Math W4045 - Algebraic Curves
Prof. A. J. de Jong
Spring 2010
Rough Lecture Notes by Alexander Moll

1 19 January

1.1 Introduction

Book: *Algebraic Curves* by William Fulton (Michigan). Also - a pile of other books - visit his office hours! We won't just work out of this book.

Organization:

1. attend lectures
2. visit webpage
3. weekly homework
4. final exam.

Mathematical Content:

- Little of algebraic varieties over $\mathbb{C}$ (can do all this over $F = \overline{F}$). What is a curve? Morphisms of curves?
- Singularities of curves.
- Resolving singularities - "desingularize curves"
- Complex manifolds and curves: associate to a nonsingular curve a complex manifold of dimension 1.
- Nonsingular projective curves to their function fields.
- Riemann-Roch and
- Applications of Riemann Roch (e.g. Hurwitz formula and linear systems on curves plus embeddings in projective space).[1]

[1] While we did not get to these last two topics in the course, we gave a much richer story on the resolution of singularities.

1.2 Today: "polynomials and points"

Let's calibrate how we talk about things. We often work with $\mathbb{C}[x_1, \ldots, x_n]$ the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{C}$. It's a $\mathbb{C}$-algebra, since $\mathbb{C} \hookrightarrow \mathbb{C}[x_1, \ldots, x_n]$ a ring map. A typical element $f \in \mathbb{C}[x_1, \ldots, x_n]$ is a finite sum

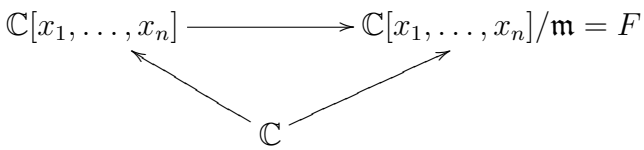
$$\sum_{I=(i_1,\ldots,i_n)} c_I x_1^{i_1} \cdots x_n^{i_n}$$

with $c_I \in \mathbb{C}$ and $c_I = 0$ for all but finitely many of these indices. Given any vector $a = (a_1, \ldots, a_n) \in \mathbb{C}^n$, can evaluate f at a, for $f : \mathbb{C}^n \to \mathbb{C}$, $f(a) = \sum_I c_I a_1^{i_1} \cdots a_n^{i_n} \in \mathbb{C}$. Note that for $f, g \in \mathbb{C}[x_1, \ldots, x_n]$, $c \in \mathbb{C}$, $(f+g)(a) = f(a)+g(a)$, $(fg)(a) = f(a)g(a)$, $(cf)(a) = cf(a)$, and $1(a) = 1$ where 1 is the constant polynomial. This means that evaluation at a is a $\mathbb{C}$-algebra map from $\mathbb{C}[x_1, \ldots, x_n]$ to $\mathbb{C}$, call it $ev_a : f \to f(a)$ (it's a ring map that is also $\mathbb{C}$-linear). We're used to thinking of polynomials as functions, but no: we can think of them as elements in this abstract ring. NB: all of our rings are commutative with unit and ring maps are unital. Obviously ev_a is surjective, so $\ker(ev_a)$ is a maximal ideal in $\mathbb{C}[x_1, \ldots, x_n]$. [Recall the definition of an ideal $I \subset R$, a prime ideal $\mathfrak{p} \subset R$ whose quotient gives integral domain, and a maximal ideal $\mathfrak{m} \subset R$ whose quotient gives a field. Also note that the quotient R/I is also a ring by $(a + I)(b + I) = ab + I$.] NB: $\{0\}$ ring has a 1: it is the only ring where $1 = 0$ - it's to add this to the category of rings, but this is not a field. We know $\ker ev_a$ must be maximal since it surjects onto a field, and any ring map $\varphi : R_1 \to R_2$ surjective satisfies $R_2 = \mathrm{Im}\varphi \cong R_1/\ker\varphi$. What are some elements of $\ker ev_a$? Well, $x_1 - a_1, \ldots, x_n - a_n$ are all in there. Also $x_1x_2 - a_1a_2 \in \ker ev_a$. Question: is this a linear combination of $(x_1 - a_1)$ and $(x_2 - a_2)$? E.g., $x_2(x_1 - a_1) + a_1(x_2 - a_2)$. Procedure: highest monomial x_1, take $\frac{x_1x_2 - a_1a_2}{x_1 - a_1}$, etc: ordering on monomials.[2]

Proposition 1 *The ideal* $\ker ev_a$ *is generated by* $x_i - a_i$ *for* $1 \leq i \leq n$

Notation: if $f_1, \ldots, f_t \in R$, then $(f_1, \ldots, f_t)$ denotes the ideal in R generated by $f_1, \ldots, f_t$, which is $\{f \in R : \ f = \sum g_i f_i, g_i \in R\}$. Exercise: prove the proposition.

Question: is every maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$ of the form $(x_1 - a_1, \ldots, x_n - a_n)$, that is, the kernel of ev_a for some $a \in \mathbb{C}$? Answer: True! This gives a bijection between points of $\mathbb{C}^n$ and maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ - *what algebraic geometry is.* Suppose $\mathfrak{m} \subset \mathbb{C}[x_1, \ldots, x_n]$ is a maximal ideal. This gives the following diagram:



where F is some field. Since a non-zero map of fields is automatically injective, we have a field extension $\mathbb{C} \subset F$. Indeed, this map is non-zero, since if $\mathbb{C} \subset \mathfrak{m}$ where we view $\mathbb{C} \hookrightarrow \mathbb{C}[x_1, \ldots, x_n]$, then $1 \in \mathfrak{m}$ forces $\mathfrak{m} = \mathbb{C}[x_1, \ldots, x_n]$ which cannot be so.

[2] Grobner bases?...

Now, we will use the fact that $\mathbb{C}$ is uncountable to give $\mathbb{C} \cong F$ a bijection. This may be a dirty trick, but that too is *what algebraic geometry is.*

Lemma 1 $\dim_{\mathbb{C}} F$ *is a cardinal number independent of the choice of basis, so* $\dim_{\mathbb{C}}(\mathbb{C}[x_1, \ldots, x_n]) = \aleph_0$

Okay, so any basis is countable and also infinite: for proof, just exhibit one basis - i.e., the monomials! $\square$

Lemma 2 *if* $\mathbb{C} \subset F$ *is a field extension, then either* $\mathbb{C} = F$ *or* $\dim_{\mathbb{C}} F$ *is uncountable.*

Proof: suppose $\mathbb{C} \neq F$, so we can choose $f \in F \setminus \mathbb{C}$. We claim that all elements $\frac{1}{t-c}$ for $c \in \mathbb{C}$ are $\mathbb{C}$-linearly independent. If this is true, we're done. Namely, suppose

$$\sum_{i=1}^{n} \frac{a_i}{t - c_i} = 0$$

with $c_i, a_i \in \mathbb{C}$, $c_1, \ldots, c_n$ pairwise distinct. Multiplying by $(t-c_1)\cdots(t-c_n)$ you get

$$\sum_{i=1}^{n} a_i (t-c_1)\cdots\hat{(t-c_i)}\cdots(t-c_n) = 0$$

in F. The LHS is a polynomial $p(t)$ in t. Since $\mathbb{C} = \overline{\mathbb{C}}$, the element t is transcendental, not algebraic, over $\mathbb{C}$. This means $p(t) = 0$ *as a polynomial*, so also as a function, so we may substitute $t = c_i$ to get 0 also, hence

$$a_i \cdot (c_i - c_1)\cdots\hat{(c_i - c_i)}\cdots(c_i - c_n) = 0$$

implies $a_i = 0$, so $\frac{1}{t-c_i}$ are all linearly independent. $\square$

Recall this transcendental business: if $K \subset L$ is a field extension, and $\alpha \in L$, then we get a dichotomy: either $\exists$ a non-zero $p \in K[x]$ such that $p(\alpha) = 0$. In this case, α is called *algebraic* over K, and there exists a minimal degree polynomial irreducible over K with leading coefficient 1 (monic) that annihilates α. Let's call this minimal polynomial $p_\alpha(x) \in K[x]$. On the other hand, we may have $\alpha \in L$ such that $\forall p \in K[x]$, $p(\alpha) \neq 0$: this is α *transcendental* over K.

Let's return to the proof of the proposition: our $\mathbb{C}[x_1, \ldots, x_n]/\mathfrak{m}$ will have dim $\leq$ over $\mathbb{C}$ as $\mathbb{C}[x_1, \ldots, x_n]$ since it is a quotient. Indeed, $\mathbb{C}[x_1, \ldots, x_n] = \langle \mathbb{X}_\ltimes \rangle$ where $\mathbb{X}_n$ is the collection of monomials, so $\mathbb{C}[x_1, \ldots, x_n]/\mathfrak{m}$ is generated by $\pi(\mathbb{X}_n)$ where π is the quotient map. The combination of Lemmas 1 and 2 prove that $F = \mathbb{C}$. If we set a_i equal to the unique element of $\mathbb{C}$ which maps to x_i mod $\mathfrak{m}$ in $\mathbb{C}[x_1, \ldots, x_n]/\mathfrak{m} = F$ (it's unique because the map $\mathbb{C} \to F$ is injective), then $x_i - a_i \in \mathfrak{m}$, so $(x_1 - a_1, \ldots, x_n - a_n) = \mathfrak{m}$. Conclusion: yes, the maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ all take the form of $\ker ev_a$ for some $a \in \mathbb{C}$. NB: the same thing works $\forall F = \overline{F}$, but Fulton's proof is harder than the way we used $\mathbb{C}$ uncountable (won't work for $\overline{Q}$ or $\overline{\mathbb{F}_p}$).

2 21 January

2.1 Algebraic Sets

Definition 1 *An algebraic set is a subset $X \subset \mathbb{C}^n$ such that there exists a set / collection of polynomials $S \subset \mathbb{C}[x_1, \ldots, x_n]$ such that*

$$X = V(S) := \{a \in \overset{n}{\mathbb{C}} : f(a) = 0 \ \forall f \in S\}$$

V is for "variety," but these are not quite varieties. S might be , or infinite... first here are some special cases.

If $S = \{f_1, \ldots, f_r\}$ is finite, write $V(f_1, \ldots, f_r)$ instead of $V(\{f_1, \ldots, f_r\})$.

If $S = \{f\}$ and $f \neq 0$, then $V(f)$ is called a hypersurface.[3]

A hypersurface in $\mathbb{C}^2$ is called an affine plane curve.

These of course are hard to draw (too many dimensions), but can look at $\mathbb{R} \times \mathbb{R} \subset \mathbb{C}^2$ as we're used to. Draw $V(xy) = V(x) \cup V(y)$, $V(x^2 - y^3)$ a cusp.

Proposition 2 *The collection of algebraic sets of $\mathbb{C}^n$ forms the closed subsets of a topology on $\mathbb{C}^n$ called the Zariski topology*

Have to show $\emptyset, \mathbb{C}^n$ are algebraic sets, that Z_1, Z_2 algebraic sets $\Rightarrow Z_1 \cup Z_2$ are algebraic sets, and $Z_i, i \in I$ algebraic sets $\Rightarrow \bigcap_{i \in I} Z_i$ is an algebraic set. Well of course $\emptyset = V(1)$, $\mathbb{C}^n = V(0) = V(\emptyset)$. Easily $\bigcap_{i \in I} V(S_i) = V\Big(\bigcup_{i \in I} S_i\Big)$, thus it remains to prove $V(S_1) \cup V(S_2) = V(S_1 \cdot S_2)$, where

$$S_1 \cdot S_2 = \{f \in \mathbb{C}[x_1, \ldots, x_n] : f = f_1 \cdot f_2 \text{for some } f_1 \in S_1, f_2 \in S_2\}.$$

Well "$\subset$" is easy, since for $a \in \mathbb{C}^n$, $a \in V(S_1)$, ten if $f = f_1 \cdot f_2 \in S_1 \cdot S_2$, then $f(a) = f_1(a) f_2(a) = 0 \cdot f_2(a) = 0$ and same for $V(S_2)$, hence both are in $V(S_1 \cdot S_2)$. For "$\supset$", suppose $a \notin V(S_1) \cup V(S_2)$, then $\exists f_1 \in S_1$, $\exists f_2 \in S_2$ such that $f = f_1 f_2 \neq 0$ at a, so $a \notin V(S_1 \cdot S_2)$. $\square$

2.2 Properties of the Zariski topology

Think of C as usual 2-dimensional topology thing: what do algebraic sets look like in the usual topology?

Remark 1**:** The Zariski topology is not Hausdorff because any two nonempty open subsets have a nonempty intersection. Indeed, the intersection of $\emptyset \neq U_1 = \mathbb{C}^n \setminus V(S_1)$ and $\emptyset \neq U_2 = \mathbb{C}^n \setminus V(S_2)$ is

$$U_1 \cap U_2 = \mathbb{C}^n \setminus \Big(V(S_1) \cup V(S_2)\Big) = \mathbb{C}^n \setminus V(S_1 \cdot S_2) \neq \emptyset.$$

[3] My aside: just as we saw maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ corresponded to points in $\mathbb{C}^n$, we see that "points" of $\mathbb{C}[x_1, \ldots, x_n] \setminus \{0\}$ correspond to hypersurfaces in $\mathbb{C}^n$.

NB: V is inclusion reversing (contravariant functor): $S \subset S' \Rightarrow V(S) \supset V(S')$. Now for $V(S_1) \subset V(f_1)$, $V(S_2) \subset V(f_2)$, then

$$U_1 \cap U_2 = \mathbb{C}^n \setminus V(S_1) \setminus V(S_2) \supset \mathbb{C}^n \setminus V(f_1) \setminus V(f_2) = \mathbb{C}^n \setminus V(f_1 f_2)$$

and since $f_1, f_2 \neq 0$, $\exists$ a point a where $(f_1 f_2)(a) \neq 0$, so $\mathbb{C}^n \setminus V(f_1 \cdot f_2) \neq \emptyset$. $\square$.

Remark 2**:** a Zariski-open (resp. closed) is a usual open (resp. closed); the reason is that if $f \in \mathbb{C}[x_1, \ldots, x_n]$ then $f : \mathbb{C}^n \to \mathbb{C}$ and is continuous in the usual sense. So $V(f) = f^{-1}(\{0\})$ is the inverse image of a closed set under a continuous map so its closed. In the general case, note that $V(S) = \bigcap_{f \in S} V(f)$ (see proof of the proposition). $\square$

Remark 3**:** Hypersurfaces have measure zero. *Proof:* exercise. Actually, if $Z \subset \mathbb{C}^n$, Z is Zariski closed, and $Z \neq \mathbb{C}^n$, then Z has Lesbegue measure 0. NB: Zariski closed subsets of Zariski closed sets are usually relatively measure zero, except in $V(xy)$ example: will return to this when we talk about irreducibility.

Many sets give rise to the same set: $V(f, f^2) = V(f)$ ... so want nice choices of S for a given $X \subset \mathbb{C}^n$.

Lemma 3 *If $S \subset \mathbb{C}[x_1, \ldots, x_n]$ is a subset, and $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is the ideal generated by S, then $V(S) = V(I)$.*

Proof: Since $S \subset I$, we have $V(I) \subset V(S)$. Conversely, if $a \in V(S)$ and $f \in I$, we want to show $f(a) = 0$. Well $f \in I = \langle S \rangle$, so $f = \sum_{i=1}^{t} g_i f_i$ for some $g_i \in \mathbb{C}[x_1, \ldots, x_n]$ and some $f_i \in S$, then $f(a) = \sum g_i(a) f_i(a) = \sum g_i(a) \cdot 0 = 0$ so $a \in V(I)$. $\square$

Thus, it suffices to just look at ideals of $\mathbb{C}[x_1, \ldots, x_n]$.

