Algebraic geometry

Lectures by Richard Borcherds, notes by Søren Fuglede Jørgensen

Math 256, UC Berkeley, Fall 2010

Contents

Disclaimer

These are notes from a course given by Richard Borcherds in 2010.[1] They have been written and TeX'ed during the lecture and some parts have not been completely proofread, so there are bound to be a number of typos and mistakes that should be attributed to me rather than the lecturer. Also, I've made these notes primarily to be able to look back on what actually happened myself,

[1] The course homepage is located at `http://math.berkeley.edu/~reb/courses/256A/index.html` – that probably won't be true forever though.

and to get experience with TeX'ing live. That being said, feel very free to send any comments and or corrections to `fuglede@imf.au.dk`. Also, let me thank Yael Degany for proofreading large part of these notes.

I chose not to include the first one and a half lecture in these notes. These were primarily about various examples that, while clearly relevant and important examples, are somewhat cumbersome to TeX, and I'm lazy. Also, Richard Borcherds more or less has these examples written out in detail in his own lecture notes, currently available at `http://math.berkeley.edu/~reb/courses/256A/256A.pdf`.

Second lecture, August 31st 2010

1 Affine varieties

Definition 1. *Affine space* is defined to be k^n (which we will also write A^n) for some field k.

Classically, the field k in question was taken to be the set of complex numbers. More generally, we will consider some algebraically closed field of characteristic 0. It is also possible to consider algebraic geometry in positive characteristic as was done by Weil or over a completely general field; however, in the latter case, one runs into considerable trouble considering $\mathbb{Q}$.

1.1 Algebraic sets and the Zariski topology

Definition 2. An algebraic set is the set of common zeros in A^n for a set T of polynomials.

Obviously, $\emptyset$ and A^n are algebraic sets, and it is also easy to see, that the set of algebraic sets is closed under intersection. It is also closed under finite union: For two algebraic sets Y_1 and Y_2 the set $Y_1 \cup Y_2$ is the set of zeros of polynomials $t_1 t_2$, for $t_1 \in Y_1$,$t_2 \in Y_2$. In other words, the algebraic sets are the *closed* sets of a topology on A^n called the *Zariski* topology.

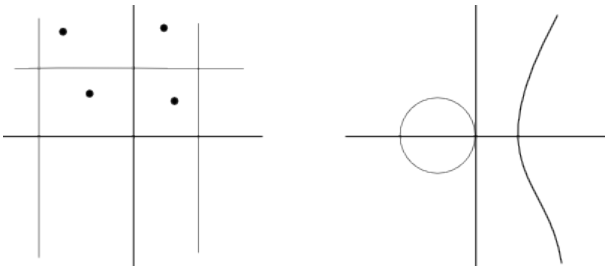


Figure 1: Closed sets in $A^1 \times A^1$ and A^2.

Example 3. For example, a non-zero polynomial in A^1 is going to have a finite set of zeros, and therefore the closed sets of A^1 are going to be finite sets and all of A^1. Likewise, the open sets will be the empty set and all cofinite sets. In particular, this topology is not Hausdorff (if $|k| = \infty$), as any two sets will have non-trivial intersection.

An obvious question is whether $A^2 = A^1 \times A^1$ as is usually the case. This isn't true. Closed sets in $A^1 \times A^1$ are finite unions of vertical and horizontal lines and points and all of $A^1 \times A^1$ (see Fig. 1). These sets will also be closed in A^2, but besides those, A^2 contains closed sets like the one depicted in Fig. 1: A typical closed set in A^2 is a finite union of curves and points.

Example 4. We consider the so-called determinantal varieties; that is, the set of linear maps from k^m to k^n with rank less than or equal to r. For example, this could be the set of singular maps $k^n \to k^n$ (as these have rank strictly less than n). Identify linear maps $k^m \to k^n$ with elements of $k^{mn} = A^{mn}$. Recall that the rank of a map is the largest r such that we can find a $r \times r$-submatrix with non-zero determinant. Such matrices are given by the vanishing of all $(r+1) \times (r+1)$-minors. In particular, the set of isomorphisms $k^n \to k^n$ is an open subset of k^{n^2} in the Zariski topology.

Proposition 5. *The Zariski topology on A^n is Noetherian. This is equivalent to every open set being compact.*

Proof. This follows from the fact that $k[x_1, \ldots, x_n]$ is Noetherian. This, on the other the hand, follows from a theorem by Hilbert. Recall that the following are equivalent:

- A ring is Noetherian
- Every ideal is finitely generated
- Every set of ideals has a maximal element
- Every increasing sequence of ideals stabilizes.

Using this, Hilbert proved that R Noetheriean implies $R[x]$ Noetherian: Assume that I is an ideal in $R[X]$ and consider the ideal I_n of elements in I of degree less than or equal to n. This sequence stabilizes and it is enough to check that I is generated by polynomials of degree at most m, and that the polynomials of degree at most m constitute a finitely generated ideal module R. □

Third lecture, September 2nd 2010

Last lecture: We had Hilbert's theorem: Every ideal of $k[x_1, \ldots, x_n]$ is finitely generated. A ring is called *Noetherian*, if every ideal is finitely generated.

Exercise 6. Show that if R is Noetherian, then so is $R[[x]]$.

A topological space is called *Noetherian*, if it satisfies one of the following two equivalent conditions:

1) Every set of closed subsets has a minimal element.

2) Every decreasing chain $C_1 \supseteq C_2 \supseteq \ldots$ of closed subsets is eventually constant.

(Compare this to the statements that every set of ideals has a maximal element, and that every increasing chain of ideals is eventually constant, considered last lecture.)

We put the Zariski topology on A^n, which then becomes a Noetherian topological space. This follows from Hilbert's theorem: Closed sets of A^n correspond to some ideals of $k[x_1, \ldots, x_n]$, and larger closed sets correspond to smaller ideals.

Exercise 7. That a space is Noetherian is equivalent to every open set being compact.

If a space is Noetherian and Hausdorff, it must be finite. Proof: The complement of a point is open and thus compact, and in Hausdorff spaces, compact sets are closed, so a point is open, and the topology is discrete. All discrete, compact spaces are finite.

1.2 Affine varieties

A non-empty set is called *irreducible*, if it is not a union of two proper closed subsets. This is a stupid concept for Hausdorff spaces, as the only irreducible Hausdorff spaces are points. In a Noetherian space, every closed set is a finite union of irreducible closed sets. The proof uses what is called *Noetherian induction*: The idea of Noetherian induction is to look for minimal closed counterexamples; minimal closed sets exist when the space is Noetherian. So in our case, suppose that C is a minimal closed subset, which is not a finite union of irreducibles. Then C is not irreducible, so $C = C_1 \cup C_2$, C_i closed, and $C_i \subset C$. By minimality, C_i are both finite unions of irreducible closed sets, contradicting the assumption that C was not.

Definition 8. An *affine variety* is an irreducible closed subset of A^n. (Problem: Look at the set $\{x \mid x \neq 0 \text{ in } A^1\}$ – this is not closed and therefore not an affine variety. In some sense, it is isomophic to the hyperbola $\{(x, y) \mid xy = 1 \text{ in } A^2\}$, which is an affine variety. It would therefore be nice, if the first set was a variety, and the definition will be modified later on.)

Example 9. Look at the algebraic set $\{x^2+y^2+z^2=0, xyz=0\}$. If $xyz=0$ then one of them equal to 0; say $x=0$. Then $y^2+z^2=0$, so $y+iz=0$ or $y-iz=0$. So the set is a union of 6 lines $x=0$, $y=\pm iz$, $y=0$, $x=\pm iz$, $z=0$, $x=\pm iy$.

Example 10. Consider $\{xy=1\}$. It looks as if this has 2 irreducible components. It has 2 connected components in the Euclidean topology, but it is still irreducible in the Zariski topology (as $xy-1$ can not be factored). Similarly, we have connected sets which are not irreducible: Take for example $\{xy=0\}$.

"Families" of irreducible varieties can have reducible "limits".

Example 11. Consider $\{xy=z\}$ (a saddle-like surface). Intersect this with varying hyperplanes $z=c$. This gives us a family of plane curves $xy=c$. For $c\neq 0$, this is irreducible, but for $c=0$, it becomes reducible as a union of two lines.

1.3 The Lasker–Noether theorem

An algebraic set is a finite union of irreducible algebraic sets. Before going on, we consider a generalization, due to Lasker, for commutative rings (schemes, really). Lasker proved that any ideal of $k[x_1,\dots,x_n]$ is a finite intersection of *primary ideals*: An ideal is called *prime* if $xy\in I$ implies $x\in I$ or $y\in I$, and *primary* if $xy\in I$ implies $x\in I$ or $y^n\in I$. For example, for $\mathbb{Z}$, the prime ideals are $(0),(2),(3),\dots$ and the primary ideals are (0) or of the form (p^n). For more general rings, however, primary is not the same as the power of a prime. This refines the composition of an algebraic set into irreducibles: Ideals give algebraic sets, and prime ideals give irreducible algebraic sets. Different ideals can give the same algebraic set though; for example, the ideals (x) and (x^2) have the same algebraic set, $x=0$.

It turns out to be a good idea to change these definitions a little bit. Lasker focused on an ideal $I\subset R$ with $I=\bigcap$primary ideals. It turns out to be better to consider a module $M=R/I$. For Noetherian rings, one can show that I is primary if and only if M has exactly one associated prime. We say that a module M is *coprimary* if it has exactly one associated prime. Here, p is an associated prime of a module M, if it is a prime ideal and the annihilator of some element of M. For example, if M is a finitely generated module over $\mathbb{Z}$, e.g. $M=\mathbb{Z}^{n_0}\oplus\mathbb{Z}_5\oplus\mathbb{Z}_7\oplus\mathbb{Z}_{13^3}$. Associated primes will be (0) if M contains $\mathbb{Z}$ and (p) if M contains some $\mathbb{Z}_{p^n}$. Coprimary modules over $\mathbb{Z}$ are $\mathbb{Z}^n$, $\mathbb{Z}_{p^{n_1}}\oplus\mathbb{Z}_{p^{n_2}}\oplus\cdots$ (modules where only one prime occurs).

Any non-zero finitely generated module over a Noetherian ring has at least one associated prime. Proof: The key idea of the proof is that if you take a maximal element of some set of ideals, it has a strong tendency to be prime. So pick a maximal element I of the set of ideals that are annihilators of a non-zero element of M. We want to show that I is prime. Suppose $xy\in I$ and that I annihilates $m\neq 0$. In the case that $ym=0$, $y\in\mathrm{Ann}(m)$, so $y\in I$. If $ym\neq 0$, then $x\in\mathrm{Ann}(ym)$, $I\mathrm{Ann}(ym)$ and since I is maximal, $x\in I$, and I is prime.

Lasker's original paper about the Lasker–Noether theorem for ideals over polynomial rings was about 100 pages long. We prove a more general version for modules over all Noetherian rings. The key simplification is the use of the *right* definitions. ´

Theorem 12 (Lasker's original version)**.** *Any ideal I is a finite intersection of primary ideals.*

A submodule N of a module M is called *primary* if M/N is coprimary. (Note that the term coprimary is somewhat more basic, as it can be used for modules and not just submodules.)

Theorem 13 (Reformulation in terms of modules)**.** *Any submodule N of a finitely generated module M is an intersection of primary submodules N_i.*

We can simplify this further by quotienting by N: We may as well assume that $N=0$, and it suffices to prove the following.

Theorem 14. *If M is a finitely generated module over a Noetherian ring R, then the submodule (0) is an intersection of a finite number of primary submodules.*

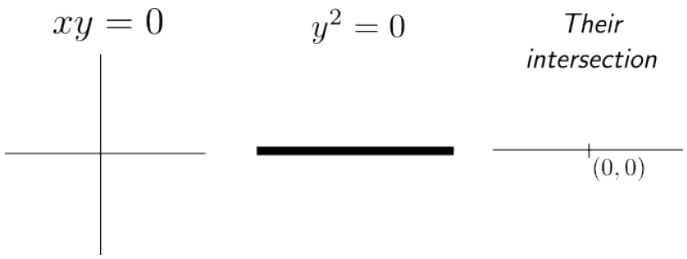


Figure 2: The sets considered in Example 17.

Proof. The first step is to prove that any submodule is a finite intersection of irreducible submodules (where a submodule is called irreducible, if it is not an intersection of two larger submodules), and the second step is to prove that every irreducible submodule is primary. For the former claim, use Noetherian induction: Choose a maximal submodule N that is not an intersection of irreducibles. Then N is not irreducible, so $N = N_1 \cap N_2$ with $N \subseteq N_1, N_2$, so N_1,N_2 are finite set of irreducibles (note that this is exactly the same as the proof that an algebraic set is a union of irreducibles). To prove that every irreducible submodule is primary, it suffices to replace M by M/N and proving that if 0 is irreducible, then 0 is a primary submodule; that is, M is coprimary. Suppose therefore that p, q are associated primes of M. Then $p = \mathrm{Ann}x$ and $q = \mathrm{Ann}y$ for some $x, y \in M$. Now, consider the submodules $Rx \cong R/p$, $Ry \cong R/q$ of M. If $p \neq q$, these have 0 intersection: The annihilator of any nonzero element of Rx is exactly p, as R/p is an integral domain (since p is a prime ideal). Similarly, the annihilator of any nonzero element of Ry is exactly q. So, if $p \neq q$, then $Rx \cap Ry = \{0\}$, since nonzero elements have different annihilators. But, 0 was assumed to be irreducible, so $p = q$, and therefore M has only one associated prime and is coprimary. □

Remark 15. Primary in Lasker's definition is equivalent to R/I coprimary.

4th lecture, September 7th 2010

Last lecture, we discussed the Lasker–Noether theorem which says that any ideal in a Noetherian ring is the intersection of a finite number of primary ideals. This is but a refinement of saying that any algebraic set is a finite union of irreducible ones. At the end of the lecture, we were in the middle of proving the remark above.

Exercise 16. Check that for Noetherian rings, R/q coprimary implies q primary (in Lasker's sense). Hints: Reduce to the case $q = 0$. If $a \in p = \sqrt{q} = \sqrt{0}$ is not nilpotent, then $R[a^{-1}] \neq 0$, so pick associated prime at $R[a^{-1}]$. Show that the inverse image in R is prime, which gives a contradiction. See [Eis] for details.

Example 17. Take the ideal (xy, y^2) in $\mathbb{C}[x, y]$. The corresponding algebraic set is the line (given by $y = 0$). Informally, the intersection is thickened slightly at $(0, 0)$. Think of the algebraic set as sticking out slightly at $(0, 0)$ (see Figure 2). The ideal sees this, but the algebraic set does not (this is why we consider the Lasker–Noether theorem a refinement). Informally, this thickened algebraic set looks like the union of the line $y = 0$ and the origin sticking out slightly. In terms of ideals, the first one is simply the ideal (y) and the second one (x, y^2). This gives the primary decomposition of the ideal (xy, y^2). It is easy to check that $(xy, y^2) = (y) \cap (x, y^2)$. Exercise: Check that these are primary.

Note however that primary decompositions need not be unique even if they are minimal. In the example above, $(xy, y^2) = (y) \cap (x + y, y^2)$.

Example 18. Primary decomposition is a sort of generalization of:

(1) The fundamental theorem of arithmetic.

(2) The structure theorem for finitely generated abelian groups.

For example, consider (2): Suppose M is a finitely generated abelian group,

$$M = \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{n_1}} \oplus \cdots .$$

Apply the Lasker–Noether theorem to M: That is, 0 is a intersection of primary submodules. $M/$(primary) is coprimary and thus of the form $\mathbb{Z}^n$ or a finite abelian p-group. The primary submodules of M are (1) Torsion subgruop T, $M/T = \mathbb{Z}^n$, (2) $\mathbb{Z}^n +$(Torsion coprime to p), $M/$this is a finite p-group. Again, note that primary decomposition is not unique, if M is infinite. Exercise: If $M = \mathbb{Z} \oplus \mathbb{Z}_2$, find 2 minimal primary decompositions, $0 = A_1 \cap A_2 = B_1 \cap B_2$, where A_i, B_i are primary.

Similarly, the fundamental theorem of arithmetic is closely realted to saying that $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{n_1}} \oplus \cdots$, where $n = p_1^{n_1} \cdots$ (note that we don't get the uniqueness part).

1.4 Hilbert's nullstellensatz and application

We want to find the relation between

(1) Algebraic subsets of A^n.

(2) Ideals of $\mathbb{C}[x_1, \ldots, x_n]$.

If we have an ideal I, we get an algebraic subset $Z(I)$ of A consisting of the common zeros of the elements in I. Conversely, if we have an algebraic subset Y of A^n, we map it to the ideal of polynomials vanishing on Y. This is not a 1:1 correspondence. For example, the ideals (x) or (x^2) in $\mathbb{C}[x]$ both give the algebraic set $Z(I) = 0$. If Y is any subset of A^n, then $Z(I(Y))$ is the closure of Y by definition of closure. The problem is that if a is an ideal, then $I(Z(a))$ need not be a. It obviously contains a, but it can be larger: If $a = (x^2)$, then $Z(a) = 0$, so $I(Z(a)) = (x) \supset (x^2)$. Suppose $p^n \in a$. Then obviously p^n vanishes on $Z(a)$, and therefore p vanishes on $Z(a)$, so $p \in a$. Recall that if a is an ideal, then so is the radical $\sqrt{a}$ of a, where $\sqrt{a} = \{p \mid p^n \in a \text{ for some } n \geq 1\}$. (Check if $p \in \sqrt{a}, q\sqrt{a}$, then $p + q \in \sqrt{a}$.) Now, perhaps $I(Z(a)) = \sqrt{a}$. We know that $\sqrt{a} \subseteq I(Z(a))$ by the argument before. This isn't true in general either though: If we work over $\mathbb{R}$ and $a = (x^2 + y^2 + 1)$ then $Z(a) = \emptyset$, so $I(Z(a)) = \mathbb{R}[x, y] \neq \sqrt{a} = a$. The problem in this case is that $\mathbb{R}$ is not algebraically closed – this turns out to be the only obstruction. This is the only obstruction:

Proposition 19. *If k is algebraically closed, and a is an ideal of $k[x_1, \ldots, x_n]$, then $I(Z(a)) = \sqrt{a}$.*

Corollary 20. *We get an 1:1 correspondence between* closed *subsets of A^n and* radical *ideals a (that is, $a = \sqrt{a}$) given by $Y \mapsto I(Y)$ and $a \mapsto Z(a)$.*

To see why the proposition holds, it is easier to first consider the case of maximal ideals and points in A^n. Points of A^n are sort of minimal algebraic subsets, which should correspond to the biggest possible ideals. For example, $(a_1, \ldots, a_n)$ should correspond to the maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$. Over $\mathbb{R}$, points do not correspond to maximal ideals: For example, $(x^2 + 1)$ is a maximal ideal of $\mathbb{R}[x]$ but doesn't correspond to points – again because $\mathbb{R}$ is not algebraically closed.

Theorem 21 (Weak Nullstellensatz)**.** *If k is algebraically closed, then any maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n$.*

Remark 22. The converse is trivial: The ideal is maximal because the quotient $k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots x_n - a_n)$ is the field k.

Proof of theorem. Let I be a maximal ideal. We know that $k[x_1, \ldots, x_n]/I$ is a field. Renumber $x_1, \ldots, x_n$ so that $x_1, \ldots, x_i$ are algebraically independent and $x_{i+1}, \ldots, x_n$ are algebraic over them. So, $k \subseteq F = k(x_1, \ldots, x_i) \subseteq K = k(x_1, \ldots, x_n)$. Notice that K is a finite module over $k(x_1, \ldots x_i)$. We also have that F is a finitely generated field extension over k.

The confusing thing here is that we have to distinguish 3 sorts of finiteness: Suppose K is an algebra over k. We can ask: Is K finitely generated as a module? Is K finitely generated as an

algebra over k? Is K finitely generated as a field over k? In general, the answers to the three will be different. For example, $\mathbb{Q}[\sqrt{2}]$ is finitely generated as a $\mathbb{Q}$-module, $\mathbb{Q}[x]$ is finitely generated as an algebra but not as a module, and finally, $\mathbb{Q}(x)$ is finitely generated as a field but not as an algebra.

We want to show that F is finitely generated as an *algebra* over k (that is, even if we don't allow the operation of division). Pick $y_1, \dots, y_m$ as basis for K as a module over F. Then $x_k = \sum t_{kj} y_j$ for some t_{kj}, and $y_k y_l = \sum t_{klj} y_j$ for some t_{klj} in F. Let T be a k-algebra generated by all t. We have $k \subseteq T \subseteq F \subseteq K$. Then T is Noetherian as the number of t is finite. In other words, T is a finitely generated k-algebra (by Hilbert's finiteness theorem). Moreover, K is generated by the y as a T-module because of the relations before, as the module contains the x and is closed under multiplication. Now, K is a finitely generated module over the Noetherian ring T, so any submodule such as F is a finitely generated T-module, and therefore F is a finitely generated k-algebra.

Now we will show that $k = F$. $F = k(x_1, \dots, x_i)$ is a purely trancendental extension of k. If F is finitely generated by elements $f_1/g_1, f_2/g_2, \dots$, where f_i, g_i are polynomials, then $k[x_1, \dots, x_i]$ has infinitely many primes, so pick one, p, not dividing $g_1, g_2, \dots$. Then $1/p$ is not in $k[f_1/g_1, \dots, f_*/g_*]$, which is a contradiction, and $k = F$. The extension $F \subset K$ was finite, so K is a finite k-module. We have not yet used the fact that k is algebraically closed; as k is, any finite extension of k is k itself so $k \cong K = k[x_1, \dots, x_n]/I$, so $x_i \mapsto a_i$ for some $a_i \in k$, so I contains $x_i - a_i$, and $I = (x_1 - a_1, x_2 - a_2, \cdots)$. □

Theorem 23 (Hilbert's Nulstellensatz)**.** *If k is algebraically closed, then $\sqrt{a} = I(Z(a))$.*

Proof. We use the Rabinowitz trick of adding an extra variable x_0. Suppose $a = (f_1, \dots, f_n)$ and suppose $f \in I(Z(a))$ so $f = 0$, whenever $f_1, \dots, f_m = 0$. Then $f_1, \dots, f_m, 1 - x_0 f$ has no common zeros in A^{n+1}, adding the extra variable. By the weak Nullstellensatz, they're not contained in any maximal ideal, so they must generate the whole ideal $k[x_0, \dots, x_n]$. Therefore we get the identity

$$1 = g_0(1 - x_0 f) + g_1 f_1 + \cdots + g_m f_m$$

for some $g_i \in k[x_0, \dots, x_n]$. Put $x_0 = 1/f$ so $1 = g_1 f_1 + \cdots g_m f_m$ in the field of rational functions. Clear denominators of the g_i by multiplying by powers of f to get $f^N = h_1 f_1 + \cdots h_m f_m$ for some h_i, where N is the maximum power of f in the denominators of the g_i. This says that $f \in \sqrt{(f_1, \dots, f_m)}$. □

Example 24. Consider the intersection of the line $y = 0$ with the parabola $y = x^2$. This is simply $(0, 0)$. Look at the ideals $(y), (y - x^2)$. The ideal generated by these is the (y, x^2), but this is not the ideal of the point $(0, 0)$. The ideal of the point $(0, 0)$ is the *radical* of (y, x^2) which is (y, x). In other words, the ideal generated by 2 radical ideals need not be radical.

Example 25. Look at the algebraic set of nilpotent $n \times n$ matrices M (that is, $M^n = 0$). For a general matrix M, the entries in M^n are polynomials of degree n in the entries of M. Consider the ideal a generated by the coefficients of the polynomials, so that the nilpotent matrices are exactly the algebraic set $Z(a)$. Now, is a radical? That is, are all polynomials vanishing on nilpotent matrices in a? This is not the case: Take for example $\mathrm{Tr}(M) = m_{11} + \cdots + m_{nn}$. This is not in a as all generators of a are homogeneous of degree n, but Tr has degree 0. On the other hand, if $M^n =$, then all eigenvalues of M are 0, so $\mathrm{Tr}(M) = 0$, so the trace vanishes but isn't one of the polynomials used to define the ideal.

More generally, if the characteristic polynomial

$$\det(\lambda I - M) = \lambda^m + m_{n-1}\lambda^{n-1} + \cdots + m_0 = \prod(\lambda - \alpha_i),$$

so all coefficients vanish for M nilpotent.

Consider

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad M^2 = \begin{bmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{bmatrix}$$

so the ideal is $(a^2+bc, ab+bd, ac+cd, bc+d^2)$. By the Nulstellensatz we know that some power of $a+d = \mathrm{Tr}M$ is in this ideal. This isn't entirely obvious. For example, $(a+d)^2 = a^2+2ad+d^2$ is *not* in this ideal, as one might expect. However, $(a+d)^3$ is.

Exercise 26. Find the smallest power of $a_{11}+\cdots a_{nn}$ in the ideal for $n \times n$ matrices. (This is probably hard.)

In general, it can be really hard to find the radical of a given ideal.

Example 27. Look at the algebraic set of *commuting* $n \times n$ matrices, $AB = BA$. This algebraic set is defined by n^2 polynomials in $2n^2$ variables given by the coefficients of $AB-BA$. We can ask the following question: Is the ideal generated by these radical? This problem appears to be open.

5th lecture, September 9th 2010

Last time, we covered

Theorem 28. *Hilbert's Nullstellensatz Suppose a is an ideal in $k[x_1,\ldots,x_n]$ (where k is algebraically closed), Z is the algebraic set of a, and IZ is the ideal of elements vanishing on Z. Then $I(Z(a)) = \sqrt{(a)}$*

This gives a complete description of the coordinate rings in an algebraic set:

Definition 29. If Z is an algebraic set in A^n, its *coordinate ring* is $k[x_1,\ldots,x_n]/\{\text{polynomials vanishing on } Z\}$, which we can think of as polynomial functions on Z.

The coordinate ring has the following properties

(1) It contains the algebraically closed field k.

(2) It is finitely generated over k.

(3) It has no non-zero nilpotents: If a function p satisfies $p^n = 0$ then $p = 0$.

Hilbert's Nullstellensatz says that algebraic sets are the same as finitely generated algebras with no non-zero nilpotents: Suppose A is finitely generated over k by $a_1,\ldots,a_n$. Then we have a surjective map $k[x_1,\ldots,x_n] \to A$, $x_i \mapsto a_i$. The kernel is some ideal I, and we define an algebraic set to be the zeros of I in A^n. This ideal has the property that $I = \sqrt{I}$. The Nullstellensatz roughly says that this identifies the category of algebraic sets with the opposite of the category of rings as above: A map $f : A \to B$ between rings corresponds to a map in the opposite direction from the algebraic set of B to the algebraic set of A.

We consider now an application of this to a problem Hilbert became famous for solving: Suppose Z is an algebraic set and suppose a group G acts on Z. Can we form a quotient Z/G of orbits of G on Z as an algebraic set? In other words, can we take quotients of algebraic sets of groups? If $Z \subseteq A^n$, how do we embed Z/G in affine space? There is no immediate obvious way to do this; looking at it geometrically, it's a bit of a puzzle but looking at it algebraically, it becomes obvious what to do. If Z is a topological space, acted on by G, then functions on Z/G are the same as functions on Z invariant under the action. So the coordinate ring of Z/G "should be" the G-invariant elements of the coordinate ring of Z. So in order to construct the quotient, we need to check that these G-invariant elements constitute the coordinate ring of some affine algebraic set: First off, it obviously contains k. Secondly, it's not obvious that it is finitely generated, but it is obvious that is contains no non-zero nilpotents. So, the obstruction to taking quotients of algebraic sets by groups is that the ring is finitely generated. There are two answers to when this happens. Hilbert's answer is that it often is, and Nagata's is that sometimes it's not. We consider some examples.

Example 30. Take affine space A^n. This is acted on by the symmetric group S_n by permuting coordinates. What is the quotient A^n/S_n? We can think of this as being "sets of n points". We take a coordinate ring $k[x_1,\ldots,x_n]$ of A^n, acted on by S_n. The coordinate ring of A^n/S_n should

be the S_n-invariant polynomials, which are just the symmetric polynomials. The ring of symmetric polynomials is a polynomial ring in the elementary symmetric polynomials

$$\begin{aligned} e_1 &= x_1 + \cdots + x_n \\ e_2 &= x_1 x_2 + \cdots \\ &\vdots \\ e_n &= x_1 \cdots x_n. \end{aligned}$$

So we just get the free polynomial ring $k[e_1, \ldots, e_n]$. That is, $A^n/S_n \cong A^n$. Note that it is very rare for the ring of invariant functions to be a polynomial ring as it happened to be in this case. This happens if G is a reflection group.

There is a puzzle here: Look at $G = \{-1, 1\}$ acting on A^1 over $\mathbb{R}$. As above, we will describe $\mathbb{R}/G$. The coordinate ring of $\mathbb{R}$ is just $\mathbb{R}[x]$, and G acts by $x \mapsto -x$. The invariant polynomials are $\mathbb{R}[x^2]$, which is a polynomial ring, so $\mathbb{R}/G = \mathbb{R}$. However, the topological quotient $\mathbb{R}/\pm 1$ seems to be the half-line.

The algebraic set quotient is not always the same as the topological quotient: In this example, the algebraic set quotient is really the set of pairs $\{x, -x\}$ that are real in the sense that they are invariant under complex conjugation. For example, the pair $\{i, -i\}$ actually appears in the algebraic set quotient $\mathbb{R}/\{\pm 1\}$.

Example 31. Take the orthogonal group $O_n(\mathbb{C})$ acting on $\mathbb{C}^n$. Again we ask what the quotient $\mathbb{C}^n/O_n(\mathbb{C})$. Geometrically, we want the orbits of $O_n(\mathbb{C})$ on $\mathbb{C}$, and we get 1 orbit for each complex $z \in \mathbb{C}$ which consists of the vectors with $(v, v) = z$. Algebraically, what are invariant polynomials on $\mathbb{C}^n$ invariant under rotation? These turn out to be polynomials in (v, v). So the ring of invariant functions is $\mathbb{C}[(v, v)]$ is the polynomial ring in one variable, so the quotient is isomorphic to $\mathbb{C}$.

Example 32. Look at the group $SL_n(\mathbb{C})$ acting on $\mathbb{C}^n$. The algebraic set quotient in this case will be a point as $SL_n(\mathbb{C})$ has a dense orbit and the invariant polynomials are constant (and here the geometric quotient is really going to be two points). To make it more interesting, look at the action of $SL_n(\mathbb{C})$ acting on $\mathbb{C}^n \oplus \cdots \oplus \mathbb{C}^n$, where here we have n copies of $\mathbb{C}^n$. A non-trivial polynomial in n^2 variables invariant under $SL_n(\mathbb{C})$ is given by the determinant, were we consider the matrix given by plugging the i'th vector as the i'th row in a matrix. The invariant polynomials in this case are just polynomials in the determinant, so $\bigoplus_{i=1}^n \mathbb{C}^n/SL_n(\mathbb{C})$ is isomorphic to the affine line.

A *binary quantic* is something of the form $a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n$. These are acted on by $SL_2(\mathbb{C})$, where a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ acts as $x \mapsto ax + by$, $y \mapsto cx + dy$. This gives an action of $SL_2(\mathbb{C})$ on $\mathbb{C}^{n+1} = (a_0, \ldots, a_n)$. The classical problem of invariant theory is to find the polynomials in $a_0, \ldots, a_n$ invariant under $SL_2(\mathbb{C})$. One example is the discriminant $b^2 - 4ac$ of the quantic $ax^2 + bxy + cy^2$. Gordan showed that the ring of invariants is finitely generated. He gave an algorithm to find the generators, but it turns out to be very complicated; people have found them up to around $n = 8$. Hilbert gave a short non-constructive proof of this:

Theorem 33 (Hilbert)**.** *Suppose G is a finite (for simplicity) group acting on complex vector space $\mathbb{C}^n$. Then the ring of G-invariant polynomials is finitely generated. In particular, A^n/G is a well-defined algebraic set.*

Proof. Put $A = \mathbb{C}[x_1, \ldots, x_n]$, so G acts on A. We want to find generators for the set of G-invariant polynomials denoted A^G. A is graded by degree. Let I be the ideal of A generated by positive degree homogeneous elements of A^G. By Hilbert's basis theorem, I is a finitely generated ideal of A. So we can ssume it has homogeneous generators $i_1, \ldots, i_m$ fixed by G. The idea is to show that $i_1, \ldots, i_m$ generate the algebra A^G. (This is not entirely straightforward: For example, consider $k[x, y]$ and consider the ring spanned by the elements in Fig. 3; this is not finitely generated as an algebra, but as an ideal, it is generated by y.)

We need to use some special property of A^G to deduce that $i_1, \ldots, i_m$ generate it: A^G has a Reynolds operator called $\rho : A \to A^G$ with the property that $\rho(ab) = a\rho(b)$ if $a \in A^G$ and $\rho(1) = 1$.

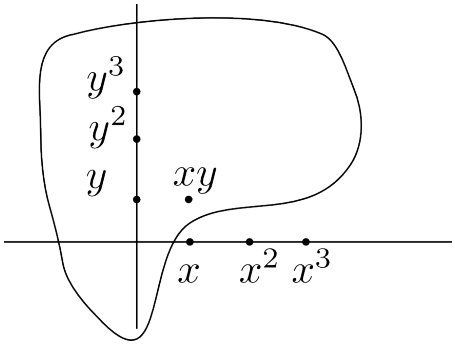


Figure 3: A certain ring of polynomials

In other words, ρ is a A^G-module homomorphism (but generally $\rho(ab) \neq \rho(a)\rho(b)$). The map is defined by $\rho(a) = \frac{1}{|G|}\sum_{g\in G} a^g$ (here we need to be in characteristic 0).

Now, put $A = A_0 \oplus A_1 \oplus \cdots$ where A_i is the set of degree i elements. We now prove by induction on deg in A_k^G that x is in the algebra generated by $i_1, \ldots, i_m$. We know that $x = a_1 i_1 + \cdots + a_m i_m$ for some $a_i \in A$. Applying the Reynolds operator we get

$$x = \rho(x) = \rho(a_1)i_1 + \cdots + \rho(a_m)i_m,$$

as x and i_j are fixed by G, and the a_j are in A^G, as they have degree less than $\deg(x)$, so they are in the ring generated by $i_1, \ldots, u_m$. So x is a polynomial in $i_1, \ldots, i_m$, so $i_1, \ldots, i_m$ generate A^G as an algebra. □

Remark 34. Hilbert proved this theorem for any field k and a general reductive algebraic group, where we only considered finite groups. In order to generalize the proof to other groups, note that the property of the group needed in the proof is, that we can integrate over it to define the Reynolds operator. The same thing works for any compact group as we can integrate over those. So for example, this also works for the special unitary group SU_2. But what about the group $SL_2(\mathbb{C})$ appearing in the invariant theory problem? This is not compact, but one can use Weyl's unitarian trick which says that the finite dimensional representations of $SL_2(\mathbb{C})$ are more or less the same as the finite dimensional representations of its compact subgroup SU_2; in particular, this can be used to transfer a Reynolds operator from SU_2 to $SL_2(\mathbb{C})$.

