1 Friday, February 4, 2011

Geometry of solutions to sets of polynomial equations.

e.g., $x^2 + y^2 + 1 = 0 \longrightarrow$ Set of solutions (over $\mathbb{C}$) is really a sphere (with two points removed)

e.g., $y^2 = x^3 - x = x(x-1)(x+1)$ Over $\mathbb{C}$, the set of solutions is a torus (with one point removed)

Lots of applications to number theory, representation theory, etc.

We'll work over the field $\mathbb{C}$.

Recall (background reading, §10-7, 10-8 in Artin's *Algebra*):

Theorem (Hilbert's Nullstellensatz (weak))**.** *The maximal ideals of* $\mathbb{C}[x_1, \ldots, x_n]$ *are exactly those of the form* $(x_1 - a_1, \ldots, x_n - a_n)$ *corresponding to points* $(a_1, \ldots, a_n) \in \mathbb{C}^n$*.*

This means we can consider $\mathbb{C}^n$ as a purely algebraic object. It's called affine n-space, $\mathbb{A}^n_{\mathbb{C}}$ or $\mathbb{A}^n$ for short.

We want to define a nice topology on this space. One choice is to take the Euclidean (complex) topology: define open balls by

$$B_r(x) = \{y \in \mathbb{C}^n \,|\, |y - x| < r\}$$

and take these to be a basis.

But this is too many open sets (closed sets), e.g. $\{(x, y) \in \mathbb{C}^n \,|\, y = e^x\}$ is closed in the Euclidean topology. But we only care about polynomials, so we'll use a coarser topology (fewer open/closed sets).

We'll use the smallest topology such that polynomial functions are continuous. This is called the Zariski topology. Defined by: for a polynomial function $f \in \mathbb{C}[x_1, \ldots, x_n]$, define $D(f) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n \,|\, f(a_1, \ldots, a_n) \neq 0\}$ and declare all $D(f)$ to be open. (Note: D stands for distinguished.) As f varies over all polynomials, these $D(f)$ are taken to be a basis.

We have, e.g, $D(0) = \emptyset$, $D(1) = \mathbb{C}^n$, $D(fg) = D(f) \cap D(g)$.

Alternatively, let's see what the closed sets are. For every ideal $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$, the vanishing locus of I is $V(I) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n \,|\, f(a_1, \ldots, a_n) = 0 \ \forall f \in I\}$. As I varies, these describe all the closed sets in the Zariski topology.

Note that $\mathbb{C}^n \setminus D(f) = V(f)$.

NOTE:

1. Because $\mathbb{C}[x_1, \ldots, x_n]$ is noetherian[1], any I can be written as $(f_1, \ldots, f_k)$ for some $f_1, \ldots, f_k$. So $V(I) = V(\{f_1, \ldots, f_k\})$.

2. The maximal ideals (the smallest non-empty closed sets) exactly correspond to the points of $\mathbb{C}^n$. (weak Nullstellensatz)

e.g.

1) $\mathbb{A}^1$: the closed sets are $\emptyset = V(1)$, $\mathbb{A}^1 = V(0)$, and sets of zeros of polynomials, that is, all finite sets of points. (also called the cofinite topology)

2) $\mathbb{A}^2$: the closed sets are $\emptyset = V(1)$, $\mathbb{A}^1 = V(0)$, finite sets of points, but also union of $V(f)$ with a finite point set for some polynomial $f \in \mathbb{C}[x, y]$.

[1] Every ascending chain of ideals stabilizes: given $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, $\exists k$ such that $I_k = I_{k+1} = \cdots$. Equivalent to that every ideal is finitely generated

Why don't we include $V(f, g)$ for $f, g \in \mathbb{C}[x, y]$? It's because the locus of points where both f and g vanish (assuming they have no common factor) is a finite set of points. Note also that $V(f_1) \cup V(f_2) = V(f_1 f_2)$.

$\mathbb{C}[x_1, \ldots, x_n]$ is called the affine coordinate ring of $\mathbb{A}^n$. (think of it as set of functions on the space $\mathbb{A}^n$)

1.1 Projective Space

Claim: $\mathbb{A}^2$ is somewhat defective.

Not all lines intersect. In particular, rotations of one line can cause it to not intersect another line.

To fix this, we add points at infinity to get $\mathbb{P}^2$.

Nice way of doing this: Let

$$\mathbb{P}^2 = \left\{(x, y, z) \in \mathbb{A}^3 \setminus \{0, 0, 0\}\right\} \big/ (x, y, z) \sim (\lambda x, \lambda y, \lambda z) \qquad (\lambda \neq 0)$$

$\mathbb{A}^2$ is contained in the set of points for which $z \neq 0$: If $z \neq 0$, then

$$(x, y, z) \overset{\mathbb{P}^2}{=} \left(\frac{x}{z}, \frac{y}{z}, 1\right)$$

We have $(x, y) \in \mathbb{A}^2 \longrightarrow (x, y, 1)$.

$$\mathbb{P}^2 = \mathbb{A}^2 \coprod \mathbb{P}^1 = \mathbb{A}^2 \coprod \mathbb{A}^1 \coprod \text{point}(= \mathbb{A}^0)$$

Elements of $\mathbb{P}^2$ are written as $(x : y : z)$.

Define a topology on $\mathbb{P}^2$. Most natural way is to take a quotient topology from the Zariski topology on $\mathbb{A}^3 \setminus \{0, 0, 0\} \subseteq \mathbb{A}^3$.

Take a polynomial function $f \in \mathbb{C}[x, y, z]$. We want to say $V(f) = \left\{(x : y : z) \in \mathbb{P}^2 \,\middle|\, f(x, y, z) = 0\right\}$ is closed. But f gives different values on equivalent points.

We can write $f = f_0 + f_1 + \cdots + f_d$, f_i homogeneous of degree i. Then $f(\lambda x, \lambda y, \lambda z) = f_0(x, y, z) + \lambda f_1(x, y, z) + \cdots + \lambda^d f_d(x, y, z)$. We need to take homogeneous polynomials ($f = f_i$ for some i). Now $f = 0$ and $f \neq 0$ makes sense. Then $V(f_1, \ldots, f_k)$ describe the closed sets.

2 Monday, February 7, 2011

2.1 Affine varieties

Definition. An *affine variety* is the set of solutions to a system of polynomial equations

$$f_1(x) = f_2(x) = \cdots = f_r(x) = 0$$

for $f_1, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$. ($x$ is shorthand for $(x_1, x_2, \ldots, x_n)$.)

Alternatively, it's $V(I)$ for some $I = (f_1, \ldots, f_r) \subset \mathbb{C}[x_1, \ldots, x_n]$.

e.g., point: $(x_0, y_0) = (x - x_0, y - y_0)$

line: all (x, y) for which $ax + by + c = 0$

conic: locus of complex zeros of a quadratic equation in two variables $q(x, y) = 0$

cubic: locus of complex zeros of a cubic polynomial

Classification of these depends on what coordinate changes one allows. If we allow arbitrary invertible linear operators and translations, any line can be converted to $x = 0$. Any conic can be converted to either $x^2 - y^2 - 1 = 0$ or $x^2 - y = 0$, by completing the square.

Zariski topology on an affine variety $(V(I_0)) = X \subset \mathbb{A}^n$ is just subspace topology induced from Zariski topology on $\mathbb{A}^n$ (i.e., closed sets of X are just all the $y = V(I)$ which are contained in X). Note: $V(0) = \mathbb{A}^n$ so $V(0) \cap X = X$.
Check:

$$\begin{aligned} V(1) &= \emptyset \\ \bigcap_{\alpha \in S} V(I_\alpha) &= V\left(\bigcup_{\alpha \in S} I_\alpha\right) \\ &= V\left(\sum_{\alpha \in S} I_\alpha\right) \end{aligned}$$

(arbitrary intersection of closed sets is closed)

$$V(I) \cup V(J) = V(I \cap J)$$

(To see, consider a point $p \in V(I \cap J)$, $p \notin V(I)$, show that $p \in V(J)$)

2.2 Projective Plane $\mathbb{P}^2$

Recall

$$\mathbb{P}^2 = \big\{(x:y:z) \in \mathbb{A}^3 \setminus \{0,0,0\}\big\} \big/ (x:y:z) \sim (\lambda x : \lambda y : \lambda : z) \qquad (\lambda \neq 0)$$

(lines through origin in $\mathbb{A}^3$ or $\mathbb{C}^3$)

A line in $\mathbb{P}^2$ is given by an equation $ax + by + cz = 0$ as long as $(a,b,c) \neq (0,0,0)$. Note that (a,b,c) and $(\lambda a, \lambda b, \lambda c$ give the same line for $\lambda \neq 0$. So the set of lines forms another projective plane (dual projective plane $\check{\mathbb{P}}$). This equation $ax+by+cz = 0$ exhibits the duality between points and lines.

Lemma. *A pair of distinct lines contains exactly one point in common, and a pair of distinct points lie on exactly one line.*

Recall that we had $\mathbb{A}^2 \to \mathbb{P}^2$, $(x,y) \mapsto (x:y:1)$. Bijection between $\mathbb{A}^2$ and $U_z := \mathbb{P}^2 \setminus \{z = 0\}$ (since $(x:y:z) \mapsto \left(\frac{x}{z}, \frac{y}{z}\right)$ if $z \neq 0$). Similarly we have U_x and U_x also in bijection with $\mathbb{A}^2$. Then $U_x \cup U_y \cup U_z = \mathbb{P}^2$. This is a cover, and is called the standard affine open covering of $\mathbb{P}^2$.

Note that $U_x \cap U_y \subseteq U_x$ (this is $\{(x:y:z) \,|\, x \neq 0, y \neq 0\} \subset \{(x:y:z) \,|\, x \neq 0\}$) is the set $\{y \neq 0\} = D(y)$. So its open in the Zariski topology. $U_x \cap U_y \subseteq U_y$ is also open: $V \subset \mathbb{P}^2$ is open iff all its intersections with the standard affines (standard affine open covers) are open (in the standard affines).

This is the same topology as the other version of the Zariski topology on $\mathbb{P}^2$ by taking $V(f)$, f homogeneous polynomial in $\mathbb{C}[x,y,z]$. to be a closed set in $\mathbb{P}^2$, and then take arbitrary intersections and finite unions. (same as quotient topology on $\mathbb{A}^3 \setminus \{0\}$)

Note: Since Zariski topology $\subseteq$ classical/complex/Euclidean topology (all open sets in Zariski are open in classical)
This means we can define a classical topology as well on $\mathbb{P}^2$. It makes $\mathbb{P}^2$ into a compact Hausdorff space.

Proof. Compact: Let $C_z \subseteq U_z$ be the set of $(u, v, 1)$ such that $|u| \leq 1$, $|v| \leq 1$ and similarly C_x and C_y. It's clear that C_x, C_y, C_z are compact (also closed subspaces of $\mathbb{P}^2$ in the complex topology). Since $\mathbb{P}^2 = C_x \cup C_y \cup C_z$, $\mathbb{P}^2$ is compact. □

2.3 Change of coordinates in $\mathbb{P}^2$

Four special points determine coordinates in $\mathbb{P}^2$:

$$e_1 = (1:0:0) \qquad e_2 = (0:1:0)$$
$$e_3 = (0:0:1) \qquad \epsilon = (1:1:1)$$

Think of these as column vectors.

Change of coordinates is described by a 3×3 invertible matrix P.

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = P \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix}$$

(x is old, x' is new)

if the matrix is a scalar (diagonal) matrix, then it doesn't affect any coordinate change. Similarly, the coordinate changes corresponding to P and sP are the same.

If $A = (a, b, c)$ and ℓ is the line $ax + by + cz = 0$, $AX = 0$, then $A(PX') = 0$ or $(AP)X' = 0$, so the equation for ℓ in the new coordinates is AP.

Proposition. *Let p_1, p_2, q_3, q be four points in $\mathbb{P}^2$, now three collinear. Then $\exists!$ change of coordinates $PX' = X$ such that $X = p_1, p_2, p_3, q$ because $X' = e_1, e_2, e_3, \epsilon$.*

Proof. p_1, p_2, p_3 are linearly independent vectors in $\mathbb{C}^3$. So $\exists$ transformation P such that $Pp_i = e_i$. Now q is non-collinear with p_1, p_2, p_3; all of its coordinates are non-zero. Then scale each coordinate to take q to ϵ (modifies P). This doesn't affect e_1, e_2, e_3. □

Conics we had $x^2 - y^2 - 1 = 0$ and $x^2 - y = 0$ in $\mathbb{A}^2$. In $\mathbb{P}^2$, these become $x^2 - y^2 - z^2 = 0$ and $x^2 - yz = 0$. We can transform the first into the second by doing $x^2 - y^2 = z^2$, $(x - y)(x + y) = z^2$, coordinate change to $x'y' = z'^2$.

3 Wednesday, February 9, 2011

3.1 Curves in $\mathbb{P}^2$

Curves in $\mathbb{P}^2$ are defined by homogeneous irreducible polynomials f: $C = V(f)$.

e.g., the line containing a pair of points $(p, q) \in \mathbb{P}^2$ is the set of points $up + vq$ for $(u, v) \neq (0, 0)$. It's equation $Ax = 0$ is obtained by solving $Ap =$, $Aq = 0$. (Think of $A = (a, b, c)$, $p = (x_1, y_1, z_1)$, $q = (x_2, y_2, z_2)$. Then $ax_1 + by_1 + cz_1 = 0$, $ax_2 + by_2 + cz_2 = 0$. Then $\begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. i.e., $[a, b, c]$ is the kernel of the 2×3 matrix, which has rank 2.)

The restriction of a homogeneous polynomial $f(x, y, z)$ to a line $\ell = \{up + vq\}$ is obtained by substitution $f(up + vq)$. This is a homogeneous polynomial in u, v of degree $= \deg(f)$. Over $\mathbb{C}$, any such polynomial can be factored into linear factors $(up_i + vq_i)$. These are the points of ℓ (not necessarily distinct) that lie on $V(f)$. Thus, a plane polynomial curve of degree d meets a line in d points, counted with multiplicity.

Let f be a homogeneous polynomial of degree d in x_1, x_2, x_2, and let $C = V(f)$. Let f_i denote $\frac{\partial f}{\partial x_i}$ and let $f_{ij} = \frac{\partial^2 f}{\partial x_i \partial x_j}$. Then the Hessian Matrix is the 3×3 symmetric matrix

$$H(f) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{ij}.$$

Proposition (Euler's Formula)**.** *Let f, $d = \deg(f)$, f_i be as above. Then $\sum_{i=1}^{3} f_i x_i = f \deg(f)$.*

Proof. Check it for monomials, since it's additive. (CHECK NOT INCLUDED) □

This works for polynomials in n variables.
Now consider the Taylor expansion of the restriction of f to $\ell = \{up + vq\}$.
Setting $u = 1$ ($v = 0$ is p, so looking near the point p):

$$f(p + vq) = f(p) + \left(\sum f_i(p) q_i\right) v + \frac{1}{2}\left(\sum f_{ij} q_i q_j\right) v^2 + \mathcal{O}(v^3)$$

with $q = (q_1, q_2, \ldots)$.

Proposition.

1. *If p is a point of C, then $f(p) = 0$.*
2. *Suppose $p \in C$, and $f_i(p)$ are not all 0. Then the equation of the tangent line T to C a t p is $\sum f_i(p) q_i = 0$.*
3. *Let h be the Hessian of f at p. Then $\det h = 0$ iff p is a* flex *point C (i.e., a restriction of f to the tangent line at p has a zero of order ≥ 3 at p*

Proof.

1. By definition.
2. Tangent line: if the restriction of f to T has at least a second order 0 (by definition). So looking at the coefficient of v, this is clear.
3. Exercise: Check that the restriction of the quadratic term to the tangent line is 0 iff $\det h = 0$. □

Definition. If all the f_i vanish at p, then p is called a *singular* point of $C = V(f)$. Otherwise, say that C is *non-singular* at p. Say that C is a *non-singular curve* if it has no singular points.

3.1.1 Nonsingular curves

e.g. 1, an irreducible conic is always non-singular

Proof. Convert to $x^2 - yz = 0$. $f_x = 2x$, $f_y = -z$, $f_z = -y$. Since $(x, y, z) \in \mathbb{P}^2$, not all these can be zero, so it's nonsingular □

e.g. 2, An irreducible plane cubic can have at most one singular point (exercise)
e.g. 3, The curve $x^d + y^d + z^d = 0$ is non-singular (smooth) for $d \geq 1$. (Fermat polynomial of degree d).
The partial derivatives are dx^{d-1}, dy^{d-1}, dz^{d-1}, not all zero (in $\mathbb{P}^2$)
e.g. 4, The curve $x^3 + y^2 - xyz = 0$ is singular at the point $(0 : 0 : 1)$.

