. Then, an $a \in \mathbb{A}^n$ corresponds to $\mathfrak{a}_a = (x_1 - a_1, \dots, x_n - a_n)$, so its image $x \in X$ corresponds to $\mathfrak{m}_x \in k[x_1, \dots, x_n]/\mathfrak{b}$.

Then, we want to show that $\mathfrak{a}_a/\mathfrak{a}_a^2 \cong k^n$. Let $\theta : \mathfrak{a}_a \to k^n$ send

$$f \mapsto \left\langle \frac{\partial f}{\partial x_1}(x), \dots, \frac{\partial f}{\partial x_n}(x) \right\rangle.$$

Since X is non-singular, then θ is surjective.

Exercise 24.3. Show that $\ker(\theta) = \mathfrak{a}_a^2$.

Thus, $\overline{\theta} : \mathfrak{a}_a/\mathfrak{a}_a^2 \twoheadrightarrow k^n$ is an isomorphism. (Alternatively, computing the dimensions, given that the map is surjective, works too.) As before, $\mathfrak{m}_x/\mathfrak{m}_x^2$ can be identified with $\mathfrak{a}_a/(\mathfrak{a}_a + \mathfrak{b})$.

Now, what's $\theta(\mathfrak{b})$? If $\mathfrak{b} = (f_1, \dots, f_n)$, then we'll obtain $\nabla f_1, \dots, \nabla f_n$. These form into the matrix of partial derivatives (à la Math 51), and therefore the rank of the image spanned by these ∇f_i is equal to the rank of the derivative matrix.

If M', N are submodules of a module M, if $\pi : M \twoheadrightarrow M'$ is the canonical projection, then $\pi(N) = (N + M')/M'$, which is similar to the isomorphism theorems for rings. Thus, by checking the dimensions once again, $\mathfrak{b}$ is sent to $(\mathfrak{b} + \mathfrak{a}^2)/\mathfrak{a}^2$. Specifically, this has dimension $\operatorname{rank} J$, and $\mathfrak{a}_x/\mathfrak{a}_x^2$ has dimension r. Then, $\mathfrak{m}_x/\mathfrak{m}_x^2 = \mathfrak{a}_x/(\mathfrak{a}_x^2 + \mathfrak{b})$, which is a quotient of the other two modules, so its dimension is $n - r$. □

In other words, when $k = \overline{k}$, regularity and smoothness are the same for affine varieties over k.

This is still a fundamentally local idea; in general, all the calculations only care about the local rings. Thus, this statement is also true for general varieties (e.g. projective varieties); the argument is in an affine neighborhood, and that's it.

Given an affine variety X, one can look at its singular locus. By thinking about determinants, this ends up being equal to the set of x whose Jacobians have the property that all of their $(n-r) \times (n-r)$-minors have determinant 0 at x. This is a finite condition (there are finitely many such minors) and the determinant is a polynomial condition, so the singular locus is a closed subvariety of X.

25. Images of Regular Maps: 3/9/15

Recall that a *prevariety* is a ringed space that locally is homeomorphic to $\mathrm{mSpec}(k[x_1,\dots,x_n]/I)$ (a nilpotent, finitely generated k-algebra), and, of course, k is algebraically closed. However, we forgot one important part of the definition: that it is required to be *quasi-compact*: every open cover has a finite subcover.

The first part says that it has a cover by affine spaces, and the second part means that it is covered by finitely many affines. This eliminates things such as infinite sets of points, etc.

Note that quasi-compactness sounds like compactness in other parts of mathematics; the difference is the Hausdorff condition, which one does not require for varieties.

Let $\pi : X \to Y$ be a map of varieties. What can we say about $\pi(X) \subset Y$? This relates to questions such as how often two polynomial curves can intersect.

One might suspect that $\pi(X)$ is closed, but if $X = k \setminus 0$, $Y = k$, and π is inclusion, then the image is open but not closed, and if $X = \{0\}$ and π is inclusion, then the image is closed but not open, so we can't say anything about whether they're closed. The image might not even be a subvariety in some particularly weird cases. Moreover, any open or closed set could be the image of something (specifically, given by inclusion).

