1. Thursday, August 23, 2012

Course website: http://math.berkeley.edu/∼reb/256A
Text: Hartshorne

Example 1.1. Find solutions $(x, y, z) \in \mathbb{Z}^3$ to $x^2 + y^2 = z^2$.

(1) Algebraic Solution: $x^2 = (z-y)(z-y)$. Assume x, y, z coprime, and x odd. So $(z-y), (z+y)$ are both squares.

Set $z - y = r^2, z + y = s^2$, with r, s odd positive numbers.

$$z = \frac{r^2 + s^2}{2}, y = \frac{s^2 - r^2}{2}, x = rs.$$

Then, for example, taking $(r, s) = (1, 3)$ gives us $(x, y, z) = (3, 4, 5)$.

(2) Geometric solution: Solve $X^2 + Y^2 = 1$ in rationals, where $X = \frac{x}{z}$ and $Y = \frac{y}{z}$. Therefore, we are looking for rational points on the circle.

Finding real points is easy, just take $X = \sin\theta, Y = \cos\theta$, however this doesn't help us very much.

Instead, fix the point at $(-1, 0)$ and look at lines from that point that intersect the tangent to the circle at $(1, 0)$. Where do these lines intersect the circle?

If the line intersects the tangent at $(1, t)$, then it intersects the circle at (X, Y) where $t = \frac{Y}{X+1}$

$$\Rightarrow Y = t(X + 1) \Rightarrow t^2(X + 1)^2 + X^2 = 1 \Rightarrow X = \frac{1 - t^2}{1 + t^2}, Y = \frac{2t}{1 + t^2}.$$

Therefore, t rational $\Rightarrow X, Y$ rational.

So rational points on the circle *almost* correspond to rational t. $t = \frac{1}{2}$ means that $X = \frac{3}{5}, Y = \frac{4}{5}$. The map $(X, Y) \to t$ is a BIRATIONAL map from circle to line. Birational means isomorphism except on a set o codimension ≥ 1.

(For smooth manifolds, "birational" maps are trivial. Any smooth manifold of dimension n can be cut along $n - 1$ dimensional sub manifolds so it is a union of $\mathbb{R}^n$s.)

Because the circle is the group of rotations, this means the set of pythagorean triples is a group.

Product of group:

$$(X_1, Y_1) \times (X_2, Y_2) = (X_1X_2 - Y_1Y_2, X_1Y_2 + X_2Y_1).$$

This algebraic formula works to send any commutative ring to a group.

Example 1.2. Solve $y^2 = x^3 + x^2$ in integers. One solution is $(3, 6)$.

We can draw the graph: INSERT GRAPH HERE.

The graph has a singularity at the origin. If we send a line from the origin, it will intersect at a point (x, y), and the line has slope $t = \frac{y}{x}$.

Given t, determine y, x. Solving for x will give a CUBIC equation; two of the roots are 0 and the third root will be rational.

$$y = tx \Rightarrow t^3x^2 = x^3 + x^2 \Rightarrow t^2 = x + 1 \Rightarrow x = t^2 - 1, y = t(t^2 - 1).$$

This example gives us a taste of singularities, which we generally want to get rid of. We accomplish this through resolution of singularities which map a singular curve to a smooth curve above it.

Here, we took the smooth curve, the line t and mapped to this singular curve $y^2 = x^3 + x^2$.

Example 1.3. Find rational solutions of $x^n + y^n = 1 \Leftrightarrow X^n + Y^n = Z^n$ for integers, or Fermat's Last Theorem. This shows us that Algebraic Geometry over $\mathbb{Q}$ is really hard.

Example 1.4. Dudeney puzzle: $x^3 + y^3 = 9$ in rationals. One solution is $(1, 2)$. Find another one.

His answer was:

$$\left(\frac{415280564497}{38671682660}\right)^3 + \left(\frac{676702467503}{348671682660}\right)^3 = 9.$$

How did he find it? Draw the curve $x^3 + y^3 = 9$. The curve has no double point. Suppose that $(x_1, y_1), (x_2, y_2)$ are two rational points on the curve; then, the line through them intersects the curve in a third point. Since the sum of roots are rational, the final point of intersection is rational.

A similar technique would be to take the tangent to a point on the curve, and see where else it intersects. This is the "Chord-tangent process". This is essentially a group law.

More explicitly, the group law goes: Fix some rational point, call it the identity. Three points lie on a straight line means that their sum is the identity.

Still it is not quite a group, because the point at infinity is missing. This is evident if you take the line between $(1, 2)$ and $(2, 1)$; this line does not meet the curve again except at infinity.

In this case, we are working with projective varieties rather than affine varieties.

Definition 1.5. Projective Space: "Add points at infinity." Points of affine space $\mathring{A}^2$ are written (x, y). Points of the projective space $\mathbb{P}^2$ are written $(x : y : z)$ not all 0, with $(x : y : z) = (\lambda x : \lambda y : \lambda z)$.

The projective plane contains the affine plane $(x : y : 1)$, the affine line $(x : 1 : 0)$ (at infinity), and another point $(1 : 0 : 0)$.

How is $x^3 + y^3 = 9$ a curve in projective plane? Make it homogeneous: $x^3 + y^3 = 9z^3$ – this is a projective cubic curve. Its points form a group. Example of an abelian variety (group and also a projective variety).

Example of an "abelian linear group" (the old name for the symplectic group) that is not abelian.

Theorem 1.6 (Pappus' Hexagon Theorem)**.** *Two lines, three points selected on each line labeled A, B, C and a, b, c.Draw lines across except between the same letters. The resulting three points of intersections are collinear.*

Theorem 1.7 (Pascal's Theorem)**.** *Take a conic (ellipse, parabola, hyperbola), with a similar set up of six points. The intersection points here are also linear. Clearly, the case with two lines in Pappus' Theorem is a degenerate case of this theorem.*

Proof. Label the lines L_i and fix any new point P on the ellipse. Suppose Line L_i is given by equation $P_i = 0$. Look at the equation

$$P_1 P_2 P_3 - \lambda P_4 P_5 P_6 = 0.$$

Choose λ so P is a solution of this. Look at the equation $X = 0$, X a degree two polynomial, of the conic. There are 7 points on the conic and cubic (the six we started with and the new P). □

Theorem 1.8 (Bezout's Theorem)**.** *Curves of degree m, n intersect in $\leq m, n$ points unless they have a curve in common.*

Therefore, the cubic and the conic must have a common component. So the cubic factorizes as equation of conic times equation of line.

Sloppy Proof of Bezout's Theorem. As stated in old books, the theorem was "Curves of degree m, n have mn intersection points." (False, as stated). The sloppy proof was "what is true up to the limit is true at the limit." (Obviously a false statement.) Given the two equations $f(x, y) = 0$ and

$g(x, y) = 0$, you deform both until each is a product of linear factors. Assuming that these lines are nonparallel and distinct, they will have the desired number of intersection points.

□

Kakeya set in $\mathbb{R}^2$ is a set containing a unit line segment in every direction. Besikovich proved that a Kakeyu set can have arbitrarily small area. Thomas Wolfe conjectured the following, later proved by Dini.

Theorem 1.9 (Finite field Kakeya Conjecture)**.** *The size of a Kakeya set in F^n for a finite field F is at least $c_n|F|^n$, where $c_n =$ some constant not depending on F.*

Dini's Proof.

(1) A Kakeya set cannot lie in a hypersurface $f(x_1, \ldots) = 0$ of degree $< |F|$. If f is a polynomial of degree $< |F|$ defining a hypersruface containing a Kakeya set, then

$$f = f_d + f_{d-1} + \ldots . (d = \text{ highest degree component of } f.)$$

For all v we can find x such that $f(x + vt)$ vanishes for all $t \in F$, so the coefficient $f_d(v)$ of t^d vanishes. As this is true for any v and deg $f_d < |F|$, we must have $f_d = 0$ so $f = 0$.

(A polynomial of degree $< |F|$ cannot vanish on all points of F)

(2) Space of polynomials of degree $\leq d$ in n variables is a vector space of dimension $\binom{n+d}{n}$ so for any set with $\leq t$ has many elements, can find a nonzero polynomial of degree $\leq d$ vanishing on this set.

So any Kakeya set has

$$\geq \frac{n + |F| - 1}{n} \geq \frac{|F|^n}{n!} \text{ elements.}$$

□

Example 1.10 (27 Lines on a Cubic Surface)**.** Consider the cubic surface $w^3 + x^3 + y^3 + z^3 = 0$. This is a cubic surface in $\mathbb{P}^3$.

It contains a line $(1 : -1 : t : -t)$. This surface has many symmetries:

(1) We can permute these four entries using S_4 which has order 24.

(2) We multiply any coordinate by $\sqrt{3}{-1}$. Gives a group of order 3^3 (not 3^4). (Multiplying all coordinates by w is identity)

So we have a group of order $3^3 \cdot 24$ acting on this cubic surface. The line above has 27 images under this group.

2. Tuesday, August 28, 2012

2.1. Affine Varieties.

Definition 2.1. Let k be a field, for convenience $\mathbb{C}$. Affine space $= k^n$, but we "forget" where the origin is. What does this mean? Consider the automorphism groups.

$$Aut(k^n) = GL_n(k).$$
$$Aut(\mathbb{A}^n) = k^n \bullet GL_n(k).$$

In taking the affine space, we allow translations.

Definition 2.2. Affine geometry = the properties of k^n invariant under the affine group $k^n \bullet GL_n(k)$.

Example 2.3. The set of conics is invariant under $k^n \cdot GL_n(k)$; however, the set of circles is not, since a linear transformation can turn it into an ellipse.

Definition 2.4. An algebraic set in $k^n = \mathbb{A}^n$ is the set of zeros of some set of polynomials.

Example 2.5. The parabola is an algebraic set, as the zero set of the equation $y - x^2$.

Definition 2.6. The Zariski topology is the topology taking algebraic sets as the closed sets. This topology is non-Hausdorf!!

Proof. To confirm topology axioms, check that algebraic sets are closed under finite unions and arbitrary intersections. Suppose $X =$ zero set of $\{p_1, p_2, \ldots\}$, and $Y =$ zero set of $\{q_1, q_2, \ldots\}$.

(1) $X \cup Y =$ zero set of $\{p_i q_j\}$.
(2) $X \cap Y \cap Z \cap \cdots =$ the zero set of the union of all of the polynomials.

□

Remark 2.7. Topology of $\mathbb{A}^1$. The closed sets are:

(1) Whole space. (Zeros of the empty set)
(2) Finite subset. (Zeros of $(x - a_1)(x - a_2)\cdots$).

Points are closed. (T_1), but any two nonempty open sets have non-empty intersection, assuming k infinite.

Remark 2.8. Topology of $\mathbb{A}^2$. Zariski topology is NOT the product topology.

In the product topology, the typical closed set is horizontal lines, vertical lines, and points.

In the Zariski Topology, the closed sets are unions of points and algebraic curves. Therefore, the Zariski topology is finer than the product topology.

Example 2.9. A determinantal variety is an example of an algebraic set. Take:

$$\mathbb{A}^{mn} = m \times n \text{ matrices} = \text{linear maps} : k^m \to k^n.$$

Look at the subset of matrices of rank $\le N$. This is an algebraic set; it is given by the subset of all matrices such that all $(N+1) \times (N+1)$ submatrices have determinant 0. Recall that the determinant is a polynomial in the entries of $\mathbb{A}^{mn}$.

Proposition 2.10. *Any algebraic set is the union of a finite number of irreducible algebraic sets (varieties).*

Definition 2.11. An irreducible set is a set that cannot be written as the union of two smaller closed subsets.

If a topological space is Hausdorff, the only irreducible sets are points, infinite closed sets are not the union of finitely many irreducibles).

The assertion in Proposition 2.10 is true for any Noetherian topological space.

Definition 2.12. A ring is called Noetherian if its ideals satisfy one of the following:

(1) The Ascending Chain Condition (ACC). If
$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots.$$
is an ascending chain of ideals, it eventually stabilizes.
(2) Every ideal is finitely generated.
(3) Every nonempty set of ideals has a maximal element.

Remark 2.13. Affine space is Noetherian (as topological space) because $k[x_1, \ldots, x_n]$ (the ring of polynomial functions on $\mathbb{A}^n$ is Noetherian as a ring.

Remark 2.14. If $X_1 \supseteq X_2 \supseteq X_3 \supseteq \cdots$ is a descending sequence of algebraic sets, then $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an ascending sequence of algebraic sets, where I_k is the ideal of polynomials vanishing on X_k.

Theorem 2.15 (Hilbert). *If R is Noetherian, then $R[x]$ is Noetherian.*

Proof. Suppose I is an ideal in $R[x]$. We want to show that it is finitely generated.

Consider $I_0 \subseteq I_1 \subseteq \cdots$, where $I_n =$ the ideal of R generated by the leading coefficients of polynomials of I of degree $\leq n$. (Exercise: show that these are ideals.)

Since R is Noetherian, we know that this chain of ideals stabilizes. Therefore, I is generated by a finite set of polynomials whose leading coefficients generate $I_0, \ldots, I_n$. □

Exercise 2.16. Prove: If R is Noetherian, so is $R[[x]]$. (Copy the proof above, using the lowest nonzero coefficient of the formal power series.)

Therefore, affine space is Noetherian.

Proof of Proposition 2.10. This proof is a typical example of Noetherian induction, where we assume a minimal counterexample, which must exist since any nonempty collection of closed sets has a minimal element.

Suppose X is minimal among closed sets that are not a finite union of varieties. X is not irreducible, so $X = Y \cup Z$, where Y and Z are closed smaller sets, both of which are finite unions of varieties. Therefore, X as well is a finite union of varieties. □

The claim that any algebraic set is the union of finitely many irreducibles is similar to the assertion that: any nonzero integer is the product of finite number of primes.

Example 2.17. Consider the algebraic set, defined by:

$$x^2 + y^2 + z^2 = 0, \quad xyz = 0.$$

Decompose into irreducibles, setting each variable in turn equal to 0. We obtain a union of six lines.

Remark 2.18. Warning! It is computationally very hard to decompose an algebraic set into irreducibles.

Example 2.19. Consider the zero set of $xy = 1$. In the usual topology on the reals, this has two connected components. However, it is irreducible in the Zariski topology.

Example 2.20. Look at the family of algebraic sets $xy = c$ as c varies.

For $c \neq 0$, the set is irreducible; but for $c = 0$, it is reducible into 2 lines.

So we have a provisional definition:

An affine variety is an irreducible algebraic set in affine space.

However, we have a problem. Consider the set $\mathbb{A}^1 - (0)$. This should be an affine variety since its isomorphic to an affine variety: simply take the x coordinate of $xy = 1$ as a subset of $\mathbb{A}^2$. To map back, simply take the set of points $(x, 1/x)$.

Though we have not defined morphisms of varieties, it is intuitive that these two sets should be isomorphic. Therefore we will need to tinker with our definition later on.

2.2. **Hilbert's Nullstellensatz.** Nullstellensatz is German for "Zero position theorem."

We would like to have a dictionary between the geometric object $\mathbb{A}^n$ and the algebraic object $k[x_1, \ldots, x_n]$.

What do subsets Y of $\mathbb{A}^n$ correspond to? There will be an ideal $I(Y)$ of polynomials vanishing on Y.

Conversely, given an ideal $\mathfrak{a}$ of R corresponds to a subset $Z(\mathfrak{a})$ of points that are zeros of all elements of $\mathfrak{a}$.

This is not a $1-1$ correspondence. Why not?

Remark 2.21. Zeros of an ideal is (by definition) closed. So only the closed subsets can correspond to ideals. Taking $Y \to I(Y) \to Z(I(Y)$ will be the closure of Y in the Zariski topology.

Do *closed* subsets correspond to ideals?

No! Look at the ideals (x), (x^2) in $k[x]$. Both have the zero set $Z((x)) = Z((x^2)) = 0$. The problem here is that $f, f^2, f^3, \ldots$ all have the same zeros.

Definition 2.22. Let $\mathfrak{a} \subset R$ be an ideal. Let $\sqrt{\mathfrak{a}}$, the radical of $\mathfrak{a}$ = the set of all polynomials f such that $f^n \in \mathfrak{a}$.

Remark 2.23. $\sqrt{\mathfrak{a}}$ is an ideal. If $f^n, g^m \in \mathfrak{a}$, then $(f+g)^{m+n}$ can be expanded via the binomial theorem, and each monomial will have a sufficiently high power of f or g.

Remark 2.24. $\sqrt{\mathfrak{a}}$ and $\mathfrak{a}$ have the same set of zeros. $\sqrt{\mathfrak{a}} = \sqrt{\sqrt{\mathfrak{a}}}$. An ideal $\mathfrak{a}$ is called radical, if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Do the *closed* subsets correspond to the *radical* ideals?

No. Look at $\mathbb{R}[x]$. Consider the ideal $\mathfrak{a} = (x^2+1)$. This ideal is radical, yet the set of zeros is empty, so it corresponds to the ideal (1).

The problem is obviously related to $\mathbb{R}$ not being algebraically closed. After all, $(x^2+1) = (x+i)(x-i)$ in $\mathbb{C}$.

Theorem 2.25 (Hilbert's Nullstellensatz)**.** *Over an algebraically closed field k, the closed algebraic subsets correspond to the radical ideals.*

What about points? $(a_1, \ldots, a_n) \in \mathbb{A}^n$ corresponds to the ideal $(x_1 - a_1, \ldots, x_n - a_n) \subset k[x_1, \ldots, x_n]$. This is obviously a maximal ideal.

(Recall that a maximal ideal of R means that it is maximal among proper ideals. M maximal in $R \Leftrightarrow R/M$ is a field.)

Is the converse true? Do maximal ideals of $R[x_1, \ldots, x_n]$ all correspond to points of k^n as above? No, for the algebraically closed reason described above. Take $(x^2+1) \in \mathbb{R}$ as a counterexample.

Theorem 2.26 (Hilbert's Weak Nullstellensatz)**.** *Over algebraically closed field k, maximal ideals of $k[x_1, \ldots, x_n] \leftrightarrow$ points $(a_1, \ldots, a_n)$ of affine space.*

Proof. Suppose I is a maximal ideal of $k[x_1, \ldots, x_n]$. Put $K = k[x_1, \ldots, x_n]/I$, so K is a field.

Renumber x_i so $x_1, \ldots, x_i$ are algebraically independent in K (over k) and $x_{i+1}, \ldots, x_n$ are algebraically dependent on them.

$$k \subseteq F = k(x_1, \ldots, x_i) \subseteq K.$$

k is a finitely generated field extension, while K is a finitely generated module over F. Note that being f.g. as a field extension is not the same as being finitely generated as a module. □

3. Thursday, August 30, 2012

Proof of Weak Nullstellensatz Continued. Let $y_1, \ldots, y_i$ be a finite generating set for the F-module K. Then $x_a = \sum t_{ab} y_b$, and $y_a y_b = \sum t_{abc} y_c$. Let T be the k-algebra generated by the t's.

Step 1: Claim T is a Noetherian ring.

Step 2: K is a finitely generated module over T. (generated as a module by y's.

Step 3: F is finitely generated as a T-module. (Reason $F \subseteq K$ a f.g. module. Any submodule of a finitely generated module over a Noetherian ring is finitely generated.)

Step 4: F is finitely generated as an algebra over k

Next, we show that $F = k$. $F = k(x_1, \ldots, x_i)$, rational functions in i variables = quotient field of $k[x_1, \ldots, x_i]$. Want to show: $i = 0$.

If $i > 0$, $k[x_1, \ldots, x_i]$ is a U.F.D. with infinitely many primes. (Missed a step here)

If $F = k$ then K is finitely generated as a k-module.

So far, we have not used the fact that k is algebraically closed. Now, we use this to conclude that $K = k$, since K is a finite field extension of an algebraically closed field (finite as module).

Therefore, $x_i = a_i \in k$ as an element of K, so I contains $(x_1 - a_1, x_2 - a_2, \ldots)$. □

Remark 3.1. What if k were not algebraically closed? Then, maximal ideals can be given by mapping $x_1, \ldots, x_n$ in some finite algebraic extension of k. In this case, maximal ideals would correspond to $\bar{k}^n$ modulo the action of the Galois group.

Example 3.2. Let $k = \mathbb{R}$. The polynomial ring $k[x]$ has maximal ideal $(x^2 + 1) \leftrightarrow$ pair of points $\pm i \in \bar{\mathbb{R}} = \mathbb{C}$.

Recall theorem from the theory of C^* algebras.

Definition 3.3. A C^* algebra is the algebra of bounded continuous functions on compact space X. Analogous to polynomial functions on $\mathbb{A}^n$.

Theorem 3.4 (Gelfand)**.** *$X \equiv$ closed maximal ideals of A. Point of $X \to$ maximal ideal of functions vanishing there.*

Theorem 3.5 (Strong Nullstellensatz)**.** *Arbitrary closed subsets of $\mathbb{A}^n$ correspond to radical ideals in $k[x_1, \ldots, x_n]$.*

Proof. We prove the Strong Nullstellensatz from the Weak one, using the Rabinowitsch Trick. The clever idea is to introduce a new variable x_0.

We want to show that $I(Z(a)) = \sqrt{a}$. The inclusion $\sqrt{a} \subseteq I(Z(a))$ is trivial. We need to show $I(Z(a)) \subseteq \sqrt{a}$.

Suppose $f \in I(Z(a))$. We need to show that $f^n \in a$ for some n. Suppose $a = (f_1, \ldots, f_m)$ so $f = 0$ at some point of $\mathbb{A}^n$ if $f_1, \ldots, f_m$ are all 0. Then: $f_1, \ldots, f_m, 1 - x_0 f$ have no zeros in $\mathbb{A}^{n+1}$

Since they have no common zeros in k^{n+1}, they are not in any maximal ideal of $k[x_0, \ldots, x_n]$ by the Weak Nullstellensatz; therefore, they must generate the whole ideal $k[x_0, \ldots, x_n]$. In particular,

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

for some $g_i \in k[x_0, \ldots, x_n]$. $1 \in$ the ideal $(1 - x_0 f, f_1, \ldots)$.

Now, let $x_0 = \frac{1}{f}$ in $k(x_1, \ldots, x_n)$. So, $1 = g_1 f_1 + \cdots g_m f_m$ in the field of rational functions with denominators powers of f. Clear denominators by multiplying by high power of f. This gives us the relation:

$$f^n = h_1 f_1 + \cdots + h_m f_m.$$

Therefore, $f \in \sqrt{a}$. □

Example 3.6. The intersection of $y = 0$ with $y = x^2$ is the point $(0, 0)$. Look at the ideal generated by (y) and $(y - x^2)$. The ideal (x^2, y) is not radical; its radical is (x, y).

Example 3.7. Look at the set of nilpotent $n \times n$ matrices M as a subset of $\mathbb{A}^{n^2}$. Such a matrix si nilpotent when $M^n = 0$. It is given by the ideal generated by all n^2 entries of M^n. Therefore, the ideal is generated by n^2 homogeneous degree n polynomials in $k[x_{11}, \ldots, x_{nn}]$.

The ideal is not radical. One polynomial vanishing on all the nilpotent matrices *not* in the ideal I is the trace of the matrix. Why is this zero and why is it not in I?

M nilpotent implies that the eigenvalues are zero, so the trace $= \sum$ eigenvalues is also 0. I is generated by homogeneous elements of degree n so it contains no elements of degree $1 < n$.

Conclusion by the Nullstellensatz: some power of the trace is in the ideal generated by entries of M^n.

Exercise 3.8. Consider the case of $n = 2$. What is the smallest power of $a + d$ (trace) in the ideal

$$\begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix}$$

Warning: $(a + d)^2$ is not in the ideal.

Problem : Find the radical of a given ideal in $k[x_1, \dots, x_n]$ given by a set of generators. Variation: Test if an ideal is radical. These problems are actually really hard.

Example 3.9. Look at ideal given by pairs of commuting matrices: Form the variety in $\mathbb{A}^{2n^2}$ given by the entries $MN - NM$, where M, N are $n \times n$ matrices. The ideal is given by n^2 polynomials of degree 2 in $2n^2$ variables.

Problem: Is the ideal radical?

Answer: No one knows.

We have shown that radical ideals correspond to closed subsets of $\mathbb{A}^n$; what do arbitrary ideals correspond to? Closed subschemes.

A closed subset is a finite union of irreducibles, and we find a similar decomposition for submodules. Proved by E. Lasker (then the world chess champion) 50 years before the definition of a scheme. He proved a theorem regarding ideals which has this nice consequence for schemes. The proof was 100 pages long, at a time when this was very rare.

Theorem 3.10 (Lasker)**.** *Any ideal in $k[x_1, \dots, x_n]$ is the intersection of primary ideals.*

Recall that intersection of ideals corresponds to union of closed subsets. Primary ideals are a generalization of the ideals of irreducible subsets.

Definition 3.11. Take $P \subset R$ ideal. P primary means that if $ab \in P$ then $a \in P$ or $b^n \in P$.

Example 3.12. In $\mathbb{Z}$, (n) prime ideal iff n is a prime p; (n) is primary iff $n =$ prime power p^k.

Noether generalized Lasker's Theorem to all Noetherian rings. Her proof was approximately 3 sentences long. Instead of looking at the ideal I, we should look

Definition 3.13. An associated prime is a prime ideal annihilating some element of a module. Roughly speaking, a f.g. module is built out of modules of the form R/P_i, where P_i are associated primes of the module.

Proposition 3.14. *I is primary iff the module R/I has only one associated prime. (The module is called coprimary.) Alternatively, I is primary iff A is a primary submodule of R.*

Remark 3.15. Primary is not defined for modules, but only for submodules. M is a primary submodule of N if N/M is coprimary.