Proposition. *For most values of the coefficients of a polynomial of degree d, the curve $C = V(f) \subseteq \mathbb{P}^2$ is smooth.*

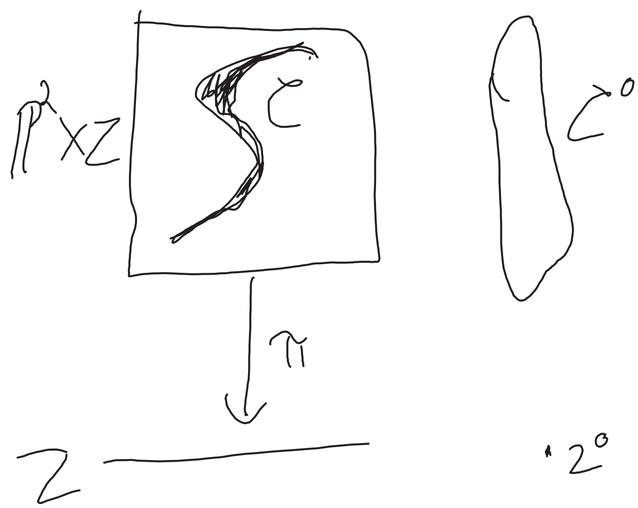
Proof. See two proofs, each of which depends on some theorem which will be proved later.

Setup: Order the monomials of degree d in x, y, z arbitrarily m_1, m_2, $\ldots$, m_N. (Note: $N = \binom{d+k-1}{k-1}$ for k variables.)

An arbitrary polynomial of degree d is a linear combination of the monomials m_ν with some coefficients z_ν. Think of z_ν as variables and let

$$F = \sum_{\nu=1}^{N} z_\nu m_\nu \in \mathbb{C}[x, y, z, \{z_\nu\}].$$

Then $F = 0$ defines a subvariety $\mathcal{C}$ of the product $\mathbb{P}^2 \times Z$, where Z is $\mathbb{A}^N$ with coordinates z_ν.



The *fiber* $\mathcal{C}^0 = \pi^{-1}(z^0)$ of $\mathcal{C}$ over a point $z^0 \in Z$ is the curve whose equation is the polynomial obtained.

by substituting z_ν^0 for z_ν. The 3 partial derivatives F_x, F_y, F_z are polynomials in x, y, z, $\{z_\nu\}$ linear in z_ν and homogeneous of degree $d-1$ in x, y, z. They define some subvariety of $\mathbb{P}^2 \times Z$. Let S be the variety $\{F_1 = F_2 = F_3 = 0\}$. Note that $S \subset \mathcal{C}$ (by Euler).

The fiber $\mathcal{C}^0$ over a point z^0 of Z is smooth if and only if $\mathcal{C}^0$ doesn't meet S.

We can construct $\Sigma = \pi(S)$ the image of S via a polynomial $\mathbb{P}^2 \times Z \to Z$. Later we'll prove that the image of the projection of any Zariski closed subvariety of $\mathbb{P}^2 \times Z$ to Z is also Zariski closed.

So the set Σ is closed in the affine space Z. But Σ is not all of Z (because the Fermat curve is smooth). So $\Sigma \subset Z$ is a proper closed subvariety. So the set of z^0 for which $\mathcal{C}^0$ is smooth is a Zariski open subset of $\mathbb{A}^N$. $\square$

4 Friday, February 11, 2011

Last time, we gave a proof that almost every plane curve of degree d is smooth parameter space $\mathbb{A}^N : N = \binom{d+2}{2}$.

Another proof, continuing from the middle of the last one:

Proof. The dimension of S (as defined last time) is $N + 2 - 3 = N - 1$ (the three from $F_x = F_y = F_z = 0$). So $\pi(S)$ is at most $N-1$ dimensional, and so it's $\overline{\pi(S)}$. But $\dim Z = N$, so $\overline{\pi(S)} \neq Z$. $\square$

Some words about topology $\mathbb{A}^N = \mathbb{C}^N$ is a complex variety of dimension N. As a real manifold, it's dimension is $2N$. In the complex topology, you can have closed disks, e.g. $|z| \leq 1$ (has positive measure). In the Zariski topology, closed subsets have no measure. e.g., in $\mathbb{C}$, the only closed subsets are finite point sets. In $\mathbb{C}^2$, $V(ax+by+c)$ has no measure (it's a complex plane (dimension 1)).

Proposition. *A smooth curve C of degree 3 in $\mathbb{P}^2$ contains exactly 9 flex points.*

Proof. Let f be a cubic defining C. The second partial derivatives of f are linear, so the determinant of the Hessian is a cubic polynomial which defines the Hessian curve H.

Theorem (Bézout's theorem)**.** *A curve of degree m in $\mathbb{P}^2$ intersects a curve of degree n in exactly mn points.*

By this theorem (not yet proved), the two cubics C and H intersect in 9 points. One can show that the multiplicities are one, and that C and H don't have a factor in common. Thus, we get exactly 9 flexes. □

Example. $y^2 = x^3 - x$
homogenization gives $y^2 z = x^3 - xz^2$
Then $\boxed{f = x^3 - xz^2 - y^2 z}$.
The Hessian matrix is

$$\begin{bmatrix} 6x & 0 & -2z \\ 0 & -2z & -2y \\ -2z & -2y & -2x \end{bmatrix}$$

Then $H(f) = 8(3zx^2 - 3y^2x + z^3)$.
The flexes: You can eliminate z from $f = H(f) = 0$. Then you get a homogeneous polynomial in x and y. You can solve for x/y, let y be 1, and then plug back in and solve for z. In this example, we get that one of the flex points is at $(x : y : z) = (0 : 1 : 0)$.

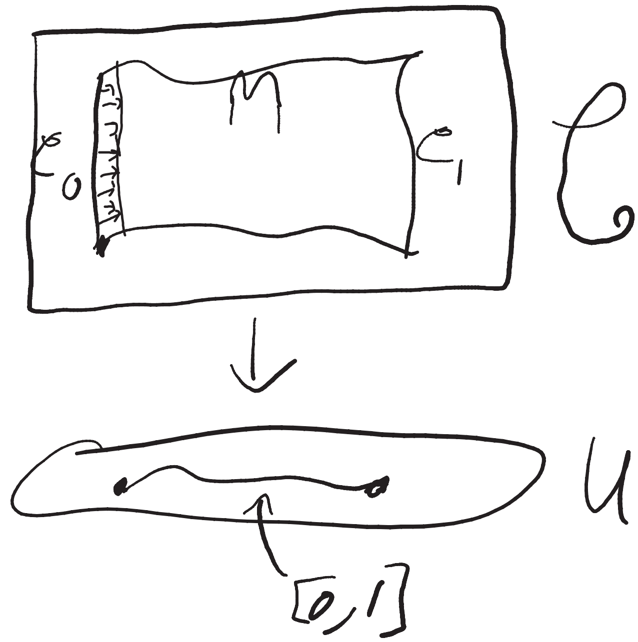
Genus and Euler characteristic

Goal: Want to understand the topological structure of smooth plane curves.

It's useful to put them in a family. Notation as above. Let $U = Z - \Sigma = Z - \pi(S)$. This is the parameter space for smooth plane curves of degree d. The smooth plane curves are the fibers of the projection $\mathcal{C} \subset \mathbb{P}^2 \times U$ to U.

Proposition. *All the smooth curves of degree d are homeomorphic to each other (as real manifolds of dimension 2).*

Proof. The problem set shows that U is path-connected (in the complex topology). Connect the two points in U (which correspond to curves in $\mathbb{P}^2 \times U$) by a path.



We have a function $f : M \to [0,1]$. Define a diffeomorphism by taking the gradient of f, and look at the gradient flow. This tells us how to identify the fibers. □

Corollary. *Smooth plane curves are orientable, connected surfaces.*

Proof. Orientability is simple. To orient a smooth surface, we must give a continuously varying orientation to the tangent planes. But tangent plane is a $\mathbb{C}$-vector space (of dimension one, $\sum f_i(p)v_i = U$). So multiplying any tangent vector by i defines a counterclockwise rotation by $90°$, which orients the tangent plane.

We'll do connected next time. □

5 Monday, February 14, 2011

5.1 Plane curves

monomials $m_1, \dots, m_N$, coefficients $z_1, \dots, z_N$

$$\begin{aligned} Z &= \text{the space of all homogeneous polynomials of degree } d \text{ in } x,\ y, \text{ and } z \\ &= \text{affine space with coordinates } z_\nu \end{aligned}$$

(We have $f(x,y,z) = z_1 x^d + z_2 x^{d-1} + \cdots$)

U = open subset in Z corresponding to smooth plane curves

$\mathcal{C} \subset \mathbb{P}^2 \times Z$

$$\begin{tikzcd} \mathcal{C} \arrow[rrd] & \subset & \mathbb{P}^2 \times Z \arrow[d] \\ & & Z \end{tikzcd} \qquad \begin{tikzcd} \mathcal{C}|_U = \mathcal{C}_U \arrow[rrd] & \subset & \mathbb{P}^2 \times U \arrow[d] \\ & & U \end{tikzcd}$$

Proposition. *Smooth plane curves are orientable and connected surfaces, and compact.*

Proof. Oreintability was done last time.

To check connectedness, we just need to check one smooth curve of degree d is connected. $\mathcal{C} : \{x^d + y^d - z^d = 0\}$.

Look at the line $y = z$. On U_2, taking $z = 1$ we have $x^d + y^d = 1$. Since $y = z$, $y = 1$, and then $x^d = 0$. Since this is a root of order d, C meets this line in only one point. This means that it's connected. (WHY?) $\square$

Given a connected, orientable, compact surface, it's topologically characterized by $g =$ the genus $=$ the # of holes.

Definition. The *Euler characteristic* of C is $2 - 2g$.

The Euler characteristic can be computed used an arbitrary triangulation, and then $E = \#\text{ vertices} - \#\text{ edges} + \#\text{ faces}$.

A sphere is, topologically, a tetrahedron, we have that the Euler characteristic is $4 - 6 + 4 = 2$. We can do a similar thing for a torus.

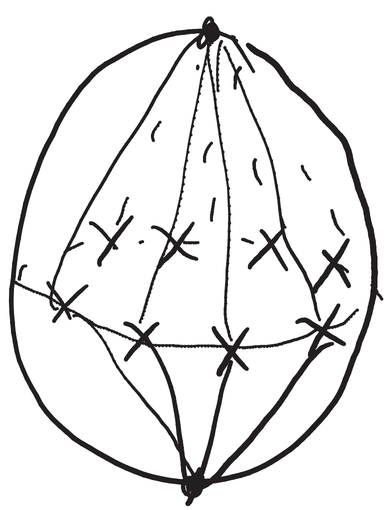
What is the Euler characteristic and genus of a smooth plane curve of degree d?

Let's represent a smooth plane curve as a branched cover of $\mathbb{P}^1$.

Method I Start with the Fermat curve, and do an explicit calculation. $C : \{x^d + y^d - z^d = 0\}$ Taking $z = 1$, $U_2 \simeq \mathbb{A}^2 \simeq \mathbb{C}^2$. Then we have $x^d + y^d = 1$. Drop y by projection. Fix a value x_0 for x. Then the line $y = x_0$ intersects the curve in $\leq d$ points. Typically, we get d values for y.

Case I $x_0^d \neq 1$. Solve $y^d = 1 - x_0^d$. There are d solution s (if y is a solution, then so is $yr^{2\pi ij/d}$ for $0 \leq j \leq d$)

Case II $x_0^d = 1$. Solve $y^d = 0$. The only solution is $y = 0$. Now we look at x_0. Triangulate $\mathbb{P}^1$, which is a sphere, as follows. There are d values for x_0, $x_i^d = 1$, $x_i = e^{2\pi ij/d}$.



These points distribute themselves along the equator of $\mathbb{P}^1$. Adding points at the poles, there are $2 + d$ vertices, $d + d + d = 3d$ edges, and $2d$ faces, which gives us 2. This is what happens "downstairs" (in the projected curve onto $X = \mathbb{P}^1$).

Upstairs, there is an induced triangulation:

- vertices: $d + d + d = 3d$
- edges: $3d^2$
- faces: $2d^2$

Then the Euler characteristic is $E = 3d - 3d^2 + 2d^2 = 3d - d^2 = d(3 - d)$. Then $g = \frac{1}{2}(d-1)(d-2)$.

Method II Let C be a smooth curve of degree d. Assume the coefficient of z^d is not zero. Divide by that coefficient, giving $f(x, y, z) = z^d - a_1(x, y)z^{d-1} + \cdots \pm a_d(x, y)$. Homogeneous polynomial $\implies$ $a_i(x, y)$ is degree i in x and y. Then drop z by projection onto $\mathbb{P}^1(x, y)$.

Fix (x_0, y_0). View $z^d - a_1(x_0, y_0)z^{d-1} + \cdots \pm a_d(x_0, y_0) = 0$ as a polynomial of degree d in z. Typically this has d roots, but for some values of (x, y), there are $d - 1$ roots.

There is a polynomial Δ, discriminant, degree $d(d-1)$ in x and y. $\Delta = 0$ iff there are less than d roots. (The discriminant for a quadratic is $b^2 - 4ac$. It tells you whether or not the polynomial has double roots.) (Note, if the discriminant has only simple roots, then the claim above (that there are only d or $d - 1$ roots at any point) is intuitively/geometrically true.)

Triangulate $X = \mathbb{P}^1$ by putting vertices at these $d(d - 1)$ points. For $\mathbb{P}^1$, the Euler characteristic is 2. Pulling the triangulation up, the Euler characteristic is approximately $2d$ (everything gets multiplied by d). However, we placed the vertices at the $d(d - 2)$ points where there are $d - 1$ roots. Then the Euler characteristic is $2d - d(d - 1) = 3d - d^2$.

6 Wednesday, February 16, 2011

7 Friday, February 18, 2011

8 Tuesday, February 22, 2011

Outline:

I. playing with curves in $\mathbb{P}^2$

II. Affine algebraic geometry (structure of spec A)

III. Projective geometry

IV cohomology

---

thm: Nullstellensatz:

Maximal ideals of $\mathbb{C}[x_1, \ldots, x_n] \longleftrightarrow$ points in $\mathbb{A}^n (= \mathbb{C}^n)$

$(a_1, \ldots, a_n) \in \mathbb{A}^n$ max ideal $\mathfrak{m}_a$ = kernel of hom. $\mathbb{C}[x] \to \mathbb{C}$, $f(x) \rightsquigarrow f(a)$

$\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$

$A = \mathbb{C}[x]/I$ quotient of $\mathbb{C}[x]$, say $I = (f_1, \ldots, f_n)$, $f_i \in \mathbb{C}[x]$

Cor: Then $\operatorname{Spec} A = \{\text{max ideals}\} \underset{\text{bij}}{\longleftrightarrow} V(I)$ = locus of zeros

Why? B/c

thm <u>Correspondence Thm</u>: ideals of $A \underset{\text{bij}}{\longleftrightarrow}$ ideals of $\mathbb{C}[x]$ that contain I

max ideals $\underset{\text{bij}}{\longleftrightarrow}$ max ideals containing I

If A is any finitely generated $\mathbb{C}$-algebra (ring that contains $\mathbb{C}$),

then $A \overset{\text{isomorphic}}{\approx} \mathbb{C}[x]/I$

$\underset{\text{Max ideals}}{\operatorname{Spec} A} \longleftrightarrow V(I)$ variety in $\mathbb{A}^n$

If $A \xrightarrow{\varphi} B \xrightarrow{\pi} \mathbb{C}$ get $\pi\varphi$

Topics for Affine Algebraic Geometry

- localization (adjoining inverses)
- integral extensions (B a finite A-module)
- prime ideals
- dimension

Ex: $A = \mathbb{C}[x]$. spec $A = \mathbb{A}^n$

$B = A[g^{-1}]$ g some non-zero polynomial

Spec B?

$B = A[y]/(yg-1) = \mathbb{C}[x, y]/(yg(x)-1)$ (x = $x_1, \dots, x_n$)

Spec B = locus $yg = 1$ in $\mathbb{A}^{n+1}_{x,y}$

Say $(x^0, y^0) \in$ Spec B. So $y g(x^0) = 1$.