It fails for some groups such as the additive group of a field k (which is essentially proved by Nagata).

So, why do we want to construct quotients? Many moduli spaces are given as such quotients. Roughly speaking, a *moduli space* is some sort of "varieties" whose points correspond to something we want to classify. For example, suppose we want to classify elliptic curves; these are going to be more or less degree 3 curves in the plane. To do this, we write down a general equation for a degree 3 curve in $\mathbb{P}^2$. This could be something like

$$a_{300}x^3 + a_{210}x^3y + \cdots + a_{003}z^3.$$

We get 10 coefficients $a_{300}, \ldots, a_{003}$. Two such sets of coefficients might very well correspond to the same elliptic curve, so they are acted on by automorphisms of the projective plane $PGL_3(\mathbb{C})$, which also acts on $\mathbb{P}^9$. We then want to take the quotient $\mathbb{P}^9/PGL_3(\mathbb{C})$.

6th lecture, September 14th 2010

Last lecture, we were looking at the Nullstellensatz which says that affine algebraic sets are more or less the same as finitely generated algebras R over k with no nilpotents. The connection between them is taking the coordinate ring $k[x_1, \ldots, x_n]/I$ and going the other way is taking the subset of

k^n where all elements of I vanish, where $R = k[x_1, \ldots, x_n]/I$. A better way of going the other way turns out to be taking the "spectrum" of R, as we will see a later. One application we saw was how to make sense of quotients of algebraic sets by groups. While it doesn't quite make sense on affine algebraic sets, we managed to do this by simply considering the fixed points R^G of R under G.

Example 35 (Cyclic quotient singularities). Take a cyclic group $\mathbb{Z}_n$ acting on k^m by $(x_1, \ldots, x_m) \mapsto (x_1\zeta_1, \ldots, x_m\zeta_m)$, where $(\zeta_i)^n = 1$. From the viewpoint of representation theory, this is the trivial example of the representation of a cyclic group. We want to take the quotient $k^m/\mathbb{Z}_n$.

The case $m = 1$ is uninteresting: The coordinate ring is $k[x]$ and the action of the group is given by $x \mapsto \zeta x$. Assume that ζ is a primitive n'th root of unity. Now the fixed points of the action on $k[x]$ is simply the subalgebra generated by x^n, $k[x^n]$, which is again a polynomial ring of 1 variable, and the quotient of the affine line by $\mathbb{Z}_n$ is just going to be the affine line again. Consider now

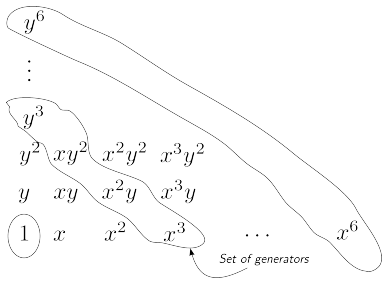


Figure 4: The fixed subspace under the cyclic action.

$k^2/\mathbb{Z}_n$. Take the action to be $(x, y) \mapsto (\zeta x, \zeta y)$. (Another action would be taking $(x, y) \mapsto (x, \zeta y)$ which would actually give a different quotient.) The coordinate ring of k^2 is just $k[x, y]$. Under the action $x^i y^j \mapsto \zeta^{i+j} x^i y^j$, and the fixed subspace is spanned by $x^i y^j$ with $n \mid (i + j)$. For example, if $n = 3$ the fixed subspaces are shown in Fig. 4. In general, the fixed subring are generated by $x^n, x^{n-1}y, \ldots, y^n$, and this is in fact the smallest possible number of generators. Denote them by $z_n, z_{n-1}, \ldots, z_0$ respectively. We have several relations between these: We have $z_i z_j = z_k z_l$ if $i + j = k + l$; again, these relations actually generate all of them. So the coordinate ring of the quotient is $k[z_0, \ldots, z_n]/I$, where I is the ideal generated by $z_i z_j = z_k z_l$ for $i + j = k + l$. The corresponding quotient variety is then equal to the subset of k^{n+1} of vectors $(z_0, \ldots, z_n)$ with $z_i z_j = z_k z_l$ for $i + j = k + l$. We will see that we can actually not embed this into something of dimension less than $n + 1$, even though we started with something 2-dimensional.

Example 36 (Moduli space in chemistry). In chemistry, we have the molecule cyclohexane (drawn simply as a hexagon). Chemists ask what the configurations of this molecule are. Each of the 6 carbon atoms goes to a point in $\mathbb{R}^3$, so we get a point in $\mathbb{R}^{3\cdot 6} = \mathbb{R}^{18}$. We can't take any points $p_1, \ldots, p_6$ ($p_6 = p_0$); corresponding to distances and angles between them in the molecule we have some polynomial relations: The distance from p_i to p_{i+1} is fixed, so $(p_i - p_{i+1})^2 = c$ constant. Similarly the angle $p_i p_{i+1} p_{i+2}$ is fixed. This means that the distance $p_i p_{i+2}$ is also fixed, so $(p_i - p_{i+2})^2 = d$ another constant. So the position of the molecule is an algebraic set in $\mathbb{R}^{18}$ given by the intersection of 12 quadrics modulo the group of isometries of Euclidean space. This last group is 6-dimensional (3 translations and the rotation group). We can guess what this looks like; for example, we can try to guess the dimension, which might turn out to be 0, saying essentially that there is only a finite number of configurations. This turns out to be wrong. In fact, the moduli space of configurations is a point + a circle; there is rigid way of joining the atoms, but there is also one which allows for a rotational freedom. This was discovered by Herman Suchse.

1.5 Dimension of algebraic sets

We begin with a quick review of dimension for Hausdorff spaces. When trying to define dimension, we run into the following problems:

(1) Cantor showed that $\mathbb{R}^2$ and $\mathbb{R}^1$ have the same number of points.

(2) We have a continuous surjective map $\mathbb{R}^1 \to \mathbb{R}^2$ given by Peano curves.

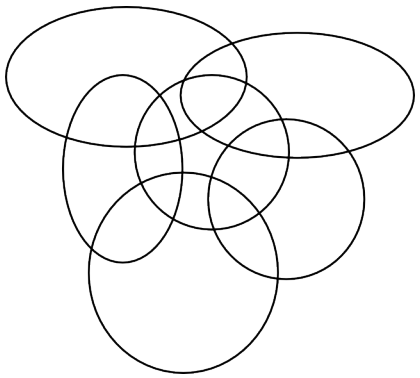


Figure 5: $\mathbb{R}^2$ has Lebesgue dimension 2.

One way of defining dimension is using Lebesgue covering dimension: A set has dimension $\leq d$, if every open cover has a refinement, so that any $d+2$ sets have empty intersection. For example in the plane, 3 open sets often intersect, but 4 don't (see Fig. 5). However, with this definition it is hard to show that $\mathbb{R}^n$ has dimension n.

Dimension for non-Hausdorff spaces is totally different. For example, Lesbesgue covering dimension simply fails, and we have to come up with something else. Look at the affine plane A^2. As we have seen, closed sets look like a union of points and curves. In other words, we can find chains of irreducible closed sets, point $\subseteq$ curve $\subseteq$ plane. It is intuitively plausible that we cannot find chains of 4 irreducible closed sets like this. This suggests the following:

Definition 37. The *dimension* of a topological space is defined to be the supremum of n so that we can find a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets.

Example 38. For the affine line, the only irreducible closed subsets are points and A^1, and we get a chain (point) $\subset A^1$, and the affine line has dimension 1. Note that the Lebesgue dimension is ∞ so any finite number of open subsets intersect – conversely, for Hausdorff space, the only irreducible closed subsets are points, so that all have dimension 0.

Example 39. The dimension of A^4 is 4: We need to know all the irreducible closed subsets of A^4. It is not clear what the irreducible closed substs are, and in general it is very hard to calculate dimensions of anything of dimension greater than or equal to 2 or 3 using this definition.

Definition 40. The *dimension of a ring* is defined to be the largest n so that we can find a chain $p_0 \subset p_1 \subset \cdots \subset p_n$ of distinct prime ideals.

This definition is reasonable by the connection between ideals and sets given above. We do have other definitions of the dimension of a ring: Something of higher dimension should have "more" functions of it. Suppose V is a variety. Then the coordinate ring R is the integral domain $k[x_1, \ldots, x_n]$/prime ideal, so it has a quotient field K. We can then define the dimension of V to be the transcendence degree of K over k – that is, the maximum number of algebraically independent elements.

Example 41. For A^n the coordinate ring is $R = k[x_1, \ldots, x_n]$, and $K = k(x_1, \ldots, x_n)$, which has transcendence degree n.

In fact, this definition was used for a long time, but it doesn't work for rings that aren't integral domains, and such ones turn up often in algebraic geometry. The best definition of dimension uses Hilbert polynomials, which we will be discussing later: Suppose that a ring R has only one maximal ideal m (such a ring is called a *local ring*). Then we can estimate the size of R by looking at $R/m, R/m^2, \ldots$. Here $R/m = k$ will be a field. Assuming $k \subset R$, each of the R/m^n will be

a vector space over k, and we can look at the growth rate of the sequence $\dim(R/m^n)$. It turns out that the dimension of R/m^n will be a polynomial of some degree d for large k. We define the dimension to be this degree d.

Example 42. Look at the ring of formal power series $k[[x_1, \dots, x_n]]$ in $x_1, \dots, x_n$. It has only one maximal ideal m given by elements of 0 constant term. The dimension of R/m is 1, a basis of R/m^2 is $1, x_1, \dots, x_n$, so it has dimension $n+1$. Similarly R/m^3 has dimension $(n+1)(n+2)/2$, and in general R/m^k has dimension $(n+1)\cdots(n+k-1)/k! = \binom{n+k}{k} = \binom{n+k}{n}$, which is a polynomial in the degree n, so the dimension of $k[[x_1, \dots, x_n]]$ is n.

Now the dimension of any ring r is the maximum of dimensions of local rings R_m, where R_m is the localization of R of R at a maximal ideal m meaning that we invert all elements of R not in m; we will talk more about localizations later. This definition is roundabout, but it is easy to use, and it is easy to calculate dimensions.

Theorem 43. *All three definitions of dimension of a ring coincide when they are defined.*

Proof. See [Eis]. □

Remark 44. It is tempting to think that finite dimension has something to do with being Noetherian; for example, the ring $k[x_1, x_2, \dots]$ in infinitely many variables turns out to be infinite dimensional, but it is not Noetherian. It turns out to be wrong: The quotient $k[x_1, \dots,]/(x_1^2, x_2^2, \dots)$ is of dimension 0, but is not Noetherian. Every Noetherian *local* ring is finite dimensional. Nagata found a Noetherian infinite-dimensional ring.

Example 45. What is the dimension of the Hilbert scheme of n points on A^m? Roughly (but rather misleadingly), the Hilbert scheme is something whose points parametrize sets of n points on A^m. More accurately, the ideal of n points has (vector space) codimension n in $k[x_1, \dots, x_m]$, and the Hilbert scheme is "really" the codimension n ideals in $k[x_1, \dots, x_m]$. Take $m = 1$: The codimension n ideals in $k[x_1]$ are polynomials of degree n, $x^n + a_{n-1}x^{n-1} + \cdots + a_0$. This will be n-dimensional. Similarly for $m = 2$, the Hilbert scheme has dimension $2n$.

One would guess that for m dimensions, the Hilbert scheme has dimension mn: Informally, we have n points, each of which give m dimensions. Surprisingly this is false in dimension $m \geq 3$. The problem is that for $m \geq 3$ there are more ideals than one might guess corresponding to many points coinciding. Even for $m = 2$ there are a lot of ideals corresponding to "2 points at $(0,0)$"; $k[x,y]/(x, y^2)$ or $k[x,y]/(y, x^2)$. For $m \geq 3$ there are too many ideals like these.

Take $m = 3$ and the ideal $M = (x_1, x_2, x_3)$. Look at ideals I with $M^k \supseteq I \supseteq M^{k+1}$. Any subspace of the vector space M^k/M^{k+1} will be an ideal, and $\operatorname{codim}(M^k)$ is some degree 3 polynomial in k, so $\dim(M^k/M^{k+1})$ is a degree 2 polynomial in k. Now the dimension of the Grassmannian of dimension a subspaces of k^b is $a(b-a)$ (give or take 2). So the Grassmannian of dimension $\approx a/2$ of k^a has dimension about $a^2/4$, so the dimension of the Grassmannian of M^k/M^{k+1} of subspaces of half the dimension of M^k/M^{k+1} is given by a degree 4 polynomial in k. The codimension of this ideal is given by a degree 3 polynomial in k. So the dimension of the Hilbert scheme is a degree 4 polynomial in k, which eventually will be larger than $mn = 3n$ which is a degree 3 polynomial in k. So the Hilbert scheme has components of unexpectedly large dimension if the dimension m of A^m is ≥ 3 and the number of points n is sufficiently large.

7th lecture, September 16th 2010

2 Projective varieties

Today, we will discuss projective varieties (corresponding to 1.2 i [Har]).

Definition 46. *Projective space* is the set of points $(x_0 : \cdots : x_n) \neq (0, \dots, 0)$ modulo scalars, $(x_0 : \cdots : x_n) = (\lambda x_0 : \cdots : \lambda x_n)$. One can think of this as lines in A^{n+1} through the origin.

We consider projective space P^n as affine space together with points at infinity, where affine space is the set of points $(1 : x_1 : \cdots : x_n)$ and the points at infinity are the points $(0 : x_1 : \cdots : x_n)$, which is just P^{n-1}, so $P^n = A^n \cup P^{n-1} = A^n \cup A^{n-1} \cup \cdots \cup \text{pt}$.

2.1 Historical background

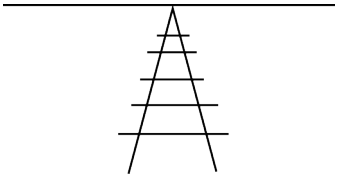


Figure 6: A pair of railway tracks

Projective geometry originated in the following question: What properties are preserved by *projections*? Consider for example a pair of railway tracks (Fig. 6): They are parallel in the real world, but drawing a picture they meet at the horizon, kind of corresponding to a point at infinity.

In *synthetic geometry*, one writes down axioms for points, lines, circles, etc. (a la Euclid). Opposed to this is *analytic geometry*, where one writes down coordinates and converts everything to algebra.

In the 19th century, one came up with axioms for projective geometry: We have a set of "points", a set of "lines", and an incidence relation between points and lines (which is the relation that the "point lies on the line"). We then have the following axioms:

(1) Any 2 distinct points lie on a unique line.

(2) Any 2 lines "in the same plane" meet at a point (as opposed to what happens in usual geometry). Here we say that 2 lines l_1, l_2 lie in the same plane, if we can find distinct points and lines a, b, c, d, e, l_3, l_4 as in Fig. 7.

(3) There are least 3 points on any line (which serves to eliminate degenerate cases).

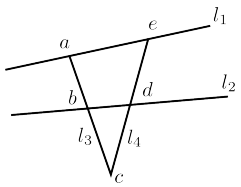


Figure 7: The set of points and lines used in the axiomatization of projective geometry.

Example 47. Projective space is an example of the above. We can think of "points" as the lines through 0 in A^{n+1} and the "lines" as planes through 0 in A^{n+1}.

We also have the concept of dimension: Dimension 0 corresponds to no lines. Dimension 1 corresponds to exactly one line. These cases are rather boring. In dimension 2 we have more than 1 line, but any 2 lines meet – an example is the Fano Plane (Fig. 8) where we have 7 points and a bunch of lines. This is exactly the projective plane over a 2 element field which on the other hand is the set of lines and planes in $(\mathbb{F}_2)^3$. In dimension greater than or equal to 3, there are 2 lines that do meet.

Theorem 48 (Desargues)**.** *We have 10 particular points and 10 lines – the bottom three points lie on a line.*[2]

[2]See `http://en.wikipedia.org/wiki/Desargues'_theorem` for an illustration that shows the situation better than I would be able to draw.

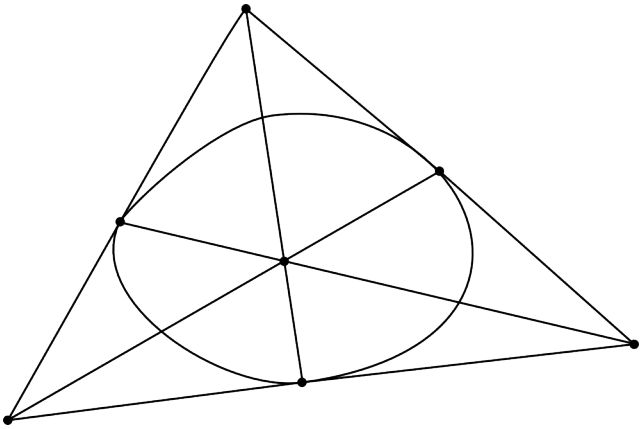


Figure 8: The Fano plane.

Proof. It is obvious: How does an artist draw an accurate picture of a triangle?[3] This can be arranged in 3 dimensions but not in 2 dimensions. □

Theorem 49 (Monge's theorem)**.** *In the same spirit consider a situation we have cones formed by three spheres*[4] *– again we have three points sitting on a line.*

Again the proof is about considering an extra dimension.
We consider now a classification of models of projective geometry.

Theorem 50. *Take dimension* > 1.

- *If the dimension is greater than or equal to 3, then Desargues's theorem holds. If Desargue's theorem holds, then the projective geometry is the set of points of lines of some projective space over some division ring.*
- *A division ring is a field if and only if Pappus's theorem holds.*

So what we are actually doing is considering the above axioms for projective geometry and demanding that Pappus's theorem holds.

Note that there are many projective planes, called non-Desarguesian, where Desargues's theorem fails – for example the projective plane over the octonions. Moulton proved the following: If we take (affine – we really have to add points of infinity) points to be the points of $\mathbb{R}^2$ and lines to be lines doubling in slope, when they cross the y-axis, we get a non-Desarguesian plane (see Fig. 9). Borcherds: "Non-Desarguesian planes are a huge pile of junk." For example, what is the planes of finite orders? Here, the order is the number of points on a line - 1. There are none of order ≤ 3, 3 of order 9 and none of order 10.

2.2 Coordinate rings in projective varieties

We know that affine space A^n corresponds to the coordinate ring $k[x_1, \ldots, x_n]$, and affine algebraic sets correspond to ideals $I = \sqrt{I}$ (this is essentially the Nullstellensatz). We want to find out what the analogue of this is for projective space. It turns out that projective space P^n corresponds in the same way to the graded ring $k[x_0, x_1, \ldots, x_n]$, and closed subsets correspond to homogeneous ideals $I = I_0 \oplus I_1 \oplus \cdots$ with the pieces having various degrees and $I = \sqrt{I}$. Roughly, this is because points of P^n corresponds to lines through 0 in A^{n+1} and subsets of P^n corresponds to "cones" (meaning unions of lines) with vertex at 0 in A^{n+1}, and this corresponds to the ideal being homogeneous. This is done in detail in [Har].

[3] Again, see `http://en.wikipedia.org/wiki/Desargues'_theorem`
[4] See `http://en.wikipedia.org/wiki/Monge's_theorem`

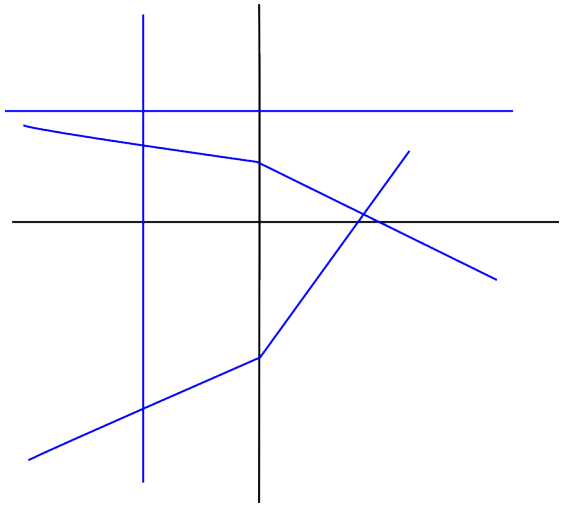


Figure 9: A non-Desarguesian plane.

2.3 Examples

Example 51. The twisted cubic in A^3 is given by points (t, t^2, t^3). We will extend this to a projective variety in P^3. Its ideal in $k[x_1, x_2, x_3]$ is $(y-x^2, z-x^3)$. The image in projective space $(1 : t : t^2 : t^3)$ is contained in the set of points of the form $(s^3 : s^2t : st^2 : t^3)$ (that is, we multiply everything by an extra variable to make it homogenouos). The twisted cubic is the points (s^3, s^2t, st^2, t^3) for $(s, t) \neq (0, 0)$. If we write $(s^3 : s^2t : st^2 : t^3) = (z_0 : z_1 : z_2 : z_3)$, we have $z_0z_3 = z_1z_2$, $z_1^2 = z_0z_2$, and $z_2^2 = z_1z_3$. These generate an ideal, but any 2 do not. If we take the ideal of the affine curve $(y - x^2, z - x^3)$ and homogenize it we get $ty = x^2$, $t^2z = x^3$. That is, homogenizing a set of generators of the ideal of an affine variety, we don't get the set of generators of the ideal of its closure as a projective variety.

Example 52. We will check the Weil conjectures (proved for general varieties in the 1970s) for projective space. Among other things the Weil conjectures give a relation between the cohomology of complex projective space and the number of points in projective space over a finite field.

First off, the cohomology of $P^n(\mathbb{C})$ is given by the decomposition $P^n(\mathbb{C}) = \text{pt} \cup \mathbb{C} \cup \mathbb{C}^2 \cup \ldots$ and using cellular homology, we get $\dim H_{2k}(P^n(\mathbb{C}); \mathbb{R}) = 1$, $H_{2k+1}(P^n(\mathbb{C}); \mathbb{R}) = 0$ (and $H_k(P^n(\mathbb{C}); \mathbb{R}) = 0$, when $k > n$).

We will now count the number of points of P^n over a finite field with q elements. There are two ways of doing this: The first method is considering $P^n(F_q) = (F_q^{n+1} \setminus (0, \ldots, 0))/F_q^*$, so the number of points is $(q^{n+1} - 1)/(q - 1)$. On the other hand, writing $P^n(F_q) = A^n(F_q) \cup A^{n-1}(F_q) \cup \cdots \cup A^0(F_q)$, and the number of points is $q^n + q^{n-1} + \cdots + 1 = (q^{n+1} - 1)/(q - 1)$.

Now, we will work out its zeta function. For fixed q, we have by definition,

$$Z_V(t) = \exp(\sum_{n \geq 1} \frac{t^n}{n} \cdot (\text{number of points of } V \text{ over } F_{q^n})).$$

This is closely related to the usual zeta function. Note that if $W = U \cup V$, we have $Z_W = Z_U \cdot Z_V$. Notice that

$$\begin{aligned} Z_{A^n} &= \exp(\sum_{n \geq 1} \frac{t^n}{b} \cdot (q^n)^m) = \exp(\sum_{n \geq 1} \frac{(tq^m)^n}{n}) \\ &= \exp(-\log(1 - tq^m)) = \frac{1}{1 - tq^m}. \end{aligned}$$

Finally,

$$Z_P^m = Z_{A^0} \cdot \cdots \cdot Z_{A^m} = \frac{1}{1-t} \cdot \frac{1}{1-qt} \cdot \cdots \cdot \frac{1}{1-q^m t}.$$

Notice that this is a rational function (this is one of the Weil conjectures, proved for general varieties in the 1960s). Secondly the poles all have absolute values integer powers of q (in general, absolute values integer powers of $q^{1/2}$) – this is actually the Riemann hypothesis for projective varieties. Thirdly, the number of poles of absolute value $q^{-k/2} = \dim H^k(P^n(\mathbb{C}))$ (and this is also one of the Weil conjectures).

Example 53. Is the product of two projective variety a projective variety? [The analogue for affine varieties is trivial, $A^m \times A^n \cong A^{m+n}$, so if $Y \subseteq A^m$, $Z \subseteq A^n$, we have $Y \times Z \subseteq A^{m+n}$, and the ideal of $Y \times Z$ is the union of the two ideals. This is in brackets as it is not really true as topological spaces: "It is the product as a product of schemes, which should shut everybody up".] We try this in projective space. The problem is that $P^m \times P^n \neq P^{m+n}$, as the product $(x_0 : \cdots : x_m)(y_0 : \cdots : y_n)$ is not well defined. Over the complex numbers, $P^1 \times P^1$ is not even homeomorphic (in the Euclidean topology) to P^2; this can be seen by using the Künneth formula of algebraic geometry, as $H^0(P^1 \times P^1) = \mathbb{C}$, $H^2(P^1 \times P^1) = \mathbb{C} \otimes \mathbb{C}$, but $H^2(P^2) = \mathbb{C}$. It can also be seen by counting the number of points over finite fields: $P^1 \times P^1$ has $(q+1)^2$ points, while P^2 has $q^2 + q + 1$ points.

To make $P^m \times P^n$ into a projective variety, we will map it as a closed subset of P^{mn+m+n} using what is known as Segre embedding given as follows:

$$(x_0 : \cdots : x_m) \times (y_0 : \cdots : y_n) \mapsto (x_0 y_0 : \cdots x_m y_0 : x_0 y_1 : \cdots : x_m y_n),$$

where the last expression consists of $(m+1)(n+1)$ coordinates. Next week, we will find the ideal of this subset.

8th lecture, September 21st 2010

Last lecture, we were looking at the problem of defining a product of projective varieties. We saw that $P^m \times P^n \neq P^{m+n}$. We are going to construct $P^m \times P^n$ as a projective variety in P^{mn+m+n}. Last time we got as fare as defining the Segre embedding $P^m \times P^n \to P^{mn+m+n}$ (see above).

Note that if we identify points of P^m with 1-dimensional subspaces L_x of k^{m+1}, the Segre embedding is given by $(L_x, L_y) \mapsto L_x \otimes L_y$.

We want to identify the image of the Segre embedding; that is, we will find generators for the *ideal* of the image. The image is the set of points $(x_0 y_0 : \cdots x_m y_0 : x_0 y_1 : \cdots : x_m y_n) = (z_{00}, z_{10}, \ldots, z_{mn})$, so the z_{ij} are the coordinates in $P^{(m+1)(n+1)-1}$. These satisfy some relations, such as $z_{ij} z_{kl} = z_{il} z_{kj}$.

Now we will show that we have found enough relations to define the image. That is, we will show that if $(z_{00}, \ldots, z_{mn})$ satisfy the above relations, then they are of the form $(x_0 y_0, \ldots)$. Assume that some $z_{ij} \neq 0$ and renumber so that $z_{00} \neq 0$. We can assume that $z_{00} = 1$. Put $y_l = z_{0l}$ and $x_k = z_{k0}$. Then $z_{kl} = z_{00} z_{kl} = z_{k0} z_{0l} = x_k y_l$, so the set of $(z_{00}, \ldots, z_{mn})$ is the image of the Segre embedding.

Example 54. Consider $P^1 \times P^1 \to P^3$, $(w : x), (y : z) \mapsto (wy, wz, xy, xz) =: (a, b, c, d)$ and the relation becomes $ad = bc$, so $P^1 \times P^1$ is identified with the quadric $ad = bc$ in P^3. Note that $P^1 \times P^1$ has 2 rulings (where a ruling means that you cover by copies of P^1; we can cover by $a \times P^1$ or by $P^1 \times b$). So the quadric $ad = bc$ also has 2 rulings, which appears to be nonsense, because every nonsingular quadric in P^3 can be put in this form by a change of variable. Really we are looking at a non-singular quadratic form Q in 4 variables, $Q = \sum a_{ij} x_i x_j$, with associated bilinear form $(x, y) \mapsto \sum a_{ij} x_i x_j$. Pick $v \neq$ in k^4 with $(v, v) = 0$ (which exists because k is algebraically closed). Pick w with $(w, v) = 1$ and λ so that $0 = (w + \lambda v, w + \lambda v) = w^2 + 2\lambda(v, w) + \lambda^2 v^2 = w^2 + 2\lambda(v, w)$ (which is possible when $\operatorname{char} k \neq 2$), so we can assume $(w, w) = 1$. What we have done is that

we have a 2-dimensional "hyperbolic plane", $w^2 = v^2 = 0$, $(w, v) = 1$. We can repeat this on the orthogonal complement of (v, w) and find vectors v_1, v_2, v_3, v_4 with inner products

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

so the quadratic form can be put in form $ab+cd$. A corollary is that the sphere $x^2+y^2+z^2 = 1$ has 2 rulings, which seems to be odd, as it obviously has none: From a real differential geometry point of view it doesn't, but over the *complex* numbers it does: it is essentially of the form $w^2+y^2+z^2 = w^2$ in $\mathbb{C}P^3$.

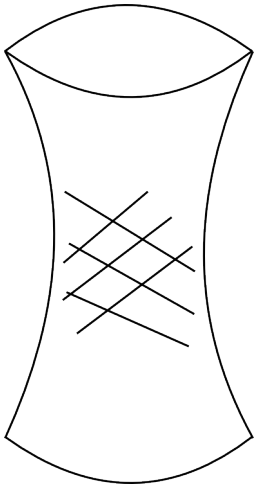


Figure 10: A hyperboloid with two rulings.

Example 55. The hyperboloid $x^2 + y^2 - z^2 = 1$ has 2 rulings over the *reals*. Projectively, $x^2 + y^2 = z^2 + w^2$. This is sometimes used in architecture (see Fig. 10, where the two rulings are the ones going in different directions).

Example 56. The *Veronese surface* is an embedding of P^2 into P^5 given by

$$(x : y : z) \mapsto (x^2 : xy : y^2 : xz : yz : z^2) =: (z_{11} : z_{12} : z_{22} : z13 : z_{23} : z_{33}).$$

These satisfy the relations $z_{ij}z_{kl} = z_{il}z_{jk}$.

We have lots of other similar embeddings $P^m \to P^n$, such as $(x_0 : \cdots : x_m) \mapsto (x_0^k, x_0^{k-1}x_1, \dots)$, where the image consists of monomials of some degree k.

Example 57. The *Grassmannian* $G(m, n)$ is the set of m-dimensional subspaces of k^{m+n}, which is the same as the set of $(m-1)$-dimensional linear subvarieties of P^{m+n-1}. For example, $G(0, n)$ is a point, and $G(m, n) \cong G(n, m)$: If we have an m-dimensional subspace W of V^{m+n}, we can map it to the dual $W^\perp$ in $V^* \cong k^{m+n}$, where $W^\perp$ is the set of all vectors of the dual V^* of V that vanish on W. This gives an isomoprhism between m-dimensional subspaces of V and $\dim(V) - m$-dimensional subspaces of V^*. Also note that $G(1, n) = P^n$.

The first non-trivial case of a Grassmannian is $G(2, 2)$ consisting of 2-dimensional subspaces of k^4 or of lines in P^3. We will find a variety whose points correspond to such lines; it is the simplest nontrivial example of a Hilbert scheme, which parametrizes subschemes of projective space. We will embed $G(2, 2)$ in P^5 by the so-called *Plucker embedding*.

Suppose a plane is spanned by two vectors $a = (a_0, a_1, a_2, a_3), b = (b_0, b_1, b_2, b_3)$. Look at the matrix $\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$. Look at all 2×2-minors, and take their determinants, so we get 6

numbers $\left(\det\begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix}, \dots\right) \in P^5$. We want to show that this depends on the subspace spanned by a, b and not of the choise of basis a, b. Any other basis is given by $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}$ for some $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_2(\mathbb{C})$. This multiplies all determinants above by $\det\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, which makes no difference in P^5. Thus we get a well-defined map $G(2,2) \to P^5$, and we will find the image of this map. It is not onto as $\dim P^5 = 5$ and $\dim G(2,2) = 4$ – in general, $\dim(G, m) = mn$. There must be some function vanishing on $G(2,2)$ but not on P^5. Suppose $s_{ij} = \det\begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix}$, and $(s_{01}, s_{02}, s_{03}, s_{12}, s_{13}, s_{23}) \in P^5$. There must be some relation between the s_{ij}. The relation is the *Plucker relation* given by (up to possible sign errors)

$$s_{01}s_{23} - s_{02}s_{13} + s_{03}s_{12} = 0.$$

The proof is given by simply expanding. For example, we have $s_{01}s_{23} = (a_0b_1 - a_1b_0)(a_2b_3 - a_3b_2)$ which has a term $a_0a_2b_1b_3$, which also appears in $s_{03}s_{12}$. In general every term $a_ia_jb_kb_l$ with i, j, k, l distinct occurs twice with opposite signs.

Now we want to check that the map from $G(2,2)$ to the points satisfying the Plucker relation is onto. We can suppose that some s_{ij} is nonzero, and assume that it is s_{01}. Put $s_{01} = 1$. Then $s_{23} = s_{02}s_{13} - s_{03}s_{12}$, so it is determined by the others. So the point $(s_{01}, \dots)$ is in the image of $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 & s_{12} & s_{13} \\ 0 & 1 & s_{02} & s_{03} \end{pmatrix}$; most of the 2×2 determinants look like $\det\begin{pmatrix} 1 & s_{13} \\ 0 & s_{03} \end{pmatrix} = s_{03}$. The final one is $\det\begin{pmatrix} s_{12} & s_{13} \\ s_{02} & s_{03} \end{pmatrix} \stackrel{?}{=} s_{23}$, so $(s_{01}, \dots)$ is in the image of the plane spanned by $(1, 0, s_{12}, s_{13})$ and $(0, 1, s_{02}, s_{03})$, so $G(2,2)$ is isomorphic to the quadric given by the Plucker embedding.

Example 58. We will consider the cohomology of a quadric in P^5. The quadric is isomorphic to $G(2,2)$. The Grassmannian can be written explicitly as a disjoint union of affine spaces – this make Grassmannians really easy to handle. We can do this explicitely; $G(2,2)$ is the union of: All planes spanned by $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}$ which gives a copy of A^4 in $G(2,2)$ (this corresponds to what we considered previously with $s_{12} \neq 0$). Similarly, we consider those spanned by $\begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}$ and $\begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ corresponding to copies of A^3 and A^2. These three give us all spaces containing $(* \; * \; * \; *)$ with the first $* \neq 0$. Finally, we add $\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. So $G(2,2)$ is a disjoint union of $A_4, A_3, A_2, A_2, A_1, A_0$, and the cohomology $H^i(G(2,2))$ has dimension $1, 0, 1, 0, 2, 0, 1, 0, 1$ for $i = 8, 7, \dots, 0$ respectively. Remark: The *ring* structure on the cohomology is quite complicated and involves Littlewood–Richardson coefficients.