Lemma 4 *Via the correspondence $\mathbb{C}^n \leftrightarrow$ maximal ideals $\mathfrak{m}$, we have $V(I) \leftrightarrow \{\mathfrak{m} : I \subset \mathfrak{m}\}$.*

Proof:

$$\begin{aligned} a \in V(I) &\Leftrightarrow \Big(f \in I \Rightarrow f(a) = 0\Big) \\ &\Leftrightarrow \Big(f \in I \Rightarrow f \in \ker ev_a\Big) \\ &\Leftrightarrow I \subset \ker ev_a \end{aligned}$$

$\square$

Lemma 5 *If R is any ring, $I \subset R$ an ideal, $I \neq R$, then $\exists$ a maximal ideal $\mathfrak{m} \subset R$ with $I \subset \mathfrak{m}$*

Proof given on the homework (use Zorn's Lemma). The only benefit of negating the axiom of choice, by the way, is that every set is measurable.

Corollary 1 *(Weak Nullstellensatz) If $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is an ideal, then $V(I) = \emptyset$ iff $I = \mathbb{C}[x_1, \ldots, x_n]$, which is the case iff $1 \in I$.*

Proof: follows immediately from previous two results.

Definition 2 *Let $I \subset R$ be an ideal of a ring R. The radical of I is $Rad(I) = \sqrt{I} := \{f \in R : \exists n > 0 \text{ s.t. } f^n \in I\}$. An ideal is called radical if $\sqrt{I} = I$.*

Remark: $\sqrt{I}$ is an ideal: it's obviously closed under multiplication, under addition, that's $f, g \in \sqrt{I}$, $f^n \in I, g^m \in I$, so $(f+g)^{n+m} \in I$ by looking at the binomial formula.

Remark: $\sqrt{I}$ is a radical ideal: $\sqrt{\sqrt{I}} = \sqrt{I}$ because of the product of exponents.

Remark: Any prime ideal is a radical ideal (think: $f \cdot g \in I \Rightarrow f \in I$ or $g \in I$).

Lemma 6 *If $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is an ideal, then $V(I) = V(\sqrt{I})$, so every algebraic set is defined by a radical ideal.*

Proof: this is clear, for $I \subset \sqrt{I}$ implies $V(I) \supset V(\sqrt{I})$, but $\sqrt{I}$ has functions that are roots of functions in I, so they vanish at the same points. $\square$
All of this material will culminate next lecture in Hilbert's Nullstellensatz.

3 26 January

Theorem 1 *(Hilbert's Nullstellensatz): The map $I \to V(I)$ of*

$$\{I \subset \mathbb{C}[x_1, \ldots, x_n] : I = \sqrt{I}\} \to \{X \subset \mathbb{C}^n : X \text{ closed }\}$$

*defines an inclusion reversing **bijection** between radical ideals and algebraic sets, where the inverse is given by*

$$Z \mapsto I(Z) := \{f \in \mathbb{C}[x_1, \ldots, x_n] : f(a) = 0 \ \forall a \in Z\}.$$

Remark: can define $I(Z)$ for any subset $Z \subset \mathbb{C}^n$, and it is always a radical ideal, for $f^n \in I(Z), n > 0 \Rightarrow f \in I(Z)$. Then the theorem says that $I(V(I)) \supset I$ and has $=$ exactly when I is a radical ideal. Also $V(I(Z)) \supset Z$ and equality holds iff Z is an algebraic set.

Proof of HN: Let $I = \langle S \rangle$ and $V(S) = V(\sqrt{I})$. We have already seen that the map is surjective, thus have to show it is injective. Two distinct radical ideals give two distinct algebraic sets: if $I \neq I'$ are radical ideals of $\mathbb{C}[x_1, \ldots, x_n]$, then $V(I) \neq V(I')$. To prove this, WLOG after switching them, $\exists f \in I' \setminus I$. It suffices to show $V(I) \not\subset V(f)$, i.e., $\exists$ a point in $V(I)$ where f does not vanish. To get a contradiction, assume $V(I) \subset V(f)$ (*). Trick: add an additional variable. Let $J \subset \mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$ be the ideal generated by all elements in I and the element $x_{n+1}f - 1$ (by $\mathbb{C}[x_1, \ldots, x_n] \subset \mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$ of course). Then if $a = (a_1, \ldots, a_n, a_{n+1}) \in V(J)$, we see that $h(a_1, \ldots, a_n) = 0 \ \forall h \in I$, which implies $(a_1, \ldots, a_n) \in V(I)$, but by (*) $f(a_1, \ldots, a_n) = 0 \Rightarrow a_{n+1}f(a_1, \ldots, a_n) - 1 = -1$ a

contradiction, but it's supposed to be 0. Since it's in $V(J)$, we can conclude that $V(J) = \emptyset$, so by the weak Nullstellensatz, $1 \in J$. Then

$$1 = \sum_{i=1}^{t} g_i h_i + g_{i+1}(x_{n+1}f - 1)$$

in $\mathbb{C}[x_1, \ldots, x_{n+1}]$ for some $g_i \in \mathbb{C}[x_1, \ldots, x_{n+1}]$ and some $h_i \in I$. Then substitute $x_{n+1} = \frac{1}{y}$.

$$1 = \sum_{i=1}^{t} g_i(x_1, \ldots, x_n, \frac{1}{y}) h_i(x_1, \ldots, x_n) + g_{t+1}(x_1, \ldots, x_n, \frac{1}{y})\Big(\frac{f(x_1, \ldots, x_n)}{y} - 1\Big)$$

and then multiplying by a huge power of y to eliminate all y in denominators we get

$$y^N = \sum_{i=1}^{t} \left(y^N g_i(x_1, \ldots, x_n, \frac{1}{y}) \right) \cdot h_i + y^{N-1} g_{t+1}(x_1, \ldots, x_n, \frac{1}{y}) \cdot (f - y).$$

By taking N large enough, $y^N g_i$ and $y^{N-1} g_{t+1}$ is a polynomial in $x_1, \ldots, x_n, y$. Substitute $y = f$: since f **is** a polynomial in $x_1, \ldots, x_n$, we get

$$f^N = \sum_{i=1}^{t} q_i(x_1, \ldots, x_n) \cdot h_i + 0$$

for some polynomials $q_i(x_1, \ldots, x_n)$ from the g_is from before. Thien this says $f \in \sqrt{I} = I$ a contradiction. $\square$

Just a quick note on this formal trickery: the substitutions above are well defined ring maps from say $\mathbb{C}[x_1, x_2] \to \mathbb{C}[x, y, \frac{1}{y}]$ with say $x_1 \mapsto x$, $x_2 \mapsto \frac{1}{y}$. Also, this doesn't explain why it has the inverse map we've stated. If $Z = V(I)$, then always $I \subset I(Z) = I(V(I))$. If $\subsetneq$, then by bijectivity, we would get $V(I) \supsetneq V(I(Z))$ but $\supset Z$ is a contradiction.

3.1 $n = 1$:

Zariski topology on $\mathbb{C}^1$. Note that a hypersurface is $V(f) = \{a \in \mathbb{C} : f(a) = 0, f \in \mathbb{C}[x] \setminus \{0\}\}$ is a finite set. Given any finite set $\{a_k\}_{k=1}^n \subset \mathbb{C}$, $f(x) = \prod_{k=1}^n (x - a_k)$ gives $V(f) = \{a_k\}$. The closed sets of $\mathbb{C}$ are finite, $\mathbb{C}$, or $\emptyset$. NB: A topological space underlying an algebraic curve is exactly this, so topology won't tell us anything about it. Though not every planar curve $C \subset \mathbb{C}^2$ are parametrizable, the induced Zariski topology is always this one.

3.2 Hypersurfaces:

Algebraic Fact 1 *$\mathbb{C}[x,y],\ldots,\mathbb{C}[x_1,\ldots,x_n]$ are UFDs.*

To prove this, use $\mathbb{C}(x_1,\ldots,x_{n-1})[x_n]$, where $\mathbb{C}(x_1,\ldots,x_{n-1})$ is the field of ratioanl functions on $n-1$ variables, and note that for a field K, $K[x]$ is a UFD by the Euclidean algorithm. Then use Gauss' Lemma:

Lemma 7 *(Gauss) Given $f\in\mathbb{C}[x_1,\ldots,x_n]$, if f factors non-trivially in $\mathbb{C}(x_1,\ldots,x_{n-1})[x_n]$, then it factors non-trivially in $\mathbb{C}[x_1,\ldots,x_n]$.*

Indeed, both factors have to have positive degree or neither one is a unit for this to be a "non-trivial" factorization. The same argument shows that if R is a UFD, then $R[x]$ is a UFD, since $\exists$ a Gauss Lemma for UFDs: $R[x]\subset K[x]$ for K the fraction field of R...

We can have an irreducible element in a Noetherian domain that's not prime. For f is irreducible iff $f=ab\Rightarrow$ either a or b is a unit, and f is prime iff (f) is a prime ideal. Always have prime $\Rightarrow$ irreducible, but we have $\leftrightarrow$ in UFD (unique factorization into irreducibles up to permutation and association (up to units)).

Back to hypersurfaces: $f\in\mathbb{C}[x_1,\ldots,x_n]$, $f\neq 0$, then write $cf_1^{e_1}\cdots f_t^{e_t}$ its factorization into primes. Then

$$V(f)=V(f_1)\cup\cdots\cup V(f_t)$$

is a factorization into irreducible hyperplanes. Later, will look at irreducible components of an algebraic set.

Corollary 2 *Any hypersurface in $\mathbb{C}^n$ is a union of a finite number of irreducible hypersurfaces*

From before, we also know that f irreducible $\Rightarrow$ f prime $\Rightarrow$ (f) a prime ideal $\Rightarrow$ (f) a radical ideal $\Rightarrow$ the $1-1$ correspondence with $I(V(f))=(f)$ is the radical ideal corresponding to $V(f)$. What is $I(V(f))$? If f is not irreducible, i.e. $f=cf_1^{e_1}\cdots f_t^{e_t}$, a general $\neq 0$ polynomial, then $V(f)=V(f_1)\cup\cdots\cup V(f_t)$, so

$$I(V(f))=I\Big(\bigcup_{k=1}^{t}V(f_k)\Big)=\bigcap_{k=1}^{t}I(V(f_k))=\bigcap_{k=1}^{t}(f_k)=(f_1\cdots f_t)$$

the square-free part of f, which is the gcd since all are irreducible aka primes [taking the radical takes the square-free part].

3.3 $n = 2$...

What are all the closed sets in $\mathbb{C}^2$? Problem: given $f, g \in \mathbb{C}[x, y]$, what can $V(f, g)$ look like? Hint:

$$V(f,g) = V(f) \cap V(g) = \Big(V(f_1) \cup \cdots \cup V(f_t)\Big) \cap \Big(V(g_1) \cup \cdots \cup V(g_s)\Big)$$
$$= \bigcup_{i,j} (V(f_i) \cap V(g_j))$$

Now silly things: the units in $\mathbb{C}[x_1, \ldots, x_n]$ are the nonzero constants $\mathbb{C}^*$, and if f_i and g_j are associates, then $V(f_i) = V(g_j)$ so just a hypersurface. The problem is to solve say the system of equations

$$y - x^3 = 0 \qquad\qquad y^2 + y - 3x = 0.$$

Next time, we'll use *resultants* to solve the general case, the question of how many points do you get (can you get) on $V(f_i) \cap V(g_j)$ if they're not associates? Turns out that the answer is only **finitely many**. For example, $V(xy^2, x + y + 1) = (V(x) \cup V(y)) \cap (V(x+y+1)) = (V(x) \cap V(x+y+1)) \cup (V(y) \cap V(x+y+1)) = \{(0, -1), (-1, 0)\}$. We'll also take a look at *Bezout's Theorem...*

4 28 January

Lemma 8 *if $f, g \in \mathbb{C}[x, y]$ irreducible and not associates, then $V(f, g)$ is finite.*

Before we use resultants to prove this, we have

Corollary 3 *Every algebraic set $X \subset \mathbb{C}^2$, $X \neq \mathbb{C}^2$ has the form*

$$V(f_1) \cup \cdots \cup V(f_n) \cup \{p_1, \ldots, p_m\}$$

where $n, m \geq 0$, $f_i \in \mathbb{C}[x, y]$ irreducible, and $p_j \in \mathbb{C}^2$.

Proof of Lemma $\Rightarrow$ corollary Although this proof is clumsy, next lecture's material on Noetherian topological spaces will make this easier. Say $X = V(I)$, $X \neq \mathbb{C}^2$, pick $f \in I$, $f \neq 0$. Factor f as $f = c \cdot f_1^{e_1} \cdots f_t^{e_t}$. Then last time we saw $X \subset V(f) = V(f_1) \cup \cdots \cup V(f_t)$. But these are not yet the pieces in the corollary, be careful! Question: how do we figure out which of these pieces appear fully in X? If the corresponding irreducible f_i divides everyone in I. Define

$$J = \{j \in \{1, \ldots, t\} : f_j | g \ \forall g \in I\}$$

and say $J = \{j_1, \ldots, j_n\}$. We see now that $V(f_{j_1}) \cup \cdots \cup V(f_{j_n}) \subset X \subset V(f_1) \cup \cdots \cup V(f_t)$ because every $g \in I$ vanishes on $V(f_{j_a})$ $\forall j_a \in J$. Now want to try to say apart from this, there are only finitely many points. If you have $j \in \{1, \ldots, t\}$, $j \notin J$, then $\exists g_j \in I$ such that $f_j \not| g_j$, which means $g_j = \tilde{c} h_1^{q_1} \cdots h_s^{q_s}$ and f_j are not associates with any h_i. This means $X \cap V(f_j)$ is contained in $V(g_j) \cap V(f_j) = \bigcup_{i=1}^s V(g_i) \cap V(f_i)$, and Lemma says each $V(g_i) \cap V(f_i)$ is finite, so $X \cap V(f_i)$ is finite, hence a finite union of finite sets is finite. $\square$ (While this doesn't give us the "trailing" points, the finite set is $\bigcup_{j \notin J, j \in [t]} X \cap V(f_j)$.)

4.1 Resultants

Suppose you have two polynomials $P(x) = a_d x^d + \cdots + a_0$, $Q(x) = b_{d'} x^{d'} + \cdots + b_0$, $a_i, b_j \in \mathbb{C}$. Although we allow the leading coefficients to be 0, we never do this in practice. Question: when do P and Q have a root in common? Want an expression that is *algebraic* in the coefficients (algebraic function for us is a polynomial). We can answer this question by a formula:

$$\mathrm{Res}_x(P,Q) = \det \begin{bmatrix} a_d & a_{d-1} & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ 0 & a_d & a_{d-1} & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & a_d & a_{d-1} & \cdots & a_0 \\ b_{d'} & \cdots & b_0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & b_{d'} & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & b_{d'} & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & b_{d'} & \cdots & b_0 \end{bmatrix}$$

where this $(d+d') \times (d+d')$ matrix is called sometimes the *Sylvester matrix*. Four triangular blocks here. For example, $P(x) = 2x+1$, $Q(x) = 3x^2 + 4x + 5$, then

$$\mathrm{Res}_x(P,Q) = \det \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 3 & 4 & 5 \end{bmatrix} = 15.$$

Facts: (A) If $a_d \neq 0$ or $b_{d'} \neq 0$, then P, Q have common root $\Leftrightarrow$ $\mathrm{Res}_x(P,Q) = 0$.
(B) $\mathbb{C}$ is algebraically closed, so if $P = a_d(x-\alpha_1)\cdots(x-\alpha_d)$, then

$$\mathrm{Res}_x(P,Q) = a_d^{d'} \prod_{i=1}^{d} Q(\alpha_i).$$

(C) If also $Q = b_{d'}(x-\beta_1)\cdots(x-\beta_{d'})$, then

$$\mathrm{Res}_x(P,Q) = a_d^{d'} b_{d'}^{d} \prod_{i,j} (\alpha_i - \beta_j).$$

(D) $\mathrm{Res}_x(Q,P) = (-1)^{dd'} \mathrm{Res}_x(P,Q)$.
(E) Think of P and Q as elements of $\mathbb{C}[a_d, \ldots, a_0, b_{d'}, \ldots, b_0]$, then $\mathrm{Res}_x(P,Q)$ is also in this ring.