Given x^0, can solve uniquely for y^0, provided $g(x^0) \neq 0$

If $g(x^0) = 0$, no solution.

Cor: spec $\mathbb{C}[x][g^{-1}] \xleftrightarrow{bij}$ points of $\mathbb{A}^n_x$ where $g(x) \neq 0$

9 Wednesday, February 23, 2011

Hilbert Basis Theorem

A ring A is Noetherian if the ideals are finitely generated.

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

Corollary. $\mathbb{C}[x_1, \dots, x_n]$ *is Noetherian*
Any finite-type (finitely generated as an algebra (everything is a polynomial in finitely many things)) $\mathbb{C}$-algebra is Noetherian. ($A \cong \mathbb{C}[x]/I$)

Equivalent conditions on A:

1. A is noetherian (ideals are finitely generated)
2. Every infinite increasing family $I_1 \subset I_2 \subset \cdots$ of ideals becomes constant eventually

($I_1 < I_2 < \cdots$ chain is finite)

3. Every non-empty set S of ideals contains maximal elements ($\exists I \in S$ such that $I \not\subset J$ for any $J \in S$, $J \neq I$)

Corollary. *If A is noetherian,I is an ideal of A, and $I < A$, then I is contained in a maximal ideal. (The maximal ideal is a maximum element in the set of ideals $< A$.)*

Corollary. *If A contains no maximal ideal, then A is the zero ring.*
$\operatorname{Spec} A \neq \emptyset \iff A = \{0\}$

Adjoining inverses to $A = \mathbb{C}[x]$ ($x = x_1, \ldots, x_n$), $B = A[g^{-1}] = \mathbb{C}[x, y]/(yg - 1)$. Then $\operatorname{Spec} A = \mathbb{A}^n$, and $\operatorname{Spec} B \approx \mathbb{A}^n - V(g)$.

Theorem (Strong Nullstellensatz)**.** *Let I be an ideal of $\mathbb{C}[x]$, $g \in \mathbb{C}[x]$. Suppose g vanishes identically on $V(I)$. Then $g^N \in I$ for some $N \gg 0$.*

Proof. Idea: Find a ring with no maximal ideal. It is therefore the zero ring. Play with this fact.

Say $I = (f_1, \ldots, f_r)$, $f_i \in \mathbb{C}[x]$ ($x = x_1, \ldots, x_n$). Let's inspect the locus of zeros in $\mathbb{A}^{n+1}_{x,y}$, $V = V(f_1, \ldots, f_r; yg - 1)$.

If $(x^0, y^0) \in V$, then $x^0 \in V(I) = V(f_1, \ldots, f_r) \subset \mathbb{A}^n_x$. Therefore $g(x^0) = 0$ (by hypothesis). Then there is no y^0 such that $y^0 g(x_0) = 1$.

Therefore, $V = \emptyset$.

We also have that $V = \operatorname{Spec} \mathbb{C}[x, y]/(f_1, \ldots, f_r, yg - 1)$. Then $\mathbb{C}[x, y]/(f, yg - 1) = \{0\}$. Therefore, $(g, yg - 1)$ is the unit ideal in $\mathbb{C}[x, y]$. This means that we can write 1 as a polynomial combination of f and $yg - 1$. Say

$$1 = p_1(x, y) f_1(x) + \cdots + f_r(x, y) f_r(x) + q(x, y)(yg - 1).$$

Now work in the ring $B = \mathbb{C}[x][g^{-1}] = \mathbb{C}[x, y]/(yg - 1)$. In B $yg - 1 = 0$ and $y = g^{-1}$. Then

$$1 = p_1(x, g^{-1}) f_1(x) + \cdots + p_r(x, g^{-1}) f_r(x) + 0.$$

Multiply by g^N to clear denominators. Then, since $g = g(x)$,

$$g^N = \tilde{p}_1(x) f_1(x) + \cdots + \tilde{p}_r(x) f_r(x).$$

Therefore, $g^N \in I$. □

Note: If $I \subset J$ are ideals in $\mathbb{C}[x]$, then $V(I) \supseteq V(J)$. But $V(x_1) = V(x_1^2)$.

Let I be an ideal. Then $\operatorname{rad} I =$ radical of $I = \{g \mid g^n \in I,\ \text{some } n > 0\}$.

Theorem.

$$V(I) \supset V(J) \iff I \subset \operatorname{rad} J$$

$$V(I) = V(J) \iff \operatorname{rad} I = \operatorname{rad} J$$

Proof. Say $V(I) \supset V(J)$. Take $g \in I$. Then $g = 0$ on $V(J)$. Then $g^N \in J$ for some N by the strong Nullstellensatz, and so $g \in \operatorname{rad} J$.

The other direction is left as an exercise. □

Definition. Let X be a topological space. Then a closed subset C is *irreducible* if you can't write $C = C_1 \cup C_2$ where C_i closed, $C_i < C$.

A a finite type algebra is noetherian, satisfies the ascending chain condition on ideals. Then $\operatorname{Spec} A$ has the descending chain condition on ideals.
Prime ideals: Given a polynomial ring R: (equivalent conditions)

- R/P is a domain
- $P < R$, $ab \in P \implies a \in P$ or $b \in P$
- A, B ideals of R, $AB \subset P \implies A \subset P$ or $B \subset P$. (Recall that the product ideal $AB = \{\text{finite sums } \sum a_i b_i \,|\, a_i \in A, b_i \in B\}$.)

Proof. (2) $\implies$ (3)
Say $AB \subset P$, but $A \subset P$.
$\exists a \in A$, $a \notin P$.
$AB \subset P \implies B \subset P$
$\forall b \in B$, $ab \in P$, $\therefore b \in P$, so $B \subset P$. □

10 Friday, February 25, 2011

Recall:
If I is an ideal of A, then $\operatorname{rad} I = \{x \in A \,|\, x^n \in I, \text{ some } n > 0\}$
$V(I) = V(\operatorname{rad} I)$
$V(I) \supset V(J) \iff I \subset \operatorname{rad} J$
irreducible closed set C: $C \neq C_1 \cup C_2$, $C_i < C$.

Proposition. *I an ideal, $V(I)$ irreducible iff $\operatorname{rad} I$ is prime ideal*

Theorem. *Let A be a finite-type noetherian ring, I an ideal. Then $\operatorname{rad} I$ is the intersection of a finite number of prime ideals $\operatorname{rad} I = P_1 \cap \cdots \cap P_k$. Then we can organize $P_i \not\subset P_j$ for $i \neq j$. Then we have that $V(I) = V(P_1) \cup \cdots \cup V(P_k)$; $V(I)$ is a finite union of irreducible closed sets.*

$\operatorname{Spec} A = \{\text{maximal ideals}\}$
$V(I) = \{\mathfrak{M} \text{ that contains } I\}$

I an ideal. Then $\bar{A} = A/I$.

$$\begin{aligned} A &\to \bar{A} \\ I &\rightsquigarrow (\bar{0}) \\ \operatorname{rad} I \quad & \operatorname{rad}(\bar{0}) \\ &= \textit{nilradical} \\ &= \{x \,|\, x^n = 0\} \end{aligned}$$

The following are equivalent:

- $\operatorname{rad} I = P_1 \cap \cdots \cap P_k$
- $\operatorname{rad}(\bar{0}) = \bar{P}_1 \cap \cdots \cap \bar{P}_k$

  (in $\bar{A}$) also prime ideals

Proof. Suppose the theorem is false for some A and some I. Let $S = \{$ideals J of A such that $\operatorname{rad} J$ is not a finite intersection of prime ideals$\}$. By hypothesis, $S \neq \emptyset$. Then there exists a maximal element I in S. Then $\operatorname{rad} I$ not a finite intersection of prime ideals, but every larger ideal is a finite intersection of prime ideals.
Note:

- $I = \operatorname{rad} I$
- I is not a prime ideal

Then there exist ideals K, L, $K \not\subset I$, $L \not\subset I$, but $KL \subset I$. Replace K by $K + I$, L by $L + I$. Then we have

$$(K + I)(L + I) \subset KL + KI + IL + II \subset I.$$

(so it's ok to do these replacements).

Now $K, L > I$. Replace K and L with their radicals.

$$(\operatorname{rad} K)(\operatorname{rad} L) \subset \operatorname{rad}(KL) \subset \operatorname{rad} I = I$$

(so it's ok to these replacements.)

We have

$$\operatorname{rad} K = P_1 \cap \cdots \cap P_r$$
$$\operatorname{rad} L = Q_1 \cap \cdots \cap Q_s$$

...

We made a mistake somewhere. (Supposed to replace I by a zero ideal?) The version on the web is probably correct. Let's skip this for now. □

Finite Group Action

Let B be a finite type domain, G the finite group of automorphisms of B. Let $A = B^G$.

Theorem.
- *A is a finite type domain*
- *G operates on* $\operatorname{Spec} B = Y$
- *Y maps to* $\operatorname{Spec} A = X$. *$Y \to X$ is surjective, and the fibers are the G-orbits in Y*

Example. $B = \mathbb{C}[x, y]$, $\sigma(x) = -x$, $\sigma(y) = -y$. Then $\langle\sigma\rangle$ is a group of order 2.

The invariant functions are $u = x^2$, $v = y^2$, and $w = xy$. It's not hard to see that every invariant function can be written as some combination of these.

$A = B^G = \mathbb{C}[u, v, w]/(w^2 - uv)$

Then $\operatorname{Spec} A = X =$ locus of $w^2 = uv$ in $\mathbb{A}^3_{u,v,w}$. This is a double cone in 3-space.

Proof. A finite type domain:

Take $\beta \in B$, orbit $\{b_1 = \beta, \ldots, b_r\}$. Let $p(x) = (x - b_1) \cdots (x - b_r) = x^r - s_1(b)x^{r-1} + \cdots \pm s_r(b)$. We have that β is a root of $p(x)$. Since the $s_i(b)$ are symmetric functions, $s_i(b) \in B^G = A$.

Since B is a finite type domain, say B is generated as an algebra by $\beta_1, \ldots, \beta_m$. Then each β_i is a root of the polynomial, coefficients in A.

Let $A_0 = \mathbb{C}$-algebra generated by these roots. Then A_0 is a finite-type domain contained in B. Every element in B is a polynomial in $\beta_1, \ldots, \beta_m$.

If a polynomial with β_i as a root has degree d_i, then we only need monomials in β_i with degree $\leq d_i$. There are only a finite number of monomials in β_i of degree $\leq d_i$. Then B is spanned as an A_0-module by these monomials. Thus, B is a finite A_0-module.

$A_0 \subset A \subset B$. Since A_0 is a finite-type domain, A_0 is noetherian. B is a finite-type A_0-module. A is a submodule. Therefore, A is a finite-type A_0 module. Thus, A is a finite-type algebra. $\square$

11 Monday, February 28, 2011

B finite type, G operator(?)

$A = B^G$

Showed A finite type

$Y = \operatorname{Spec} B$

$X = \operatorname{Spec} A$

$X \leftrightarrow \{G \text{ orbits in } Y\}$

$G \times B \to B$

$\sigma, b \rightsquigarrow \sigma(b)$

(left) $\sigma\tau(b)$: first τ, then σ

Then G operates on the *right* on Y.

$q \in Y$, σ sends $q \to q^\sigma$

$q^{\sigma\tau}$: first σ, then τ

View

$$\begin{aligned}
y &\leftrightarrow \{\text{homomorphisms } B \to \mathbb{C}\} \\
q &\leftrightarrow \pi_q : B \to \mathbb{C} \\
&\leftrightarrow \{\text{max ideals of } B\} \\
q &\leftrightarrow m_q
\end{aligned}$$

Operation on Y:

$$\begin{tikzcd}
B \arrow[r, "\sigma"] \arrow[dr, "\pi\circ\sigma"'] & B \arrow[d, "\pi"] \\
& \mathbb{C}
\end{tikzcd}$$

$\pi_q \circ \sigma(b) = \pi_q(\sigma b)$

Define q^σ = that point such that $\pi_{q^\sigma} = \pi_q \circ \sigma$.

Operation on max ideals:

$\mathfrak{M}_{q^\sigma} = \sigma^{-1}\mathfrak{M}_q$

$Y \to X$?
For any $p \in X$,

$$\begin{tikzcd} B \arrow[r, "\pi \circ p"] & \mathbb{C} \\ A \arrow[u, hook] \arrow[ur, dashed, "\pi_p"'] & \end{tikzcd}$$

$Y \to X$ sends $q \rightsquigarrow r$

$$\begin{tikzcd} B \arrow[r, "\sigma"'] \arrow[rr, bend left, "\pi"] & B \arrow[r, "\pi_q"'] & \mathbb{C} \arrow[d, equal] \\ A \arrow[u, hook] \arrow[r, "\mathrm{id}"] \arrow[rr, bend right, "\pi_p"'] & A \arrow[u, hook] \arrow[r, "\pi_p"] & \mathbb{C} \end{tikzcd}$$

Therefore, G-orbits in Y map to points of X.

We want to show that different orbits $\{q_1, \dots, q_r\} \neq \{q'_1, \dots, q'_s\}$ in Y map to different points p, p' in X.

Proof. *Plan*: Find an element $a \in A$ such that $a = 0$ on orbit $\{q_i\}$, $\pi_q(a) = 0$, $a \neq 0$ on orbit $\{q'_j\}$. Then $\pi_{q'_j}(a) \neq 0$. This would give us that $a \in \mathfrak{M}_{q_i}$ (same as $\in \mathfrak{M}_p$) and $a \notin \mathfrak{M}_{q'_j}$ (same as $\notin \mathfrak{M}_{p'}$).

In B, choose $b \in \mathfrak{M}_{q_1}$ (then) such that $b \notin \mathfrak{M}_{q'_j}$ for all $j = 1, \dots, s$. (Note: $b(q) := \pi_q(b)$.)

(Diversion: Suppose $B = \mathbb{C}[x_1, \dots, x_n]/(f_1, \dots, f_k)$. b represented by the polynomial $p(x_1, \dots, x_n)$. $\operatorname{Spec} B \approx V(f_1, \dots, f_k)$ in $\mathbb{C}^n$.
$\operatorname{Spec} B = $ (max ideals) $=$ (homomorphisms $B \to \mathbb{C}$) $= (V(I)$ if $B = \mathbb{C}[x]/I))$)

We can do this. (Think about choosing (hyper-?)planes that do not pass through finite sets of points.)

Let $a = \prod_{\sigma \in G} \sigma(b)$. a is invariant. $a = 0$ on q_1 because b divides a in B (since some $\sigma \in G$ is the identity). Therefore $a = 0$ on the orbit (q_1). $a \neq 0$ on q'_1.

$\sigma(b)$ evaluated at q'_1 is $\pi_{q'_1}(\sigma b) = \pi_{{q'}_1^\sigma}(b) = b$ evaluated at ${q'}_1^\sigma$.

Therefore, $a \neq 0$ on the orbit. □

11.1 Localization

Note: we always assume that the rings are domains and assume (whenever possible) that they're finite type algebras.

Definition. A *multiplicative system* S in a domain A is a subset of A satisfying

- $1 \in S$
- $0 \notin S$
- if $s, t \in S$, then $st \in S$

Definition. The elements of S serve as denominators in the *ring of fractions*

$$A_S := \left\{ \frac{a}{s} \,\middle|\, s \in S, a \in A \right\} \Big/ \sim$$

where $\frac{a}{s} \sim \frac{b}{t}$ if $at = bs$

$$A \hookrightarrow A_S$$
$$a \rightsquigarrow a/1$$

Example. $S = \{1, s, s^2, \ldots\}$, $s \neq 0$. $A_S = A[s^{-1}] = A[y]/(sy-1)$

Example. $S = A - \{0\}$, $A_S =$ fraction field

Example. P a prime ideal of A, $S = A - P = \{s \mid s \notin P\}$. Then $s \notin P$, $t \notin P \implies st \notin P$. Then A_S is the *localization of* A *at* P. This is (perversely) denoted A_P.