Theorem 3.16 (Lasker-Noether for Finitely Generated Modules over a Noetherian Ring)**.** *If M is a finitely generated module over a Noetherian ring R, 0 is the intersection of primary submodules. Special case: $M = R/I$, for $I \subset R$ ideal, then $I = \bigcap$ primary ideals.*

4. Tuesday, September 4, 2012

Recall Theorem 3.16 from last time.

Proof. (1) In any finitely generated module M over a Noetherian ring R, 0 is the intersection of irreducible submodules.

Recall that, by definition, an irreducible submodule cannot be expressed as the intersection of two larger submodules. Look at the maximal ideal not an intersection of two larger ideals.

(2) With M and R as above, every irreducible submodule N is primary.

M/N is coprimary means that M/N has only one associated prime $\mathfrak{p}$. This means that $\mathfrak{p}$ is the annihilator of some element. Take quotient by N. Reduce to case when $N = 0$.

We only need to show that 0 irreducible in $M \Rightarrow M$ coprimary (only one associated prime).

Suppose $\mathfrak{p}, \mathfrak{q}$ are two associated primes. Then M has submodules isomorphic to $R/\mathfrak{p}$ and $R/\mathfrak{q}$ with 0 intersection, as the annihilator of any nonzero element of these submodules is $\mathfrak{p}$ in $R/\mathfrak{p}$ or $\mathfrak{q}$ in $R/\mathfrak{q}$. Therefore, the intersection is 0 if $\mathfrak{p} \neq \mathfrak{q}$.

So if M has > 1 associated prime, 0 is not irreducible.

□

Exercise 4.1. Show that for R Noetherian, $R/\mathfrak{q}$ coprimary $\Rightarrow$ $\mathfrak{q}$ is primary in Lasker's sense.

Example 4.2. Consider the ideal $I = \langle xy, y^2\rangle \subset k[x, y]$. Geometrically, the algebraic set is the intersection of the pair of axes and the y-axis; could be thought of as the x-axis and an "infinitesimal distance" at the origin.

We can then decompose this as the union of the x-axis, and the infinitesimal distance. The corresponding ideals are (y) and (x, y^2).

This gives a (non-unique) primary decomposition $\langle xy, y^2\rangle = \langle y\rangle \cap \langle x, y^2\rangle$. The radical of these ideals are $\langle y\rangle \cap \langle x, y\rangle$.

The decomposition of an algebraic set into irreducible components, however, *is* unique (assuming you do it sensibly).

For schemes and ideals, decomposition not always unique. In the example, $(xy, y^2) = (y) \cap (x, y^2) = (y) \cap (x + y, y^2) =$ many other decompositions. However, the (y) part is the same in each.

The non-unique part is called an embedded component: the underlying algebraic set is contained in the underlying algebraic set of another component. Primary ideals of embedded components tend not to be unique, though their radicals are unique.

Example 4.3 (Structure Theorem for Finitely-Generated Abelian Groups)**.** Recall that any abelian group A can be written

$$A \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \frac{\mathbb{Z}}{p_1^{n_1}} \oplus \frac{\mathbb{Z}}{p_2^{n_2}} \oplus \cdots .$$

What are the primary submodules? Those with quotient $\mathbb{Z}$ or $\frac{\mathbb{Z}}{p^n}$. This means that $0 \subsetneq A$ is the intersection of primary submodules.

However, as above, if you take $A \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, the decomposition is not unique. If a generates the $\mathbb{Z}$ subgroup, and b generates the $\mathbb{Z}/2\mathbb{Z}$ subgroup, then $(a + b)$ is another generator for the $\mathbb{Z}$ subgroup. The ideal corresponding to $\mathbb{Z}$ is (0) and the ideal corresponding to $\mathbb{Z}/2\mathbb{Z}$ is (2). Since $(0) \subsetneq (2)$, the latter ideal corresponds to an embedded component; therefore, the submodule with quotient $\mathbb{Z}/2\mathbb{Z}$ is not unique.

Warnning: Primary does not mean power of a prime. (It only does in a Dedekind domain)

Example 4.4. $R = k[x, y]$. $\mathfrak{p} = (x, y)$ the prime ideal of functions vanishing at the origin. $\mathfrak{p}^2 = (x^2, xy, y^2)$, etc., but there are many other primary ideals. Take any ideal in $\mathfrak{p}$ containing $\mathfrak{p}^n$.

Summary:

Affine algebraic sets	$\Leftrightarrow$	finitely generated algebras R over k with no nilpotent elements.
$Z \subseteq k^n$	$\Leftrightarrow$	ideal I of polynomials in $k[x_1, \ldots, x_n]$ vanishing on it. $R = k[x_1, \ldots, x_n]/I$.

Hilbert's Nullstellensatz says that this is essentially a bijection. A finitely generated algebra R is of the form $k[x_1, \ldots, x_n]/I$ for some I. R has no nilpotents iff $I = \sqrt{I}$. The corresponding affine algebraic set is the subset of points where I vanishes.

What is this theorem good for?

Example 4.5. Take the quotient of algebraic set A by group of automorphisms G. Does A/G have natural structure of an algebraic set?

Thanks to Hilbert, we can translate this to an algebraic problem: What should be the polynomial functions on A/G?

They should be the polynomial functions on A invariant under G.

This is obviously a k-algebra, and it obviously has no nonzero nilpotents. Is it finitely generated as a k-algebra?

If so, then we get a good candidate for the quotient.

Consider the affine space $\mathbb{A}^n$ acted on by symmetric group S_n permuting coordinates. What is the quotient $\mathbb{A}^n/S^n$ as an algebraic set?

The coordinate ring is $k[x_1, \ldots, x_n]$. S_n permutes the set $x_1, \ldots, x_n$. The ring of invariants are the symmetric polynomials in $x_1, \ldots, x_n$ = Polynomial ring on the elementary symmetric polynomials:

$$e_1 = x_1 + \cdots x_n; \qquad e_2 = x_1x_2 + \cdots + x_{n-1}x_n; \qquad \cdots \qquad e_n = x_1x_2 \cdots x_{n-1}x_n.$$

Therefore, the ring of invariant functions is a polynomial ring $k[e_1, \ldots, e_n]$ so the corresponding quotient is isomorphic to $\mathbb{A}^n$.

Warning: the quotient by group action is usually very messy. Quotients by (complex) reflection groups such as S_n happen to be very nice.

Example 4.6. Take $n = 1$, $k = \mathbb{R}$. Take the action of pairing x and $-x$. The topological quotient is the half-line originating at 0, however the algebraic set of $\mathbb{R}[e_1]$ = the affine line with pairs of real numbers to the right of the origin, and pairs of imaginary numbers to the left.

Over non-algebraically closed fields, the quotient given by the ring of invariants is not exactly the same as the quotient of topological spaces.

4.1. **Classical Invariant Theory.** Take group $SL_2(\mathbb{C})$, i.e. 2×2 matrices with determinant 1. This acts on the space of all homogeneous polynomials, mapping

$$f(x, y) = a_nx^n + a_{n-1}x^{n-1}y + \cdots + a_0y^n \qquad \text{via } x \mapsto ax + by, y \mapsto cx + dy.$$

i.e. action of $SL_2(\mathbb{C})$ on $(n+1)$-dimensional space $\langle a_0, \ldots, a_n \rangle$. What is the quotient $\mathbb{A}^{n+1}/SL_2(\mathbb{C})$?

Answer: Look at the ring of invariants = polynomials $k[a_0, \ldots, a_n]$ invariant under $SL_2(\mathbb{C})$. This should be coordinate ring of quotient IF it is finitely generated.

Question 4.7. Problem 1: Is this ring finitely generated?

Answer: Yes. (Paul Gordan)

Question 4.8. Problem 2: Find the set of generators.

This is a real mess. In the 19th century, they calculated up to $n = 8$ (or 12), where they found hundreds of generators.

For the case $n = 2 : a_2x^2 + a_1xy + a_0y^2$, the invariants are generated by the discriminant $a_1^2 - 4a_0a_2$.

Question 4.9. Variation 1: What is the big deal about these particular representations of $SL_2(\mathbb{C})$?

Answer: Nothing really. Any representation of $SL_2(\mathbb{C})$ is a direct sum of copies of these representations. What are the invariants of $SL_2(\mathbb{C})$ acting on a sum $V_1 \oplus V_2 \oplus \cdots$ of irreducibles?

[Notation was strange back then, invariants were sometimes called concomitants.]

"Covariants": invariants of $SL_2(\mathbb{C})$ acting on $V \oplus V_2 \oplus V_2 \oplus \cdots$ where the latter denotes two-dimensional representations of $SL_2(\mathbb{C})$.

Gordan proved that these rings of invariants are also finitely-generated.

Another variation: Change $SL_2(\mathbb{C})$ to $SL_n(\mathbb{C})$.

$SL_n(\mathbb{C})$ acts on homogeneous polynomials in n variables of degree m.

Question 4.10. Is this ring of invariants finitely-generated?

Answer: Yes (Hilbert).

Note 1: Gordan probably did NOT complain that this was theology.

Note 2: Hilbert's proof was essentially constructive.

Question 4.11. Suppose G is a group acting on $k[x_1, \ldots, x_n]$. Is the ring of invariants finitely-generated?

Hilbert: Yes, if $k = \mathbb{C}$ and $G = SL_n(\mathbb{C})$ or a finite or reductive group.

Haboush-Nagata: Yes, if k is any field and G is reductive.

Nagata: NO, in general. Look at k acting on k^2 by $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Take 16 copies of this: we get k^{16} acting on $k^{32} = \mathbb{A}^{32}$. Nagata: Take G = 13-dimensional generic subspace of k^{16}, acting on $k[x_1, \ldots, x_{32}]$. Then the ring of invariants is not finitely-generated.

This counterexample is quite disturbing, especially since we have an abelian group producing this non-f.g. ring of invariants, where the non-abelian group $SL_n(\mathbb{C})$ produces a f.g. ring.

5. Thursday, September 6, 2012

Recall: Affine algebraic sets $\longleftrightarrow$ finitely-generated k-algebras with no nilpotents (the "coordinate rings", or ring of functions on the set).

Analogous to: Compact space $\longleftrightarrow$ Commutative C^* algebras.

We used this correspondence to turn a question of solutions to $x^2+y^2 = z^2$, i.e. homomorphisms

$$\mathbb{Z}[x, y, z]/(x^2 + y^2 - z^2) \to \mathbb{Z}.$$

into a question of finding points on a circle.

In the opposite direction, we turned the question of whether an algebraic set modulo a group action is algebraic, into a question of looking at whether the ring of G-invariants as a subset of the coordinate ring was finitely generated.

Theorem 5.1 (Hilbert)**.** *Suppose G is a reductive group [over $\mathbb{C}$] acting on a vector space V. Then the ring of invariants R^G is finitely generated. (R = polynomials on V).*

Proof. We do the case when G is a finite group.

$R = R_0 \oplus R_1 \oplus \cdots$ is a graded polynomial ring. $R_0 = k$, and $R_1 = V$ (or V^*).

R^G is a graded subring of R: $R^G = R_0^G \oplus R_1^G \oplus \cdots$.

Let I be the ideal of R generated by positive degree elements of R^G.

Then I is finitely-generated as an ideal in R by Hilbert's basis theorem.

So we can find a generating set $i_1, i_2, \ldots, i_k$ of I of elements that we can assume are homogeneous. These generate I as an ideal.

We want to show that they generate $R^G \subseteq I \oplus k$ as an algebra. This generally is a much stronger statement.

Example 5.2. Consider $R = k[x, y]$, with subring S which has monomials $1, y^n, x^m y^n$, for $m \geq 1, n \geq 1$. As an ideal, the positive degree monomials of S are generated by y. However, as an algebra, it is not finitely generated; a generating set is $\{1, y, xy, x^2y, x^3y, \ldots\}$.

How do we exclude this sort of behavior? Need some special property of the subring R^G of R not satisfied by all subrings. The special property: R^G has a Reynolds Operator $\rho : R \to R^G$ mapping each element of R to its average value. In our context,

$$\rho(r) = \frac{1}{|G|} \sum_{g=G} g(r).$$

In defining this operator, we rely on the fact that G is finite, and that we work in characteristic 0. (Much harder in positive characteristic).

Remark 5.3 (Historical Note)**.** Reynolds was a fluid mechanic, famous for the Reynolds number. The Reynolds operator was originally the idea to replace a turbulent flow by its average value over time. Take average under group of time translations.

What properties does ρ have?

$$\rho(a+b) = \rho(a) + \rho(b). \qquad \rho(a)\rho(b) = \rho(ab), \text{ if } a \in R^G(\rho(a) = a), \qquad \rho\rho(a) = \rho(a).$$

Essentially, ρ is a projection from R onto R^G, and is a homomorphism of R^G-modules.

We show by induction on degree of $x \in R^G$ that x is generated by $i_1, \dots, i_k$ as an algebra.

We know that $x = r_1 i_1 + r_2 i_2 + \cdots + r_k i_k$ for some $r_k \in R$ since those are generators of the ideal. Now, we apply the Reynolds operator.

$$\Rightarrow x = \rho(x) = \rho(r_1) i_1 + \cdots + \rho(r_k) i_k.$$

Recall that the i's are fixed by G. By induction, $\rho(r_i)$ is a polynomial in the i's, so x is also a polynomial in i's. □

Extension to other groups:

(1) Compact groups. Because we can take average under compact group.

$$\frac{1}{|G|} \sum_{g \in G} g(r) \longrightarrow \int_{g \in G} g(r) d\mu.$$

where μ is a Haar measure.

(2) What about noncompact groups? This sometimes fails: Nagata's counterexample shows that it does not work for the group $\mathbb{C}^{16}$.

(3) $SL_2(\mathbb{C})$, though non-compact, has a Reynolds operator. The reason is that its finite-dimensional representations are more or less the same as those of the compact group SU_2. (This proof uses Lie algebras) $SL_2(\mathbb{C})$ has Lie algebra $SL_2(\mathbb{C}) = 2 \times 2$ matrices of trace 0. SU_2 has a Lie algebra $SU_2 =$ skew-hermitian matrices of trace 0.

The complexification of SU_2, i.e. $SU_2 \otimes \mathbb{C} = SL_2(\mathbb{C})$. Actions of the real Lie algebra SU_2 on complex vector spaces are the same as actions of complex Lie algebra $SL_2(\mathbb{C})$ on complex vector spaces.

Weyl's unitarian trick states that groups with such a property work like compact groups in certain ways. (The same works for any semi simple Lie group over $\mathbb{C}$).

What is the point of all this? Specifically, why should algebraic geometers care about quotients A/G? Geometric invariant theory, invented by Mumford. Many moduli spaces constructed are quotients of this form.

Moduli space is roughly a space whose points classify some geometric objects, such as elliptic curves.

Example 5.4. Suppose we try to classify elliptic curves. Naive definition: a (non-singular) degree 3 plane curve. Degree 3 (projective) plane curves are written as

$$a_{300}x^3 + a_{210}x^2y + \cdots + a_{003}z^3 = 0.$$

The 10 coefficients can live in some 10-dimensional affine space. We should really quotient out by k^* and throw away the point with all $a_i = 0$.

So, rather than affine space $\mathbb{A}^{10}$, we should really work with projective space $\mathbb{P}^9$.

Often, two of these degree 3 curves will be isomorphic. For example, if we make a linear change of variables in x, y, z. So we have a group $GL_3(\mathbb{C})$ acting on 10-dim affine space.

So, the isomorphism classes of elliptic curves should really have something to do with $\mathbb{P}^9/\mathbb{P}GL_3(\mathbb{C})$. Since the former has (projective) dimension 9 and the latter has dimension 8, we would expect the space to have dimension 1.

Example 5.5. Problem: Classify hyperelliptic curves. If we define elliptic curves as the solution set of $y^2 = x^3 + ax + b$. Hyperelliptic curve (naive definition): $y^2 = a_n x^n + a_{n-1}x^n + \cdots + a_0$.

A more abstract definition: a curve which is a branched double cover of the affine/projective line. One morphism may take $(x, y) \mapsto x$. This is mostly a $2 : 1$ map. However, whenever $y = 0$, there is only one value, so we get a branch point.

Taking $a_n x^n + \cdots + a_0 = a_n(x - \alpha_1) \cdots (x - \alpha_n)$, the branch points will be at the α_i's.

How do we classify these curves? Same as classifying homogeneous polynomials: $a_n x^n + a_{n-1}x^{n-1}z + \cdots + a_0 z^n$, which in turn is the same as classifying "sets" (allowing repetitions) of n points in projective line. We want to classify up to isomorphism. In other words, up to action of $SL_2(\mathbb{C})$ on these sets.

$SL_2(\mathbb{C})$ acts on homogeneous polynomials by $x \mapsto ax + bz$, and $z \mapsto cx + dz$. $SL_2(\mathbb{C})$ acts on the Riemann sphere $\mathbb{C} \cup \infty$ by $\alpha \mapsto \frac{a\alpha+b}{c\alpha+d}$ for $\alpha \in \mathbb{C} \cup \infty$.

So we get action on finite sets of points in $\mathbb{C} \cup \infty$.

What is the quotient? Coefficients of $a_n x^n + \cdots + a_0 z^n$ form $(n + 1)$-dimensional affine space acted on by $SL_2(\mathbb{C})$. So we can take the quotient to be the space with coordinate ring, the ring of invariants

$$\mathbb{C}[a_0, a_1, \ldots, a_n]^{SL_2(\mathbb{C})},$$

which was studied by 19th century invariant theory of binary quintics.

Example 5.6. Cyclic quotient singularities. Let G = finite cyclic group $\mathbb{Z}/n\mathbb{Z}$ acting linearly on a complex vector space V. What does the quotient V/G look like? V splits as the sum of 1-dimensional spaces. $V = V_1 \oplus V_2 \oplus \cdots$. Let v_i = basis of V_i, and g be a generator of G. We have $g(v_i) = \epsilon(v_i)$, for some ϵ_i, with $\epsilon_i^n = 1$. Put $\epsilon = e^{2\pi i/n}$ = primitive n-th root of unity.

Take $\dim V = 2$, spanned by x, y, with $g(x) = \epsilon x, g(y) = \epsilon y$.

Find the ring of invariants:

$$\begin{array}{ccccc}
y^n & & & & \\
\vdots & y^{n-1}x & & & \\
y^2 & & \ddots & & \\
y & xy & & & \\
1 & x & x^2 & \cdots & x^n
\end{array}$$

where each diagonal has a factor some power of ϵ, and the n-th diagonal has $\epsilon^n = 1$, so is invariant.

So the invariants are spanned by $x^i y^j$, where $i + j$ divisible by n.

Generators for the ring are $x^n, x^{n-1}y, \cdots, y^n$ (corresponding to the a_i's), together with a bunch of relations, e.g. $x^{n-3}y^3 * x^n = x^{n-1}y * x^{n-2}y^2$. In other words, $a_i a_j = a_k a_l$ if $i + j = k + l$.

So the ring has $n+1$ generators and *lots* of relations. Corresponding algebraic set has complicated singularity at origin. Symmetric group S_n acting on $\mathbb{A}^n$. Quotient needed few generators, no relations, no singularities.

6. Tuesday, September 11, 2012

6.1. **Dimension.** Intuitively, it is obvious what dimension is; yet, it is hard to define or work with.

First, we consider the notion of dimension in Hausdorff spaces.

Cantor proved that $\mathbb{R}^1$ has the same number of points as $\mathbb{R}^2$. Polya provided a continuous map from $\mathbb{R}^1$ onto $\mathbb{R}^2$. Problem: Show $\mathbb{R}^3$ not homeomorphic to $\mathbb{R}^4$.

Example of a definition of dimension:

Definition 6.1. Lebesgue covering dimension of a space is the smallest number n such that any open cover has a refinement with no point in $> n+1$ open sets.

It is *hard* to prove that $\mathbb{R}^n$ has Lebesgue covering dimension n.

All definitions above fail in algebraic geometry. The affine line with Zariski topology has covering dimension $= \infty$.

One option is to find "flags" of point $\subset$ curve $\subset \mathbb{A}^2$, for example. This leads to the following definition:

Definition 6.2. The dimension is the supremum of integers n such that we can find strictly increasing chains $I_0 \subset I_1 \subset \cdots \subset I_n$ of irreducible subsets.

It is obvious that $\mathbb{A}^n$ has dimension $\geq n$. Specifically, $\mathbb{A}^0 \subset \mathbb{A}^1 \subset \cdots \subset \mathbb{A}^n$. However, it is hard to show that $\mathbb{A}^n$ has dimension $\leq n$. Not clear what "all" irreducible subsets of $\mathbb{A}^n$ look like.

Another option is to transfer to a question about rings.

Definition 6.3. The Krull dimension of a ring R is defined as the supremum of integers n with a chain of prime ideals $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$.
(Recall that prime ideals correspond to irreducible subsets).

We can reduce to the case of local rings. (Recall that a local ring is a ring with a unique maximal ideal. Informal picture: Ring of functions defined near a point.)

Example 6.4. Consider $\mathbb{A}^n$, with coordinate ring $R = k[x_1, \ldots, x_n]$. What is the local ring at $(0, \ldots, 0)$? Informally, all functions defined near 0. We can take the inverse at an polynomial p, such that $p(0, \ldots, 0) \neq 0$. The local ring is the ring of all rational functions p/q with $q \neq 0$ at $(0, \ldots, 0)$. [This is the localization $R_{(x_1, \ldots, x_n)}$.]

In general, we can "invert" those elements not in a specified prime ideal. If R is an integral domain, then this is straightforward: Localization is a subring of the field of fractions. (If R is not an integral domain, things get trickier.)

If $\mathfrak{p}$ is a maximal ideal of R (corresponding to a point), then primes of R contained in $\mathfrak{p} \leftrightarrow$ primes of localization of R at $\mathfrak{p}$. So, using this notion:

Definition 6.5.

$$\dim(R) = \sup_{\mathfrak{p} \text{ prime}} \dim R_{\mathfrak{p}}.$$

Geometric meaning: dimension of local ring is roughly "local" dimension of an algebraic set.

We end up using a less intuitive but easier-to-work-with algebraic definition. The basic idea is that higher dimensional spaces have more functions on them.

Definition 6.6. Dimension is the transcendence degree of the quotient field of the coordinate ring.

Example 6.7. $\mathbb{A}^n$ has coordinate ring $k[x_1, \ldots, x_n]$. The quotient field is $k(x_1, \ldots, x_n)$ (rational functions); this has transcendence degree $= n$.

The elliptic curve $y^2 = x^3 + ax + b$. The coordinate ring is $k[x,y]/(y^2 - x^3 - ax - b)$. The quotient field is in $k(x,y)$, and in the chain

$$k \subset k(x) \subset k(x,y),$$

the first extension has transcendence degree 1, and the second is algebraic. So the function field has tr.deg 1.

Problems with using transcendence degree for dimension:

It breaks down for schemes. It only works for coordinate rings that are defined over a field, and with no zero divisors.

The problem remains to: find a definition that

(1) Works for all rings.
(2) Is easy to calculate.

Remark 6.8 (In response to a question about non-Noetherian ring)**.** Consider the ring $\frac{k[x_1, x_2, \ldots]}{(x_1^2, x_2^2, \ldots)}$. This is a non-Noetherian ring, but it has Krull dimension zero.

Furthermore, Nagata showed that Noetherian rings can have dimension $= \infty$.

Only need this for *local* rings R. R has a maximal ideal $\mathfrak{m}$: "functions vanishing at a point." $\mathfrak{m}^2$ are "functions vanishing to order 2. $\mathfrak{m}^3, \mathfrak{m}^4, \ldots$ can be understood in the same way.

If R is Noetherian, $\mathfrak{m}^n$ is finitely generated as an ideal, so $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is a finite dimensional vector space over $R/\mathfrak{m}$.

We will see later that $\dim(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ is polynomial in n for n large (if R is Noetherian). The degree of this polynomial +1(?) is dimension.

Example 6.9. Let $R = k[x, y]/(y^2 - x^3)$. What is the dimension of the local ring at 0? In this case, $\mathfrak{m} = (x, y), \mathfrak{m}^2 = (x^2, xy, y^2) = (x^2, xy)$, since $y^2 = x^3$.

$n =$	0	1	2	3	$\cdots$
dim	1	2	2	2	$\cdots$

This is polynomial of degree 0 for large n, so the ring has dimension 1.

6.2. **Examples of "Unexpected" Dimension.**

Example 6.10. Dimension of space of configurations of cyclohexane, a molecule of roughly hexagonal shape with one fixed angle.

Let us guess the dimension:

We start with 18-dimensional space of all possible positions of vertices in $\mathbb{A}^3$.

The possible intersection of 12 quadrics giving distance between adjacent points or next-to-adjacent points. There is a 6-dimensional group of translations/rotations.

So space of configurations should have dimension $18-12-6 = 0$, which would mean the molecule should be rigid.

However, something surprising happens and we have two components: one with degree 0 and one with degree 1.

Example 6.11. Dimension of the Hilbert scheme of n points in $\mathbb{A}^m$. (Misleading description: the space whose points parametrize collections of n points).

Naive guess for dimension: mn, each of the n points contributing m coordinates to the dimension. This works for $m = 1, 2$, and fails horribly for $m \geq 3$.

Consider the Hilbert scheme of n points $\alpha_1, \ldots, \alpha_n$ in $\mathbb{A}^1$. Look at the polynomial $(x-\alpha_1)\cdots(x-\alpha_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. This is the space of polynomials of degree n with leading coefficient 1, indexed by affine space $\mathbb{A}^n$ which has dimension n.