Example 59. We will consider in a bit more detail the twisted cubic consisting of points $(s^3 : s^2t : st^2 : t^3) \in P^3$, which is the closure of the points $(t, t^2, t^3) \in A^3$, which corresponds to the ideal generated by $y - x^2, z - x^3$. The first one has degree 2 and the second one degree 3, and their intersection should have degree 6 by Bezout's theorem (which we haven't really covered yet), but from the name "cubic" it should have degree 3 (where we haven't really defined degree either). The missing "degrees" turn up "at ∞".

Suppose we look at the projective algebraic set given by the projectivizations of $y - x^2$, $z - x^3$, that is $wy - x^2, w^2z - x^3$. Again, the algebraic set given by these should have degree 6. To see what it looks like, we cover P^3 by four copies of A^3; if P^3 has coordinates $(w : x : y : z)$, these are given by one of the four coordinates being non-zero. For $w = 1$, the equations become $y - x^2 = 0$, $z - x^3 = 0$, we get the twisted cubic in A^3 we started with. If $x = 1$, we get $wy = 1, w^2z = 1$, we get a single curve, $w \neq 0, y = 1/w, z = 1/w^2$. If $y = 1$, we have $w - x^2 = 0, w^2z = x^3$. We get the equation $x^4z = x^3$ or $x^3(xz - 1) = 0$. This algerabic set has 2 components $x = 0$ and

$xz = 1$; the last one turns out to be the twisted cubic again, while the $x = 0$ corresponds to an extra line at ∞. Finally if $z ==$, we have $wy = x^2, w^2 = x^3$. If $w \neq 0$, eliminating y as $y = x^2/w$ we get $w^2 = x^3$, which is again a twisted cubic. Here we also get a line $w = 0$, $x = 0$, which is the same one as before. So, the projective algebraic set defined by $wy = x^2$, $w^2z = x^3$ has two components as before. The total degree of these seems to be $1 + 3 = 4 < 6$, but the line sort of has "multiplicity"; the line is given by $x^3 = 0$ rather than $x = 0$. What is going on is that the ideal $(wy - x^2, w^2z - x^3)$ is not radical. For example, $(y^2 - xz)x$ is not in this ideal, but its cube is.

9th lecture, September 23rd 2010

We will continue to run though examples of projective varieties. Last time we considered $G(2, 2)$ which can be deined as lines in P^3, 2-dimensional subspaces of k^4, or as the conic $s_{01}s_{23} - s_{02}s_{13} + s_{03}s_{12}$ in P^5 (the Plucker embedding).

Example 60. We will now generalize this to arbitrary Grassmannians $G(m, n)$, the m-dimensional subspaces of k^{m+n} or the $m - 1$-dimensional linaer algebraic sets in P^{m+n-1}. We will copy the construction of $G(2, 2)$, but with more variables to keep track of.

We pick m vectors spanning the subspace, $a_{11}, a_{12}, \ldots, a_{1,m+n}, \ldots, a_{m1}, \ldots, a_{m,m+n}$ and form the matrix $(a_{ij})_{ij}$. We will find functions of these invariant under a change of basis. As before, we take determimants of $m \times m$-minors. There are $\binom{m+n}{m}$ ways of doing this. These are almost but not quite invariant: If we act on the basis by an element A of GL_m, then each determinant is multiplied by $\det(A)$. So all $\binom{m+n}{n}$ determinants give a well defined vector in $P^{\binom{m+n}{n}-1}$. The next problem is to find its image. We need to find lots of relations satisfied by these $\binom{m+n}{n}$ determinants, generalizing the Plucker relations from before. The relations turn out to be:

$$0 = \sum_{\lambda} (-1)^{\lambda} P_{i_1,\ldots,i_{m-1},j_\lambda} P_{j_1,\ldots,j_{\lambda-1},j_{\lambda+1},\ldots,j_{m+1}},$$

where $P_{abc\ldots}$ is the determinant formed by columns $a, b, c, \ldots$, and $i_1, \ldots, i_{m-1}, j_1, \ldots, j_{m+1}$ are integers. The idea of the proof is the following:

(1) It's enough to do the case of an $m \times 2m$-matrix

(2) Expand everything out: Every term occurs twice with opposite signs

It is not necessary to write everything out like this; there is a fancy definition: A point of a Grassmannian is a subspace $W \subseteq V$. We consider exterior powers $\bigwedge^m W \to \bigwedge^m(V)$ which is a point in $P^{\binom{m+n}{m}-1}$.

We will check (/give a sketch) that this map is onto. We can assume that some $P_{abc\ldots}$ is 1 and assume that $P_{12\ldots m} = 1$. We can find a point of the Grassmannian with given values of $P_{12\ldots,r-1,r+1,\ldots,m,s}$ for any r, s. There are m choices of r and n choices of s. By choosing a point of Grassmannian with basis

$$\begin{pmatrix} 1 & 0 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & 0 & * & * & * \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & * & * & * \end{pmatrix}$$

with mn choices for the last columns, and these are the one giving the $P_{12\ldots,r-1,r+1,\ldots,m,s}$. Next we use the Plucker relations to show that all other coordinates $P_{***\ldots}$ are determined by these ones. The idea is that $P_{1\ldots m} \cdot P - i_1, \ldots, i_m$ is a sum of terms with more indices in the set $\{1, \ldots, m\}$.

We see that Grassmannians are given as an intersection of a huge number of quadrics – all Plucker relations have degree 2 in the coordinates. Grassmannians are also homogeneous spaces; it is possible to write them as the quotient of groups: The group GL_{m+n} acts transitively on m-dimensional subspaces, so $G(m,n) = GL_{m+n}/H$ for some subgroup H fixing some m-dimensional subspace. Taking the m-dimensional subspace to be spanned the first m coordinate vectors $e_1, \dots, e_m$. The matrices mapping this to itself is the set of block matrices $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, where the 0-block is of dimension $n \times n$. The set of these has dimension $m^2 + n^2 + mn$, so the Grassmannian $G(m,n)$ has dimension $(m+n)^2 - (m^2 + n^2 + mn) = mn$.

Notice that $G(m,n)$ is given by the quotient an *affine* algebraic group with an affine algebraic group, but the Grassmannian itself is projective. At first sight, GL_m doesn't look affine, as it's given by the equation $\det! = 0$, which is an *open* subset of A^{mn}. It is closed in $A^{m \cdot m+1}$ though: We can think of GL_m as pairs (m,t) with $m \in M_m$, $t \in k$ with $\det(m) \cdot t = 1$, which is a closed hypersurface. (Notice also that open subsets of A^n are not all isomorphic to affine varieties: This works for complements of 1-hyperplane but not for say $A^2 \setminus (0,0)$.)

Next we can ask what Grassmannians are good for. They were used by Grothendieck to construct Hilbert schemes. The construction is easy, but the definition of Hilbert schemes is much harder.

The idea is the following: A Hilbert scheme should parametrize algebraic subsets of P^n (in the same way as $G(m,n)$ parametrizes linear algebraic subsets). Rather, instead of algebraic subsets, we should have subschemes, which we haven't defined yet. In affine space, algebraic subsets correspond to radical ideals. The difference between algebraic subsets and subschemes is that the subscheme corresponds to all ideals. So really, instead of parametrizing subschemes of P^n, we parametrize graded ideals in $k[x_0, \dots, x_n]$. A graded ideal is an ideal $I = I_0 \oplus I_1 \oplus \cdots$, where I_d consists of homogeneous polynomials of degree d. By Hilbert's basis theorem, we can find d so that I_d generates $I_d \oplus I_{d+1} \oplus \cdots$. We can use I_d to define a point of a Grassmannian: I_d is a subspace of dimension $\dim(I_d)$ in s space of dimension the number of polynomials of degree d, so we get a well defined point of some Grassmannian. Suppose we fix the dimensions of $I_d, I_{d+1}, \dots$ as $\dim(I_d) = p(d)$ (we will see later that $p(d)$ is in fact a polynomial in d for large d, called the Hilbert polynomial). Look at the map from $I_d \times S_n \to S_{d+n}$, where S_n is the set of polynomials of degree n. The key point is that the rank of this map is at most $p(d+n)$ because the image lies in I_{d+n}. Recall a determinantal variety is given by linear maps $k^m \to k^n$ of rank less than or equal to r, so the rank requirement above gives a closed subset of the Grassmannian. The result is that for a sequence $p(d), p(d+1), \dots$, the ideals with dimension $\dim(I_d) = p(d)$ correspond to points of a certain closed subset of the Grassmannian. This is roughly the idea of the construction of Hilbert scheme: We take the scheme and map it to Grassmannians and notice that the map given above gives a closed point.

We have a couple of easy examples of Hilbert schemes:

(1) Grassmannians; these parametrize linear subspaces.

(2) Hypersurfaces in P^n given by $\sum a_* x_0^* x_i^* \cdots = 0$. We take the coefficients a_* as points of projective space of some high dimension. Here the Hilbert scheme is just some projective space.

(3) Consider n points on a line P^1. The roots of $a_n x^n + \cdots + a_0$ parametrized by $(a_0 : \cdots : a_n) \in P^n$.

These examples are misleading though, and in general Hilbert schemes exhibit every imaginable sort of weird behavior.

When we say that the Grassmannian parametrizes subspaces of P^n – rather than just saying that we parametrize by for example a discrete set of points – we really have the following idea by Grothendieck in mind: We don't just look at single subspaces but at families of subspaces of P^n. This means that we take some variety S and look at $P^n \times S \to S$. Consider now a subvariety $V \subseteq P^n \times S$ such that the intersection with V of each fiber is a linear subspace. We can think of

this as a family of linear subspaces parametrized by S. We need to add a condition saying that this is a well-behaved family; this condition is *flatness*. Then flat families of linear subspaces of P^n parametrized by S are the same as morphisms from S to the Grassmannian. This characterizes the Grassmannian.

This is a special case of a general problem: Suppose we have a functor from algebraic varieties to sets. For example taking a variety S to the linear subspaces of P^n parametrized by S. We can then ask to "represent" S; that is, can we find a variety V such that the functor is maps from S to V.

Example 61 (Hirzebruch surfaces). Take $(A^2 - 0) \times (A^2 - 0)$ with coordinates (s, t) and (x, y) respectively. Take the quotient by $G_m \times G_m$ where G_m is the set of nonzero elements of k. Here (λ, μ) acts as

$$(\lambda, \mu)(s, t, x, y) = (\lambda s, \lambda t, \mu x, \lambda^{-1}\mu y).$$

Denote the resulting so-called Hirzebruch surface by F.

If for example $a = 0$ λ acts only on the first two coordinates and μ only on the last two, so we get $(A^2 - 0)/G_m \times (A^2 - 0)/G_m = P^1 \times P^1$.

In general there is a map from F to P^1 mapping $(s, t, x, y) \mapsto (s, t) \in P^1$. The fiber (i.e. inverse image) at a given point (s, t) is just P^1. If we have fixed s, t, we also fixed λ, so we just get points of the form $(x, \lambda^{-1}y)$ modulo the scalars, which is P^1. Slightly more generally, P^1 can be written $P^1 = A^1 \cup A^1$, with $s = 1, t = 1$ respectively. Over the affine line $s = 1$, the inverse image is isomorphic to $P^1 \times A^1$, and similarly for $t = 1$. So F is a fiber bundle: We have a map $F \to P^1$, and P^1 is covered by open subsets U_i and on each U_i the map looks like $P_1 \times U_i \to U_i$. Locally, it looks like a product, but globally it's not if $a \neq 0$. This is the algebraic geometry analogue of the Möbius band.

We haven't actually seen that this can be embedded in projective space. We do this for the following more general case.

Example 62 (Scrolls). The scroll $F = F(a_1, \ldots, a_n)$ is the quotient of $(A^2 - 0) \times (A^n - 0)$ with coordinates (s, t), respectively $(x_1, \ldots, x_n)$ by $G_m \times G_m$ with coordinates (λ, μ), where now

$$(\lambda, \mu)(s, t, x_1, \ldots, x_n) = (\lambda s, \lambda t, \lambda^{-a_1}\mu x_1, \lambda^{-a_2}\mu x_2, \ldots).$$

As before there is a map from F to P_1 taking $(s, t, x_1, \ldots, x_n)$ to $(s, t) \in P^1$, where the fiber at each point is now P^{n-1}.

We will now embed F into projective space. Assume that all a_i are positive – this is harmless as we can change μ to μ times some power of λ. Now look at all monomials of the form $s^i t^{a_j - i} x_j$. This gives us $(a_1 + 1) + \cdots + (a_n + 1)$ monomials. They are not invariant under $G_m \times G_m$, but any two are multiplied by the same constant under any element of $G_m \times G_m$, so $(s^0 t^{a_1} x_1 : s^1 t^{a_1 - 1} x_1 : \cdots : s^0 t^{a_2} x_2 : \ldots)$ gives a welldefined point of projective space $P^{\sum(a_i+1)-1}$. Moreover we can see that the image of each fibe rof the map $F \to P^1$ is a linear subspace of $P^{\sum(a_i+1)-1}$. For $n = 2$, we just recover the Hirzebruch surfaces.

10th lecture, September 28 2010

2.4 Toric varieties

Before going on from projective varieties to morphisms, we consider so-called toric varieties. It turns out that projective varieties can be covered by open subsets that are affine. This is basically because P^n is a union of $n + 1$ copies of A^n, as we can take $(x_0 : \cdots : x_n)$ with $x_j = 1$.

For example differential or Riemannian manifolds, the old view was that these were given as subsets of $\mathbb{R}^n$ defined by zeroes of some equations. For example, the sphere $x^2 + y^2 + z^2 = 1$. On the other hand the current view is that we don't bother embedding into Euclidean space, but instead it should locally look like Euclidean space (that is, it is covered by an "atlas of charts").

Projective varieties are similar. They are defined as in the "old" way: As a subset of projective space. The current view (essentially due to Weil) is that varieties are "things", looking locally like affine varieties. For example, the Grassmannian $G(m,n)$ was easy to cover by affine subsets isomorphic to A^{mn} but it was much harder to embed it in projective space.

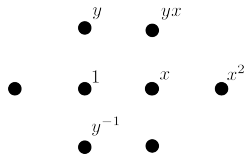


Figure 11: The points of $\mathbb{Z}^n$.

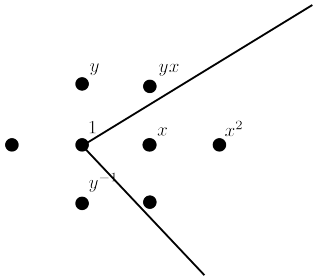


Figure 12: A convex cone in $\mathbb{Z}^n$.

Look at the ring $k[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$, which is the coordinate ring of the affine ring A^n minus the coordinate planes, which is the same as the product of n copies of $A^1 - 0$. A basis corresponds to points of $\mathbb{Z}^n$ (Fig. 11). Taking a convex cone with a point at 0 as in Fig. 12, we get a ring with a basis of monomials in the cone. This ring is finitely generated if the cone is polyhedral with finite number of rational faces (one could easily get something not finitely generated by choosing irrational slopes). Then, it is a coordinate ring of an affine variety.

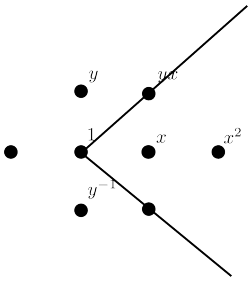


Figure 13: A particular convex cone.

Example 63. The cone consisting of the first quadrant just gives $x^i y^j$, $i, j \geq 0$, which just gives $k[x,y]$ and we get A^2.

Consider the cone in Fig. 13. Put $X = xy$, $Y = x$, $Z = xy^{-1}$, the ring is generated by X, Y, Z with relations $Y^2 = XZ$. So we get the ring $k[X,Y,Z]/(Y^2 = XZ)$, which is essentially a conical singularity.

Bigger cones tend to correspond to smaller varieties. Look at $\mathbb{Z}^n$ as above. We also have the dual of $\mathbb{Z}^n$, and the dual of a smaller cone gives a bigger cone (see Fig. 14). Here, the dual of a cone C is the set $\hat{C}$ of vectors in $\mathbb{Z}^n$ with non-negative inner product with everything in C. For each cone in the dual $\widehat{\mathbb{Z}^n}$, we get an affine variety, and if $C_1 \subseteq C_2$, we get a map $\hat{C}_1 \supseteq \hat{C}_2$, so we

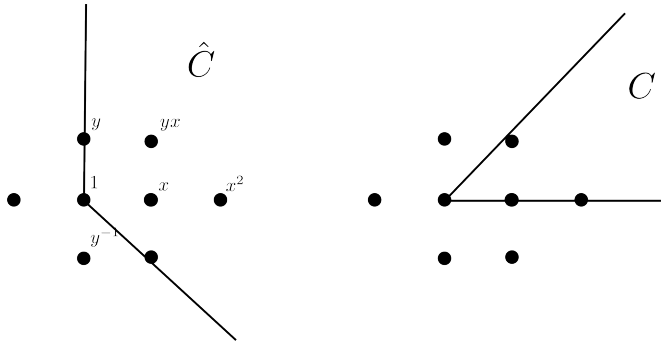


Figure 14: A cone and its dual.

get a map $V_1 \to V_2$ between varieties (which now goes in the "right" direction). Now we divide up $\mathbb{R}^n$ into a union of cones and glue together the corresponding varieties.

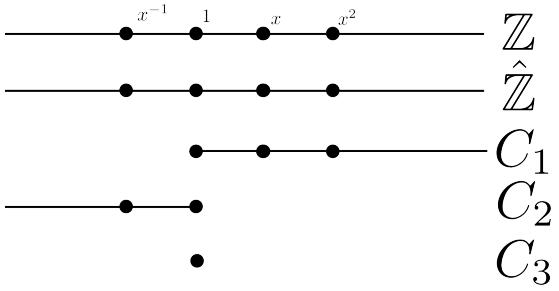


Figure 15: Three cones in $\hat{\mathbb{Z}}$.

Example 64. Divide up the dual $\hat{\mathbb{Z}}$ in three cones C_1, C_2, C_3 as in Fig. 15. The dual of C_1 will just be C_1, and the same is true for C_2. On the other hand, the dual of C_3 will be all of $\mathbb{Z}$. The corresponding varieties are $k[x] = A^1$, $k[x^{-1}] = A^1$ and $k[x, x^{-1}] = A^{-1} - 0$ respectively. We now glue together the two copies of A^1 by gluing along the $A^1 - 0$. Doing this we get $P^1 = A^1 \cup A^1$ where the intersection of the two parts in the union is $A^1 - 0$.

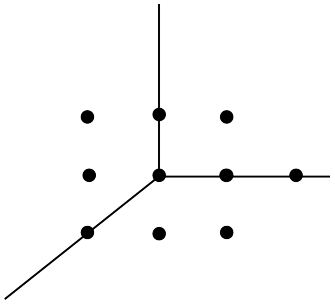


Figure 16: Another division of the plane.

Example 65. Divide the plane into the four quadrants (Fig. 16) obtaining 9 cones. In this case we get $P^1 \times P^1$.

Example 66. Divide the plane as in Fig. 16. This gives P^2.

This procedure gives an enormous amount of projective varieties. In fact covering $\mathbb{R}^n$ by any finite collection of convex rational cones gives some projective variety.

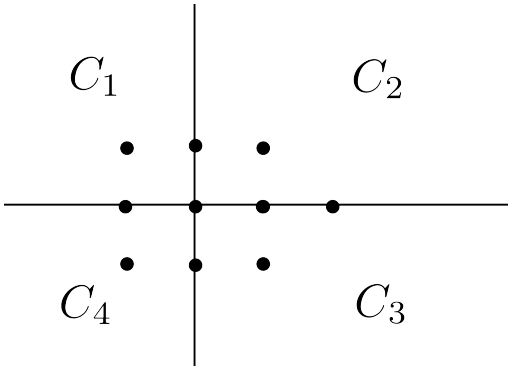


Figure 17: Yet another.

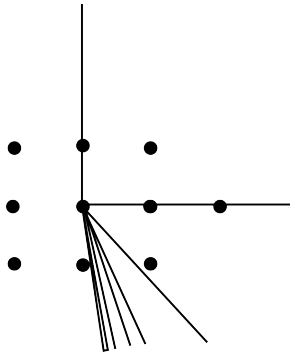


Figure 18: An infinite number of cones.

Example 67. One can construct weird objects this way. For example we can take an infinite number of cones as in Fig. 18 and apply the construction.

For more information on tonic varieties, see [Ful].

3 Morphisms of varieties

We now go to morphisms of varieties corresponding to Section 1.3 of [Har].

We begin by recalling some facts from category theory.

Example 68. An example of a category is the category of sets with objects the sets and morphisms from A to B is the set of functions from A to B.

Example 69. Another one has objects the commutative rings and morphisms the homomorphisms of rings.

Example 70. Objects are abelian groups and morphisms are the homomorphisms of groups.

Example 71. Objects are smooth manifolds and morphisms are smooth maps between smooth manifolds.

Considering these four examples and extracting what they have in common, we get the following definition of a category.

Definition 72. A *category* is something that resembles the above:

(1) We have a set or class of objects.

(2) For each two objects A, B we have a set of morphisms from A to B.

(3) For each object A there is an identity morphism 1_A form A to A.

(4) If $f : A \to B$, $g : B \to C$ are morphisms, there is a *composite* morphism $g \circ f : A \to C$.

(5) Composition is associative; $(f \circ g) \circ h = f \circ (g \circ h)$.

(6) Identities behave in the obvious way.

The key points is that if you are considering any sort of mathematical objects, you should ask what the morphisms between them are. We should thus ask what the morphisms between varieties are. There are two different sorts of morphisms:

(1) Regular maps: These are similar to smooth maps of manifolds.

(2) Rational maps: Maps that are "not defined everywhere". For example $1 \mapsto 1/x$ is a rational maps from A^1 to A^1; notice that this does not correspond to a function on the underlying sets.

To define morphisms (regular maps) between varieties, we first look at the case of differentiable manifolds M, N. A morphism $f : M \to N$ is a *function* from M to N such that if g is a smooth function on N, then $g \circ f$ is smooth on M; in other words, smooth functions are smooth. We can use the same idea to define morphisms of affine varieties: We will first define the analogue of smooth real functions, called regular functions $f : V \to k$, and a regular map will be a function $f : V \to W$ such that if g is regular on W, then $g \circ f$ is regular on V. (Note as a warning that we need to modify this for projective varieties, as there are not enough regular functions.)

Definition 73. *Regular functions on affine varieties* are defined to be elements of the coordinate ring. For example the regular functions on A^2 are just elements of $k[x, y]$.

We now turn to open subsets U of affine varieties V.

Definition 74. A map $f : U \to k$ is called *regular*, if we can write $f = g/h$ on U, where g, h are regular on V, and $h \neq 0$ at any point p of U.

Example 75. If $V = A^1$, $U = A^1 - 0$, then $1/x$ is regular on U.

We should check that the above two definitions are compatible for affine varieties: Suppose $V = U_1 \cup \cdots \cup U_n$ with U_i open (note that V is compact, so we always use finitely many open sets). Suppose f is regular on V by the second definition. This means that $f = g_i/h_i$ on U_i. We need to check that f is in the coordinate ring of V. We know that $h_i \neq 0$ on U_i, and the U_i cover V, so there is no point where all h_i vanish. So the h_i generate the unit ideal by the weak Nullstellensatz, and we can write $1 = a_1 h_1 + \cdots + a_n h_n$ for some a_i in the coordinate ring. This suggests that $f = f a_1 h_1 + f a_2 h_2 + \cdots$ (note that this is meaningless as we don't know yet that f is in the coordinate ring). Define $f = a_1 g_1 + \cdots a_n g_n$. Now we need to check that $f = g_i/h_i$ on U_i. In other words, we should check that $(a_1 g_1 + \cdots + a_n g_n) h_i = g_i$, which follows from the fact that $h_i g_j = h_j g_i$ for all i, j, which proves that the definitions are compatible.

Definition 76. Similarly, a function on an open subset of a (quasi-)projective variety is called *regular* if it is regular on every open affine subset (so it is enough to check it for a cover of affine subsets).

This makes (projective) varieties into ringed spaces.

Definition 77. A *ringed space* is given by the following data:

(1) A topological space V.

(2) For each open set U, we have a ring $R(U)$ (which we can *sometimes* (this fails for schemes) think of as functions on U).

(3) If $T \subseteq U$, we have a morphism $R(U) \to R(T)$ (which we think of as restriction).

(4) We have an identity morphism $R(U) \to R(U)$ behaving in the obvious way.

(5) For $S \subseteq T \subseteq U$ then $R(U) \to R(S)$ is the composition $R(U) \to R(T) \to R(S)$.

(6) If U is covered by $U_1, \ldots, U_n$, then $f \in R(U)$ is determined by its restrictions to U_i.

(7) If we are given $f_i \in R(U_i)$ with $f_i = f_j$ on $U_i \cap U_j$, then we can find f whose restrictions to U_i are f_i.

Example 78. The following are ringed space.

(1) For a differentiable manifold M, let $R(U)$ be the smooth functions on U.

(2) For a topological manifold, let $R(U)$ be the continuous functions on U.

(3) For a variety let $R(U)$ be the regular functions on U.

Example 79. The regular functions on P^1: Cover P^1 by affine open subsets $P^1 = A^1 \cup A^1$ as before. The regular functions on P^1 are given by

(1) Regular functions f on the first A^1.

(2) Regular functions g on the second A^1.

(3) That are equal on $A^1 \cap A^1 = A^1 - \text{pt}$.

For example, writing the points on P^1 as $(x : y)$ we have $f \in k[x]$, $g \in k[y]$ that are the same on $k[x, y] = k[x, x^{-1}]$. The restriction of f to $k[x, x^{-1}]$, the coordinate ring of $A^1 - \text{pt}$, is a polynomial in x, and the restriction of g is a polynomial in x^{-1}, so if $f = g$, both of them must be constant, so the regular functions on P^1 are just *constants*. The same is true on *any* projective variety (which is why we spend time bothering with defining functions on open subsets of projective varieties).

Definition 80. A *morphism* $f : X \to Y$ is a function from X to Y such that if g is a regular function on a open subset U of Y, we get $g \circ f : f^{-1}(U)$ is regular.

Note as before that this definition is wrong for schemes.

11th lecture, September 30th 2010

Last lecture we defined a *regular function* on an open set of a variety to be something locally of the form f/g with $g \neq 0$. We defined a regular map $f : V \to W$ between varieties to be something satisfying that the pullback of a regular function on an open subset is regular. We mentioned that varieties are (locally) ringed spaces: On each open subset U, we are given a ring $R(U)$ satisfying a list of conditions. A morphism of a variety is a special case of a morphism of a ringed space.

Example 81. Suppose V is a real smooth algebraic variety. We can form lots of different ringed spaces out of this: We could form $C^0(V)$ with $R(U)$ the continuous functions on U, $C^1(V)$ with $R(U)$ differentiable functions, and so on, as well as $C^\infty(V)$ the smooth functions, $C^\omega(V)$ the real analytic or considering V as a ringed space with $R(U)$ the regular functions. We have morphisms

$$C^0(U) \to C^1(U) \to \cdots \to C^\infty(U) \to C^\omega(U) \to V.$$

That is, we have different structures (topological, smooth, analytic, algebraic) corresponding to different ringed spaces with underlying topological space V (the topology actually changes with the last morphism, but ...).

Example 82. Look at the curve $y^2 = x^3$ and the affine line A^1 with coordinate t. There is a morphism from A^1 to $y^2 = x^3$ given by $t \mapsto (t^2, t^3)$. This is regular: We should check that the pullback of a regular function is regular, but this is trivial; a regular function on $y^2 = x^3$ looks like $\sum a_{ij} x^i y^j$. Pulling back we get $\sum a_{ij}(t^2)^i(t^3)^j$, which is obviously regular on A^1. More generally, any morphism defined by polynomials will be regular. Our map is also a *homeomorphism* on the underlying topological spaces (it is bijective, and the open sets in both cases are empty or complements of finite sets). It is not, however, an isomorphism of varieties (defined below). This can be seen for example by noting that the coordinate rings of regular functions are different. The coordinate ring of A^1 is spanned by $1, t, t^2, t^3, \dots$, while the coordinate ring of $y^2 = x^3$ is spanned by $1, t^2, t^3, \dots$ and these two rings are not isomorphic (exercise).

Definition 83. An *isomorphism of varieties* f means the obvious thing: If $f : A \to B$, there exists an inverse $g : B \to A$, that is $fg = 1_A, gf = 1_B$.

Note that this definition makes sense for any category.

We can ask the following: Given varieties X, Y, what are the morphisms $X \to Y$? In general, this is tricky to work out. There is one easy case:

Theorem 84. *If Y is affine, then morphisms (regular maps) from $X \to Y$ are essentially "the same as" ring homomorphisms $\mathcal{O}(Y) \to \mathcal{O}(X)$, where $\mathcal{O}$ means the ring of regular functions (note the change of directions).*

As an application of this is that a category of affine algebraic sets is (equivalent to) the opposite of a category of commutative algebras over k, finitely generated and with no nilpotents.

Definition 85. The *opposite* of a category is given by changing the direction of all morphisms. If objects A, B in a category C has morphisms $\mathrm{Mor}(A, B)$ from A to B, then the morphisms from A to B in C^{op} are $\mathrm{Mor}(B, A)$.

Proof of theorem. Suppose ϕ is a morphism from X to Y (algebraic sets). Then ϕ^* takes regular functions g on Y to regular functions $g\phi$ on X; $X \xrightarrow{\phi} Y \xrightarrow{g} k$. So we get $\phi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. This works even if Y is not affine. So we have a map $\mathrm{Mor}(X, Y) \to \mathrm{Hom}(\mathcal{O}(Y), (\mathcal{X}))$, and we want to construct an inverse map $\mathrm{Hom}(\mathcal{O}(Y), \mathcal{O}(X)) \to \mathrm{Mor}(X, Y)$. Constructing this inverse needs Y to be affine. Suppose Y is affine given by the zeros of some ideal $I = \sqrt{I}$ in $k[x_1, \dots, x_n]$, so $\mathcal{O}(Y) = k[x_1, \dots, x_n]/I$. Suppose that $h : \mathcal{O}(Y) \to \mathcal{O}(X)$ is a homomorphism. Define $\psi : X \to Y$ as follows. Look at $x_1, \dots, x_n \in \mathcal{O}(Y)$. We have $h(x_1), \dots, h(x_n) \in \mathcal{O}(X)$, so if p is any point of X, then $h(x_i)(p)$ is an element of k. Define $\psi(p) = (h(x_1)(p), \dots, h(x_n)(p)) \in k^n$. This gives a map $\psi : X \to k^n$. We now have to check that the image is in y, that ψ is a regular map, and that the map $h \mapsto \psi$ is the inverse to the map $(X \to Y) \mapsto (\mathcal{O}(Y) \to \mathcal{O}(X))$. For example, that the image is in Y, follows because $h(I) = 0$ (if a polynomial is in I, then it vanishes on $(h(x_1)(p), \dots)$). To check that ψ is a regular map, notice that $x_i \circ \psi$ is regular on X for each x_i on Y. So if $f(x_1, \dots, x_n)$ is regular on Y, then $f \circ \psi = f(x_1 \circ \psi, x_2 \circ \psi, \dots)$ which is a polynomial in $x_1 \circ \psi$, $x_2 \circ \psi, \dots$, so it is regular. So ψ^* takes regular functions on Y to regular function on X, so it is regular. The remaining steps are left as exercises. □

Example 86. We consider *algebraic groups*: These are varieties G that are also groups so that multiplication $G \times G \to G$ and inverse $G \to G$ are morphisms of varieties.

For example, consider the additive group G_a. The variety is A^1, the additive group of k. The group law is given by $(x, y) \mapsto x + y$. The corresponding map on coordinate rings is the following: G_a has coordinate ring $k[t]$, and $G_a \times G_a$has coordinate ring $k[t_1, t_2]$, so we get a map $k[t] \to k[t_1, t_2]$ given by $t \mapsto t_1 + t_2$. Writing $k[t_1, t_2] = k[t] \otimes k[t]$, we get an example of a coproduct. If we have a multiplication $R \otimes R \to R$, we have a notion of a coproduct $R \to R \otimes R$. So for example, the coproduct is the induced map $\mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$ for G an algebraic group.

Another example is the multiplicative group G_m. The underlying variety is $A^1 - 0$ with group operation $(x, y) \mapsto xy$. The corresponding coproduct $k[x, x^{-1}] \to k[y, y^{-1}] \otimes k[z, z^{-1}]$ maps $x \mapsto yz$.

Now look at the group $SL_2(k)$ of invertible 2×2-matrices with determinant 1. The co-ordinate ring is $k[a,b,c,d]/(ad-bc-1)$. Again we will find the map $R \to R \otimes R$ induced by the product of $SL_2(k)$. We will define a map $R = k[a,b,c,d]/(ad-bc-1) \to R \otimes R = k[a_1,b_1,c_1,d_1,a_2,b_2,c_2,d_2]/(a_1d_1 - b_1c_1 - 1, \dots)$. Writing out the product of matrices, we see that $a \mapsto a_1a_2 + b_1c_2$, $b \mapsto a_1b_2 + b_1d_2$ and so on. Similarly we can find a map $R \to R$ corresponding to $g \mapsto g^{-1}$. This map is given by $a \mapsto d$, $b \mapsto -b$, $c \mapsto -c$ and $d \mapsto a$. These maps $R \to R \otimes R$, $R \to R$ make the ring R into a *Hopf algebra*; that is, basically a ring R with maps $R \to R \otimes R$, $R \to R$ satisfying several axioms (we should also somehow get a co-unit).

Example 87. We will see that the twisted cubic in P^3 is isomorphic to P^1. Recall that the twisted cubic is the set of points $(s^3 : s^2t : st^2 : t^3)$ in P^3, which is also the projective variety of the ideal $(wy = x^2, xy = wz, xz = y^2)$ in coordinates $(w : x : y : z)$. We define a map P^1 to the cubic by $(s : t) \mapsto (s^3 : s^2t, st^2, t^3)$. (We can check this is regular by checking it is regular on to affine subsets $(1 : t)$, $(s : 1)$.) In fact this map is a homeomorphism, but as above this is *not* enough to show it is an isomorphism of varieties. We now define a map from the cubic to P^1. We could try defining $(w : x : y : z) \mapsto (w : x)$. This almost gives an inverse, but it is not defined on $(0 : 0 : 0 : 1)$. A second try would be $(w : x : y : z) \mapsto (y : z)$ or $(x : y)$, but this has the same problem. Instead to define the map, we chop the cubic into two pieces. We cover the cubic by two copies of A^1, and define a map on each of these and check these maps are the same on their intersection $A^1 \cap A^1$ – this is really the difference between defining morphisms of affine and projective varieties. The first A^1 consists of (w,x,y,z) with $w \neq 0$, which we map to $(w : x)$. For the second one, $z \neq 0$, and we define the map to be $(w : x : y : z) \mapsto (y : z)$. We need to check that these two maps are the same on the intersection $w \neq 0, z \neq 0$ of the cubic. So we have to check that $(w : x) = (y : z)$, which follows as $wz = yx$ on the twisted cubic, and we get a map from the cubic to P^1. To check that this is the inverse of the first map is left as an exercise.