If $A \subset B$ a subring, then we can relate ideals of A and B:
Extended ideal: I^e

I ideal of A

$IB =$ ideal of B generated by $\{I\}$

The elements are

$$\sum_{\text{finite}} x_i b_i \qquad , \; x_i \in I, \; b_i \in B$$

Contracted ideal: J^c: For J an ideal of B, $(J \cap A) =$ ideal of A

$(I^e)^c \supset I$

$(J^c)^e \subset J$

For $A \subset B = A_S$:

$I^e = IA_s = \{x/s \mid x \in I, \; s \in S\} / \sim$

$J^c = J \cap A$. If $y/s \in J$, then $y \in J \cap A = J^c$. Therefore, $y/s \in (J^c)^e$. Thus, $J \subset (J^c)^e$, so $J = (J^c)^e$.

Corollary. *If A noetherian, then A_S noetherian*

Proof. Take an increasing sequence $J_1 \subset J_2 \subset \cdots$ of ideals in A_S. Let $I_\nu = J_\nu \cap A$. Then $I_1 \subset I_2 \subset \cdots$. Since A is noetherian, this is eventually constant. Therefore $I_\nu^e = (J_\nu^c)^e$ eventually constant. Thus A_S is noetherian. □

12 Wednesday, March 2, 2011

S a multiplicative system

$1 \in S$

$0 \in S$

$S_1, S_2 \in S \implies S_1 S_2 \in S$.

Ring of fractions A_S localized ring

$A \hookrightarrow A_S$

$(J^c)^e = J$

$(A \cap J)A_S$

Localizing prime ideal (s...?)
I ideal of A, $I \cap S \neq \emptyset \implies I^e =$ unit ideal of A_S

Proposition. *P prime ideal of A. $P \cap S \neq \emptyset$. Then*

- $(P^e)^c = P$
- *P^e ($= P_S$) is a prime ideal of A_S*

$P^e = PA_S = \left\{s^{-1}x \,\middle|\, x \in P\right\}$

Proof. For any ideal P, $(P^e)^c \supset P$.

We want to show $\subset$. Let $z \in (P^e)^c$. Then $z = s^{-1}x$ for some $x \in P$, and $z \in A$. Then $sz = ss^{-1}x = x \in P$. Since P is prime, and $s \notin P$, $z \in P$, and so $(P^e)^c \subset P$.

Now we show that P^e is prime:
We have that $z_1 z_2 \in P^e$ for $z_i \in A_S$. Then $z_1 = s_1^{-1}a_1$, $z_2 = s_2^{-1}a_2$. Then $z_1 z_2 = (s_1 s_2)^{-1}(a_1 a_2) \in P^e$. Therefore $(s_1 s_2)(z_1 z_2) = a_1 a_2 \in P^e$. Since $a_1 a_2 \in A$, this is also in $(P^e)^c = P$. Since $a_1 a_2 \in P$ and P prime, either $a_1 \in P$ or $a_2 \in P$, $s_1^{-1}a_1 \in P^e$ or $s_2^{-1}a_2 \in P^e$.[2] □

$$P \operatorname{Spec} A_S \longleftrightarrow \text{subset of } P \operatorname{Spec} A = \{P \,|\, P \cap S \neq \emptyset\}$$

Back to the case where P is a prime ideal of A and $S = A - P = \{s \in A \,|\, s \notin P\}$.
Write A_P for A_S. If I is an ideal of A, $I_P = I_S$ extended ideal.

Proposition. *P_P is a maximal ideal of A_P and it is the only maximal ideal of A_P.*

Lemma. *For a ring R, the following are equivalent:*

(1) R has a unique maximal ideal $\mathfrak{M}$

(2) The elements of R that are not invertible form an ideal

Proof. (2) $\implies$ (1) Suppose that the non-units form an ideal I. Then R/I is a field because every element is the residue of a unit, and therefore invertible. Thus I is a maximal ideal. Since any other element is a unit, we cannot include any other element without turning the ideal into the entire ring. Thus, this is maximal.

(1) $\implies$ (2) Suppose there exists a unique maximal ideal $\mathfrak{M}$. Let $u \in R$. Then $(u) = R$ if and only if u is a unit. If u is not a unit, then $(u) < R$, and so $(u) \subset$ some maximal ideal.[3] Then $(u) \subset \mathfrak{M}$. Then $\mathfrak{M}$ contains all the non-invertible elements, and so the non-invertible elements of R form an ideal (in particular $\mathfrak{M}$).

□

Proposition above. $s^{-1}a \in A_P$, $s \notin P$.
If $a \in P$, then $s^{-1}a \in P_P$. If $a \notin P$, then $s^{-1}a$ is invertible, and so $a^{-1}s \in A_S$. □

[2] Sorry if this proof is unclear. I was trailing behind Prof. Artin, and so wasn't understanding the proof well.
[3] If R is not noetherian, this requires Zorn's Lemma/The Axiom of Choice.

Definition. A (noetherian) ring R is *local* if it has a unique maximal ideal $\mathfrak{M}$. (Note that $R/\mathfrak{M}$ is a field.)

Example. $A = \mathbb{C}[x, y]$. The prime ideals are

- (0)
- $(f(x, y))$ for f irreducible
- maximal ideal $\mathfrak{M}_{(a,b)} = (x - a, y - b) \longleftrightarrow (a, b) \in \mathbb{C}^2$

  $A_{(0)}$: fraction field $\mathbb{C}(x, y)$ of $\mathbb{C}[x, y]$

  $A_{\mathfrak{M}_{(a,b)}}$: a local ring. The prime ideals $\operatorname{PSpec} A_{\mathfrak{M}} = \{P \mid P \cap S \neq \emptyset\} = \{P \mid P \subset \mathfrak{M}\} = \begin{cases} (0) \\ P = (f) \mid f(a, b) = 0 \\ \mathfrak{M}_{(a,b)} \end{cases}$

Lemma. *Suppose I is an ideal of the ring A and M is a finite A-module such that $M = IM$. Then there exists a $z \in I$ such that $(1 - z)M = 0$.*

Proof. Say $(x_1, \ldots, x_r$ generate M. We can write x_i as a combination of $\{x_1, \ldots, x_r\}$ with coefficients in I:

$$\begin{aligned} x_i &= \sum_j p_{ij} x_j & p_{ij} &\in I \\ X &= PX & P &\text{ matrix } (p_{ij}) \\ (\mathbb{I} - P)X &= 0 \\ Q(\mathbb{I} - P) &= \delta\mathbb{I} \end{aligned}$$

where Q is the cofactor matrix for $\mathbb{I} - P$ with entries in A, and $\delta = \det(\mathbb{I} - P)$.

$$\begin{aligned} Q(\mathbb{I} - P)X &= 0 \\ \therefore \delta X &= 0 \\ \mathbb{I} - P &= \begin{pmatrix} 1 - p_{11} & \cdots & \\ & \ddots & \\ & & 1 - p_{nn} \end{pmatrix} \\ \delta &= 1 - z \end{aligned}$$

Since the $p_{ij} \in I$, we have $z \in I$. Then $(1 - z)X = 0$, so $(1 - z)$ kills M. $\square$

Lemma (Nakayama Lemma)**.** *Let A be a local ring with a maximal ideal $\mathfrak{M}$, and let M be a finite A-module. If $M = \mathfrak{M}M$, then $M = 0$.*

Proof. Take $z \in \mathfrak{M}$. We have a z with $(1 - z)M = 0$. Since $1 - z \notin \mathfrak{M}$, $1 - z$ is invertible, and so $M = 0$ (since we can multiply by $(1 - z)^{-1}$). $\square$

13 Friday, March 4, 2011

Integral Extensions

$A \subset B$ domains

Definition. $b \in B$ is *integral over A* if it's a root of a monic polynomial.
$f(x) = x^n - a_1 x^{n-1} + \cdots \pm a_r$ coefficients in A

Proposition. *The following are equivalent:*

(1) b is integral over A

(2) $A[b]$ is a finite A-module

(3) There exists an $A[b]$-module M which:

- *(i) is faithful[4] as an $A[b]$-module*
- *(ii) is a finite A-module*

Proof.

(1) $\implies$ (2) Clear

(2) $\implies$ (3) Clear

(3) $\implies$ (1) Take the generators for M as an A-module, $(v_1, \dots, v_n)$. Then $bv_i = \sum a_{ij} v_j$ for $a_{ij} \in A$. We can write this as

$$(b\mathbb{I} - A)V = 0 \qquad V = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Let C be the coefficient matrix of $(b\mathbb{I} - A)$. Then $C(b\mathbb{I} - A) = \det(b\mathbb{I} - A)\mathbb{I}$. Let $\delta := \det(b\mathbb{I} - A)$. Then $\delta V = 0$. Since M is faithful, $\delta = 0$.) Expanding δ gives $\delta = b^n - (\operatorname{tr} A)b^{n-1} + \cdots \pm \det A$ is a monic polynomial for b. The coefficients are in A, so $A[b]$ is integral.

□

Proposition. *Let A be noetherian.*

- *If B is generated as an A-algebra by elements integral over A, then every element of B is integral over A.*
- *If B is generated over A by a finite number of integral elements, then B is a finite A-module. (e.g., B integral over A and a finite type $\mathbb{C}$-algebra.)*

Proof. Take $z \in B$. Then $z \in A[b_1, \dots, b_k]$ for b_i integral. $A[b_1, \dots, b_k]$ is a finite A-module. Therefore $A[z]$ is contained in a finite module, so it itself is finite. □

[4] A module is faithful if for any $z \in A[b]$, $z \neq 0$, $zM \neq 0$.

Proposition (Noether Normalization). *Let K be a field, and let A be a finite-type K-algebra and a domain. There exist $y_1, \ldots, y_d \in A$ algebraically independent*[5]*, and A is a finite module over $K[y_1, \ldots, y_d]$.* [6]

$$\begin{tikzcd} A & \operatorname{Spec} A \arrow[d] \\ \mathbb{C}[y_1, \ldots, y_d] \arrow[u, hook] & \mathbb{A}^d \end{tikzcd}$$

Proof. Given A generated by $x_1, \ldots, x_n$ (some finite set). Independent on n.(???) If $x_1, \ldots, x_n$ dependent, there exists a polynomial relation $f(x_1, \ldots, x_n) = 0$ of degree d. Let $h(x)$ be the degree d part of f. Then $h(0, 0, 0, \ldots, 1) =$ coefficient of x_n^d in h and in f. If the coefficient of $x_n^d \neq 0$, then $f(x)$ looks like $cx_n^d + g_{n-1}(x_1, \ldots, x_{n-1}^{d-1} + \cdots + g_0(x_1, \ldots, x_{n-1})$. If $c \neq 0$, this is a monic polynomial of which x_n is a root, and its coefficients are in the ring $K[x_1, \ldots, x_{n-1}]$. Therefore, x_n is integral over $K[x_1, \ldots, x_{n-1}]$. By induction, we get a tower of integral extensions.

If $c = 0$, then make a change of variables $x_i \mapsto x_i + u_i x_n$ (for $i < n$), $x_n \mapsto u_n x_n$. Now the coefficient of x_n^d will be $h(x_1 + u_1 x_n, \ldots, x_{n-1} + u_{n-1} x_{n-1}, u_n x_n)|_{x_1 = \cdots = x_{n-1} = 0,\ x_n = 1} = h(u_1, \ldots, u_n)$. This is non-zero for most choices of u_i.[7] □

Corollary (A version of Nullstellensatz). *Let K be a field, B a finite-type K-algebra that is also a field. Then B is a finite K-module.*

(It follows, without much trouble, from this that if $K = \mathbb{C}$, $B = \mathbb{C}$, too; if B is a finite field extension of $\mathbb{C}$, then $B = \mathbb{C}$.

Proof. Take $b \in B$. $\mathbb{C}[b]$ is a finite $\mathbb{C}$-module. Therefore, b is a root of an irreducible polynomial with coefficients in $\mathbb{C}$. Therefore, it is a root of a linear polynomial over $\mathbb{C}$, so $b \in \mathbb{C}$. □)

Proof. Noether Normalization says B a finite module over polynomial ring $A = K[y_1, \ldots, y_d]$. If $d = 0$, then we're done. If $d > 0$, then $y_1 \in A, B$, so $\frac{1}{y_1} \in B$. Thus B is a field. But $\frac{1}{y_1}$ is not integral over $K[y_1, \ldots, y_d]$. □

If A is a domain with fraction field K, then A is *integrally closed* in K if every element of K which is integral over A is an element of A.

Example. $A = \mathbb{C}[x, y]/(y^2 - x^3)$. This is not integrally closed: Let $z = \frac{y}{x}$.
Then $z^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x$.
$z^3 = \frac{y^3}{x^3} = \frac{x^3 y}{x^3} = y$.
z is a root of the monic polynomial $z^2 - x$, and of $z^3 - y$.

Theorem. *Let A be a finite-type algebra and a domain, and let K be the fraction field of A. Then the* integral closure *of A in K, the set of integral elements, is a finite A-module.*

Preview:
Given an A-module M, then $M^* := \hom_A(M, A)$ is also an A-module.

If $M \subset N$, then $M^* \supset N^*$ (in good situations).

[5] There are no polynomial relations among them.
[6] I'm still confused by this statement.
[7] For fields with finite characteristic, you'll have to make a non-linear change of variables.

14 Monday, March 7, 2011

15 Wednesday, March 9, 2011

Theorem. *Let A be a finite type algebra and a domain, and let K be the field of fractions. Then the integral closure of A is a finite extension L/K, and is a finite A-module.*

Proof. Had the trace pairing $L \times L \to K$, $x, y \rightsquigarrow tr(xy)$. It's non-degenerate because:
$yx \neq 0$, put $y = x^{-1}$
$\langle x, y\rangle = t(1) = [L : K]$
Reduce to the case of A integrally closed by Noether Normalization.
$k[y] \subset A$, A a finite $k[y]$-module
$k[y] \subset K \subset L$.
Replace A by $k[y]$.
$\therefore$, we may assume that A is integrally closed. Then if $\alpha \in L$ is integral over A, $tr(\alpha) \in A$.

Therefore, if B is any subring of L, and a finite A-module, then all elements are integral over A. Therefore, $B \times B \to A$, $x, y \rightsquigarrow \langle x, y\rangle = tr(xy)$.

We want to show that there is a maximal such B. Then B is the integral closure in L.

Start with one, B_0, big enough so that it contains a basis for L/K. (We can do this because for any $\gamma \in L$, γ is algebraic in K; $\gamma^n - a_1\gamma^{n-1} + \cdots \pm a_n = 0$ with $a_i \in K$. Since K is the field of fractions, we can clear denominators, getting $d\gamma^n - a_1'\gamma^{n-1} + \cdots \pm a_n' = 0$, with $d, a_i' \in A$. Then $d\gamma$ is integral over A; multiply everything by d^{n-1}.) Denote the basis by $(v_1, \ldots, v_n)$, $v_i \in B_0$, $n = [L : K]$.

Investigate some larger algebra (which is still a finite A-module) B. Then $A \subset B_0 \subset B$.

$$\begin{aligned} &B \times B \to A \\ &\quad \beta, v_i \rightsquigarrow b_i := \langle \beta, v_i\rangle \in A \end{aligned}$$

map

$$\begin{aligned} &\beta \rightsquigarrow (b_1, \ldots, b_n) \in A^n \\ &B \xrightarrow{\Phi} A^n \end{aligned}$$

This is A-linear (homomorphism of A-modules)

Φ is injective: $\Phi(\beta) = 0$ means $\langle \beta, v_i\rangle = 0$ for all i. Since $\{v_i\}$ is a basis for L/K, $\langle \beta, y\rangle = 0$ for all $y \in L$. Thus, $\beta = 0$.

Then we can identify B with $\Phi(B)$ as a submodule of A^n. Since A is noetherian, submodules have the ascending chain condition. □

(DIGRESSION ABOUT GALOIS GROUPS AND G-ORIBTS NOT INCLUDED)
Let $A \subset B$ be a domain, A finite-type and integrally closed, and B a finite A-module.
What about prime ideals in A and B?

extended ideal of $P \subset A$ is $P^e = PB$ ideal of B

contracted ideal of $Q \subset B$ is $Q^c = A \cap Q$ ideal of A

Fact (General Fact)**.** If Q is a prime ideal of B, then Q^c is a prime ideal of A.

$$\begin{tikzcd} A \arrow[rr, hook] \arrow[dr, "\text{kernel } Q^c"'] & & B \arrow[dl, "\text{kernel } Q"] \\ & B/Q \text{a domain } (Q \text{ prime}) & \end{tikzcd}$$

The image is a domain, so Q^c is a prime ideal.

