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

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

$\mathbb{A}^2$ 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

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

(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-singluar* 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 nonsinular □

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.*

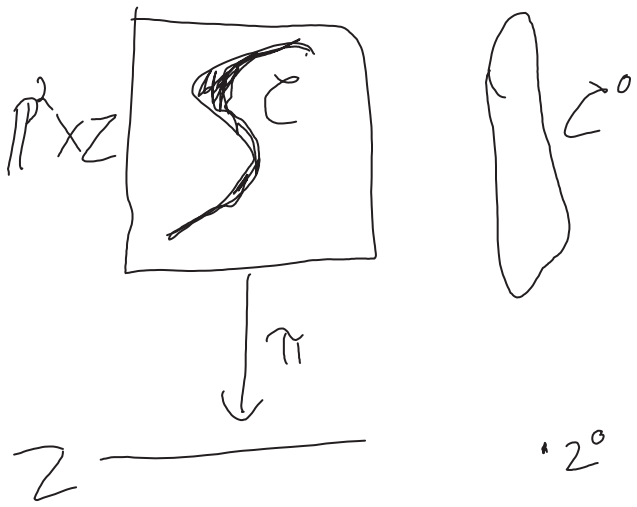
Proof. See two proofs, each of which depends on some theorem which will be proved later.

Setup: Order the monomials of degree d in x, y, z arbitrarily m_1, m_2, ..., 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 $\mathbb{A}^N$. □

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 $\overline{\pi(S)} \neq Z$. □

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 $y^2z = x^3 - xz^2$
Then $\boxed{f = x^3 - xz^2 - y^2z}$.
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 $(x : y : z) = (0 : 1 : 0)$.

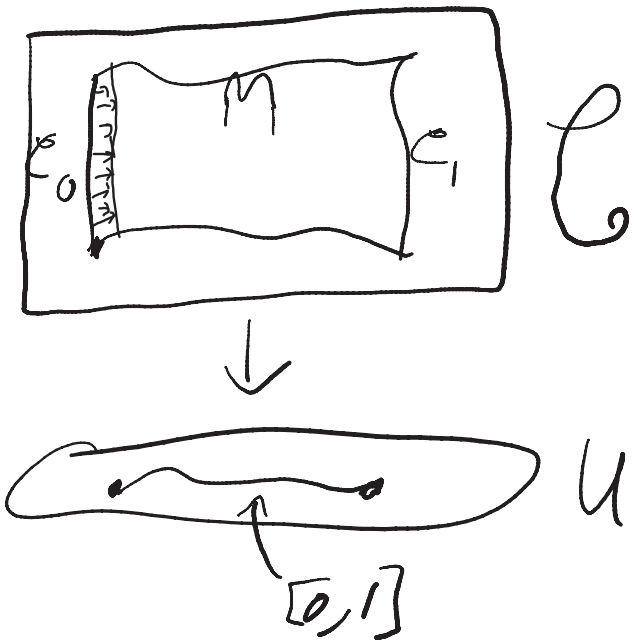
Genus and Euler characteristic

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 $m_1, \ldots, m_N$, coefficients $z_1, \ldots, z_N$

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

(We have $f(x, y, z) = z_1x^d + z_2x^{d-1} + \cdots$)

U = open subset in Z corresponding to smooth plane curves

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

$$\begin{array}{ccc} \mathcal{C} & \subset & \mathbb{P}^2 \times Z \\ & \searrow & \downarrow \\ & & Z \end{array} \qquad \begin{array}{ccc} \mathcal{C}|_U = \mathcal{C}_U & \subset & \mathbb{P}^2 \times U \\ & \searrow & \downarrow \\ & & U \end{array}$$

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?) □

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 = # vertices − # edges + # 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.

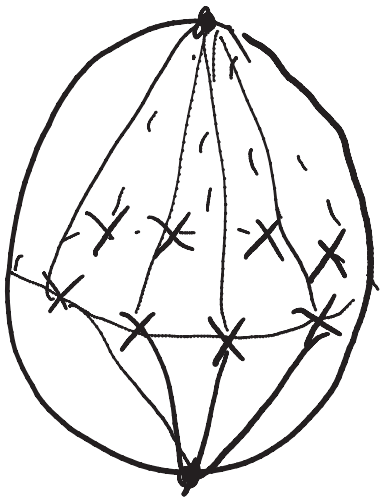
What is the Euler characteristic and genus of a smooth plane curve of degree d?

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 $f(x, y, z) = z^d - a_1(x, y)z^{d-1} + \cdots \pm a_d(x, y)$. Homogenous 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

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. $\mathbb{C}[x_1, \ldots, x_n]$ *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 $\bar{A} = A/I$.

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

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 i
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. □

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.

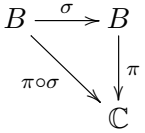
$q \in Y$, σ sends $q \to q^\sigma$

$q^{\sigma\tau}$: 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:



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

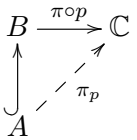
Define $q^\sigma =$ that point such that $\pi_{q^\sigma} = \pi_q \circ \sigma$.

Operation on max ideals:

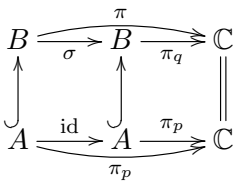
$\mathfrak{M}_{q^\sigma} = \sigma^{-1}\mathfrak{M}_q$

$Y \to X$?

For any $p \in X$,



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



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

We want to show that different orbits $\{q_1, \ldots, q_r\} \neq \{q'_1, \ldots, q'_s\}$ 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 $j = 1, \ldots, s$. (Note: $b(q) \coloneqq \pi_q(b)$.)

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

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

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*

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

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, $S = A - P = \{s \,|\, s \notin P\}$. *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 $A \subset B = A_S$:

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

$J^c = J \cap A$. 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

(2) ~~Proof.~~ ⟹ (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) ⟹ (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 $a^{-1}s \in A_S$. □

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*

[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.

- *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* $\operatorname{PSpec} A_{\mathfrak{M}} = \{P \,|\, P \cap S \neq \emptyset\} = \{P \,|\, P \subset \mathfrak{M}\} = \begin{cases} (0) \\ P = (f) \,|\, f(a,b) = 0 \\ \mathfrak{M}_{(a,b)} \end{cases}$

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:

$$\begin{aligned} x_i &= \sum_j p_{ij} x_j & p_{ij} &\in I \\ X &= PX & P &\text{ matrix } (p_{ij}) \\ (\mathbb{1} - P)X &= 0 \\ Q(\mathbb{1} - P) &= \delta \mathbb{1} \end{aligned}$$

where Q is the cofactor matrix for $\mathbb{1} - P$ with entries in A, and $\delta = \det(\mathbb{1} - P)$.

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

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

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 $(1-z)^{-1}$). □

13 Monday, March 7, 2011