The key point of the last example was that we cover projective varieties by affine ones and define the morphisms on affine open subsets.

Example 88. Recall that $A^1 - 0$ is isomorphic to $xy = 1$ by an isomorphism $x \mapsto (x, x^{-1})$ with inverse $(x,y) \mapsto x$. We can then ask what affine variety $A^2 - (0,0)$ is isomorphic to. The answer is none: We calculate the ring of regular functions on $A^2 - (0,0)$; if $A^2 - (0,0)$ was an affine variety, this ring would be the coordinate ring of the variety. To do this, we use the same idea as before. Cover $A^2 - (0,0)$ by open affine subsets $A^2 - x$-axis, $A^2 - y$-axis. The first one has coordinate ring $k[x,y,y^{-1}]$ and the second one has coordinate ring $k[x,y,x^{-1}]$. A regular function on $A^2 - (0,0)$ can be given as follows. It is the same as a regular functions on each of the two affine sets that are the same on their intersection. That is, elements of $k[x,y,y^{-1}]$ and $k[x,y,x^{-1}]$ that coincide in $k[x,y,x^{-1},y^{-1}]$, the coordinate ring of A^2 with both axes removed. The only posibility is that the two regular functions are the same and they should be a polynomial in x and y. So the ring of regular functions $\mathcal{O}(A^2 - (0,0))$ is $k[x,y] = \mathcal{O}(A^2)$, so the only possibility for $A^2 - (0,0)$ to be affine is that $A^2 - (0,0) \cong A^2$, but they are obviously not the same, so $A^2 - (0,0)$ is not isomorphic to any affine variety. This is a general phenomemon: If one throws away a codimension one set from an affine variety, the result is usually affine, while that is usually not the case, when you throw away a codimension two set as in this case.

Example 89. The group $GL_2(k)$ acts on the projective line by mapping $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} as + bt \\ cs + dt \end{pmatrix}$, where we write $(s : t) \in P^1$. This fixes a point $(1 : 0) \in P^1$, and we get a morphism $GL_2(k) \to P^1$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a : c)$. This is a *surjective* map from an affine variety to a projective variety.

This is another example where the quotient of 2 affine algebraic groups is projective.

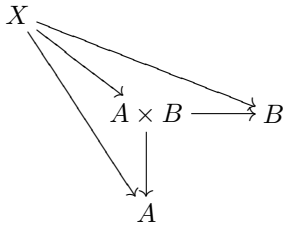
12th lecture, October 5, 2010

3.1 Products of affine varieties

We continue giving more examples of morphisms by discussing products of affine varieties. The first question is what a product is. As we have already discussed, it is not clear what $A^1 \times A^1$ should be, as we are not taking the product topology. The answer is given by category theory: The product $A \times B$ has the following properties:

(1) We have morphisms $A \times B \to A$ and $A \times B \to B$.

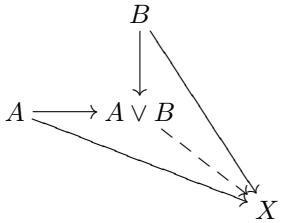
(2) It is universal: If some object X has morphisms to A and B, there is a unique morphism $X \to A \times B$, so that the following diagram commutes.



That is, $A \times B$ is a universal object with maps to A and B. Note that it is unique up to a canonical isomorphism: Suppose X and Y are two products. Using the universal property we get maps $Y \to X$ and $X \to Y$, and we want to check that these are inverses of each others. The composition of the two maps must be the identity by the uniqueness requirement.

Example 90. To see that products are not necessarily unique, we consider the product of two sets A and B. This will be the set of ordered pairs (a, b), $a \in A$, $b \in B$ – it is an easy exercise to check that it satisfies the universal property. The question is what an ordered pair is, and there are lots of differents definitions. For example (a, b) can be considered as $\{a, \{a, b\}\}$, $\{\{a\}, \{a, b\}\}$, or $\{\{a, 1\}, \{b, 2\}\}$. It really doesn't matter which one to use here, as all of the definitions have the key universal property, so they give canonically isomorphic products.

We can also define coproducts, which are the same but with all arrows reversed. That is, we have a commutative diagram as below, where every time we have maps $B \to X$ and $A \to X$, there should exist a map $A \vee B \to X$ making everything commute.



Exercise 91. Check that the coproduct of 2 sets is the disjoint union of the sets.

Example 92. We will see that the coproduct of 2 commutative rings R, S is the tensor product $R \otimes S$. To do this, we check the universal property. We certainly have maps $R \to R \otimes S$, and $S \to R \otimes S$ given by $r \mapsto r \otimes 1$, and $s \mapsto 1 \otimes s$ respectively. Suppose that we have maps $f : R \to X$ and $g : S \to X$. We need to show that there is a unique map $R \otimes S \to X$ making everything commute. This is the additive map taking $r \otimes s$ to $f(r)g(s)$. It is left as an exercise to check that this works.

Note that the coproduct of R, S depends on the category we work in: The coproduct of the sets R, S is the disjoint union, thet coproduct of commutative rings R, S is $R \otimes S$, and the coproduct of general rings R, S is the free product of R and S. We will only really consider the second one.

Recall that the category of affine varieties is more or less the opposite of the category of finitely generated commutative rings over k with no nilpotents. Taking opposites turns products into

coproducts. So, products of affine varieties corresponds to taking coproducts in the category of commutative rings, which by the example above corresponds to tensor products. A product of affine varieties can thus be given by first finding the coordinate rings, then taking the tensor product of the coordinate rings, and then taking some variety corresponding to this coordinate ring. It doesn't really matter which variety you take, as they all have the universal property.

Exercise 93. Check that this is equivalent to the previous definition of a product of $X \subseteq A^m$, $Y \subseteq A^n$ given by $X \times Y \subseteq A^{m+n}$ with a suitable topology.

3.2 Products of projective varieties

We consider only $P^n \times P^m$, as general projective varieties are then easy to do. Remember that we have the Segre embedding $P^m \times P^n \to P^{mn+m+n}$

Theorem 94. *The image in P^{mn+m+n} of the Segre embedding is a product of P^m and P^n (in the category of quasi-projective varieties).*

Proof. We need to show that

(1) we have maps from the Segre embedding to P^m and P^n, and that

(2) these maps are universal.

The key idea here is to cover everything by open affine subsets. To construct a map from the image of Segre embedding to P^m, recall that the image is points of the form $(z_{00} : z_{01} : \dots)$ with $z_{ij}z_{kl} = z_{il}z_{jk}$. Pick an affine subset, say $z_{00} \neq 0$. Now map $(z_{00} : z_{01} : \dots)$ to $(z_{00} = 1 : z_{10} : \cdots : z_{m0}) \in P^m$. Suppose we chose a different open affine subset, say $z_{01} = 1$. Then we map $(z_{00} : z_{01} : \dots)$ to $(z_{01} : z_{11} : \cdots : z_{m1}) \in P^m$. We need to check that these two maps are the same on the intersection. In other words, we should check that $(z_{00} : z_{10} : \cdots : z_{m0}) = (z_{01} : \cdots : z_{m1})$ in P^m. This follows from the Segre relations $z_{i0}z_{j1} = z_{i1}z_{j0}$. Similarly we can define a map from the Segre embedding to P^m on any open affine of the form $z_{ij} \neq 0$ and check that these are all compatible on intersections $z_{ij} \neq 0$ and $z_{kl} \neq 0$.

It now remains to check the universal property. That is, suppose we have maps $X \to P^m$, $X \to P^n$, and let us see that we can find a map from X to the Segre embedding. In general, a morphism $X \to P^n$ is complicated and involves line bundles on X. We avoid this problem by instead considering only small open affine subsets of X. We cover P^m and P^n by open affine subsets A^m, A^n. Now look at open affine subsets Y of X whose images lie in A^m, A^n; these are just given by coordinate functions and are easier to deal with. So we have maps $Y \to A^m = \{x_0 : \cdots : x_m\}$ with $x_i = 1$ and $Y \to A^n = \{y_0 : \cdots : y_m\}$ with $y_j = 1$. We can define a map $Y \to P^{mn+m+n}$ by mapping it to points with coordinates $(x_0y_0 : x_0y_1 : \cdots : x_my_m)$. This is in the image of the Segre embedding, as we have

$$z_{ij}z_{kl} = x_iy_jx_ky_l = x_iy_lx_ky_j = z_{il}z_{kj}.$$

So we can cover X by open affine subsets Y and we have defined a map to the Segre embedding on each Y. We then need to check that these maps are the same on intersections, which is left as an exercise. This gives a map from X to the Segre embedding, and this is unique, which is an exercise as well. □

This is really a combination of to unrelated properties.

(1) We need to construct a product of P^m and P^n.

(2) We need to embed this product in projective space.

If we don't really care about embedding the product in projective space, we can construct a sort of "abstract product" of A and B without worrying about embeddings into projective space like in Fig. 19. Here we get 6 products of open affine subsets (the rectangles). Gluing these together we get a product of A and B. This construction reflects what we are going to do for general schemes later, and we will not see the details here. The key idea is that we do not embed the product into projective space but instead consider it as being covered by affine subsets.

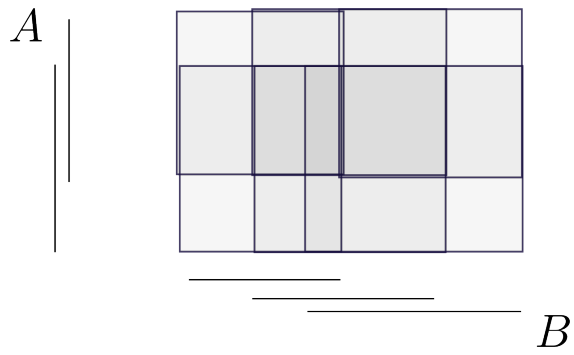


Figure 19: An abstract product of A and B. A is covered by two open subsets, and B is covered by three.

3.3 Automorphisms

Example 95. We consider first automorphisms of A^n; that is, isomorphisms from A^n to itself.

First, consider A^1. We find all regular maps $A^1 \to A^1$. This is the same as regular functions $k[x]$. Composition of regular maps correspond to composition of polynomials $f(g(x))$. Note that the identity is just the map x (corresponding to $x \mapsto x$). Note that $\deg(f \circ g) = \deg f \cdot \deg g$, so if $\deg(f \circ g) = 1$ then $\deg f = 1$, $\deg g = 1$, so the only regular maps $A^1 \to A^1$ with inverses are those corresponding to polynomials of degree exactly 1; that is, maps $x \mapsto ax + b$ with $a \neq 0$. These form a 2-dimensional non-commutative group.

Now look at $A^n \to A^n$. There are some obvious automorphisms generalizing the above: We can map $X \mapsto AX + B$, where $X = (x_1, \ldots, x_n)$, A is an $n \times n$ matrix and $B = (b_1, \ldots, b_n)$. However, these are far from being all automorphisms. For example, for A^2 we have a map $x \mapsto x$, $y \mapsto y + p(x)$ for any polynomial p. This has an inverse $x \mapsto x$, $y \mapsto y - p(x)$, and this gives an infinite dimensional abelian group of automorphisms. It is natural to ask for all automorphisms. Endomorphisms are easy: We map $x_i \mapsto f_i(x_1, \ldots, x_n)$ for polynomials $f_1, \ldots, f_n$, and we want to see when the set of the $f_1, \ldots, f_n$ gives an automorphism. We look at the Jacobian, $\det(\frac{\partial}{\partial x_i} f_j)$. The Jacobian of $f \circ g$ is the product of the individual Jacobians. So if f is invertible, so is its Jacobian; that is, $\det(\frac{\partial f_j}{\partial x_i}) \in k$. One can ask if the converse holds, which is the notorious *Jacobian conjecture*: If $\det(\frac{\partial f_j}{\partial x_i})$ is in k, is the map $x_i \mapsto f_i(x_1, \ldots, x_n)$ an automorphism? This is unsolved, even in the 2-dimensional case.

Example 96. We consider now morphisms from P^1 to itself. Any morphism $P^1 \to P^1$ restrics to a map from an open subset of A^1 (consisting of points not being mapped to ∞, where we write $P^1 = A^1 \cup \infty$) to A^1. These are regular functions on A^1 minus some points (or the empty set), which are given by rational functions $f(x)/g(x)$ (or $\infty = 1/0$), so morphisms $P^1 \to P^1$ are all birational functions $(x : y) \mapsto (f(x, y) : g(x, y))$, with f, g homogeneous of the same degree. Rational functions $f(x)/g(x)$ are invertible if f, g have degree 1, so the automorphisms are given by maps of the form $x \mapsto \frac{ax+b}{cx+d}$, with $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$. But $x \mapsto \frac{ax+0}{0+a}$ is the identity, so we need to divide out by $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, so

$$\mathrm{Aut}(P^1) = PGL_2(k) = GL_2(k)/(\text{diagonal matrices}).$$

So, note that the automorphism group of the affine line over $\mathbb{C}$ is the group $z \mapsto ax + b$ (where $a \neq 0$), which is the same as the automorphism group of the complex plane to itself in complex analysis (the morphisms from the complex plane to itself is the set of all holomorphic functions).

Similarly, automorphisms of the projective line over $\mathbb{C}$ are the "same as" automorphisms of the Riemann sphere $\mathbb{C} \cup \infty$ in complex analysis. In this case, all holomorphic maps from the Riemann

sphere to itself are the "same as" morphisms from P^1 to P^1. This is a special case of Serre's paper GAGA: For *projective* varieties, analytic things tend to be algebraic.

Example 97. The following is a standard counterexample in algebraic geometry. Look at the map from $A^2 \to A^2$ given by $(x, y) \mapsto (x, xy)$. The image is the set of points (x, y) such that $x = 0$ implies $y = 0$. That is, it contains all of A^2, except from the part of the y-axis away from the origin. In particular it is neither open nor closed, and it is not an affine variety. In other words, the image of a map from an affine variety to an affine variety need not be affine. The image is in fact constructible: This means that it is a finite union of locally closed sets, and a theorem due to Chevalley says that the image of a constructible set is constructible – the example at hand shows that we cannot do much better than that.

Example 98. We now turn to the Ax–Grothendieck theorem: Suppose that f is an injective morphism from a variety V (over an algebraically closed field) to itself. Then f is surjective. The proof is amazingly simple.

(1) Note that the theorem is trivial over finite fields, as the number of points is finite, and any injective map from a finite set to itself is surjective.

(2) It is still true over the algebraic closure of a finite field: Just take the finite field generated by the coefficients of the polynomials defining the map and the point we want to show is in the image.

(3) Therefore it is true for all algebraically closed fields. This follows from the following: Any statement of a first order language of fields that is true for some algebraically closed fields of characteristic p for all $p > 0$, is true for all algebraically closed fields of characteristic 0. See the next lecture for a more precise statement.

13th lecture, October 7th 2010

Last time we were looking at the Ax–Grothendieck theorem: If $\phi : V \to V$ is injective, then it is surjective. We noticed that this is true for algebraic closures of finite fields; essentially because over finite fields, we can just count things. Therefore it is true for all algebraically closed fields:

Suppose that S is a statement in first order language (made precise below) of fields, then the following are equivalent:

(1) S is true in some algebraically closed field of characteristic zero.

(2) S is true for all algebraically closed fields of characteristic zero.

(3) S is true for some algebraically closed fields in arbitrarily large characteristic $p > 0$.

(4) S is true for all algebraically closed fields of sufficiently large characteristic (depending on S).

This is a case of the Lefschetz principle: If you can prove "something" (meaning first order statements) for complex numbers (using Riemannian geometry, Hodge theory, ...), then it is true for all algebraically closed fields of characteristic 0; using the geometric part wasn't essential, and can be done algebraically instead.

Notice also that characteristic 0 looks like characteristic p for p "large". Here is a method for proving things in characteristic 0: First prove the thing in characteristic p (using counting, the Weil conjectures, etc.). An example of this is the Ax–Grothendieck theorem. Another example is Mori's so-called bend and break technique.

The first order language of fields is (roughly) something where you can use

(1) Variables $x_1, x_2, \ldots$ taking values in the field.

(2) The logical symbols $\wedge, \vee, \neg, \to, =, \neq$ and so on.

(3) Operations $+, -, \cdot, /$.

(4) Quantifiers "for all x such that", "there exists x such that".

The first order language of fields is somewhat restricted, and for example we cannot do the following:

(1) We cannot say "for all integers n", so for example, how do we say that the field in question has characteristic 0? For characteristic p this is easy, since $1+1+\cdots+1=0$, but we can't say something like $\forall n > 0$, $n \neq 0$. Instead we say $1+1 \neq 0$, $1+1+1 \neq 0$, and so on, needing an infinite number of statements.

(2) We cannot say "for all subsets X of a field, ...". This is instead contained in so-called second order logic.

(3) We cannot say what the cardinality of the field is, if it is infinity.

It turns out that the Ax–Grothendieck is a countable collection of first order statements, and we can use the above method. A standard reference for this method is Chang and Keislev. The key idea of how to transfer characteristic 0 to characteristic p is the following: The theory of algebraically closed fields of some fixed characteristic is *complete*, meaning that *any* statement can be proved either true or false from the axioms. This by the way means, that there is an algorithm for finding proofs or disproofs of any statement by enumerating all sequences of symbols. It might take some time for the algorithm to terminate though.

So why is the theory complete? The key point is that the theory of algebraically closed fields in some characteristic is "uncountably categorized". That is, if you have an uncountable cardinal k, there is up to isomorhpism only one algebraically closed field of a given characteristic with this cardinality. This field is the algebraic closure of F_p(adjoin k indeterminates). For countable cardinality, we could have more fields with a given cardinality; for example $\overline{\mathbb{Q}}, \overline{\mathbb{Q}(x_1)}, \overline{\mathbb{Q}(x_1, x_2)}, \ldots$. If a field is categorized in some cardinality, it is complete – this is an easy corollary of Gödel's completeness theorem.

Suppose we have a proof of S for characteristic 0 with the axioms for characteristic 0: $2 \neq 0$, $3 \neq 0$, $5 \neq 0$, and so on. Any proof has finite length, so it uses only a finite number of the axioms $2 \neq 0$, $3 \neq 0, \ldots$. If it uses $2 \neq 0, \ldots, p \neq 0$, then all axioms are satisfied for any field of characteristic $p > 0$. So the statement is also true for all such fields. We will leave it at that.

3.4 Rational maps

We first define *rational functions* on a variety (these will be the analogue of meromorphic functions). For affine varieties it is easy: We look at the coordinate ring $\mathcal{O}(Y)$ of Y, which we can think of as polynomials on Y. $\mathcal{O}(Y)$ is an integral domain as Y is irreducible, so we take its quotient as the field of rational functions.

Example 99. Take $Y = A^1$. The coordinate ring is $\mathcal{O}(Y) = k[x]$, so the ring of rational functions is $k(x)$, consisting of elements like $(7x^2+3x+2)/(5x^9+8)$.

Note that there is no analogue of rational functions for smooth manifolds.

For projective varieties the above approach doesn't work; $\mathcal{O}(Y)$ is too small – usually it's just k. An alternative definition is the following:

Definition 100. A *rational function* is given by a regular function f on a dense open subset U of Y. Note that different rational functions can correspond to different open subsets. We say that two rational functions (f_1, U_1) and (f_2, U_2) are the same if $f_1 = f_2$ on $U_1 \cap U_2$.

For varieties V, rational functions form a field: If (f, U) is rational, $f = 0$ on a closed set, $f \neq 0$ on an open set, which is dense if $f \neq 0$ as V is irreducible, so $1/f$ is defined on a dense open set. If V is not irreducible, rational functions will not form a field though.

At this point, the lecture was interrupted by a fire alarm.

14th lecture, October 12 2010

Last time, we defined a rational function on some variety V as something represented by a regular function on some dense open set U. Recall that (f_1, U_1) and (f_2, U_2), if $f_1 = f_2$ on $U_1 \cap U_2$. We write $k(V)$ for the ring of rational functions on V. This is an integral domain, if V is irreducible. In fact, $k(V)$ is the direct limit (which we won't define) of $\mathcal{O}(U)$ with $U \subseteq V$ open and dense.

Similarly, we can define a *rational map* $f : X \to Y$ to be given by a morphism from a dense open subset of X to Y, where, as above, two such maps are considered the same, if they agree on their intersection. One thing to be a little bit careful about: The rational maps do not form the morphisms of a category, since composition is not always defined; for example the map $f : A^1 \to A^1$ taking any point x to 0 can't be composed with $x \mapsto 1/x$. What goes wrong here is that the map f is degenerate in some sense, meaning that the image is not dense. We call a rational map *dominant*, if the image of some dense open set contains a dense open set. Now, dominant rational maps form the morphisms of a category. Two varieties are called *birational*, if they are isomorphic in the category, so they have dense open subsets, that are isomorphic as varieties.

Example 101. Consider A^1, P^1, $xy = 1$ in A^2, or $x^3 = y^2$ in A^2. These are all birational. For example, the map $A^1 \to \{x^3 = y^2\}$ given by $t \mapsto (t^2, t^3)$ has an inverse $(x, y) \mapsto y/x$, defined for $(x, y) \neq (0, 0)$, so $A^1 - \{0\}$ is isomorphic to $\{x^3 = y^2\} - (0, 0)$. However, the varieties are not isomorphic, since $\{x^3 = y^2\}$ has a singularity in $(0, 0)$.

Similarly A^2, P^2, $P^1 \times P^1$, $A^2 - (0, 0)$ are all birational but not isomorphic.

Example 102. The affine line A^1 is not birational to $x^3 + y^3 = 1$ (but it is in fact birational to $x^2 + y^2 = 1$). We will show, that there is no dominant birational map from A^1 to $x^3 + y^3 = 1$. Suppose $t \mapsto (x(t), y(t))$ is a dominant birational map. Then $x(t)$,$y(t)$ are rational functions at t, not constants, such that $x(t)^3 + y(t)^3 = 1$. The question is, whether or not we can find rational functions $x(t)$, $y(t)$ satisfying this equation. Clear the denominators to get $f(t)^3 + g(t)^3 = h(t)^3$, with f, g, h non-constant polynomials. Factor the left hand side to obtain

$$(f(t) + g(t))(f(t) + \omega g(t))(f(t) + \omega^2 g(t)) = h(t)^3,$$

with $\omega^3 = 1$, $\omega \neq 1$, $\omega^2 + \omega + 1 = 0$. Polynomials in $k[t]$ form a unique factorization domain and every unit is a cube (since k is algebraically closed). We can assume that f, g, h are pairwise coprime, so all three terms on the left are cubes. So $f + g = h_0^3$, $f + \omega g = h_1^3$ and $f + \omega^2 g = h_2^3$ for some h_0, h_1, h_2. Eliminate f, g from these to get a linear relation between h_0^3, h_1^3, h_2^3. So we get a solution $ah_0^3 + bh_1^3 = ch_2^3$, for $a, b, c \in k$, and $\deg h_0, h_1, h_2 < \deg h$, so we find a solution to $x^3 + y^3 = z^3$ of smaller degree. By induction on degree, there are no nonconstant solutions.

The same proof works for $x(t)^n + y(t)^n = 1$ for $n > 2$, so we can solve Fermat's last theorem for polynomials over the rationals for all cases except polynomials of degree 0.

There is in fact a one line proof of the above with a small catch: Any map from a curve to one of higher genus is constant. E.g. from A^1 which has genus 0, and $x^3 + y^3 = 1$ has genus 1. The catch is that we didn't define genus.

Example 103. We will show that the affine line A^1 is not birational to any elliptic curves of the form $y^2 = x^3 + ax + b$ using complex analysis. Recall the Weierstrass $\wp$ function. We will use it to construct an isomorphism from a complex torus $\mathbb{C}/\Lambda$ to some curve of the form $y^2 = 4x^3 - g_2 x - g_3$. Here Λ is a lattice in $\mathbb{C}$ of all complex numbers of the form $m\omega_1 + n\omega_2$, where ω_1, ω_2 are fixed and m, n are integers. Topologically, $\mathbb{C}/\Lambda$ is just the torus $S^1 \times S^1$. Now $\wp(z)$ is an elliptic function, meaning that it's doubly periodic, $\wp(z + \omega_1) = \wp(z)$, $\wp(z + \omega_2) = \wp(z)$, so $\wp(z + \lambda) = \wp(z)$ for all $\lambda \in \Lambda$. Any holomorphic elliptic function is bounded, so it is constant by Liouville's theorem. We will try to construct a meromorphic elliptic function.

Take any function $f(z)$. Form $F(z) = \sum_{\lambda \in \Lambda} f(z + \lambda)$. This is formally doubly periodic, but the sum might not converge. For example, if $f(z) = 1/z$, $\sum \frac{1}{z+\lambda}$ diverges drastically. Try instead $f(z) = 1/z^2$ and $\wp(z) = \sum_{\lambda \in \Lambda} \frac{1}{(z+\lambda)^2}$. It doesn't quite converge. The convergence of $\sum \frac{1}{(z+\lambda)^2}$ is like the convergence of $\sum_{n \geq 1} \frac{c \cdot N}{k \cdot N^2} = \frac{c}{k} \sum_{n \geq 1} \frac{1}{n}$, which almost converges. In the case with $\wp$, we

make it converge by "renormalizing" it by subtracting an "infinite" constant: define

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Now, it is not obvious that $\wp(z)$ is invariant under $z \mapsto z + \lambda$. This is easy to fix though, and is done in any complex analysis book.

In summary, the function $\wp$ is doubly periodic, and we will find its poles. The only singularities are at $z = \lambda$ for $\lambda \in \Lambda$. Since it is periodic, we only need to know what the singularity at 0 looks like: We have $\wp = z^{-2} + O(z^2)$. Now, notice that $\wp'(z) = -2z^{-3} + O(z)$, so

$$(\wp'(z))^2 = 4z^{-6} + *z^{-2} + * + \cdots,$$
$$4(\wp(z))^3 = 4z^{-6} + *z^{-2} + \cdots,$$

where $*$ means some constant. Thus $\wp'(z)^2 - 4\wp(z)^3 = *z^{-2} + *$, so $\wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) = O(1)$ at $z = 0$, and the left hand side is doubly periodic and holomorphic, so it is a constant g_3. We have thus found a differential equation

$$\wp'(z)^2 = 4\wp(z)^3 + g_2\wp(z) - g_3.$$

This is the same form as $y^2 = 4x^3 + g_2 x - g_3$, which is some affine curve in the plane. So we get a map from $\mathbb{C}/\Lambda$ to the projective curve, by mapping $z \mapsto (\wp(z), \wp'(z)) = (x, y)$. and $\lambda \in \Lambda$ maps to (∞, ∞). We thus get an isomorphism from $\mathbb{C}/\Lambda$ to the curve $y^2 z + 4x^3 + g_2 x z^2 - g_3 z^3$. Note that this isomorphism is not algebraic; it cannot be described in terms of polynomials and so on. Note also that $y^2 = 4x^3 - g_2 x - g_3$ is not birational to A^1, because it is the torus $S^1 \times S^1$ (minus a finite number of points), while A^1 looks like a sphere minus a finite number of points. Such things are never homeomorphic.

Trying to integrate the equation $\wp'(z)^2 = 4\wp(z)^3 + g_2\wp(z) - g_3$, we find

$$\frac{d\wp}{dz} = \sqrt{4\wp^3 - g_2\wp - g_3},$$
$$\int_a^{\wp} \frac{d\wp}{\sqrt{4\wp^3 - g_2\wp - g_3}} = \int dz = z + \text{const}.$$

This integral comes from finding the arc length of an ellipse, which is given by $\int_0^\theta \frac{dt}{\sqrt{t^3+at+b}}$. Thus $\wp$ is the inverse of the elliptic integral, hence the name "elliptic curve".

Example 104. We will show that cubic surfaces are rational (meaning birational to A^n) and mostly have 27 lines in them. Warning: The argument is very sketchy and resembles algebraic geometry as it was done in the first part of the 20th century.

A cubic surface is something of the form $w^3+x^3+y^3+z^3 = 0$ in P^3 – that is, something defined by a cubic polynomial. Take 6 points $P_1, \ldots, P_6$ in A^2 (or P^2) in general position, meaning that the author is too lazy to say exactly what he means – in this case it means no 3 points on a line and no 6 on a conic. The space of all cubics $a_{300}x^3 + a_{210}x^2y + \cdots + a_{003}z^3$ is 10-dimensional. The space of cubics vanishing on $P_1, \ldots, P_6$ has dimension $10 - 6 = 4$ (usually). Take a basis f_1, f_2, f_3, f_4 of the cubics vanishing on $P_1, \ldots, P_6$. Now map $(x, y) \mapsto (f_1(x, y), f_2(x, y), f_3(x, y), f_4(x, y)) \in P^3$. The image is some hypersurface. To find the degree of the hypersurface (i.e., informally the number of intersections with a "generic" line). Say $f_1 = f_2 = 0$, then f_1, f_2, which are of degree 0, have $3 \cdot 3 = 9$ points of intersection; 6 points are $P_1, \ldots, P_6$. The images of the other 3 points are the intersection of the hypersurface with the line $(0, 0, *, *) \in P^3$, so the degree of the image of A^2 is a degree 3 hypersurface. So, 6 general points in P^2 gives a cubic hypersurface in P^3. Look at the dimensions of "moduli spaces" of both sides. The space of cubic surfaces has dimensional $20 - 1 = 19$ (since there are 20 possible coefficients in $\sum a_{ijkl}x^i y^j z^k w^l = 0$), and is isomorphic to P^{19}. P^3 has automorphism group $PGL_4(\mathbb{C})$, which has dimension $4 \cdot 4 - 1 = 15$. So we really only have a space of dimension $19 - 15 = 4$ of cubic surfaces up to isomorphism. For the 6 points in P^2,

the dimension is $2 \cdot 6 = 12$, and the automorphism group of P^2 is $PGL_3(\mathbb{C})$, which has dimension 8. So now the dimension of the space of isomorphism classes of 6 points in P^2 has dimension $2 \cdot 6 - 8 = 4$. "So" this makes it plausible that every cubic surface is birational to P^2.

Now to the 27 lines: To construct the lines, suppose that the cubic surface is obtained as above by picking 6 points $P_1, \ldots, P_6$, then 27 points can be obtained as follows:

(1) 6 lines come from "blowing up" (which we will define next lecture) 6 points.

(2) 15 lines are images of P_i, P_j.

(3) 6 lines are the image of the conic through 5 of 6 points.

Example 105. Here's an example of what happens in higher dimension. Consider a cubic 3-fold, such as $v^3 + w^3 + x^3 + y^3 + z^3 = 0$ in P^4. These are unirational: There is a a finite to 1-map from P^n to a cubic 3-fold. Griffiths and Clemens showed in 1974, that this is not rational. Castelnuovo showed that unirational surfaces are rational.

15th lecture, October 14th 2010

3.5 Blow-ups

Today, we will consider giving examples of birational maps given by "blowing up". The idea is to replace a point of A^n by a copy of P^{n-1}. The blow up the point $(0, 0, \ldots) \in A^n$ is given by points $(x_1, \ldots, x_n) \times (y_1 : \cdots : y_n) \in A^n \times P^{n-1}$ such that $x_i y_j = x_j y_i$ for all i, j. Denote the set of these by Z. There is an obvious projection $Z \to A^n$. What is the inverse image of a point $(x_1, \ldots, x_n) \in A^n$? If $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$, there is just one point in Z mapping to it. If on the other hand $(x_1, \ldots, x_n) = (0, \ldots)$, the inverse is the whole of P^{n-1}, so $(0, \ldots, 0) \in A^n$ has been replaced by a copy of P^{n-1}. P^{n-1} is covered by affine spaces $y_1 \neq 0$. We may as well put $y_i = 1$, and on this , the blow-up is given by $x_j = y_j x_i$, so we get new coordinates $y_1, \ldots, y_{i-1}, x_i, \ldots, y_n$. So we have replaced x_j by $y_j x_i$.

Example 106. Consider $C = (x_2^2 = x_1^3)$ in A^2. We will blow up A^2 at $(0, 0)$ and look at the image inverse of C in the blow-up – see the picture in the blow-up section of [Har]. The blow-up Z is covered by 2 copies of A^2, $y_1 = 1$ or $y_2 = 1$. On one A^2 we put $x_2 = y_2 x_1$, and on the other $x_1 = y_1 x_2$.

Considering the first one, we get $(y_2 x_1)^2 = x_1^3$. So the inverse image of C is $x_1^2(y_2^2 - x_1) = 0$, and has two components $x_1 = 0$ (the line P^1 mapping to 0), and $y_2^2 = x_1$ (which is a parabola). What is interesting is that the curve C behaves badly at the origin: The inverse image is the union of a line and a parabola; now the parabola is smooth everywhere, so blowing up at 0 has resolved the singularityu of C.

Let's look at the other chart $x_1 = y_1 x_2$. Here we get $x_2^2 = x_1^3 = (y_1^3 x_2^3)$, so $x_2^2(1 - y_1^3 x_2) = 0$, which again gives a P^1 and a nonsingular curve.

Example 107. Consider $x^2 + y^2 = z^2$ in A^3. This has a conical singularity at the origin. We will blow up A^3 at $(0, 0, 0)$, and look at the inverse image. So replace $(0, 0, 0)$ by a copy of P^2 covered by 3 copies of A^2 as before:

(1) Put $x = zs$, $y = zt$.

(2) Put $y = zt$, $z = xt$.

(3) Put $x = ys$, $z = yt$.

Consider the first one. We get $(zs)^2 + (zt)^2 = z^2$, so $z^2(1 - s^2 - t^2) = 0$. The $z^2 = 0$ gives a copy of P^2 above $(0, 0, 0)$, and $1 - s^2 - t^2 = 0$, which is a smooth cylinder.

For the second one, we get $x^2 + (xs)^2 = (xt)^2$, so $x^2(1 + s^2 - t^2) = 0$, so the x^2 is the P^2 as before, and $1 + s^2 - t^2 = 0$ gives a hyperbola (times the x-axis), which again is smooth.

The last case is identical.

Example 108. Here is an example, where blowing up does not get rid of the singularity. Take $y^8 = x^5$, which is singular at $(0,0)$, and we try to blow it up. As before there are 2 cases to do: $y = xt$ and $x = yt$. On the first chart, $(xt)^8 = x^5$, which gives $x^5(x^3t^8 - 1) = 0$. This gives an $x^5 = 0$, which is P^1 as before, and a $x^3t^8 = 1$, which is actually a smooth curve as before. On the other chart, $y^8 = (yt)^5$, or $y^5(y^3 - t^5) = 0$. This gives a P^1 for the $y^5 = 0$ and a $y^3 = t^5$, which is still singular – however the singularity is "better" than the one we began with, as the exponents have gone down. So we blow it up again getting $y = st$, and $t = sy$. The first one gives a $t^2(s^3 - t^2)$, which is still singular, and the second one a $y^3(1 - s^5y^2) = 0$, which is non-singular. Blowing it up once more, we get rid of the singularity: Blowing up A^2 3 times gives a variety Z such that the inverse image of $y^8 = x^5$ is a union of a non-singular curve and 3 copies of P^1 (note that the inverse image is singular, as the 4 curves intersect).