Well then, let's talk about what (sub)sets can be the images of maps of varieties. This includes all open and all closed sets, but also unions, intersections, and complements of these sets.

Definition.

- If X is a topological space, an $A \subseteq X$ is *locally closed* if $A = C \cap U$, where C is closed in X and U is open in X.
- A subset A of a topological space X is *constructible* if it can be built from finite unions, intersection, and complements, starting with open and closed sets.

Note that all open sets are locally closed.

Proposition 25.1. *The constructible sets are exactly the finite unions of locally closed sets.*

Theorem 25.2 (Chevalley)**.** *If $\pi : X \to Y$ is a morphism of varieties, then* $\mathrm{Im}(\pi)$ *is constructible.*

This is actually quite powerful; thus (of course!) we will use it to prove the Nullstellensatz. As tends to happen in this class, the theorem is true both for varieties and schemes, but the proofs differ.

Specifically, we will prove the most general version.

Theorem 25.3 (Nullstellensatz, general version)**.** *Let k be any field and K/k be a field extension. Then, if K is finitely generated as an algebra, then it is a finite extension of fields.*

Proof. If K isn't a finite extension of fields, but is finitely generated as a k-algebra, then there exists an $x \in K$ that is transcendental over k. Thus, $k[x] \hookrightarrow K$, so $\mathrm{Spec}\, k[x] \leftarrow \mathrm{Spec}\, K$, so mapping a point into an affine line, and we know what the points are.

In particular, we know the locally closed subsets of the affine line.

Exercise 25.4. Using the fact that $\mathbb{A}^1_k$ has the cofinite topology (as was on one of the homeworks), determine all of its locally closed sets.

This can be used to embed $\mathrm{Spec}(K)$ into $\mathrm{Spec}(K[x]/I)$, for some ideal I. But this establishes an algebraic relation for x, which is a contradiction. □

The statement about the image being closed can be recovered in a different form. Specifically, using projective space makes things work better.

Proposition 25.5. *The image of projection $\pi : \mathbb{P}^n \times Y \to Y$ is closed.*

Consider the following related problem. If we want to solve the following system of equations,

$$\begin{aligned} ax + by + cz &= 0 \\ dx + ey + fz &= 0 \\ gx + hy + kz &= 0 \end{aligned}$$

they constitute a curve in $\mathbb{A}^9$, but mapped from three curves in $\mathbb{A}^3$. This suggests that a constructive proof of Proposition 25.5 would provide a determinant. It's also related to the question as to whether two polynomials share a root, because each polynomial condition can be restated as projections from projective space.

Another result, called elimination of quantifiers, relates to interesting results in model theory and Banach's real algebras.

In $\mathbb{P}^2$, with coordinates x_0, x_1, and x_2, consider four polynomials $g_1,\dots,g_4$. Then, do they have a common solution? (We'll be able to do this for any values of 4 and 2.) It will turn out they do share a root iff they have a nontrivial solution

in $\mathbb{A}^3$ other than just $\mathbf{0}$, i.e. iff $V(g_1,\dots,g_4) \not\subset V(x_0,x_1,x_2)$, i.e. $\sqrt{(g_1,\dots,g_4)} \not\supseteq (x_0,x_1,x_2)$, i.e. $(g_1,\dots,g_4)^N \not\supseteq (x_0,x_1,x_2)$, or for all N, $(g_1,\dots,g_4) \not\supseteq (x_0^N,x_1^N,x_2^N)$ for all N, but this latter ideal is just that of degree-N homogeneous polynomials.

Then, we ran out of time, but this does lead down the right direction for this theorem (called the "fundamental theorem of elimination theory"): if S_m is the ideal of degree-m homogeneous polynomials, then there's a map $S_{N-\deg(g_1)} \oplus \cdots S_{N-\deg(g_4)} \to S_n$ (given by $(\cdot g_1,\dots,\cdot g_4)$).