Sets of n points correspond to ideals of $k[x]$ of codimension n. The ideal is $(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$. Really, the Hilbert scheme classifies subschemas of dimension 0, degree n rather than sets of n points; ideals of $k[x_1, \ldots, x_m]$ of codimension n.

What is the dimension of this space of ideals? Naive arguments suggest dimension is mn, but this is wrong. Suppose $m \geq 3$. Focus on "sets of points all at $(0, \ldots, 0)$". In other words, look at the ideals contained in the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_m)$.

Look at the ideals I that lie between $\mathfrak{m}^k$ and $\mathfrak{m}^{k+1}$, i.e. $\mathfrak{m}^k \supseteq I \supseteq \mathfrak{m}^{k+1}$. What is the dimension of this space of ideals I? Ideal $\mathfrak{m}^k$ has codimension (polynomial of degree 3 in k), since $\dim(\mathbb{A}^3) = 3$. So $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ has degree (polynomials of degree 2 in k).

$\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a vector space. Any subspace gives an ideal of $k[x_1, \dots, x_m]$.

Set of all subspaces of dimension a of vector space of dim $a + b$, is called the Grassmannian and has dimension ab. So look at the subspaces of $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ of about half its dimension. The space of such subspaces has dimension about $\left(\frac{\dim(\mathfrak{m}^k/\mathfrak{m}^{k+1})}{2}\right)^2 \cong$ polynomials of degree 4 in k gives the space of ideals of codimension $\leq \dim R/\mathfrak{m}^k$, which is described by $P(k)$ a polynomial of degree 3, has dimension given by the polynomial $Q(k)$ in k of degree 4.

Eventually, $Q(k) > 3P(k) = mn$. So, the dimension of spaces of codimension n ideals in $k[x_1, \dots, x_m]$ has dimension *much* bigger than one would guess from naive arguments (if $m \geq 3, n$ large).

6.3. **Projective Varieties.**

Definition 6.12. Projective space = 1-dimensional subspaces of $\mathbb{A}^{n+1}$ = points $(x_0 : x_1 : \cdots : x_n)$ not all zero, with the equivalence relation $(x_0 : x_1 : \cdots) \equiv (\lambda x_0 : \lambda x_1 : \cdots)$, for $\lambda \neq 0$.

Remark 6.13. The projective space $\mathbb{P}^n$ contains an affine space $\mathbb{A}^n = (1 : x_1 : \cdots : x_n)$. Specifically,

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

where $\mathbb{A}^n$ has first coordinate 1, and $\mathbb{P}^{n-1}$ has first coordinate 0. By induction,

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \cdots \cup \mathbb{A}^1 \cup \mathbb{A}^0.$$

An alternative visualization is $\mathbb{P}^n$ = the union of $n + 1$ copies of affine space: open subsets given by fixing each of the $n + 1$ variables to be 1. [Note that these are *not* disjoint.]

Remark 6.14. $\mathbb{P}^n$ is a "compactification" of affine space over $\mathbb{R}$ or $\mathbb{C}$. Over $\mathbb{R}$: map from $S^n \to \mathbb{P}^n$, by $(x_0, \dots, x_n), \sum x_i^2 = 1 \mapsto (x_0 : \cdots : x_n)$. This map is $2 : 1$ and onto, so because the pre-image is compact, $\mathbb{P}^n$ is also compact.

Historical Note: The synthetic definition of projective space. Study of properties of space $\mathbb{R}^3$ invariant under projection.

Example 6.15. Projection of real world object onto 2-dimensional painting.

7. Thursday, September 13, 2012

7.1. **Classical (Synthetic) Projective Geometry.**

"Synthetic" means that it uses axioms for lines and points, while "analytic" geometry uses coordinates.

The basic data for projective space are the set of points, set of lines, and *incidence relation* between points, lines, i.e. "this point lies on that line."

Axioms for Projective Space:

(1) Any two distinct points lie on a unique line.
(2) Any two lines in the same plane meet at a point.
(3) (What is a plane? Two lines are said to be in the same plane, if there are two pairs of points, one in each line, such that the lines joining them intersect. See Figure 1.)
(4) (Non-degeneracy: Any line meets ≥ 3 points.)

Example 7.1 (Basic example)**.** "Point" is a line in vector space over a division ring. "Line" is a plane in the vector space. This corresponds to the projective space of the vector space.

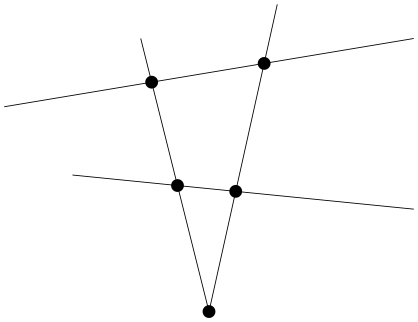

FIGURE 1. Lines in the Same Plane.

Example 7.2 (Other examples)**.** 1 line, with many points on it. Many examples in 2 dimensions called "non-Desarguesian planes."

Theorem 7.3 (Desargues' Theorem)**.** *Given an image as in Figure 5 then the three points are collinear.*

Proof. Three points lie in $\cap$ of two planes, so they lie on a line as long as the two planes are distinct (only in ≥ 3 dimensions). □

Examples of projective spaces where Desargues' Theorem does not hold have been found up to order 11 (i.e. with 11 points on each line) with the aid of computers. Order 12 seems to be outside the scope of computing power.

Remark 7.4 ("Fundamental Theorem of Projective Space")**.** Suppose a projective geometry in dim ≥ 2 satisfies Desargues' Theorem (automatic if dimension is ≥ 3). Then it comes from a vector space over a division ring.

When we mention dimension in synthetic geometry, we mean:

dim 0	Only points
dim 1	One line
dim 2	Distinct lines, but every pair meets
dim ≥ 3	Pair of non-intersecting lines.
$\vdots$	$\vdots$

Pappus's theorem in this context is equivalent to commutativity of the division ring. So, Synthetic projective geometry + Pappus's Theorem is equivalent to the study of projective space $(x_0 : \cdots : x_n)/\sim$ in algebraic geometry.

This approach has mostly been abandoned , but it has been generalized to BN pairs.

The BN pairs for the case of $GL_n(k)$ corresponds to axioms for projective geometry.

7.2. **Affine Space and Projective Space.** We want to translate our theorems about affine space to theorems in projective space. We have these correspondences in affine algebraic geometry:

$$\begin{array}{rcl} \text{Affine space } \mathbb{A}^n & \leftrightarrow & k[x_1, \ldots, x_n]. \\ \text{Affine Algebraic sets} & \leftrightarrow & \text{(radical) ideals.} \end{array}$$

We obtain the following for projective algebraic geometry:

Projective space $\mathbb{P}^n$	$\leftrightarrow$	$k[x_0, \dots, x_n]$ graded ring.
Projective algebraic set	$\leftrightarrow$	graded radical ideals.
Projective varieties in $\mathbb{P}^n$	$\leftrightarrow$	cones in $\mathbb{A}^{n+1}$.
all points $(x_0, x_1, \dots, x_n) \in \mathbb{A}^{n+1}$ on which elements of I vanish.	$\leftarrow$	I [where I is graded, this set is closed under multiplication by λ. So, it gives a subset of projective space.]

Example 7.5 (Twisted Cubic)**.** In affine space, this is the set of points

$$(t, t^2, t^3) \in \mathbb{A}^3.$$

The corresponding ideal is $(z - x^3, y - x^2)$.

We can extend to projective space $\mathbb{P}^3$ by homogenizing everything:

$$(t, t^2, t^3) \longrightarrow (1 : t : t^2 : t^3).$$

this point is not fixed by multiplication by λ, so we add in a variable s so that everything is the same degree:

$$(w : x : y : z) = (s^3 : s^2 t : st^2 : t^3),$$

for $(s : t) \neq (0, 0)$.

What is the corresponding ideal in $k[w, x, y, z]$?

Naive guess: Homogenize the ideal generators,

$$(z - x^3, y - x^2) \longrightarrow (w^2 z - x^3, wy - x^2).$$

Is this the ideal of the twisted cubic? A: No.

Something is wrong: $wz - xy$ vanishes on the twisted cubic, but is not in the ideal above!

What *is* the set of zeros of $(w^2 z - x^3, wy - x^2)$ in $\mathbb{P}^3$?

$\mathbb{P}^n$ is covered by $n + 1$ copies of $\mathbb{A}^n$; in our case, $\mathbb{P}^3$ is covered by 4 copies of $\mathbb{A}^3$. Look at each of these copies, setting $w = 1$, etc.

- For $w = 1$, we have the affine twisted cubic as expected.
- For $x = 1$, we get $wy = 1, w^2 z = 1$. This is again a single irreducible curve.
- When $y = 1$, we get $w = x^2, w^2 z = x^3 \subset \mathbb{A}^3$. Eliminate w we get $x^4 z = x^3$. We obtain two curves: $xz = 1$ (a piece of the twisted cubic), and $x^3 = 0$, an extra line with multiplicity 3.
- When $z = 1$, we get $wy = x^2, w^2 = x^3$. Eliminating gives $y^2 x^3 = x^4 \Rightarrow y^2 = x$ or $x^3 = 0$. This second piece is also a line of multiplicity 3.

We get not only the twisted cubic, but a "triple line." This corresponds to $(wy - x^2, w^2 z - x^3)$ not being irreducible.

It has primary decomposition:

$$(wy - x^2, y^2 - xz, wz - xy) \cap (wy - x^2, w^2, wx).$$

The first ideal is the true ideal of the twisted cubic. The second is not radical, and corresponds to the line at infinity.

(Moral of the story: Be careful when homogenizing.)

Example 7.6. Is the product of two projective varieties a projective variety?

This is trivial for affine varieties: Take $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$ with corresponding ideals $I \subseteq k[x_1, \dots, x_n], J \subseteq k[y_1, \dots, y_m]$ respectively. Then the ideal of $X \times Y$ is the ideal generated by $I + J \subseteq k[x, y]$.

This depends on the fact that

$$\mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}.$$

This is false for projective spaces:

$$\mathbb{P}^1 \times \mathbb{P}^1 \neq \mathbb{P}^2.$$

This fails Bezout's theorem, for instance. Any two curves in $\mathbb{P}^2$ intersect; however, the lines $\mathbb{P}^1 \times a, \mathbb{P}^1 \times b$ do not intersect.

Over $\mathbb{C}$, the cohomology groups of $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2$ are non-isomorphic, so the varieties are non-isomorphic. However, they are birational.

We can embed $\mathbb{P}^1 \times \mathbb{P}^1 \subseteq \mathbb{P}^3$, by the Segre embedding:

$$(a_0 : a_1) \times (b_0 : b_1) \longrightarrow (a_0 b_0 : a_0 b_1 : a_1 b_0 : a_1 b_1).$$

We label the coordinates $w_{ij} = a_i b_j$. This gives a map from $\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^3$, which is not onto. Is the image a projective variety?

Problem: Find homogeneous polynomials in $w_{ij}, i, j \in \{0, 1\}$ so that if polynomials vanish, the point of $\mathbb{P}^3$ is in the image of $\mathbb{P}^1 \times \mathbb{P}^1$. Obvious polynomial that vanishes on the image:

$$w_{00} w_{11} = w_{10} w_{01}.$$

Suppose the polynomial vanishes. By symmetry we can assume that $w_{00} \neq 0$, so we set $w_{00} = 1$. This leaves $w_{11} = w_{10} w_{01}$. This point is then the image of $(1 : w_{10}) \times (1 : w_{01})$.

Therefore, we have a map of $\mathbb{P}^1 \times \mathbb{P}^1$ onto a projective variety in $\mathbb{P}^3$. The variety is a quadric in $\mathbb{P}^3$, so it has two "rulings " by straight lines.

Any two nonsingular quadrics are isomorphic over $\mathbb{C}$. So any nonsingular quadric in 3-dimensional space has two rulings by straight lines. For example of such a quadric:

$$x^2 + y^2 + z^2 = 1,$$

the sphere. We can factor that equation as

$$(x + iy)(x - iy) = (1 - z)(1 + z)$$

which has lots of lines (?).

The construction for $\mathbb{P}^m \times \mathbb{P}^n$ is similar.

$$(a_0 : \cdots : a_m) \times (b_0 : \cdots : b_n) \mapsto (w_{ij})_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n}},$$

where $w_{ij} = a_i b_j$. This is a point with $(m + 1)(n + 1)$ coordinates. So we have a map:

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

Relations between the w's: $w_{ij} w_{kl} = w_{il} w_{kj}$.

As before, we can check that the map is onto the variety cut out by these equations.

Example 7.7 (Veronese Surface)**.** The Veronese surface is the set of points in $\mathbb{P}^5$ of the form

$$(x^2 : xy : y^2 : xz : yz : z^2), \qquad (x, y, z) \in \mathbb{P}^2.$$

The image is a projective variety, cut out by degree 2 polynomials like $w_{xx} w_{yy} = w_{xy} w_{yx}$, etc.

The Veronese Surface is given by the zeros of all similar equations, so it is a projective variety.

It is isomorphic to $\mathbb{P}^2$. We have a morphism from $\mathbb{P}^2 \to \mathbb{P}^5$, mapping $(x : y : z) \mapsto (x^2 : xy : y^2 : xz : yz : z^2)$.

Generalizations:

$$\mathbb{P}^n \longrightarrow \mathbb{P}^{N \text{ large}}, (x_0 : \cdots x_n) \mapsto (\text{coordinates are monomials of degree } m).$$

8. Thursday, September 20, 2012

[I was absent for class on Tuesday, September 18 due to Rosh Hashanah]

8.1. **Toric Varieties.** A rational cone gives you a finitely generated algebra (whose basis is the points in the cone), which leads to an algebraic variety.

If you have a map of cones $C_1 \to C_2$, this induces a map of algebras $A_1 \to A_2$, which gives a map $V_1 \leftarrow V_2$. We would prefer to avoid inverting arrows in this way.

Therefore, we introduce the dual cone.

Definition 8.1. The dual of a cone $C \subseteq R^n$ is the set of points x in dual space R^{n*}, such that $\langle x, c\rangle \geq 0$ for all $c \in C$.

So given rational cone C in R^n, the associated variety has coordinate ring with basis integral points in the dual cone C^*.

Definition 8.2. A "fan" of cones is obtained by gluing together varieties of cones.

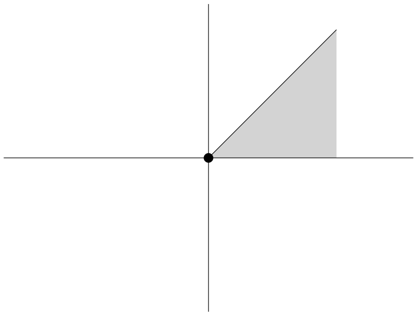

Figure 2. A Fan of Cones.

Example 8.3. Take two 1-dimensional cones glued together at a 0-dimensional cone.The dual cones to the 1-d cone are copies of the affine line, we can glue them together at the 0-d cone, by taking $k[x]$ and $k[y]$ to $k[x^{\pm 1}]$. This is the algebra of an affine line minus a point.

We could glue them to get a projective line, though we could also glue them to obtain the line with two origins.

Example 8.4. How would we obtain the projective plane? First guess: take the coordinate axes in the plane, and consider the four 2-d cones, the four 1-d cones, and the single 0-d cone. In fact, this gives us $\mathbb{P}^1 \times \mathbb{P}^1$. This fan is a product of 2 copies of the fan for $\mathbb{P}^1$.

Instead for the projective plane take three lines based at the origin as in Figure 3. This gives three 2-d cones, three 1-d cones and a point. This variety has coordinate ring $k[x, y, x^{-1}, y^{-1}]$.

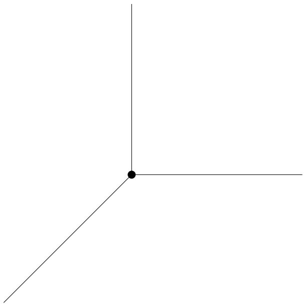

Figure 3. Projective Plane as a Toric Variety.

Remark 8.5. Why are they called toric? Because they all contain the torus as a dense subset. The torus as in product of copies of $\mathbb{A}^1-$ point. Corresponding dual cone $= \mathbb{R}^n$. So the coordinate ring is $k[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$.

The coordinate ring of $\mathbb{A}^n$ - hyperplanes $x_i = 0$ is $= S^1 \times R_{>0}$.

8.2. **Morphisms of Varieties.** Recall category theory. Look not only at objects, but at the morphisms between them.

Objects	Morphisms
Groups	Group Homomorphisms
Rings	Ring Homomorphisms
Topological Spaces	Continuous Maps

What is a morphism of varieties? One could give at least three reasonable answers:

(1) Two varieties in $\mathbb{P}^n$ are isomorphic if the map $\mathbb{P}^n \to \mathbb{P}^n$ taking one to the other. Oldest concept of morphism

Example 8.6. The Veronese surface is the image of a natural map $\mathbb{P}^2 \to \mathbb{P}^5$ by $(s : t : u) \mapsto (s^2 : st : t^2 : su : u^2 : tu)$. This does not constitute an isomorphism under the first definition.

(2) Birational equivalence and birational maps: "Morphisms defined almost everywhere." Birational varieties have the *same* field of rational functions on them. (Used until about 1950.)

Example 8.7. $\mathbb{P}^1$ and $\mathbb{A}^1$ are the same except on a subset of codim > 0.

(3) Regular map. The regular function on an affine variety (or algebraic set), is just an element of its coordinate ring. A regular function on an open subset (in the Zariski topology) of an affine variety is one locally of the form f/g, where $g \neq 0$ on some neighborhood of the point.

Remark 8.8. This seems to give two different definitions of regular functions on affine varieties; let us check that they agree. Suppose $V = U_1 \cup U_2 \cup \cdots$, for U_i affine open. Taking the second definition, suppose f is a function on V such that $f = g_i/h_i$ on U_i with $h_i \neq 0$ on U_i, and g_i, h_i regular functions on U_i (in its coordinate ring).

Is f then in the coordinate ring of the variety V?

The open sets U_i cover V. Suppose $V = k[x_1, \dots, x_n]/I$ for some ideal I. Then,

$$1 = a_1 h_1 + \cdots + a_n h_n \mod I,$$

for some $a_1, \dots, a_n$. Why? No maximal ideal contains all the h_i and I, as the U_i cover V. So, $1 \in$ the ideal generated by $I, h_1, \dots, h_n$.

So multiply both sides by f:

$$f = a_1 h_1 f + \cdots + a_n h_n f = a_1 g_1 + \cdots + a_n g_n \mod I.$$

Regular functions on a variety form a *sheaf.*

Example 8.9. A function is continuous/differentiable/smooth/analytic if it has this property locally everywhere.

Definition 8.10. Let V be a topological space. A presheaf S over V is given as follows:

(1) For each open set $U \subseteq V$, we have an abelian group $S(U)$. [Think of $S(U)$ as continuous real functions on U, e.g.]

(2) If $T \subseteq U$ we are given a morphism
$$\rho_{TU} : S(U) \to S(T).$$

(3) ρ_{TT} is the identity. $\rho_{RT}\rho_{TU} = \rho_{RU}$. (If we restrict from U to T then to R, the same as restricting from U to R).

Sheaf is a contravariant functor from the category of open sets of V to the category of Abelian Groups. (In the category of open sets of V, the morphisms: $T \to U$ are 1 if $T \subseteq U$ and none otherwise.)

[This is generalized by Grothendieck to give sheaves over Grothendieck topologies.]

This is a presheaf. The extra axioms are meant to capture the property that if a function is locally continuous/regular, then it is so globally. If f is continuous on U and g is continuous on V, and they agree on $U \cap V$, they give a continuous function on the union.

We need to translate into properties of S : open sets $\to$ groups.

Suppose V is covered by open sets U_i. Suppose given $f_i \in S(U_i)$ ("continuous function on U_i"), we have agreement on $U_i \cap U_j$. We cannot say that $f_i = f_j$ as they are elements of different groups. Instead we say that for all i, j,
$$\rho_{U_i, U_i \cap U_j}(f_i) = \rho_{U_j, U_i \cap U_j}(f_j).$$

Then, there exists a unique $f \in S(U)$ such that "$f = f_i$ on U_i"; this again does not make sense. We require instead that $\rho_{U,U_i}(f) = f_i$.

The regular functions of variety form a sheaf: $S(U) =$ regular functions on U. $S(U)$ is not just an abelian group, but is a ring. So, we have a sheaf of rings over any variety, whose restriction maps are ring homomorphisms.

We have something called a *ringed space*– a topological space with a sheaf of rings.

Definition 8.11. A morphism of varieties $U \to V$ is a continuous map of topological spaces such that the pullback of any regular function on an open set of V is regular. [Really a special case of a morphism of ringed spaces.]

Warning: analogous definition for schemes is incorrect– we should use morphisms of locally ringed spaces.

Example 8.12 (Regular Functions on Open Sets of $\mathbb{P}^1$)**.** What about $\mathbb{P}^1-$ point? This is just the affine line, so the regular functions $\cong k[x]$.

$\mathbb{P}^1-$ several points? This is again an affine line - points $a_1, \dots, a_n$. The regular functions are $k[x, (x-a_1)^{-1}, \dots, (x-a_n)^{-1}]$.

What about all of $\mathbb{P}^1$? We cover $\mathbb{P}^1$ by affine subsets. $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{A}^1$, which intersect in $\mathbb{A}^1-$ point. We want to find regular functions f, g on each $\mathbb{A}^1$ that agree on the intersection.

$$\begin{tikzcd}
k[x] \arrow[dr, "x\mapsto x"'] & & k[y] \arrow[dl, "y\mapsto x^{-1}"] \\
& k[x,x^{-1}] &
\end{tikzcd}$$

We want to find $f \in k[x]$ and $g \in k[y]$, so that $f = g$ in $k[x, x^{-1}]$. This is only possible if $f = g =$ constant.

The morphisms are *important*. What if we accidentally used $y \mapsto x$ instead of $y \mapsto x^{-1}$? Then we have plenty of regular functions; take any polynomial $f \in k[x]$, and g the same polynomial but in $k[y]$. So, regular functions are $k[x]$. This corresponds to the line with two origins, which is a scheme but not a variety.

Example 8.13. Suppose we have a morphism of varieties that is an isomorphism of underlying topological spaces. Is it an isomorphism of varieties?

No! Take the map from $\mathbb{A}^1 \to$ curve $y^2 = x^3$, mapping $t \mapsto (t^2, t^3)$. The corresponding varieties are the affine line, and a curve with a cusp at the origin. This is a homeomorphism of topological spaces, and the inverse takes

$$(x, y) \mapsto \begin{cases} \frac{y}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

This is not regular. Look at the rings of regular functions.

On $\mathring{A}^1$ the regular functions are $k[t]$, and on the cuspidal curve, it is $k[x, y]/(y^2 - x^3) = k[t, t^2, \ldots]$ which has t missing (this is not even finitely generated as an algebra).

Example 8.14. Show that the twisted cubic $(s^3 : s^2t : st^2 : t^3)$ is isomorphic to $\mathbb{P}^1$. We have a morphism $\mathbb{P}^1 \to$ Twisted cubic, taking $(s : t) \mapsto (s^3 : s^2t : st^2 : t^3)$. It is easy to check that this is a homeomorphism of topological spaces; however, as noted above this is not sufficient for isomorphism.

We need to construct an inverse morphism from the twisted cubic to $\mathbb{P}^1$. Recall the locality property of regular functions. This means that to construct a morphism from $A \to B$, we can cover A by open sets A_i, construct morphisms $A_i \to B$, that are compatible on intersections.

Let us cover the twisted cubic by open (affine) subsets. The twisted cubic sits in $\mathbb{P}^3$ which is covered by four open copies of $\mathbb{A}^3$. So the idea is to construct four morphisms

9. Tuesday, September 25, 2012

We began discussing the twisted cubic last time:

Example 9.1 (Twisted Cubic, Continued)**.** For affine varieties X, it is easy to construct morphisms from X to something – we have a large supply of regular functions, i.e. elements of the coordinate ring, which can be thought of as morphisms to $\mathbb{A}^1$.

However, for projective varieties, the only regular functions are constants!

Idea: Write projective variety X as the union of affine varieties $X_1, X_2, \ldots$. Construct morphisms from X_i to something that coincide on $X_i \cap X_j$. ("Sheaf property" – i.e. morphisms are local)

$$\begin{tikzcd} \text{Twisted Cubic} \arrow[r] \arrow[d] & \mathbb{P}^1 \\ \mathbb{P}^3 = (w : x : y : z) & \end{tikzcd}$$

The down arrow is an inclusion. It is covered by $w = 1, \ldots, z = 1$. For the twisted cubics, we only need two of these.

$$(s^3 : s^2t : st^2 : t^3) = (w : x : y : z)$$

so either w or z is $\neq 0$. So just need two open subsets: $w = 1, z = 1$.

Observe that

$$(w : x) = (s^3 : s^2t) = (s : t) \text{ when } s \neq 0 \Leftrightarrow w \neq 0.$$
$$(y : z) = (st^2 : t^3) = (s : t) \text{ when } t \neq 0 \Leftrightarrow z \neq 0.$$

So the twisted cubic is covered by two copies of $\mathbb{A}^1$. We mapped each $\mathbb{A}^1 \to \mathbb{P}^1$, and checked that maps agree on the intersection.

It is easy to check that the map is the inverse of the map $\to$ Twisted Cubic. Recall the theorem:

Theorem 9.2 (Hartshorne)**.** *Two affine varieties are isomorphic if and only if their coordinate rings are isomorphic.*

Why don't we use the same idea for projective varieties? Just check that the homogeneous coordinate rings are isomorphic.