Example 109. Consider the Whitney umbrella (or pinch point) given by $xy^2 = z^2$.[5] This has a singularity at $(0,0,0)$ and along the axis $y = z = 0$. Instead of blowing up at $(0,0,0)$, we blow up along $y = z = 0$. This means that we take the subset of points $(x,y,z) \times (s:t)$, such that $yt = zs$. The inverse image of (x,y,z) looks as follows: If $(y,z) \neq (0,0)$ the inverse image is a point. If $(y,z) = (0,0)$, the inverse image is a P^1. So we have replaced every point of the x-axis by a copy of P^1.

We cover P^1 by 2 copies of A^1, $s = 1$ or $t = 1$. For $s = 1$, we get $z = yt$, and the Whitney umbrella becomes $xy^2 = z^2$ becomes $xy^2 = y^2t^2$ or $y^2(x - t^2) = 0$, so $y = 0$ gives a P^1 times the x-axis, and $x = t^2$ gives a parabola times the y-axis, which is nonsingular. For $t = 1$, we get $y = zs$, and $xy^2 = z^2$ becomes $x(zs)^2 = z^2$, so $z^2 = 0$ or $xs^2 = 1$, and again the last one is nonsingular.

So, blowing up the x-axis resolves the singularity.

A natural idea is to repeatedly blow-up along the "worst" singularities to resolve a singularity. This does not work naively for the Whitney umbrella: In this case, the origin is the worst singularity, but if we blow up at $(0,0,0)$, the following happens. As before, there are three possibilities. First off, $y = sx, z = tx$, secondly $x = sy, z = ty$, and lastly $x = sz, y = tz$. In each of them we blow up by 3 coordinate charts. We obtain $x(sx)^2 = (tx)^2$, $syy^2 = (ty)^2$, and $sz(tz)^2 = z^2$ respectively. These give $x^2(s^2x - t^2) = 0$, $sy^2 = t^2$, and $szt^2 = 1$. While the last two give nonsingular curves, the first one doesn't, and the singularity is exactly the one we started with.

Example 110. We want to blow up the *real* affine plane at $(0,0)$ and see what surface we get. The set of lines through 0 is $P^1(\mathbb{R})$, which is S^1. The blow-up is $\mathbb{R} \times P^1(\mathbb{R})$ with coordinates $(x,y) \times (s:t)$, $xt = sy$. Consider the projection to S^1. The inverse image of $(s:t)$ is a line $xt = sy$, so the blow-up is a line bundle over S^1. Examples of such are the cylinder or the Möbius bundle. In fact in our case we get the last one (which is left as an exercise in geometrical intuition).

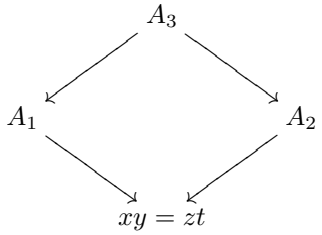
There are also more general versions of blow-ups: We can blow up a point in *any* variety, and we can blow up any subvariety of any other variety. More generally we can blow up any sheaf of ideals over any scheme, or we can blow up any sheaf of graded algebras over any scheme.

Roughly, blowing up a point corresponds to replacing the point by a copy of the projective space of its tangent space. Blowing up a subvariety corresponds to replacing each point of a subvariety by the projective space of its normal space. For the last one, given a graded algebra at each point, remember that a graded algebra corresponds to a projective variety, and we replace each point by a projective variety.

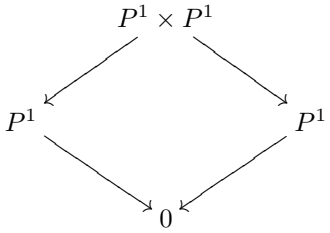
Example 111. Now we will discuss the *Atiyah flop* introduced by Atiyah in 1958. The name was introduced by Miles Reid. The flop is a special sort of birational map, of which nontrivial examples only exist in dimension greater than or equal to 3.

Consider the 3-dimensional variety $xy = zt$ in A^4. It's singular at the origin (see next week) and non-singular everywhere else. We blow up $(0,0,0,0)$ to eliminate the singular point. Consider therefore $(x,y,z,t) \times (X:Y:Z:T)$ with relations $xY = yX$ etc. We consider the inverse image of $xy = zt$ intersected with P^3, which is just $XY = ZT$ in P^3. This is a non-singular quadric in P^3 isomorhpic to $P^1 \times P^1$. There are two ways to project this to P^1. We can collapse to P^1 in two ways:

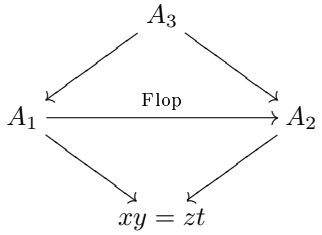
[5] See `http://en.wikipedia.org/wiki/Whitney_umbrella` for a picture – that's better than I'd be able to do it.



with the inverse image of 0 being as follows:



Blowing up along the line $y = t = 0$, we cover by 2 coordinate charts. A typical one for $xy = zt$ is $xZ = zX$, $tZ = yX$. Considering $(x, y, z, t) \times (X : Z)$ with $X = 1$ we get $z = xZ$, $y = tZ$, so $xtZ = xZt$. This is just affine 3-space. which is nonsingular. So the point is that both the A_1 and the A_2 in the above diagram are nonsingular. We introduce a birational map called the Atiyah flop:



We can think of it as cutting out one copy of P^1 and gluing it back in another way. This causes problems: We would like to find a canonical minimal resolution of a singular variety V. That is, we would like to find $X \to V$ with X nonsingular such that X is as small as possible. This is possible in dimensions 1 and 2, but the Atiyah flop shows that it is impossible in dimension 3. Both A_1 and A_2 are resolutions that are "minimal" neither factors through the other by a regular map. The flop is only a birational map (and any two resolutions will be birational). In other words, there is no canonical minimal resolution in dimension greater than or equal to three that all others factor through. One solution to his is to allow "mild" singularities: The idea is to find a canonical minimal variety $X \to V$ such that X only has very mild (so-called terminal) singularities. Another solution is to try to show that all minimal resolutions are related by "flops".

16th lecture, October 19th 2010

4 Singular points

In today's lecture, we will start on section 5 of [Har], which is about singular varieties. So, what is a singular point of a variety? It is sort of obvious, when you see it. For example for $y^2 = x^3$, there is something going on at the origin, and for $xy = 0$, there is something going on at the origin as well.

We describe singular points in terms of tangent spaces of varieties.

Definition 112. The *tangent space* at a point p of V is defined by the vanishing of *linear* parts of the equations defining V near p. Take $(0, 0, \dots)$ by linear change of variables $x_i \to x_i + a_i$.

Consider for example $y^2 = x^3$. The linear part is 0 at $(0,0)$, so the tangent space is all of k^2. If for example $y = x^2$, the linear part is $y = 0$.

Definition 113. A point is called *singular* if its tanget space has the wrong dimension; in other words, its dimension is greater than the dimension of V.

Example 114. If V is a hypersurface $f(x_1, \ldots, x_n) = 0$ of dimension $n-1$, the singular points are where $f = 0$, $\frac{\partial f}{\partial x_i} = 0$ for all i.

Proposition 115. *The set of singular points is* closed.

Proof. To see this, suppose that V is given by $f_1 = f_2 = \cdots = f_m = 0$. Then the dimension of the tangent space is given in terms of the rank of the matrix $\left(\frac{\partial f_i}{\partial x_j}\right)$. So the dimension of the tangent space being bigger than the dimension of V corresponds to the rank of this matrix being less than or equal to something. The condition that the rank is less than or equal to something is just the condition for a determinantal variety, which is closed as in an early lecture. □

Proposition 116. *The set of non-singular points in a variety is* non-empty.

There appears to be a counter-example to this: Look at the Fermat curve $x^3 + y^3 = 1$. The singular points are given by $x^3 + y^3 = 1$, $3x^2 = 0$, and $3y^2 = 0$. No points (x, y) satisfy this if $\operatorname{char} k \neq 3$. If $\operatorname{char} k = 3$, we see that all points are singular. This seems to be a counter-example to the fact, that not all points are singular. What goes wrong is that in $\operatorname{char} k = 3$, we have $(1 - x^3 - y^3) = (1 - x - y)^3$, so the equation did not define a reduced ideal. (In terms of schemes, in $\operatorname{char} k = 3$, the scheme $x^3 + y^3 = 1$ has no nonsingular points.)

Proof. Let us prove the proposition for varieties. First, we can reduce to the case of hypersurfaces, as every variety is birational to a hypersurface. Suppose the variety is $f(x_1, \ldots, x_n) = 0$. If all points are singular, then $\frac{\partial f}{\partial x_i} = 0$, whenever $f = 0$. So, as f is irreducible, we have $f \mid \frac{\partial f}{\partial x_i}$, but $\deg f > \deg \frac{\partial f}{\partial x_i}$, so $\frac{\partial f}{\partial x_i} = 0$ on all of A^n. If all derivatives of f vanish, this does not imply that f is constant; the usual counter-example for $\operatorname{char} k = p$ is $f = x_1^p + x_2^p$. However, if all derivatives vanish, then f is a polynomial in $x_1^p, x_2^p, \ldots$, where $\operatorname{char} k = p$, so $f = g(x_1^p, x_2^p, \ldots) = g(x_1, x_2, \ldots)^p$, so f is not irreducible. □

So non-singular points form an open non-empty set, so they are *dense* in any variety. Over $\mathbb{R}$ and $\mathbb{C}$, varieties correspond to smooth manifolds at non-singular points. This follows from the inverse function theorem. The converse isn't quite true though: The curve $y^2 = x^3$ is still a topological manifold at the singular point.

There is a problem with the definition of singular points: It seems to depend on the embedding of the variety into affine space A^n. If $f : V_1 \to V_2$ is an isomorphism, does it take singular points of V_1 to singular points V_2? This is by no means obvious, and we will find a better definition, that of a Zariski tangent space to a variety at a point, that is in some sense more "intrinsic", meaning that it does not depend on the embedding, and which also works for all schemes.

Definition 117. The *Zariski tangent space* of a variety V at a point p is $(m/m^2)^*$ where m is the maximal ideal of the local ring at p.

Recall that the local ring at a point is roughly functions defined "near" the point p. For example, the local ring of A^1 at 0 is equal to the set of all rational functions $f(x)/g(x)$, with $g(0) \neq 0$; these are regular functions in some neighborhood of 0. A slightly more formal definition is the following: The local ring is given by the direct limit of all open neighborhoods U of p of all regular functions on U.

Let us check that the above definition corresponds with the previous definition of a tangent space. We can assume that p is the point $(0, 0, \ldots, 0)$ in A^n. The local ring is the ring of all rational functions f/g, $g(0) \neq 0$, quotient the ideal of functions vanishing on V. The maximal ideal m of the local ring of functions vanishing at 0 is generated by $x_1, \ldots, x_n$, and m^2 are generated by degree 2 monomials $x_i x_j$. So the Zariski cotangent space m/m^2 is given by $(x_1, \ldots, x_n)/((x_i x_j), f_k)$, where

V is given by $f_1, \ldots, f_k = 0$. This is equal to a vector space spanned by $x_1, \ldots, x_n$ modulo relations given by the linear parts of $f_1, \ldots, f_n$. This is equal to the dual of k^n on which the linear parts of $f_1, f_2, \ldots$ vanish, which is the previous definition of tangent space.

There are several other ways to look at the tangent space. For smooth manifolds, the tangent space is sometimes defined as equivalence classes of "short smooth curves" at a point – see Fig. 20. There is an analogue of this in algebraic geometry: The analogue of a short smooth curve is the scheme with coordinate ring $k[\varepsilon]/\varepsilon^2$, whose elements are of the form a point together with another point "infinitely close". A map from this "short smooth curve" to a variety V with coordinate ring R corresponds to homomorphisms of rings $R \to k[\varepsilon]/\varepsilon^2$. Let us find homomorphisms over the point $(0, \ldots, 0)$. If $R = k[x_1, \ldots, x_n]/I$, a homomorphism f should map x_i to some element of $k[\varepsilon]$ with constant term 0, so $x_i \mapsto a_i\varepsilon$, $a_i \in k$. The linear parts of the generators of I map to 0. So, the homomorphisms $R \to k[\varepsilon]/\varepsilon^2$ over $R \to k$ corresponds to the tangent space.

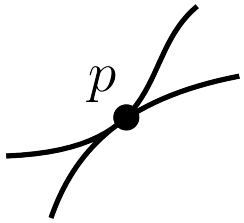


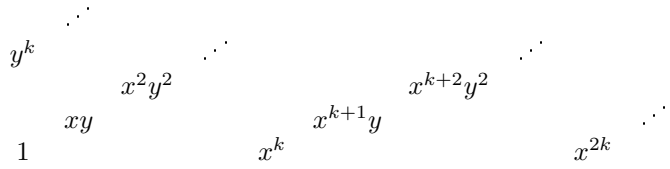
Figure 20: Two curves going through the point p – these are considered equal, since they are equal in the vicinity of p – they have the same tangent.

There is a third way to define the tangent space. We consider first what is happening on manifolds. Let M be a smooth manifold. It has two vector bundles over it, given by tangents and cotangents. Vector fields form a module over the ring of smooth functions, given by multiplying the vector field in each point by the value of the function in that point – so do cotangent vector fields. There is a linear map d from smooth functions to 1-forms (which are cotangent vector fields). In local coordinates, this maps $f \mapsto \frac{\partial f}{\partial x_1}dx_1 + \frac{\partial f}{\partial x_2}dx_2$, satisfying $d(fg) = f(dg) + (df)g$. We can define the module of 1-forms as a "universal" module M over smooth functions S, with a map $d : S \to M$ satisfying the relations above (the linearity and the Leibniz rule).

Example 118. Take $S = k[x_1, \ldots, x_n]$ (an approximation to smooth functions on $\mathbb{R}^n$). The module M is generated by elements df (with f a polynomial) with relations as above. We notice that $d1 = 0$, and $d(fg)$ is in the module generated by df and dg, so M is generated by $dx_1, \ldots, dx_n$. In fact, M is the free module with basis $dx_1, \ldots, dx_n$, because we can define a map d form S to this free module by putting $df = \sum \frac{\partial f}{\partial x_i}dx_i$ and check that it satisfies the relations above.

So, from a module A of cotangent vector fields M, we can construct the module of tangent vector fields as the "dual" $\mathrm{Hom}_S(M, S)$, and we can get tangent and cotangent spaces at a point from these modules, by (say) localizing and taking a quotient by a maximal ideal. The nice thing about this construction is that it works for arbitrarity schemes: It gives a sheaf of contangent or tangent vectors for any scheme.

Example 119. We will now examine the singularity $x^2 + y^3 + z^5 = 0$. Here's the background of this singularity: It is one of the du Val singularities, also called Kleinian singularities, rational double points, simple surface singularities, 2-dimensional canonical singularities, their importance being illustrated by the number of different names they have. These are quotients of $\mathbb{C}^2$ by a finite subgroup G of $SL_2(\mathbb{C})$. For example, the group could be $G = \mathbb{Z}/k\mathbb{Z}$ acting as $(x, y) \mapsto (\zeta x, \zeta^{-1}y)$, where $\zeta = e^{2\pi i/k}$. The coordinate ring is going to be functions in $\mathbb{C}[x, y]$, invariant under the group G. If $G = \mathbb{Z}/k\mathbb{Z}$ as above, $g(x^m y^n) = \zeta^{m-n}x^m y^n$, so the coordinate ring has a basis consiting of elements $x^m y^n$ with $k \mid (m-n)$. From the following diagram it is clear that the ring has generators $X = x^k$, $Y = y^k$ and $Z = xy$, with the relation $Z^k = XY$, which is called a du Val singularity of type A_{k-1}.



There is a complete list of finite subgroups of $PSL_2(\mathbb{C})$; namely the following, listed together with their generators:

- cyclic A_n, $X^2 + Y^2 + Z^{n+1} = 0$,
- dihedral D_n, $X^2 + ZY^2 + Z^{n-1} = 0$,
- tetrahedral E_6, $X^2 + Y^3 + Z^4 = 0$,
- octahedral E_7, $X^2 + Y^3 + YZ^3 = 0$,
- icosahedral E_8, $X^2 + Y^3 + Z^5$.

We look at the stucture of $x^2+y^3+z^5 = 0$, and we wish to find a *resolution* of this (for $\operatorname{char} k = 0$), and we do this by blowing up at the singular points. Differentiating with respect to x, y, and z we see that the only singular point is $(x, y, z) = (0, 0, 0)$. Blowing up, we now look at $x, y, z, (x_1 : y_1 : z_1) \in \mathbb{C}^3 \times P^2$ with relations $xy_1 = yx_1$ etc. We cover P^2 by three copies of A^2 given by $x_1 = 1$, $y_1 = 1$, or $z_1 = 1$.

For $x_1 = 1$, $yx_1 = xy_1$, so $y = xy_1$ and similarly $z = xz_1$, so we get $x^2 + (xy_1)^3 + (xz_1)^5 = 0$, which can be written as $x^2(1 + xy_1^3 + x^3z_1^5) = 0$. The x^2 is just the P^2, not giving rise to new singular points. The singular points of the bracketed term can be found as before and it turns out there are none.

For $y_1 = 1$, we put $x = x_1y$, $z = z_1y$, and we get $(x_1y)^2+y^3+(z_1y)^5 = 0$, and $x_1^2+y+z_1^5y^3 = 0$ has singularities if $2x_1 = 0$, $1 + z_1^5 3y^2 = 0$, and $5z_1^4y^3 = 0$, which again has no solutions.

For $z_1 = 1$, things get more interesting. Here, $x = x_1z$, $y = y_1z$, and we get $(x_1z)^2+(y_1z)^3+z^5 = 0$, and dividing by z^2, we get $x_1^2 + y_1^3z + z^3 = 0$. This has the singularity $x_1 = y_1 = z = 0$. We might hope that this new singularity of $x_1^2 + y_1^3z + z^3 = 0$ is better than the one we started with, and we can try to resolve it by blowing up again. As before we introduce new coordinates for another P^2, denoted $(x_2 : y_2 : z_2)$. Again we cover P^2 by $\{x_2 = 1\}$, $\{y_2 = 1\}$, and $\{z_2 = 1\}$. For $x_2 = 1, z_2 = 1$, everything is non-singular once again. For $y_2 = 1$, $x_1 = x_2y$, $z = z_2y_1$, and we get $x_2^2y_1^2 + y_1^4z_2 + y_1^3z_2^3 = 0$ (up to possible mistakes in indices and powers). Dividing by y_1^2, we get $x_2^2 + y_1^2z_2 + y_1z_2^3 = 0$, which is again singular at $(0, 0, 0)$. Comparing with the equation from before, we seem to have seen no improvement here, and we once again have a sum of monomials with terms of degree 2, 3, and 4. We continue considering this example next time.

17th lecture, October 21st 2010

We continue considering the E_8 duVal singularity $x^2 + y^3 + z^5 = 0$. Last time we blew it up at $(0, 0, 0)$ getting $x_1^2 + y_1^3z + z^3 = 0$, which also has a singularity at $(0, 0, 0)$. Blowing it up again, we get $x_2^2 + y_1^2z_2 + y_1z_2^3 = 0$, which does not seem to improve the singularity. Both are sums of monomials with degrees 2, 3, 4.

This illustrates two points: Firstly, blow-ups may only improve singularities very slightly. Secondly, it is difficult to measure the "badness" of a singularity.

Let us blow it up again, and introduce coordinates $(x_3 : y_3 : z_3)$ on a new P^2. We have 3 open covers on P^2 to consider, given by $x_3 = 1$, $y_3 = 1$, $z_3 = 1$. The case $x_3 = 1$ turns out to be non-singular (exercise). For $y_3 = 1$, we have $x_2^2 + y_1^2z_2 + y_1z_2^3 = 0$ and put $x_2 = y_1x_3$, $z_2 = y_1z_3$, so we get $x_3^2y_1^2 + y_1^2y_1z_3 + y_1y_1^3z_3^3 = 0$, and dividing by y_1^2 we get $x_3^2 + y_1z_3 + y_1^2z_3^3 = 0$ with the

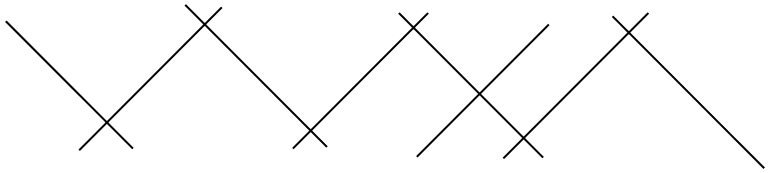


Figure 21: The 8 copies of P^1 and how they intersect.

singular point $x_3 = y_1 = z_3 = 0$. For $z_3 = 1$, there is only one singular point $x_3 = y_3 = z_2 = 0$. Note that neither of the singular points are in both $y_3 = 1$ and $z_3 = 1$.

If we first look at $x_3^2 + y_1 z_3 + y_1^2 z_3^2 = 0$ (it seems we lost a power of z_3 here, but oh well ...) and blow up at $(x_3 : y_3 : z_3) = (0 : 1 : 0)$, we completely resolve the singularities by blowing up. If we look at $x_3^2 + y_3^2 z_2 + y_3 z_2^2 = 0$. Introducing $(x_5 : y_5 : z_5)$ we now get no singularities at $x_5 = 1$, for $y_5 = 1$ we get two singularities, at $x_5 = 0, y_3 = 0$, and $z_5 = 0$ or -1. For $z_5 = 1$, we have singularities at $x_5 = 0$, $z_2 = 0$, $y_5 = 0$, and -1. Note that two of the singularities are the same, so now we have 3 singularities to deal with. Fortunately, each of these can be resolved by blowing up.

In summary, we needed 8 blow-ups to resolve the singularities, and we needed 27 variables, illustrating how messy calculations become.

The above example was particularly simple, as all singular sets had dimension 0.

Singularities of the form $x_1^{a_1} + x_2^{a_2} + \cdots + x_n^{a_n} = 0$ turns out to be related to exotic spheres. If we take the intersection of this with a small sphere around the origin, $|x_1|^2 + \cdots + |x_n|^2 = \varepsilon$, a *real* sphere of dimension $2n - 1$. The intersection has real dimension $2n - 3$.

Example 120. If we take $x^2 + y^3 + z^5 = 0$ with $|x|^2 + |y|^2 + |z|^2 = \varepsilon$. This gives the Poincaré 3-sphere, which has H_1 trivial and π_1 of order 120.

Example 121. Milnor's examples of 7-spheres: Consider $v^2 + w^2 + x^2 + y^3 + z^{5+6k} = 0$ and $|v|^2 + |w|^2 + |x|^2 + |y|^2 + |z|^2 = \varepsilon$. For $k = 1, \ldots, 28$ this gives 28 different smooth manifolds, all homeomorphic to S^7.

The resolution of the variety is closely related to the smooth manifolds you get. We resolve the surface S given by $x^2 + y^3 + z^5$ by blowing up 8 times. Each blow-up adds a copy of P^1 to the inverse image of S. So the inverse image of the singular point is a union of 8 copies of P^1. These intersect like in Fig. 21, where every line represents a P^1. We can dualize this by replacing each line by a point and join 2 lines if the P^1 intersect. Doing this we get the Dynkin diagram of E_8. This is related to the Poincaré 3-sphere, which can be constructed by "plumbing" according to the E_8 diagram.

Example 122. Consider the curve $x^4+y^4 = z^2$ (which was used by Fermat to show that $x^4+y^4 = z^4$ has no solutions in integers greater than 0. His idea was that any solution to $x^4 + y^4 = z^2$ gives a smaller solution of $a^4+b^4 = 4c^2$ (writing the first one as $(x^2)^2+(y^2)^2 = z^2$ and using a result from the beginning of the course), and any solution of this gives a smaller solution of $x^4 + y^4 = z^2$). The only singularity of $x^4 + y^4 = z^2$ is at $(0, 0, 0)$. We blow up by introducing coordinates $(x_1 : y_1 : z_1) \in P^2$. As always, there are 3 cases to look at: $z_1 = 1$ becomes non-singular (exercise). For $y_1 = 1$ put $x = x_1 y$, $z = z_1 y$. We get $(x_1 y)^4 + y^4 = (z_1 y)^2$, so $x_1^4 y^2 + y^2 = z_1^2$, which has singularities at $y = z_1 = 0$. The key point of this is example is, that the singular set of the blow-up is now the line $y = z_1 = 0$ of dimension 1. So blowing up a singular point can produce a singular line.

Example 123. Why do people care about resolving singularities? We give an application: Suppose we have a polynomial $f(x_1, \ldots, x_n)$ of several variables, and assume (for simplicity) that $f \geq 0$. Look at f^s for s complex. The question is: Can we continue this as a distribution for all complex s? In other words, look at

$$P(s) = \int g(x_1, \ldots, x_n) f(x_1, \ldots, x_n)^s dx_1 \ldots dx_n,$$

where g is some rapidly decreasing test function. This function is well-defined for $\mathrm{Re}(s) \geq 0$. One example of this is the function $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$. We know that $\Gamma(s)$ has poles at $s = 0, -1, -2, \ldots$ and is holomorphic elsewhere. So in general, we cannot expect P to be holomorphic, but we can ask to continue it as a meromorphic function of s. The problem is the set where $f = 0$.

Suppose $f(x_1, \ldots, x_n) = x_1 \cdots x_n$. This f corresponds to a normal crossing singularity with hyperplanes meeting transversly. This case is easy to do, since $\int g(x_1, \ldots, x_n) x_1^s \cdots x_n dx_1 \ldots dx_n$ can more or less be split into 1-dimensional integrals of the form $\int g(x_i) x_i^s dx$ which can be solved by integration by parts. Doing this we pick up poles, and by repeated use of integration by parts, the function can be continued with poles at $s = -1, -2, \ldots$.

Atiyah did the following: Suppose f has complicated singularities, and assume that we have a resolution of the singularities, lifting f to g. By a theorem by Hironaka, we can find such a resolution, and this can be done so that the map $V \to \mathbb{R}^n$ is proper (meaning that the inverse image of a compact set under the map is compact), and so that the inverse image of $f = 0$ has normal crossing singularities. As the map $V \to \mathbb{R}^n$ is proper, we can "push forward" g^s to f^s by "integrating over fibers".

In fact, Bernstein found an "elementary" proof that f^s can be continued, and in this sense the theorem by Hironaka is rather overkill.

Example 124. Another example is the Malgrange–Ehrenpreis theorem: Every differential equation with constant coefficients has a fundamental solution. The (extremely sketchy) proof goes as following: Suppose $P(D_1, \ldots, D_n)$ is a differential operator $D_i = \frac{\partial}{\partial x_i}$. For example the Laplacian $\frac{\partial^2}{\partial x_1^2} 0 \cdots + \frac{\partial^2}{\partial x_n^2}$. Suppose we have a distribution f such that $Pf = \delta$, the Dirac δ function. Taking the Fourier transform we get $P(x_1, \ldots, x_n)\tilde{f} = 1, \tilde{} = 1/P(x_1, \ldots, x_n)$. The problem is that P might have zeroes. The solution is to look at $P(x_1, \ldots, x_n)^s$ (s complex), and we can use resolution of singlarities.

Example 125. Look at the scheme with coordinate ring $\mathbb{Z}[\sqrt{-3}]$ of all numbers of the form $a+b\sqrt{-3}$. So, pretend that this is a coordinate ring of an algebraic variety. For example, points of this corresponds to maximal ideals. Consider the non-principal prime ideal $(2, \sqrt{-3} - 1)$. We want to show that it is a singular point of the scheme $\mathrm{Spec}(\mathbb{Z}[\sqrt{-3}])$. Look at the local ring of this point. We take $\mathbb{Z}[\sqrt{-3}]$, and invert anything not in the ideal $(2, \sqrt{-1} + 1)$; we think of it as "things not vanishing at the point".

So we get a local ring with maximal ideal m generated by $(2, -\sqrt{-3} + 1)$. Look at m/m^2, the Zariski cotangent space. Here m^2 is generated by $(2^2, 2(\sqrt{-3}+1), (\sqrt{3}+1)^2) = (4, 2\sqrt{-3}+2)$. Then R/m is a ring of order 2 (which is the field F_2). Look at R/m^2. this maps onto $\mathbb{Z}/4\mathbb{Z}[\sqrt{3}]/(2\sqrt{3}-2)$ which has order 8. So R/m^2 has order at least 8, and m/m^2 has order at least 4. In fact it is exactly 4. It thus has dimension 2 over $R/m = F_2$, so the Zariski tangent space has dimension at least 2. But the ring $\mathbb{Z}[\sqrt{-3}]$ has dimension 1, since all non-zero primes are maximal, so the dimension of the Zariski tangent space has dimension greater that the dimension of the ring, so the point is singular. This is related to the fact $\mathbb{Z}[\sqrt{-3}]$ does not have unique factorization.

Let us try to resolve the singularity. A resolution of a singularity in V would be a map $W \to V$, giving rise to a map $\mathcal{O}(V) \to \mathcal{O}(W)$. In our case we want to map $\mathbb{Z}[\sqrt{-3}]$ to something. This something turns out to be the integral closure (also called the normalization) of $\mathbb{Z}[\sqrt{-3}]$ in the quotient field. This is the ring $\mathbb{Z}[(\frac{-3}{+}1)/2]$. The points of this are called the Eisenstein integers, and they form a unique factorization domain. So the $\mathrm{Spec}\, Z[\sqrt{-3}] \longleftarrow \mathrm{Spec}\, Z[(\sqrt{-3}+1)/2]$ is a resolution of singularities.

18th lecture, October 26 2010

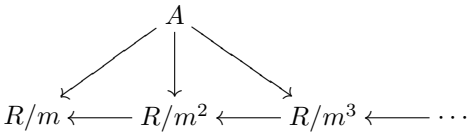
4.1 Completions

Today we will cover completions, which is another way to analyze local rings. There are a who series of ways to study a variety at a point: One is to look at the local ring – that is, you invert all functions that are nonzero at a point. Suppose that R is some local ring with maximal ideal m. We

can think of R/m as the field of functions at the point. Similarly, we could look at R/m^2, which sort of describes "2nd order neighborhood", and we could continues this way. The completion is putting all of these R/m^n together. In other words, we take the inverse limit. Before defining the inverse limit, let us do an actual example.

Example 126. Look at A^1 near the point 0. The local ring R is the set of rational functions f/g, $g(0) \neq 0$. A maximal ideal is the set of functions f/g, with $f(0) = 0, g(0) \neq 0$. Now $R/m = k$, $R/m^2 = k[x]/(x^2)$, $R/m^3 = k[x]/(x^3)$. Notice that we have natural maps $\cdots \to R/m^3 \to R/m^2 \to R/m$. The inverse limit is a ring $\hat{R}$ mapping to all R/m: It is given by all sequences $(a_1, a_2, \dots)$, $a_i \in R/m^i$, which are compatible, such that the image of a_i under the above mentioned maps is a_{i-1}. So $a_1 = b_0 \in R/m = k$, and $a_2 = c_0 + c_1 x \in R/m^2$, and compatibility tells us that $c_0 = b_0$, and so on. Putting these together, we see that an element of the inverse limit is the same as a formal power series $b_0 + b_1 x + b_2 x^2 + \cdots$, where b_0 is determined by the image in R/m, $b_0 + b_1 x$ is determined by the image in R/m^2 and so on.

The inverse limit has the following universal property: If A is any ring mapping to all the rings R/m^i such that the below diagram commutes, then there is a unique map $A \to \hat{R}$ such that everything commutes (this is an easy exercise).



Moreover, this property charaterizes $\hat{R}$ up to isomorphism (which is another easy exercise). Notice that we can define *inverse limits* in any category in a similar way; it may or may not exist.

Now we can ask what the relation between the local ring and its completion is. There is an obvious map $R \to \hat{R}$. This map is sometimes injective, and sometimes it's not. It is if R is Noetherian (because of a theorem due to Krull). We consider a few examples of what goes wrong if R is not Noetherian.

Example 127. Take R to be germs of smooth functions on $\mathbb{R}$ near 0 – that is, we take smooth functions and identify two of these, if they are the same near 0. R is a local ring with a maximal ideal m represented by smooth functions that are 0 at 0. To see that it is a local ring, suppose $f \notin m$. Then $f \neq 0$ at 0, so $f \neq 0$ in some neighborhood, and so f^{-1} exists in some neighborhood of 0. We have $R/m \cong \mathbb{R}$, $R/m^2 = \mathbb{R}[x]/(x^2)$, and in general $R/m^n \cong \mathbb{R}[x]/(x^n)$. So as before, the completion is the formal power series ring $\mathbb{R}[[x]]$. But the map from germs of smooth functions to formal power series is not injective. The standard example is something like e^{-1/x^2}, whose formal power series is 0, since all derivatives vanish at 0. So R is not Noetherian, and one might wonder what its not finitely generated ideals are; one example is the ideal I of functions vanishing to all orders.

Example 128. We consider the ring of Puiseux series. Consider $\mathbb{R}[[x]] \subseteq \mathbb{R}[[x^{1/2}]] \subset \mathbb{R}[[x^{1/6}]] \subset \cdots$. The union of all these is the ring R of Puiseux series; that is, it is the union of power series in $x^{1/n}$, $n = 1, 2, \dots$. We have a maximal ideal m of all series with vanishing constant term. Now $R/m = \mathbb{R}$, but notice that $m^2 = m$. To see this note that $a_1 x^{1/n} + a_2 x^{2/n} + \cdots \in m$ can be written $x^{1/n}(a_1 + a_2 x^{1/n} + \cdots)$, where the last term is a unit. Therefor, the completion is just $\mathbb{R}$.

Theorem 129 (Hensel's lemma)**.** *We have Hensel's lemma: Suppose R is a local ring and $\hat{R}$ its completion. Suppose $f \in \hat{R}[x]$. Suppose $f_0 = g_0 h_0$, with f_0 the imaeg of f in $k = R/m$. Suppose g_0, h_0 are coprime in $k[x]$. Then $f = gh$ for some lifts of g, h.*

The geometric meaning of this is the following:

Example 130. Consider for example $y^2 = x^3 + x^2$ with a singularity at the origin as in the first image in Fig. 22. Then the singularity sort of looks like the singularity shown in the second image in Fig. 22: Take R to be the local ring of $k[x, y]$ at 0. Look at $z^2 = x + 1$. This has roots $z = \pm 1$ in $R/m = k$, since $z^2 - (x+1) = (z-1)(z+1)(\mod m)$. If $\operatorname{char} k \neq 2$, then $z - 1$ and $z + 1$ are coprime, and by Hensel's lemma, $(z^2 - (x+1)) = g(z)h(z)$ for $g, h \in \hat{R}[x]$. This says that $1 + x$ has

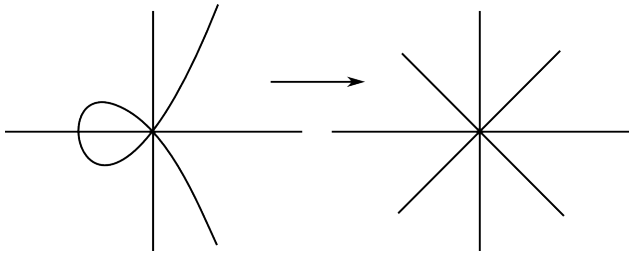


Figure 22: The picture considered in Example 130.

a square root in $\hat{R}$, so $y^2 - x^2(1+x)$ factorizes as $(y - x + \text{higher powers})(y - x - \text{higher powers})$. This gives the split in the illustration meaning that the cusp looks like 2 lines intersecting over the completion. (Note that this fails for $\operatorname{char} k = 2$ since here $(y-x)^2 0 y^2 - x^2 (\mod 2)$).