Let's prove a strengthening of (A) above.

(A'): Let R be a UFD or a field, and suppose we have P, Q as above with $a_i, b_j \in R$ such that $a_d \neq 0$ or $b_{d'} \neq 0$. Then we can compute

$$\mathrm{Res}_x(P,Q) = 0 \ \Leftrightarrow P, Q \text{ have a non-constant common factor in } R[x].$$

In our use of this strengthening, we'll have $R = \mathbb{C}[y]$. Given two curves, want to know that as y varies, when we fix y and look at the fibers above y under $\pi : (x, y) \mapsto y$, how many solutions do we get (aka, the size of the fibers). Remember, sharing a root over our algebraically closed $\mathbb{C}$ really means sharing the linear factor $(x_i - \alpha_i)$.

Proof of strengthening: By Gauss' lemma, we know that P, Q have a non-constant common factor in $R[x]$ iff they have one in $k[x]$ where k is the fraction field of R. Look at the linear map

$$\psi : k[x]_{<d'} \oplus k[x]_{<d} \to k[x]_{<d+d'}$$

by $(u, v) \mapsto (Pu + Qv)$ where $k[x]_{<m} = \{f \in k[x] : \deg f < m\}$. What's the matrix of this linear map? Well, we have a basis $\{1, x, \ldots, x^d, 1', \ldots, x^{d'}\}$. THen the matrix of ψ is actually that which when we take the determinant we get $\mathrm{Res}_x(P, Q)$. This is because $(x^j, 0) \mapsto x^j P$ and $(1, 0) \mapsto a_0 + a_1 x + \cdots + a_d x^d$ gives columns. If $P = HP'$ and $Q = HQ'$ for some H of degree > 0, then P' and Q' have degree $< d$, $< d'$ respectively and

$$\psi(Q, -P') = PQ' - QP' = HP'Q' - HQ'P' = 0.$$

So $\ker \psi \neq 0$ so $\mathrm{Res}_x(P, Q) = 0$. Conversely, if $\mathrm{Res}_x(P, Q) = 0$ then $\ker \psi \neq 0$ so $(U, V) \in \ker \psi$ so $PU = -QV$. Now because $k[x]$ is a UFD, factorizing you conclude P and Q have a common factor, since $\deg P > \deg V$, some degree must come from A (but using UFD of $k[x]$). $\square$

Proof of Lemma: Let $f, g \in \mathbb{C}[x, y]$ be irreducible and not associates. The case when only x or y occurs in f or g is easy - because one of them $V(f)$, $V(g)$ is then a line, so assume that both x and y occur in both f and g. Gauss' Lemma implies that $f, g \in \mathbb{C}(x)[y]$ are irreducible and not associates. This means that

$$r = \mathrm{Res}_y(f, g) \neq 0.$$

Well, $r \in \mathbb{C}(x) \setminus \{0\}$. Write

$$f = a_d(x)y^d + \cdots, \quad g = b_{d'}(x)y^{d'} + \cdots$$

and then since r is a non-zero polynomial it is clear that $\#\{\alpha \in \mathbb{C} : r(\alpha) = 0\} < \infty$. This implies that

$$\{\alpha \in \mathbb{C} \ : \ a_d(\alpha) \neq 0 \text{ or } b_{d'}(\alpha) \neq 0 \text{ and } r(\alpha) = 0\} < \infty$$

and this implies

$$\{\alpha \in \mathbb{C} : \ a_d(\alpha) \neq 0 \text{ or } b_{d'}(\alpha) \neq 0 \text{ and } \exists \beta \in \mathbb{C} \text{ st } f(\alpha, \beta) = g(\alpha, \beta) = 0\} < \infty,$$

Now removing this condition about not both leading coefficients degenerating can only add at worst finitely many points (finitely many roots of a_d or b_d), then we know

$$\{\alpha \in \mathbb{C} : \ \exists \beta \in \mathbb{C} \text{ st } f(\alpha, \beta) = g(\alpha, \beta) = 0\} < \infty.$$

This allows you to conclude that $V(f,g)$ is finite and same for β, α switched, because $V(f,g)$ is in the product of finite sets. $\square$

Remark: if these polynomials had more variables, $f(x_1,\ldots,x_n)$, $g(x_1,\ldots,x_n)$ irreducible and not associates, then also $\mathrm{Res}_{x_n}(f,g) \in \mathbb{C}[x_1,\ldots,x_{n-1}]$ is not 0. Then the image of $V(f,g) \subset \mathbb{C}^n$ under $\pi_{1\cdots(n-1)}$ projection is contained in a hypersurface. This is proved using the exact same argument. [Elimination Theory]. Towards a big old useful theorem in algebraic geometry: images of algebraic sets under polynomial maps aren't always algebraic sets (not closed maps).

5 2 February

Definition 3 *A ring R is Noetherian if every ideal is finitely generated. Equivalently, R has the ascending chain condition for ideals: any chain $I_1 \subset I_2 \subset \cdots$ stabilizes ($\exists k \in \mathbb{N}$ st $I_k = I_{k+1} = \cdots$).*

Rings that have both ACC and DCC are called Artinian rings.

Lemma 9 *R Noetherian $\Rightarrow$ any quotient R/I is Noetherian.*

Proof: Hint: ideals in I are in bijection with ideals J in R containing I.

Theorem 2 *(R Noetherian) $\Rightarrow$ ($R[x]$ Noetherian).*

Corollary 4 *The rings $\mathbb{C}[x_1,\ldots,x_n]$ are Noetherian since fields are Noetherian.*

For example, $\mathbb{C}[x,y] \supset \mathbb{C}[x,x,y,xy^2,xy^3,\ldots]$ where the rhs is the smallest subring containing all xy^n - subrings of Noetherian rings aren't necessarily Noetherian. Ask ourselves: under what operations are the properties retained? In HNS, bijection between radical ideals and algebraic sets tells us that $\mathbb{C}^n$ is Noetherian (will see this definition later).

Proof of Thm: Let $I \subset R[x]$ be an ideal; for $d \geq 0$ set

$$J_d = \{a \in R : \exists f \in I \text{ with } f = ax^d + l.o.t.\}$$

where l.o.t. stands for "lower-order terms" of course. Easy to check that (a) $\forall d$, $J_d \subset R$ is itself an ideal and (b) $J_0 \subset J_1 \subset J_2 \subset$. Since R is Noetherian, J stabilizes. There is some $n \in N$ where $J_n = J_{n+1} = \cdots$: fix it! Further, each $J_0,\ldots,J_n$ is finitely generated. Pick for each $d = 0,\ldots,n$ elements $f_{d_1},\ldots,f_{d_{m_d}} \in I$ such that $\deg(f_{d_j}) = d$ and leading coefficients a_{d_j} of f_{d_j} generate J_d. Hence $J_d = (a_{d_1},\ldots,a_{d_{m_d}})$ is the ideal of leading coefficients of $f \in I$ of degree d. We claim:

$$I = (f_0,\ldots,f_{0_{m_0}},f_1,\ldots,f_{1_{m_1}},\ldots,f_n,\ldots,f_{n_{m_n}}).$$

This would prove that every ideal is finitely generated, hence completing the proof. *Proof of claim:* The inclusion $\supset$ is clear. To show $\subset$, suppose $f \in I$. Let $d = \deg f$; proof by induction on degree of f.

- $\underline{d = 0}$: $f_{0_j} = a_{0_j}$ because there are no l.o.t. – this is clear (convince yourself).
- $\underline{0 < d \leq n}$: Writing $f = ax^d + l.o.t.$, then $a \in J_d$, so $a = \sum_{j=1}^{m_d} c_j a_{d_j}$ for some $c_j \in R$. Hence
$$f - \sum_{j=1}^{m_d} c_j f_{d_j}$$
cancels off the leading coefficients, hence this has degree $< d$ because the difference in I and $f_{d_j} \in I$ implies $f \in I$.
- $\underline{d > n}$: $a_d = J_d = J_n$ by stabilization, so we can write $a_d = \sum_{j=1}^{m} c_j a_{n_j}$ for some $c_j \in R$, hence $f - \sum_{i=1}^{m_n} c_j x^{d-n} f_{n_j}$ has degree $< d$. $\square$

5.1 Noetherian topological spaces

FIrst, $\mathbb{C}[x_1, \ldots, x_n]$ Noetherian implies A.C.C. for ideals of $\mathbb{C}[x_1, \ldots, x_n]$ which implies A.C.C. for radical ideals of $\mathbb{C}[x_1, \ldots, x_n]$. Then by HNS this implies the D.C.C. for Zariski closed subsets of $\mathbb{C}^n$. This is definitely not like the standard topology on $\mathbb{C}^n$ ($[-1, 1] \supset [-\frac{1}{2}, \frac{1}{2}] \supset \cdots$). Now, some topology for a while.

Definition 4 *A topological space X is called <u>Noetherian</u> iff we have D.C.C. for closed subsets of X.*

Corollary 5 *Zariski topology on $\mathbb{C}^n$ is Noetherian.*

Lemma 10 *Let X be a Noetherian topological space.*
*(1) **Any subset** of X is a Noetherian topological space with the induced topology.*
(2) X is quasi-compact.

Proof of (1) Let $Y \subset X$ be a subset, then $Z \subset Y$ is closed iff $Z = Y \cap T$ for some $T \subset X$ closed. Then $Z = Y \cap \overline{Z}$ where $\overline{Z}$ where $\overline{Z}$ is the closure of Z in X, so if you have $Z_1 \supset Z_2 \supset \cdots$ closed in Y, since taking closures preserves inclusions, then $\overline{Z_1} \supset \overline{Z_2} \supset \cdots$ in X, but X Noetherian implies $\overline{Z_n} = \overline{Z_{n+1}} = \cdots$ which implies by remark $Z_t = Y \cap \overline{Z_t}$ that $Z_n = Z_{n+1} = \cdots$. $\square$

Proof of (2) Note that "quasi-compact means compact as we know it: every open cover has a finite sub-covering (many people use compact to mean quasi-compact and Hausdorff). Combining (1) and (2) tells us that every subset is quasi-compact! Suppose that the open covering $X = \bigcup_{i \in I} U_i$ has no finite subcovering. Then inductively choose $i_1 \in I$ with $U_{i_1} \neq \emptyset$, then $i_2 \in I$ with $U_{i_2} \not\subset U_{i_1}$, then $i_3 \in I$ with $U_{i_3} \not\subset (U_{i_1} \cup U_{i_2})$, and so on. Set $V_k = \bigcup_{j=1}^{k} U_{i_j}$, so $Z_k = X \setminus V_k$ is an infinite decreasing chain of closed subsets, a contradiction. $\square$

Noetherian is much stronger than quasi-compact.

Definition 5 *A topological space X is called irreducible if $X \neq \emptyset$ and $X = Z_1 \cup Z_2$ with Z_i closed, $Z_i \neq X$ for $i = 1, 2$, then either $X = Z_1$ or $X = Z_2$. A subset of a topological space is irreducible if it is irreducible space with it's induced topology. Finally, $S \subset X$ is an irreducible component of X if S is an irreducible subset of X* ***maximal*** *wrt inclusion.*

In $\mathbb{R}$ in the usual topology, only points are irreducible. [Compare all of this to connectedness].

Facts: Let X be a topological space.

- (a) $Y \subset X$ is irreducible $\Rightarrow \overline{Y} \subset X$ irreducible.
- (b) irreducible components of X are closed.
- (c) any point of X is contained in an irreducible component.

The proof of (c) uses Zorn's lemma, much like every ring has a maximal ideal. Examples: $\mathbb{C}^n$ with the usual topology is definitely not irreducible (can separate any pair of points by a hyperplane). Irreducible components are the singletons here; say reducible = not irreducible. On the other hand, $\mathbb{C}^n$ with the Zariski topology is irreducible. If $\mathbb{C}^n = Z_1 \cup Z_2$ and neither $Z_1, Z_2 = \mathbb{C}^n$, then

$$(\overset{n}{\mathbb{C}} \setminus Z_1) \cap (\overset{n}{\mathbb{C}} \setminus Z_2) = \emptyset$$

is a contradiction, since in a Noetherian topological space any two non-empty opens have a non-empty intersection. [See the Stacks project topology chapter].

Lemma 11 *In the Zariski topology on $\mathbb{C}^n$, for algebraic sets $X = V(I)$ where I is a radical ideal, we have X irreducible if and only if I is a prime ideal.*

Proof: say $V(I)$ is not irreducible. The only way $V(I) = \emptyset$ is when I is the unit ideal (weak HNS), so it's not prime. If $V(I) \neq \emptyset$, then by contradiction assume we can decompose it into $V(I) = V(I_1) \cup V(I_2)$ where neither $V(I_i) = V(I)$ for $i = 1, 2$. Then we also know $V(I_1) \cup V(I_2) = V(I_1 I_2)$ so this means $I \supset I_1 I_2$. Can't say $\subset$ because the product of radical ideals is not necessarily radical. Then if I were prime, either $I_1 \subset I$ or $I_2 \subset I$. [**Algebraic fact:** if $\mathfrak{p}, I, J$ ideals, $\mathfrak{p}$ prime, then $\mathfrak{p} \supset I \cdot J \Rightarrow \mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$.] So then $V(I) \subset V(I_1)$ or $V(I) \subset V(I_2)$, which is a contradiction! On the other hand, suppose $V(I)$ is irreducible. We want to show I is prime. Then say $f, g \in I$ with $f, g \in \mathbb{C}[x_1, \ldots, x_n]$. Then $V(I) \subset V(fg) = V(f) \cup V(g)$ but this implies

$$V(I) = \Big(V(I) \cap V(f)\Big) \cup \Big(V(I) \cap V(g)\Big)$$

which implies (i) that $V(I) = V(f)$ or $V(g)$ hence $f \in I$ or $g \in I$ since I is radical.$\square$. Preview of what's going to happen: $V(xy(x-1), xy(y-1)) = X$ has irreducible components x-axis, y-axis, and the point $(1, 1)$... unique decomposition?

6 4 February

Theorem 3 *Any Noetherian topological space has finitely many irreducible components $X = Z_1 \cup \cdots \cup Z_n$ with each Z_i closed, irreducible and $Z_i \not\subset \bigcup_{j\neq i} Z_j$; further, up to permutation, this decomposition is unique.*

Note that for the anti-containment condition, it suffices to check $Z_i \not\subset Z_j \ \forall j \neq i$. Remark: since $Z_i \not\subset \bigcup_{j\neq i} Z_j$ by irreducibilty, therefore

$$Z_i \setminus Z_i \cap \Big(\bigcup_{j\neq i} Z_j\Big) = X \setminus \bigcup_{j\neq i} Z_j.$$

While this is an easy inequality, LHS is non-empty and RHS is open, hence every irreducible component of a Noetherian space X contains a non-empty open of X (SO not true in $\mathbb{R}^n$). [Interesting finite topological spaces: all of them are Noetherian.]