A: It does not work. Specifically, the homogeneous coordinate rings of $\mathbb{P}^1$ and the twisted cubic are not isomorphic.

$$k[x,y] \not\cong \frac{k[w,x,y,z]}{(wy-x^2, wz-xy, y^2-xz)}.$$

Remark 9.3. Coordinate ring of a projective variety really depends on

(1) Projective variety
(2) Choice of (very ample) line bundle.

Question 9.4. Is there a canonical line bundle for (nonsingular) projective varieties?

Yes. The Canonical Line Bundle = the highest exterior power of the cotangent sheaf.

Problems:

(1) Might have no nonzero sections.
(2) Ring you obtain from it is not obviously finitely generated. (Proved recently for most varieties)

Remark 9.5. Theorem 9.2 holds in one direction for projective varieties. If you have the same coordinate ring, then the projective varieties are indeed the same.

Theorem 9.6. *It is easy to describe morphisms to an affine variety. If $\mathcal{O}(X)$ = the coordinate ring of X, i.e. the regular functions on X, the morphisms from $X \to Y$ are the same as ring homomorphisms $\mathcal{O}(Y) \to \mathcal{O}(X)$. If Y is affine! (false if Y is not affine). X does not need to be affine.*

Proof. Suppose $\varphi \in \mathrm{Hom}(X,Y)$. Then φ^* takes regular functions f on Y to regular functions on X.

$$\varphi^*(f) = f \circ \varphi.$$

So we get an element of $\mathrm{Hom}(\mathcal{O}(Y), \mathcal{O}(X))$. (Note contravariance.)

So we have a map $\mathrm{Hom}(X,Y) \to \mathrm{Hom}(\mathcal{O}(Y), \mathcal{O}(X))$.

We want to construct an inverse map. We need to use that Y is affine.

Suppose $h \in \mathrm{Hom}(\mathcal{O}(Y), \mathcal{O}(X))$. Put $\mathcal{O}(Y) = k[x_1, \ldots, x_n]/I$ for some ideal I.

Define the morphism $\psi : X \to Y$ as follows: $h(x_i) \in \mathcal{O}(X)$ so if $p \in X$, $h(x_i)(p) \in k$.

$$\psi(p) = (h(x_1)(p), h(x_2)(p), \ldots, h(x_n)(p))$$

The image is in Y as $h(I) = 0 \Rightarrow h(f) = 0$, if $f \in I$.

Left to prove:

(1) ψ is a morphism $X \to Y$.
(2) Map taking h to ψ is the inverse of the map $\varphi \to \varphi^*$.

Left as exercise.

□

Recall the idea of *products* in a category.

Definition 9.7. In any category, the product of two objects X, Y is some universal object $X \times Y$ with morphisms to X, Y.

$$\begin{tikzcd}
S \arrow[dr] \arrow[drr] \arrow[ddr] & & \\
& X \times Y \arrow[r] \arrow[d] & Y \\
& X &
\end{tikzcd}$$

If S has morphisms to X, Y, there is a unique map $S \to X \times Y$ making the diagram commute.

The coproduct $X \cup Y$ is the same thing but with all arrows reversed.

$$\begin{tikzcd}
S & & \\
& X \times Y \arrow[ul] & Y \arrow[l] \arrow[ull] \\
& X \arrow[u] \arrow[uul] &
\end{tikzcd}$$

What is a product of two varieties?

What is the coproduct of 2 k-algebras R, S? Denote it by $R \otimes S$.

$$\begin{tikzcd}
R \arrow[dr] \arrow[ddr, "f"'] & & S \arrow[dl] \arrow[ddl, "g"] \\
& R \otimes S \arrow[d] & \\
& T &
\end{tikzcd}$$

The usual tensor product of R, S has this universal property: If we have homs f, g to T, construct $R \otimes S$ to T by $r \otimes s \to f(r)g(s)$.

Easy to check that this is a homomorphism (as the rings are all commutative). In the category of noncommutative rings, coproduct is much different.

This gives coproduct of k-algebras Problem: tensor of two reduced k algebras is possibly not reduced, so in the category of reduced k-algebras, we may need to replace $R \otimes S$ by $R \otimes S/(\text{nilpotents})$.

The product of affine algebraic sets corresponds to tensor product of f.g. k-algebras.

This is not product $R \times S$ of k-algebras which corresponds to the coproduct of affine algebraic sets, which is essentially the disjoint union.

9.1. **Affine Algebraic Groups.** In any category with products, we can define analogs of groups (maps $X \times X \to X$). So we can define affine algebraic groups as "groups in the category of affine algebraic sets."

Example 9.8. $G = \mathbb{A}^1$ the affine line. The group action $G \times G \to G$ takes $(x, y) \mapsto x + y$. Inverse: $G \to G$, takes $x \mapsto -x$.

Problem: $G \times G$ has coordinate ring $k[x_1, x_2]$. What is the corresponding algebra homomorphism $k[x] \to k[x_1] \otimes k[x_2]$ to this map of affine algebraic sets?

Morphism takes x to $x_1 + x_2$.

$k[x]$ has the following algebra structure:

(1) $k[x] \otimes k[x] \to k[x]$ (gives the multiplication).
$f \otimes g \mapsto fg$.

(2) $k \to k[x]$ (identity).

It also has the coalgebra structure:

(1) $k[x] \to k[x] \otimes k[x]$ (group structure on $\mathbb{A}^1$).
(2) $k[x] \to k$ (identity).
$x \mapsto 0$.
(3) $k[x] \to k[x]$ (Inverse in group on $\mathbb{A}^1$).
$x \mapsto -x$.

This makes $k[x]$ with this group structure a Hopf algebra.

Example 9.9. Let $GL_2(k) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, such that $ad - bc \neq 0$. The coordinate ring is $\dfrac{k[a,b,c,d,e]}{(ad-bc)e = 1}$.

We focus on those with determinant 1.

This has a group structure $G \times G$ by multiplication of matrices.

What is the corresponding map of k-algebras?

$$\frac{k[a,b,c,d]}{(ad-bc-1)} \to \frac{k[a_1,b_1,c_1,d_1]}{(a_1d_1 - b_1c_1 - 1)} \otimes \frac{k[a_2,b_2,c_2,d_2]}{(a_2d_2 - b_2c_2 - 1)}?$$

Multiply two generic matrices and map each coordinate to the binomial in that position.

Example 9.10. $\mathbb{A}^1 - 0$ is isomorphic to the affine variety $xy = 1$ in $\mathbb{A}^2$. So, $x \mapsto (x, x^{-1})\mathbb{A}^2$.

What about $\mathbb{A}^2 - 0$? A Quasi-affine variety is an open subset of an affine variety.

Is this (isomorphic to) an affine variety? Answer: no. Cover $\mathbb{A}^2 - 0$ by the sets $(\mathbb{A}^1 - 0) \times \mathbb{A}^1$ and $\mathbb{A}^1 \times (\mathbb{A}^1 - 0)$.

10. Thursday, September 27, 2012

Last time:

Products of affine algebraic sets correspond to tensor products of finitely generated reduced k-algebras.

This works for k algebraically closed, but can fail for non-perfect fields. We can have two f.g. reduced algebras S, T over k, such that $S \otimes T$ has nilpotent elements.

Example 10.1. Let $\mathbb{F}_p(t)$ be the field of rational functions with coefficients in $\mathbb{F}_p$. Take the purely inseparable extension $k = \mathbb{F}_p(t^p) \subseteq \mathbb{F}_p(t) = K$. This is purely inseparable since t is the only root of $x^p - t^p = 0$ in $k[x]$. This is a f.g. k-algebra, with no nilpotents, so it is reduced.

$K \otimes_k K$ is not reduced. It is $\cong k(r) \otimes k(s)$, where $r^p = s^p = t^p \in k$. So, $(r-s)^p = t^p - t^p = 0$. This makes $r - s$ a nonzero nilpotent, which means that $K \otimes_k K$ cannot be the coordinate ring of a variety.

Moral: Char p algebraic geometry is sometimes weird.

We defined the categorical product using a universal property, and we also defined products of projective spaces using the Segre embedding.

Problem: Check that the product via the Segre embedding is equal to the categorical product.

So we need to show: Image of Segre embedding has properties of the categorical product.

Recall that the image of Segre embedding was all points $(z_{00} : z_{01} : \cdots)$, such that $z_{ij}z_{kl} = z_{il}z_{kj}$, for all i, j, k, l.

(1) We need to construct morphisms from the Segre product to $\mathbb{P}^m$ and $\mathbb{P}^n$.

[Strategy: Cover the Segre product by affine varieties, and define the map locally and check that the morphisms agree on intersections.]

Typical open affine subset might be $z_{ij} \neq 0$.

Example 10.2. Define morphism to $\mathbb{P}^m$ on an open subset where $z_{00} \neq 0$. Then:

$$(z_{00} : z_{01} : \cdots : z_{mn}) \mapsto (z_{00} : z_{10} : \cdots : z_{m0}).$$

On some other open subset, say $z_{01} \neq 0$, define the morphism as:

$$(z_{00} : z_{01} : \cdots : z_{mn}) \mapsto (z_{01} : z_{11} : \cdots : z_{m1}).$$

We need to check that they agree on the intersection $z_{00} \neq 0, z_{01} \neq 0$. They are *not* the same on $\mathbb{P}^{mn+m+n}$.

But the relations $z_{00}z_{11} = z_{01}z_{10}, \ldots$ means that they are the same in $\mathbb{P}^m$. So we get a well defined morphism from the Segre product to $\mathbb{P}^m$.

(2) Next we check the universal property.

Suppose T maps to $\mathbb{P}^m$ and $\mathbb{P}^n$. We need to construct a morphism $T \to$ Segre product. The uniqueness will be easy; the problem is to show existence.

It is hard to construct maps from arbitrary T to something. It is easy to do if T is affine. It will be sufficient to do this for the case where T is affine, and where the image is contained in one of the standard open affine sets covering $\mathbb{P}^m, \mathbb{P}^n$.

Why?

(a) We can cover T by such open affine subsets T_i.
(b) We construct maps $T_i \to$ Segre product.
(c) Glue maps together, and need to check that they are the same on $T_i \cap T_j$. (Follows from the uniqueness of the product)

(Largely, bookkeeping)

Let us assume, w.l.o.g. that the image of T in $\mathbb{P}^m$ is contained in the open affine $z_0 \neq 0$, and the image in $\mathbb{P}^n$ is contained in $z_0 \neq 0$. These opens are congruent to $\mathbb{A}^m, \mathbb{A}^n$ respectively.

So we get maps $T \to \mathbb{A}^m, \mathbb{A}^n$, and $t \to (f_1, f_2, \ldots, f_m) \in \mathbb{A}^m = (1 : f_1 : \cdots : f_m) \in \mathbb{P}^m$, similarly for $\mathbb{A}^n$. This gives a map $T \to \mathbb{A}^m \times \mathbb{A}^n$; just map this to the Segre product in the canonical way.

Finally check that this has the required properties: 1) that the image is in the Segre product (and that the relations on the Segre product hold), 2) Check that the diagram commutes, i.e. the map indeed factors through the Segre product.

The Segre embedding is really the composition of two constructions:

(1) Construct $\mathbb{P}^m \times \mathbb{P}^n$ as an abstract variety.
(2) Embed abstract variety in projective space $\mathbb{P}^{mn+m+n}$.

This first step works for all schemes.

10.1. **Automorphism Group of a Variety.**

Example 10.3. Try the affine space $\mathbb{A}^1$.

$$\mathrm{Aut}(\mathbb{A}^1) \cong \mathrm{Aut}(k[x]).$$

For $f(x)$ a polynomial, if it has an inverse, the polynomial must have degree 1. Why?

If the inverse is g, then

$$f(g(x)) = x.$$

So, both sides must have degree 1. Since degree multiplies in composition, both polynomials f and g must have degree 1. So automorphisms of $k[x]$ are $x \mapsto ax + b(a \neq 0)$. Same as automorphisms of $\mathbb{A}^1$: $(x) \to (ax + b)$.

Example 10.4. Now we try to find the automorphism group of $\mathbb{A}^2$.

Obviously the affine group $X \to AX + B$, where A is a 2×2 matrix and B is a vector are automorphisms of $\mathbb{A}^2$.

BUT, $\mathbb{A}^2$ has *lots* of extra automorphisms. For example,

$$x \mapsto x, \qquad y \mapsto y + (\text{favorite polynomial in } x).$$

The inverse is given by:

$$x \mapsto x, \qquad y \mapsto y - (\text{favorite polynomial in } x).$$

This is an infinite-dimensional abelian group of automorphisms.

Open Problem: What does the group of all automorphisms look like?

Endomorphisms of $\mathbb{A}^2$: $x \mapsto f(x,y), y \mapsto g(x,y)$. Where f, g are polynomials in x, y. Under what conditions is this map invertible?

Easy necessary condition: The Jacobian, i.e. the determinant

$$\begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial g}{\partial x} & \frac{\partial g}{\partial y} \end{vmatrix} \neq 0$$

Why? The Jacobian of MN, a composition of maps, is the product of Jacobians of M and N.

Conjecture 10.5 (Jacobian Conjecture)**.** This condition is sufficient (for $\mathbb{A}^m$).

Conclusion: It is really hard to describe automorphisms of varieties in general.

Example 10.6. Group of autmorphisms of projective line $\mathbb{P}^1$.

First we describe morphisms $\mathbb{P}^1 \to \mathbb{P}^1$, and then we check which are invertible.

Consider $\mathbb{A}^1$ as an open affine in $\mathbb{P}^1$. Any morphism $f : \mathbb{P}^1 \to \mathbb{P}^1$, then induces a morphism (open subset of $\mathbb{A}^1$) $\to \mathbb{A}^1$.

This is a Zariski open subset by continuity, so it is either empty, or it is a copy of $\mathbb{A}^1-$ a finite number of points $x_1, \ldots, x_n$. Maps from this to $\mathbb{A}^1$ are equal to rational functions with poles at $x_1, \ldots, x_n$. So the morphisms $\mathbb{P}^1 \to \mathbb{P}^1$ correspond to rational functions of x (including $\frac{1}{0}$).

All morphisms are described by $x \mapsto \frac{f(x)}{g(x)}$ not both identically 0.

Which have inverses? Easy to show that f, g must have degree ≤ 1.

So the group of automorphisms of $\mathbb{P}^1$ are given by $x \mapsto \frac{ax+b}{cx+d}$, such that $ad - bc \neq 0$. Think of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as a 2×2 matrix. Then composition of morphisms corresponds to product of matrices. In particular $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ are identity morphisms.

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

$\mathrm{Aut}(\mathbb{P}^1)$ over $\mathbb{C}$ is $PGL_2(\mathbb{C})$. This is the same as the automorphisms of the Riemann sphere S^2, the Riemann surface analogue of the projective line.

Serre's GAGA: Projective and analytic $\Rightarrow$ Algebraic.

(Projectivity is key: Endomorphisms of $\mathbb{A}^1(\mathbb{C})$ (polynomials) $\neq$ endomorphisms of Riemann surface $\mathbb{C}$, which are the holomorphic functions.)

Example 10.7. The image of a morphism can be quite bad locally. Consider the map:

$$\mathbb{A}^2 \to \mathbb{A}^2, \qquad (x,y) \mapsto (x, xy).$$

The image are the points (x,y) such that $x = 0 \Rightarrow y = 0$. Image neither open or closed.

Theorem 10.8 (Chevalley)**.** *The image of a variety under morphism is a constructible set, i.e. can be formed from open sets using the operations of union and complement.*

Theorem 10.9 (Ax-Grothendieck)**.** *If a morphism from a variety to itself over an algebraically closed field is injective, then it is surjective.*

Why is this surprising?

Obviously false over $\mathbb{Q}$: $x \mapsto x^3$ is injective, but not surjective.

Hierarchy of manifolds: In topology, we talk about

$$C^0 \subseteq C^1 \subseteq \cdots \subseteq C^\infty \qquad \subseteq \qquad C^\infty_{an} \subseteq Alg.Var.$$

The left-hand group tends to be floppy and topological, while the right-hand group tend to be rigid and algebraic, satisfying analogous theorems.

Surprisingly, the Ax-Grothendieck theorem fails completely for analytic manifolds C^∞_{an}. For example let $U =$ the unit ball in $\mathbb{C}^1$. The map $x \mapsto x/2$ is injective, not surjective.

Proof. We prove it for complex varieties by first proving it for varieties over finite fields.

1) The Ax-Grothendieck theorem is trivial for varieties over finite fields, since any variety has a finite number of points, and any injective map from a finite set to itself is surjective.

2) Ax-Grothendieck theorem is trivial for algebraic extensions of finite fields.

Reason: Just take finite algebraic extension generated by coefficients of polynomials defining a morphism, which reduces to the case of finite fields.

It is true for the complex numbers using the fact that anything true for algebraic closures of all finite fields is true for the complex numbers. (?????) (Obviously false, example: Characteristic $\neq 0$).

We modify this: Not “anything” is true, but “anything” that can be stated in the first-order language of fields in one sentence.

(Closely related to the Lefschetz principle)

□

11. Thursday, October 4, 2012

[Class on Tuesday, October 2 missed for Sukkot]

Consider the plane cubic given by

$$y^2 = 4x^3 - g_2x - g_3.$$

We want to show that it is not birational to $\mathbb{A}^1$.

Idea: Show that the underlying manifold of the homogenization $y^2z = 4x^3 - g_2xz^2 - g_3z^3$ is a torus.

We will construct analytic algebraic isomorphism:

$$\mathbb{C}/\Lambda \to \text{ Projective elliptic curve.}$$

The first surface is not really algebraic, but both are Riemann surfaces.

We need to construct functions on $\mathbb{C}/\Lambda \equiv$ functions on $\mathbb{C}$ invariant under Λ.

If f is any function,

$$\sum_{\lambda\in\Lambda} f(z+\lambda)$$

is invariant if the sum converges. Try:

$$\mathcal{P}(z) = \sum_{\lambda\in\Lambda} \frac{1}{(z+\lambda)^2}.$$

Problem: this does not converge. Look at the convergence of

$$\sum_{\lambda\in\Lambda} \frac{1}{(z+\lambda)^n}.$$

The absolute value of each summand is $\sim \frac{1}{r^n}$. Since we sum in the plane, there are about r terms of each absolute value. Therefore, convergence is like $\sum \frac{1}{r^n} \times r = \sum \frac{1}{r^n}$ which converges if $n > 2$. The $n = 2$ case is borderline.

Renormalize sum for

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \neq 0} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}.$$

This converges, but is not obviously invariant under Λ.

Look at

$$\mathcal{P}'(z) = \sum_{\lambda \in \Lambda} \frac{-2}{(z-\lambda)^3}.$$

Obviously this is invariant, and it also converges.

So $\mathcal{P}(z)$ is invariant up to constant, as $\mathcal{P}'$ is invariant. (Constant of integration)

Therefore,

$$\mathcal{P}(z+\lambda) = \mathcal{P}(z) + c_\lambda \Rightarrow c_{-\lambda} = -c_\lambda.$$

$\mathcal{P}$ is even, so

$$\mathcal{P}(-z-\lambda) = \mathcal{P}(-z) + c_\lambda \Rightarrow c_{-\lambda} = c_\lambda \Rightarrow c_\lambda = 0.$$

So $\mathcal{P}(z)$ has periods Λ.

Now construct a map from $\mathbb{C}/\Lambda \Rightarrow$ elliptic curve. We will just define this on $\mathbb{C}/\Lambda - \Lambda$. Idea: Find a differential equation involving $\mathcal{P}(z)$.

Recall: any holomorphic elliptic function is constant. Reason: Holomorphic imp lies continuous, implies bounded in fundamental domain of lattice (compactness), implies bounded on $\mathbb{C}$ by periodicity, implies constant by Liouville.

$\mathcal{P}(z)$ is holomorphic *except* at 0 (and its translates under Λ). Idea: Eliminate the pole at 0 to get holomorphic elliptic function.

$$\mathcal{P}(z) = \frac{1}{z^2} + a_2 z^2 + a_4 z^4 + \cdots.$$

$$\mathcal{P}'(z) = \frac{-2}{z^3} + 2a_2 z^1 + 4a_4 z^3 + \cdots.$$

$$\Rightarrow (\mathcal{P}'(z))^2 = \frac{4}{z^6} + *z^{-2} + \cdots.$$

$$\Rightarrow (\mathcal{P}'(z))^2 - 4\mathcal{P}(z)^3 = *z^{-2} + * + *z^2 + \cdots.$$

$$\Rightarrow (\mathcal{P}'(z))^2 - 4\mathcal{P}(z)^3 - *\mathcal{P}(z) = * + *z^2 + \cdots,$$

a holomorphic, thus constant, function. So,

$$(\mathcal{P}'(z))^2 = 4\mathcal{P}(z)^3 - g_2\mathcal{P}(z) - g_3,$$

where g_2, g_3 are some constants. This mirrors the form of the elliptic curve, so we can map

$$z \in \mathbb{C}/\Lambda(\notin \Lambda) \to (\mathcal{P}(z), \mathcal{P}'(z)) \in \mathbb{C}^2,$$

and map Λ to the point at infinity in the projective curve.

Summary: Some elliptic curve $zy^2 = 4x^3 - g_2xz^2 - g_3z^3$ (a purely algebraic construction) has underlying topological space of the form $\mathbb{C}/\Lambda$ (an analytic structure). Furthermore,

Elliptic functions = Meromorphic doubly periodic functions on $\mathbb{C}$ = Rational functions on an algebraic curve.

Elliptic functions/curves are misnamed. Elliptic curves have parabolic (=flat) geometry, while parabolas have elliptic (curvature > 0). Why was it named this? Because the inverse of $\mathcal{P}(z)$ is closely related to the integral for an arc length of an ellipse.

Remark 11.1. 1A Calculus Digression: $\sum_{\lambda\in\Lambda}\frac{1}{(z+\lambda)^2}, \sum_{\lambda\in\mathbb{Z}}\frac{1}{z+\lambda}$ both fail to converge.

Taking the derivative: $\mathcal{P}'(z) = \sum_{\lambda\in\Lambda}\mathcal{P}'(z)$, and $\sum_{\lambda\in\mathbb{Z}} frac{-}1(z+\lambda)^2$ both converge.

The second series is actually $\frac{-\pi^2}{\sin(\pi z)^2}$. So modifying the second of the original series, gives

$$\int\frac{-\pi^2}{\sin(\pi z)^2} = \frac{\pi\cos(\pi z)}{\sin(\pi z)} = \frac{1}{z} + \sum_{\lambda\in\mathbb{Z}}\left(\frac{1}{(z+\lambda)} - \frac{1}{\lambda}\right).$$

This formula is also obtained by taking the log derivative of the formula:

$$\sin(\pi z) = \pi z\prod\left(1 - \frac{z^2}{n^2}\right).$$

11.1. **Cubic Surfaces.**

Definition 11.2. Recall that a rational variety is one birational to $\mathbb{P}^n$.

Plane quadrics $y = x^2$ rational. Plane cubics are usually not rational. They can be if they have singularity, e.g. $y^2 = x^3$.

What about surfaces? Cubic surfaces are rational, but this is not obvious.

Informal argument: Take 6 points in general position in plane (or generic). This means they satisfy extra conditions that the author can't be bothered to write down.

Look at the space of all cubics

$$a_{000}x^3 a_{001}x^2y + \cdots.$$

Dimension of space of cubics is 10, since there are 10 possible coefficients. These points give six conditions, independent by genericity, which means the dimension of cubics vanishing on them is $10 - 6 = 4$.

Take a basis f_0, f_1, f_2, f_3. Then, the map

$$(x, y) \to (f_0 : f_1 : f_2 : f_3)$$

is a map from $\mathbb{A}^2 - 6$ points $\to \mathbb{P}^3$. This is not defined on the six points, since all the f's are 0.

The image is some hypersurface. What is its degree? Degree = number of intersections with a generic line.

Look at the number of intersection points with some line in $\mathbb{P}^3$, say $f_0 = f_1 = 0$. These are two cubic equations, so there are $3 \times 3 = 9$ points where f_0, f_1 intersect in $\mathring{A}^2$. Six of these do not count, as they are the six points we started with.

So this leaves three points of intersection of the surface with the line, so the degree is 3. So this suggests that the image of $\mathbb{A}^2 -$ (6 points) in $\mathbb{P}^3$ is dense in a degree 3 hypersurface birational to $\mathbb{A}^2$.

Count dimensions of the space of cubic hypersurfaces / 6 points in $\mathring{A}^2$. The cubic surface is given by degree 3 homogeneous polynomial in four variables, so depends on 20 coefficients. So the dimension $= 20 - 1 = 19$ (since we can multiply by constants).

The dimension of space of 6 points in $\mathbb{A}^2 = 6 \times 2 = 12$. The symmetries of $\mathbb{P}^2$ has dimension 8 as it is a $PGL_3(\mathbb{C})$. So, we have dimension 4.

$$\dim \mathrm{Aut}(\mathbb{P}^3) = \dim PGL_4(\mathbb{C}) = 15.$$

So this suggests that the moduli space of cubic surfaces has dimension $19 - 15 = 4$. The fact that these dimensions match is encouraging.

What about cubic hyper surfaces in $\mathbb{P}^4$? Are they rational? This was a hard open problem for many years. They are unirational, i.e. there is a finite to 1 map from rational surface onto them. Hard to distinguish unirational from rational.

In dimension 1 (Luroth) and dimension 2 (Castelnuovo), unirational implies rational. Clemens and Griffiths showed that cubic 3-folds are unirational but not rational.

Recall: we defined a map from $\mathbb{P}^2 - (6 \text{ points})$ onto the cubic hyper surface:

$$(x : y : z) \to (f_0 : f_1 : f_2 : f_3),$$

and the f_i vanish on these 6 points. What happens at these six points?