Back to the case above,

$$\begin{array}{lll} A \hookrightarrow & B & \\ P' & Q' & \text{we mean } P' = A \cap Q' \\ P & Q & P = A \cap Q, \quad Q' \supset Q \end{array}$$

Fact 15.1 (Lying Over)**.** Given P a prime ideal of A, there exists a A prime ideal of B, with $A \cap Q = P$. (The map $\operatorname{PSpec} B \to \operatorname{PSpec} A$ is injective.)

Fact 15.2 (Going Up)**.** Given

$$\begin{array}{ll} A \hookrightarrow & B \\ P' & Q' \longleftarrow \text{exists} \\ P & Q \end{array}$$

Fact 15.3 (Going Down)**.** If A is integrally closed, then given

$$\begin{array}{ll} A \hookrightarrow & B \\ P' & Q' \\ P & Q \longleftarrow \text{exists} \end{array}$$

Lemma. *Given*

$$\begin{array}{ll} A \hookrightarrow & B \\ P' & Q' \\ P & Q \end{array}$$

If $P' = P$, then $Q' = Q$.

Proof. Case 1: $P = 0$. We need to show that if $P' = 0$, then $Q' = 0$. Take $\alpha \in Q' \subset B$. Then α is integral over A (because it's in B?). We have $\alpha^r - a_1\alpha^{r-1} + \cdots \pm a_r = 0$. Since $a_r \in Q'$ and $a_r \in A$, we have $a_r \in P' = \{0\}$. Thus $a_r = 0$. If $\alpha \neq 0$, then cancel α from the relation, and repeat until $r = 1$. Then $\alpha^1 - a_1 = 0$. Since $a_1 \in A$ and $a_1 \in Q'$, $a_1 \in P'$. Then $a_1 = 0$ and $\alpha = 0$, which is a contradiction.

Case 2: (general case). Go to $\bar{A} = A/P \subset \bar{B} = B/Q$.

$$\begin{array}{ll} \bar{A} \hookrightarrow & \bar{B} \\ \bar{P}' & \bar{Q}' \\ (0) & (0) \end{array}$$

Then case 1 says that $\bar{P}' = (0)$ implies that $\bar{Q}' = (0)$. Then $\bar{P}' = (0) \iff P' = P$ and $\bar{Q}' = (0) \iff Q' = Q$.

$\square$

Lemma. *If Q is a maximal ideal of B, then $Q^c = P$ is maximal in A.*

Proof. Q is maximal in B if and only if $\bar{B} = B/Q$ is a field. Then $A/P = \bar{A} \subset \bar{B}$ is a field. Then $\bar{B}$ is a finite $\bar{A}$-module.

Lemma. *If $A \subset B$ is a field and B is a finite A-module, then A is a field.*

Proof. Take a non-zero element in $\alpha \in A$ (we want to show that it's invertible). Then α is invertible in B. Since B is a finite A-module, so $u = \alpha^{-1}$ is integral over A. Then $u^r - a_1 u^{r-1} + \cdots \pm a_r = 0$ with $a_i \in A$. Multiply by α^{r-1}. Then we get $u - a_1 + a_2\alpha - \cdots \pm a_r\alpha^r = 0$, with all of these elements of A. □

(To be finished next time?) □

16 Friday, March 11, 2011

Finite group action on an integrally closed finite-type domain B, $A = B^G$, (has the?) invariants

$\max A \leftrightarrow G$-orbit in $\max B$

A is finite type and integrally closed

B is a finite A-module

Definition. A is *normal* if it's integrally closed in the field of fractions of A (i.e., it's own fraction field).

Theorem. *Let G be a finite group that acts on an integrally closed finite-type domain B, $A = B^G$. Then*

- $\operatorname{PSpec} A \leftrightarrow (\operatorname{PSpec} B)/G$
- *This preserves inclusions. More formally, If $P \leftrightarrow$ orbit $\{Q_j\}$ and $P' \leftrightarrow$ orbit $\{Q'_i\}$, then $P \subset P'$ if and only if $\forall j \exists i$ such that $Q_j \subset Q'_i$.*

  We have $Q \rightsquigarrow A \cap Q$, $\operatorname{Spec} B \to \operatorname{Spec} A$

Lemma. *Let $Q_1, \ldots, Q_m$; $Q'_1, \ldots, Q'_n$ be prime ideals of B. Suppose $Q_j \not\subset$ any Q'_i, $j = 1, \ldots, m$, $i = 1, \ldots, n$. Then there exists $\alpha \in B$, $\alpha \in Q_1, \ldots, Q_m$, $\alpha \notin Q'_1, \ldots, Q'_n$.*

Proof. Plan: Solve for a single Q_j. Find $\alpha_j \in Q_j$, $\notin Q'_1, \ldots, Q'_n$. Then the product $(\alpha_1 \cdots \alpha_m)$ works; $\alpha_1 \cdots \alpha_m \in Q'_i \implies$ some $\alpha_j \in Q'_i$. This would be a contradiction.

Take $Q_1 = Q$, $Q'_1, \ldots, Q'_n$, $\alpha \in Q$, $\notin Q'_i$.

$\alpha = \beta_i \in Q$, $\notin Q'_i$, $i = 1, \ldots$. $\beta_1 \cdots \beta_n \in Q$. …(Proof not included) □

Proof. (of theorem)
In C:

$$\begin{tikzcd} B \arrow[r, "\sigma"] & B \\ A \arrow[u, hook] \arrow[r, "\text{id}"] & A \end{tikzcd}$$

Since Q is a prime ideal of B and $P = A \cap Q$, we have that σQ is a prime ideal of B and $P = A \cap \sigma Q$. Then an orbit of Q corresponds to one point in $\operatorname{PSpec} A$. By the lying over theorem, $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective. Therefore $(\operatorname{Spec} B)/G \to \operatorname{Spec} A$ is also surjective.

Injective: $\{Q_1, \ldots, Q_m\}$, $\{Q'_1, \ldots, Q'_n\}$ distinct orbits. $A \cap Q_j = P$, $A \cap Q'_i = P'$, show $P \neq P'$.

Claim. *We can't have $Q_i \subset Q'_j$ for some i, j and also $Q'_k \subset Q_\ell$ for some k, ℓ.*

Proof. We can renumber, $i = j = 1$. $Q'_k \subset Q_\ell \implies \sigma Q'_k \subset \sigma Q_\ell$. We may then assume that $\ell = 1$; since σ runs through the whole orbit, we can choose an appropriate σ.

Then $Q_1 \subset Q'_1$, $Q'_k \subset Q_1$. Then $Q'_k \subset Q_1 \subset Q'_1$. Then $Q'_k \subset Q'_1$. Thus $k = 1$, because $Q'_k = \sigma Q'_1$ for some σ (and permutations can't take sets to proper subsets of themselves). Then $Q'_1 \subset Q_1 \subset Q'_1$, so $Q_1 = Q'_1$. This is a contradiction, since orbits are disjoint. Thus, we may suppose that $Q_j \not\subset Q'_i$ for any i, j. $\square$

There exists an $\alpha \in Q_1 \cap \cdots \cap Q_m$, $\notin Q'_i$. Take $\gamma = \prod_\sigma \sigma\alpha$, $\gamma \in Q_j$, $\notin Q'_i$, and $\gamma \in A$. Thus, $\gamma \in P$, $\notin P'$, so $P \neq P'$.

The proof of the second point is skipped (See notes that Prof. Artin posted). $\square$

Let B be a finite A-module for a normal A.

$$\begin{tikzcd}
A \arrow[r, hook] & B \\
P' \arrow[u, hook] & Q' \arrow[u, hook] \\
P \arrow[u, hook] & Q \arrow[u, hook]
\end{tikzcd}$$

$P' = A \cap Q'$, $P = A \cap Q$

Theorem (Going Up)**.** *In the diagram above, given P, P', Q, there exists a Q'.*

Theorem (Going Down)**.** *In the diagram above, given P, P', Q', there exists a Q.*

Proof. Let K be the fraction field of A and L be the fraction field of B.

Case 1: L/K is Galois, has Galois group G(?). B is normal.

σ acts on B: The elements of B are integral of A. If β is integral, so is $\sigma\beta$. Then, since B is normal, B is the integral closure of A in L. Thus, $\sigma\beta \in B$.

$A = B^G$. (We know that B is a finite B^G-module.): $A \subset B^G$ and A is normal. Since B is integral over A, B^G is integral over A, so $A = B^G$.

Then the theorem follows from the previous theorem.

Case 2: (general case): L/G not Galois, and/or B not normal: Put $L \subset F$ a Galois extension of K with Galois group G. Let C be the integral closure of A in F. This is a finite A-module. Then G operates on C. Then $A = C^G$ (by the same reasoning as in case 1).

$$\begin{tikzcd}
A \arrow[r, hook] & B \arrow[r, hook] & C \\
P' & Q' & R' \\
P & & R
\end{tikzcd}$$

By lying over, there exists a prime ideal R', $B \cap R' = Q'$. Case 1 says that there exists an R. Then $A \cap R = P$. Put $Q = B \cap R$.

$\square$

17 Monday, March 14, 2011

Definition. The *Krull dimension* of a ring A is the length of the longest chain of prime ideals $P_0 < P_1 < \cdots < P_d$.

In a dimension zero ring, every prime ideal is maximal and also minimal. Therefore, there are a finite number of prime/minimal ideals.

If A is a domain of dimension 1, then (0) is a prime ideal and all the other prime ideals are maximal.

Definition. The *codimension* of a prime ideal P is the length of the longest chain $P_0 < P_1 < \cdots < P_d = P$.

If A is a domain, then P has codimension 0 if $P = (0)$, and P has codimension 1 if it's not zero and there does not exist P' with $(0) < P' < P$.

Theorem (Knull's Principal Ideal Theorem)**.** *Let A be a domain. Let $x \in A$ with $x \neq 0$, and let P be a prime ideal. If $x \in P$ and P is is the minimal prime ideal containing x, then P has codimension 1.*

($P/x \in P \longleftrightarrow$ prime ideals $\bar{B}$ of $\bar{A} = A/(x)$.

Therefore, the Krull dimension of $\bar{A}$ is the Krull dimension of A, - 1.)

Discrete valuations

Generalize order of vanishing of $f(x)$ at $x = a$. For $f(x_1, \ldots, x_n)$, talking about order of vanishing at $(a_1, \ldots, a_n)$ doesn't make much sense. But we can define the order of vanishing along a subvariety of codimension 1.

Let K be a field. A discrete valuation(?) v is a group homomorphism $K^\times \xrightarrow{v} \mathbb{Z}^+$ such that $v(\alpha+\beta) \geq \min\{v(\alpha), v(\beta)\}$ and $v(\alpha\beta) = v(\alpha) + v(\beta)$. "$v(\alpha) = k$ means α vanishes to order k (has a zero of order k)". $v(\alpha) = -k$, "α has a *pole* of order k.

A homomorphism $K^\times \xrightarrow{v} \Gamma^+$ (an ordered group with $+$) is also a valuation. This is unimportant!

Definition. The (discrete) valuation ring R associated to a discrete valuation v is $R = \{\alpha \in K^\times \,|\, v(\alpha) \geq 0\} \cup \{0\}$ ("no pole").

Remorse: You always have to add $\{0\}$, or define $v(0) = \infty$ (but this is artificial)

Definition. A *fractional ideal* is a non-zero finitely generated submodule of K.

Properties of DVR (discrete valuation ring):

- subring of K and local domain (local ring that's a domain, ring with one maximal ideal)
- $\mathfrak{M} = \{\alpha \in K \,|\, v(\alpha) > 0\} \cup \{0\}$
- $\mathfrak{M}$ is a principle ideal generated by any $t \in K^\times$ with $v(t) = 1$.
- ideals of R are $\mathfrak{M}^k = (t^k)$ and zero ideal $(K \geq 0)$ $(\mathfrak{M}^k = \{\alpha \,|\, v(\alpha) \geq k\})$
- R is normal
- The fractional ideals of R are (t^k), $k \in \mathbb{Z}$.

Write $(t^k) = \mathfrak{M}^k$ also for $k < 0$. Then $\mathfrak{M}^{k+l} = \mathfrak{M}^k\mathfrak{M}^l$, $k, l \in \mathbb{Z}$.

Lemma. $v(1) = 0$, $v(-1) = 0$, $v(a^{-1}) = -v(a)$

Take $\alpha \in K^\times$, $v(\alpha) = k$. Also, $v(t^k) = k$. $v(t^{-k}\alpha) = 0$. Then $t^{-k}\alpha = u$ is a unit in R, so $\alpha = ut^k$.

Proposition. *The following are equivalent conditions on a local noetherian domain A:*

(1) A is a DVR

(2) A is normal and has dimension 1

(3) A is normal and there exists an $x \in A$ such that $\mathfrak{M}$ is the minimal prime ideal containing x

(4) $\mathfrak{M}$ is principle

Proof.

(1) $\implies$ (2) We're not doing it (it follows from the properties of a DVR)

(2) $\implies$ (3) There exist only two prime ideals in A: $(0) \neq \mathfrak{M}$. $x \in \mathfrak{M}$, $x \neq 0$ also works.

(3) $\implies$ (4) Take x as in (3). Then $\bar{A} = A/(x)$ has only one prime ideal $\bar{\mathfrak{M}}$ both maximal and minimal. The intersection of the minimal prime ideals is the nilradical of $\bar{A}$. Therefore $\bar{\mathfrak{M}}$ is the nilradical. Therefore, $\bar{\mathfrak{M}}^N = (0)$, $N \gg 0$. Thus $\mathfrak{M}^N < (x)$.

Choose r such that $\mathfrak{M}^{r-1} \not\subset (x)$ but $\mathfrak{M}^r \subset (x)$. Take $y \in \mathfrak{M}^{r-1}$, $y \notin (x)$. We want to show that $w = x/y$ generates $\mathfrak{M}$. Let $z = w^{-1} = y/x$. Since $y \notin (x)$, $z \notin A$. Now consider $z\mathfrak{M}$.

Lemma. *Let A be a normal noetherian domain, I a non-zero ideal, $\gamma \in K = \mathrm{Fract}(A)$. If $\gamma I \subset I$, then $\gamma \in A$.*

Proof. $\gamma I \subset I$ means that I is an $A[\gamma]$-module. I (γI?) is faithful, and a finite A-module. Then γ is integral over A, and thus an element of A. □

$z\mathfrak{M} = \frac{y}{x}\mathfrak{M} \subset \frac{\mathfrak{M}^r}{x} \subset A$. We stop here (continue next time).

□

18 Wednesday, March 16, 2011

19 Friday, March 18, 2011

GK-dimension A (finite-type algebra, domain)
Choose V a one-dimensional subspace which

- generates A
- contains 1 (that is, $1 \in V$)

V^n is the span of products of length n of elements of V.
$V \subset V^2 \subset \cdots$
$\bigcup V^n = A$
The generating function g is $g(n) = \dim V^n$
GK-$\dim V = d$ means that $g(n) \leq cn^d$ and $\not\leq cn^{d-\epsilon}$

Lemma.

- *This is independent of the choice of V.*
- $\operatorname{gk}(k[x_1, \ldots, x_n]) = d$ *(?)*

  Take $V =$ polynomials of degree ≤ 1. Then $\dim V^n = \binom{n+d}{d}$.
  Trivial fact: If $\bar{A} = A/I$ then $\operatorname{gk}(\bar{A}) \leq \operatorname{gk}(A)$.

Lemma. *Suppose $A \subset B$, B a finite A-module. Then* $\operatorname{gk}(B) = \operatorname{gk}(A)$.

Proof. Choose a finite dimensional subspace U of B that generates B as an A-module. Then $U^2 \subset B = AU$. Now choose a (one-dimensional) generating space V for A large enough so that $U^2 \subset VU$. Take $W = V + U$ to generate B as an algebra. Then we have

$$W^n = V^n + V^{n-1}U + V^{n-2}U^2 + \cdots + U^n.$$

Since $V^{n-2}U^2 \subset V^{n-1}U$, by induction, $U^n \subset V^{n-1}U$. Then $W^n \subset V^n + V^{n-1}U$. Since $W = V + U$, we also have that $V^n \subset W^n$.

Let $h(n) = \dim W^n$. Then

$$g(n) \leq h(n) \leq g(n) + rg(n-1) \leq (r+1)g(n)$$

with $r = \dim U$. □

Let K be the fraction field of A. Define $\operatorname{tr\,deg} A = \operatorname{tr\,deg} K/\mathbb{C}$.[8]

Corollary. $\operatorname{gk}(A) = \operatorname{tr\,deg} K/\mathbb{C}$.