Proof of Theorem: we proceed by "Noetherian induction" . Well, we have the DCC for closeds in Noetherian topological spaces. It turns out that "any nonempty collection of closed subsets of X has a minimal element" is equivalent to this DCC for closeds. Let's begin the proof. Let

$$\mathcal{Z} = \{Z \subset X \text{ closed st } Z \text{ has } \infty\text{ly many irreducible components}\}.$$

We want to show $\mathcal{Z} = \emptyset$. By contradiction, take $\mathcal{Z} \neq \emptyset$, it has a minimal element, say $Z \in \mathcal{Z}$. Then Z is not irreducible, otherwise if it were the ! irreducible component, it would contradict membership in $\mathcal{Z}$. Hence, decompose $Z = Z_1 \cup Z_2$, $Z_1 \neq Z$, $Z_2 \neq Z$, so $Z_1, Z_2 \notin \mathcal{Z}$ since Z was minimal. Then $Z_1 = Z_{1,1} \cup \cdots \cup Z_{1,n}$ and $Z_2 = Z_{2,1} \cup \cdots \cup Z_{2,m}$. But then the next lemma will furnish the contradiction (think). [Formal Zorn's Lemma thing says any p is in an irreducible component.][4]

Lemma 12 *X top. space, $Z, Z_1, \ldots, Z_n$ closed, $Z_1, \ldots, Z_n$ irreducible and $Z = Z_1 \cup \cdots \cup Z_n$, then any irreducible component of Z is one of the $Z_1, \ldots, Z_n$.*

Proof: $T \subset Z$ an irreducible component, $T \subset \bigcup_{i=1}^n Z_i$ then since T is irreducible $T \subset Z_i$ for some i. Hence, by definition of an irreducible component, T is a maximal irreducible subset, so Z_i irreducible means $T = Z_i$. Exercise: prove uniqueness up to permutation. $\square$.

Remark: actually it follows that you obtain the irreducible components of $Z = Z_1 \cup \cdots \cup Z_n$ as in the Lemma by discarding any Z_i if it is contained in Z_j for some $j \neq i$.

[4] As an alternate proof, once we have $Z_1 \cup Z_2 = Z$, can we say by pigeonhole principle that if Z has ∞ly many irreducible components then so must one of the Z_i for $i = 1, 2$, contradicting minimality of Z?

6.1 Application to Algebraic Sets

Our ($\mathbb{C}^n$, Zariski) is Noetherian topological space because $\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian. For all algebraic sets $X = V(I) \subset \mathbb{C}^n$, we have a ! decomposition (up to permutation) $X = V(I) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_m)$ with $\mathfrak{p}_i \subset \mathbb{C}[x_1, \ldots, x_n]$ prime ideals and not redundant (no inclusions $V(\mathfrak{p}_i) \subset V(\mathfrak{p}_j)$ if $i \neq j$). If I is radical, then we conclude $I = I(X) = I(V(I))$, but this is

$$I(X) = I(V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_m) = I(V(\mathfrak{p}_1)) \cap \cdots \cap I(V(\mathfrak{p}_m)) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$$

since $\mathfrak{p}_i$ prime ideals are radical. This implies that radical ideal in $\mathbb{C}[x_1, \ldots, x_n]$ is the intersection of finitely many prime ideals; this is unique if we have eliminated redundancies. NB: essential to have $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$ and not $\mathfrak{p}_1 \cdots \mathfrak{p}_m$ multiplied (something about Dedekind domains).

Example: if $f \in \mathbb{C}[x_1, \ldots, x_n]$ is non-zero then it factors $f = cf_1^{e_1} \cdots f_t^{e_t}$ and then $V(f) = V(f_1) \cup \cdots \cup V(f_t)$ IS the decomposition into irreducible components. We can also write this as $V(f) = V((f_1)) \cup \cdots \cup V((f_t))$ where the $V((f_i))$ are prime ideals since the f_i are irreducible.

Corollary 6 *Irreducible components of hypersurfaces are also hypersurfaces.*

This corresponds to the prime factors of the defining equation. Prime decomposition of ideal (radical) is harder than factoring polynomials. Singletons are irreducible, so closed subsets of $\mathbb{C}^2$ Zariski, we remember that we can uniquely decompose up to permutation our algebraic sets into finitely many points and hyperplanes, and we showed these were irreducible, so we're done - we can conclude $\mathbb{C}^n$ is Noetherian.

6.2 Algebraic Facts

Definition 6 *An affine variety is an irreducible algebraic set $X \subset \mathbb{C}^n$*

We'll do something with these soon – these are the objects; will find out the morphisms later [skip Fulton's polynomial maps. Now some algebra. Let $\varphi : R \to S$ be a ring map.

Definition 7 *We say φ is of finite type or that S is a finitely-generated R-algebra if and only if $\exists s_1, \ldots, s_n \in S$ which generate S as an R-algebra.*

That is, $\forall s \in S, \exists \{a_I\} \subset R$ almost all 0 such that

$$s = \sum_{I=(i_1,\ldots,i_n)} \varphi(a_I) s_1^{i_1} \cdots s_n^{i_n}.$$

Definition 8 *$s \in S$ is called integral over R if $\exists$ a **monic** polynomial $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in R[x]$ such that $f(s) = 0$, i.e.,*

$$s^d + \varphi(a_{d-1})s^{d-1} + \cdots + \varphi(a_0) = 0$$

in S.

Definition 9 *We say S is integral over R iff every $s \in S$ is integral over R.*

Definition 10 *$\varphi : R \to S$ is called finite iff S is finitely generated as an R-**module**.*

That is, $\exists s_1, \ldots, s_N \in S$ such that $\forall s \in S$, we can write

$$s = \varphi(a_1)s_1 + \cdots + \varphi(a_N)s_N$$

for some $a_1, \ldots, a_N \in R$. Compared to (1), here we only take linear combinations of the s_i.

Facts:

- (a) ($R \to S$ finite) $\Leftrightarrow$ ($R \to S$ is integral and of finite type)
- (b) Given $\varphi : R \to S$, the set $S' = \{s \in S : s \text{ is integral over } R\}$ is an R-subalgebra of S. This is called the integral closure of R in S.
- (c) If $\varphi : R \to S$, $s_1, \ldots, s_n \in S$ given, each s_i is integral over R, and $s_1, \ldots, s_n$ generate S as an R-algebra, then S is finite over R.
- (d) Compositions of integral ring maps are integral.
- (e) Compositions of finite ring maps are finites.

See exercises in the Algebra chapter in the Stacks project. For example,

$$S = \mathbb{C}[x, y]/(x^2 + 5, y^2 + y)$$

with $R = \mathbb{C}$ is generated by $s_1 = \overline{x}$ and $s_2 = \overline{y}$ as an R-algebra but by $1, \overline{x}, \overline{y}, s_1 s_2$ as an R-module. They key implications in all of this we'll do in the homework.

How are "finite' and "integral" related to the topology of algebraic sets? Tune in next time! Or scroll down.

7 9 February

Proposition 3 *$X \subset \mathbb{C}^{n+m}$ an algebraic set, $\pi : X \to \mathbb{C}^n$ the projection. Assume $\forall 1 \leq j \leq m$ there is some*

$$f_j = (x_{n+j})^{d_j} + \sum_{i<d_j} \alpha_{j_i}(x_1, \ldots, x_n)x_{n+j}^i$$

in the ideal $I(X)$. Then (a) all the fibres of π are finite and (b) $\pi : X \to \mathbb{C}^n$ is a proper continuous map in the usual topology.

Proof of (a): prescribing $x_1, \ldots, x_n$ at a fibre, so $\exists$ finitely many solutions; at most d_j – [substitute $(a_1, \ldots, a_n) \in \mathbb{C}^n$; $\pi^{-1}(a) = \{z \in X \ : z_1 = a_1, \ldots, z_n = a_n\}$ so

$$\pi^{-1}(a) \subset \{(a_1, \ldots, a_n, b_1, \ldots, b_m) \in \mathbb{C}^{n+m} \ : (b_j)^{d_j} + \sum_{i<d_j} \alpha_{i,j}(a_1, \ldots, a_n) b_j^i = 0\}.$$

Now, the left hand side is finite since the right hand side is, because $\forall j$, $b_j \in \mathbb{C}$ satisfies a monic equation of degree d, so there are at most $d_1 \cdots d_m$ solutions. (?)

Proof of (b): In $\mathbb{C}^n$, subsets are compact iff they are closed and bounded. $K \subset \mathbb{C}^n$ is compact implies $\exists C_1 > 1$ such that $\forall a = (a_1, \ldots, a_n) \in K$ we have $|a_i| \leq C_1$. This implies $\exists C_2 > 0$ such that $\forall a = (a_1, \ldots, a_n) \in K$, $|\alpha_{ij}(a_1, \ldots, a_n)| \leq C_2$. This means that if $z = (a_1, \ldots, a_n, b_1, \ldots, b_m) \in \pi^{-1}(K)$ then

$$\left|b_j^{d_j}\right| \leq \sum_{i<d_j} C_2 |b_j|^i \leq d_j C_2 \max\{|b_j|^{d-1}, 1\} \leq d_j C_2 C_1^{d-1} \leq C_3$$

so $\pi^{-1}(K)$ is bounded. Now, π is continuous so $\pi^{-1}(K)$ is closed in X; since X is closed in $\mathbb{C}^{n+m}$, we have transitively $\pi^{-1}(K)$ closed in $\mathbb{C}^{n+m}$, hence plus bounded means compact $\square$.

Remark: the converse of the proposition is also true:

(a) if $X \subset \mathbb{C}^n$ is an algebraic set, and bounded, then it's compact in the *usual* topology. (b) if $X \subset \mathbb{C}^{n+m}$ and $\pi : X \to \mathbb{C}^n$ the projection is proper, then such f_j as in the proposition do exist (the proof of this is too hard). We can do (a) after some dimension theory. Also, a remark unrelated to above: if $X \subset \mathbb{C}^n$ is al algebraic set, $X \neq \mathbb{C}^n$, then X is nowhere dense in the usual topology (this is weaker than measure-zero comment)...

7.1 Criterion for Finiteness in "our" case

Proposition 4 *Suppose we have a $\mathbb{C}$-algebra map $\psi : \mathbb{C}[y_1, \ldots, y_s] \to \mathbb{C}[x_1, \ldots, x_t]$[5] and suppose we have an ideal $I \subset \mathbb{C}[x_1, \ldots, x_t]$. Then the ring map $\mathbb{C}[y_1, \ldots, y_s] \to \mathbb{C}[x_1, \ldots, x_t]/I$ is finite if and only if $\exists$ monic polynomials*

$$f_i = T^{d_i} + \sum_{j<d_i} g_{ij} T^j, \quad g_{ij} \in \mathbb{C}[y_1, \ldots, y_s]$$

such that $f_i(x_i) = x_i^{d_i} + \sum \psi(g_{ij}) x_i^j \in I$ for $1 \leq i \leq t$.

Recall that $R \to S$ is finite iff $\exists g_1, \ldots, g_n \in S$ which generates S as an R-module. NB: this says the hypothesis preceding is equivalent to $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_{n+m}]/I$ being finite. Recall: criterion last time: generators of target are finitely generated;

[5] we just have to specify $\psi(y_j)$ $\forall 1 \leq j \leq s$ to give a map, since $1 \mapsto 1$.

each one satisfying a monic equations; finite implies int...

Proof: $R = \mathbb{C}[y_1, \ldots, y_s] \to S = \mathbb{C}[x_1, \ldots, x_t]/I$. Then S is generated by $\overline{x_1}, \ldots, \overline{x_t}$ over $\mathbb{C}$, so a fortiori over R. The existence of the polynomials f_i implies $\overline{x_i}$ is integral over R, so by the algebraic fact (c) from last time, S is finite over R. Conversely, if $R \to S$ is finite, it's integral, and so each $\overline{x_i}$ satisfies a monic equation, which exactly translates into the existence of the f_i. Note that the proof doesn't use $I = I(X)$ is radical. $\square$

7.2 Noether Normalization

Theorem 4 *Noether Normalization Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then there exists a linear change of coordinates $y_1 = \sum a_{1i}x_i$, ..., $y_n = \sum a_{ni}x_i$, a matrix $[a_{ji}]$ invertible for this change of coordinates, and $0 \leq d \leq n$ such that*

$$\begin{array}{ccc} \mathbb{C}[y_1, \ldots, y_d] & \longrightarrow & \mathbb{C}[y_1, \ldots, y_n] = \mathbb{C}[x_1, \ldots, x_n] \\ & \overset{\psi}{\searrow} \quad \nearrow & \\ & \mathbb{C}[x_1, \ldots, x_n]/I & \end{array}$$

such that ψ is finite and injective.

What does this mean for algebraic sets? $X \subset \mathbb{C}^n$ an algebraic set, then $\exists$ a projection $\mathbb{C}^n \to \mathbb{C}^d$ onto the first d coordinates (after a linear change of coordinates) such that π is proper. For ψ being a finite ring map implies π is proper; injective will later turn out that in this situation, ψ injective also guarantees ψ surjective. X gives a covering of $\mathbb{C}^d$, maybe with ramification[6]. First, an example: $xy = 1$ is unbounded in $B(0, \epsilon) \subset \mathbb{C}$; we have the change of coordinates $x = u + v$, $y = u - v$, then $(u + v)(u - v) = u^2 - v^2 = 1$ then π to the u axis works (because complex); because $u^2 - v^2 = 1$ is monic in V. Basically, the following Lemma is needed first:

Lemma 13 *Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ be nonzero. There exists a linear change of coordinates $y_1, \ldots, y_n$ such that f is monic in y_n over $\mathbb{C}[y_1, \ldots, y_{n-1}]$.*

Proof: Let f_i be the part of f which is homogeneous of maximal total degree. Consider $x_1 = y_1 + \lambda_1 y_n$, ..., $x_n = \lambda_n y_n$. This change is invertible as long as $\lambda_n \neq 0$. Then $f_d(x_1, \ldots, x_n) = f_d(\lambda_1, \ldots, \lambda_n)y_n^d + \text{l.o.t. in } y_n$ since we picked $f_d \neq 0$ – can find some $\mu_1, \ldots, \mu_n$ in $\mathbb{C}$ with $\mu_n \neq 0$ such that $f_d(\mu_1, \ldots, \mu_n) \neq 0$, then set $\lambda_i = t\mu_i$ with $t \in \mathbb{C} \setminus \{0\}$ such that $t^d f_d(\mu_1, \ldots, \mu_n) = 1$ which is equal to $f_d(\lambda_1, \ldots, \lambda_n)$ because f is homogenous of degree d. Since $f = f_0 + f_1 + \cdots + f_d$, highest degree occurrence of y_n happens in f_d, so we win! $\square$

With this Lemma, it's easy to prove Noether Normalization.

[6]What is this?

Proof given $\mathbb{C}[x_1, \ldots, x_n] \supset I$, induct on n. If $n = 1$, then either $I = (0)$, which means $x_1 = y_1$, $d = 1$ works, since $\mathbb{C}[y_1] \hookrightarrow \mathbb{C}[x_1]/I$ is finite, or $I \neq 0$ - then pick $f \in I, f \neq 0$, and rescale to make it monic. Then $\mathbb{C} \to \mathbb{C}[x_1]/I$ works.

For $n > 1$, if $I = (0)$, then $d = n$, $y_i = x_i$ works. If $I \neq 0$, pick $f \in I \setminus \{0\}$. By the Lemma, there exists $y_1, \ldots, y_n$ a linear change of coordinates so that f is monic in y_n over $\mathbb{C}[y_1, \ldots, y_{n-1}]$. This means $\mathbb{C}[y_1, \ldots, y_{n-1}] \to \mathbb{C}[y_1, \ldots, y_n]/I$ is finite by the criterion above. It's not injective, however, so $J \subset \mathbb{C}[y_1, \ldots, y_{n-1}]$ the kernel; apply induction to this; $J = I \cap \mathbb{C}[y_1, \ldots, y_{n-1}] = \{g \in \mathbb{C}[y_1, \ldots, y_{n-1}] :$ map to 0 in $\mathbb{C}[y_1, \ldots, y_n]/I\}$ then $\alpha : \mathbb{C}[x_1, \ldots, x_{n-1}]/J \to \mathbb{C}[y_1, \ldots, y_n]/I$ the same criterion applies to maps like this, when LHS isn't necessarily a polynomial ring. By Induction hypothesis, we can find a linear change of coordinates $z_1, \ldots, z_{n-1}$ of $y_1, \ldots, y_{n-1}$ and $d_0 \in \mathbb{Z}$ such that

$$\beta : \mathbb{C}[z_1, \ldots, z_d] \to \mathbb{C}[z_1, \ldots, z_{n-1}]/J = \mathbb{C}[x_1, \ldots, x_n]/J$$

is injective and finite. Then $\alpha \circ \beta : \mathbb{C}[z_1, \ldots, z_d] \to \mathbb{C}[y_1, \ldots, y_n]/I$ is a composition of injective and finite maps and hence is injective and finite. $\square$

In fact, d ends up being the dimension of the algebraic set; hence, we can always find $n - d$ polynomials that cut it out. Given a $d \times n$ matrix, of ful rank, add $n-d$ vectors for the rest of coordinates (take $z_n = y_n$); over $\overline{\mathbb{F}_p}$, doesn't always work...