Hensel's lemma also occurs in algebraic number theory: Here the local ring might be $Z_{(p)}$, all rational numbers f/g with $p \not| g$. This is analogous to rational functions f/g, $g(0) \neq 0$ with $x \not| g$. The completion of the ring is given as follows: The maximal ideal m is all rationals f/g with $p \mid f$, $p \not| g$. We find that $R/m^n = \mathbb{Z}/p^n\mathbb{Z}$. The completion is the inverse limit of $\mathbb{Z}/p \leftarrow \mathbb{Z}/p^2 \leftarrow \cdots$. The result is the p-adic numbers – a typical p-adic number looks like a number to pase p going off to the left (unlike the way we usually right real numbers). The number $\cdots a_2 a_1 a_0$ means $a_0 + a_1 p + a_2 p^2 + \cdots$, which is analogous to the formal power series $a_0 + a_1 x + a_2 x^2 + \cdots$. For formal power series, however, the completion $\hat{R}$ has the same characteristic as the quotient ring R/m. For p-adic numbers, the quotient field has characteristic p, but the completion has characteristic 0. This seems to be a fundamental difference between algebraic number theory and algebraic geometry.

Proof of Hensel's lemma. We prove the theorem since the proof is typical for proofs about completions. The key point of proving things about completions is to prove first for R/m, then for R/m^2, R/m^3, and so on, putting everything together. Suppose $f \in \hat{R}[x]$ Suppose $f_0 = g_0 h_0 \in \hat{R}$. To simplify notation, just take $\hat{R} = \mathbb{R}[[y]]$. Then we want to find $h_1, g_1 \in R/m^2[y]$. Write $h_1 = h_0 + a_1 x$, and $g_1 = g_0 + b_1 x$, where a_1, b_1 have to be found. Now

$$\begin{aligned} f &= h_1 g_1 (\mod x^2) \\ &= h_0 g_0 + x(h_0 b_1 + g_0 a_1) + (\cdots) x^2. \end{aligned}$$

We need to choose the term in the first paranthesis to be the coefficient of x in f. Note that h_0, g_0 are coprime by assumption, so they generate a unit ideal in $k[y]$, and we can solve (coeff. of x in f) $= h_0 b_1 + g_0 a_1$ for b_1, a_1. Next we want $f = (h_0 + h_1 x + h_2 x^2)(g_0 + g_1 x + g_2 x^2) (\mod x^3)$, and given h_0, h_1, g_0, g_1, f we want to solve for g_2, h_2. Again we find that the coefficient of x^2 in f is $h_2 g_0 + h_1 g_1 + h_0 g_2$, and we can solve for h_2, g_2, as g_0, h_0 gneerate the unit ideal. We can just keep going like this to produce $f = gh$, where g, h are polynomials in y with coeffcients that are formal power series in x. □

Elimination theory is about the following problem: Suppose V is a variety in (say) A^3. What is the image of V under projection to (say) A^2 – see Fig. 23. Suppose V is given by $f(x,y,z) = 0$, $g(x,y,z) = 0$. We want to elimiate z from these equations. The problems occur when the equations are not linear in the variable we are trying to eliminate.

Example 131. Suppose V is given by $x^3 y^4 - 7xy^2 + 6x^3 y + 7x - 1$ and $x^5 y - 6xy^3 + 7$ in A^2, and we want to eliminate y. What equation must x satisfy? We expect that the equation must be of degree about 42, since the equations are of degree 7 of 6. We will give an algorithm for eliminating y.

A more general problem is the following: Suppose $f = a_m x^m + \cdots + a_0$, $g = b_n x^n + \cdots + b_0$ are polynomials in x (with coefficients in some ring, maybe polynomials in $y, z, \ldots$). What is

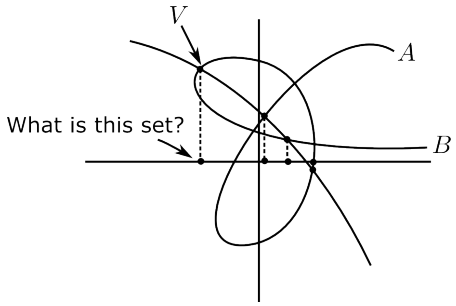


Figure 23: A variety V arises as the intersection of A and B, and we are interested in its projection.

the condition on $a_0, \cdots, a_m, b_0, \cdots, b_m$ for the polynomials to have a common root – this is a generalization of the previous problem, and this is what we want to solve.

Suppose f, g have a common root, so $f(x) = (x-\alpha)q(x)$ and $g(x) = (x-\alpha)p(x)$. Then $f(x)p(x) = g(x)q(x)$, and $\deg p < \deg g$ and $\deg q < \deg f$. This is a set of $\deg f + \deg g$ linear equations for the coefficients of p, q; p has $\deg g$ unknown coefficients and q has $\deg f$, so it has a nontrivial solution, if and only if the determinant of the matrix of the coefficients of these linear equations vanishes. The matrix of linear equations is

$$\begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ & a_m & a_{m-1} & \cdots & a_0 & \cdots & 0 \\ & & \ddots & & & & \\ & & & & a_m & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ & b_m & b_{n-1} & \cdots & b_0 & \cdots & 0 \\ & & \ddots & & & & \\ & & & & b_n & \cdots & b_0 \end{pmatrix}$$

This is called the Sylvester matrix, and the determinant is called the resultant of f and g. The above condition is almost but not quite the condition for f, g to have a commen root. The problem is that the leading coefficients a_m, b_n might be 0. The determinant also vanishes if $a_m = b_n = 0$. If $a_m = 0$, we say that f has a "root at ∞", and similarly for $b_m = 0$ and g. Then the determinant vanishes if and only if f, g have a common root, possibly at ∞.

Example 132. What is the condition for f to have a multiple root (or leading coefficient 0)? We can do the case where $g = f'$, and $f(x) = x^3 + bx + c$ to try to find the double roots of f. Plugging everything into the Sylvester matrix, we get

$$\det \begin{pmatrix} 1 & 0 & b & c & 0 \\ 0 & 1 & 0 & b & c \\ 3 & 0 & b & 0 & 0 \\ 0 & 3 & 0 & b & 0 \\ 0 & 0 & 3 & 0 & b \end{pmatrix} = 4b^3 + 27c^2,$$

which is the discriminant of a cubic.

If we rewrite the above over projective space, the result becomes a bit clearer. Suppose f, g are homogeneous polynomials $a_m x^m + a_{m-1}x^{m-1}y + \cdots + a_0 y^m$ and $b_n x^n + \cdots + b_0 y^n$ with coefficients a_i, b_i in $k[z_1, \ldots, z_t]$. Then f, g define hypersurfaces H_f, H_g in $A^t \times P^1$, where A^t has variables $z_1, \ldots, z_t$, and x, y are coordinates for P^1.

The resultant of f, g then gives the condition for f, g to have a common zero in P^1 at any given point of A^t. Then the resultant gives the image of $H_f \cap H_g$ in A^t. The key point is that the image

of a closed set $H_f \cap H_g$ in A^t is closed. This is unusual, and in general there is no reason that the projection of a closed set is closed; this for example doesn't happen for $xy = 1$ in $A^1 \times A^1$. Next time we will see that $A^t \times P^n \to A^t$ is a proper map: It takes closed sets to closed sets.

19th lecture, October 28 2010

Recall that last time we were looking at

$$f(x,y) = a_n x^n + a_{n-1} x^{n-1} y \cdots a_0 y^n$$
$$g(x,y) = b_m x^m + \cdots b_0 y^m.$$

The condition for these two to have a common root in P^1 with coordinates x, y is a polynomial in a's and $b's$ called the resultant, which by definition is the determinant of the Sylvester matrix.

If H_f, H_g are hypersurfaces in $A^t \times P^1$ then the projection of the closed set $H_f \cap H_g$ under $\subseteq A^t \times P^1 \to A^t$ is closed (the zero set of the resultant). The a's and b's are polynomials in $z_1, \ldots, z_t$ are coordinates in A^t. We want to generalize this and show that under $A^t \times P^n \to A^t$ the image of any closed set in $A^t \times P^n$ in A^t is closed. (This is false for affine space, as we saw last time. It is not even true that the image of a polynomial map from $\mathbb{R}^n$ to $\mathbb{R}$ is closed – there is a counterexample: $x^2 + (xy-1)^2 : \mathbb{R}^2 \to \mathbb{R}$.)

The motivation for all this is to find an analogue of the fact that $P^n(\mathbb{C})$ with the usual topology is compact – a quick proof of this is that the image of S^{2n-1} is all of $P^{n-1}(\mathbb{C})$ under the quotient, and S^{2n-1} is compact. We see that $P^n(k)$ is compact in the Zariski topology – this is the wrong analogue though, as $A^n(k)$ is also compact in the Zariski topology. We need to find a different description of compactness. Recall the notion of a proper map of locally compact Hausdorff spaces.

Definition 133. A map $X \to Y$ is called *proper* if it is universally closed. That is, $X \times Z \to Y \times Z$ is closed for all Z (i.e. the image of every closed set is closed).

Note that X is compact, if and only if $X \to 1$ is proper (as a special case: If X is compact, then $X \to Y$ is always closed: If $C \subseteq X$ is closed, then C is compact, so the impage of C is compact and therefore closed).

For locally compact Hausdorff spaces, saying that $X \to Y$ is proper is equivalent to saying that it is closed with all fibers being compact.

Definition 134. We say that a morphism $X \to Y$ of algebraic sets is *proper* if it is universally closed: $X \times Z \to Y \times Z$ is closed for the Zariski topology on $X \times Z$, $Y \times Z$, which is *not* the product topology.

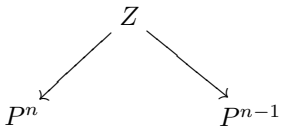
If $X \to 1$ is proper, this is an analogue of saying that X is compact in the complex topology.

The key property of projective varieties V says that $V \to 1$ is proper. It is suffcient to show that the map $P^n \to 1$ is proper (as V is closed in P^n). We need to show that $P^n \times Z \to Z$ is closed for all Z. It is easy to reduce to the case $Z = A^m$, so we want to show that $P^n \times A^t \to A^t$ is closed. We already did the an easy case of this.

Let us first show that $P^1 \times A^t \to A^t$ is closed. Suppose S is a closed set in $P^1 \times A^t$ given by the zeros of polynomials $f_1, f_2, \ldots$, in variables $X, Y, Z_1, \ldots, Z_t$, where X, Y are homogeneous coordinates on P^1, and the Z_i are coordinates on A^t. We look at the resultant of $F = t_1 f_1(X, Y, Z_1, \ldots, Z_t) + t_2 f_2 + t_3 f_3 + \ldots$, and $G = s_1 f_1 + s_2 f_2 + \cdots$. We think of the coefficients as homogeneous polynomials in X, Y whose coefficients are polynomials in $s_1, \ldots, t_1, \ldots, Z_1, \ldots, Z_t$. Then the projection of S into A^1 is given by the vanishing of all coefficients $s^\alpha t^\beta$ in the resultant of F, G (exercise). So, the image is closed as each coefficient of $s^\alpha t^\beta$ in the resultant is a polynomials in $Z_1, \ldots, Z_t$. This shows that $P^1 \times A^t \to A^t$ is closed.

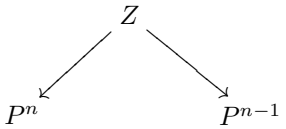
Let us try to do the general case $P^n \times A^t \to A^t$ by induction on n. An obvious way to do this would be to write $P^n = P^{n-1} \times P^1$, isn't true – if it was true, it would be easy, since we could write $P^n \times A^t = P^1 \times (P^{n-1} \times A^t) \to P^{n-1} \times A^t \to A^t$ and use induction to see that the map

is closed. While P^n is not $P^{n-1} \times P^1$, it is quite close to be. The correct statement is that the blow-up Z of P^n at a point is a bundle over P^{n-1} with fiber P^1



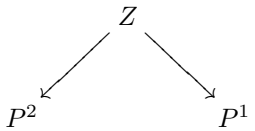
Z is a sort of "twisted" product or fiber bundle over P^{n-1}. We have a birational map $P^n \to P^1 \times P^{n-1}$; birational map can be turned into morphisms by blowing things up. (This is a common application of blowing up).

More precisely, we have a rational map $P^n \to P^{n-1}$ mapping $(x_0 : \cdots : x_n) \mapsto (x_1 : \cdots : x_n)$ defined except at the point $(1 : 0 : \cdots : 0)$. We look at the graph of this map, the subset of $P^n \times P^{n-1}$ consisting of the points $(x_0 : \cdots : x_n) \times (y_1 : \cdots : y_n)$ with $x_i y_j = x_j y_i$ for all i, j and some x_i $(i > 0)$ nonzero. Let Z be tehe closure of this graph; we add a copy of P^{n-1} lying over $(1 : 0 : \cdots : 0)$. That is, all points of the form $(1 : 0 : \cdots : 0) \times (y_1 : \cdots : y_n)$. This corresponds to dropping the second condition above. We now have the following maps:



The map on the left is an isomorphism abvoe all points other than $(1 : 0 : \cdots : 0)$, and the inverse image of $(1 : 0 : \cdots : 0)$ is a copy of P^{n-1}, so Z is just a blow-up of P^n at this point. What is the fiber of a point P^{n-1} under the second map? By symmetry, we may as well look at $(1 : 0 : \cdots : 0)$, which has fiber the points $(x : y : 0 : \cdots : 0) \in P^n$, which is a copy of P^1 as we claimed before. Note again that this does not imply that $Z = P^{n-1} \times P^1$. However, locally it is a product. Recall that P^{n-1} is covered by n copies of affine space A^{n-1}. Over each copy of A^{n-1}, Z does look like a product $P^1 \times A^{n-1}$. For example, over the open subset $y_1 = 1$ in P^{n-1}, the equations for Z are $x_i = x_1 y_i$ for $i \neq 1$, so if we map $(x_0 : \cdots : x_n)$ to $(x_0 : x_1) \times (x_2, \ldots, x_n)$ we get a map from an open subset of Z to $P^1 \times A^{n-1}$. This gives an isomorphism from the inverse image of A^{n-1} in Z to $P^1 \times A^{n-1}$. Now we can finish off the proof, since $Z \to P^{n-1}$ looks locally like a product $P^1 \times \text{something} \to \text{something}$, so it is a proper map (since if it is locally proper, it is proper). The map $P^n \to 1$ is proper, since we can lift it to $Z \to P^{n-1} \to 1$, which is a composition of two proper maps.

For $n = 2$, the setup is the following:



Z is then a surface mapping to P^1 with fiber P^1, it is birational to P^2 (and $P^1 \times P^1$), but it is not isomorphic to either surface. This is an example of a Hirzebruch surface, having P^1 fibers over P^1.

We turn now to a second proof, which is shorter. The first proof has the advantage of being constructive: It actually gives a (complicated) algorithm for finding the equations of the projection of a closed subset $S \subseteq P^n \times A^t$ in A^t. Here's the second one: Suppose $f_1, f_2, \ldots$ are homogeneous polynomials in $Z_1, Z_2, \ldots$. We want to show that the condition they have a common zero is given by a closed condition on their coefficients; in other words, it is given by the condition that some polynomials in the coefficients vanish – this is just a reformulation that $P^n \to A^t \to A^t$ is closed. By the (projective) Nullstellensatz, they have no common zero if and only if the ideal they generated contains $(Z_1, \ldots, Z_t)^d$ for some $d \geq 0$. For each d the condition that linear combinations of the f's contain all degree d monomials in $Z_1, \ldots, Z_t$ just says that a certain linear map to the space of monomials is onto. The conditions that a linear map $k^m \to k^n$ is onto is open (it is the complement of a determinantal variety). So, the points where the f have no common zero is the union over d of various open sets, thus open, and the points where all f have a common zero is

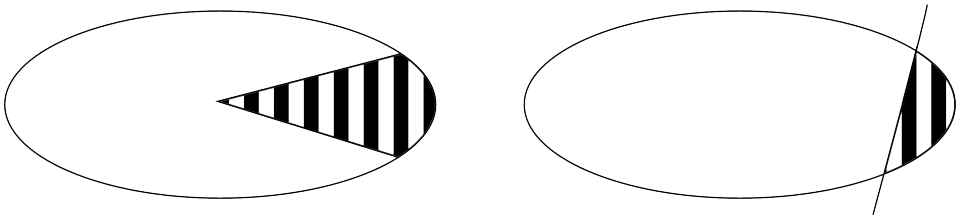


Figure 24: Two of the ovals in the example.

closed. (This proof is ineffective, as we took an infinite union over d – by compactness we can do with a finite number of sets, but it is hard to know which ones.)

We consider now a historical application of singular points.

Theorem 135 (Newton)**.** *Smooth ovals cannot be algebraically integrated.*

The historical background is the following: We would like to find the location of a planet moving along an ellipse (or rather any orbit) at a given time. Due to one of Kepler's laws, the area swept out by the line from the planet to the sun increases at a constant rate. The first thing Newton showed was that this condition is equivalent to the planet moving under some centripetal force directed to the sum. So we want to consider the following problem: Given some oval, is the area in the first image of Fig. 24 an algebraic function of the lines bounding it? Equivalently, is the area A shown in the second image of Fig. 24 an algebraic function of the secant $ax + by = c$? Is there a non-zero polynomial p such that $p(A, a, b, c) = 0$? If this is possible, you can write up an algebraic equation for the planet moving along an orbit with the centripetal force desribed above.

The answer is sometimes yes. For example, if the oval is a triangle. Calculus gives a lot of examples; parabolas, cubics, etc. where the area can be calculated by integration, giving an algebraic function of the secant.

Consider instead for example $y^2 = x^2 - x^4$. In this case, it is always possible since $\int y\,dx = \int \sqrt{x^2 - x^4}\,dx = \int x\sqrt{1 - x^2}\,dx$, which can be calculated and gives an algebraic expression. Newton showed that for any oval, the area cut off by a secant is not algebraic function of the secant. The proof is pretty graphical, and I got a bit lazy at this point (see Borcherds' notes) – the key point is to construct a certain spiral from the ovals that is not algebraic. The above examples seem to be counter-examples to Newton's theorem. In each of the examples, the spirals considered in Newton's proof will contain singular points; that is, they will not be infinitely differentiable. The additional assumption pointed out by Arnold (300 years later) therefore is that the oval must be infinitely differentiable.

20th lecture, November 2 2010

5 Non-singular curves

A basic invariant of a curve is its genus. A topological definition of this over $\mathbb{C}$ is the following; the complex points form a surface. If the curve is projective, the surface is compact. The surface is always oriented and its orientation is given by a complex structure on the tangent spaces – each tangent space is a complex vector space, which can be given an orientation by the pair of vectors (v, iv). Recall now the classification of compact (closed) oriented connected surfaces; these are classified by their genus. A better invariant is really the Euler characteristic $2 - 2g$.

We will mostly give examples of nonsingular, projective, complex curves.

Example 136. For genus 0, the only example is the projective line $P^1(\mathbb{C}) = \mathbb{C} \cup \infty$, which is just a sphere.

Example 137. For genus 1, we have the *elliptic curves*. Recall that we have an analytic construction: We can define them as $\mathbb{C}$ modulo a lattice, making it obvious that these are tori, but this

construction is not algebraic, and gives problems for arbitrary fields. An algebraic construction is given by $y^2 = 4x^3 + bx + c$. The connection between these is the Weierstrass $\wp$-function, which is periodic under lattice translations, $\wp(z + \lambda) = \wp(z)$ for λ in the lattice, and on the other hand, it satisfies a differential equation, $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, so $z \mapsto (\wp'(z), \wp(z))$ mapping $\mathbb{C}/\Lambda - \text{pt} \to y^2 = 4x^3 - g_2x - g_3$. This really gives the elliptic curve as a double cover of P^1 branched in 4 points.

The 4 points are the roots of $4x^3 - g_2x - g_3$, which is really a degree 4 polynomial with a root at ∞. This means that we could consider the map $y^2 = 4x^3 - g_2x - g_3 \mapsto x \in P^1$, which is a $2:1$ map in general; there are two values of y for each x, except if x is a root of $4x^3 - g_2x - g_3$ or $x = \infty$.

This gives rise to an algebraic construction given by cutting the double cover along certain curves and gluing them together – see Fig. 25.

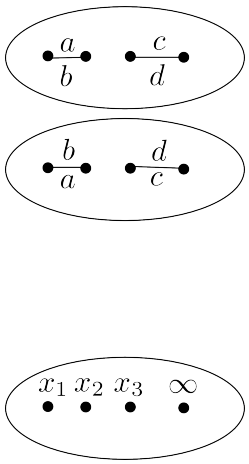


Figure 25: A genus 1 curve can be pictured as a result of cutting and gluing.

We can calculate the genus (or rather the Euler characteristic χ) of this double cover of S^2 branched at 4 points. Recall that χ is the number of points − the number of lines + the number of 2-cells. In our case, the Euler characteristic is given by the Euler characteristic of the union of 2 spheres with 4 points removed, and $2 + 2 - 4 = 0$, which is the Euler characteristic of a torus.

Next we can ask how to classify all the elliptic curves. In the curve $y^2 = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$ we can substitute $x \mapsto \frac{ax+b}{cx+d}$ without affecting the isomorphism class. This gives a group of transformations, which is nothing but $PSL_2(\mathbb{C})$. This can take any three points to any other three points. So take x_1, x_2, x_3 to $0, 1, \infty$, so the curve becomes $y^2 = x(x - 1)(x - \lambda)$ for some λ. The problem is the following: When is $y^2 = x(x-1)(x-\lambda_1)$ isomorphic to $y^2 = x(x-1)(x-\lambda_2)$? This happens when there is an automorphism of P^1 taking $\{0, 1, \infty, \lambda_1\}$ to $\{0, 1, \infty, \lambda_1\}$. This is possible if λ_2 is λ_1, $1 - \lambda_1$, $1/\lambda_1$, $1 - 1/\lambda_1$, $\lambda_1/(1 - \lambda_1)$, or $1/(1 - \lambda_1)$. These form a group of order 6, generated by $\lambda \mapsto 1 - \lambda$ and $\lambda \mapsto 1/\lambda$. This group can also be thought of as the permutations of $\{0, 1, \infty\}$. The moduli space (i.e. the space of isomorphism classes of elliptic curves) turns out to be A^1 modulo this group of order 6. So we want to find a rational function invariant under $\lambda \mapsto 1 - \lambda$, $\lambda \mapsto 1/\lambda$. Such a function is $j = 256\frac{\lambda^2-\lambda+1}{\lambda^2(\lambda-1)^2}$. This is the so-called j-invariant of elliptic curves. One can show that 2 elliptic curves over $\mathbb{C}$ are isomorphic, if and only if they have the same j-invariant in $\mathbb{C}$. (A problem is that the moduli space of elliptic curves is really a stack and not a space; elliptic curves have non-trivial automorphisms, and whenever you try to classify things with non-trivial automorphisms, you run into the following problem: We know that elliptic curves correspond to maps from a point to the moduli space; we would like to have that "nice" ("flat") families of elliptic curves over a space X correspond to maps from X to the moduli space. Suppose an elliptic curve $\mathcal{E}$ has an automorphism σ; say $x \mapsto -x$. In the topological picture, take $\mathcal{E} \times I$ (which is not a variety). Join $\mathcal{E} \times 0$ to $\mathcal{E} \times 1$ using the automorphism σ. Doing this we

have a non-trivial family of elliptic curves over $I/(0=1) = S^1$, but they are all isomorphic, so the corresponding map to the moduli space has image a point, but this map corresponds to the trivial family. The theory of stacks is a way of getting around this problem.)

We could also ask the following question: Suppose we have a lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$; what is the j-invariant of $\mathbb{C}/\Lambda$? The answer is if $\tau = \omega_2/\omega_1$, j is a function of $q = e^{2\pi i \tau}$, $|q| < 1$, and $j(\tau) = q^{-1} + 755 + 196884q + 21493760q^2 + \cdots$, the elliptic modular function.

Example 138. For genus 2, all curves are hyperelliptic, meaning that they are all branched double covers over P^1, meaning that they are $y^2 = x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_0$, branched at $2n$ roots of this polynomial. In degree 2, $y^2 = x^2 + a_1 x + b$, this is P^1 as a double cover of P^1. In degree 4, $y^2 = x^4 + a_3 x^3 + \cdots + a_0$, these are exactly the elliptic curves. In degree 6, $y^2 = x^6 + \cdots + a_0$, these are genus 2 curves; in general, we can check the Euler characteristic like in the genus 1 picture. Here, χ can be calculated to be $2 + 2 - 2n = 4 - 2n$, and since $\chi = 2 - 2g$, so $g = n - 1$. In particular, in the degree 6 case, we do indeed have genus 2 curves, and we also get every genus ≥ 0. In fact, all genus 2 curves are hyperelliptic (by the Riemann–Roch theorem), and the classification is given by sets of 6 numbers $x_1, \ldots, x_6$ in P^1 up to the action of the group $PSL_2(\mathbb{C})$. This is equivalent to the problem of finding the invariants of the binary sextic form $a_6x^6 + a_5x^5y + \cdots + a_0y^6 = a_6(x - x_1y)\cdots(x - x_6y)$; this is a hard problem in invariant theory. The final answer looks like this: The moduli space is A^3 modulo the cyclic group of order 5 acting as $(x, y, z) \mapsto (\zeta x, \zeta^2 y, \zeta^3 z)$, where $\zeta^5 = 1$. There seems to be no such explicit description of the moduli space of curves of genus > 2. The dimension of the moduli space in our case is 3; we can choose 6 points of P^1 and quotient by the action of $PSL_2(\mathbb{C})$, which has dimension 3.

Example 139. For genus 3, some curves are hyperelliptic, $y^2 = x^8 + \cdots + a_0$, and we get a 5-dimensional family of such, as here we can choose 8 points in P^1 and quotient by the action of the group $PSL_2(\mathbb{C})$ of dimension 3. We can also get examples as nonsingular degree 4 curves in the plane. Suppose we have a nonsingular curve of degree d in P^2. We can then ask for its genus or Euler characteristic. Taking $f(x, y) = 0$, where f has degree d, we consider the curves as a degree d cover of P^1, mapping $f(x, y) = 0$ to $x \in P^1$. In general this is a $d : 1$ map. Sometimes it has branch points; most of the time, all branch points will be order 2, and we can ask how many branch points there are. The answer is $d(d-1)$, so the Euler characteristic is $d \cdot \chi(S^2) - d(d-1) = 2d - d(d-1) = 2 - 2g$, so $g = (d-1)(d-2)/2$. Not every genus can appear, so most curves cannot be represented as non-singular plane curves. The family of such curves of genus 3 has dimension 6: The space of polynomials of degree 4 has dimension 15. We subtract 1 as multiplying a polynomial by a constant does not change the curve; curves correspond to the projective space of k^{15}, which has dimension 14. We then subtract 8, which is the dimension of the group $PSL_3(\mathbb{C})$ consisting of the automorphisms of P^2, so we get a $15 - 1 - 8 = 6$ dimensional family of genus 3 curves. Note that there are more plane curves than hyperelliptic, as $6 > 5$.

A typical example of the geometry of genus 3 curves is the following: A plane genus 3 curve has 28 bitangents. For example the Trott curve[6]: $144(x^4 + y^4) - 225(x^2 + y^2) + 350x^2y^2 + 81 = 0$ – it has 1 bitangent for each "bean", touching once of them. Similarly, we have 4 bitangents for each pair of beans, and in total we get $4 + \binom{4}{2} \cdot 4 = 28$. Note also that we have 56 special points, where the 28 bitangents meet the curve.

Example 140. For genus 4, we can get curves as intersections of a cubic or quadric in P^3. For genus 5, we could consider 3 quadrics in P^4, and so on. For sufficiently high genus (≥ 22), this becomes harder due to technical reasons.

We will (topologically) give a picture of *every possible* algebraic curve: Consider P^1 with $n+1$ points $x, x_1, \ldots, x_n$ in it; choose cuts joining x_i to x (which is a topological rather than algebraic process) – see Fig. 26. Choose a set of d numbers $1, 2, \ldots, d$. Choose n involutions (an order 2 permutation) on $\{1, \ldots, d\}$. For example, if $d = 6$, an involution might exchange $(1, 2)$ and $(4, 5)$. Take d copies of P^1, cut along these n lines, and join then up along the branch cuts according to n involutions; 1 for each branch cut. This procedure will not always give an algebraic surface, as

[6] See `http://en.wikipedia.org/wiki/Trott_curve` for an illustration of the curve and its bitangents

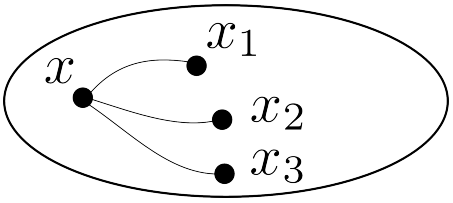


Figure 26: The topological construction of general algebraic curves.

the result might be disconnected, but all algebraic surfaces can be produced like this for suitable $x_1, \ldots, x_n$, n involutions on d points. An open problem is to make algebraic sense out of the choice of cuts from x to x_i.

21st lecture, November 4 2010

Today, we will consider more examples of complex projective curves. Last time, we saw that plane curves come in various families. We will consider the most symmetric ones.

Example 141. Recall that elliptic curves are the curves of genus 1. As we saw, they arise like $\mathbb{C}/\Lambda$ and are groups, so as curves they an infinite number of automorphisms $z \mapsto z + z_1$ and $z \mapsto -z$. There are two elliptic curves that are even more symmetric than that. We look at the lattice Λ and ask when it is especially symmetric. One example is the square lattice $\mathbb{Z} + i\mathbb{Z}$ which has the extra automorphism $z \mapsto iz$. Another example is the traingle lattice, with the extra automorphism $z \mapsto \omega z$, where $\omega^2 + \omega + 1 = 0$. In the first case, we can write down the curve explicitly as $y^2 = x^3 + x$, where we see the extra automorphism explicitly as $x \mapsto -x$, $y \mapsto iy$. In the triangle case, the curve is $y^2 = x^3 + 1$ with the automorphism $x \mapsto \omega x$. These two automorphisms are special cases of complex multiplication: Some other elliptic curves have extra endomorphisms given in a similar way.

Example 142. We can try to find the most symmetric curves of genus greater than 1; these are called Hurwitz curves. The key idea of studying these is the following: Suppose we have a finite group G acting on a curve C (which we consider as a Riemann surface). We look at the quotient C/G. Think of this as an orbifold, which is something that looks like a manifold quotient a finite group and is a cheap approximation to a stack. Suppose we have a manifold, which locally looks like a circle and consider the quotient $z \mapsto -z$. This gives rise to an orbifold singularity, which can be thought of as half a point, and it only counts as a half when computing the Euler characteristic. The advantage of this is that the orbifold Euler characteristic satisfies $\chi(C/G) = \chi(C)/|G|$, where we carefully count things with fractional values. We can get conical singularities of orders $n = 1, 2, 3, \ldots$, by considering $z \mapsto \zeta z$, $\zeta = e^{2\pi i/n}$, which is a rotation by $1/n$ revolutions. Now C/G will be a compact orientable Riemann surface with a few orbifold singularities. These come whenever some group element of G fixes a point of C. The subgroup fixing any point of C is cyclic and usually of order 1. If the Riemann surface in question has genus h, the orbifold Euler characteristic is $2 - 2h - (1 - \frac{1}{p_1}) - (1 - \frac{1}{p_2}) - \cdots$, where $p_1, p_2, \ldots$ are orders of the conical singularities; these summands arise since we remove a point ($\chi = 1$) and add in a singularity ($\chi = 1/p$). So we find that $\chi(C)/|G| = \chi(C/G)$. That is, $\frac{2-2g}{|G|} = 2 - 2h - (1 - \frac{1}{p_1}) - \cdots$. The key point is that for $g > 1$, the left hand side is less than 0. We want the right hand side to be small in absolute value, but we see that $\chi(C/G) \leq -2$ if $2 - 2h = -2, -4, \ldots$. If $2 - 2h = 0$, then $\chi(C/G) = 0$ or $\chi(C/G) \leq -1/2$, so we should take $h = 0$ and need $2 - 2h - (1 - \frac{1}{p_1}) - (1 - \frac{1}{p_2}) - \cdots$ to be negative but close to 0. If we have 4 numbers $(1 - \frac{1}{p})$, we get either 0 or something less than $-1/6$. If we have less than 3 numbers, the result is always positive. So we have exactly 3 numbers and want to solve the problem of making $2 - a - b - c < 0$ as close to 0 as possible, where a, b, c are of the form $1 - \frac{1}{p}$. An exercise is, that the best solution is $2 - \frac{1}{2} - \frac{2}{3} - \frac{6}{7} = -\frac{1}{42}$. So $\frac{2g-2}{|G|} \leq -1/42$, so $|G| \leq 84(g-1)$. This is Hurwitz' bound for the order of the automorphism group of a Riemann surface of genus g. (It

should be mentioned that orbifolds can also be used to classify the 17 wallpaper groups in a similar way. This is an exercise; one does it by considering the quotient of $\mathbb{R}^2$ with the wallpaper groups as an orbifold (which might possibly non-orientable) – the key point is that this is an orbifold with $\chi = 0$, and one has to solve an equation like above.)

We consider now the following problem: Can we find an algebraic curve of genus $g > 1$ with $84(g-1)$ automorphisms? We consider the case $g = 2$, so we want to find a genus 2 curve, with automorphism group G of order 84. The group G is a quotient of the orbifold fundamental group of the orbifold, which if the orbifold points have order p, q, r is generated by elements a, b, c of orders p, q, r with $abc = 1$. So the automorphism group G has the following properties:

(1) $|G| = 84$.

(2) G is generated by elements a, b, c with $a^2 = b^3 = c^7 = abc = 1$. Finite groups with this property are called Hurwitz groups.