Answer: We get an isomorphism between $\mathbb{P}^2$ blown up at six points and the cubic hypersurface.

11.2. **Blowups.** Blowing up (G-transformation, monoidal transformation) gives examples of birational curves.

Blowing up a point of $\mathbb{A}^n$: The blowup Z of $\mathbb{A}^n$ at $(0, \dots, 0)$ is given by the following subvariety:

$$Z \subseteq \mathbb{A}^n \times \mathbb{P}^{n-1}.$$

where $\mathbb{A}^n$ has coordinates $(x_1, \dots, x_n)$ and $\mathbb{P}^{n-1}$ has coordinates $(y_1 : \cdots : y_n)$, given by the equations $x_i y_j = x_j y_i$. What does Z look like?

We have projection morphism $Z \to \mathbb{A}^n$. Look at the inverse image of $(x_1, \dots, x_n)$. Suppose (e.g.) $x_1 \neq 0$. Then $x_1 y_i = x_i y_1 \Rightarrow y_i = \frac{x_i}{x_1} y_1$. So the inverse image is a point. More precisely on $x_i \neq 0$, we get an isomorphism.

However, the inverse image of the origin is the whole of $\mathbb{P}^{n-1}$ The map $Z \to \mathbb{A}^n$ is an isomorphism except above $(0, \dots, 0)$; it replaces $(0, \dots, 0)$ by a copy of $\mathbb{P}^{n-1}$.

In other words, $(0, \dots, 0)$ has been *blown up* to a projective space.

Look at the projection $Z \to \mathbb{P}^{n-1}$ (covered by n copies of $\mathbb{A}^{n-1}$). Typical example: $y_1 = 1$. What does the projection look like over $y_1 = 1$? If $y_1 = 1$, then $x_i y_1 = x_1 y_i$, so $x_i = x_1 y_i$. So we have taken out a factor of x_1 from each x_i.

Suppose $V \subseteq \mathbb{A}^n$ is a sub variety. We can look at the inverse image of V in blowup of $\mathbb{A}^n$ at $(0, \dots, 0)$ This will be $\mathbb{P}^{n-1} \cup$ (something) map to V.

Example 11.3.

$$y^2 = x^3$$

Blowup $\mathbb{A}^2$ at $(0,0)$. Replace y by yx. This gives $y^2x^2 - x^3) = 0$, which gives $x^2(y^2 - x)$. The latter factor is a nonsingular curve in the inverse image.

So we have found a nonsingular curve $y^2 = x$ in the blowup mapping onto singular curve $y^2 = x^3$. This is an example of *resolving a singularity.*

12. Thursday, October 11, 2012

[Class missed on Tuesday for Simchat Torah.]

The nonsingular points of a variety are those points whose tangent space has the "correct" dimension.

Remark 12.1. The nonsingular points of an algebraic variety form an open dense subset.

An apparent counterexample:

Example 12.2. The Fermat Curve $x^3 + y^3 = 1$, which has singular points $3x^2 = 0, 3y^2 = 0$. This curve is nonsingular everywhere, except if char $= 3$, when all the points seem to be singular.

The explanation is that:

$$x^3 + y^3 - 1 = (x + y - 1)^3 \mod 3.$$

so this is not *reduced* in characteristic 3.

[The scheme $x^3 + y^3 - 1 = 0$ *is* singular at all points. For schemes, it is not always true that singular points form a closed set.]

The set of singular points is closed.

The set of singular points is the set of points where the rank of the matrix

$$\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}$$

Therefore it is a closed Zariski set given by the vanishing of lots of determinants of minors. (Possibly very complicated)

The set of nonsingular points is dense; since nonsingular points are open, it is enough to show that there is at least 1. Can easily reduced to the case of hypersurfaces by projecting into lower-dimensional space.

Suppose $f(x_1, \dots, x_n) = 0$ is an irreducible variety, with all points singular. Then $\frac{\partial f}{\partial x_i} = 0$ whenever $f = 0$, as the point is singular. So $f | \frac{\partial f_i}{\partial x_j}$, as f is irreducible; therefore, $\frac{\partial f_i}{\partial x_j} = 0$ as

$$\deg \frac{\partial f_i}{\partial x_j} < \deg(f).$$

This does not mean that because all derivatives $\frac{\partial f_i}{\partial x_j}$ are 0, that f is constant. Consider, for example, x^p in characteristic p.

The correct result: If all derivatives are 0, then $f = g^p$ for some g, where p is the characteristic of the field. (This result is over algebraically closed fields.)

But since we assumed that f irreducible, we must have $f =$ constant. So the variety is empty.

The problem with our definition of a tangent space is that it seems to depend on the embedding of the variety into affine or projective space.

Suppose $f : X \to Y$ is an isomorphism from X to Y, taking $x \in X$ to $y \in Y$.

Question 12.3. How do we know the tangent space to x at X is isomorphic to the tangent space to y at Y?

Answer: Find better definition of tangent space *not* depending on the embedding of X into $\mathbb{A}^n$. We use the Zariski tangent space, which we define in two steps:

(1) Define local ring of a point $x \in X$ (not depending on the embedding).
(2) Define the Zariski tangent space of any local ring.

Recall the local ring of X at a point x is roughly the ring of functions defined "near" x.

More precisely, it is the direct limit over open sets U containing x:

$$\varinjlim_{x \in U} \mathcal{O}(U) \text{ (Regular functions on } U)$$

This makes sense for any ringed space.

Example 12.4. The local ring of $\mathbb{A}^1$ at 0. Typical $U = \mathbb{A}^1 - \{\text{points } \alpha_1, \dots, \alpha_r\}$, such that no $\alpha = 0$. The regular functions on U are the rational functions with poles at $\alpha_1, \dots, \alpha_r$.

If $U_1 \supseteq U_2$, then the regular functions $\mathcal{O}(U_1) \subseteq \mathcal{O}(U_2)$. [Careful, this does not always hold.

So the direct limit is the union of rational functions with no pole at 0.

Example 12.5. Look at a *smooth* manifold R. Look at the local ring at 0.

$$\lim_{0 \in U} (\text{smooth functions on } U)$$

is not given by a union. A function may be nonzero on U but 0 on V, even if U and V are connected. There are smooth functions that are 0 on $(-1, 1)$, but not on $(-2, 2)$.

Definition 12.6. A local ring R has a unique maximal ideal $\mathfrak{m}$ = functions vanishing at the point. The Zariski cotangent space is defined as $\mathfrak{m}/\mathfrak{m}^2$, a vector space over $R/\mathfrak{m}$.

The Zariski tangent space, is then the dual vector space $(\mathfrak{m}/\mathfrak{m}^2)^*$.

For smooth manifolds, the tangent space is the set of tangent vectors. We can differentiate functions in the direction v. So we get a linear map, $\mathfrak{m} \to \mathbb{R}$ (derivatives in the direction v). This linear map vanishes on $\mathfrak{m}^2$, so we get a linear map $(\mathfrak{m}/\mathfrak{m}^2) \to \mathbb{R}$.

Example 12.7. The Zariski tangent space of $\mathbb{A}^n$ at $(0,0,0,\dots,0)$.

The coordinate ring $= k[x_1,\dots,x_n]$.

The local ring $=$ rational functions f/g such that $g \neq 0$ at $(0,0,\dots,0)$.

Maximal ideal $\mathfrak{m}$ is generated by $(x_1,\dots,x_n)$. Consequently, $\mathfrak{m}^2 = (x_ix_j \qquad 1 \le i,j \le n)$.

Therefore, $\mathfrak{m}/\mathfrak{m}^2$ is the vector space spanned by $x_1,\dots,x_n$. The Zariski tangent space is the dual of this.

Example 12.8. The Zariski tangent space of $y^2 = x^3$ (a singular curve) at $(0,0)$. The coordinate ring is

$$k[x,y]/(y^2 - x^3).$$

Setting $x = t^2, y = t^3$, this gives a coordinate ring:

$$k[1, t^2, t^3, t^4, \dots]$$

with only t missing.

The completion of the local ring R given as follows

$$R/\mathfrak{m} \leftarrow R/\mathfrak{m}^2 \leftarrow R/\mathfrak{m}^3 \leftarrow R/\mathfrak{m}^4$$

Take the inverse limit $\varprojlim_n R/\mathfrak{m}^n$. which is equal to sequences $(r_1, r_2, r_3, \dots)$, where $r_i \in R/\mathfrak{m}^i$, and $r_i =$ image of r_{i+1}.

Example 12.9. The completion of the local ring of $\mathbb{A}^1$ at 0 is given by the ring of formal power series. Let $R =$ rational functions, nonzero at 0. Then,

$$\begin{array}{ccc} R/\mathfrak{m} & R/\mathfrak{m}^2 & R/\mathfrak{m}^3 \cdots \\ k = k[x]/(x) & k[x]/(x^2) & k[x]/(x^3) \cdots \\ r_1 & r_2 & r_3 \cdots \\ a_0 + ? & a_0 + a_1x + ? & a_0 + a_1x + a_2x^2 + ? \cdots \end{array}$$

This explains why the completion gives a formal power series.

Returning to Example 12.8:

Example 12.10 (Example 12.8, Continued)**.** The completion of the local ring is the ring of formal power series $a_0 + a_2t^2 + a_3t^3 + \cdots$ with a_1t missing.

$$\hat{\mathfrak{m}} = \text{ power series } a_2t^2 + a_3t^3 + \cdots .$$
$$\hat{\mathfrak{m}}^2 = \text{ power series } a_4t^4 + a_5t^5 + \cdots .$$

Therefore,

$$\hat{\mathfrak{m}}/\hat{\mathfrak{m}}^2 \text{ has basis } t^2, t^3.$$

This is the Zariski cotangent space, so the Zariski tangent space has dimension 2.

A local ring is called regular if the dimension of the global ring...

Example 12.11. Another example of a local ring is $R = \mathbb{Z}_p$. The regular functions are the set of all rational numbers a/b, such that $p \not| b$. The maximal ideal $\mathfrak{m} =$ set of a/b with $p|a$. What is its completion?

$$R/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}.$$
$$R/\mathfrak{m}^2 \cong \mathbb{Z}/\mathfrak{p}^2\mathbb{Z}.$$

$$R/\mathfrak{m}^3 \cong \mathbb{Z}/\mathfrak{p}^3\mathbb{Z}.$$

We can write the completion in base p.

$$\varprojlim (\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots).$$

An element of the direct limit is an infinitely long number $\cdots a_3a_2a_1a_0$ in base p. Analogous to completion of local ring of $\mathbb{A}^1$ at 0.

12.1. **The DuVal singularity of type E_8.**

The DuVal singularities are also known as "simple surface singularities", "Kleinian singularities", "rational double points", and "canonical singularities in $\dim 2$".

Take the quotient of $\mathbb{C}^2$ by the action of a finite group.

Example 12.12. The cyclic group $\mathbb{Z}/n\mathbb{Z}$ acting on $\mathbb{C}^2 = \{(x,y)\}$ by $x \mapsto \xi x$, $y \mapsto \xi^{-1}y$. What is the quotient? What is the ring of coordinate functions on a quotient?

Answer: The polynomials in x, y invariant under $x \mapsto \xi x$, $y \mapsto \xi^{-1}y$.

$$\begin{array}{cccccc}
y^n & & & & & \\
\vdots & & & & & \\
y^3 & & & & & \\
y^2 & xy^2 & x^2y^2 & & & \\
y & xy & x^2y & & & \\
1 & x & x^2 & x^3 & \cdots & x^n
\end{array}$$

The northeast rays originating at $y^n, 1$, and x^n are fixed by the group action.

So the coordinate ring is $k[x^n, xy, y^n]$. Set

$$X = x^n, Y = y^n, Z = xy.$$

These are related by $XY = Z^n$. So the coordinate ring is $k[X,Y,Z]/(XY - Z^n)$. This has a Kleinian singularity.

List of Kleinian singularities:

A_n	Cyclic	$x^2 + y^2 + z^{n+1} = 0.$
D_n	Dihedral	$x^2 + zy^2 + z^{n-1} = 0.$
E_6	Tetrahedral	$x^2 + y^3 + z^4 = 0.$
E_7	Octahedral	$x^2 + y^3 + yz^3 = 0.$
E_8	Icosahedral	$x^2 + y^3 + z^5 = 0.$

What is $\mathbb{C}^2/$ Icosahedral group? Does not exist as icosahedral group has no irreducible 2-dimensional complex representations. However, its *double cover* does!

Use the Quaternions: $a + bi + cj + dk$, where $i^2 = j^2 = k^2 = -1$, etc. The group of Quaternions $a + bi + cj + dk$ such that $a^2 + b^2 + c^2 + d^2 = 1$ is a group isomorphic to S^3.

S^3 acts as rotations on $\mathbb{R}^3 = \{bi + cj + dk\}$. An element g acts by

$$g(v) = gvg^{-1}.$$

So we get a homomorphism $S^3 \to SO_3(\mathbb{R})$ with kernel $\{\pm 1\}$.

The icosahedral groups are really double covers of rotation groups.

So the zeros of $x^2 + y^3 + z^5 = 0$ can be thought of as $\mathbb{C}^2/$ double cover of rotations of icosahedron.

We will analyze this by repeatedly blowing it up.

First, we check for singular points. The partial derivatives are:

$$\frac{\partial f}{\partial x} = 2x, \qquad \frac{\partial f}{\partial y} = 3y^2, \qquad \frac{\partial f}{\partial z} = 5z^4.$$

So the only singular point is $(0, 0, 0)$ (assuming char $k = 0$).

Let us blow up at $(0, 0, 0)$. Note: Every blowup introduces three new variables, and there is no good notation for these. The first blowup gives:

$$\begin{array}{ccc} \mathbb{A}^3 & \times & \mathbb{P}^2 \\ (x, y, z) & & (x_1 : y_1 : z_1) \end{array}$$

Remark 12.13. One might suggesting simply stepping up the subscripts after each blowup. However, blowups have a tree-like structure, depending which subspace contains the point you blow up.

Recall that $\mathbb{P}^2$ is covered by three copies of $\mathbb{A}^2$, namely $x_1 = 1, y_1 = 1, z_1 = 1$.

13. Tuesday, October 16, 2012

13.1. Detailed look at Kleinian singularity of $x^2 + y^3 + z^5 = 0$ (Continued).

Recall that the only singular point is $(0, 0, 0)$.

We analyze it by repeatedly blowing up at the singularity.

Blow up once:

$$\begin{array}{ccc} \mathbb{A}^3 & \times & \mathbb{P}^2 \\ (x, y, z) & & (x_1 : y_1 : z_1) \end{array}$$

This is covered by three copies of $\mathbb{A}^2$: $x_1 = 1, y_1 = 1, z_1 = 1$.

- If $x_1 = 1$, then $x_1 y = y_1 x$, so $y = y_1 x$. Similarly, $z = z_1 x$.
$$x^2 + y^3 + z^5 = 0 \qquad \Rightarrow x^2 + (y_1 x)^3 + (z_1 x)^5 = 0.$$
$$1 + y_1^3 x + z_1^5 x^3 = 0 \qquad \to \text{ non-singular.}$$
- If $y_1 = 1$, then $x = x_1 y$ and $z = z_1 y$.
$$x^2 + y^3 + z^5 = 0 \qquad \Rightarrow (x_1 y)^2 + y^3 + (z_1 y)^5 = 0.$$
$$x_1^2 + y + z_1^5 y^3 = 0 \qquad \to \text{ non-singular.}$$
- If $z_1 = 1$, then $y = y_1 z$ and $x = x_1 z$.
$$x^2 + y^3 + z^5 = 0 \qquad \Rightarrow (x_1 z)^2 + (y_1 z)^3 + z^5 = 0.$$
$$x_1^2 + y_1^3 z + z^3 = 0 \qquad \to \text{singular point at } (0, 0, 0).$$

Now we need to analyze the singularity:

$$x_1^2 + y_1^3 z + z^3 = 0,$$

whose only singularity is at $(0, 0, 0)$.

We blow up again. Add new variables for a new $\mathbb{P}^2$.

$$\begin{array}{ccc} \mathbb{A}^3 & \times & \mathbb{P}^2 \\ (x_1, y_1, z) & & (x_2 : y_2 : z_2) \end{array}$$

This is again covered by three copies of $\mathbb{A}^2$.

- If $x_2 = 1$, we obtain something non-singular.
- If $y_2 = 1$, then $z = z_2 y_1$ and $x_1 = x_2 y_1$.
$$x_1^2 + y_1^3 z + z^3 = 0 \qquad \Rightarrow (x_2 y_1)^2 + y_1^3 z_2 y_1 + (z_2 y_1)^3 = 0.$$
$$x_2^2 + y_1^2 z_2 + z_2^3 y_1 = 0 \qquad \to \text{ unique singularity at } (0, 0, 0).$$
- If $z_2 = 1$, what we obtain is non-singular again.

Have we gained anything by blowing up the point? This new equation looks about as complicated as the last one.

Despite appearances, this really is better than the previous singularity.

Let's blow it up again! Our new equation is:

$$x_2^2 + y_1^2 z_2 + z_2^3 y_1 = 0$$

$$\begin{array}{ccc} \mathbb{A}^3 & \times & \mathbb{P}^2 \\ (x_2, y_1, z_2) & & (x_3 : y_3 : z_3) \end{array}$$

Yet again, this is covered by three copies of $\mathbb{A}^2$.

- If $x_3 = 1$, we obtain something non-singular.
- If $y_3 = 1$, then we obtain:

  $$x_3^2 + y_1 z_3 + y_1 z_3^2 = 0 \qquad \to \text{ unique singularity at } (0,0,0).$$

- If $z_3 = 1$, then we obtain:

  $$x_3^2 + y_3 z_2 + y_3 z_2^2 = 0 \qquad \to \text{ unique singularity at } (0,0,0).$$

This is a new phenomenon – we covered $\mathbb{P}^2$ by three copies of $\mathbb{A}^2$, and *two* of these copies have singular points. This is actually a favorable property, in a way, we are "spreading out" the singularity. Also, the degrees of the equation for each singularity have terms of lower or equal degree to the original equation.

Remark 13.1. Let us confirm that these are indeed distinct singularities, and not just the same one at different spots. Look at the pre-image in the product space. For one the projective coordinates are $(0 : 1 : 0)$ and the other are $(0 : 0 : 1)$.

Let us first look at $x_3^2 + y_1 z_3 + y_1^2 z_3^2 = 0$, this has the $(0 : 1 : 0)$ singularity. Blowup introducing $(x_4 : y_4 : z_4)$. None of the covers are singular! So we have no further singularities on this "branch". (Recall that this blow-up procedure has a natural tree structure.)

Now we look at the other branch: $x_3^2 + y_3 z_2 + y_3 z_2^2 = 0$, which has the $(0 : 0 : 1)$ singularity. We introduce $\mathbb{P}^2$ coordinates $(x_5 : y_5 : z_5)$ to blow up at 0:

- If $x_5 = 1$, we obtain something non-singular.
- If $y_5 = 1$, then we obtain:

  $$x_5^2 + y_3 z_5 + y_3 z_5^2 = 0.$$

  The partial derivatives at a singularity satisfy:

  $$\partial_{x_5} f = 2x_5 = 0, \qquad \partial_{y_3} f = z_5 + z_5^2 = 0, \qquad \partial_{z_5} f = y_3 + 2 z_5 y_3 = 0.$$

  So the curve has singularities at $(x_5, y_3, z_5) = (0,0,0)$ and $(0,0,-1)$.

- If $z_5 = 1$, then similar to $y_5 = 1$, we find two singular points:

  $$(x_5, y_5, z_2) = (0,0,0) \text{ or } (0,0,-1).$$

  The latter singular point is actually the same as the second singularity in the previous affine cover. So, we have a total of three singular points.

The three singular points have homogeneous coordinates: $(0 : 0 : 1), (0 : 1 : 0)$, and $(0 : 1 : -1)$. The first is in $z_5 = 1$, and the second two are in $y_5 = 1$. We have three more singularities to resolve. Each of them looks like $x^2 + yz + yz(\text{monomial in } yz) = 0$, and can be resolved by one more blowup.

Remark 13.2. In summary, we resolved the singularity of $x^2 + y^3 + z^5 = 0$ by blowing up singular points 8 times. WARNING: This example was particularly easy. For example, the only singular sets were points. In general, blowup of singular points may produce singularities of higher dimension.

Each blowup (roughly) adds new copy of $\mathbb{P}^1$ to the surface. So we have added eight extra copies of $\mathbb{P}^1$. How are these arranged?

Answer: They can be represented in a Dynkin diagram in which each point represents a line, and edges are intersections. See Figure 4.

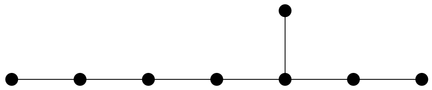

Figure 4. Dynkin Diagram for $E8$.

Remark 13.3. Consider the equation:

$$v^2 + w^2 + x^2 + y^3 + z^{5+6k} = 0.$$

This is a 4-dimensional complex hyper surface in $\mathbb{C}^5$. Look at the intersection of this hyper surface with small real sphere:

$$|v|^2 + |w|^2 + |x|^2 + |y|^2 + |z|^2 = 1.$$

This is a surface with real dimension 9. The intersection is a smooth manifold of dimension 7.

Theorem 13.4 (Brieskorn). *As k varies, the manifold is a topological S^7, but not diffeomorphic to S^7. So, we get Milnor's exotic spheres!*

13.2. **Blowing up Fermat's Surface.** This is an example in which blowing up an isolated singular point can produce singular sets of dimension > 0.

Fermat's surface is defined by the equation $x^4 + y^4 = z^2$.

Historical remark: Studied by Fermat in showing $x^4 + y^4 = z^4$ has no solutions in integers x, y, z with $xyz \neq 0$.

At all singularities, the partial derivatives will satisfy:

$$\partial_x f = 4x^3 = 0, \qquad \partial_y f = 4y^3 = 0, \qquad \partial_z f = 2z = 0.$$

So the only singularity is $(0, 0, 0)$. Blow up at $(0, 0, 0)$: introduce coordinates $(x_1 : y_1 : z_1)$ for $\mathbb{P}^2$.

Cover with three copies of $\mathbb{A}^2$:

- If $x_1 = 1$, the result is singular along a line.
- If $y_1 = 1$, the result is $x_1^4 y^2 + y^2 = z_1^2$. Singular along the line $z_1 = y = 0$.
- If $z_1 = 1$, we get a nonsingular curve.

Blowing up along the singular line gives a nonsingular surface.

In general, getting a singularity of higher dimension is actually a good thing – in the spirit of "spreading out" the singularity.

13.3. **Singularities of a Scheme.** Consider $\mathbb{Z}[\sqrt{-3}]$. Find singularities of "something" (a scheme) with coordinate ring $\mathbb{Z}/[\sqrt{3}]$.

Remark 13.5. Suppose $R =$ the coordinate ring of a variety V and x is a point of V.

The local ring of R at x is given as follows: invert everything *nonzero* at x; i.e. everything not in maximal ideal $m_x =$ functions vanishing at x.

What should the points be? For an affine variety, the points correspond to maximal ideals. So which maximal ideals of $\mathbb{Z}[\sqrt{-3}]$ are nonsingular? The ideal (2) is "singular". What does this mean?

Look at the local ring of this "point." This is given by inverting all elements of $\mathbb{Z}[\sqrt{-3}]$ not in maximal ideal (2). This local ring is denoted $\mathbb{Z}_2[\sqrt{-3}]$ (Note that this is the local ring, not the quotient ring $\mathbb{Z}/2\mathbb{Z}$.)

The maximal ideal generated by $\mathfrak{m} = (2, \sqrt{-3} - 1)$. Then, $\mathfrak{m}^2 = (4, 2\sqrt{-3} - 2)$. Then, $R/\mathfrak{m}^2$ maps onto $(\mathbb{Z}/4\mathbb{Z})[\sqrt{-3}]/(2\sqrt{-3} - 2)$.

So $\mathfrak{m}/\mathfrak{m}^2$ has four elements, and has dimension 2.

$$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}\left[\frac{\sqrt{-3}+1}{2}\right].$$

This latter ring is the integral closure of $\mathbb{Z}[\sqrt{-3}]$ in the quotient field.

Question 13.6. Why do number theorists most work with integral closures of rings of algebraic integers?

Answer: Taking the integral closure (for 1-dimensional curves or number fields) is equivalent to resolution of singularities.

14. Thursday, October 18, 2012

14.1. **Applications of Resolution of Singularities.**

The sketch of proof of resolution of singularities implies the Malgrange-Ehrenpreis Theorem.

Atiyah, Bernstein: If f is a polynomial in several variables then $|f|^s$ can be analytically continued in s as a distribution.

$$\int_{\mathbb{R}^n} |f(x)|^s g(x)dx. \qquad x = (x_1, \dots, x_n),$$

where g is any smooth function of compact support. This integral is a meromorphic function of s.

Example 14.1.

$$\int_0^\infty e^{-t} t^{s-1} dt$$

which converges if $Re(s) > 0$. (even though it does not have compact support, it is small enough to work)

To show $\Gamma(s)$ analytic in s, use integration by parts:

$$\int_0^\infty e^{-t} t^{s-1} dt = \int_0^\infty e^{-t} \frac{t^s}{s} dt.$$

The power of s is bigger, so the convergence will be better near the pole of $s = 0$. Same argument works if $n = 1$, but breaks down if $n \geq 2$.

Atiayh: Use resolution of singularities. Problems occur at zeros of $f(x) = 0$, a variety. At points where f looks like $x_1^{k_1} \cdots x_n^{k_n}$, this easily reduces to the 1-dimensional case. "Divisors with normal crossings."