8 11 February

Definition 11 *Let $X \subset \mathbb{C}^n$ be an algebraic set. The coordinate ring of X is the ring $\Gamma(X) := \mathbb{C}[x_1, \ldots, x_n]/I(X)$.*

Fulton only makes this definition when X is an affine variety (aka when $I(X)$ is a prime ideal).

Lemma 14 *If $X \subset \mathbb{C}^{n+m}$ is an algebraic set such that the map*

$$\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_{n+m}] \to \Gamma(X)$$

is finite, then the map $\pi : X \to \mathbb{C}^n$ by $(z_1, \ldots, z_{n+m}) \mapsto (z_1, \ldots, z_n)$ maps Zariski closed sets to Zariski closed sets (π is a closed map in the Zariski topology).

Remark: proper maps between locally compact spaces are always closed in the usual topology. Zariski closed is better. In particular, $\pi(X) \subset \mathbb{C}^n$ is closed. This doesn't work for arbitrary projections.

- Examples to see that the associated ring map isn't finite for an arbitrary projection. COnsider $X = V(xy - 1)$, $X \to \mathbb{C}$ the projection by $(x, y) \mapsto x$. Then $\Gamma(X) = \mathbb{C}[x, y]/(xy - 1)$, and $\mathbb{C}[x] \to \Gamma(X)$ is not finite as a ring map. Think of $\mathbb{C}[x, y]/(xy - 1)$ as $\mathbb{C}[x, \frac{1}{x}]$. This is saying that $\mathbb{C}[x, \frac{1}{x}]$ is not finite as a $\mathbb{C}[x]$-module. Why? For $f_1, \ldots, f_t \in \mathbb{C}[x, \frac{1}{x}]$, can write $f_i = \frac{g_i}{x^{n_i}}$ for some $g_i \in \mathbb{C}[x]$, then $\frac{1}{x^{\max(n_i)+1}} \in \mathbb{C}[x, \frac{1}{x}]$ is not in the $\mathbb{C}[x]$-module generated by $f_1, \ldots, f_t$.

Proof of Lemma: Let $Y \subset X$ be Zariski closed. Then $\Gamma(X) \to \Gamma(Y)$ is surjective, because $I(Y) \supset I(X)$ and a surjective map is finite, so the composition $\mathbb{C}[x_1, \ldots, x_n] \to \Gamma(Y)$ is a composition of finite ring maps, hence finite. Thus, we just have to prove for X. We want to show that $\pi(X) \subset \mathbb{C}^n$ is Zariski closed. Show that the complement is open. Choose $a \in \mathbb{C}^n \setminus \pi(X)$. By the weak Hilbert Nullstellensatz, we know $(x_1 a_1, \ldots, x_n - a_n) + I(X) = \mathbb{C}[x_1, \ldots, x_{n+m}]$, and note that we are seeing the left most ideal as generated in the ring $\mathbb{C}[x_1, \ldots, x_{n+m}]$. This means that

$$\sum_{i=1}^{n} (x_i - a_i)\Gamma(X) = \Gamma(X)$$

a decomposition of modules in *both* $\mathbb{C}[x_1, \ldots, x_{n+m}]$ and $\mathbb{C}[x_1, \ldots, x_n]$. Note that this is not $\bigoplus$. By Nakayama's Lemma, which we will prove later, which uses the fact that $\Gamma(X)$ is finite over $\mathbb{C}[x_1, \ldots, x_n]$, we know $\exists f \in \mathbb{C}[x_1, \ldots, x_n]$ of degree only up to n with

$$f = 1 + \sum f_i (x_i - a_i)$$

with $f_i \in \mathbb{C}[x_1, \ldots, x_n]$ such that $f \cdot \Gamma(X) = 0$. This implies $f \in I(X)$. Now, we have an equation for X that depends only on the first n variables, and $f(a) = 1$, $f \in \mathbb{C}[x_1, \ldots, x_n]$. This implies $\pi(X) \subset V(f)$ and $a \notin V(f)$ because if $z \imath n X$, $z = (z_1, \ldots, z_{n+m})$, then $f(z_1, \ldots, z_{n+m}) = 0$ but the f is really $f(z_1, \ldots, z_n) = 0$. This means $\mathbb{C}^n \setminus V(f)$ is an open region of a not meeting $\pi(X)$.

Lemma 15 *(Nakayama's Lemma, first form): Let R be a ring, $I \subset R$ an ideal, M an R-module; assume M is finite over R and $I \cdot M = M$. Then $\exists f \in R$, $f = 1 + x$, $x \in I$, such that $f \cdot M = 0$, i.e., $fm = 0$ $\forall m \in M$.*

Note that we applied this when $R = \mathbb{C}[x_1, \ldots, x_n]$, the ideal is $(\{x_i - a_i\}_{i=1}^n)$; and f is an annihilator of the module.

Proof: M finite over R implies $\exists m_1, \ldots, m_r \in M$ such that $M = \langle m_1, \ldots, m_r \rangle$, $M = Rm_1 + \cdots + Rm_r$. Note, we use regular "+" not $\oplus$ because it is not a decomposition; there might be relations among the m_j. The condition $IM = M$ means that every $m \in M$ is a sum $m = \sum x_j n_j$ for $x_j \in I$, $n_j \in M$. [In our case, I was finitely generated]. but these n_j are themselves linear combos of the m_i, so we can write any $m \in M$ as a linear combo

$$m = \sum x_j n_j = \sum x_j \big(\sum r_{jl} m_l \big) = \sum_l \Big(\sum_j (x_j r_{jl}) \Big) m_l = \sum y_l m_l$$

for some $y_l \in I$. This is true $\forall m \in M$, so in particular, m_i! $l \mapsto j$ just change dummy variable in what follows:

$$m_i = \sum_j y_{ij} m_j$$

with $y_{ij} \in I$. Let $f = \det[\lambda I_{r\times r} - (y_{ij})] = p(1)$. Observe that $f = 1 + x$ for some $x \in I$; moding out by the ideal gives the identity matrix! Also, $f \cdot I = T^{adj}T$, where T is the matrix above and the adjoint is a matrix with coefficients in R. We want to show $f \cdot M = 0$. Prove first for generators: tricky – convince yourself. $f = \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = fI_{n\times n} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = T^{adj}T \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = T^{adj} \cdot \tilde{T} = 0$ since

$$\tilde{T} = \begin{pmatrix} m_1 - y_{11}m_1 - y_{12}m_2 \cdots - y_{1r}m_r \\ \vdots \\ -y_{r1}m_1 - \cdots - y_{rr}m_r + m_r \end{pmatrix}$$

is the zero column vector. This is true for all $1 \leq i \leq r$, so $\forall m \in M$, $fm = 0$ because m is a linear combination of the generators m_i. $\square$

Lemma 16 *If $X \subset \mathbb{C}^{n+m}$ is an algebraic set, $\mathbb{C}[x_1, \ldots, x_n] \to \Gamma(X)$ finite and injective, then $\pi : X \to \mathbb{C}^n$ is surjective.*

Proof: by the previous lemma, $\pi(X) \subset \mathbb{C}^n$ is Zariski closed. If $\pi(X) \neq \mathbb{C}^n$, then $\pi(X) \subset V(f)$ for some $f \neq 0$, $f \in \mathbb{C}[x_1, \ldots, x_n]$. Then $f \in \mathrm{Ker}(\mathbb{C}[x_1, \ldots, x_n]) \to \Gamma(X))$ but that means $\to 0$ in $\Gamma(X)$, a contradiction. $\square$

Lemma 17 *If $X \subset \mathbb{C}^n$ is Zariski closed and bounded, then $\#X < \infty$.*

Proof: Pick a linear map $\mathbb{C}^n \to \mathbb{C}^d$ such that the associated map $\pi : X \to \mathbb{C}^d$ satisfies the conclusions of Noether Normalization, i.e., $\mathbb{C}[x_1, \ldots, x_d] \to \Gamma(X)$ is injective and finite. Then π is surjective (by the Lemma above) and has finite fibers (previous proposition 2/9). We're done because $\mathbb{C}^d$ is bounded iff $d = 0$ (equivalent to a ring map being finite). Next time: transcendence degree of field extensions, then relate to d.

9 16 February

9.1 Transcendence Degree of Field Extensions

Definition 12 *Let $K \subset L$ be a field extension. Note that ring maps of fields are always injective.*

- *(a) we say $K \subset L$ is a finitely-generated field extension iff $\exists$ finitely many $t_1, \ldots, t_n \in L$ such that any $x \in L$ is of the form $x = \frac{P(t_1,\ldots,t_n)}{Q(t_1,\ldots,t_n)}$ with $P, Q \in K[x_1, \ldots, x_n]$ and $Q(t_1, \ldots, t_n) \neq 0$. Think subfields generated by $t_1, \ldots, t_n$.*
- *(b) Given $t_1, \ldots, t_r \in L$, we say that $t_1, \ldots, t_r$ are algebraically independent over K if $\forall P \in K[x_1, \ldots, x_r]$ we have $P(t_1, \ldots, t_r) = 0 \Rightarrow P = 0$ as a polynomial.*

- *(c) A transcendence basis for L/K is $t_1, \ldots, t_r \in L$ which are algebraically independent over K, and such that any $t \in L$ is algebraic over $K(t_1, \ldots, t_r)$, in other words, $t_1, \ldots, t_r, t$ are not algebraically independent.*
- *(d) The transcendence degree of L/K is the cardinality of a transcendence basis.*

Facts (not proved in course):

- (a) TD is well defined.
- (b) If L can be generated as a field over K by r elements, then tr $\deg_K L \leq r$.
- (c) if $K \subset L \subset M$ then $\text{trdeg}_K(M) = \text{trdeg}_K(L) + \text{trdeg}_L(M)$.
- (d) if L/K is finitely generated and $t_1, \ldots, t_r$ is a trans basis, then

$$K \subset K(t_1, \ldots, t_r) \subset L$$

is a chain of first a purely transcendental field extension and then secondly a finite extension; this means that $K(t_1, \ldots, t_r)$ is the quotient field of a polynomial ring over K; no relations among $t_1, \ldots, t_r$.[7] Compare to finite extension case: if $K \subset L \subset M$ are finite field extensions, then $[M : K] = [M : L] \cdot [L : K]$ is multiplication. Recall: $K \subset L$ a finite field extension iff $K \subset L$ is a field extension and $K \to L$ is finite as a ring map. Also, the example $\mathbb{Q} \subset \overline{Q}$ is infinite extension with transcendence degree zero! infinitely many $\sqrt{p}$ prime; think ALGEBRAIC closure.

Definition 13 *If $X \subset \mathbb{C}^n$ is an affine variety, then its function field, or its field of rational functions, is $\mathbb{C}(X)$ the quotient field of $\Gamma(X)$ the coordinate ring, which is a domain since $I(X)$ is prime, so we can do this quotient construction.*

Lemma 18 *$\mathbb{C}(X)$ is a finitely generated field extension of $\mathbb{C}$.*

Proof: we have $\Gamma(X) = \mathbb{C}[x_1, \ldots, x_n]/I(X)$, so the images $t_i = x_i \bmod I(X)$ generate $\Gamma(X)$ as a $\mathbb{C}$-algebra. Then of course $t_1, \ldots, t_n$ generate $\mathbb{C}(X)$ the f.f. of $\Gamma(X)$. Additionally, tr $\deg_{\mathbb{C}} \mathbb{C}(X) \leq n$. $\square$

Definition 14 *the dimension of an affine variety X is $\text{trdeg}_{\mathbb{C}} \mathbb{C}(X)$. We say X is a curve or surface or threefold etc if* $\dim X = 1, 2, 3 \ldots$.

An algebraic curve is an affine variety of dimension 1.

Definition 15 *Dimension of an algebraic set $X \subset \mathbb{C}^n$ is the maximum of* $\dim X_i$ *when X_i are the irreducible pieces of $X = X_1 \cup \cdots \cup X_t$.*

Examples:

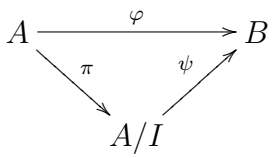
[7] Algebraic Geometry Question: can you make the second $\subset$ an $=$? How low can you make the finite part?

- $\dim \mathbb{C}^n = n$.
- dim of an affine plane curve is 1. This means $C = V(f) \subset \mathbb{C}^2$ where $f \in \mathbb{C}[x, y]$ is irreducible which means $\Gamma(C) = \mathbb{C}[x, y]/(f)$. Without loss of generality assume $y \in (f)$. Then we show that the transcendence degree is 1 over $\mathbb{C}$. Then the map $\mathbb{C}[x] \to \mathbb{C}[x, y]/(f)$ is injective. If $g(x) \in \ker$, then $g(x) = f \cdot h$, but g is purely a polynomial in x and so the f contributes a y that h cannot possibly undue. OTher way: use $f \in \mathbb{C}[x, y]$ irreducible then Gauss' lemma to show $f \in \mathbb{C}(x)[y]$ still irreducible (?). This implies x is algebraically independent over $\mathbb{C}$ in $\mathbb{C}(C)$. So we get an injective map of fraction fields (induced): $\mathbb{C}(x) \to \mathbb{C}(C)$ a map of fields so its injective. This field is generated as a field over $\mathbb{C}$ by x and y so its generated over $\mathbb{C}(x)$ by just y. Moreover, y is algebraic over $\mathbb{C}(x)$ by assumption because $f(x, y) = 0$, so this is a finite extension $[\mathbb{C}(C) : \mathbb{C}(x)] < \infty$. So $\operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(C) = \operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(x) + \operatorname{trdeg}_{\mathbb{C}(x)} \mathbb{C}(C) = 1 + 0 = 1$.
- Example: a hypersurface in $\mathbb{C}^n$ has dimension $n - 1$. We've seen that a hypersurface is a union of irreducible hypersurfaces, and if $f \in \mathbb{C}[x_1, \ldots, x_n]$ is irreducible, then $\operatorname{trdeg}_{\mathbb{C}}(f.f. \mathbb{C}[x_1, \ldots, x_n]/(f)) = n-1$ - same as before: WLOG x_n occurs in (f), then $\mathbb{C} \hookrightarrow \mathbb{C}(x_1, \ldots, x_{n-1}) \hookrightarrow \mathbb{C}(V(f))$. If $g(x_1, \ldots, x_n) \in (f)$, then $g(x_1, \ldots, x_{n-1}) = f \cdot h$, then a product of elements imposes one relation on $x_1, \ldots, x_n$.

The link: let $X \subset \mathbb{C}^n$ be an algebraic set. Let $\pi : X \to \mathbb{C}^d$ be the one projection you get from Noether normalization. Then $d = \dim X$. Proof: let $X = X_1 \cup \cdots \cup X_r$ be the irreducible components. Then

- $\psi : \mathbb{C}[x_1, \ldots, x_d] \to \Gamma(X)$ is injective and finite
- $\Gamma(X) \to \Gamma(X_i)$ is onto, and each $\Gamma(X_i)$ is a domain
- $\Gamma(X) \hookrightarrow \Gamma(X_1) \times \cdots \times \Gamma(X_r)$.