Proof. Noether Normalization says that A is a finite module over $k[x_1, \ldots, x_k]$, $k[x] \subset A$. Then $k = \operatorname{tr\,deg} K/\mathbb{C}$. □

Corollaries:

- $\operatorname{gk}(A) \in \mathbb{N}$
- $s \neq 0, s \in A \implies \operatorname{gk}(A_s) = \operatorname{gk}(A)$ (same field of fractions, therefore same degree)

Let A be a finite type domain, P a prime ideal of codimension 1 ($(0) < P$ and no primes in between).

Proposition. $\operatorname{gk}(A/P) = \operatorname{gk}(A) - 1$ *or* $\operatorname{tr\,deg} A/P = \operatorname{tr\,deg} A - 1$

Proof. Replace A by its normalization A', a finite A-module.

$$\begin{array}{ccc} A & \hookrightarrow & B \\ P & Q & \text{also codim } 1\ (P = A \cap Q) \\ (0) & & (0) \end{array}$$

$$\operatorname{tr\,deg} A = \operatorname{tr\,deg} B$$

B/Q is a finite A/P-module, $\operatorname{tr\,deg} B/Q = \operatorname{tr\,deg} A/P$.

[8] tr deg is the transcendence degree.

Assume A is normal. Then the local ring A_P is a DVR (discrete valuation ring). The maximal ideal $P_P = tA_P$ for some $t \in A_P$. It's a principal ideal. t is a fraction $s^{-1}a$, $s \notin P$.

Localize: Replace A by A_s, P by P_s. (It still has codimension 1 because the prime ideals in the localized ring are subsets of the original prime ideals.(?)) Now $t \in A$, but it might not generate P. Say $P = (u_1, \ldots, u_r)$. In the local ring, $t \mid u_i$. Then, we can get a common denominator, so $u_i = t(s_1^{-1}b_i)$, $b_i \in A$, $s \notin P$. Now replace A by A_{s_1}. Now t generates P.

We've reduced to the case that $P = tA$ (A normal). Extend t to a transcendence basis[9] for the fraction field of A, $(t, x_1, \ldots, x_k)$, $x_i \in A$.

Now $k[t, x_1, \ldots, x_k] \subset A$ and the elements of A are algebraic over $k[t, x]$. Look at $k[x_1, \ldots, x_k] \to \bar{A} = A/P = A/tA$. What's the kernel? $f(x) \rightsquigarrow 0$ means that $f(x) = t\alpha$, $\alpha \in A$.

... We seem to not have a proof. (To be posted online. We'll assume the proposition is true.) □

Theorem. $\mathrm{gk}(A) = \operatorname{tr\,deg} A =$ *Krull* $\dim A$. *More precisely, every maximal chin of prime ideals* $(0) < P_1 < P_2 < \cdots < P_d$ *has length* $d = \mathrm{gk}(A) = \operatorname{tr\,deg} A$.

Proof. We have already done $\mathrm{gk}(A) = \operatorname{tr\,deg} A$.

We induct on d. We prove the statement: If a maximal chain has length d, then $d = \mathrm{gk}(A)$. Look at $\bar{A} = A/P_1$. A maximal chain in $\bar{A}$ is $(0) = \bar{P}_1 < \bar{P}_2 < \cdots < \bar{P}_d$ (by the correspondence theorem) has length $d-1$. Then the Krull dimension of $\bar{A}$ is $\mathrm{gk}(A) = d - 1$. Therefore, $\mathrm{gk}(A) = d$.

(Where is Krull's Theorem?!) □

20 Monday, March 28, 2011

21 Friday, April 1, 2011

A (Zariski) closed set in $\mathbb{P}^n$ (projective variety) is the set of zeros of some homogeneous polynomial.

Segre embedding $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N$, $(x_i), (y_j) \rightsquigarrow (u_{ij})$, $u_{ij} = x_i y_j$, $N = (m+1)(n+1) - 1$. The defining equations are $u_{ij}u_{kl} = u_{il}i_{kj}$. This mapping is bijective.

If $X \subset \mathbb{P}^N$ is a closed set, then the Zariski topology on X is the induced topology: a closed subset C of X is a subset that is closed in $\mathbb{P}$ or $C = Y \cap X$ with Y closed in $\mathbb{P}$.

So we can get the Zariski topology on $\mathbb{P}^m \times \mathbb{P}^n$ ($= X$). What are the closed subsets? If C is closed in $\mathbb{P}^m \times \mathbb{P}^n$, then it is the intersection of the set of zeros of some homogeneous polynomials $f(u)$ with $\mathbb{P}^m \times P^n$. We may replace $f(u)$ with $f(x_i y_j)$ homogeneous in x and in y, with the same degree.

Proposition. *Closed subsets of* $\mathbb{P}^m \times \mathbb{P}^n$ *are zeros of some polynomials* $f(x, y)$ *homogeneous in* x *and homogeneous in* y*, not necessarily of the same degree.*

Proof. Say C is the set of zeros of $f(x, y)$ homogeneous of degree r in x and homogeneous of degree s in y. Say $r \le s$. Look at the zeros of $x_i^{s-r} f(x, y)$ (homogeneous of degree s in x), $i = 0, 1, \ldots, m$. □

Corollary.

$$\mathbb{P}^n \xrightarrow{\Delta} \mathbb{P}^n \times \mathbb{P}^n$$
$$(x) \rightsquigarrow (x), (x)$$

The diagonal is a closed subset.

[9] *Transcendence basis*: Maximally algebraically independent set in the fraction field.

Proof. Label the coordinates $(x_i), (x_i') \in \mathbb{P}^n \times P^n$. We want $x_i = x_i'$. The (homogeneous polynomial) equation that defines this is $x_i x_j' - x_j x_i'$, so this is a closed set. □

What is the product topology on $\mathbb{P}^n \times \mathbb{P}^n$? The closed subsets are given by the basis $(C \times \mathbb{P}) \cap (\mathbb{P} \times C')$. This is bad, because we don't get curves.

Definition. A space X is *Hausdorff* if, for any p, q distinct points, there exist disjoint open subsets U, V with $p \in U$ and $q \in V$.

Proposition. *A space X is Hausdorff if and only if the diagonal is closed in $X \times X$ in the product topology.*

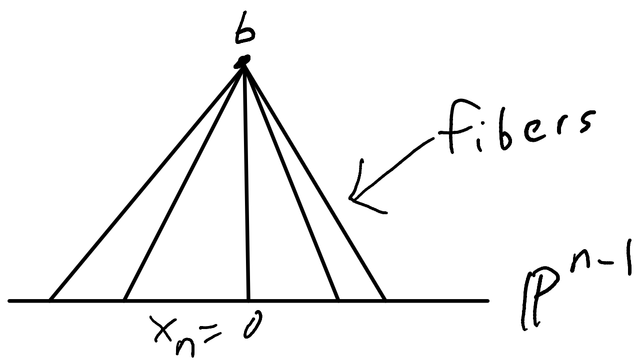
Proof. Exercise □

Theorem (Hrushovski-Zilber Theorem). *A "*Zariski topology*" is a set X and, for all products $X \times X \times \cdots \times X$, a collection of "closed" subsets of X, satisfying the following axioms:*

- *Compatible with projection and inclusions of $X \times X \times \cdots \times p \times \cdots \times X$.*
- *Noetherian (descending chain condition)*
- *dimension 1*

Then there exists an algebraically closed field K and an algebraic curve X over K in the Zariski topology.[10]

Projection: $\mathbb{P}^n \xrightarrow{\pi} \mathbb{P}^{n-1}$, $(x_0, \dots, x_n) \rightsquigarrow (x_0, \dots, x_{n-1})$. This is undefined at the "center of the projection," $(0, 0, 0, \dots, 0, 1) = p$.



In $\mathbb{P}^n \times P^{n-1}$ let Γ be the graph. $\bar{\Gamma}$ is the Zariski closure of Γ. Label the points $(x_i), (y_i) \in \mathbb{P}^n \times \mathbb{P}^{n-1}$. Γ: $x_i = y_i$ for $i = 0, \dots, n-1$. The equations $x_i y_j - x_j y_i$ for $i, j = 0, \dots, n-1$ define a Zariski closed set of $\bar{\Gamma}$. Look where $x_0 \neq 0$: Take $x_0 = 1$. Then $y_j = x_j y_0$. We can't have $y_0 = 0$: Take $y_0 = 1$. Then $y_j = x_j$, $j = 0, \dots, n-1$, x_n arbitrary. Only the center $p = (0, 0, \dots, 0, 1)$ escapes. In this case, all the equations are trivial. So no conditions on (y). The result is

$$\bar{\Gamma} = \{(x, \pi(x)) \,|\, x \neq p\} \cup \{(p, y) \,|\, y \text{ arbitrary}\}.$$

[10]See `http://en.wikipedia.org/wiki/Zariski_geometry`. Wikipedia references the paper "Hrushovski, Ehud; Zilber, Boris (1996). "Zariski Geometries". *Journal of the American Mathematical Society* 9 (01): 1–56. doi:10.1090/S0894-0347-96-00180-4." (`http://www.ams.org/jams/1996-9-01/S0894-0347-96-00180-4/S0894-0347-96-00180-4.pdf`) This is a theorem of model theory, which Wikipedia defines as "the study of (classes of) mathematical structures such as groups, fields, graphs or even models of set theory using tools from mathematical logic."

Grassmannians: $G(r, n)$ is the r-dimensional subspace of $\mathbb{C}^n$. For example, $\mathbb{P}^n = G(1, n+1)$. Look at $G(2, 4) =$ 2-dimensional subspaces of $\mathbb{C}^4$ or lines in $\mathbb{P}^3$.

V a vector space of dimension 4, basis (v_1, v_2, v_3, v_4). There is an exterior algebra $\bigwedge V$. The rule is $vw = -wv$. (Or $v \wedge w = -w \wedge v$.) Then $vv = 0$.
$\bigwedge^2 V$ has a basis $v_i v_j$ for $i = j$ dimension $\binom{4}{2} = 6$
$\bigwedge^3 V$ has a basis $v_i v_j v_k$ for $i < j < k$ dimension 4
$\bigwedge^4 V$ has a basis $v_1 v_2 v_3 v_4$ dimension 1
$\bigwedge^k V = 0$ for $k > 4$

Proposition. *The following are equivalent:*

- *There is a subspace $W \subset V$ of dimension 2*
- *Vectors w in $\bigwedge^2 V$, non-zero, and decomposable into $w = uv$, $u, v \in V$.*
- *w in $\bigwedge^2 V$, $ww = 0$ /(scalar)*
- *Let $w = \sum\limits_{i<j} a_{ij} v_i v_j \longleftrightarrow (a_{ij})$ in $\mathbb{P}^5$. Then $a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0$.*

Proof. Partial sketch of one of the implications: $w = \sum a_{ij} u_i v_j$, $ww = \sum\limits_{i<j, k<l} a_{ij} a_{kl} v_i v_j v_k v_l$. Plug in all the possible values. □

22 Monday, April 4, 2011

Review

$G(2, 4) =$ planes in V^4, lines in $\mathbb{P}^3$
V has basis u_1, u_2, u_3, u_4
$\bigwedge^2 V$ has basis $u_1 u_2, \ldots, u_3 u_4$ ($u_i u_j$ for $i < j$), dimension 6
W a 2-dimensional subspace of V with basis (u, v), then $w = uv \in \bigwedge^2 V$ determines W, and conversely W determines uv. $(u', v') = (u, v)P \implies u'v' = uv \det P$.

Proposition. *2-dimensional subspaces of V correspond to decomposable non-zero elements $w = uv$ of $\bigwedge^2 V$ modulo scalars.*
$w \in \bigwedge^2 V$ is decomposable $\iff ww = 0 \iff w = \sum\limits_{i<j} a_{ij} u_i u_j$ and $a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0$.
The grassmanian $G(2, 4)$ is the locus of $a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0$ in $\mathbb{P}^5_{(a_{ij})}$ (dimension = 4).

We can show directly that $\dim G(2, 4) = 4$. W is a subspace of dimension 2 with basis (u, v). $(u = \sum a_i u_i$, $v = \sum b_i u_i)$

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix} \overset{\text{choose a basis}}{\longrightarrow} \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}$$

Ask for the locus of pairs (p, ℓ) with $p \in \mathbb{P}^3$ a point and ℓ a line in $\mathbb{P}^3$. Let $\Gamma = \text{locus}\, \{(p, \ell) \,|\, p \in \ell\}$. We can embed this in $\mathbb{P}^3 \times \mathbb{G}$ where $\mathbb{G} = G(2, 4)$.

$$\Gamma \subset \mathbb{P}^3 \times G \subset \mathbb{P}^3 \times \mathbb{P}^5 \overset{\text{Segre}}{\to} \mathbb{P}^{23}$$

We can show that Γ is a closed set in $\mathbb{P}^3 \times \mathbb{G} \subset \mathbb{P}^3 \times \mathbb{P}^5$ (with coordinates $(x) \times (a_{ij})$): Find defining homogeneous equations. We need $f(x, a)$ homogeneous in x_i and in a_{ij}. If ℓ is the line through

(u, v) (basis for $W \longleftrightarrow \ell$), $(x) \in \ell$ means $x = su + tv$ for some s, t. This is the case if and only if x, u, v dependent, which is true if and only if $xuv = 0$ in $\bigwedge^3 V$.

$$uv = \sum_{i<j} a_{ij} u_i u_j \longleftrightarrow (a_{ij}) \in \mathbb{P}^5$$

Then $(x) = \sum x_i u_i$ and so $xuv = \sum x_i a_{ijk} u_i u_j u_k$. Expand this and plug in the relation $a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0$.

Surfaces of degree d in $\mathbb{P}^3$

Given as $f = 0$, f homogeneous of degree d in (x_1, x_2, x_3, x_4). The number of monomials of degree d is $\binom{d+3}{d}$.

$$\{\text{surfaces of degree } d\} \longleftrightarrow \mathbb{S} \coloneqq \text{points in } \mathbb{P}^N$$

with $N = \binom{d+3}{d} - 1$.

We ask in $\mathbb{G} \times \mathbb{S}$ for $\Theta \coloneqq \{(\ell, S) \,|\, \ell \subset S\}$.

The following isn't quite right. (Something is wrong with the degree of f?)

We can show that Θ is closed in $\mathbb{G} \times \mathbb{S}$. What are its defining equations? Say ℓ is a line through u, v, and say that S is the surface given by $f = 0$. Then $\ell \subset S \iff f(su + tv) = 0$ for all s, t. Expand $f(su + tv)$:

$$f(su + tv) = s^d f_0(u) + s^{d-1} t f_1(u, v) + \cdots + st^{d-1} f_{d-1}(u, v) + t^d f_d(v)$$

Then $f(su + tv) = 0$ for all s, $t \iff f_i(u, v) = 0$ for all i.

Example.

$$f = x_i x_j x_k$$

$$f(su+tv) = s^3 u_i u_j u_k + s^2 t(u_i u_j v_k + u_i v_j u_k + v_i u_j u_k) + st^2(u_i v_j v_k + v_i u_j v_k + v_i v_j u_k) + t^3(v_i v_j v_k)$$

Lemma. *f_i depends only on f, not on u and v.*

That is, if we change basis to $(u', v') = (u, v)P$, the f_i don't change.

Check: We check this for P elementary; say $u = u' + \varepsilon v'$, $v = v'$. Then $f(su + tv) = f(su' + s\varepsilon v' + tv') = f(su' + (s\varepsilon + t)v')$. We can say $t' = s\varepsilon + t$. Then the expansion doesn't change, except for the transformation of $t \mapsto t'$ (which doesn't change the f_i).

The above isn't quite right. (Something is wrong with the degree of f?)

What's the dimension of Θ?

Plan: We can carry any line in $\mathbb{P}^3$ to any other line by a change of coordinates.

Take a particular line ℓ_0. Suppose we determine $\dim\{S \,|\, \ell_0 \subset S\} = r$. Then $\dim \Theta = \dim \mathbb{G} + r = r + 4$.

Suppose we take ℓ_0 to be the line $\{(x_1, x_2, 0, 0)\}$. Is $f(x_1, x_2, 0, 0)$ identically zero? When we substitute in, we get a homogeneous polynomial of degree d in x_1, x_2:

$$f(x_1, x_2, 0, 0) = \alpha_0 x_1^d + \alpha_1 x_1^{d-1} x_2 + \cdots + \alpha_d x_2^d$$

The $d + 1$ coefficients of f must then be zero, so $\dim\{S \,|\, \ell_0 \subset S\} = \dim \mathbb{S} - (d + 1)$. So $r = \binom{d+3}{d} - 1 - (d + 1)$. Then $\dim \Theta = \binom{d+3}{d} - d + 2$.