We apply the Sylow theorems to the group. We know that there are 1 mod 7 Sylow 7-subgroups and divides $84/7 = 12$. So there is only 1 Sylow 7-subgroup, say S_7, so it is normal. Now look at $H = G/S_7$ which has order 12. Now, the number of Sylow 3-subgroups might be 1 or 4. If there is only 1, S_3, then it is normal and $1 \subseteq S_7 \subseteq S_7 \cdot S_3 \subseteq G$, where the last inclusion has index 4. Every element of order 3 or 7 is contained in $S_7 \cdot S_3$, so G cannot be generated by elements of order 3,7, so it is not a Hurwitz group. Suppose there are 4 Sylow 3-subgroups (e.g. A_4). Any 2 Sylow 3-subgroups are cyclic, so they intersect only in 1. So the group has $(3-1) \cdot 4 = 8$ elements of order 3. This leaves only 4 elements left, so these must form a Sylow 2-subgroup, so the Sylow 2-subgroups must be normal. So, G looks like this: $1 \subseteq S_7 \subseteq S_7 \cdot S_2 \subseteq G$. We now run into the same problem as before: Every element of order 2 or 7 is contained in this subgroup $S_7 \cdot S_2$ of order 28, so G cannot be generated by elements of order 2 and 7, so G is not a Hurwitz group. In other words, there is no algebraic curve of genus 2 with 84 automorphisms.

We now move on to genus 3 and show that there *is* an algebraic curve with $84(g-1) = 168$ automorphisms. This is the *Klein quartic* $x^3y+y^3z+z^3x = 0$. We first check that it is non-singular. Differentiating with respect to x, y, z, one gets $3x^2y + z^3 = 0$, $3y^2z + x^3 = 0$, $3z^2x + y^3 = 0$, and these have no common solution. It is a non-singular plane curve of degree $d = 4$, so its genus is $(d-1)(d-2)/2 = 3 \cdot 2/2 = 3$. It has obvious automorphisms of order 3 mapping $x \mapsto y \mapsto z \mapsto x$. There is an automorphism of order 7: Try mapping $x \mapsto ax$, $y \mapsto by$, $z \mapsto cz$ for some a, b, c. We want $a^3b = b^3c = c^3a$, and one solution is $a = \zeta^4, b = \zeta^2, c = \zeta$, $\zeta^7 = 1$. Automorphisms of this type generate a group of order 21. It is hard to find any other automorphisms; instead we cheat slightly, and start with the group G and try to find a curve it acts on, rather than finding the automorphism group of the Klein quartic. One group of order 168 is $PSL_2(F_7)$. Note that $GL_2(F_7)$ has order $(7^2-1)(7^2-7)$ and $SL_2(F_7)$ has order $(7^2-1)(7^2-7)/6 = 6 \cdot 7 \cdot 8$, which shows that $PSL_2(F_7)$ has order $6 \cdot 7 \cdot 8/2 = 168$. Another group of $PSL_3(F_2)$ has order 168, and the two groups happen to be isomorphic, and they are both simple. We want to show that $PSL_2(F_7)$ is a Hurwitz group (of smallest possible order). So, we want to find elements a, b, c with $a^2 = b^3 = c^7 = abc = 1$. The standard generators of $SL_2(\mathbb{Z})$,

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$$

satisfy $S^2 = -1$, $(ST)^3 = \pm 1$, so $S^2 = 1$, $(ST)^3 = 1$ in $PSL_2(\mathbb{Z})$. Now $T^7 = 1$ in $PSL_2(F_7)$, and $PSL_2(F_7)$ is a Hurwitz group. Any Hurwitz group is in fact a group of automorphisms of a complex Riemann surface. The idea of the topological proof is to tile the hyperbolic plane by triangles with angles $2\pi/(2 \cdot 2), 2\pi/(2 \cdot 3), 2\pi/(2 \cdot 7)$.

The group of automorphisms of this tiling (with triangles colored alternatively black and white) is a group with generators and relations $a^2 = b^3 = c^7 = abc = 1$. Any Hurwitz group is the quotient of this by a subgroup X, and the quotient of the hyperbolic plane with this subgroup X is going to be a Riemann surface.

Suppose we know that $PSL_2(F_7)$ is the automorphism group of a genus 3 algebraic curve. It must then be a nonsingular quartic in P^2. Now $PSL_2(F_7)$ has a complex representation of

dimension 3 acting on A^3, so it acts on $\mathbb{C}[x,y,z]$. We want to find an invariant quartic; that is, we want to find a polynomial in 3 variables of degree 4, which is invariant under the action of $PSL_2(F_7)$. $PSL_2(F_7)$ has a subgroup of order 21 acting on $\mathbb{C}^3$ as follows: it has an element of order 3 acting as $(x,y,z) \mapsto (z,x,y)$, and an element of order 7 acting as $(x,y,z) \mapsto (\zeta^4 x, \zeta^2 y, \zeta z)$ (with $\zeta^7 = 1$). Any polynomial invariant under $PSL_2(F_7)$ is also invariant under this subgroup of order 21, so there are not many invariant elements of degree 4: The only monomials of degree 4 invariant under the element of order 7 are x^3y, y^3z, z^3x. If in addition we require invariance under the order 3 element, the only possibility is a constant times $(x^3y + y^3z + z^3x)$, which is the Klein quantic. So in other words, what we have shown is that if any Hurwitz group acts on a curve, then $PSL_2(F_7)$ acts on $x^3y + y^3z + z^3x = 0$.

22nd lecture, November 9 2010

6 Resolving singularities

6.1 Overview of curves/function fields/Riemann surfaces

Take k algebraically closed. The following are essentially equivalent:

(1) Non-singular projective curves up to isomorphism.

(2) All curves up to birational isomorphism.

(3) Finitely generated function fields over k of transcendence degree 1.

(4) (Over $\mathbb{C}$) compact (connected) Riemann surfaces.

The map (1) $\to$ (2) is trivial. (2) $\to$ (3) is easy: Just take the field of rational functions. Non-singular curves over $\mathbb{C}$ to Riemann surfaces is also easy, since it is easy to put a complex structure on the curve. Some of the correspondences are much harder. (4) $\to$ (3) looks easy at first: Take the field of meromorphic functions on the surface. However, it is hard to show that there are any non-constant meromorphic functions. Let us consider a few examples of why this is hard.

Example 143. A Riemann surface might be $\mathbb{C}/\Lambda$ with Λ a lattice. To construct a non-constant meromorphic function on the Riemann surface, we need to construct an elliptic function such as $\wp(z)$ – this wasn't difficult, but it wasn't completely trivial. It is not clear how to do it for general surfaces.

Example 144. We consider the Hopf surface. The group $\mathbb{Z}$ acts on $\mathbb{C}^2 \setminus (0,0)$. 1 acts as $(a,b) \mapsto (2a, 2b)$ and n as $(a,b) \mapsto (2^n a, 2^n b)$. Consider $\mathbb{C}^2 \setminus (0,0) = S^3 \times \mathbb{R}_{>0}$, where $\mathbb{Z}$ acts only in the second factor, and here $n \in \mathbb{Z}$ acts as $x \mapsto 2^n x$. Under this action, we have $\mathbb{C}^2 \setminus (0,0) \cong S^3 \times S^1$, which is a compact complex surface with *no* non-constant meromorphic functions (so it is not projective).

More generally, one could consider $\mathbb{C}^n \setminus (0,\dots,0)/\mathbb{Z} \cong S^{2n-1} \times S^1$ which again has no non-constant meromorphic functions for $n > 1$. For $n = 1$ we get $S^1 \times S^1$, an elliptic curve. (Exercise: Find non-constant meromorphic function f on $\mathbb{C} \setminus \{0\}$ with $f(2z) = f(z)$.)

The correspondence (3) $\to$ (2) is not hard: For a function field K, take a separating transcendence base $z \in K$. (It has only 1 element, as the transcendence degree is 1.) So K is a finite separable extension of $k(z)$, so it is a simple extension of the form $k(z,t)$ for some t, and z,t satisfy some polynomial relation $p(z,t) = 0$ giving a curve.

We will mainly be concerned with (2) $\to$ (1). Obviously sending a curve to a projective curve is trivial, as we can just take its closure in projective space, so the problem is: Given a projective curve C, find a projective curve D birational to it with no singularities; this is the famous problem of resolving singularities in a curve, and there are various essentially different ways of doing it. The original method due to Newton was using Newton polygons and Puiseux expansions. Before considering that one, we first look at some of the other popular methods.

(1) The method in [Har, section 6] is to reconstruct the non-singular curve from the function field as the set of valuations (or places) of the function field. This method is essentially due to Riemann in the case of Riemann surfaces.

(2) Another method is to repeatedly blow up singular points.

(3) We can normalize: Every variety has a "normalization", where, roughly speaking, one replaces the coordinate rings by their integral closures, eliminating the codimension 1 singularities. So for dimension 1, it eliminates all singularities. It doesn't seem to be that useful in higher dimension.

6.2 Newton's method

Suppose we have a curve $f(x,y) = 0$ passing through $(0,0)$. The key point is to expand y as a Puiseux series in x; these were first invented by Newton. These are essentially Taylor series in $x^{1/N}$ for some integer N.

Example 145. If for example $y^2 = x^2 + x^4$, we have two branches $y = x + *x^2 + *x^3 + \cdots$, $y = -x + \cdots$, so in this case the Puiseux series is just a Taylor series.

If for example $y^2 = x^3 + x^4$, we have $y = (x^3 + x^4)^{1/2} = x^{3/2}(1+x)^{1/2}$, which gives a Taylor series in $x^{1/2}$.

In general, one finds the Newton polygon. Consider for example $y^5 + 7x^3y^2 + 6x^5y^4 + 7x^6 = 0$. One looks at which monomials $x^a y^b$ occur, and plots the values of $(a,b) \in \mathbb{Z}^2$. One takes the convex hull of these points together with $(\infty, 0)$ and $(0, \infty)$ as in Fig. 27. We assume that the curve $f(x,y) = 0$ is irreducible, so it contains monomials y^b and x^a for some a, b (otherwise it would be divisible by x or y), so the Newton polygon contains some points on the y-axis and x-axis.

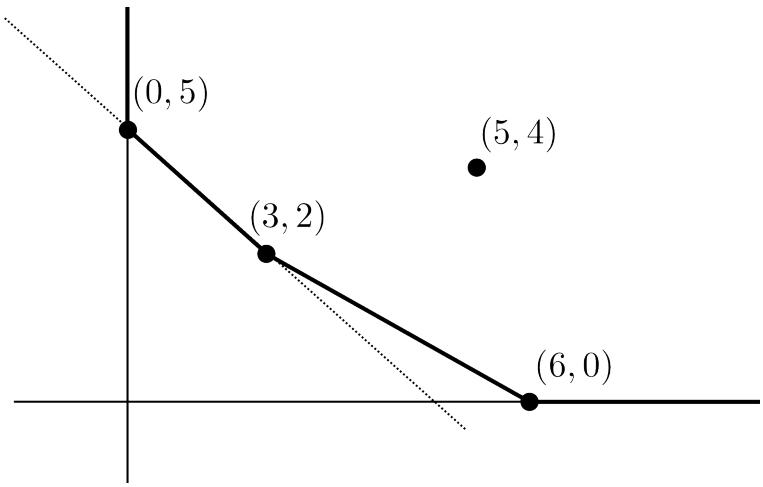


Figure 27: The Newton polygon of $y^5 + 7x^3y^2 + 6x^5y^4 + 7x^6 = 0$ consists of part of the first quadrant. The leading edge is illustrated with the dotted line.

We now use Newton's method of the rotating ruler: Rotate a ruler through the point $(0,b)$ until it hits some point; this gives the edge of steepest slope of the Newton polygon. On the resulting line of steepest slope, there will be at least 2 points, and all the points in the Newton polygon are on one side of the line – see Fig. 27.

Now, look at the piece of $f(x,y)$ on this line. In other words, we can choose a grading of polynomials in x, y, $\deg(x) = m$, $\deg(y) = n$, such that the monomials on the line all have the same degree, and the slope of the line is $-m/n$ (or maybe $-n/m$). So we are looking at the terms of smallest degree for this grading.

Example 146. Consider $y^5+7y^4x^2+6y^3+x^4+y^3x^7+y^7x^3+x^{18}$. In this case the terms of minimal degree will be the first three, $y^5+7y^4x^2+6y^3x^4$.

We want to make changes of variables in x, y to simplify the Newton polygon. This can mean two things: We will either reduce the smallest power of y (if we can get a y^1, the curve is non-singular, and y is a Taylor series in x), or we reduce the slope of the leading line from before. To do this, we look at the terms of smallest degree. This is a homogeneous polynomial in x, y for suitable weights of x, y (for instance, in the example above, the degree of y is 2, and the degree of x is 1). Look at the roots of this homogeneous polynomial; there are two cases: (1) Not all roots are equal. (2) All roots are the same. If not all the roots are the same, we have $(y^a-\alpha_1 x^b)(y^a-\alpha_2 x^b)\cdots$, where not all the α_i are the same. We then make a substitution, say $y \mapsto y-\alpha_1 x^{b/a}$, which will reduce the minimum power of y occuring. This can only happen a finite number of times. If all the roots are equal, $(y^a-\alpha x^b)^N$, and we substitute $y \mapsto y-(\alpha x^b)^{1/a}$, the power of y does not decrease, but the absolute value of the slope of the leading edge does. This can happen an infinite number of times, as the slope of the leading edge is rational. But it does at least converge to a formal Puiseux series for $y=\sum a_n x^{n/N}$. (A slight variation of this actually shows that the field of formal Puiseux–Laurent series, series of the form $\sum_{n\geq -k} a_n x^{n/N}$ for some integer N, is algebraically closed. To prove this, one uses a similar argument, except that f is allowed to be a Puiseux series in x rather than just a polynomial. This is a rare example of an explicit algebraically closed field other than $\mathbb{C}$. It also shows that the field of Laurent series $\sum_{n\geq -k} a_n x^n$ $(a_n \in \mathbb{C})$ is a *quasi-finite field* – this is, a field that has a unique extension of degree n for any n. For example, for finite fields $\mathbb{F}_q$, there are unique extensions $\mathbb{F}_{q^n}$ of degree n; this means that one can compute the Galois group of its algebraic closure, $\varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$.)

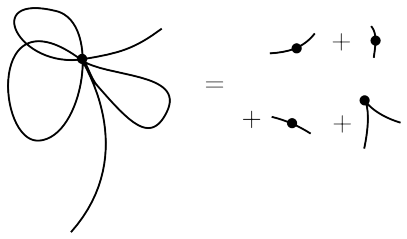


Figure 28: Seperating out the branches of a singularity.

Newton's algorithm is the following: Given a polynomial $f(x,y)$, it will produce a root the form $y=\sum_{n\geq 0} a_n x^{n/N}$ for some N. So what does this have to do with resolution of singularities? Suppose we have a polynomial $f(x,y)=0$ singular at 0. Newton's algorithm will then "seperate out" the various analytic branches (Fig. 28). Each analytic branch looks like $y=\sum a_n x^{n/N}$ or $y^N=\sum b_n x^n$. However, *different* analytic branches may be the *same* algebraic branch. For example, if $y^2=x^2+x^3$ has two analytic branches at the origin, but there is only one algebraic branch.

So, to resolve singularities, we want to find invariants of a singularity, that are improved by blowing up. Suitable invariants are:

(1) The multiplicity of the singularity.

(2) The minimal value of the leading slope of the Newton polygon taken over all choices of local analytic coordinates, such that y^N is the term of minimal degree, and there are no terms of the form $y^{N-1}x^m$ for any m; such terms can be eliminated in characteristic 0 by changing variable $y \mapsto y+$ power series in x, since then $y^N \mapsto y^N+N(y^{N-1}x)+\cdots$. (For curves this restriction to characteristic 0 is not hard to avoid, but in higher dimensions, a similar problem is the obstruction to resolution of singularities in characteristic >0.)

We consider now the effect of blowing up on these invariants. This depends as usual on the roots of the polynomial of terms of smallest degree: If the roots are not all the same, the multiplicity

of the singularity is reduced (corresponding to what happens in Newton's algorithm) – this only happens a finite number of times. When all the roots are the same, then the absolute value of the slope of the leading edge is less than 1, as the coefficient of $y^{N-1}x = 0$. Then, blowing up increases the absolute value of the slope of the leading edge. If the absolute value of the slope is > 1, the multiplicity is reduced (without this condition, the coefficients of $y^{N-1}x^m$ vanish, and we end up going in circles).

23rd lecture, November 16 2010

7 Hilbert polynomials

Today we will consider Hilbert polynomials. The basic problem is the following: Suppose we have a module M over some ring, say $k[x_1, \ldots, x_m]$; how do we measure the "size" of M? We do this by *grading* M, writing $M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots$ and grading $k[x_1, \ldots, x_m]$ by letting, say, $\deg x_i = 1$.

Assume that M is a graded module over a graded ring $k[x_1, \ldots, x_m]$. This means that $\deg(pm) = \deg p + \deg m$, where $m \in M_i$, and $p \in k[x_1, \ldots, x_m]$. The idea is to look at the growth of $\dim(M_i)$ (this is finite-dimensional if M is a finitely generated module over $k[x_1, \ldots, x_m]$). We do this by encoding $\dim(M_i)$ as a power series. Put

$$f_M(t) = \sum_n t^n \dim(M_n).$$

Hilbert's key discovery was that $f_m(t)$ is a power series of a *rational function*. The only pole is at $t = 1$. This gives us tight control over the growth of $\dim M_i$, as the rational function can be specified by a finite amount of information. This can be proven by induction on the number of generators of $k[x_1, \ldots, x_m] = R$. Suppose r is one of the generators of the ring R. Look at the sequence

$$0 \to \ker(r) \to M \to M(1) \to M(1)/rM(1) \to 0,$$

where $M(1)$ is M with the grading shifted by 1, and the third map is multiplication by r. This is an exact sequence of graded modules. We now use the following fact: If

$$0 \to V_0 \to V_1 \to \cdots \to V_k \to 0$$

is an exact sequence of vector spaces, then $\dim(V_0) - \dim(V_1) + \dim(V_2) - \cdots = 0$. (This is a special case: The Euler characteristic of a complex is the Euler characteristic of the homology.) It can be proved directly by induction on the number k of vector spaces in the sequence. Applying this to our sequence above, we get that $f_{\ker(r)} - f_M + f_{M(1)} - f_{M(1)/rM(1)} = 0$. We consider the various bits: $f_{\ker(r)}$ is a graded module over the ring with $< m$ generators, so it is rational by induction on m. Also, $f_{M(1)}$ differs from f_M by a factor of x, and so does $f_{M(1)/rM(1)}$ [?]. So we find that $(1-t)f_M$ is a rational function, and so f_M is a rational function. By induction, the only poles are at $t = 1$. (A slight generalization is this: In the previous case we assume that all generators have degree 1. If more generally the generators have degrees n_i, then we get a rational function $(1-t^{n_i})f_M$, so f_M can have poles at the zeros of $(1-t^{n_1})(1-t^{n_2})\cdots$.)

An immediate consequence is that for n sufficiently large, $\dim(M_n)$ is a polynomial in n. This follows, since it is true for the coefficients of any rational function with poles only at $t = 1$: We can write $f_M(t)$ as a Laurent series

$$\frac{b_{-k}}{(1-t)^k} + \frac{b_{1-k}}{(1-t)^{k-1}} + \cdots + b_0 + b_1(1-t) + \cdots + b_*(1-t)^*,$$

and the coefficient of t^n is 0 for $n \gg 0$. We have

$$\frac{1}{1-t} = 1 + t + t^2 + \cdots$$
$$\frac{1}{(1-t)^2} = 1 + 2t + 3t^2 + \cdots$$
$$\frac{1}{(1-t)^3} = 1 + 3t + 6t^2 + 10t^3 + \cdots,$$

and here the coefficients for postive powers of t are given by polynomials (note that they come from Pascal's triangle).

The polynomial $\dim(M_n)$ (for n large) is called a Hilbert polynomial $P(t)$. These polynomials have the following special property: $P(n)$ is *integer* (that is, it takes integer values on integers) for $n \gg 0$ (so $\dim(M_n)$ is integer). So we can ask the following: What polynomials are non-negative integers for n a large integer? This is the case if all coefficients of p are integers, but this does not give all cases. For example, $\frac{t(t-1)}{2} = -\frac{t}{2} + \frac{t^2}{2}$ is an integer for all integers t. In general, that p takes integer values on the integers is equivalent to p being an integral linear combination of expressions of the form $\frac{t(t-1)\cdots(t-(n-1))}{n!}$ (note that these are all binomial coefficients, and therefore integral linear combination of these terms gives an integer polynomial). To prove this, note that the expression above is 0 at $0, \ldots, n-1$ and 1 at n. Suppose that p is integral on integers. We want to show that p is an integral combination of polynomials as above. First, change p to $p - p(0) = p_1$, which vanishes at 0. Now, change p_1 to $p_1 - p_1(1)\binom{t}{1} = p_2$, which vanishes at 0,1. Carry on like this to find p minus some linear combination of $\binom{t}{0}, \binom{t}{1}, \binom{t}{2}, \ldots, \binom{t}{n}$ vanishing at $0, 1, \ldots, n$, where $n = \deg(p)$. So we have a polynomial of degree n vanishing at $n+1$ points $0, \ldots, n$, so it is 0. Thus p is a linear combination of $\binom{t}{0}, \binom{t}{1}, \binom{t}{2}, \ldots, \binom{t}{n}$ with integer coefficients. This ends the proof.

In particular, suppose p is integral for integral t, then $p = \frac{a_n}{n!}t^n +$ (smaller degree), where a_n is an integer. The most important invariants of the Hilbert polynomial are (1) its degree n and (2) its leading coefficient times $n!$. These are both integers ≥ 0. (The remaining coefficients tend to depend on the choice of grading.)

An application of this is that we can define the dimension of Noetherian local rings.

(1) Suppose R is a Noetherian local ring with maximal ideal m (for instance, it might be the coordinate ring of some variety localized at the point, so the dimension would be the dimension of the variety at that point). We will turn it into a graded ring. Filter it, taking $R/m \oplus m/m^2 \oplus m^2/m^3 \oplus \cdots$. Here R/m is a field k, and the other terms are finite dimensional vector spaces over k, generated by the degree 1 elements. It is a module over itself, so we can take the Hilbert polynomial of it. A Hilbert polynomial measures the growth of $\dim(m^n)$ which you can think of as "how many functions there are on the variety". In fact, $\dim(R)$ is equal to the degree of the Hilbert polynomial of $\dim(m^n)$, which is also 1 plus the degree of the Hilbert polynomial of m^n/m^{n+1}. There are also other definitions of dimensions of Noetherian local rings.

(2) Another one is as the supremum of lengths of chains of prime ideals $p_0 \subset p_1 \subset \cdots \subset p_n$ (where $p_i \neq p_{i+1}$).

(3) You can also define it as the smallest size of a system of parameters: The set of elements of m generating an ideal of finite codimension (which may be less than the minimum of number of generators of m).

The proofs of their equivalence is quite hard commutative algebra. The definition in terms of Hilbert polynomials seems less intuitive but is easier to calculate than the two others.

As an example, we consider the degree of a projective variety. An informal definition is, that for a hypersurface, the degree should be the number of intersections with a "generic" line. If V has codimension r in P^n, then $\deg(V)$ is the number of intersection points of V with a *generic* linear subvariety of dimension r. We need the word "generic": For example for the cubic surface $w^3 + x^3 + y^3 + z^3 = 0$, most lines intersect in 3 points, while some lines lie on the surface and intersect it in an infinite number of points. This definition of degree is intuitive and geometric, but one runs into technical difficulties.

Instead, we give a definition of degree in terms of Hilbert polynomials. Suppose I is a graded ideal of a variety $V \subseteq P^n$, $I \subseteq k[x_0, \ldots, x_n] = R$. Then $M = R/I$ is a graded module over $k[x_0, \ldots, x_n]$, $\dim(V)$ is the degree of the Hilbert polynomial of M, and $\deg(M)$ is $r!$ times the leading coefficient of the Hilbert polynomial, which as before is a positive integer.

Example 147. Consider projective space P^n. Here the coordinate ring is $k[x_0, \ldots, x_n] = R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$. In the last expression, the dimensions are 1, $n+1$, $\binom{(n+1)(n+2)}{2}$, and so on. In general, R_k has dimension $\binom{(k+n)(k+n-1)\cdots(n+1)}{k}$. The Hilbert polynomial is $\binom{k+n}{n} = 1 \cdot \frac{k^n}{n!} +$ lower order terms. We read off that P^n has dimension n and degree 1.

Example 148. Consider a hypersurface of degree d in P^n, so consider f of degree d in $k[x_0, \ldots, x_n]$. We have an exact sequence

$$0 \to k[x_0, \ldots, x_n] \xrightarrow{f} k[x_0, \ldots, x_n] \to k[x_0, \ldots, x_n]/(f) \to 0.$$

Multiplication by f raises the degrees by d. Here, the Hilbert polynomial is

$$\binom{k+n}{n} - \binom{k+n-d}{n} = d\frac{k^{n-1}}{(n-1)!} + \text{lower order terms.}$$

So in this case, the hypersurface has dimension $n-1$ and degree d the degree of the polynomial f defining it.

Example 149. Consider a twisted cubic in P^3. This is defined by the ideal $(wz - xy, x^2 - wy, y^2 - xz)$ in $k[w, x, y, z]$. Then the graded coordinate ring of the twisted cubic is $k[w, x, y, z]/(wz - xy, x^2 - wy, y^2 - xz)$. By converting $x^2 \to wy$, $y^2 \to xz$, $xy \to wz$, we can assume that we have ≤ 1 copy of x or y. We have the following possible monomials in various degrees:

Degree	0	1	2	3
Polynomials	1	w, x, y, z	$w^2, z^2, wz, wx, wy, zx, zy$	$w^3, w^2z, wz^2, z^3, \ldots$
Number of polynomials	1	4	7	10

In general, there are $3k^1 + 1$ polynomials of degree k. It follows that the twisted cubic has dimension 1 and degree 3.

We can ask why the Hilbert polynomial is not always equal to M_k; it turns out that $\dim(M_k) = \dim H^0(\mathcal{O}(M)(k))$, where $\mathcal{O}(M)(k)$ is a certain sheaf on P^n associated to M. The Hilbert polynomial is always the Euler characteristic of $\mathcal{O}(M)(k)$, given by an alternating sum of dimensions of cohomology groups of the sheaf.

Example 150. The Euler characteristic χ of a variety can be defined as the constant term of the Hilbert polynomial. For historical reasons, some people consider the *arithmetic genus* $(-1)^{\dim}(\chi - 1)$. As an example, we consider a plane curve of degree d. It is a degree d hypersurface in P^2, so the Hilbert polynomial is $\binom{k+2}{2} - \binom{k+2-d}{2}$. The constant term is $\binom{2}{2} - \binom{2-d}{2} = 1 - \frac{(2-d)(1-d)}{2} = \chi$, so the arithmetic genus is

$$1 - \chi = \frac{(2-d)(1-d)}{2} = \frac{(d-1)(d-2)}{2},$$

which is the same as the topological genus for non-singular curves over $\mathbb{C}$, explaining the name.

The Hilbert polynomial is essentially the only discrete invariant of algebraic sets in P^n: Hartshorne proved that 2 algebraic sets with the same Hilbert polynomial are in the same component of the "Hilbert scheme", so Hilbert polynomials roughly describe components of the Hilbert scheme (which is where the name of Hilbert schemes come from).

24th lecture, November 18 2010

8 Sheaves and schemes

A scheme is a generalization of an algebraic set. As we have seen, affine algebraic sets correspond to finitely generated algebras over a field with no nilpotents. A projective algebraic set is a subset of projective space covered by affine algebraic sets. Schemes are similar, but:

(1) We do not insist on finite generation. For example, we could use $k[x_1, x_2, \dots]$ in infinitely many variables. These correspond *roughly* to infinite-dimensional objects.

(2) They do not to be over a field. For instance we can work over $\mathbb{Z}$. As an example, considering $x^n + y^n = z^n$ one could ask for integral solutions rather than complex, and one would work with $\mathbb{Z}[x, y, z]/(x^n + y^n - z^n)$.

(3) The most dramatic change is that we allow nilpotents. One reason for this is that things with nilpotents turn up naturally. As an example, consider the intersection of the parabola $y = x^2 - a$ with the line $y = 0$. This intersection is an algebraic set consisting of the points $x = \pm\sqrt{a}$, which is 2 points if $a \neq 0$, and 1 if $a = 0$. We look at the coordinate ring of the intersection: $k[x, y]/(y, (x^2 - a)) = k[x]/(x^2 - a)$. If $a \neq 0$ this is $k \oplus k$, and if $a = 0$ this is $k[x]/(x^2)$, which is a 2-dimensional algebra over k with a nilpotent – the scheme keeps track of this extra information. (Remark: One could consider superspaces. These are essentially $\mathbb{Z}/2\mathbb{Z}$ graded spaces: One works with elements in a ring $R_0 \oplus R_1$ which are supercommutative, $xy = (-1)^{\deg x \deg y} yx$, so if $\deg x = 1$, we have $x^2 = -x^2$, and so x is nilpotent)

So, for affine schemes we consider all rings rather than rings finitely generated over k with no nilpotents. Similarly, general schemes are things that are covered by affine schemes – we don't consider things embedded into say P^n. One could compare this to the modern definition of a manifold: Previously, one considered manifolds as things embedded in Euclidean space, but this embedding is usually irrelevant.

8.1 Sheaves

Sheaves were invented by Leray in the 1950s. They were initially used for smooth Hausdorff manifolds and were introduced into algebraic geometry by Serre (in [Ser]). A key point is that sheaves also work on non-Hausdorff spaces. Before introducing sheaves, we introduce presheaves.

As an example, take a topological space X. For each open set U let $F(U)$ be the set of continuous real functions on U. F is a basic example of a sheaf. We extract the key properties of this example.

(1) For each $U \subseteq V$, we have a restriction map $\rho_{VU} : F(V) \to F(U)$ such that ρ_{UU} is the identity and $\rho_{VW}\rho_{UV} = \rho_{UW}$

This defines a *presheaf*: The data of a presheaf F is a set $F(U)$ for every open $U \subseteq X$ with a map $\rho_{UV} : F(U) \to F(V)$ for $V \subseteq U$ satisfying the above condition (1).

An alternative definition is the following: We form a category from X, letting the objects be the open sets $U \subseteq X$ with morphisms inclusions $U \subseteq V$ (so there is one morphism $U \to V$ if $U \subseteq V$ and no morphisms otherwise). Then a *presheaf* is a contravariant functor F from this category to the category of sets. We then have a set $F(U)$ for each object U and a morphism of sets $\rho_{UV} : F(V) \to F(U)$ whenever we have an inclusion $U \to V$. We can also define a presheaf of

"things", whenever we are given a category of "things". Important examples are sheaves of abelian groups and sheaves of sets.

There are extra properties of a presheaf F of continuous functions of $U \subseteq X$.

(1) Suppose U is covered by sets $\{U_i\}$, then if $\rho_{UU_i}(f) = \rho_{UU_i}(g)$ for all i, then $f = g$.

(2) Suppose that given $f_i \in F(U_i)$ and $U = \bigcup U_i$. Then, whenever $\rho_{U_i, U_i \cap U_j}(f_i) = \rho_{U_j, U_i \cap U_j}(f_j)$, we can find $f \in F(U)$ such that $\rho_{UU_i}(f) = f_i$. By the first condition, f is unique.

A *sheaf* is a pre-sheaf satisfying the above conditions (1) and (2).

Example 151. A basic example in algebraic geometry is the following: Let X be an algebraic set or variety, and $F(U)$ the regular functions on U.

Sheaves and presheaves form a category. Morphisms of sheaves/presheaves are the same as natural transformations of functors: I.e. a morphism $F \to G$ is given by maps $F(U) \to G(U)$ such that the following diagram is commutative:

$$\begin{array}{ccc} F(U) & \longrightarrow & G(U) \\ \downarrow & & \downarrow \\ F(V) & \longrightarrow & G(V) \end{array}$$

Sheaves form a (full) subcategory as presheaves.

Grothendieck's philosophy of sheaves is that sheaves over a space form a weak model of set theory: Any "constructive" operation on sets should have an analogue for sheaves. Given sets A, B, one can form a product $A \times B$, a union $A \cup B$, maps A^B from B to A, the power set of A, and so on. All of these have analogues for sheaves. In particular, we can define rings, groups, etc., in the category of sheaves. Sheaves of abelian groups should then behave like abelian groups.

Example 152. Given abelian groups A, B, we can form $A \oplus B$, $A \otimes B$, $\mathrm{Hom}(A, B)$ and so on, so there are similar operations for sheaves.

There are two important differences between sets and sheaves of sets though: The analogue of the axiom of choice fails, and classical logic fails. Sheaves use "intuitionistic logic". A more technical way of saying this is that the category of sheaves form a *topos*. This also means that any set theoretical proof that uses only intuitionistic logic has an analogue for sheaves.

Example 153. We could consider sheaves of continuous/smooth/regular/holomorphic functions on topological spaces/manifolds/algebraic varieties/complex manifolds.

Example 154. Pick a group A and a point x in X. Define the *skyscraper sheaf* F by $F(U) = A$ if $x \in U$ and $F(U) = 0$, if $x \neq U$. The picture is that we have s copy of the group A sitting over the point x. This is a special case of something more general: Suppose $Y \to X$ is any continuous map. Let $F(U)$ consist of the sections of this map over U – this is a sheaf as well. In fact we can get all sheaves like this.

Example 155. Another example is the *constant presheaf*: Fix an abelian group A and let $F(U) = A$ for all U. This is usually *not* a sheaf. Similarly, let A be an abelian group with the discrete topology and define the *constant sheaf* by letting $F(U)$ be the set of continuous functions from U to A. This is the same as the constant presheaf if U is connected, but in general the two are not the same.

The above example leads to the problem of turning a presheaf into a sheaf. First, you form the étalé space of a presheaf: The *fiber* F_x of a point x is defined to be $F_x = \varinjlim_{U \ni x} F(U)$. Informally, these are functions defined "near" x.

Example 156. If $X = \mathbb{R}$ and F is the sheaf of continuous functions, then the fiber at x is the set of continuous functions defined near x with the relation that $f \equiv g$ if $f = g$ in a neighbrhood of x.

The *étalé space* is the union of the fibers over X. We put a (typically not Hausdorff) topology on this: If $f \in F(U)$, then f has an image in F_x for each $x \in U$, so we get a map from X to the étalé space. The basis of open sets is given by the open sets U under these maps. We define a sheaf F^+ letting $F^+(U)$ be the sections of the étalé space over U.

Exercise 157. Do the above construction for F the constant presheaf, and show that the result is the constant sheaf. Show that if F is the sheaf of continuous functions on $\mathbb{R}$, then the étalé space is not Hausdorff. Show that if F is the holomorphic functions on $\mathbb{C}$, then the étalé space is Hausdorff.

If one applies the above construction to a sheaf, the result will be the same sheaf as one begins with, up to isomorphism, and one can think of étalé spaces as giving a canonical retraction of presheaves to sheaves.

Sheaves generalize vector bundles. For example, Suppose X is a smooth manifold. It has a tangent bundle TX assigning to each point the tangent space. We get a sheaf of tangent vector fields, by putting $F(U)$ equal to the vector fields on U. Vector bundles are not general enough for our purpose (for example, vector bundles form an additive category, which is not abelian, while sheaves form an abelian category. The problem is illustrated by the following example).