Let $\mathfrak{p}_i = \ker(\mathbb{C}[x_1, \ldots, x_d] \to \Gamma(X_i))$ then we see that $\mathbb{C}[x_1, \ldots, x_d]/\mathfrak{p}_i \to \Gamma(X_i)$ is finite. Now, algebraic fact: if the following diagram commutes



then φ is finite iff ψ is finite. Surjections are finite, ψ finite, conclude what we want. Hence, by last condition, $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = (0)$; but $\mathbb{C}[x_1, \ldots, x_n]$ a domain implies that for some i we have $\mathfrak{p}_i = (0)$. This implies f.f. $(\mathbb{C}[x_1, \ldots, x_d]/\mathfrak{p}_i) \subset_{\text{finite}} \mathbb{C}(X_i)$, and since the transcendence degree of this is less than or equal to d, we conclude $\operatorname{trdeg}_{\mathbb{C}} \leq d$ and for some i, trdeg $= d$ since $\mathfrak{p}_i = (0)$. $\square$ Advice: look at Mumford's Red Book for good stuff though hard about dimension.

Lemma 19 *If $Y \subset X \subset \mathbb{C}^n$ are varieties, $Y \neq X$, then $\dim Y < \dim X$.*

Proof: set $d = \dim(X)$. Consider $\Gamma(X) \twoheadrightarrow \Gamma(Y)$. If the Lemma is false, then $\exists \overline{f_1}, \ldots, \overline{f_d}$ in $\Gamma(Y)$ which are algebraically independent over $\mathbb{C}$ (exercise). Pick $f_i \in \Gamma(X)$ mapping to $\overline{f_i}$ in $\Gamma(Y)$. Also pick a non-zero $f \in \ker(\Gamma(X) \to \Gamma(Y))$. By assumption, $f_1, \ldots, f_d, f$ are algebraically dependent over $\mathbb{C}$, so choose an irreducible polynomial $p \in \mathbb{C}[T_1, \ldots, T_{d+1}]$ such that $p(f_1, \ldots, f_d, f) = 0$ in $\Gamma(X)$. Then $0 = P(\overline{f_1}, \ldots, \overline{f_d}, \overline{f})$ in $\Gamma(Y)$, so $0 = P(\overline{f_1}, \ldots, \overline{f_d}, 0)$ in $\Gamma(Y)$ then $P(T_1, \ldots, T_d, 0)$ is identically zero since $\overline{f_1}, \ldots, \overline{f_d}$ are alg. ind. This means that T_{d+1} divides P, which means $P = c \cdot T_{d+1}$ for some $c \in \mathbb{C} \setminus \{0\}$, which implies $cf = 0$ a contradiction. Next, resolving singularities, then projective curves (gluing together...)

10 February 18

10.1 wrapping up dimension

We won't prove this theorem:

Theorem 5 *If $X \subset \mathbb{C}^n$ is a variety, then*

(a) for $Y \subsetneq X$ a subvariety we have $\dim(Y) = \dim(X) - 1 \Leftrightarrow \nexists$ a variety Z such that $Y \subsetneq Z \subsetneq X$ and

(b) if $f \in \mathbb{C}[x_1, \ldots, x_n]$ is not 0 on X, then any irreducible component of $X \cap V(f)$ has dimension $\dim(X) - 1$.

Remark:

(a) It's not hard to show that (2) $\Rightarrow$ (1) above

(b) the proof of (2) is a bit harder (see Mumford)

(c) using this we can *redefine* $\dim X$ as

$\max\{n : \exists X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$ with X_i irreducible subvarities and closed in Zariski top$\}$.

The RHS can be used to define *Krull dimension* (sometimes called combinatorial dimension) of *any* topological space. There is also an algebraic version of this for rings: consider chains of prime ideals; works well for Noetherian *local*[8] rings; important invariant. The assuring thing is that this is well defined, and can also define codimension: for $Y \subset X$, $\dim(X) = \dim(Y) + \operatorname{codim}(Y, X)$. There are many more results about dimension of varities: e.g., dimensions of fibres of polynomial maps of varieties...

10.2 Morphisms

If M and N are differentiable manifolds, then $f : M \to N$ is differentiable $\Leftrightarrow$ for all locally differentiable $\varphi : N \to \mathbb{R}$, the composition $\varphi \circ f$ is diff. Later, we'll say that a map $f : X \to Y$ of (quasi affine or quasi projective) varieties is a morphism iff it's continuous and it pulls back regular functions to regular functions (also locally). Regular will mean given by polynomials. Motivating examples to come, but first give a name to an open subset of an affine variety:

[8] local rings := have exactly one maximal ideal

Definition 16 *a quasi-affine variety X is an open subset of an affine variety. In other words, $X \subset \mathbb{C}^n$ is an irreducible Zariski locally closed subset.*

Note that the closure of something locally closed means that thing is open in that closure; this means you are defined by polynomial equalities and "not"-equalities (no ordered ones), plus you're irreducible.

- ex: $X_1 = \{(x,y) \in \mathbb{C}^2 : xy \neq 0\} \subset \mathbb{C}^2$ is quasi-affine
- ex: $X_2 = \{(x,y) \in \mathbb{C}^2 : \sin(x+y) \neq 0\} \subset \mathbb{C}^2$ is not quasi-affine
- ex: $X_3 = \{(x,y) \in \mathbb{C}^2 : x^3 + y^3 = 1, x \neq 0\} \subset \mathbb{C}^2$ is quasi-affine
- ex: $X_4 = \{(x,y) \in \mathbb{C}^2 : xy = 0, (x+y) \neq 0\} \subset \mathbb{C}^2$ is not irreducible so not a quasi-affine variety.

What is a regular function on one of these $q - A$ sets? Motivation: examples of regular functions. Take X_1 above, and consider the functions $(x,y) \mapsto x + y \in \mathbb{C}$, or $\mapsto \frac{1}{x} \in \mathbb{C}$, or $\frac{x^3+y^{10}+111}{x^{10}y^{100}} \in \mathbb{C}$. But $(x,y) \mapsto \frac{1}{x+y}$ does not make sense. This suggests we allow $\frac{P}{Q}$ if Q is never 0 on X. But what about this example:

$$X = \{(a_1,a_2,a_3,a_4) \in \mathbb{C}^4 : a_1a_2 = a_3a_4 \text{ and } (a_2 \neq 0 \text{ or } a_4 \neq 0)\}.$$

Consider $f : X \to \mathbb{C}$ by $(a_1,a_2,a_3,a_4) \mapsto \frac{a_3}{a_2}$ if $a_2 \neq 0$ or $\frac{a_1}{a_4}$ if $a_4 \neq 0$. This is well defined on the overlaps!!! It's a patched up function on 2 Zariski opens; maybe we should thus only require locally $\frac{P}{Q}$.

Definition 17 *Let $X \subset \mathbb{C}^n$ be a q-affine variety. A function $f : X \to \mathbb{C}$ is a regular function iff $\forall a \in X$ $\exists P, Q \in \mathbb{C}[x_1, \ldots, x_n]$ with $Q(a) \neq 0$ such that $f(b) = \frac{P(b)}{Q(b)}$ is true $\forall b$ in some open neighborhood of $a \in X$ (Zariski topology throughout). Denote $\mathcal{O}(X)$ to be the set of regular functions on X.*

[9]

Lemma 20 *$\mathcal{O}(X)$ is a $\mathbb{C}$-algebra.*

Well $f, g \in \mathcal{O}(X) \Rightarrow f + g, fg \in \mathcal{O}(X)$. Given $a \in X$, $f = \frac{P}{Q}$ in $U \subset X$ of a, and $q = \frac{H}{L}$ in $V \subset X$ of a, take $U \cap V$, and define $f + g$; now since $Q(a)L(a) \neq 0$, we have $f + g = \frac{PQ' + QP'}{QQ'}$ and $fg = \frac{PP'}{QQ'}$. $\square$

Well what do you think is $\mathcal{O}(\mathbb{C}^2)$? It's $\Gamma(\mathbb{C}^)$ the coordinate ring $\mathbb{C}[x_1, x_2]$. The map $\mathbb{C}^2 \to \mathbb{C}$ by $(x,y) \mapsto \frac{x+y}{xy}$ where $xy \neq 0$ and 1 elsewhere can't be a regular function.

Lemma 21 *(Regular functions and topology) Let $X \subset \mathbb{C}^n$ be q-A and $f_1, \ldots, f_r \in \mathcal{O}(X)$. Then the map $X \to \mathbb{C}^r$ by $a \mapsto (f_1(a), \ldots, f_r(a))$ is continuous in both the usual and Zariski topology.*

[9] "Things you call regular functions aren't functions in Scheme theory to come

Proof: it suffices to find $\forall p \in X$ a neighborhood $U_p \subset X$ where the map restricted to it is continuous (local formulation of continuity). If we can find an open neighborhood U of any point of X such that $f\big|_U : U \to \mathbb{C}^r$ is continuous, then were done. Open U are always quasi-affine. Assuming $f_1 = \frac{P_1}{Q_1}, \cdots, f_r = \frac{P_r}{Q_r}$ and

$$X \subset Y := \{a \in \mathbb{C}^n : (Q_1, \ldots, Q_r)(a) \neq 0\}$$

and every point $\exists$ neighborhood where f looks like a quotient of 2 polynomials. Now $f_i\big|_{U_i} = \frac{P_i}{Q_i}$; replace X by $U_1 \cap \cdots \cap U_r$. Since X has the induced topology from Y, it suffices to show that $\tilde{f} : Y \to \mathbb{C}^r$ by $a \mapsto \left(\frac{P_1(a)}{Q_1(a)}, \cdots, \frac{P_r(a)}{Q_r(a)}\right)$ is continuous in either topology. In the usual topology we're done – polys are continuous, the denominator is never 0 on X. We have to show now that it's continuous in the Zariski topology; remember this is defined on $\mathbb{C}^n \setminus$ a hypersurface from $Q_1 \cdots Q_r = 0$. Take the hypersurface $V(h) \subset \mathbb{C}^r$, $h \in \mathbb{C}[x_1, \ldots, x_r]$, then we know

$$\tilde{f}^{-1}(V(h)) = \{a \in Y : h\big(\frac{P_1(a)}{Q_1(a)}, \cdots, \frac{P_r(a)}{Q_r(a)}\big)\}$$

clear denominators and get a polynomial equation

$$\{a \in Y : \Big[(a_1 \cdots a_r)^N h\big(\frac{P_1}{Q_1}, \cdots, \frac{P_r}{Q_r}\big)\Big](a) = 0\}.$$

We can clear denominators since $Q_1 \cdots Q_r \neq 0$, and if N is larger than the total degree of h, then this is a polynomial in $X_1, \ldots, X_r$, so it's Zariski closed. Now, since every Zariski closed set is an intersection of hypersurfaces, we're done (check). $\square$

Going to show next time that X an affine variety implies $\Gamma(X) = \mathcal{O}(X)$. $\langle$We won't define abstract varieties.$\rangle$.

11 February 23

Last time, we defined the regular functions $\mathcal{O}(X)$ for X a quasi-affine variety (everywhere locally quotients of polynomials), and proved that $(f_1, \ldots, f_n) : X \to \mathbb{C}^n$ is continuous in both topologies if $f_i \in \mathcal{O}(X)$. [For example, on the homework, you have to show $\mathcal{O}(\mathbb{C}^n \setminus V(f)) = \mathbb{C}[x_1, \ldots, x_n]_f$] [10] Following this, we have

Corollary 7 *Let X be a q-Affine variety. If $f \in \mathcal{O}(X)$ and $f = 0$ on a non-empty Zariski open subset then $f = 0$ identically on X.*

[10] Note that "=" is NOT equal as sets but indicates that the LHS and RHS are in canonical isomorphism (in this case, $\frac{P}{f^n} \mapsto \left(a \mapsto \frac{P(a)}{f(a)^n}\right)$ in the reverse direction; note that this representation $\frac{P}{f^n}$ is not unique, so we must show that this map is well defined.) Now, we have to be careful with using = for such a thing: a diagram $A = B = D$ and $A = C = D$ might make us think that as maps the diagram of canonical isomorphisms commutes, which is not necessarily true.

Proof: define $V_X(f) = V(f) \cap X = \{a \in X : f(a) = 0\} \subset X$ is closed and X is irreducible, so $V_X(f) \supset U$ means $V_X(f) \supset \overline{U}$ but any non-empty open is dense always, so $V_X(f) \supset X$ and hence we have equality. $\square$ Remark: the corollary also holds if f is 0 on a usual non-empty open subset (will not prove this).

Lemma 22 *(Miracle Lemma) If X is affine variety, then $\Gamma(X) = \mathcal{O}(X)$.*

Proof: a trick! It is clear that $\Gamma(X) \subset \mathcal{O}(X)$ is a subring. Pick $f \in \mathcal{O}(X)$. Consider

$$I = \{Q \in \mathbb{C}[x_1, \ldots, x_n] : Qf \in \Gamma(X)\}.$$

The Qs morally are all the denominators that can appear when you write $\frac{P}{Q} = f$ on a set of points where $Q \neq 0$. Claim: I is an ideal of $\mathbb{C}[x_1, \ldots, x_n]$ because $\Gamma(X)$ is a ring.[11] If $Q = 0$ exactly, then $Qf = 0 \in \Gamma(X)$. Now note that $I(X) \subset I$; $\forall a \in X$ we can write $f\big|_U = \frac{P}{Q}\big|_U$ for some $a \in U \subset X$ open, $P, Q \in \mathbb{C}[x_1, \ldots, x_n]$, $Q(a) \neq 0$, actually $Q \neq 0$ on U. Then $(P - Qf)\big|_U = 0$ implies by the corollary that $P - Qf = 0$ in $\mathcal{O}(X)$ which means $Qf \in \Gamma(X)$ which means $Q \in I$. We can then conclude that $\forall a \in X$, $\exists Q \in I$ such that $Q(a) \neq 0$ which implies with $I(X) \subset I$ that $1 \in I$ which means $V(I) = \emptyset$ which means by Weak Hilbert N. that $I = \mathbb{C}[x_1, \ldots, x_n]$ hence $f \in \Gamma(X)$. $\square$

Lemma 23 *X a q-A variety, $f_1, \ldots, f_s, g_1, \ldots, g_t \in \mathcal{O}(X)$, and suppose $P \in \mathbb{C}[S_1, \ldots, S_s]$, $Q \in \mathbb{C}[T_1, \ldots, T_t]$. Then*

$$\frac{P(f_1, \ldots, f_s)}{Q(g_1, \ldots, g_t)} \in \mathcal{O}(U)$$

where $U = \{a \in X : Q(g_1(a), \ldots, g_t(a)) \neq 0\}$ is open in X.

Proof of this statement for polynomial combinations is the "same" (ish) as that proof of $\mathcal{O}(X)$ a ring. In the simplest case, which usually comes up, we have $f, g \in \mathcal{O}(X) \Rightarrow \frac{f}{g} \in \mathcal{O}(U)$ where $U = \{a \in X : g(a) = 0\}$; write $f = \frac{P}{Q}$, $q = \frac{P'}{Q'}$, then $\frac{f}{g} = \frac{Q'P}{P'Q}$, and the condition $g(a) \neq 0$ above makes $P'(a) \neq 0$, and $Q(a) \neq 0$ already by assumption. Warning: U might be $\emptyset$. We should define $\mathcal{O}(\emptyset) = \{0\}$, but $\emptyset$ is not irreducible (conventions...)...

Definition 18 *Let X, Y be q-affine varieties. A morphism $\varphi : X \to Y$ is a map of sets such that*

(a) φ is continuous in the Zariski topology and

(b) $\forall V \subset Y$ Zariski open, $\forall f \in \mathcal{O}(V)$, we have $f \circ \varphi \in \mathcal{O}(\varphi^{-1}(V))$ by pullback.