For $d = 1$, $\dim \Theta = 5$. $\dim \mathbb{S} = 3$. We expect the set of lines in a given S to have dimension 2, so this is correct.

For $d = 2$, $\dim \Theta = 10$. $\dim \mathbb{S} = 9$ (10 coefficients, but it's projective space). We expect a particular S to have a 1-dimensional family of lines.

For $d = 3$, $\dim \Theta = 19$. We expect a finite number of liens in a cubic. The number of lines contained in a generic cubic surface is 27.

23 Wednesday, April 6, 2011

Double Planes

Affine case: $A = \mathbb{C}[x, y]$, $\operatorname{Spec} A = \mathbb{A}^2 = X$

$f(x, y) \in A$, square-free (no square factors, non-constant). Let $B = A[w]/(w^2 = f)$, $Y = \operatorname{Spec} B$.

B is a domain, free A-module with basis $(1, w)$.

Automorphism $\sigma : B \to B$, $w \mapsto -w$. $A = B^{\langle\sigma\rangle}$

Lemma. *B is normal.*

Proof. Let $\beta = a+bw$ in $\operatorname{fract}(B)$. It is integral over A, and not in A ($b \neq 0$), irreducible polynomial has coefficients in A. $t^2 - (\beta + \beta')t + \beta\beta'$, $\beta' = \sigma\beta$. Then $\beta + \beta' = 2a \in A$, $\beta\beta' = a^2 - b^2 f$ with $b^2 f \in A$. Since f is square-free, $b \in A$, and so $\beta \in B$. □

General theory says $\operatorname{PSpec} B/\langle\sigma\rangle = \operatorname{PSpec} A$.

Prime ideals of A: (0); (g) prime ideal, g irreducible; $\mathfrak{M}_p$ maximal $\leftrightarrow p \in X$.

What prime ideals of B lie over P?

(0) lies over (0).

Maximal ideals of $B \longleftrightarrow$ points of $Y = \operatorname{Spec} B$

inclusion $A \hookrightarrow B$ gives map $Y \to X$ ($q \rightsquigarrow p$) $\implies$ $\mathfrak{M}_q$ lies over $\mathfrak{M}_p$. (usually 2 points of Y $\rightsquigarrow$ 1 point of X)

Say $P = (g)$, g irreducible in A.

What is a description of Q, the prime ideals lying over P ($A \cap Q = P$)?

Cases:

- P remains prime: $PB = Q$ is a prime ideal
- $f \in P$ (g divides f) Then P ramifies: there exists a unique prime Q of B over P, and $Q^2 = PB$.
- P does not remain prime, and $f \notin P$. Then there exist two primes Q, $Q' = sigmaQ$ over P and $PB = Q \cap Q'$.

(EXPLANATION OF FIRST BULLET NOT INCLUDED)

Second bullet: Say $f \in P$. What is B/PB? It's $A[w]/(w^2 - f, g)$. Let $\bar{A} = A/(g)$. Then we can write B/PB as $\bar{A}[w]/(w^2)$. Then $P \longleftrightarrow (0) \in \bar{A}$, and $PB \longleftrightarrow (0) \in B/PB$. Then w generates the prime ideal of $\bar{B}$, and the quotient is $\bar{A}$. This gives, using the correspondence theorem, a prime ideal Q of B, $Q = (w, g)$.

$Q^2 = (w^2, wg, g^2) = (f, wg, g^2)$. Then $\gcd(f, g^2) = g = uf + vg^2$, so $g \in Q^2$.

Third bullet: $f \notin P$, PB not prime. Choose Q lying over P. Let $Q' = \sigma Q$. Since Q lies over P, so does Q' because σ fixes A. Since PB is not prime, $Q \neq B$.

Lemma. *$Q \cap Q' = PB$*

($Q \neq PB$, $\therefore Q \neq Q'$)

Proof. Take $\beta \in Q \cap Q'$, $\beta = a + bw$. Then $\beta' = \sigma\beta = a - bw$, so $\beta' \in Q \cap Q'$. Note that σ fixes $Q \cap Q'$: $\sigma(Q \cap Q') = \sigma Q \cap \sigma Q' = Q' \cap Q$.

$$\begin{aligned} \beta + \beta' &= 2a \in Q \cap Q' \cap A = P \\ \beta\beta' &= a^2 - b^2 f \in Q \cap Q' \cap A = P \\ &\therefore b^2 f \in P \end{aligned}$$

$f \notin P$, $\therefore b \in P$, $ainP$, $\beta \in PB$. Thus, $PB = Q \cap Q'$. $\square$

Example. $w^2 = f = x^2 + y^2 - 1$, $g = y$

Then $g \nmid f$. So we have $P = (g)$ remains prime.

Take $B/PB \approx \mathbb{C}[x, w]/(w^2 - x^2 + 1)$. This is a domain, so the 0-ideal is prime. Therefore, P remains prime. Take $g = y - 1$. (This divides $y^2 - 1$.)

Then $B/P_2B \approx \mathbb{C}[x, w]/(w^2 - x^2)$, so P_2B does not remain prime.

If we draw a picture, we see that $y = 0$ goes through the middle of the circle, but $y = 1$ is tangent.

Show: If $\Delta = \{f = 0\}$ (branch locus) and $C = \{g = 0\}$ (curve) intersect $\pitchfork$ (intersect transversely; the tangent lines are distinct) at some point p.

Theorem. *C remains prime.*

Proof. Choose coordinates so that $p = (0, 0)$. Then $f = \sum a_{ij} x^i y^j$, $g = \sum b_{ij} x^i y^j$. Δ and C meet at p, so $a_{00} = b_{00} = 0$.

Then $f = a_{10}x + a_{01}y + \cdots$. The tangent line is $a_{10}x + a_{01}y = 0$. We also have $g = b_{10}x + b_{01}y + \cdots$, with tangent line $b_{10}x + b_{01}y = 0$.

Let's make a linear change of coordinates: $f = x + u$, $g = y + u$, u, v have all terms of degree ≥ 2.

Now let's make an analytic change of coordinates. Set $x' = x + u$, $y' = y + v$. Then $\left(\frac{\partial(x', y')}{\partial(x, y)}\right)_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is invertible. The inverse function theorem says that this operator is invertible locally (analytically).

$\mathbb{C}^2_{x,y} \to \mathbb{C}^2_{x',y'}$: replace x, y with x', y'. Then $w^2 = x'$ and $g = y'$. This doesn't split locally. $\square$

(A power series $c_k x^k + c_{k+1} x^{k+1} + \cdots$, $c_k \neq 0$ is a square of a series $\iff$ k is even.)

Projective Double Plane

Start with an affine double plane $w'^2 = F(x', y')$. Say F has degree $d = 2k$.

Make the substitution $\frac{x}{z} = x'$, $\frac{y}{z} = y'$, $\frac{w}{z^k} = w'$. Then $\left(\frac{w}{z^k}\right)^z = F\left(\frac{x}{z}, \frac{y}{z}\right) \to \boxed{w^2 = f(x, y, z)}$ (homogeneous of degree d), a double cover of $\mathbb{P}^2_{xyz}$.

To embed, we need weighted projective space, where x, y, z have weight 1 and w has weight k. In this space, $(w, x, y, z) = (\lambda^k w, \lambda x, \lambda y, \lambda z)$. (Note: "weighted projective spaces are a bit pathological.") A better way to do this is to treat this as a sheaf of algebras over $\mathbb{P}^2_{xyz}$.

24 Friday, April 8, 2011

Category Theory

Definition. A *category* is a collection of objects, together with morphisms (maps) between objects satisfying the following axioms:

- Composition of morphisms is defined.

$$\begin{tikzcd} x \arrow[r, "f"] \arrow[rr, bend right, "f \circ g \text{ is defined}"'] & y \arrow[r, "g"] & z \end{tikzcd}$$

- Associative law: If we have
$$f \xrightarrow{f} y \xrightarrow{g} z \xrightarrow{h} w,$$
then $(h \circ g) \circ f = h \circ (g \circ f)$

- For all objects y, there exists an identity $y \xrightarrow{i_y} y$ such that $g \circ i_y = g$, $i_y \circ f = f$ for all f and g with the appropriate domains and ranges.

Examples of categories include the category of: sets; topological spaces, algebras.

Definition. Let C and D be categories. Then a *functor* F is a map $C \xrightarrow{F} D$ which maps $\mathrm{Obj}(C) \to \mathrm{Obj}(D)$ and maps $\mathrm{Morph}(C) \to \mathrm{Morph}(D)$ and which (1) is compatible with composition and (2) maps identity morphisms to identity morphisms.

Example. (top) $\to$ (sets), $x \rightsquigarrow$ underlying set

Example. (groups) $\to$ (abelian groups), $G \to G/(aba^{-1}b^{-1} = 1)$

Example. (top) $\xrightarrow{1-1_q}$ abelian groups, $x \rightsquigarrow H_q(x)$ homology

Example. pointed path connected topologies $\to$ groups, $x \rightsquigarrow \pi_1(x)$ (homology group)

Definition. The *dual category* C° of a category C is defined by:

$$\mathrm{Obj}(C^\circ) = \mathrm{Obj}(C)$$

$$\begin{array}{ccc} \text{A morphism} & & \text{A morphism} \\ x^\circ \xleftarrow{f^\circ} y^\circ & = & x \xrightarrow{f} y \\ \text{in } C^\circ & & \text{in } C \end{array}$$

Definition. A *contravariant functor* is a functor F on C from $C^\circ \to D$.

Example. (vect) = category of complex vector spaces. $(\text{vect})^\circ \to (\text{vect})$, $v \rightsquigarrow v^*$. This functor takes a vector space to its dual space.

Example. (top) $\to$ (abelian groups), $x \rightsquigarrow H^q(x)$ cohomology

Example. Let X be a topological space. Then let (opens) denote the category where the objects are open sets in X, and the morphisms are inclusions $U \subset V$; if $U \subset V$, $\exists! U \to V$, and if $U \not\subset V$, $\nexists U \to V$.

Definition. The *sheaf of functions* F on X is the contravariant functor on (opens): $(\text{opens})^\circ \xrightarrow{F}$ (algebras), $U \rightsquigarrow F(U) =$ complex valued functions with domain U (an algebra).

If $V \to U$ (i.e., $V \subset U$), then we can restrict a function on U to V; we get $F(U) \xleftarrow{\text{rest}_V} F(U)$, $f|_V \leftarrow\!\!\rightsquigarrow f$.

Sheaf Axiom for F: Functions on U can be defined "locally." More formally, suppose U is open in X and U^i are open subsets of U that together cover U. Let U^{ij} denote $U^i \cap U^j$.

$$U \leftarrow \{U^i\} \leftleftarrows \{U^{ij}\}$$

$$\begin{tikzcd} U^i & \\ & U^{ij} \arrow[ul, hook'] \arrow[dl, hook] \\ U^j & \end{tikzcd}$$

Then, given functions f^i on U^i such that the restriction of f^i and f^j to U^{ij} are equal for all i, j, the sheaf axiom requires that there exists a unique function f on U such that the restriction of f to U^i is f^i.

Example. Let $X = U$ be the real line. Let $U^1 = (-\infty, 1)$ and let $U^2 = (0, \infty)$. Then $U = U^1 \cup U^2$. Let $U^1 \cap U^2 = U^{12}$ $(= (0, 1))$. Then if f^1 and f^2 are functions on U^1 and U^2 and if the restriction of f^1 to U^{12} is equal to the restriction of f^2 to U^{12}, then $\exists!\ f$ on U, such that its restriction to $U^i = f^i$.

Definition. A *sheaf on a topological space* X is a contravariant functor $(\text{opens})^\circ \xrightarrow{M} C$ (some category), $U \rightsquigarrow M(U)$ which satisfies the sheaf axiom:

Suppose $\{U^i\}$ covers U and let $U^{ij} = U^i \cap U^j$. Given an element $\alpha^i \in M(U^i)$, if the restriction[11] of α^i and α^j to $M(U^{ij})$ are equal for all i, j, then $\exists! \alpha \in M(U)$ whose restriction to U^i is α^i for all i.

We want to (eventually) write the sheaf axiom more compactly. First, we rewrite it in terms of $M(U)$. Recall

$$\begin{tikzcd} U^i & \\ & U^{ij} \arrow[ul, hook'] \arrow[dl, hook] \\ U^j & \end{tikzcd}$$

Then

$$0 \to M(U) \to \prod_i M(U^i) \underset{d_1^*}{\overset{d_0^*}{\rightrightarrows}} \prod_{i,j} M(U^{ij})$$

$$U \leftarrow \{U^i\} \underset{d_1}{\overset{d_0}{\leftleftarrows}} \{U^{ij}\}$$

Then the sheaf axiom says that the above sequence is exact[12] if we replace $\rightrightarrows$ by the difference $d_0^* - d_1^*$.[13]

Think about for next time: The structure sheaf on $X = \mathbb{A}^1$ (with the Zariski topology): U open $= X - S$ (with S a finite set) together with $U = \emptyset$. If $S = (s_1, \ldots, s_k)$. Let $f = (x_1 - s_1) \cdots (x - s_k)$, $\mathcal{O}(U) = \mathbb{C}[x][f^{-1}]$. Check the sheaf axiom.

[11] If $V \to U$, then $M(V) \xleftarrow{\text{"restriction"}} M(U)$.

[12] A sequence is exact if the kernel of each map is equal to the image of the preceding map.

[13] We're assuming that the category we're mapping into has a $-$ (e.g., that of abelian groups), i.e., that each $M(U)$ has a zero element and subtraction.

25 Monday, April 11, 2011

26 Wednesday, April 13, 2011

Structure Sheaf on Affine Variety

$X = \operatorname{Spec} A$

Define on basis $\mathcal{B}$ for topology $\mathcal{B} = \{\text{opens } X_x, s \in A\} = \{X - V(s)\}$

Put $\mathcal{O}_X(X_s) = A_s$.

Similarly, if M is an A-module, get sheaf $\mathcal{M}$, $\mathcal{M}(X_s)$ =localized module M_s.

$A_s = A[s^{-1}] = \{s^{-r}a\}$, $M_s = \{s^{-r}m \,|\, r \text{ integer}, m \in M\}$

$s^{-r}a = s^{-r'}a'$ if $s^{r'}a = s^r a'$

Eqivalence relation: $m/s^r = m'/s^{r'}$ if $s^n s^{r'} m = s^n s^r m'$ for some n

M_s is an A_s-module

Sheaf axiom on $\mathcal{B}$

$X_{s_1} \cup \cdots \cup X_{s_k}$ means $s_1 \cdots s_k$ generate a unit ideal. $\sum r_i s_i = 1$, $r_i \in A$.

Note $s_1^n, \ldots, s_k^n$ also generate the unit ideal. So we can also write $\sum r_i s_i^n = 1$ (difference coefficients r_i. We can replace s_i by s_i^n.

Then the sheaf axiom (for X) says that

$$0 \to \mathcal{M}(X) \to \prod_i \mathcal{M}(X_{s_i}) \xrightarrow{\text{diff}} \prod_{i,j} \mathcal{M}(X_{(s_i s_j)}$$

is exact.

$$0 \to M \to \prod M_{s_i} \xrightarrow{\text{diff}} \prod_{i,j} M_{s_i s_j}$$

is exact.

We also need to check this for when we replace X by $U \in \mathcal{B}$ ($U = X_t$)

Suppose $m \in M$, $m \rightsquigarrow 0$ in M_{s_i} for all i. This means that $s_i^n m = s_i^n 0 = 0$ for $n \gg 0$.

Checking the exactness of the first $\to$: $m = 1 \cdot m = \sum r_i s_i^n m = 0$.

Given $\alpha_i \in M_{s_i}$ and $\alpha_i = \alpha_j m M_{s_i s_j}$, we want to find $w \in M$ with $w = \alpha_i$ in M_{s_i} for all i.

$$\alpha_i = s^{-n} m_i, \quad \alpha_j = s^{-n} m_j, \quad m_i \in M$$

$\alpha_i = \alpha_j$ in $M_{s_i s_j}$ means $(s_i s_j)^N s_j^n m_i = (s_i s_j)^N s_i^n m_j$. Let's absorb s_i^N into m_i, so that our new equation looks like

$$\boxed{s_j^\ell m_i = s_i^\ell m_j} \qquad (\ell = N + n)$$

Write $\sum r_i s_i^\ell = 1$.

$$\begin{aligned} m_j &= \sum r_i s_i^\ell m_j \\ &= \sum r_i s_j^\ell m_i \\ &= s_j^\ell w & w = \sum r_i m_i \\ \boxed{m_j = s_j^\ell w} & \quad \forall j \end{aligned}$$

bring s_js to the other side

$$s_j^{-\ell} m_j = w \in M$$

But we need n, not ℓ...