Resolution of singularities:

$$\begin{tikzcd} X \arrow[r] \arrow[d] & Y \arrow[d] \\ V \arrow[r] & \mathbb{R}^n \end{tikzcd}$$

X is the inverse image of V via the blowup Y. Suppose Y is nonsingular, and X has normal crossings in Y. So this reduces to the trivial one-dimensional case. Recall that the case of $x^2+y^3+z^5$ had an inverse image of a chain of lines.

Theorem 14.2 (Malgrange-Ehrenpreis)**.** *Any linear PDE D with constant coefficients has a fundamental solution f for which $Df = \delta$, the Dirac delta function at 0.*

Proof. Take Fourier transforms: $P\hat{f} = \hat{\delta} = 1$, where P is a polynomial. This implies $\hat{f} = \frac{1}{P}$ – but there is a problem if P has zeros.

We want to know:

$$\int P^{-1}(x)g(x)dx.$$

where $g(x)$ is a smooth function of compact support.

Recall that

$$\int P^{s}(x)g(x)dx$$

is a meromorphic function of s, which might have a pole at $s = -1$. This is not a problem. Just take the constant coefficient of the Laurent expansion at $s = -1$. □

14.2. **Elimination Theory.**

Remark 14.3. Weil said: We have eliminated elimination theory. Abhyankar said: We must eliminate the eliminators of elimination theory.

Example 14.4. Suppose

$$x^3y^4 - 7x^2 + y^6 - xy^8 = 0.$$
$$3x^2y^5 + 4y^2 + 7x^6 + x^4y^7 = 0.$$

What is y? The strategy is to eliminate x from the two equations to get an equation involving only y. The result, by Bezout's theorem, should be a polynomial in y of degree 99.

Problem 14.5. Given 2 polynomials:

$$f(x) = a_mx^m + \cdots + a_0.$$

$$g(x) = b_nx^n + \cdots + b_0.$$

Find conditions on $a_m, \dots, a_0, b_n, \dots, b_0$ for f, g to have a common zero.

Suppose they have a common root $(x - \alpha)$, then $f(x)p(x) = g(x)q(x)$ for some p, q with $\deg p < n, \deg q < m$ as

$$p = g/(x - \alpha), q = f/(x = \alpha).$$

This is a set of linear equations in coefficients of p, q, so the condition for nonzero solution is vanishing of some determinant.

The determinant in question is called the Sylvester resultant:

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

Sylvester came up with a multitude of invariants with silly names:

(1) Determinant
(2) Resultant
(3) Bezoutiant
(4) Catalecticant
(5) Harmonizant, and more

The catalecticant vanishes if a form $a_{2n}x^{2n} + a_{2n-1}x^{2n-1}y + \cdots + a_0y^{2n}$ is the sum of n $(2n)$-th powers of linear forms.

Example 14.6. What is the condition for the polynomial $f = a_mx^m + \cdots + a_0$ to have a double root? f has a double root α

if and only if f, f' have a root α in common

if and only if the resultant of f, f' vanishes.

Example 14.7. When does $f = x^3 + bx + c$ have a double root? $f' = 3x^2 + b$.

The Sylvester resultant is $4b^3 + 27c^2$, which is ± the discriminant of the elliptic curve.

The geometric meaning of the resultant:

Consdier f, g to be homogeneous polynomials in x, y.

$$f(x, y) = a_mx^m + \cdots a_0y^m.$$

$$g(x, y) = b_nx^n + \cdots b_0y^n.$$

The coefficients in $k[a_0, \ldots, a_m, b_0, \ldots, b_m]$ = coordinate ring of k^{m+n+2}.

So, f, g define hypersurfaces X, Y in k^{m+n+2} (with variables a, b) $\times\mathbb{P}^1$ (with coordinates x, y). The resultant gives a hypersurface in k^{m+n+2}.

This hypersurface is projection of $X \cap Y$ in k^{m+n+2}. In particular, the image of closed set $X \cap Y$ in k^{m+n+2} is closed.

Problem 14.8. Suppose $A \to B$ is a morphism. C closed subset of A. Is the image of C a closed subset of B.

Answer: Usually not. For example, let $A = k^2, B = k$, map $A \to B$ takes $(x, y) \mapsto x$. The closed set $C = \{xy = 1\}$ is closed, but its image is missing the origin.

Remark 14.9. Standard blunder: Suppose we have a polynomial f on $\mathbb{R}^n$. Is the set of values taken by f closed? No. $x^2 + (xy - 1)^2$ takes all positive real values – so is not closed.

Projective varieties have the following fundamental property:

Proposition 14.10. *If X is any variety, Y is projective, then $X \times Y \to X$ is closed (i.e. takes closed sets to closed sets). This property does not hold for $Y = \mathbb{A}^1$ as shown above.*

$\mathbb{P}^n(\mathbb{C})$ is compact in complex topology, while $\mathbb{A}^n(C)$ is not.

Question 14.11. What is the correct analogue of compactness in the Zariski topology?

Recall: all varieties are compact under the Zariski topology.

Recall the concept of a proper map for locally compact Hausdorff spaces:

Definition 14.12.

$$f : X \to Y$$

is called proper if it is continuous and *universally closed.*

The map is universally closed, if for all Z,

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

is closed.

These conditions are equivalent to: Continuous, closed, compact fibers.

Informal meaning: the fibers are compact, and "well-behaved." So a proper map $f : X \to Y$ is a sort of well-behaved family of compact spaces $f^{-1}(y)$ indexed by points of Y.

For locally compact Hausdorff spaces X, X compact ⇔ $X \to 1$ is proper.

Therefore, we take this definition for the Zariski topology. In algebraic geometry, we say $f : X \to Y$ of varieties is proper if it is universally closed, i.e. that $X \times Z \to Y \times Z$ is closed. Remember: Use the Zariski topology here, *not* the product topology.

Correct analogy of compactness for variety X: the map $X \to pt$ is proper, in other words $X \times Z \to Z$ is closed for all Z.

Problem 14.13. Show that if X is a projective variety, it has this property. Easy to reduce this to the following problem:

$$\mathbb{A}^n \times \mathbb{P}^n \to \mathbb{A}^n$$

is closed.

Proof. First step: prove $\mathbb{A}^m \times \mathbb{P}^1 \to \mathbb{P}^1$ is closed. We do this using resultants.

Suppose a closed set S is given by zeros of $f_1, \dots, f_n$. each is a polynomial in $X, Y, Z_1, \dots, Z_m$ where the first two variables are coordinates of $\mathbb{P}^1$ and the rest are coordinates of $\mathbb{A}^m$.

We look at the resultants of $t_1 f_1 + t_2 f_2 + \cdots$ and $s_1 f_1 + s_2 f_2 + \cdots$, considered as homogeneous polynomials in X, Y. The resultant is a polynomial in $t_1, \dots, s_1, \dots, Z_1, \dots, Z_m$. Projection of close set S given by vanishing of all coefficients of monomials $s^\alpha t^\beta$ so is closed.

So we have shown that $\mathbb{A}^m \times \mathbb{P}^1 \to \mathbb{A}^m$ is closed. Now show: $\mathbb{A}^m \times \mathbb{P}^n \to \mathbb{A}^m$ closed. If $\mathbb{P}^m = \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$, this would be trivial. We know $Z \times \mathbb{P}^1 \to Z$ is always closed.

We could proceed by projecting down one $\mathbb{P}^1$ at a time.

The problem is that this fails, since $\mathbb{P}^2 \neq \mathbb{P}^1 \times \mathbb{P}^1$. However, $\mathbb{P}^2$ is "close to" $\mathbb{P}^1 \times \mathbb{P}^1$.

There is no surjective map from one to the other. The correct meaning of "close to" is that the blowup of $\mathbb{P}^2$ at a point is not $\mathbb{P}^1 \times \mathbb{P}^1$, but is a $\mathbb{P}^1$ bundle over $\mathbb{P}^1$, which looks locally like $\mathbb{P}^1 \times \mathbb{P}^1$.

The general version: The blowup of $\mathbb{P}^n$ at a point is (nontrivial) $\mathbb{P}^1$ bundle over $\mathbb{P}^{n-1}$. (This is a twisted product like a Möbius band) Let Z be the graph of correspondence from $\mathbb{P}^n$ to $\mathbb{P}^{n-1}$. For $Z =$ set of pairs $(x_0 : \cdots : x_n) \times (y_1 : \cdots : y_n)$ with $x_i y_j = x_j y_i$.

$Z \to \mathbb{P}^n$ is an isomorphism except it maps a whole $\mathbb{P}^{n-1}$ to $(1 : 0 : \cdots : 0)$. So Z is a blowup of $\mathbb{P}^n$ at a point. □

15. Tuesday, October 23, 2012

Theorem 15.1. *$\mathbb{P}^n \to$ point is a proper map. (Universally closed)*

We showed that $\mathbb{P}^1 \to$ point is proper. If $X \to$ point is proper then $\mathbb{P}^1 \times X \to$ point is also proper.

Problem 15.2. $\mathbb{P}^n$ is not quite $\mathbb{P}^{n-1} \times \mathbb{P}^1$. The exact relation is that the blowup of $\mathbb{P}^n$ at a point is a $\mathbb{P}^1$-bundle over $\mathbb{P}^{n-1}$.

We have a rational map

$$\mathbb{P}^n \to \mathbb{P}^{n-1}, \qquad (x_0 : \cdots : x_n) \mapsto (x_1 : \cdots : x_n).$$

(This is not defined at $(1 : 0 : \cdots : 0)$).

Put $Z =$ the closure of the graph of this map, i.e.

$$Z \subset \mathbb{P}^n \times \mathbb{P}^{n-1} \qquad (x_0 : \cdots : x_n) \times (y_1 : \cdots : y_n)$$

with $x_i y_j = x_j y_i$ for all i, j. This gives us projection maps from Z onto both spaces $\mathbb{P}^n$ and $\mathbb{P}^{n-1}$.

The map $Z \to \mathbb{P}^n$ is just the blowup of $\mathbb{P}^n$ at $(1 : 0 : \cdots : 0)$. This is an isomorphism except it takes a copy of $\mathbb{P}^{n-1}$ to $(1 : 0 : \cdots : 0) \in \mathbb{P}^n$.

Now look at $Z \to \mathbb{P}^{n-1}$: Z is not quite the product $\mathbb{P}^1 \times \mathbb{P}^{n-1}$ but a "twisted version". $\mathbb{P}^{n-1}$ covered by n copies of $\mathbb{A}^{n-1}$ (some coordinate $= 1$). One of these copies of $\mathbb{A}^{n-1}$, $Z \to \mathbb{P}^{n-1}$ restricts to $\mathbb{P}^1 \times \mathbb{A}^{n-1} \to \mathbb{A}^{n-1}$.

Example 15.3. On the open affine subset $y_1 = 1$, we have $x_j = x_i y_j$, so

$$(x_0 : \cdots : x_n) \mapsto (x_0 : x_1) \times (x_2 : \cdots : x_{n-1})$$

is an isomorphism.

So $\mathbb{P}^{n-1}$ is covered by open subsets A_i on which $Z \to \mathbb{P}^{n-1}$ looks like $\P^1 \times A_i \to A_i$. This does not imply that $Z \cong \mathbb{P}^1 \times \mathbb{P}^{n-1}$.

So $Z \to \mathbb{P}^{n-1}$ is proper. (Being proper is a local condition: to check $A \to B$ proper, it is enough to check for an open cover of B. We know $\mathbb{P}^1 \times A_i \to A_i$ is proper.

So $\mathbb{P}^n \leftarrow Z \to \mathbb{P}^{n-1}$ is proper by the above. Therefore, $Z \to$ point is proper; so $\mathbb{P}^n \to$ point is proper.

$$\begin{tikzcd}
Z \times X \arrow[d] \arrow[dr, "\text{proper}"] & \\
\mathbb{P}^n \times X \arrow[r] & \text{point}
\end{tikzcd}$$

We can lift closed sets along the vertical map.

So $\mathbb{P}^n \to$ point is proper.

Remark 15.4. This proof is a typical example of the following problem. Turn a rational map $X \to Y$ (not defined somewhere) into a regular map

$$\begin{tikzcd}
& \hat{X} \arrow[dl] \arrow[dr] & \\
X & & Y
\end{tikzcd}$$

Remark 15.5. If $n = 2$, so we had a map

$$\begin{tikzcd}
& Z \arrow[dl] \arrow[dr] & \\
\mathbb{P}^2 & & \mathbb{P}^1.
\end{tikzcd}$$

Z is an example of a surface birational to $\mathbb{P}^2$ and to $\mathbb{P}^1 \times \mathbb{P}^1$ but not isomorphic to either. (Surfaces Z which are $\mathbb{P}^1$-bundles over $\mathbb{P}^1$ are called Hirzebruch surfaces).

The proof above is constructive. An alternative, nonconstructive proof uses the Nullstellensatz and determinantal varieties. (Hartshorne's book includes a proof using schemes and valuation rings.)

Suppose $f_1, \ldots, f_r$ are homogeneous polynomiasl in $z_1, \ldots, z_n$. We want to show:

Proposition 15.6. *The condition that they have a common zero in projective space is a closed condition in their coefficients.*

Note: This is equivalent to saying $\mathbb{P}^n \to$ point is proper.

They do not have a common zero in projective space $\Leftrightarrow$ their ideal contains $(z_1, z_2, \ldots, z_n)^d$ for some $d \geq 1$, by the Nullstellensatz.

For any fixed d, the condition that combinations of polynomials f contain all degree d monomials $\Leftrightarrow$ some linear map in coefficients of f's is onto.

Using determinantal varieties, the condition that a linear map is onto is *open* in coefficients of linear equations. So points where f has no common zero is the union over $d \geq 1$ of open subsets, so is open. So the points where they have a common zero is closed.

(This is nonconstructive: we have to take an infinite union over $d \geq 1$.) This can be made constructive by estimating the maximal d needed.

The following is a very early application of singularities on algebraic curves:

Question 15.7. Planets have a periodic orbit. Can we define a position of the planet at time t by an algebraic function of t?

This question applies to any reasonable attractive force. Kepler's law says that area swept out is proportional to time. So the problem reduces to the following: Given an oval (or a smooth = C^∞ curve), look at the area cut off by a line ($ax + by + c = 0$).

Theorem 15.8 (Newton's Theorem on Ovals)**.** *The area is not an algebraic function of the line.*

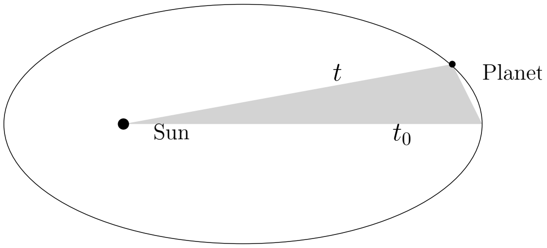

Figure 5. Area Swept Out by Orbit.

Example 15.9. If the curve is not smooth, this theorem does not apply. Consider for instance, a triangle, or a lemniscate given by $y^2 = x^2 - x^4$.

Proof. Consider a spiral given by the setting the distance from 0 to be the area swept out by the line rotating through the angle θ. (ZR - Sanity check: $r(\theta + 2\pi) = r(\theta)+$ area of oval.) Suppose the area is algebraic as a function of the line cutting off the area.

Then the spiral is locally algebraic, i.e. made up of lots of algebraic curves stuck together at singularities. Suppose oval is smooth. Then the spiral is also smooth – but singular points of algebraic curves cannot be smooth. So the oval being smooth implies that the spiral is an algebraic curve.

This contradicts Bezout's theorem (*really* due to Newton) which states that the number of intersection points of a degree d curve with a line is $\leq d$. So a spiral cannot be algebraic as it has infinitely many intersection points with a line. □

Remark 15.10. For any integer $d \geq 1$, we can find an oval, so that it will be smooth C^∞ at all but one point, and C^d at this point, such that the area cut off by a line is algebraic.

15.1. **Nonsingular complex projective curves.** Any nonsingular complex projective curve has a compact oriented 2-dimensional manifold as an underlying set.

Complex manifolds are oriented: Any complex vector space has canonical orientation depending on a choice of i with $i^2 = -1$.

Reason: Choose basis $v_1, \ldots, v_n$ for V, as a complex vector space. $v_1, iv_1, v_2, iv_2, \ldots$ is then a basis for V as a real vector space, defining orientation. Switching v_i, v_j does not change the orientation of V as a *real* vector space. Similarly, any change of basis does not affect orientation. ($GL_n(\mathbb{C})$ is connected, $GL_n(\mathbb{R})$ is not.)

Remark 15.11. Compact Connected Orientable 2-dimensional manifolds: Sphere, Torus, Two-holed torus, etc. The genus g describes the number of holes; a better invariant is the Euler characteristic $\chi = 2 - 2g$. In any case, genus is an invariant of smooth projective curves.

Example 15.12. Examples of curves of given genus:

(1) $g = 0$: Projective line $\mathbb{P}^1 = \mathbb{A}^1 \cup \infty \cong S^2$. Only example up to isomorphism.

(2) $g = 1$: Elliptic curves: can obtain them analytically as $\mathbb{C}/\text{Lattice} \cong S^1 \times S^1$.

$$\mathbb{C}/\text{Lattice} \overset{(1,\mathcal{P},\mathcal{P}')}{\to} (1 : x : y)$$

such that y^2 =cubic in x, we can put this in the form $y^2 = x(x-1)(x-\lambda)$ by a change of variable, and we get a map of this affine curve to $\mathbb{A}^1$ via $(x, y) \to x$.

So an elliptic curve is a branched double cover of $\mathbb{P}^1$ with four branch points $0, 1, \lambda, \infty$. Take any four points and look at the branched double cover with these branched points.

When do two sets of four branch points give the same elliptic curve (up to isomorphism)?

$\mathbb{P}SL_2(\mathbb{C})$ acts on $\mathbb{P}^1$ by $\tau \mapsto \dfrac{a\tau + b}{c\tau + d}$ for $\tau \in \mathbb{P}^1$. This action is three-fold transitive; it can take any three points to $0, 1, \infty$.

We do not quite get a map:

$$\begin{array}{ccc} \text{Isomorphism Classes of Quadruples of Points } /\mathbb{P}SL_2(\mathbb{C}) & \to & \lambda \\ (0, 1, \infty, \lambda) & \to & \lambda \end{array}$$

as we can permute $0, 1, \infty$ to get these other values instead of λ:

$$\lambda, 1-\lambda, 1-\frac{1}{\lambda}, \frac{1}{\lambda}, \frac{\lambda}{\lambda-1}, \frac{1}{1-\lambda},$$

a group S_3 of order 6.

SO, the moduli space of Quadruples of points in $\mathbb{P}^1/$ action of $\mathbb{P}SL_2(\mathbb{C})$ = Affine line $\lambda/$ group S_3 of order 6.

Let us get rid of the group of order 6. Find a rational function j of λ invariant under group S_3. The standard choice:

$$j = \frac{256(\lambda^2 - \lambda + 1)}{\lambda^2(\lambda - 1)^2},$$

called the elliptic modular function.

So the elliptic modular function is a function of Quadruples of points in $\mathbb{P}^1/$ action of $\mathbb{P}SL_2(\mathbb{C})$, so is a function of elliptic curves. Two complex elliptic curves are isomorphic iff they have the same value of j.

Therefore, genus 1 curves are parametrized by complex numbers j (j-invariant of elliptic curve), a coarse moduli space of elliptic curves.

This is a bit misleading: whenever the elliptic curve has extra automorphisms (example – $\mathbb{C}/(m+ni)$ has an extra automorphism given by multiplication by i) then the corresponding point of the moduli space is “bad”. This requires the theory of stacks to properly describe.

16. Thursday, October 25, 2012

16.1. **Classification of Elliptic Curves.** Elliptic curves or genus 1 curves are given by branched double covers of $\mathbb{P}^1$ at four points.

Classify these as $\{$ sets of four points in $\mathbb{P}^1\}$/Action of $PSL_2(\mathbb{C})$. The j-invariant is defined on this set. j = some rational function of λ, if four points are $(0, 1, \lambda, \infty)$.

Alternative construction of elliptic curves: take two complex numbers w_1, w_2, such that $\text{Im}(w_1/w_2) \neq 0$. Look at the lattice

$$\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2.$$

Then $\mathbb{C}/\Lambda$ is an elliptic curve. If we send $w_1 \mapsto aw_1 + bw_2, w_2 \mapsto cw_1 + dw_2$, we have a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Rescale so that $w_2 = 1$, and set $w_1 = \tau$. Elliptic curves are then points τ in the upper half plane modulo action of $SL_2(\mathbb{Z}), \tau \mapsto \frac{a\tau+b}{c\tau+d}$.

The j-invariant is a function of $q = e^{2\pi i\tau}$, since adding 1 preserves the lattice, and includes the number 196884.

John McKay: $196884 = 196883 + 1$ where the former summand is the dimension of the smallest representation of the monster simple group.

16.2. **Genus 2 curves.** Genus 2 curves are all hyper elliptic, i.e. branched double covers of $\mathbb{P}^1$. .

All genus two curves can be given as branched double covers of $\mathbb{P}^1$ branched at six points.

"Moduli space" given roughly by sets of 6 points in $\mathbb{P}^1$ modulo action of $\mathbb{P}SL_2(\mathbb{C})$.

Moduli space has dimension 3. Sets of six points are more less the same as binary sextics

$$a_0x^6y^0 + a_1x^5y^1 + \cdots + a_6y^6 = a_0(x - \alpha_1 y)\cdots(x - \alpha_6 y).$$

(though not quite the same, since some of the α_i's may be equal (semistable).

So we want to classify binary sextics modulo the $\mathbb{P}SL_2(\mathbb{C})$ action.

This corresponds to finding invariants of $SL_2(\mathbb{C})$ acting on 7-dimensional irreducible representations spanned by $a_0, \ldots, a_6$. The moduli space looks like $\mathbb{A}^3/$ action of $\mathbb{Z}/\zeta\mathbb{Z}$ acting as $(x, y, z) \mapsto (x\zeta, y\zeta^2, z\zeta^3)$.

The ring of invariants contains

$$(x^5, x^3y, xy^2, y^5, x^2z, xz^3, z^5, yz).$$

16.3. **Genus 3 Curves.** We can find hyperelliptic curves of any genus g (double branched cover of $\mathbb{P}^1$ branded at $2g + 2$ points). For genus $0, 1, 2$, this gives all curves. For genus 3 most curves are *not* hyper elliptic.

Example 16.1. Nonsingular plane curve of degree 4.

Question 16.2. What is the genus of a nonsingular plane curve of degree d?

A degree d curve $f(x, y) = 0$ maps to $\mathbb{P}^1$ by $(x : y) \to x$. So it is a degree d branched cover of $\mathbb{P}^1$. In general it has $d(d - 1)$ branch points of order 2, so the genus is $\dfrac{(d-1)(d-2)}{2}$. So, when $d = 4, g = 3$.

Question 16.3. How many curves do we get?

The dimension of the space of degree 4 polynomials in x, y, z is 15. The dimension of the group $\mathbb{P}GL_3(\mathbb{C})$ (the automorphisms of $\mathbb{P}^2$) is 8. Multiplying the polynomial by a constant gives the same curve, so we have:

$$15 - 8 - 1 = 6.$$

We have a 6 dimensional family of genus 3 curves. The hyper elliptic genus 3 curves have dimension 8; dimension of $\mathbb{P}SL_2(\mathbb{C}) = 3$, so this space has dimension 5.

Plane curves of degree 3 have, in general, 28 bitangents.

Example 16.4. Trott:

$$144(x^4 + y^4) - 225(x^2 + y^2) + 350x^2y^2 + 81 = 0.$$

The curve looks a bit like Figure 6. Each pair of beans has 4 bitangents, and each bean has one additional bitangent to itself.

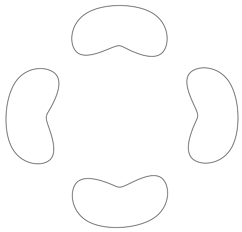

Figure 6. Curve with 28 Real Bitangents.

16.4. **Higher Genus Curves.** These cannot be nonsingular plane curves. Most are not hyperlliptic. They can be given as the intersection of a cubic and quadric in $\mathbb{P}^3$.

For large genus, it is very hard to describe all curves explicitly. It is hard even to describe one "generic" example.

Instead, we give an *analytic* description of all nonsingular complex projective curves. Pick points $x, x_1, \ldots, x_n$ in $\mathbb{P}^1$. Catalog the lines from x to x_i.

Take d copies of plane - n cuts, and glue them together. Specify how to glue them together. For each x_i choose some transposition of $(1, \ldots, d)$ (e.g. swap 3 and 7). Then glue cuts from x to x_i by making surfaces 3 and 7 cross over along the cut.

If transpositions generate a transitive subgroup of S_d, then the resulting surface is connected. We also want the product of transpositions, in order, to be 1 for convenience. The resulting surface has Euler characteristic $2d - n$. For suitable choices of $x_1, \ldots, x_n, d$ and the transpositions, we get all complex nonsingular projective curves.

16.5. **Symmetric Curves of Different Genera.**

Question 16.5. What about "special" curves? For example, can we find unusually symmetric curves?

For genus 1, we have elliptic curves, given by $\mathbb{C}/\Lambda$. The automorphism group is infinite – translate by $\mathbb{C}$.

Additional symmetries fixing 0: This is given by complex numbers z so that $z\Lambda = \Lambda$ – obvious example: $z = \lambda$.

More possibilities: If $\Lambda = \mathbb{Z} + \mathbb{Z}i$ then another symmetry is multiplication by i.