Here's an example of (a) but not (b): any non-usual bijection $\mathbb{C} \to \mathbb{C}$ call it w will satisfy this, because of the "stupid" topology over $\mathbb{C}$ (where the non-trivial closed subsets are just finite) w is continuous, since preimage of points is point, but given a polynomial function say $\mathrm{id} : \mathbb{C} \to \mathbb{C}$, it can't pull back through w to a polynomial (we might have w swap π and e and leave the rest fixed!). Now, many lemmas:

[11] Called the *conductor ideal*...

Lemma 24 *Composition of morphisms is a morphism; also identities are morphisms (category).*

Objects are characterized by (i) topology and (ii) regular functions on them. A morphism is an isomorphism iff φ a bijection, φ continuous (i..e φ a homeomorphism of Zariski sets) and φ^{-1} is a morphism too (part (b) above).

Lemma 25 *If $X \subset \mathbb{C}^n$ is q-affine, then the inclusion map $i : X \to \mathbb{C}^n$ is a morphism.*

Tautological because of definition of regular $f \in \mathcal{O}(X)$ as a restriction of polys in $\mathbb{C}^n$.

Lemma 26 *If $f : X \to \mathbb{C}$ is a set map, then $f \in \mathcal{O}(X)$ iff f is a morphism $X \to \mathbb{C}$.*

Proof: "$\Leftarrow$" is obvious: take $\mathbb{C} \subset \mathbb{C}$ open, then the identity map $\mathrm{id} : \mathbb{C} \to \mathbb{C}$ will pull back to a regular function, which is exactly f, hence $f \in \mathcal{O}(X)$. For "$\Rightarrow$", this is true because $\frac{P(y)}{Q(y)}$ is regular on some open of $\mathbb{C}$ .... CHECK AND FINISH

Lemma 27 *If $X \subset \mathbb{C}^n$, $Y \subset \mathbb{C}^m$ are q-affine and $\varphi : X \to Y$ is a map of sets then TFAE:*

(i) φ a morphism

(ii) $y_j \circ \varphi : X \to \mathbb{C}$ is regular, where $y_j : \mathbb{C}^m \to \mathbb{C}$ are the jth coordinate functions (same as in smooth manifold theory)

Proof: $(i) \Rightarrow (ii)$: $y_i : \mathbb{C}^m \to \mathbb{C}$ is regular over $\mathbb{C}^m$ a morphism, also when restricted to Y because i is a morphism; this means $y_i \circ i \circ \varphi$ is a morphism, so it's regular. For $(ii) \Rightarrow (i)$, we show that if $\varphi = (f_1, \ldots, f_m)$ where $f_i = y^i \circ \varphi$ is regular, we've seen that such a φ is continuous: since Y has induced topology, the map $(f_1, \ldots, f_m) : X \to \mathbb{C}^m$ continuous agreeing as we'd want means it descends to a continuous map to the subspace Y. Now, show that regular functions pull back to regular functions. If $V \subset Y$ is open and $h \in \mathcal{O}(V)$ then locally on V we can write $h = \frac{P}{Q}$, $P, Q \in \mathbb{C}[y_1, \ldots, y_m]$ so then $h \circ \varphi$ is equal locally on $\varphi^{-1}(V)$ to

$$\frac{P(y_1 \circ \varphi, \ldots, y_m \circ \varphi)}{Q(y_1 \circ \varphi, \ldots, y_n \circ \varphi)} = \frac{P(f_1, \ldots, f_m)}{Q(f_1, \ldots, f_m)}$$

and thus the regular functions are on suitable opens by the previous lemma. □

Corollary 8 *A morphism of q-affine varities is continuous in the usual topology.*

Proof: we've seen this form maps $X \to \mathbb{C}^m$ given by m regular functions. Instructive example, where things go wrong: $f(x, y) = xy + x^3 + y^3$ and at $V(f) \subset \mathbb{C}^2$. Consider the point $p = (-\frac{1}{2}, -\frac{1}{2})$ and the projection from this point. Is this regular? Well, first, what is projection from a point? To any $q \in C = V(f)$, take q to the slope of the line joining q and p. For points on the vertical line $\{-\frac{1}{2}\} \times \mathbb{C}$, we can't assign infinite slope; perhaps we'll take values in $\mathbb{C}\P^1$ – more on this later.... Also, at p we should assign the slope of the tangent line, which should be -1... Other thing: this does work: the new function will be regular on $V(f) \setminus \{A, B\}$ where A and B are points not equal to P but on $\{-\frac{1}{2}\} \times \mathbb{C}$. Other thing, helpful for the exercises: want to make a function regular at A and B, but it doesn't care so much you get the same function – find a polynomial 0 on A and B...

12 February 25

12.1 Recap

Here's an overview of what we've done so far:

- Weak HNS: $V(I) = \emptyset \Leftrightarrow I = \mathbb{C}[x_1, \ldots, x_n]$.
- HNS: algebraic sets $\Leftrightarrow$ radical ideals in $\mathbb{C}[x_1, \ldots, x_n]$.
- Resultants.
- Noetherian Rings and Spaces, decomposition into irreducible components.
- Affine Varieties.
- Algebra: finite type, integral, finite ring maps.
- Relating finite ring maps and "finite morphisms" aka projections being "finite" or proper.
- Noether Normalization: gives rise to closed maps in Zariski topology.
- Nakayama's Lemma.
- Transcendence degree and the dimension of a variety.
- Dimension and projections.
- Quasi-affine varities and regular functions; nice result that $(f_1, \ldots, f_n) : X \to \mathbb{C}^n$ is continuous in both topologies if $f_i \in \mathcal{O}(X)$ and that $\mathcal{O}(X) = \Gamma(X)$ if X is affine.
- Morphisms of quasi-affine varities.

We now say that X is affine not if it's a closed subset of $\mathbb{C}^n$ but if it's isomorphic to some affine (redefinition). Silly example: $\mathbb{C} \setminus \{0\} \subset \mathbb{C}$ is not closed, but by $\mathbb{C} \setminus \{0\} \to \mathbb{C}^2$ as $a \mapsto (a, a^{-1})$, this is an isomorphism of varities from $\mathbb{C} \setminus \{0\}$ to $V(xy - 1) \subset \mathbb{C}^2$. The inverse map is $Y \to X$ by $(a, b) \mapsto a$. This is a regular function, hence it's a morphism in our category. In the exercises we will prove a super generalization of this: (a) $X \subset \mathbb{C}^n$ affine, $f \in \mathbb{C}[x_1, \ldots, x_n]$ then $X \setminus V(f)$ is affine and (b) $\forall X$ a q-A var and any point $p \in X$, $\exists$ open neighborhood $a \in U \subset X$ which is affine. Just like for all differentiable manifolds, $p \in M$ has a nieghborhood that's a ball: analogue of affines here (a basis for the topology). Quasi-affines are unions of affines; hence, a general variety will be (though we won't cover in the course; look in Mumford's book for example):

Definition 19 *A pre-variety X is an irreducible quasi-compact topological space X together with an atlas $X = \bigcup U_i$ of opens such that*

(i) for each i, $\exists$ a homeomorphism $\varphi_i : U_i \to X_i \subset \mathbb{C}^{n_i}$ with an affine variety X_i in the Zariski topology

(ii) $\forall i, j$, the transition map $\varphi_i \circ \varphi_j^{-1}$ is a morphism:

$$\begin{array}{ccccccc} & & & U_i \cap U_j & & & \\ & & \swarrow^{\varphi_i} & & \nwarrow^{\varphi_j^{-1}} & & \\ X_i \supset & & \varphi_i(U_i \cap U_j) & & & \varphi_j(U_i \cap U_j) & \subset X_j \end{array}$$

Definition 20 *A prevariety is a variety iff diagonal map $\Delta(X) \subset X \times X$ is closed (here $X \times X$ is the product pre-variety); $\sim$ Hausdorff conditions (separability)*

Why we're not doing this: so hard to write a variety that is NOT quasi-affine or quasi-projective (to come). Don't need gluing procedure. Can also do the definition of prevariety with notion of regular functions on every open (sheaves). Plane curves: delete finitely many points: then it's affine! Hard theorem (might have to go to high $\mathbb{C}^n$)....

12.2 Projective space

$\mathbb{P}^n := \mathbb{P}^n_{\mathbb{C}} := \left(\mathbb{C}^{n+1} \setminus \{0\}\right) / \mathbb{C}^*$ the quotient of the action of $\mathbb{C}^*$ on vectors by multiplication (it's $G_1(\mathbb{C}^{n+1})$). Recall from topology $\mathbb{R}\,\mathbb{P}^2$ is a nice example of a non-orientable surface. Points of $\mathbb{P}^n$ are denoted $[a_0 : a_1 : \cdots : a_n]$ which means $(a_0, \ldots, a_n) \neq \vec{0}$ and denotes the line containing $\vec{a}$. Let $F \in \mathbb{C}_d[X_0, \ldots, X_n]$ be a homogeneous polynomial of degree d: that is, every monomial in F has degree d. We use these capital X_is for homogeneous polynomials. Then $(\lambda F) = \lambda^d F$. Then we let

$$V_+(F) = \{[a_0 : \cdots : a_n] \in \overset{n}{\mathbb{P}} : F(a_0, \ldots, a_n) = 0\}.$$

First off, F isn't a function on $\mathbb{P}^n$, but this is well defined because $F(\lambda \cdot \vec{a}) = \lambda^d F(\vec{a}) = \lambda^d \cdot 0 = 0$. These are the hypersurfaces; we say the closed sets are intersections of the hypersurfaces.

Definition 21 *A Zariski closed set in $\mathbb{P}^n$ is any subset of the form $Z = \bigcap_{F \in E} V_+(F)$ where E is a set of homogeneous elements of $\mathbb{C}[x_0, \ldots, x_n]$ not necessarily all of the same degree.*

Can directly check that this is a topology (omitted). We can write $\mathbb{P}^n = U_0 \cup \cdots \cup U_n$ as covered by the standard charts of affine n-spaces

$$U_i = \overset{n}{\mathbb{P}} \setminus V_+(X_i) = \{[1 : a_1 : \cdots : a_n]\} \cong \overset{n}{\mathbb{C}}$$

by the natural bijection $\Phi_i : U_i \to \mathbb{C}^n$ by

$$[a_0 : \cdots : a_n] \mapsto \left(\frac{a_0}{a_i}, \ldots, \frac{\hat{a_i}}{a_i}, \ldots, \frac{a_n}{a_i}\right)$$

with inverse $(c_1, \ldots, c_n) \mapsto [c_1 : \cdots : c_{i-1} : 1 : c_{i+1} : \cdots : c_n]$.

Proposition 5 *Φ_i is a homeomorphism.*

Note U_i gets subspace topology from $\mathbb{P}^n$. Well, in usual topology

$$\left(\overset{n+1}{\mathbb{C}} \setminus \{0\}\right) / \overset{*}{\mathbb{C}} \cong S^{2n+2}/S^1$$

so $\mathbb{P}^n$ is compact. In regular space, affines are never compact unless finite; here, rather, all projective varieties are compact. Now let's begin the proof of the proposition - we'll homogenize. *Proof:* first prove that $Z \subset \mathbb{P}^n$ closed means $\Phi_0(Z \cap U_0) \subset \mathbb{C}^n$ is Zariski closed. This reduces immediately to the case $Z = V_+(F)$.[12] Then it's clear from the formula

$$\Phi_0(V_+(F) \cap U_0) = V(F(1, x_1, \ldots, x_n))$$

(check this). Suppose $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is an ideal. We have to show $\mathbb{C}^n \supset V(I) = \Phi_0(U_0 \cap Z)$ for some Zariski closed $Z \subset \mathbb{P}^n$. We know by the Hilbert basis theorem that $I = (f_1, \ldots, f_r)$ for some r. Set

$$F_i(X_0, \ldots, X_n) = X_0^{\text{totaldegree}(f_i)} \cdot f_i\Big(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\Big)$$

and when $X_0 = 1$, we get our old f_i back. Set $Z = V_+(F_1) \cap \cdots \cap V_+(F_n)$. This is Zariski-closed in $\mathbb{P}^n$ and then $\Phi_0(Z \cap U_0) = V(I)$ (check!) because

$$\begin{aligned} \left(\Phi_0^{-1}\right)^{-1}(Z \cap U_0) &= \{(a_1, \ldots, a_n) \in \overset{n}{\mathbb{C}} : \ F_i(1, a_1, \ldots, a_n) = 0 \ \forall 1 \le i \le r\} \\ &= V(f_1) \cap \cdots \cap V(f_r) = V(I) \end{aligned}$$

where the inverse is $c_1 \cdots c_n \mapsto (1, c_1, \ldots, c_n)$.

Corollary 9 *$\mathbb{P}^n$ is a Noetherian topological space.*

Proof: $\mathbb{P}^n = \bigcup_{i=0}^n U_i$ and each U_i is Noetherian.

Let's show that any two lines meet in $\mathbb{P}^n$. Even though $x = 0$ and $x = 1$ dont meet in $\mathbb{C}^2$, setting $x = \frac{X_1}{X_0}$ and $y = \frac{X_2}{X_0}$ we get $X_1 = 0$ and $X_1 - X_0 = 0$ which has an intersection at $[0 : 0 : 1]$ a unique point.

13 March 2

[Recalls facts from last week]. Be careful: in the usual topology our compact manifold $\mathbb{P}^n$ is Hausdorff but not in the Zariski topology.

Definition 22 *A projective variety is an irreducible Zariski closed $X \subset \mathbb{P}^n$ for some $n \in \mathbb{Z}_+$.*

Definition 23 *A quasi-projective variety is an irreducible Zariski-locally-closed $X \subset$ ¶^{n} for some $n \in \mathbb{Z}_+$.*

[12] ???

13.1 Regular functions on quasi-projective varities

We want to discuss regular functions on quasi-projective varieties. But first the quasi-affine case:

Facts: (1) if $X \subset Y \subset \mathbb{C}^n$ are q-affine vars then the restriction map $f \to f\big|_X$ gives a map $\mathcal{O}(Y) \to \mathcal{O}(X)$ (have already seen this).
(2) if X is q-affine, $X = V_1 \cup \cdots \cup V_m$ with $V_i \subset X$ Zariski open then

$$\mathcal{O}(X) = \{(f_1, \ldots, f_m) \in \mathcal{O}(V_1) \times \cdots \times \mathcal{O}(V_m) \ : \ f_i\big|_{V_i \cap V_j} = f_j\big|_{V_i \cap V_j}\}$$

The functions *glue*; this is clear from the local nature of the condition of defining regular functions; here $=$ actually means canonical isomorphism.

Reformulation: $f : X \to \mathbb{C}$ a set map is a regular function iff $f\big|_{V_1}, \ldots, f\big|_{V_m}$ are regular functions (plus gluing).
(3) If $\varphi : Y_1 \to Y_2$ is an isomorphism of quasi-affine varieties and $X_i \subset Y_i$ is locally closed and irreducible, so themselves are quasi-affine varieties with $\varphi(X_1) = X_2$ then $\varphi\big|_{X_1}$ is an isomorphism.

Lemma 28 *If $X \subset \mathbb{P}^n$ is irreducible and Zariski locally closed, and $X \subset U_i \cap U_j$, then the transition map*

$$\left(\Phi_j \circ \Phi_i^{-1}\right)\big|_{\Phi_i(X)} : \Phi_i(X) \to \Phi_j(X)$$

is an isomorphism of quasi-affine varities.

In particular, $\mathcal{O}(\Phi_i(X)) = \mathcal{O}(\Phi_j(X))$ is a canonical isomorphism. This is where we'll get our notion of $\mathcal{O}(X)$ for projective varieties (to come).