Now this is just a linear algebra problem, and the question boils down to determining whether a certain matrix is surjective. And we can do that using the determinant. This is a lot of things to check, in practice, but the point is we can do it.

26. The Fundamental Theorem of Elimination Theory: 3/11/15

Definition. If X and Y are topological spaces, a *closed map* is a continuous function $f : X \to Y$ such that the image of every closed set is closed.

Theorem 26.1. *Let k be an algebraically closed field and Y be a variety. Then, $\pi : \mathbb{P}^n \times Y \to Y$ is a closed map.*

Proof. It suffices to do this in a local basis, since intersecting with an open set doesn't change the condition. In particular, one can assume Y is affine, i.e. there's a ring R such that $Y = \mathrm{mSpec}(R)$. In particular, these will be homogeneous equations with R-coefficients, and without loss of generality all of them have positive degree.

If $R = k$ is a field, then this boils down to asking if a bunch of homogeneous polynomials $g_1, g_2, \dots$ have a common nontrivial solution in $\mathbb{A}^{n+1}$ (equivalently, a solution in $\mathbb{P}^n$).

We know $V(g_1,\dots) \supseteq \overline{0} = V(x_0,\dots,x_n)$, i.e. $\sqrt{(g_1,\dots)} \subseteq (x_0,\dots,x_n)$ (since the latter ideal is already radical). Then, they have a common nontrivial solution if this inclusion is strict.

In particular, there's *no* nontrivial solution if $x_0,\dots,x_n \in \sqrt{(g_1,\dots)}$, and this is equivalent to $x_1^N,\dots,x_n^N \in (g_1,\dots)$ for some $N \in \mathbb{N}$. That is, S_M, the M^{th} graded piece of the ring $k[x_1,\dots,x_n] \subset (g_1,\dots)$ for some M (in the forward direction, $M = N$, but not necessarily in the reverse direction). That is, S_M is equal to the M^{th} graded piece of $(g_1,\dots)$, corresponding to a map $S_{M-\deg(g_1)} \oplus S_{M-\deg(g_2)} \oplus \cdots \to S_M$ that is not surjective (for all M, it's not surjective). But this is equivalent to all of the maximal minors of the corresponding matrix being 0. This is a little strange to think about, but this condition is polynomial, so the map is closed. □

Corollary 26.2. *If Y is a variety and $X \subset \mathbb{P}^n$ is a closed subset, then $\pi : X \times Y \to Y$ is also a closed map.*

We'll be able to use this in many ways; for example, consider three conics; this triple of conics lives in $Y = \mathbb{P}^5 \times \mathbb{P}^5 \times \mathbb{P}^5$. Then, the points form a $\mathbb{P}^2$. The points that pass through all three conics form a closed condition, so one can apply Corollary 26.2 to get some conditions for the conics having an intersection.

The same story works for schemes, but some of the steps of the proof need to be different.

Upper Semicontinuity of Fiber Dimension. The preimage of a point (e.g. under $\mathbb{P}^n \times Y \to Y$) is called a *fiber*,[28] I guess because it looks fibrous and is fun to say. The dimension of the fiber can vary, and we'll see how that will affect the number of solutions.

Consider $y = mx$ within $\mathbb{A}^3$, projected to the xy-plane. Most points have a single preimage, but the preimage of the origin is an $\mathbb{A}^1$ (since if $x = y = 0$, then any m works). But we would like to work in $\mathbb{P}^1$, so instead we have $ny = mx$, which is homogeneous. Once again, the dimension only jumps up on closed sets, as any m and n work at the origin, giving a $\mathbb{P}^1$.

Remark. Let $X \subset \mathbb{P}^n$ be irreducible and have dimension $d > 0$. Then, every hyperplane meets X, but also there is a hyperplane not containing X, because the intersection of all of the hyperplanes is empty. Thus, a randomly chosen hyperplane will knock the dimension down by 1.

Definition. Let Z be a closed subset of $\mathbb{P}^n \times Y$ and $\pi : Z \to Y$ be the (restriction of the) canonical projection map. Then, the *fiber dimension* $\mathrm{fd} : Y \to \mathbb{Z}$ sends $p \mapsto \dim(\pi^{-1}(p))$,[29] with $\dim(\emptyset) = -1$.