If $\Lambda = \mathbb{Z} + \frac{1+i\sqrt{3}}{2}\mathbb{Z}$, then another symmetry is multiplication by 6-th root of 1. Looking at the equations of these two curves $y^2 = x^3 + x$ and $y^2 = x^3 + 1$ makes the symmetries clear.

If genus $g > 1$ then the automorphism group of the curve is finite. The order of the automorphism group is finite.

In particular, the order is $\leq 84(g-1)$. (This bound is achieved for infinitely many values of g, but not for every value) Curves which achieve this are called *Hurwitz curves.*

Suppose a group G acts on a complex curve C. Form the quotient C/G and look at its Euler characteristic. The quotient is an orbifold, not a manifold. Locally, this looks like a manifold/finite group.

If G acts freely, C/G is a manifold. But if some elements of G have fixed points, we get an orbifold.

Example 16.6. Take $\mathbb{C}/$ Group of n-th roots of 1. The coordinate ring is $\mathbb{C}[x]$. The ring of invariants is $\mathbb{C}[x^n]$ = polynomial ring. So the quotient $\mathbb{C}/G$ seems to be $\mathbb{C}$.

This is misleading: the quotient is really an orbifold with a strange point at 0. In the case of $n = 2$, we have a double cover of $\mathbb{C}$, and we can think of this as a conical singularity.

The fundamental domain of the orbifold looks like a cone, with a $1/n$ of a point. The Euler characteristic = # points $-$# lines $+$#2-cells $\cdots$.

For orbifolds, points should be counted with fractional values. Why? The *Orbifold Euler characteristic* of C/G = Orbifold Euler characteristic of C/Order of G.

Given C a nonsingular algebraic curve of genus $g > 1$, it has Euler characteristic $\chi = 2g - 2 < 0$. So orbifold Euler characteristic of C/G is negative $\dfrac{2g-2}{|G|}$. So $|G|$ large means that orbifold Euler characteristic close to 0.

The quotient C/G will be topologically some orientable compact surface. However, it might have some orbifold points.

What is the orbifold Euler characteristic of a surface with conical points? The ordinary Euler characteristic $= 2 - 2h$. $h =$ the genus of underlying topological manifold. This miscalculates the orbifold Euler characteristic.

What is the error? Euler characteristic is an alternating sum of n-cells. The ordinary Euler characteristic counts each orbifold point as 1 point. The Orbifold Euler characteristic counts $1/n$ points where n is the order of some cyclic group. SO, we need to subtract $(1 - \frac{1/n}{)}$ for each orbifold point of order n.

So the orbifold Euler characteristic is

$$\chi = 2 - 2h - (1 - \frac{1}{n_1}) - (1 - \frac{1}{n_2}) - \cdots .$$

The subtracted numbers are between 1/2 and 1. We want this number to be negative and as close to 0 as possible.

If $h > 0, 2 - 2h = 0$, so $\chi \leq -\frac{1}{2}$. What if $h = 0$? Then $\chi = 2 - a_1 - a_2 - \cdots$. How close can χ be to 0 while being negative?

Answer: $2 - \frac{1}{2} - \frac{2}{3} - \frac{6}{7} = -\frac{1}{42}$.

17. Tuesday, October 30, 2012

[Some material at the beginning of class was missed.]

Question 17.1. Can we find a genus 2 curve of genus $84(g-1) = 84$.

Answer: No. There is no group of order 84 generated by x, y, z with $x^2 = y^3 = z^7 = xyz = 1$. By the Sylow theorem, the number of subgroups of order 7 is $1 \mod 7$ and divides 84, so it must be 1. So G has a normal subgroup of order 7.

Consider the quotient G/normal subgroup of order 7. This has order 12, and any group of order 12 has a normal subgroup of order 3 or 4. In the first case, G has normal subgroup of order 3×7 containing all elements of order 3 and 7. So the product of elements of order $3, 7$ cannot have order 2.

In the second case, G has a normal subgroup of order 4×7 which leads to a contradiction in a similar way.

The next largest possibility for order of $Aut(G)$ is $48(g-1) = 48$. We construct a genus 2 curve with this number of automorphisms.

Hyperelliptic curves of genus 2 given by branched double covers of $\mathbb{P}^1$, branched over 6 points. The automorphism group

$$1 \to (\text{group of order 2 in center}) \to G \to (\text{subgroup of } Aut(\mathbb{P}^1) \text{ fixing set of 6 points}) \to 1.$$

So we want to find a "symmetric" set of points in $\mathbb{P}^1$. Recall:

$$S^2 = Aut(\mathbb{P}^1) = PSL_2(\mathbb{C})$$

contains $SO_3(\mathbb{R})$. Take six corners of octahedron. The rotation group of the octahedron has order 24 (and is isomorphic to the symmetric group S_4).

Take the 6 points to be:

$$0, \infty, 1, -1, i, -i.$$

Show that there is a group of order 24 acting on these:

The map $z \mapsto iz$ maps the set to itself, fixing ∞.

$z \mapsto \frac{1+z}{1-z}$ maps the set to itself, fixing $i, -i$. Together , these two generate the permutation group.

Brancehd double cover of $\mathbb{P}^1$ over $0, \infty, \pm 1, \pm i$ is a genus 2 curve with 48 automorphisms, the most possible.

What are the equations defining this curve?

$$y^2 = x(x^2+1)(x^2-1).$$

Take the projective curve in $\mathbb{P}^2$:

$$y^2z^3 = x(x^2+z^2)(x^2-z^2) = \text{ Affine curve and point at infinity.}(0:1:0).$$

This does not define a nonsingular hyper elliptic curve.

Problem 17.2. The point at ∞ is singular. Put $y = 1$:

$$z^3 = x(x^2+z^2)(x^2-z^2).$$

This is singular at $x = z = 0$.

Nonsingular projective plane curves never have genus 2. The degree-genus formula states that

$$g = \frac{(d-1)(d-2)}{2} = 0, 1, 3, 6 \dots.$$

Explicit construction: Glue together two copies of the affine curve $y^2 = x(x^2+1)(x^2-1)$. So we construct the curve as an abstract variety. Take the curve

$$y^2 = x(x^2+1)(x^2-1).$$

Remove the point $(0,0)$. This gives an open subset with automorphism $x \mapsto x^{-1}, y \mapsto yx^{-3}$ of order 2.

Now take 2 copies of $y^2 = x(x^2+1)(x^2-1)$ in $\mathbb{A}^2$. Glue together their subsets with $x \neq 0$ using automorphism of order 2 (i.e. glue the point to its target via the automorphism).

This gives a nonsingular hyper elliptic curve of genus 2 with automorphism group of order 48.

17.1. **Genus 3 curves.** By the identity from earlier, $Aut(C) \leq 84(g-1) \leq 168$.

The unique genus 3 curve with automorphism group of this order is the Klein quartic

$$x^3y + y^3z + z^3x = 0.$$

This is nonsingular (left as exercise), so the curve has genus $(4-1)(4-2)/2 = 3$.

The automorphism group is a simple group $SL_3(F_2) = PSL(F_7)$ of order 168.

The obvious automorphisms of the curve

$$\begin{cases} x \mapsto y \mapsto z \mapsto x & \text{order } 3 \\ x \mapsto \zeta^4 x, y \mapsto \zeta^2 y, z \mapsto \zeta z & \text{order } 7 \quad (\zeta^7 = 1). \end{cases}$$

Remark 17.3. When proving the Hurwitz bound, we also found all possibilities with $\chi = 0$.

$$\{n_i\} = \begin{cases} 2,2,2,2 & \text{Elliptic Curve } \mathbb{C}/L, z \mapsto -z \\ 2,4,4 & \mathbb{C}/\mathbb{Z} + i\mathbb{Z}, z \mapsto iz \\ 2,3,6 & \mathbb{C}/\text{Eisenstein }, z \mapsto e^{2\pi i/6} z \\ 3,3,3 & \mathbb{C}/\text{Eisenstein }, z \mapsto e^{2\pi i/3} z \end{cases}$$

These correspond to finite groups acting on elliptic curves, fixing a point. The quotient is an orbifold with these conical points.

Exercise 17.4. Classfiy the 17 wallpaper groups. The orientable ones are listed above.

The non-orientable ones are similar, but uses nonorientable orbifolds. Complications:

(1) the topological surface $\mathbb{C}/G$ may have boundary. (Could be disk or Möbius strip.)
(2) Non-orientability (Could be $\mathbb{R}P^2$ or Klein bottle.)
(3) Additional possiblities – singularities, corners.

Possibliites for $\chi > 0$:

(1) One conical point: *bad* orbifold – not covered by manifold.
(2) Two conical points, order m, n: *bad* if $m \neq n$. If $m = n$, this is okay – S^2/cyclic group.
(3) Three conical points will have orders $2, m, n$.

Orders		Group Order
2,3,3	$\frac{\chi 1}{6}$	12 - Tetrahedral group
2,3,4	$\frac{1}{12}$	24 - Octahedral group
2,3,5	$\frac{1}{30}$	60 - Icosahedral group

So the finite groups acting on genus 0 curves are:

(1) A_n Cyclic.
(2) D_n Dihedral.
(3) E_6 Tetrahedral.
(4) E_7 Octahedral.
(5) E_8 Icosahedral.

We have bridges from these objects to the worlds of algebra and analysis:

Geometry		Analysis
Algebraic Curves	↔	Riemann Surfaces
(Curves up to Birational Equivalence)	↔	(f.g. extensions of $\mathbb{C}$ of transcendence degree 1.)
or (nonsingular projective curves up to isomorphism)		Algebra

Given three realms: 1) Nonsingular curves, 2) Function Field of Curve, 3) Riemann Surfaces, passing from 1 to 2 is easy, 1 to 3 is easy, 3 to 1 we accomplish by resolution of singularities, 3 to 2 is HARD.

Take the field of meromorphic functions. It is hard to prove the existence of nonconstant meromorphic functions. (Warning: in dim > 1, compact complex manifolds may have no nonconstant meromorphic functions.)

Example 17.5. An example of the difficulty of constructing meromorphic functions.

Dimension 1: Take $\mathbb{C} - 0$. Acted on by the group Z, generated by $z \mapsto 2z$ (?). Acts freely so $\mathbb{C} - 0$/action of Z is isomorphic to $S^1 \times S^1$, which is a Riemann surface.

Problem: Find a meromorphic function on it. (A meromorphic function on $\mathbb{C}-0$, with $f(z) = 2z$.)

Similarly: Take $\mathbb{C}^2 - (0, 0)$. Again acted on by Z, $(x, y) \mapsto (2x, 2y)$.

$\mathbb{C}^2/$ action of Z is compact 2-dimensional complex manifold topologically isomorphic to $S^1 \times S^3$. Called a Hopf surface, weird property: 1) Not projective. 2) No non constant meromorphic functions.

Resolution of singularities of curves: Given a curve find a nonsingular projective curve birational to it. Originally solved by Newton, using Newton polygons and Puiseux expansions.

Definition 17.6. A *Puiseux expansion* is a power series in $x^{1/n}$, or a Taylor series in $x^{1/n}$ for some integer n.

Example 17.7. Consider the curve

$$y^2 = x^3 + x^4.$$

This is singular at 0. y is not a Taylor series in x, but we have a Puiseux series:

$$y = x^{3/2}(1+x)^{1/2} = x^{3/2} + \frac{1}{2}x^{5/2} + \cdots$$

18. Thursday, November 1, 2012

We began discussing Newton's method for analyzing singularities.

Definition 18.1. Newton polygon. Given a function $f(x,y) = \sum a_{ij}x^iy^j$, plot the pairs (i,j) with $a_{ij} \neq 0$. The *Newton polygon* is the convex hull of these points.

Find the smallest N so that y^N occurs in the monomial. (If no such N, then $f(x,y)$ is divisible by x).

Newton's Rotating Ruler: Put the ruler through $(0,N)$. Rotate it until it hits the first points of Newton polygon.

Look at the terms $a_{ij}x^iy^j$ in $f(x,y)$ lying on this line. These are the terms in f of lowest weighted degree where we give x,y certain weights (depending on the slope of the line).

So we obtain a weighted homogeneous polynomial in x,y.

Example 18.2. Consider the function

$$y^6 + y^5 + y^2x^2 + 3x^5 = 0.$$

The Newton polygon is pictured in Figure 7.

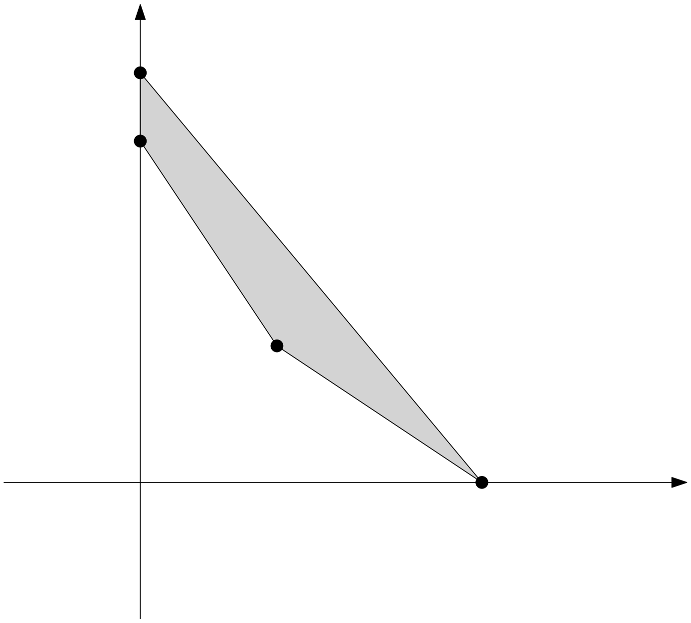

Figure 7. Newton Polygon.

The idea for analyzing the curve: Make substitutions in x,y so that we

(1) *Either* reduce N, or

(2) Reduce slope of Newton's leading edge.

Look at

$$g(x,y) = \text{ Lowest wegihted degree terms in } f(x,y).$$

Two cases:

(1) Not all roots are equal. Substitute $y \mapsto y - ax^{N/s}$ for a one of the roots. This reduces minimal power y^N of Y in the polynomial.
(2) All roots are equal. We can substitute $y \mapsto y - ax^{N/s}$. This does not reduce the power of y, but reduces the slope of the leading edge.

Slight extension of this method: Field of PUiseux-Laurent Series is Algebraically closed. (Like Puiseux series, but we allow a finite number of negative powers.)

The ring of Puiseux series is a local ring. Maximal ideal is all series with vanishing constant term. It is not Noetherian, as generators for them axial ideal are:

$$(x, x^{1/2}, x^{1/3}, x^{1/4}, \ldots)$$

Noetherian local rings have the property that

$$\cap \mathfrak{m}^n = 0.$$

"The function is determined by power series expansion", since

$$\mathfrak{m}^n \sim \text{ functions with first } n \text{ derivatives equal to } 0.$$

This fails for Laurent-Puiseux series: $\mathfrak{m} = \mathfrak{m}^2$, since for any $n, x^{1/n} \in (x^{1/2n}) \times (x^{1/2n})$.

The quotient field of Puiseux series is just given by inverting x. Therefore, it is the ring of Laurent-Puiseux series. (Laurent series form quotient field of local ring of Taylor series.)

The reason that L-P series are algebraically closed: Observe that if f is a polynomial $f(x,y)$ we can write y as a Puiseux series in x by using Newton's method of analyzing singularities.

This gives the algebraic closure of the field of Laurent series over $\mathbb{C}$.

Similar to a finite field! It is a perfect, quasi-finite field. It has a unique extension of degree n for every integer $n > 0$. Galois group of $(\bar{K}/K)$ = Profinite completion of $\mathbb{Z}$ = the inverse limit of finite quotients $\mathbb{Z}/n\mathbb{Z}$, which is also the Galois group of (F_{p^n}/F_p).

$$\Rightarrow Gal(F_{p^n}/F_p) = Gal(\mathbb{C}[x^{-1/n}][[x^{1/n}]]/\mathbb{C}[x^{-1}][[x]]).$$

Question 18.3. What does this all have to do with resolution of singularities?

Idea: A curve with a singular point looks locally like union of curves of the form $y = x^{r/s}+$ higher powers, or $y^s = x^r+$ higher powers.

The analytic branch $\neq$ algebraic branch.

Example 18.4. Consider the singular curve:

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

Only one branch algebraically, however, analytically, near 0, the two branches $y = \pm x(1+x)^{1/2}$ make the curve look reducible.

[This shows that completion of a local ring is an integral domain may have zero divisors.]

18.1. **Hilbert Polynomials and Intersections in Projective Space.**

Problem 18.5. The basic problem is: Suppose we have a graded module $M = \bigoplus_{n\geq 0} M_n$, finitely generated over a graded ring $R = \bigoplus_{n\geq 0} R_n$, finitely generated over a field R_0.

Then $\dim M_n$ is finite. How fast does it grow?

If R is generated by elements of degree 1 then $\dim M_n$ is a polynomial in n for n large. (Not polynomial for all n, as $\dim(M_n) = 0$ for $n < 0$.)

Encode $\dim M_n$ as a power series

$$f(x) = \sum_{n\geq 0} \dim(M_n)x^n.$$

The key point: $f(x)$ is a rational function (described by finite data). If generators of R have degree 1, then the only pole of f is at $x = 1$.

Suppose we choose finite number of homogeneous generators of R. Suppose r is one of these generators. Look at:

$$0 \to \ker(r) \to M \xrightarrow{r} M(n) \to M(n)/rM(n) \to 0.$$

If we have an exact sequence of vector spaces:

$$0 \to V_0 \to V_1 \to \cdots \to V_n \to 0,$$

then the alternating sum of the dimensions is 0.

So

$$\dim\ker(r)_k - \dim M_k + \dim M(n)_k - \dim\left(\frac{M(n)}{rM(n)}\right)_k = 0.$$

This gives $0 = f_{\ker(r)}(x) - f_M(x) + x^n f_M(x) - f_{M(n)/rM(n)}(x)$. Note that $x^n f_M(x) = f_{M(n)}(x)$. The first and last subscripts refer to graded modules over the graded ring R/rR with fewer generators. The functions f_{-} are rational functions by induction on the number of generators of R.

If R needs no generators then $R = R_0$ is a field, so $M = \oplus M(n)$ is a finite dimensional vector space, so $f_M(x)$ is a polynomial.

$(1 - x^n)f_M(x) =$ a rational function, so $f_M(x)$ is rational. The poles are zeros of $(1 - x^n)$ where $n_i =$ degrees of generators of R.

If all the degrees of generators n_i are 1, then the dimension of M_n is a polynomial in n for n large. This si true for coefficients of any rational function with only poles at $1, \infty$. Linear combination of

$$x^i, \frac{1}{(1-x)^n}, \text{ where } \frac{1}{(1-x)^n} = \sum \binom{-n}{i} x^i.$$

This is called the Hilbert polynomial $P(n)$ of M. The values of $P(n)$ are integers.

Question 18.6. What polynomials take integer vales at all (large) integers?

Our first guess: polynomials with integer coefficients. Wrong – consider $x(x + 1)/2$.

In fact, these have as a basis the polynomials $\binom{x}{n}$. Each of these polynomials are 0 at the first $n - 1$ integers (starting at 0).

Proof. We prove that these polynomials form a basis. Suppose p is a degree integer-valued polynomial.

(1) Subtract multiple of $\binom{x}{0} = 1$ to make value at 0 vanish.
(2) Subtract multiple of $\binom{x}{1}$ to make value at $0, 1$ vanish.
(3) Continue until subtracting $\binom{x}{n}$ so that it vanishes on $0, \ldots, n$.

This gives us a degree $\leq n$ polynomial with $n+1$ zeroes so it must be identically 0.

□

So we have written p as an integer linear combination of $\binom{x}{0}, \binom{x}{1}, \ldots$. The leading coefficient of p is of the form $\frac{dx^n}{n!}$ for some integer d.

The most important invariants of the Hilbert polynomial tend to be the integers d, n.

[The remaining coefficient tend to be less important since they depend on the choice of grading of the module M.]

18.2. **Applications of the Hilbert polynomial.** We have several applications of this polynomial.

Dimension of a local ring.

(1) Maximum length of proper increasing chain of prime ideals. (Correspondingly, decreasing chain of irreducible subvarieties). This is very hard to compute directly.

(2) Consider $R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \cdots$. This is a finitely generated graded ring (if R is Noetherain) and a module over itself. Therefore, it has Hilbert polynomial:

$$P(n) = \dim(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \qquad (n \text{ large}).$$

The dimension of a local ring is then $\deg P(n) - 1$. This is in practice easy to calculate. For equivalence of the definitions, we need some slightly hard commutative algebra, see e.g. Atiyah-MacDonald.

Degree of a Projective variety.

Old informal definition: Degree is the number of intersections with a generic linear subspace of complementary dimension. Alternative definition using Hilbert polynomials:

The projective variety has graded homogeneous coordinate ring

$$k[x_0, \ldots, x_n]/I = \text{ graded module over } k[x_0, \ldots, x_n].$$

in which the degree of $x_i = 1$.

So it has Hilbert polynomial $d\frac{x^n}{n!} + \cdots$.

Example 18.7. Find the degree of projective space $\mathbb{P}^n$. The homogeneous coordinate ring $k[x_0, \ldots, x_n] = \oplus R_n$. The dimension of R_n is given by $1, n+1, \ldots, \binom{n+k}{n}$. So the polynomial begins with $\frac{k^n}{n!}$, implying that the projective space has degree 1.

Check that the degree of the polynomial defining a degree d hyper surface has Hilbert polynomial with leading coefficient d. Hilbert polynomial of a hyper surface of degree d is

$$f(k) = \binom{n+k}{n} - \binom{n+k-d}{n}.$$

where the second term refers to multiplies of degree d polynomials defining the hyper surface.

This expands to have leading term $d\frac{k^{n-1}}{(n-1)!}$. So the degree and dimension are as we would hope.

19. Tuesday, November 6, 2012

19.1. Hilbert Polynomials of Varieties.

Example 19.1. Consider the Twisted Cubic in $\mathbb{P}^3$. It is parametrized by

$$(s^3 : s^2t : st^2 : t^3),$$

and cut out by the ideal

$$I = \langle wz - xy, wy - x^2, xz - y^2 \rangle.$$

The homogeneous coordinate ring is $k[w, x, y, z]/I$. Let the grading give each variable degree 1.

What is the dimension of the piece of degree k?

Eliminate xy, x^2, y^2 using the relations. The degree k coordinate ring is spanned by $w^i z^{k-i}, w^i xz^{k-i-1}$, and $w^i yz^{k-i-1}$.

This implies that $\dim R_k$ is $1, 4, 7, 10, \ldots$. The Hilbert polynomial is $3k+1$.

Question 19.2. Why is the Hilbert polynomial only the correct dimension for large k?

Answer: The Hilbert polynomial really gives the Euler characteristic χ of the line bundle $\mathcal{O}(n)$.

$$\chi(\mathcal{O}(n)) = \dim H^0(\mathcal{O}(n)) - \dim H^1(\mathcal{O}(n)) + \dim H^2(\mathcal{O}(n)) - \cdots .$$

The later terms vanish for large n, and the first term is the dimension piece of the coordinate ring.

For $n = 0$, $\chi = \chi(\mathcal{O}(0))$, the constant sheaf is called the holomorphic Euler characteristic of the variety. $(-1)^{\dim}(\chi - 1)$ is called the *arithmetic genus*.

Remark 19.3. The Hilbert polynomial of a subvariety of $\mathbb{P}^n$ is essentially the only "discrete" invariant.

Grothendieck noted that the Hilbert polynomial is constant on components of the "Hilbert scheme."

Hartshorne: 2 points of Hilbert scheme with the same Hilbert polynomial are in the same component.

19.2. **Schemes.** Schemes generalize algebraic sets in 3 ways:

(1) They need not be over fields, so we can look at $x^n + y^n = z^n$ over $\mathbb{Z}$.
(2) They need not be "finitely generated."; it allows us infinite-dimensional objects.
(3) The coordinate rings may have nilpotent elements.

Example 19.4. Consider the intersection of $y = x^2$ and $x^2 = 0$, a point and a parabola.

The intersection (as varieties) is a point; however, this is wrong – it is really more like two points in the same place.

In terms of varieties, the coordinate ring is $k[x, y]/(x, y) = k$. On the other hand,

$$k[x, y]/(x^2, y - x^2) = k[x]/(x^2).$$

which is 2-dimensional over k, but has nilpotent elements.

Recall that affine algebraic sets correspond to f.g. algebras over k with no nilpotents. We map the algebra to the affine set via the "spectrum" of all maximal ideals.

For an abstract algebraic set, we glue together affine algebraic sets along open subsets.

In the world of schemes, the correspondence is:

Affine schemes	$\Leftrightarrow$ $\longleftarrow$	Any Commutative ring.
	Spectrum of Prime Ideals	
Schemes		Glue together affine schemes along open sets.

The tool we need to define schemes is *sheaves* (Leray 1950 in topology). It was introduced into algebraic geometry by Serre.

Example 19.5. This example illustrates how sheaves clean up algebraic geometry. The old definition of arithmetic genus of a surface:

$$p_a = \binom{\mu_0 - 1}{2} - (\mu_0 = 4)\varepsilon_0 + \varepsilon_1/2 + 2t,$$

with these symbols describing sections of the surface by hyperplanes and similar features.

The problem is – how would we generalize this to higher dimensions??

In terms of sheaves, p_a is essentially the Euler characteristic:

$$\chi = \sum (-1)^n \dim H^i(V, \mathcal{O}(0)).$$

where the H^i is a sheaf cohomology group.