Example 158. Take X to be the real line. Let V be the vector bundle $X \times \mathbb{R} \to X$. Sections of the vector bundle is simply real functions. Now look at $V \xrightarrow{x} V$ given by multiplication by $x \in \mathbb{R}$. What is the kernel and cokernel of this map? The kernel is easy enough: If $xf = 0$ then $f = 0$, so the kernel is 0. The cokernel has fiber 0 at $x \neq 0$, so the cokernel as a vector bundle would have to be 0. So from the point of view of vector bundles, $V \xrightarrow{x} V$ has zero kernel and co-kernel, but it is not an isomorphism. For example, the section 1 of V is not in the image of x, so vector bundles do not form an abelian category.

But for sheaves, the map $V \xrightarrow{x} V$ has a non-zero cokernel. Notice that the quotient F_0/xF_0 – i.e. the smooth functions near zero modulo the smooth functions vanishing at 0 – is nothing but the skyscraper sheaf at 0.

25th lecture, November 23rd 2010

8.2 The spectrum of a ring

Schemes were invented in the 1950's, after much experimentation by Weil, Zariski, Chevalley, and Grothendieck, to find a replacement for the inadequate notion of a projective variety. Some propositions were Abstract varieties (by Weil) and Zariski surfaces (confusingly called Riemann surfaces by Zariski), and finally schemes. They were named by Chevalley. There are various generalizations, to for example algebraic spaces (introduced by Artin), toposes (by Grothendieck) and stacks (also by Grothendieck).

Affine schemes are locally ringed spaces: We need to construct the underlying space, construct a sheaf of rings on it, and figure out what "locally" means. Affine schemes correspond to commutative rings. For a commutative ring R we will define an affine scheme called the spectrum, $\mathrm{Spec}(R)$, of R. The reason for the name "spectrum" is the following. Remember that the spectrum of an operator is the set of its eigenvalues. Let the operator be A acting on (say) a finite dimensional complex vector V, so the spectrum is the set of values $\lambda \in \mathbb{C}$ with $Av = \lambda v$ for some $v \in V$, $v \neq 0$. In our case, look at the commutative ring $\mathbb{C}[A]$ consisting of all operators that are polynomials in A. This is some finite dimensional commutative algebra. Notice now that the spectrum of A corresponds to the maximal ideals of $\mathbb{C}[A]$. If we have an eigenvector v we get a maximal ideal I of $\mathbb{C}[A]$ equal to the elements that vanish on v, and we get a homomorphism $\mathbb{C}[A] \to \mathbb{C}$ mapping p to the eigenvalue of $p(A)$ acting on V.

This is extended by Gel'fand in the theory of commutative C^*-algebras. Suppose X is a compact Hausdorff space. Look at the ring $R = C(X)$ of continuous functions on X. We can then ask how to reconstruct X from R. The answer is that X is the set of maximal ideals of the ring R. A point $x \in X$ gives a maximal ideal by associating to it the maximal ideal of functions vanishing at x. We have a topology on the space of maximal ideals: If $f \in C(X)$, then the maximal ideals containing f form a closed set (which we can think of as the zeros of f). The topology is generated by the complements of these. So, for each f we have an open set U_f of the maximal ideals not containing f. Here, we get a correspondence between compact Hausdorff spaces X with commutative C^*-

algebras. associating to a C^*-algebra R the set $\mathrm{Spec}_m(R)$ of its maximal ideals, and going in the other direction by taking continuous functions.

The idea in algebraic geometry is to do this construction for commutative rings rather than C^*-algebras. By Hilbert's Nullstellensatz, the points of a variety V correspond to the maximal ideals of the coordinate ring of V, so varieties correspond to finitely generated integral domains over k. Here, given a finitely generated integral domain R, we associate to it the set $\mathrm{Spec}_m(R)$ of its maximal ideals, and we can go the other way by taking coordinate rings. A homomorphism $f : R \to S$ between commutative C^*-algebras induces a homeomorphism $\mathrm{Spec}_m(S) \to \mathrm{Spec}_m(R)$. For general rings, this *fails*: Suppose $f : R \to S$ is a ring homomorphism, and define $F^* : \mathrm{Spec}_m(S) \to \mathrm{Spec}_m(R)$ by letting $f^*(I)$ be the inverse image of I, where I is a maximal ideal of S. We have the following problem: The inverse image of a maximal ideal need not be maximal. For example, for $f : \mathbb{Z} \to \mathbb{Q}$, the pre-image of the maximal ideal (0) in $\mathbb{Q}$ is not maximal in $\mathbb{Z}$. Note that a maximal ideal S corresponds to a homomorphism from S *onto* a field k, and the composition $R \to S \to k$ need not be onto, but its image is certainly an integral domain. So while the inverse image of a maximal ideal need not be maximal, but it is prime, and the inverse image of a prime ideal is always prime, so this indicates that instead of using maximal ideals, we should use prime ideals.

Definition 159. The points of $\mathrm{Spec}(R)$ correspond to prime ideals of R. Its topology is given by copying the definition of the topology on $\mathrm{Spec}_m C[X]$: The topology has a basis of open sets $D(f) = U_f$, the set of prime ideals not containing f (for $f \in R$). (Think of f as a "function" on $\mathrm{Spec}(R)$, and U_f the points where "$f \neq 0$".)

A *key* idea is to ignore all open sets not of the form $D(f)$, which will often simplify constructions.

Example 160. For R a field k the spectrum is just a point.

Example 161. If R is $\mathbb{Z}$, it has prime ideals $(0), (2), (3), \ldots$, where all but the first of these ideals are maximal. We can find the closed sets. If $f \in \mathbb{Z}$, $f \neq 0$, then $D(f)$ is the set of prime ideals not containing f, which is the set $(0) \cup (p)$ for $p \nmid f$, which is the complement of any finite set of $(2), (3), (5), \ldots$. Notice that this is not Hausdorff: Any 2 non-empty open sets intersect. Even worse, it has a non-closed point, (0).

Exercise 162. The closed points of $\mathrm{Spec}(R)$ correspond to maximal ideals, so all the extra non-maximal prime ideals are non-closed.

Example 163. Let $R = C(X)$ be the set of continuous functions on a compact Hausdorff space. The closed points of $\mathrm{Spec}(R)$ are all the points of X. The non-closed points are weird; they involve ultrafilters. (The moral of this is example is that you shouldn't mix analysis and algebraic geometry too much.)

Example 164. Let R be the ring $\mathbb{C}[x]$ of polynomials in x. This has maximal ideals the points of A^1. There is just one non-maximal prime ideal, (0) (in general, this occurs for any principal ideal domain). This looks like a copy of $\mathbb{C}$ (with the Zariski topology) together with a dense generic point (0).

Example 165. Consider now $\mathbb{C}[x, y]$. Prime ideals in this case are points (x, y) (giving maximal ideals), ideals (f), for f irreducible, and (0).

Example 166. Consider a discrete valuation ring such as $\mathbb{Z}_{(p)}$, of all rational numbers m/n with $p \not| n$, or the ring $k[[x]]$ of formal power series in x, or $\mathbb{Z}_p$ the p-adic numbers. In each of these cases there is just one non-zero prime p, and every element is a unit times p^n for $n = 0, 1, 2, \ldots$.

So, there are just 2 prime ideals, the maximal ideal (p) and the non-maximal (0). Here the topology consists of 3 open sets: $\emptyset$, $\{(0), (p)\}$, and $\{(0)\}$, which is the "Kuratowski topology" of a 2 point set.

Example 167. Consider $\mathrm{Spec}\,\mathbb{Z}[x]$. First, notice that the map $\mathbb{Z} \to \mathbb{Z}[x]$ gives a map $\mathrm{Spec}\,\mathbb{Z}[x] \to \mathrm{Spec}\,\mathbb{Z}$, and we know what $\mathrm{Spec}\,\mathbb{Z}$ is. We can analyze $\mathrm{Spec}\,\mathbb{Z}[x]$ by looking at the fibers of this map. In other words, we find the prime ideals whose intersection with $\mathbb{Z}$ is $(2), (3), (5), \ldots, (0)$. Consider first the fiber at (0): The prime ideals of $\mathbb{Z}[x]$ whose intersection with $\mathbb{Z}$ is (0) are the

prime ideals of $\mathbb{Q}[x]$, which is a discrete valuation ring, so the prime ideals are (0), and (f) for $f \in \mathbb{Z}[x]$ irreducible. We can think of this as the orbit of algebraic numbers under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. So, just to describe the fiber over (0) we need the theory of algebraic numbers. Next, consider the fiber over (p). These are prime ideals of $\mathbb{Z}[x]$ containing $p \in \mathbb{Z}$. These are the same as the prime ideals of $\mathbb{F}_p[x]$. Again, this is a discrete valuation ring, so prime ideals are (0) and orbits of $\bar{\mathbb{F}_p}$ under $\mathrm{Gal}(\bar{\mathbb{F}_p}/\mathbb{F}_p)$. These correspond to irreducible polynomials of $\mathbb{F}_p$. One then goes on to considering the closures of points of $\operatorname{Spec}\mathbb{Z}[X]$. It turns out that these closures are 1-dimensional subspaces of $\operatorname{Spec}\mathbb{Z}[X]$ at generic points. A natural question then is where these 1-dimensional subspaces intersect: For example, the closures of (x^2+1) and $(x-5)$ intersect at two points, so we want to find all prime ideals containing $x-5, x^2+1$. We see that $x=5$, $x^2+1=0$ implies that $26=0$, so we must be working modulo 2 or 13, and the ideals are $(2, x-1), (13, x-5)$. The point is that one should think of $\operatorname{Spec}\mathbb{Z}[x]$ as being similar to a 2-dimensional variety.

26th lecture, November 30 2010

We begin with a strange example of an affine scheme.

Example 168. We consider Nagata's counterexample to almost everything: This is an infinite dimensional Noetherian scheme. Take the ring $k[x_1, x_2, \dots]$ and look at prime ideals $(x_1), (x_2, x_3), (x_4, x_5, x_6), \dots$, and invert everything not in one of these ideals. Call the result R. The ideals above then become maximal ideals of R. Any prime ideal is generated by irreducibles, so by elements in just one of the ideals $(x_1), (x_2, x_3), \dots$. So all prime ideals are finitely generated, and by a theorem by Cohen this implies that all ideals are finitely generated, so R is Noetherian. On the other hand, it is infinite dimensional, as it contains arbitrarily long chains of prime ideals, e.g. $(x_2) \subseteq (x_2, x_3)$, $(x_4) \subseteq (x_4, x_5) \subseteq (x_4, x_5, x_6)$ and so on.

There are lots of variations of this idea. One is a 1-dimensional integral domain with all points singular: Take a subring of $k[x_1, \dots]$ generated by x_i^2, x_i^3 for all i. Again, invert everything not in of the ideals (x_i^2, x_i^3). This forces (x_i^2, x_i^3) to be the maximal ideals. (But all local rings at these points are singular: They look like the local ring of a cusp $x^2 = y^3$ over a field of ∞ transcendence degree.)

So the main problem is how to avoid examples like the above ones. We want to find a definition of a "nice" ring that includes all geometric examples and excludes all "pathological" examples. One possible answer (by Grothendieck) is the concept of an *excellent ring*, which we won't discuss.

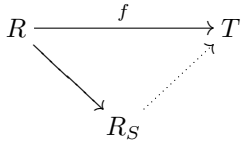
We consider now some basic properties of $\operatorname{Spec}(k)$.

(1) Every irreducible closed set is the closure of a unique point: If S is a closed set of prime ideals, then it is a set of prime ideals containing their intersection I. If I is not prime, then choose $a, b \notin I$, $a \in I$, $b \in I$. Then S is the union of primes containing (I, a), and (I, b), so S is not irreducible. If S is irreducible, it is the set of primes containing prime I, so it is the closure of a point corresponding to I, and so irreducible closed subsets correspond to points.

(2) $\operatorname{Spec}(R)$ is always compact. This follows from the fact that if some set of elements generate the unit ideal, then some finite subset generates the unit ideal.

8.3 Schemes

Now, we will make $\operatorname{Spec}(R)$ into a ringed space. That is, for every open subset, we want to define a ring $\mathcal{O}(U)$. To do this, we first recall the localization R_S of a ring R at a subset S. Informally we just invert all elements of S. Consider the following universal property: Suppose R has a homomorphism to a ring T such that the image of all elements of S are invertible. Then the ring R_S is defined by the property that for any $R \to R_S$ there exists a map $R_S \to T$ forming a commutative diagram



So, R_S is a "universal ring" with everything in S invertible. The existence is obvious: We could simply take $\frac{R[t_1,t_2,\dots]}{s_1t_1=1,s_2t_2=1,\dots}$ for all $s_1, s_2, \dots \in S$. This construction however, is useless: We have no control over the ring, and for example it is hard to see, what the kernel of $R \to R_S$ is.

To obtain a better construction, we mimic the construction of $\mathbb{Q}$ from $\mathbb{Z}$, noting that $\mathbb{Q}$ is the localization at $\mathbb{Z}$ at all non-zero integers. Recall that $\mathbb{Q} = \frac{\mathbb{Z}\times\mathbb{Z}}{(r_1,s_1)\equiv(r_2,s_2) \text{ if } s_1r_2=s_2r_1}$. We can then define $+, \cdots, -$ as always, letting $(r_1, s_1) + (r_2, s_2) = (r_1s_2 + r_2s_1, s_1s_2)$ and $(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$.

Trying to copy this for any subset S of a ring R, we run into problems:

(1) The relation $\equiv$ from above will not define an equivalence relation. This we can fix by demanding that S is closed under multiplication (for exmaple, we can replace S by the set of finite products, and 1)

(2) S might have zero divisors. This we can fix by modifying $\equiv$, and saying that $(r_1, s_1) \equiv (r_2, s_2)$, if $s(r_1s_2 - r_2s_1) = 0$ for some $s \in S$.

A check shows that the equivalence classes form a ring R_S with the universal property. One key advantage is that we can describe the kernel of $R \to R_S$. This turns out to consist of all elements r with $rs = 0$ for some $s \in S$. If R is an *integral domain* and $0 \notin S$, then R_S is just the subring of the quotient field generated by s^{-1} for $s \in S$.

We are now in a position to dfine the ringed space structure. Recall that $\mathrm{Spec}(R)$ has a basis for the topology consisting of sets $D(f)$ for $f \in R$. Here $D(f)$ is the set of prime ideals not containing f. We think of f as a "function" on $\mathrm{Spec}(R)$, and $D(f)$ as the complement of the zeros of f. We put $\mathcal{O}(D(f)) = R_f = R[f^{-1}]$. That is, functions regular except at zeros of f. For an arbitrary set U, we don't really care: The key point in working with schemes is to ignore all open sets not of the form D_f. We can do this because of the following.

Lemma 169. *Sheaves $\mathcal{O}$ can be defined on a space X by defined $\mathcal{O}(U)$ for a base of the topology, and checking the covering for condition for covers of U_i in the base by other sets of the base.*

The point is that if we know the sheaf $\mathcal{O}(U)$ for U in the base, this determines it on any open set V, as we can cover V by basis elements: We define $\mathcal{O}(V)$ to be the elements of $\mathcal{O}(U_1)\times\mathcal{O}(U_2)\times\cdots$ that agree on $U_i \cap U_j$. This will be well-defined and independent of the cover of V.

So to show we have a sheaf on $\mathrm{Spec}(R)$, we just need to check the sheaf condition for covers of $D(f)$ by $D(f_1), D(f_2), \dots$. We can do this as follows: The first step is to replace R by R_f, so we may assume $f = 1$. Next we notice that $\mathrm{Spec}(R)$ is covered by the open sets $D(f_1), D(f_2), \dots$. As before this means that $1 \in (f_1, f_2, \dots)$, so $1 \in (f_1, f_2, \dots, f_n)$ for some n, and so we can assume that the number of f_i in the covering is finite. (Notice that we almost did this for affine varieties, the only difference being that our ring in question here might have zero divisors.) We need to check that if $r \in R$ is 0 on each $D(f_i)$, then $r = 0$. If $r = 0$ in $D(f_i)$, then $(f_i)^{n_i}r = 0$ for some n_i: This is true since an element x is 0 in $D(f_i)$ if and only if x is killed by some element of the semigroup generated by f_i. As $R_{f_i} = R_{f_i^{n_i}}$, we can replace f_i by $f_i^{n_i}$ and assume that $f_ir = 0$. Since $f_1, \dots f_n$ were generators, $a_1f_1 + \cdots + a_nf_n = 1$ for some a_i, $r = a_1f_1r + \cdots + a_nf_nr = 0$.

The hard part is the following: Suppose we are given $r_i/f_i^{n_i} \in R_{f_i} = D(f_i)$ that are compatible, $r_i/f_i^{n_i} = r_j/f_j^{n_j}$ in $R_{f_if_j} = D(f_i) \cap D(f_j)$. We then want to find $r \in R$ so that $r = r_i/f_i^{n_i}$ in R_{f_i}. To do this, we want to solve the following problem. Suppose given a_i, f_i with $a_1f_1 + \cdots + a_nf_n = 1$, and $r_i/f_i^{n_i}$ with $(f_if_j)^{m_{ij}}(r_if_j^{n_j} - r_jf_i^{n_i}) = 0$ for some m_{ij}. We want to show that we can find r with $f_i^{k_i}(f_i^{n_i}r - r_i) = 0$ for some k_i. The relations are a bit of a mess, and the first thing we do is to simplify them. The first simplification is given by replacing the f_i by some high power: If $(f_i, f_2, \dots, f_n) = 1$, then $(f_1^{t_1}, \dots, f_n^{t_n}) = 1$ for any $t_1, t_2, \dots, t_n$. Thus we have reduced the problem solve the following: Suppose $a_1f_1 + \cdots + a_nf_n = 1$, and $f_if_j(r_if_j - r_jf_i) = 0$, we want to

find r with $f_i(f_i r - r_i) = 0$. Replace $r_i f_i$ by s_i, so $s_i f_j^2 = s_j f_i^2$, and we want to solve $f_i^2 r = s_i$. We replace f_i^2 by g_i, so the equations become $s_i g_j = s_j g_i$, and $b_1 g_1 + b_2 g_2 + \cdots + b_n g_n = 1$, and we want to solve $g_i r = s_i$. Now, we can just write down a solution. We see that $b_1 g_1 r + \cdots + b_n g_n r = r$, so $r = b_1 s_1 + \cdots + b_n s_n$ is the only possibility for r, so define r to be $b_1 s_1 + \cdots + b_n s_n$, and we need to check that $g_i r = s_i$. Now

$$g_i r = b_1 s_1 g_i + \cdots = b_1 g_1 s_i + \cdots = (b_1 g_1 + \cdots) s_i = s_i.$$

In conclusion, putting $\mathcal{O}(D_f) = R_f$ defines a unique sheaf of rings on $\mathrm{Spec}(R)$. The stalk of this sheaf $\mathcal{O}$ at a point p by definition is the direct limit of $\mathcal{O}(U)$, U containing p, and we might as well consider the direct limit of $\mathcal{O}(D_f)$, D_f containing p. This is nothing but R_S, where S is the set of all elements not in p, which happens to be also denoted by R_p.

The easy way to do this construction is to start with $\mathcal{O}(D_f) = R_f$ and calculate the stalk at the point R_p (unlike in [Har], where instead we define the stalk at a point and calculate $\mathcal{O}(D_f)$ from this).

Definition 170. A general *scheme* is a (locally) ringed space looking locally like an affine scheme (which we can think of as giving "local coordinates").

We can compare this definition to that of a smooth manifold, which is a ringed space locally isomorphic to a ringed space of smooth functions on $\mathbb{R}^n$.

Morphisms of schemes are *not* morphisms of the underlying ringed space. Schemes are *locally* ringed spaces in the sense that the stalk of any point is a local ring, meaning that it has a unique maximal ideal. Informally, this maximal ideal is informally the set of functions vanishing at this point. So, instead, morphisms of schemes are morphisms of *locally* ringed spaces. Let us define these terms.

We will define a morphism of a ringed space. First look at $f : X \to Y$ for topological spaces X and Y, and take first the sheaves of continuous real functions on X and Y. If U is any open subset of Y, then $f^{-1}(U)$ is an open subset of X, and if g is a function, then $g \circ f$ is a function on $f^{-1}(U)$, so we have a morphism of rings from $\mathcal{O}(U)$ to $\mathcal{O}(f^{-1}U)$. We continue from here next time, but rather obviously, a morphism of ringed spaces will be a morphism between these spaces.

27th lecture, December 2 2010

Last lecture we were discussing morphisms of schemes. Recall of schemes are special cases of ringed spaces, and we will define morphisms of these. Special cases of ringed spaces are locally ringed spaces, which also have a sense of morphisms. Note that a morphism $A \to B$ of ringed spaces A, B need not be a morphism of locally ringed spaces, even if A and B are locally ringed spaces. In terms of category theory, the locally ringed spaces form a non-full subcategory of ringed spaces. Keeping in mind the example of the set of continuous functions on a space, we come up with the following definition:

Definition 171. A *morphism of ringed spaces* $f : X \to Y$ satisfies:

(1) It is a continuous map between the underlying topological spaces.

(2) For each open set $U \subseteq Y$, $f^{-1}(U)$ is open in X. We should have a homomorphism of rings $\mathcal{O}(U) \to \mathcal{O}(f^{-1}(U))$ for all open $U \subseteq Y$. For $V \subset U$ we have a commutative diagram

$$\begin{array}{ccc} \mathcal{O}(U) & \longrightarrow & \mathcal{O}(f^{-1}(U)) \\ \downarrow & & \downarrow \\ \mathcal{O}(V) & \longrightarrow & \mathcal{O}(f^{-1}(V)) \end{array}$$

We consider now locally ringed spaces. The idea is that a locally ringed space has a concept of "vanishing at a point". For example, if $p \in X$, one can look at all functions defined near p,

i.e. $\lim_{U \ni p} \mathcal{O}(U)$. So this ring, $\mathcal{O}_p$, is a *local* ring, where the maximal ideal can be thought of as "functions as vanishing at p". So suppose $f : X \to Y$ is a continuous map, and suppose g is a real function on Y vanishing at $y \in Y$. Then $g \circ f$ vanishing at all points with image y under f. In terms of local rings we have that if $f : x \mapsto y$, we get an induced map between local rings $\mathcal{O}_y \to \mathcal{O}_x$. The extra condition we need in the definition of *morphisms of locally ringed spaces* is that this induced map should take the maximal ideal of $\mathcal{O}_y$ to the maximal ideal of $\mathcal{O}_x$.

Example 172. The following is an example of a morphism of ringed spaces between locally ringed spaces that is not a morphism of locally ringed spaces.

Take a discrete valuation ring. For example the set $\mathbb{Z}_{(p)}$ of all rationals m/n where $p \not| n$. This has 2 prime ideals: The maximal ideal (p) which is closed in $\mathrm{Spec}(\mathbb{Z}_{(p)})$ and (0) which is not maximal and an open point. Let $Y = \mathrm{Spec}(\mathbb{Z}_{(p)})$ be the space of these two points. Let $X = \mathrm{Spec}(\mathbb{Q})$, which is just a point. We will define a morphism of ringed spaces $f : X \to Y$. The image of X is the closed point (p) of Y. Suppose U is open, containing the image of X, say $U = (p)$. We want a map $\mathcal{O}(U) \to \mathcal{O}(f^{-1}(U)) = \mathcal{O}(X) = \mathbb{Q}$. We define this to be the map $\mathcal{O}(U) \to \mathbb{Z}_{(p)} \to \mathbb{Q}$, where the last map is the injection. Now $\mathbb{Z}_{(p)}$ is the local ring at (p), and $\mathbb{Q}$ is the local ring of (0) in X. But now, the maximal ideal of $\mathbb{Z}_{(p)}$ does not map to the maximal ideal of $\mathbb{Q}$.

There is a morphism (of locally ringed spaces) from $\mathrm{Spec}(\mathbb{Q})$ to $\mathrm{Spec}(\mathbb{Z}_{(p)})$. In general, morphisms $\mathrm{Spec}(R) \to \mathrm{Spec}(S)$ correspond exactly to ring homomorphisms $S \to R$, as we will see below. So we want a morphism $g : \mathbb{Z}_{(p)} \to \mathbb{Q}$, where we just use the obvious injection. On the level of locally ringed spaces, we have a map $\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Z}_{(p)})$ mapping $(0) \mapsto g^{-1}(0) = (0)$, so the morphism takes (0) to the open point of $\mathrm{Spec}(\mathbb{Z}_{(p)})$.

For rings R, S, there is a correspondence between ring homomorphisms $R \to S$ and morphisms of locally ringed spaces $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$. The corresponds to the fact that Spec is functor from the rings to ringed spaces. The inverse is given by the fact that $R = \mathcal{O}(\mathrm{Spec}(R)) \to \mathcal{O}(\mathrm{Spec}(S)) = S$ defines a morphism $R \to S$. One should check that this defines a categorical isomorphisms.

Remark that $\mathrm{Spec}(R)$ is a sort of "universal" locally ringed space generated by R. Morphisms $\mathcal{O}(X) \to R$ corresponds exactly to morphisms $\mathrm{Spec}(R) \to X$ (or maybe the other way around), so Spec is an adjoint functor to $\mathcal{O}$, and by category theory, there is a unique such one, up to isomorphism (see Fig. 29).

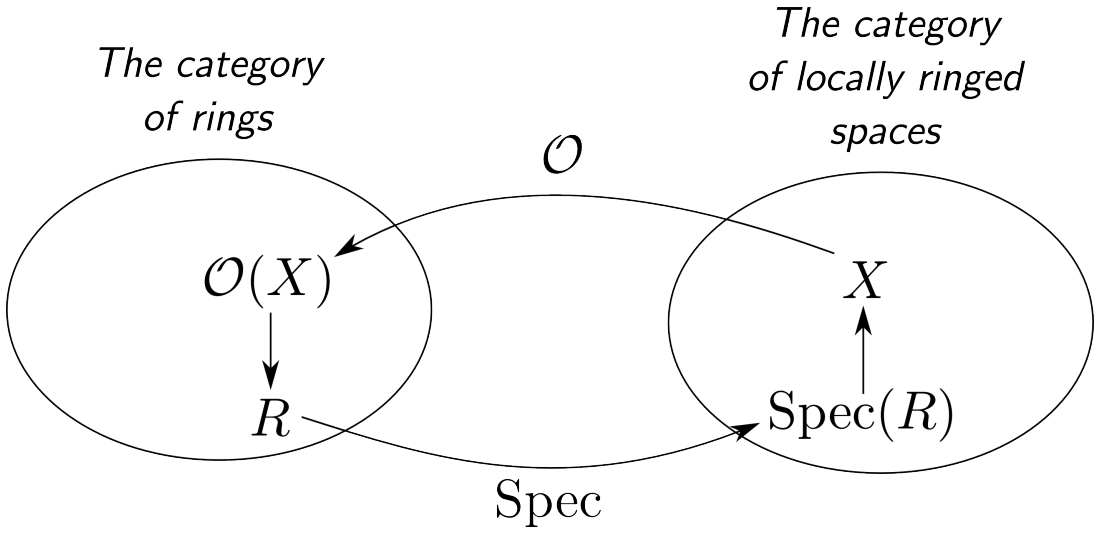


Figure 29: The functor Spec as an adjoint to $\mathcal{O}$.

Example 173. We will construct the scheme of a graded ring. So recall that a scheme is a locally ringed space locally isomorphic to affine schemes (which we think of as coordinate charts). We can

constructs manifolds by gluing together open sets in $\mathbb{R}^n$, and we do the same for schemes: We glue together affine schemes pretty much the same way.

Recall first the usual construction of P^n from $k[x_0, \ldots, x_n]$: P^n is the union of $n+1$ copies of A^n- These copies of affine space has coordinate rings $k[x_0, \ldots, x_i, x_{i+1}, \ldots, x_n] = k[x_0, \ldots, x_n][x_i^{-1}]_0$, where the $_0$ denotes the degree 0 part. We will now glue these together. These n copies are subsets D_{x_i} of $(x_0 : \cdots : x_n)$ with $x_i \neq 0$. We glue them together along $D_{x_i} \cap D_{x_j}$ which is the set of points with $x_i, x_j \neq 0$. The coordinate ring of $D_{x_i} \cap D_{x_j}$ is $k[x_0, dots, x_n][x_i^{-1}, x_j^{-1}]_0$. Now P^n is the union of D_{x_i} glued along $D_{x_i} \cap D_{x_j}$.

Now let $R = R_0 \oplus R_1 \oplus \cdots$ be any graded ring. Let f be any homogeneous element of degree greater than 0, and let R_f^0 be the degree 0 elements of $R_f = R[f^{-1}]$. Put $D_f = \operatorname{Spec}(R_f^0)$. These are the analogues of the complements of a hypersurface of P^n. We now want to glue these together. Notice for this that if f, g are homogeneous, then $\operatorname{Spec} R_{fg}^0$ is an open subset of $\operatorname{Spec}(R_f^0)$. (This is the analogue of saying that $\operatorname{Spec} k[x_0, \ldots, x_n][x_i^{-1}, x_j^{-1}]_0$ is an open subset of $\operatorname{Spec} k[x_0, \ldots, x_n][x_i^{-1}]_0$.) We glue together *all* affine subschemes $\operatorname{Spec}(R_f^0)$ for all homomorphisms f (with degree greater than 0), by identifying $\operatorname{Spec}_{fg}^0$ with an open subset of $\operatorname{Spec}(R_f^0)$.

This scheme is called $\operatorname{Proj}(R)$. What does the underlying space of $\operatorname{Proj}(R)$ look like? We first find the space of $D_f = \operatorname{Spec}(R_f^0)$. This is just the prime ideals of R_f^0, which is the same as the homogeneous prime ideals of R_f, which again is the same as the homogeneous prime ideals of R not containing f. So the space of $\operatorname{Proj}(R)$ is equal to the union over f of the spaces D_f, which is then just the union over f of graded prime ideals not containing f. This on the other hand is the set of graded prime ideals not containing the ideal $(R_1 \oplus R_2 \oplus \cdots)$.

Notice that this is very similar to the definition of projective space over a field, as $P^n(k)$ is the set of graded maximal ideals of $k[x_0, \ldots, x_n]$ not containing $(x_0, x_1, \ldots, x_n) = R_1 \oplus R_2 \oplus \cdots$.

Example 174. Look at the projective line over $\mathbb{Z}$; that is, $\operatorname{Proj} \mathbb{Z}[x, y]$. We can ask the question: What are points of the projective line with values in a ring R? That is, we want to find morphisms from $\operatorname{Spec}(R) \to \operatorname{Proj}(\mathbb{Z}[x, y])$. First we do the case where R is a field k. In this case $\operatorname{Spec}(k)$ is just a point, and $\mathcal{O}(\text{pt}) = k$. $\operatorname{Proj}(\mathbb{Z}[x, y])$ is covered by 2 open sets, $D_y = \operatorname{Spec}(\mathbb{Z}[x, y][y^{-1}]_0) = \operatorname{Spec}(\mathbb{Z}[x])$ and $D_x = \operatorname{Spec}(\mathbb{Z}[x, y][x^{-1}]_0) = \operatorname{Spec}(\mathbb{Z}[y])$. These we calculated previously. Since $\operatorname{Spec}(k)$ is a point, the image is in either D_x or D_y, so we just look at morphisms $\operatorname{Spec}(k) \to D_x = \operatorname{Spec} \mathbb{Z}[y]$. As we saw earlier, these are just morphisms $\mathbb{Z}[y] \to k$. The simply correspond to points of k (which we can think of as the affine line over k). Similarly, morphisms $\operatorname{Spec}(k) \to D_y$ also correspond to $A^1(k)$. So, morphisms $\operatorname{Spec}(k) \to \operatorname{Proj} \mathbb{Z}[x, y]$ correspond to the union of 2 copies of k glued over there intersection. This turns out to be $P^1(k)$, the set of pairs $(x : y)$, where x, y are not both 0.

We consider now the case of a general ring R and ask for the set of morphisms $\operatorname{Spec}(R) \to \operatorname{Proj} \mathbb{Z}[x, y]$. The following answers are wrong

(1) Pairs (x, y), $x, y \in R$, $(x, y) \neq 0$.

(2) Pairs (x, y) where x, y generate the unit ideal in R.

(3) Since $P^1(k) = k \cup k$ (glued along something), we could think that $P^1(R) = R \cup R$ (glued along something), but this is also wrong (since $\operatorname{Spec}(R)$ is not necessarily a point as before and might not have image contained completely in a covering set).

The correct answer is that the morphisms $\operatorname{Spec}(R) \to \operatorname{Proj} \mathbb{Z}[x, y]$ correspond to invertible modules M over R having a pair of elements $x, y \in M$ that generate all stalks of M at a point of R, up to isomorphism. Notice that this gives the right answer, when k is a field, as here invertible modules are just 1-dimensional vector spaces.

Look at $\mathbb{Z}$-valued points of the projective line, so we consider a morphism $f : \operatorname{Spec}(\mathbb{Z}) \to \operatorname{Proj} \mathbb{Z}[x, y]$. Again, $\operatorname{Spec} \mathbb{Z}$ is not a point, so instead we consider $f^{-1}(D_x)$ and $f^{-1}(D_y)$. These must be open sets covering $\operatorname{Spec}(\mathbb{Z})$. So to construct a morphism, we cover $\operatorname{Spec}(\mathbb{Z})$ by open sets U_1, U_2 and define morphisms $U_1 \to D_x$, $U_2 \to D_y$ and check that they agree on $U_1 \cap U_2$. The open sets of $\operatorname{Spec} \mathbb{Z}$ are the sets $\operatorname{Spec} \mathbb{Z}_n = \operatorname{Spec} \mathbb{Z}[n^{-1}]$, where $n \neq 0$. Here $\operatorname{Spec} \mathbb{Z}_n$ is just the ideal (0) together

with all primes not dividing n. So $\operatorname{Spec}\mathbb{Z}_m$ and $\operatorname{Spec}\mathbb{Z}_n$ cover $\operatorname{Spec}\mathbb{Z}$ if $(m,n)=1$. Morphisms $\operatorname{Spec}\mathbb{Z}_n \to D_x = \operatorname{Spec}(\mathbb{Z}[y])$ are now easy to find, as these are just morphisms $\mathbb{Z}[y] \to \mathbb{Z}[n^{-1}]$. These correspond to elements of $\mathbb{Z}[n^{-1}]$. Similarly morphisms $\operatorname{Spec} D_y$ correspond to elements of $\mathbb{Z}[m^{-1}]$. Working more with this, it should turn out that points correspond to pairs $(x:y)$, x, y coprime, up to multiplication by units.

References

[Eis] David Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Springer, 1995.

[Ful] William Fulton. *Introduction to Toric Varieties*. Princeton University Press, 1993.

[Har] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[Ser] Jean-Pierre Serre. Faisceaux Algébriques Cohérents. *Annals of Mathematics*, 61:2:197–278, 1955.