Theorem 26.3 (Upper semicontinuity of fiber dimension)**.** $\mathrm{fd}^{-1}([d, d+1, \cdots])$ *is closed.*

Notice that the case $d = 0$ is Theorem 26.1.

Proof. As seen above, pick a hyperplane H, which intersects Z, so there's a $\pi_H : Z \cap H \to Y$. The image is a closed subset, and in particular, the intersections of the images for all of the hyperplanes is still a closed set.

For the more general case d, choose d intersecting hyperplanes. □

[28] The British and French often prefer the alternate spelling *fibre*.

[29] One thing to be careful of: dimension isn't quite well-defined on open sets. So in this case, take the maximum over all compact subsets.

Theorem 26.4. *Let $\pi : X \to Y$ be a regular map of varieties; then,* $\mathrm{fd} : X \to \mathbb{Z}$ *can be defined as* $p \mapsto \dim(\pi^{-1}(\pi(p)))$*, i.e. the largest dimension of the components of* $\pi^{-1}(p)$*. Then, this* fd *is also upper semicontinuous on* X*.*

The trick in the proof is to restrict to a small open set (so we don't have to worry about affine or projective or general), so that $X \hookrightarrow \mathbb{A}^n \times Y \xrightarrow{\pi} Y$, and Y is affine too, but we can take the compatification and use $\mathbb{P}^n$ in place of $\mathbb{A}^n$. This doesn't change anything dimension-wise, since this is the closure, but allows Theorem 26.3 to imply upper semicontinuity on X.

This also works just fine for schemes.

27. Chevalley's Theorem: 3/13/15

"I feel sorry for the scribes."

Proposition 27.1. *Suppose X and Y are irreducible varieties and $\varphi : X \to Y$ is a dominant map. Then, the fiber dimensions might jump, but we know that it's upper semicontinuous. Then, it's constant on some nonempty (and therefore dense) open set.*

Proof. Without loss of generality, we can assume X and Y are affine, since we're just looking for some open set, and can shrink as necessary.

Then, $\dim(X) = \dim(Y) + \dim(\text{most fibers})$. There are two ways to prove this.

- The first will use schemes, or I guess generic points, and is meant to illustrate how they can enrich the tools one uses to prove things. Consider the generic points of X and Y; the former must be sent to the latter, because if not, then the closure, i.e. X, is sent to some non-generic point, whose closure isn't all of Y. We know the function field of Y, $FF(Y)$, has transcendence degree $\dim(Y)$ over k (by definition), and $FF(X)$ has dimension r (which is the dimension of fibers on some nonempty open) over $FF(Y)$, and dimension is additive, so we can express $\dim(X) = \dim(Y) + r$.

  There's lots to check here; specifically, some of the facts this proof leaned on require schemes, where we proved the results only for varieties. □
- There is a way to do this without generic points. Can you find it?

Theorem 27.2 (Chevalley)**.** *Let $\pi : X \to Y$ be a map of varieties. Then, $\pi(X)$ is constructible, i.e. it's a finite union of locally closed subsets.*

Proof. First, we can reduce to the case where X is irreducible; then, since all varieties are quasicompact, they have finitely many irreducible components, and finite unions of finite unions remain finite. This means we can assume Y is irreducible as well, by just choosing the irreducible component of Y that $\pi(X)$ is contained into (since $\pi(X)$ is also irreducible, and therefore contained in an irreducible component of Y). This means we can also assume Y is affine, and that π is dominant, by working within the closure of $\pi(X)$.

Proposition 27.3. *There is a dense open $U \subset Y$ such that $\pi(X) \cap U = U$, or $\pi(X) \cap U = \emptyset$.*

Proof. Since π is dominant, then $FF(Y) \hookrightarrow FF(X)$ as fields; let r be the transcendence degree of this extension, so that $r \geq 0$.