Definition 19.6. Let X be a topological space. A *pre sheaf* assigns a set $S(U)$ to each open set $U \subseteq X$. Morphisms $\rho_{UV} : S(U) \to S(V)$ whenever $V \subseteq U$ such that

(1) ρ_{UU} is the identity.
(2) For $W \subseteq V \subseteq U$, $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

So, S is a contra variant functor from the category of open sets of X to $Sets$. Recall that the open sets of X form a category whose

objects are open sets of X,

morphisms are the unique morphism $U \to V$ whenever $U \subseteq V$.

(Hartshorne's definition of presheaves adds a condition for $S(\varnothing)$; this is not in agreement with mainstream definitions.)

Example 19.7. Typical example of a pre sheaf. If we have a map $f : Y \to X$, for any $U \subseteq X$, look at continuous sections $f^{-1}(U) \to U$. Then ρ_{UV} is the restriction from U to V.

Example 19.8. $S(U) = A$ for some fixed set A.

Example 19.7 has the following additional properties:

(1) If U is covered by $U_1, U_2, \ldots$, then any element s of $S(U)$ is uniquely determined by the restrictions $\rho_{UU_1}(s)$.
(2) Suppose we choose $s_i \in S(U_i)$. When can we "glue" these together to get a map $s \in S(U)$? A necessary condition is that $\rho_{U_1 \to U_1 \cap U_2}(s_1) = \rho_{U_2 \to U_1 \cap U_2}(s_2)$. These are both equal (by presheaf axioms) to $\rho_{U \to U_1 \cap U_2}(\mathrm{s})$.

    Conversely, if this condition is satisfied for all pairs U_i, U_j, then s exists and is unique.

A presheaf satisfying the two conditions above is called a sheaf.

Example 19.9. One example of a presheaf that is not a sheaf: the constant sheaf from the example above. Taking two disjoint open sets U_1 and U_2 with $a_1 \in S(U_1)$ and $a_2 \in S(U_2)$, such that $a_1 \neq a_2$, then there is no a in $S(U_1 \cup U_2)$ restricting to a_1, a_2.

More generally, we can form sheaves with values in any category: Just replace sets with objects of the category. The most important example: sheaves of abelian groups.

Example 19.10. The Philosophy of Sheaves: sheaves of sets over a topological space behave like a weak model of set theory.

Many operations with sets extend to sheaves.

Sets have operations: $X \cup Y$ disjoint union, $X \times Y$ product, X^Y function spaces, $P(X)$ power sets.

These all have analogues for sheaves. However, the category of sheaves obeys intuitionistic logic rather than classical logic. (Topos)

Similarly, sheaves of abelian groups behave in a very similar way to abelian groups.

Example 19.11. We have operations: direct sum $\oplus$, tensor product $\otimes$ of sheaves of abelian groups.

Sheaves of abelian groups form an abelian category.

A sheaf of abelian groups over a space X is something like a *family* of abelian groups indexed by X.

19.3. **Examples of Sheaves.** The theory of sheaves is boring, so we will only discuss examples. From now on, "sheaf" refers to a sheaf of abelian groups.

Example 19.12. Sheaf of continuous/ differentiable/ analytic/ regular functions on a topological space/ manifold/ algebraic set.

Example 19.13 (Skyscraper Sheaf)**.** Suppose x is a point of X. Suppose A is an abelian group. Put $S(U) = A$ if $x \in U$ and 0 if $x \notin U$.

Informal picture: S represents a family of abelian groups, A at x, and 0 elsewhere.

Example 19.14 (Constant sheaf and presheaf)**.** Constant Presheaf: $S(U) = A$ for all U.

Constant Sheaf: $S(U) =$ continuous maps from $U \to A$, where A is given the discrete topology.

$$S(U) \cong A^{\#\text{components of } U}.$$

Example 19.15. If $Y \to X$ is a continuous map, then we have a sheaf: $S(U) =$ sections of $f^{-1}(U)$.

Specifically, if $Y \to X$ is a vector bundle, then we get a sheaf corresponding to this vector bundle. So Vector Bundles $\subseteq$ (abelian) Sheaves, even though the former is not an abelian category, and the latter is.

Let us prove this assertion:

Proposition 19.16. *Vector bundles do not form an abelian category.*

Proof. Consider $X = \mathbb{R}$. Look at the trivial 1-dimensional vector bundle $V : \mathbb{R} \times X \to X$, with a map $V \to V$ given by multiplication by $x \in X = \mathbb{R}$.

What is the kernel/cokernel? The only possible vector bundle that can be kernel/cokernel is 0. So we would have an exact sequence

$$0 \to V \to V \to 0.$$

This means $x : V \to V$ would be an isomorphism, but it is not. □

On the other and, in the category of sheaves, this is somehow fixed by a skyscraper sheaf with support at 0. This does not correspond to any vector bundle.

Question 19.17. Given a sheaf over X does it come from sections of some continuous map $f : Y \to X$?

Yes. There is a canonical choice for $f : Y \to X$, Y is called an etale space (usually non-Hausdorff, even if X is Hausdorff).

Very brief sketch of construction of Y:

Definition 19.18. The *stalk* of a sheaf S at point $x \in X$ is the direct limit $\lim_{x \in U} S(U)$.

The space$Y$ has a <u>points</u> unions of stalks at all points of X. Put topology on Y (see Hartshorne). Check that sections of Y correspond to sets $S(U)$.

Exercise 19.19. Let $X = \mathbb{R}$. If S is the sheaf of smooth functions, the etale space of S is non-Hausdorff.

If S is a sheaf of analytic functions, then the etale space is Hausdorff.

20. Tuesday, November 13, 2012

[Class missed last Thursday (11/8) due to travel]

Example 20.1. Examples of Spec $(R) =$ the set of prime ideals.

1. Spec $(\mathbb{Z}) = \{(0), (2), (3), (5), \ldots\}$. Note that the point (0) is not closed, since it is contained in other prime ideals.
2. Spec $(\mathbb{C}[x])$ = maximal ideals $(x - a)$ for $a \in \mathbb{C}$, which puts it in bijection with the affine line. We also have a non-maximal prime ideal (0), which is a non-closed point. Its closure is the whole space. This can be visualized as the affine line + a *generic point* (0).

   These last two are both Dedekind domains, which is why they are similar.

(3) Spec $(\mathbb{C}[x, y])$ has maximal primes $(x - a, y - b)$ in bijection with points of the affine plane $\mathbb{C}^2$.

It also has non-maximal prime (0) whose closure is the whole space.

Further prime ideals are $(f(x, y))$ where f is an irreducible polynomial. These ideals are in bijection with the irreducible 1-dimensional subvarieties of $\mathbb{C}^2$. The closure of such a point is the point itself and all closed points (maximal ideals) that lie on the curve.

So, the points of Spec $\mathbb{C}[x, y]$ are in bijection with the points, curves, and the whole plane.

(4) Discrete valuation ring, such as $\mathbb{Z}_{(p)} = \{\text{all rational numbers } a/b,\ p \not| b\}$ for p prime.

This has exactly two prime ideals: $(0), (p)$. (All the ideals are of the form (0) or (p^n)). So Spec $Z_{(p)}$ has two points, one of which is closed.

(5) Spec $\mathbb{Z}[x]$. The injection of rings $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ implies a map Spec $(\mathbb{Z}) \leftarrow$ Spec $(\mathbb{Z}[x])$ fibered over Spec $(\mathbb{Z})$.

What do the fibers look like?

Spec $(\mathbb{Z})$ has points $(0), (p)$ for p prime. What is the fiber of Spec $\mathbb{Z}[x]$ over $(0) \in$ Spec $(\mathbb{Z})$? The fiber is just Spec $\mathbb{Q}[x]$ which is a Dedekind domain. The points are $(0), (f(x))$, for f irreducible polynomial in $\mathbb{Q}[x]$. These are in bijection with irreducible polynomials in $\mathbb{Z}[x]$ with content 1, which are also orbits of algebraic numbers under $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

Look at the fibers over $(p) \in$ Spec $(\mathbb{Z})$, p prime. The fiber is the same as Spec $F_p[x]$ also a Dedekind domain. The spectrum is $(0), (f(x))$, for f irreducible polynomial in $F_p(x)$. These are in bijection with orbits of points in finite fields F_{p^n} under $Gal(F_{p^n}/F_p)$.

There is extra structure: Suppose we pick a point in the fiber over $(0) \in$ Spec $(\mathbb{Z})$. This will be a non-closed point in Spec $\mathbb{Z}[x]$, even though ti is closed in the fiber. The closure contains points in other fibers.

For example, Pick point $(x^2 + 1)$. The closure contains points over all fibers over (p). When $p = 2$, $(x^2 + 1) = (x + 1)^2$ so it contains the point $(x - 1, 2)$.

In the fiber over (5), $x^2 + 1$ in F_5 has two roots $2, 3$. So the intersection with this fiber has two points.

Over F_3, $x^2 + 1$ is irreducible, so its intersection with the fiber has 1 point.

We now attempt to draw Spec $\mathbb{Z}[x]$.

	(0) generic point of Spec $F_2(x)$				(0) (closure is whole space) (x^2+1), (x^3+x+1), $\vdots$ (irred. polynomials over $\mathbb{Q}[x]$)
	(x^3+x+1) (x^2+x+1) $(x-1)$	(x^2+2) (x^2+1) $(x-2)$ $(x-1)$			$(x-a), a \in \mathbb{Q}$
Spec $\mathbb{Z}$	(2)	(3)	(5)	$\cdots$	(0)

Exercise 20.2. Find the intersection of closures of $(x^2 + 1), (x - 5)$.

The idea: Spec $\mathbb{Z}[x]$ can be thought of as a *surface*, with 1-dimensional curves on it: such as fibers of Spec $\mathbb{Z}[x] \to$ Spec $\mathbb{Z}$, and closures of points of Spec $\mathbb{Q}[x]$. This is an arithmetic surface.

Remark 20.3 (Properties of Spec R)**.** (1) Spec (R) is always (quasi-)compact. Follows from the fact that if (1) is generated by some set of elements, it is generated by a finite number of them.

(2) Every irreducible set is the closure of some point. (Exercise) There is a $1:1$ correspondence between irreducible closed sets and points of Spec.

20.1. **Local ringed structure of Spec (R).** We need to assign a ring to every open subset. Recall localization of a ring R at some multiplicative subset S.

A multiplicative subset is defined as a set closed under multiplication (If S is not multiplicative just replace it by the multiplicative subset it generates.)

Localization is the ring obtained from R by forcing all elements of S to be invertible.

Construction: Take ring $R[t_1, t_2, \ldots]$ with t_i corresponding to elements $s_1, s_2, \ldots$ of S.

Then take the quotient $R[t_1, \ldots]/(t_1s_1 - 1, t_2s_2 - 1, \ldots)$. The obvious universal property is that any homomorphism from R to any ring T so that the images of S are invertible factors uniquely through the localization.

Problem 20.4. We have a homomorphism $R \to R_S$. What is its kernel?

If $s \in S$ is a zerodivisor, i.e. $sr = 0$, then $r \in$ kernel.

If s is nilpotent, then the kernel is the whole ring, so the localization is the 0 ring.

Concrete construction of localization:

Recall the ring of fractions of $\mathbb{Z}$. The set of points $(a, b), b \neq 0$; we write these as a/b. We mod out be the equivalence relations $a/b = c/d$ if $ad = bc$. This suggests a definition for localization R_S. Look at pairs a/b such that $b \in S$.

We want to mod out by the equivalence relation $a/b = c/d$ if $bc = ad$ — however, if S contains zerodivisors this will make a mess. The modified relation is: $a/b \equiv c/d$ if $s(ad - bc) = 0$ for some $s \in S$. This complication is only needed if S has zerodivisors.

Now, check that this gives localization R_S. (Long series of boring checks.)

The advantage of the explicit construction of R_S is that we can identify the kernel of $R \to R_S$. Since $a \mapsto a/1$, the equivalence relation tells us that $a/1 = 0/1$ when $s(a - 0) = sa = 0$ for some $s \in S$. Therefore, the kernel is the set of elements in R annihilated by some $s \in S$.

Recall, Spec R has a basis of open sets $D_f =$ prime ideals not containing $f \in R$ (places where $f \neq 0$).

Let $\mathcal{O}(D_f) =$ localization of R at $f = R[f^{-1}]$, where $\mathcal{O}(D_f)$ is the ring of the locally ringed space associated to the open set D_f.

Problem 20.5. What about the open sets U not of the form D_f?

Bad news: $\mathcal{O}(U)$ is hard to describe explicitly.

Good news: No need to describe $\mathcal{O}(U)$. Key point: We can construct sheaves by giving their values on a basis for the topology, and checking the sheaf axioms for covers by sets in this basis.

Suppose $\{U_i\}_{i \in I}$ form a basis fro the topology and we have groups $S(U_i)$, maps $S(U_i) \to S(U_j)$ whenever $U_j \subseteq U_i$ compatible for $U_i \subseteq U_j \subseteq U_k$. Suppose these satisfy the sheaf axiom for all covers of some U_i by sets $U_j, U_k, \ldots$

Then: S can be extended uniquely to a sheaf. The proof is left as an exercise.

Remark 20.6. The key philosophy for working with sheaves on Spec (R): Concentrate on the open sets D_f and ignore other open sets.

Example 20.7. In Spec $k[x, y]$, the open sets $x \neq 0, y \neq 0$ has union $\mathbb{A}^2 \setminus \mathbf{0}$, not of the form D_f.

Problem 20.8. We need to check the sheaf axioms for open sets D_f. That is, suppose D_f is covered by open sets $D_{f_1}, D_{f_2}, \ldots$– we want to show that given elements in $\mathcal{O}(D_{f_1}), \mathcal{O}(D_{f_2}), \ldots$, there is a unique element in D_f restricting to them all.

Simplifications: 1. Replace the ring R by R_f so we can assume $f = 1$. So, Spec (R) covered by $D_{f_1}, D_{f_2}, \dots$ means that $f_1, f_2, \dots$ generate the unit ideal in R. So, $1 = a_1f_1 + a_2f_2 + \cdots$ for some a_i.

First check that $r \in R$ is determined uniquely by its restrictions to the open sets D_{f_i}. Suppose r has image 0 in D_{f_i} – what does this mean? $R \to R_{f_i}$ then $r \in$kernel if and only if $f_i^{n_i}r = 0$ for some n_i, since the multiplicative subset is generated by f_i.

So we want to show that if:

$$1 = a_1f_1 + a_2f_2 + \cdots \qquad \text{and} \qquad f_1^{n_1}r = 0, f_2^{n_2}r = 0, \dots$$

then $r = 0$.

Trick: Replace each f_i by $f_i^{n_i} = g_i$. Then there is still a relation $1 = b_1g_1 + b_2g_2 + \cdots$ for some b_i as $1 = (a_1f_1 + \cdots)^N$, and for N sufficiently large, every term in this expansion is divisible by one of $f_i^{n_i}$. So we have $1 = b_1g_1 + b_2g_2 + \cdots$, and $g_1r = 0, g_2r = 0$. Multiplying both sides of the first equation by r and substituting, we find $r = 0$.

Hard part: Suppose we have compatible elements $r_i/f_i^{n_i}$ in $\mathcal{O}(D_{f_i}) = R_{f_i}$. We need to find $r \in R$ whose image in R_{f_i} is $r_i/f_i^{n_i}$.

What do we mean by compatible elements? That $r_i/f_i^{n_i}$ and $r_j/f_j^{n_j}$ are the same in $R_{f_if_j}$. This means:

$$(f_if_j)^{m_{ij}}(r_if_j^{n_j} - r_jf_i^{n_i}) = 0$$

for some m_{ij}.

As before, we have $1 = a_1f_1 + a_2f_2 + \cdots$ for some a_i. We want to find $r = r/1$ with

$$f_i^{m_i}(f_i^{n_i}r - r_i) = 0$$

for some m_i. We need to solve this equation, which we will do next time.

21. Thursday, November 15, 2012

21.1. Spec R is a sheaf.

Last time we were discussing the Construction of Spec (R). So far:

- **Points** are prime ideals of R.
- **Base** for open sets: $D_f, (f \in R) =$ prime ideals not containing f. "Points where $f \neq 0$."
- **Ringed Structure:** $\mathcal{O}(D_f) = R[f^{-1}]$ for each f.

We need to check sheaf property whenever D_f is covered by open sets D_{f_i}.

Step 1: We can assume $f = 1$ by replacing R with R_f.

We are given $1 = a_1f_1 + \cdots$, where D_{f_i} cover Spec R.

Assuming that r is in the kernel of the localization, there exists m_{ij} such that

$$f_i^{m_{ij}}f_j^{m_{ij}}(r_if_j^{n_j} - r_jf_i^{n_i}) = 0$$

This implies that

$$\frac{r_i}{f_i^{n_i}} = \frac{r_j}{f_j^{n_j}} \qquad \text{on } D_{f_i} \cap D_{f_j}.$$

We want to find $r \in R$ such that $f_i^{k_i}(f_i^{n_i}r - r_i) = 0$. This is hard to solve directly.

The result is

$$\frac{r_i}{f_i^{n_i}} = r\text{on } D_{f_i}.$$

We replace f_i by suitable powers of f_i. Then, we can assume that $1 = a_1f_1 + a_2f_2 + \cdots$ such that $f_if_j(r_if_j - r_jf_i) = 0$. We want to find r with $f_i(f_ir - r_i) = 0$. Now we replace r_if_i by s_i.

We get $0 = s_if_j^2 - s_if_i^2$. We have to solve $f_i^2r = s_i$. Again we replace by f_i^2 by g_i, so $1 = b_1g_1 + b_2g_2 + \cdots$ for some b_i's.

We have reduced to the following problem: Given $1 = b_1g_1 + b_2g_2 + \cdots$ such that $s_ig_j = s_jg_i$ we want to solve, $g_ir = s_i$.

Remark 21.1. Motivation: What is r? Suppose $g_i r = s_i$. Then $r = r \cdot 1 = rb_1g_1 + rb_2g_2 + \cdots = b_1s_1 + b_2s_2 + \cdots$.

So we *define* r to be $b_1s_1 + b_2s_2 + \cdots$. Now it is easy to check that $g_ir = s_i$.

Remark 21.2. Key properties of Spec R:

(1) $\mathcal{O}(D_f) = R[f^{-1}]$ for $f \in R$.

(2) Local ring at $\mathfrak{p} \in \text{Spec } R = R_\mathfrak{p}$ = localization of R at $\mathfrak{p} = R_S$ where S is the *complement* of $\mathfrak{p}$, which is multiplicative.

You can also consider this as the

$$\lim_{\mathfrak{p}\in U} \mathcal{O}(U) = \lim_{\mathfrak{p}\in D_f} \mathcal{O}(D_f) = \lim_{f\notin\mathfrak{p}} R[f^{-1}] = R_\mathfrak{p}.$$

(3) Ignore open sets not of the form D_f.

Definition 21.3. A *scheme* is a ringed space locally isomorphic to Spec (commutative ring). This is a *locally ringed space*: localization at any points is a local ring.

Remark 21.4. Two different concepts: Morphisms of ringed spaces and morphisms of locally ringed spaces $f : X \to Y$ are NOT the same.

Morphisms of locally ringed spaces (informally) are morphisms such that a function g on Y vanishes at a point $y \in Y$ its pullback should vanish at $f^{-1}(y)$. Rephrase this in terms of ringed space structure.

Definition 21.5. Morphism of ringed spaces $X \to Y$ consists of

(1) Continuous map f from X to Y.

(2) If $U \subset Y$, we need to be given a morphism of rings $\mathcal{O}(U) \to \mathcal{O}(f^{-1}U)$.

(3) Should satisfy various compatibility conditions.

For locally ringed spaces, we need to add the extra condition:

If $y \in Y$ and $f(x) = y$, we get a homomorphism:

$$(\text{local ring at } y) \quad \to \quad (\text{local ring at } X)$$

This is a homomorphism of *local rings*, meaning it maps the maximal ideal of the first into the maximal ideal of the second.

Example 21.6. There are ringed space morphisms between locally ringed spaces that are *not* morphisms of locally ringed spaces.

Take $R = \mathbb{Z}_{(p)} = \{m/n \mid p \not| n\}$. (Alternatively, any discrete valuation ring), and $\mathbb{Q}$ = rationals = quotient field of R.

Spec $\mathbb{Q}$ = 1 point. $\mathcal{O}(\text{Spec } (\mathbb{Q})) = \mathbb{Q}$. Spec R has 2 points: (p) closed, (0) not closed.

What about morphisms Spec $\mathbb{Q} \to$ Spec R. The obvious one, coming from $R \subset \mathbb{Q}$ takes a point of $\mathbb{Q}$ to the *open* point of Spec R. Then $f : R \to \mathbb{Q}$ will have $f((0)) = (0)$.

This is a morphism of locally ringed spaces. The corresponding homomorphism of local rings is just $\mathbb{Q} \to \mathbb{Q}$.

Another morphism of ringed spaces is g which takes the point $(0) \in \text{Spec } \mathbb{Q}$ to the point (p) in Spec R.

$g : \text{Spec } (\mathbb{Q}) \to \text{Spec } R$. We need to define the map from $\mathcal{O}(\text{Spec } R) \to \mathcal{O}(\text{Spec } \mathbb{Q})$. Look at the effect on local rings, which is of course $R \subseteq \mathbb{Q}$.

Local ring of Spec R at closed point (p) is R. So we get a homomorphism of rings $R \hookrightarrow \mathbb{Q}$. However this is not a hom. of local rings, since it does not map $(p) \subset R$ into $(0) \subset \mathbb{Q}$.

Reason for this:

Homomorphisms of rings from $R \to S \quad \longleftrightarrow \quad$ morphisms of *locally* ringed spaces from Spec $S \to$ Spec R.

Otherwise you would get morphisms of affine schemes *not* corresponding to morphisms of rings.

So, the category of Rings is essentially the opposite of the category of affine schemes.

Special case of the following: We can describe morphisms of any scheme to Spec (R) for R a commutative ring. If X is a scheme and we have a morphism $X \to$ Spec (R), then in particular we get a homomorphism of rings from R to $\mathcal{O}(X)$. (R is the ring of the open set Spec (R)).

This is an isomorphism: maps of schemes $X \to$ Spec R are the "same" as homomorphisms of rings from R to $\mathcal{O}(X)$.

Remark 21.7. Consequence of this fact: The definition of an affine scheme Spec R is *correct.*

This isomorphism indicates a pair of adjoint functors:

$$\begin{array}{ccc} \text{Locally Ringed Spaces} & & \text{Rings} \\ X & \longrightarrow & \mathcal{O}(X) \\ \text{Spec } R & \longleftarrow & R \end{array}$$

These are unique up to equivalence. So, spec of a ring could be defined as adjoint functors of the natural forgetful functor from locally ringed spaces to rings.

21.2. **Constructing Schemes from Graded Rings.**

(1) The points of Spec R are prime ideals.
(2) Base of open sets are D_f.
(3) $\mathcal{O}(D_f) = R[f^{-1}]$.

We can consider R as the local ring of an affine variety.

Recall that a projective variety has a homogeneous coordinate ring R which is graded: $R = R_0 \oplus R_1 \oplus \cdots$.

From the homogeneous coordinate ring of a projective variety, we are able to construct the projective variety. Similarly, we want to take any graded ring to a scheme Proj R.

Definition 21.8. (1) The points of Proj R are graded prime ideals, not containing *all* positive homogeneous elements.
(2) Basis for the open sets: D_f for f homogenous. This is graded prime ideals of Proj (R) not containing f. (informally) points where f does not vanish.
(3) Ringed space structure: $\mathcal{O}(D_f) = R[f^{-1}]_0$.

Example 21.9. Take $R = k[x_0, \ldots, x_n]$. Taking the graded prime deals corresponds to subvarieties that are *cones.*

Not containing all positive homogeneous elements corresponds to not being 0.

So homogeneous primes not containing all pos. degree elements gives subvarieties of $\mathbb{P}^n$.

Example 21.10. Let $R = k[x_0, \ldots, x_n]$. Let $f = x_0$. Then D_f should be the affine space of all points $(1 : x_1 : \cdots : x_n)$. Coordinate ring will be $k[x_1, \ldots, x_n]$ = degree 0 elements of $k[x_1, \ldots, x_n][x_0^{-1}]$.

Moreover, the open subset D_f is in fact an affine scheme Spec (D_f). So Proj R is covered by open affine subschemes Spec D_f for f homogeneous, so it is a scheme. (Left as exercise.)

As with affine schemes, we work with D_f and ignore open sets of other types.

Remark 21.11. Given a scheme X, it determines a functor of points: a functor from schemes S to sets taking $S \to Mor(S, X)$, where the latter set is called the S-valued points of X.

Example 21.12. Suppose X = affine scheme Spec R. Then the corresponding functor of points takes S to $\mathrm{Hom}_{Rings}(R, \mathcal{O}(S))$.

For $R = \mathbb{Z}[x]$, the functor of points maps to $\mathrm{Hom}(R, \mathcal{O}(S)) = \mathcal{O}(S)$. So the functor of scheme Spec $\mathbb{Z}[x]$ takes any scheme to its ring of global functions.

Now we look at the same question for Proj R. Given a scheme S, what are the morphisms from S to Proj R?

Example 21.13. Let $R = \mathbb{Z}[x_0, x_1]$. Proj R = projective line (over $\mathbb{Z}$). Then, $Mor(S, \text{Proj } R) =$ projective line over S.

Suppose S is an affine scheme Spec A. What are the points of the projective line over a ring A? For a field A, the answer is

(1) $(x : y)/(x : y) \sim (\lambda x : \lambda y)$ where x, y are not both 0.
(2) Union of 2 affine lines $(1 : y) \cup (x : 1)$ glued together.

In general, both of these are wrong.