Structure sheaf on $\mathbb{P}^n$

Coordinates $(x_0, \ldots, x_n)$. Say we have covered $\mathbb{P}^n$ by the standard affine $U_i = \{x_i \neq 0\}$. We have a structure sheaf on $U_i \approx \mathbb{A}^n$.

Open subsets of U_i form a basis for the topology on $\mathbb{P}^n$. So we get a structure sheaf $\mathcal{O}_\mathbb{P}$ by descrbing it on each U_i.

We must check that if we restrict the structure sheaf on U_i and U_j to $U_i \cap U_j$, we get the same answer in both cases.

What's the benefit of describing the structure sheaf this way? If you give a variety by the topological space X and a sheaf $\mathcal{O}_X$ of algebras, then you "know" (in principle) $\mathcal{O}_X(U)$ for every U. The benefit is that we can define "morphism" easily.

Definition. A *regular function* on an open set U is an element of $\mathcal{O}_X(U)$. (Given a regular function f, and a point p, we can evaluate f at p to get a function.)

Definition. Given two varieties, we can define a *morphism*

$$(Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$$

given by

- a continuous map $Y \xrightarrow{f} X$
- which carries regular functions to regular functions

$$(\text{Functions on } X) \xrightarrow{\circ f} (\text{Functions on } Y)$$
$$g \rightsquigarrow g \circ f$$

If U is an open set in X, then $V = f^{-1}U$ in Y.

$$(\text{Functions on } U) \xrightarrow{\circ f} (\text{Functions on } V)$$

F_X = sheaf of functions on X

$$F_X(U) \xrightarrow{\circ f} F_Y(V)$$

$$F_X \xrightarrow{f^* = \circ f} F_Y$$

$$\begin{tikzcd} F_X(U) \arrow[r, "\circ f"] & F_Y(V) \\ \mathcal{O}_X(U) \arrow[u, hook] \arrow[r, "\circ f"] & \mathcal{O}_Y(V) \arrow[u, hook] \end{tikzcd}$$

$$V = f^{-1}(U)$$

27 Friday, April 15, 2011

Sheaf on $\mathbb{P}^n$

Define on standard affine, $U_i = \operatorname{Spec} \mathbb{C}\left[\left\{\frac{x_j}{x_i}\right\}\right]$.

Other affine opens: take homogeneous polynomial in $f(x_0, \ldots, x_n)$, degree r. (A function on $\mathbb{P}^n$: ratio $\frac{f}{g}$ of homogeneous polynomials of some degree $\frac{f(\lambda x)}{g(\lambda x)} = \frac{f(x)}{g(x)}$.)

The locus $\{f = 0\}$ exists in $\mathbb{P}^n$, and is a closed set. Let $U_{(f)} = \mathbb{P}^n - \{f = 0\}$. $U_{(f)}$ is an affine variety. Coordinate ring $R_{(f)} = \left\{\frac{p(x)}{f(x)^k} \,\middle|\, p \text{ has degree } kr\right\}$. $\frac{p}{f^k}$ is a well-defined function on $U_{(f)}$.

$R_{(f)}$ is generated by $\left\{\frac{m}{f} \,\middle|\, m \text{ is a monomial of degree } r\right\}$.

Example. $f = x_0^2 + x_1^2 + x_2^2$

$R_{(f)}$ is generated by $\frac{x_0^2}{f}$, $\frac{x_0 x_1}{f}$, …, with many relations.

Proposition.

$$U_{(f)} \approx \operatorname{Spec} R_{(f)}$$

On $V_{(f)}$, this has the structure sheaf $\mathcal{O}_{V_{(f)}}$.

The definition says that the slobal struture sheaf(?) $\mathcal{O}_{V_{(f)}}(V_{(f)}) = R_{(f)}$, $\mathcal{O}_{V_{(f)}}(V_{(f)} - \text{zeros of } s) = R_{(f)}[s^{-1}]$.

We have defined the structure sheaf $\mathcal{O}_{\mathbb{P}^n}$

(If we have $Y \xrightarrow{j} X$ (variety) is an inclusion of an open set and has structure sheaf $\mathcal{O}_X$, then Y is the topological space with the "indced topology": a subset $V \subset Y$ is open if V is open in X.
The structure sheaf $\mathcal{O}_Y :=$ restriction of the structure sheaf $\mathcal{O}_X$.
V open in Y, $\mathcal{O}_Y(V) = \mathcal{O}_X(V)$, $\mathcal{O}_Y = [j^* \mathcal{O}_X]$)

$\therefore$ We have defined the structure sheaf $\mathcal{O}_{U_{(f)}}$.

The statement of the proposition $U_{(f)} \approx V_{(f)}$ then means:

- homomorphism $U_{(f)} \to V_{(f)}$
- & $\mathcal{O}_{U_{(f)}} \overset{\approx}{\longleftrightarrow} \mathcal{O}_{V_f}$

A morphism

$$(Y, \mathcal{O}_Y) \xrightarrow{f} (X, \mathcal{O}_X)$$

(a) *continuous* map $Y \to X$

(b) Map $\mathcal{O}_Y \xleftarrow{f^*} \mathcal{O}_X$

If U is open in X, then $f^{-1}U = V$ open in Y. Then we have a homomorphism of algebras $\mathcal{O}_Y(X) \xleftarrow{f^*} \mathcal{O}_X(U)$.

An *isomorphism* is an invertible morphism.

Proof. In Prof. Artin's notes. $\square$

Suppose f and g are homomorphisms of degrees r, respectively. Then we have three finite-type algebras $R_{(f)}$, $R_{(g)}$, $R_{(fg)}$.

Proposition. *Let* $w = \frac{g^r}{f^s} \in R_{(f)}$. *Then*

$$R_{(f)}[w^{-1}] \approx R_{(fg)} \approx R_{(g)}[w]$$

Proof. $R_{(fg)}$ is generated by $\frac{M}{(fg)}$ (M is a monomial), M has degree $r+s$. We can write $M = m_1 m_2$, with m_1 of degree r and m_2 of degree s.

$$\frac{M}{fg} = \frac{m_1}{f}\frac{m_2}{g}$$

$$\frac{m}{g} = m\frac{f^s}{g^r}\frac{g^{r-1}}{f^s} = \frac{mg^{r-1}}{f^s}w$$

Let's not check the rest. $\square$

$\{U_{(f)}\}$ = all affine opens in $\mathbb{P}^n$

Definition. A *quasi-coherent sheaf* $\mathcal{M}$ on an affine scheme $X = \operatorname{Spec} A$ corresponds to an A-module M given by the following rules:

- Given a quasi-coherent sheaf $\mathcal{M}$, $M = \mathcal{M}(X)$ =global sections.
- Gven an A-module M, define $\mathcal{M}$ by $\mathcal{M}(X_s) = M_s$.

Note $\mathcal{M}(X_s)$ (M_s) is a $\mathcal{O}_X(X_s)$-module (A_s).
$\mathcal{M}$ is a sheaf of $\mathcal{O}_x$-modules.[14]
A sheaf is *coherent* if M is finite-type.
If $(X, \mathcal{O}_X)$ is a variety, e.g., $\mathbb{P}^n$, not necesarily affine, then a *quasi-coherent sheaf* $\mathcal{M}$ on X is the sheaf of $\mathcal{O}_X$-modules, and when we restrict to an affine open, we get a quasi-coherent sheaf on that affine.

Example. The sheaf $\mathcal{O}(n)$ on $\mathbb{P}^n$:
Its section on an affine open $U_{(f)}$ case: (f homomorphism of degree r)

$$[\mathcal{O}_{\mathbb{P}}(n)]\,(U_{(f)}) = \left\{ \frac{p(x)}{f(x)^k} \,\middle|\, p \text{ has degree } rk+n \right\}$$

$$\mathcal{O}_{\mathbb{P}}(U_{(f)}) = R_{(f)} = \left\{ \frac{p}{f^k} \,\middle|\, p \text{ has degree } rk \right\}$$

The global sections $\mathcal{O}_{\mathbb{P}}(n)(\mathbb{P}^n) = H^0(\mathbb{P}^n, \mathcal{O}(n))$ are homogeneous polynomials of degree n.

[14] Why not call it an $\mathcal{O}_x$-module? Don't know.

Let h be a polynomial of degree m.

$$0 \to \mathcal{O}_{\mathbb{P}}(n) \xrightarrow{\text{multiplication by } h} \mathcal{O}_{\mathbb{P}}(n+m) \to \text{cokernel}$$

Let Y be the locus $h = 0$ in $\mathbb{P}^n$.

$$0 \to \mathcal{O}_{\mathbb{P}}(-m) \xrightarrow{h} \mathcal{O}_{\mathbb{P}} \to \mathcal{O}_Y \to 0$$

is exact, and so is

$$0 \to \mathcal{O}_{\mathbb{P}}(n-m) \xrightarrow{h} \mathcal{O}_{\mathbb{P}}(n) \to \mathcal{O}_Y(n) \to 0$$

This is something analogous to $\mathcal{O}(n)$, but on Y.

($\mathcal{O}_{\mathbb{P}}(-m)$, $\mathcal{O}_{\mathbb{P}}$ are independent of h)

Example. $x_0 = h$

$$\mathcal{O}_{\mathbb{P}^n}(-1) \xrightarrow{x_0} \mathcal{O}_{\mathbb{P}^n} \to \mathcal{O}_{\mathbb{P}^{n-1}} \to 0$$

$Y = \text{locus } \{x_0 = p\} = \mathbb{P}^{n-1}$ (hyperplane at ∞)

Next week: cohomology of coherent sheaves

28 Wednesday, April 20, 2011

29 Friday, April 22, 2011

30 Monday, April 25, 2011

Axioms for Cohomology

(q. cohomology sheaves)

- $H^0(X, M) = M(X)$
- $H^0, H^1, \ldots$ is cohomology functor(?)
- $Y \xrightarrow{f} X$ is the inclusion of affine oben subset N q. cohomology on Y, $\implies H^q(X, f_N) = 0$ for all $q > 0$

Y open $\implies H^q(X, f_*N) \approx H^q(Y, N)$

Uniqueness: Choose an affine open cover of X: $U = \{U^\nu\}$, $U \xrightarrow{j} X$, $M \xrightarrow{q} j_*j^*M$ ...(SOME MATERIAL NOT INCLUDED)

Define $R_M^0 = j_*j^*M$

$$0 \to M \to R_M^0 \to M^q \to 0$$

exact.

$H^q(R_M^0) = 0$ for $q > 0$.

$\therefore$

$$0 \to H^0(M) \to H^0(R_M^0) \to H^0(M^1) \to H^1(M) \to 0 \to H^1(M^1) \to H^2(M) \to 0 \cdots$$

H^0 is the identity by axiom 1, $\therefore H^1(M) = H^0(M^1)/\operatorname{im}(H^0(R_M^0))$

$\therefore H^1(M)$ is unique for all M. Then $H^1(M^1) \approx H^2(M)$, so $H^2(M)$ is unique for all M.

$$0 \to M^1 \to R_M^1 \to M^2 \to 0$$

So we can repeat the construction, replacing M^1 in $0 \to M \to R_M^0 \to M^1 \to 0$ with M^1 to get an *acyclic resolution* of M (resolution means exact, acyclic means that $H^q(R_M^i) = 0$ for $q > 0$).

$$0 \to M \to R_M^0 \to R_M^1 \to R_M^2 \to \cdots$$

$R_M^1 = j_* j^* M^1$

Look at the complex

$$0 \to R_M^0 \to R_M^1 \to \cdots$$

Take $H^0(R_M^\cdot) = R_M^\cdot(X)$ global section ($\cdot$ is a "variable"). Not exact. But it's a complex.[15] Define $H^q(X, M) = \mathcal{H}^q(R_M^\cdot(X)) = (\ker / \operatorname{im})$ in the complex $R_M^\cdot(X)$.

We know

$$0 \to M(X) \to R_M^0(X) \to R_M^1(X)$$

is exact. $\therefore M(X) \approx \mathcal{H}^0(R_M^\cdot(X))$ (First axiom ✓)

Second axiom: If $0 \to M \to M' \to M'' \to 0$ is exact, want long cohomological sequence. $R_M^0 = j_* j^* M$. j^* is the trivial restriction which is exact. Since $U^\nu \xrightarrow{j^\nu} X$ is the inclusion of an affine open, so j_*^ν is exact. $\therefore j_*$ is exact.

$N \to N' \to N''$, quasi-coherent on U, is exact if for all affine open sets $V \subset U$, $N(V) \to N(V') \to N(V'')$ is exact.

?W is an affine open in X?

?$j_* N(W) \to j_* N'(W) \to j_* N''(W)$ exact?

$$j_* N(W) = N(U^\nu \cap W)$$

affine because U^ν and W are both affine (therefore $U^\nu \cap W$ is affine). So yes.

$$* = N(U \cap W) \to N'(U \cap W) \to N''(U \cap W)$$

If $0 \to M \to M' \to M'' \to 0$ is exact, then $0 \to R_M^0 \to R_{M'}^0 \to R^{M''} \to 0$ is exact.

$$\begin{aligned} R_M^0 &= j_* j^* M \\ R_M^0(X) &= j^* M(U) \qquad U \text{ affine} \\ &= M(U) \end{aligned}$$

If $0 \to M \to M' \to M'' \to 0$ is exact, then $0 \to M(U) \to M'(U) \to M''(U) \to 0$ is exact (because U is affine).

Therefore

$$0 \to R_M^0(X) \to R_{M'}^0(X) \to R_{M''}^0(X) \to 0$$

is exact.

Applying this to each degree separately,

$$0 \to R_M^\cdot(X) \to R_{M'}^\cdot(X) \to R_{M''}^\cdot(X) \to 0$$

[15] Definition of *complex*: if you compose two maps, you get zero.

is an exact sequence of complexes. (So $\mathcal{H}^q$ is a cohomological functor.) (Second axiom ✓)

$$\begin{tikzcd} V \arrow[r, "f'"] \arrow[d, "j'"] & U \arrow[d, "j"] \\ Y \arrow[r, "f"] & X \end{tikzcd}$$

with $V^\nu = Y \cap U^\nu$ an affine open cover of Y. We now suppress indices.

Let N be quasicoherent on Y.

We want to show $H^q(X, f_*N) = 0$ for $q > 0$. We can show that $H^q(X, f_*N) \approx H^q(Y, N)$ whether or not Y is affine.

On Y: say $S^0_N = j'_*j'^*N$ We get an acyclic resolution

$$0 \to N \to S^0_N \to S^1_N \to \cdots$$

On the other hand, take $j_*j^*(f_*N) = R^0_{f_*N}$. We get an acyclic resolution

$$0 \to f_*N \to R^0_{f_*N} \to R^1_{f_*N} \to \cdots$$

$$H^q(Y, N) \approx \mathcal{H}^q(S^{\cdot}_N(Y))$$
$$H^q(X, f_*N) \approx \mathcal{H}^q(R^{\cdot}_{f_*N} * (X))$$

Plan: Show that $R^{\cdot}_{f_*N} \approx f_*S^{\cdot}_N$. Then $R^{\cdot}_{f_*N}(X) \approx [f_*S^{\cdot}_N](X) = S^{\cdot}_N(Y)$ (by the definition of f_*). Then we get isomorphisms(?).

$R^0_{f_*N} = j_*j^*f_*N$

$$j^*f_*N \approx f'_*j'^*N$$

Then

$$R^0_{f_*N} = j_*j^*f_*N \approx j_*f'_*j'^*N$$

By commutativity of the diagram above,

$$j_*f'_* = f_*j'_*$$

Then

$$R^0_{f_*N} = j_*j^*f_*N \approx j_*f'_*j'^*N \approx f_*j'_*j'^*N = f_*S^0_N$$

(Third axiom ✓(almost; we need to check compatibility))

$$0 \to M \to R^0_M \to M^1 \to 0$$
$$0 \to H^{q-1}(M^1) \to H^q(M) \to 0$$