We will reduce to the case when $r = 0$: if $Y = \mathrm{mSpec}(B)$ and X is given from $B[x_1, \ldots, x_n]$, then setting $x_1 = 0$ is a nontrivial equation which reduces the dimension by 1, since x_1 is transcendent over Y. Then, pick an irreducible, affine component of this set and continue. Repeating this over and over leads to the zero case, and if the $n-1$ case has a dense open subset, then this will still be dense and open when considered within X, so the induction goes through.

Now, let's talk about the base case, when $r = 0$. We can map $X \hookrightarrow \mathbb{A}^n \times Y \to Y$, so we can also map $\overline{X} \hookrightarrow \mathbb{P}^n \times Y$. Then, $\pi(\overline{X})$ is closed, and, since π is dominant, then the image is Y! But since $\overline{X}$ is irreducible, then $\overline{X} \setminus X$ has smaller dimension than X (which has the same dimension as Y), so the image can't be all of Y; instead, it's a closed strict subset, and therefore the image of X contains a nonempty open. □

Now, since we've reduced to $Y = \overline{\pi(X)}$, but if $U = \emptyset$, then its closure must be in the closed complement, which is a finite union of locally closed subsets (which requires a little more thinking). And if $U \subset \pi(X)$, then we're done. □

There's a nicer way to deal with the inner proposition for generic points; specifically, the image of a generic point is generic, so the map in question is always dominant. Maybe this shines some light on why one would care about these weird, fat points. Furthermore, in either case, dimension theory and upper semicontinuity also have to come together to make the proof happen.

Retrospective. Well, that was an insane idea realized: teaching algebraic geometry to undergraduates. What all have we done?

- Polynomials and the curves they cut out in k^n.
- Homogeneous polynomials in $\mathbb{P}^n_k$, and that $\mathrm{Aut}(\mathbb{P}^n) = \mathrm{PGL}(n+1)$. Linear polynomials in projective space. Bézout's theorem.
- Higher-degree polynomials, where it's useful to have k algebraically closed. As a particular case, conics (degree-2): their classification, as long as k is algebraically closed. In degree-3 cubics, we talked about the group law (though we never did prove associativity...), and their Weierstrass normal forms, so long as they had a flex point.
- This group law makes a lot more sense if we had topology, e.g. over $\mathbb{C}$. But more generally, we have the Zariski topology, which began with vanishing sets $V(I) \subset \mathbb{A}^n$, the closed sets of a weird and wild topology. This leads to Noetherian rings, with the consequences that infinitely many equations on $\mathbb{A}^n$ are the same as finitely many, and that every affine variety has finitely many irreducible components. In the other direction, we have $I(S)$, so that $V(I(S)) = \overline{S}$ and $I(V(J)) = \sqrt{J}$, which is the Nullstellensatz! Moreover, all affine varieties are quasicompact.

(This is already well over a quarter's work, but we were just a few weeks in!)

- Affine varieties, with their maps $X \to Y$, form a category. So do affine schemes (just for fun).
- The relation between rational functions and regular functions, relating to localization in algebra; domains of definition, which are big (i.e. nonempty) open sets. We saw birational maps between algebraic varieties; whenever we can easily solve a Diophantine equation, it was birational to $\mathbb{A}^n$, but there are cubics that aren't birational, and therefore are somewhat harder to solve.
- We defined varieties, and prevarieties; this involved talking about sheaves, including the sheaf of regular functions on (irreducible) affine varieties. Then, varieties are given by quasicompact locally ringed spaces (so with the sheaf of functions) which locally look like affine varieties. This allows one to define manifolds, products, Hausdorff spaces, projective varieties, and so forth.

If you're keeping track, this is a second quarter's worth of stuff.

- Dimension theory! The transcendence degree and Krull dimensions agree in the cases we care about, and the definition of smoothness and the Zariski cotangent space, which are a sort of calculus. A nontrivial equation cuts the dimension down by one.
- The fundamental theorem of elimination theory, upper semicontinuity of dimension, and Chevalley's theorem.

I think that makes for a third quarter of content. How wonderfully insane. The writing projects will add at least a quarter's more worth of material.