Corollary 10 *If $X \subset \mathbb{P}^n$ is irreducible and Zariski locally closed and $X \subset U_i$ for some i, then can define $\mathcal{O}(X)$ to be $\mathcal{O}(\Phi_i(X))$ and it doesn't matter which i I pick.*

Proof: $X \subset U_i \cap U_j$, then show $\Phi_i(U_i \cap U_j) = \Phi_j(U_i \cap U_j)$, then apply (3) above. We can give the map explicitly: from $[a_0 : \cdots : a_n]$ we get $(\frac{a_0}{a_i}, \ldots, \frac{\hat{a_i}}{a_i}, \cdots, \frac{a_n}{a_i}) \to (\frac{a_0}{a_j}, \ldots, \frac{\hat{a_j}}{a_j}, \cdots, \frac{a_n}{a_j})$ by the map $(b_0, \ldots, \hat{b_i}, \ldots, b_n) \mapsto \left(\frac{b_0}{b_j}, \ldots, \frac{\hat{b_j}}{b_j}, \ldots, \frac{1}{b_i}, \ldots, \frac{b_n}{b_j}\right)$ and you get the inverse by swapping i and j.

Definition 24 *If $X \subset \mathbb{P}^n$ is quasi-projective, then*

$$\mathcal{O}(X) = \{f : X \to \mathbb{C} : f\big|_{X \cap U_i} \in \mathcal{O}(X \cap U_i) \text{ defined as in corollary}\}.$$

Now a leap of faith: we move to the quasi-projective case.

Remarks (a) if $Y \subset X$ then restriction of functions gives $\mathcal{O}(X) \to \mathcal{O}(Y)$.
(b) if $X = V_1 \cup \cdots \cup V_m$ is an open covering, then

$$\mathcal{O}(X) = \{(f_1, \ldots, f_m) \in \mathcal{O}(V_1) \times \cdots \times \mathcal{O}(V_m) : \ f_i\big|_{V_i \cap V_j} = f_j\big|_{V_i \cap V_j}\}$$

as before (can be reformulated as before; this is nice because it's not necessarily the standard covering $U_0 \cup \cdots \cup U_n$ of $\mathbb{P}^n$.

Definition 25 *A morphism of quasi-projective varieties $\varphi : X \to Y$ is a (Zariski) continuous map such that $\forall V \subset Y$ open, $\forall f \in \mathcal{O}(V)$, we have $f \circ \varphi \in \mathcal{O}(\varphi^{-1}(V))$.*

[13] Remark: since $\mathbb{C}^n = U_0 \subset \mathbb{P}^n$, we can think of any q-affine varieties as q-projective ones! We can't compare affine and projective varieties: if a variety X is both affine and projective, then its usual topological space is compact, hence $X \subset \mathbb{C}^n$ is bounded, and we saw that this implies compact, and for an algebraic set irreducible implies its a single point! Also, at this point we're accepting that quasi-projective morphisms are continuous in the usual topology.

13.2 Examples

A projective plane **curve** is $X = V_+(F) \subset \mathbb{P}^2$ where $F \in \mathbb{C}[X_0, X_1, X_2]$ is irreducible and homogeneous. For example, $F = X_0^2 + X_1^2 + X_2^2$. This of course came from the following lemma:

Lemma 29 *If $F \in \mathbb{C}[X_0, \ldots, X_n]$ is irreducible and homogeneous then $V_+(F) \subset \mathbb{P}^n$ is irreducible.*

Proof: later.

Claim: any closed subset $Z \subset \mathbb{P}^2$ is a union $C_1 \cup C_r \cup \{p_1, \ldots, p_s\}$ for some $C_i \subset \mathbb{P}^2$ projective plane curves and $p_1, \ldots, p_s \in \mathbb{P}^2$ points; or $Z = \emptyset, \mathbb{P}^2$. Reason: it suffices to prove that an irreducible in $\mathbb{P}^2$ is either $\mathbb{P}^2$, a projective plane curve, or a point because $\mathbb{P}^2$ is Noetherian. Consider $Z \cap U_0$: this is either empty or irreducible. In empty case, renumber 0, 1, 2 to make it non-empty. Then because U_0 is $\mathbb{C}^2$ with Zariski topology, we know $Z \cap U_0$ is either a point or $Z \cap U_0 = V(f)$ for $f \in \mathbb{C}[x, y]$ irreducible. This implies $Z = \{p\}$ or $Z = V_+\Big(X_0^{\deg f} f\big(\frac{X_1}{X_0}, \frac{X_2}{X_0}\big)\Big)$ (minimally homogenize). This is irreducible in $\mathbb{C}[X_0, X_1, X_2]$ because f is irreducible in $\mathbb{C}[x, y]$ by the lemma, so $V_+(F)$ irreducible and $Z \cap U_0 \neq \emptyset$, $V_+(F) \cap U_0 \neq \emptyset$ and contain the same open so they're equal (Zariski type property).

Scholium 1 *If $Z \subset \mathbb{P}^n$ is irreducible and $Z \cap U_0 \neq \emptyset$ then Z is the closure of $Z \cap U_0$.*

So we get an inclusion-preserving bijection between (i) $Z \subset \mathbb{P}^n$ irreducible Zariski closed $Z \cap U_0 \neq \emptyset$ and (ii) irreducible closed subsets $Z' \subset U_0 = \mathbb{C}^n$. If $Z' \subset U_0 = \mathbb{C}^n$ corresponds to a prime $\mathfrak{p} \subset \mathbb{C}[x_1, \ldots, x_n]$, then the corresponding Z is $\bigcap_{f \in \mathfrak{p}} V_+\Big(X_0^{\text{totaldeg}(f)} \cdot f\big(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\big)\Big)$. This takes some work to prove, but it's a nice exercise. We can now prove the lemma from before.

Proof of Lemma: Given $F \in \mathbb{C}[X_0, \ldots, X_n]$ irreducible and homogeneous, we

[13] Continuous: pulls back topology into topology. Algebraic: pulls back sheaf of regular functions into domain sheaf.

must have $F(1, x_1, \ldots, x_n)$ irreducible in $\mathbb{C}[x_1, \ldots, x_n]$ or a unit if $F = X_0$ say. Because if not, then $F(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)$ can be homogenized to

$$X_0^{A+B-\deg F} \cdot F(X_0, \ldots, X_n) = (X_0^A f(\frac{X_1}{X_0}, \ldots), X_0^B g(\frac{X_1}{X_0}, \ldots))$$

then by unique factorization in $\mathbb{C}[X_0, \ldots, X_n]$ you get either $X_0^A f = \lambda X_0^A$ or $X_0^B g = \mu X_0^B$ which implies either f or g is a constant. Thus $V_+(F) \cap U_0 = V(F(1, x_1, \ldots, x_n))$ is either empty or irreducible. ... will give one irreducible component; show that they're no others, then it's the same as this one. $\square$

We want to show: what is it good for? (1) Two projective curves always meet. (2) Bezout's theorem. Next time: any two projective plane curves meet.

14 March 4

Lemma 30 *Any two projective plane curves (irreducible hypersurfaces in $\mathbb{P}^2$) meet.*

Proof: say $C_i = V_+(F_i) \subset \mathbb{P}^2$ with $_i \in \mathbb{C}[X_0, X_1, X_2]$ irreducible homogeneous of degree d_i for $i = 1, 2$. If the monomial $X_0^{d_1}$ does not occur in F_1 and $X_0^{d_2}$ does not occur in F_2, then the point $[1 : 0 : 0] \in C_1 \cap C_2$. Thus we may assume $F_1 = aX_0^{d_1} + A_1 X_0^{d_1-1} + \cdots + A_{d_1}$ and $F_2 = bX_0^{d_2} + B_1 X_0^{d_2-1} + \cdots B_{d_2}$ with $a \neq 0$ or $b \neq 0$ and A_i, B_i homogeneous of degree i in X_1, X_2 (coefficients in $\mathbb{C}_i[X_1, X_2]$). For example, $X_0^3 + (X_1)X_0^2 + (X_1X_2 + X_2^2)X_0 + (X_2^3)$. Now set $R = \mathrm{Res}_{X_0}(F_1, F_2)$; looking at the formula for R you see that R is also homogeneous of degree $d_1 d_2$ in the two variables X_1, X_2. For example $d_1 = 2$, $d_2 = 1$, then we get a $(2+1) \times (2+1)$ matrix

$$R = \det \begin{bmatrix} a & A_1 & A_2 \\ b & B_1 & 0 \\ 0 & b & B_1 \end{bmatrix}.$$

Hence, using the fact that any homogeneous polynomial in two variables is a product of linear terms over $\mathbb{C}$, there are $\lambda_1, \lambda_2 \in \mathbb{C}$ such that $R(\lambda_1, \lambda_2) = 0$. Indeed then $F = cX_1^n \prod_{i=1}^{\deg F - n}(X_2 - \alpha_i X_1)$ for some $n \geq 0$ and some $c \in \mathbb{C}^*$ and some $\alpha_i \in \mathbb{C}$. Since the resultant has a zero, $F_1(X_0, \lambda_1, \lambda_2)$ and $F_2(X_0, \lambda_1, \lambda_2)$ have a common solution. Here we use that $a \neq 0$ or $b \neq 0$ (see previous result). $\square$

Remark: the proof suggests that $\#C_1 \cap C_2 = d_1 d_2$ provided $C_1 \neq C_2$. We have to say that they have no irreducible components in common. The truth is

$$d_1 d_2 = \sum_{p \in C_1 \cap C_2} e_p(C_1, C_2)$$

where $e_p(C_1, C_2)$ is the **intersection multiplicity** of C_1, C_2 at p. Intersection Theory: find nice ways to count multiplicities - match with order of vanishing of resultant at λ_1, λ_2. Now let's look at examples of curves in $\mathbb{P}^2$: lines, conics, and cubics.

14.1 Lines in $\mathbb{P}^2$

A line $L = V_+(F)$ with F linear. I claim: any such line is isomorphic to $\mathbb{P}^1$ which is S^2. For example, $X_0 + X_1 + X_2 = 0$ is shorthand for $V_+(X_0 + X_1 + X_2)$. Then look at the map $[a_0 : a_1] \mapsto [a_0 : a_1 : -a_0 - a_1]$. This is well defined on equivalence classes because it scales. This is a morphism (show on standard affine pieces that you get morphisms) and has an inverse $L \to \mathbb{P}^1$ by $[b_0 : b_1 : b_2] \mapsto [b_0 : b_1]$. Have to be careful that $\pi_{12} : \mathbb{P}^2 \to \mathbb{P}^1$ is nonsense, since $[0 : 0 : 1] \mapsto [0 : 0]$ is not allowed. To show it's a morphism, show that on nice open parts it's regular. As set maps, these are inverse to each other; since they are morphisms, this is an isomorphism. Conclusion: every projective line is $\cong$ to $\mathbb{P}^1$ as a (projective) variety. (On U_0 of $\mathbb{P}^1$, goes to $L \cap (U_0 \text{ of } \mathbb{P}^2)$ as in $\mathbb{C} \to \mathbb{C}^2$ by $c_1 \to (c_1, -1 - c_1)$.

14.2 Conics in $\mathbb{P}^2$

A (possibly singular) conic is $V_+(F)$ in $\mathbb{P}^2$ where F is homogeneous of degree 2. Two cases: (1) F is reducible $\Rightarrow F = L_1 L_2$ where (1a) $L_1 = L_2$ a line with multiplicity two or (1b) $L_1 \neq L_2$ two lines intersecting at one point. Two lines carving out the same space - in the dual space they differ by a scalar, so in (1b), $F = L^2$ for some bilinear form (taking square roots).[14] (2) F is irreducible. Write $F = \sum_{0 \le i \le j \le 2} a_{ij} X_i X_j$ which we can write as

$$F = a_{00}\big(X_0 + \frac{a_{01}}{2a_{00}} X_1 + \frac{a_{02}}{2a_{00}} X_2\big)^2 + \sum_{1 \le i \le j \le 2} b_{ij} X_i X_j$$

if $a_{00} \neq 0$. [Note: there's nothing special about having 3 variables here, so things can generalize...] Write $b_{11} = a_{11} - \frac{a_{01}^2}{4a_{00}}$. If $b_{11} \neq 0$, then

$$F = a_{00}\big(X_0 + \frac{a_{01}}{2a_{00}} X_1 + \frac{a_{02}}{2a_{00}} X_2\big)^2 + b_{11}\big(X_1 + \frac{b_{12}}{2b_{11}} X_2\big)^2 + c_{22} X_2^2.$$

If here $c_{22} = 0$, then $aL_1^2 + bL_2^2 = (\sqrt{a}L_1 + i\sqrt{b}L_2)(\sqrt{a}L_1 - \sqrt{b}L_2)$ but F irreducible implies $c_{22} \neq 0$. So

$$F = \big(\sqrt{a_{00}} X_0 + \cdots\big)^2 + \big(\sqrt{b_{11}} X_1 + \cdots\big)^2 + \big(\sqrt{c_{22}} X_2\big)^2 = L_0^2 + L_1^2 + L_2^2$$

linearly independent. Symmetric square matrix: think of it as a bilinear form, saying there exists a basis on which it's diagonalizable! This works whenever $a_{00} \neq 0$ and $4a_{00}a_{11} - a_{01}^2 \neq 0$ (the discriminant). Symmetric in $X_{0,1,2}$ by $S(3)$. Let's check on an example: $F = X_0X_1 + X_0X_2 + X_1X_2$: this is

$$\begin{aligned} F &= X_0X_1 + X_0X_2 + X_1X_2 \\ &= \frac{1}{2}\big[(X_0 + X_1)^2 - (X_0 - X_1)^2\big] + X_2(X_0 + X_1) \\ &= \frac{1}{4}L_0^2 - \frac{1}{4}L_1^2 + X_2L_0 \\ &= \frac{1}{4}(L_0 + 2X_2)^2 - X_2^2 - \frac{1}{4}L_1^2 \end{aligned}$$

[14] ???

the sum of three squares of linearly independent linear forms. Check that $X_2, L_1, L_0 + 2X_2$ are linearly independent.

Fact: by example (fudge), if F is irreducible of degree 2 homogeneous form in X_0, X_1, X_2 then $\exists$ linearly independent linear forms [by no means a unique representation]. $O(3)$ acts... consider the map $\mathbb{P}^2 \to \mathbb{P}^2$ by (L_0, L_1, L_2). By the previous discussion, this is an okay map. It's an isomorphism of $\mathbb{P}^2$; an automorphism of $\mathbb{P}^2$ as a variety. There's an inverse: 3×3 invertible matrix in $\mathbb{C}$. Conclusion: every non-degenerate conic is isomorphic to C_{std} given by $X_0^2 + X_1^2 + X_2^2 = 0$. The map (L_0, L_1, L_2) maps C_{std} isomorphically onto C: $F = \sum L_i^2 = 0$ in $\mathbb{P}^2$.

Claim: as an algebraic variety, $C_{std} \cong \mathbb{P}^1$. Same as pythagorean theorem: $X_0^2 + X_1^2 = X_2^2$ by $X_2 \mapsto iX_2$ first of course. Every pythagorean triple is one of them. $\mathbb{P}^1 \to C_{std} \subset \mathbb{P}^2$ by $[a_0 : a_1] \mapsto [a_0^2 - a_1^2 : i(a_0^2 + a_1^2) : 2a_0a_1]$ is an isomorphism. Look on patches to see that it's an isomorphism, and same for inverse. Conclusion: every conic is isomorphic to $\mathbb{P}^1$ as a variety (where conic means non-degenerate). Next time, cubics.

15 March 9

15.1 Cubics in $\mathbb{P}^2$

A cubic projective plane curve is $V_+(F) \subset \mathbb{P}^2$ for $F \in \mathbb{C}_3[X_0, X_1, X_2]$. Reducible type: (1) 3 times a line: (1a) L_1^3 or (1b) $L_1^2 L_2$ or (1c) $L_1 L_2 L_3$ (note: 1c can degenerate if all three lines intersect at the same point). Also (2) can get (2a) conic and line or (2b) conic and tangent line (more rare; also, haven't defined tangent line). For (3) the irreducible ones we either have (3a) smooth (3b) node or (3c) cusp. This is what this course is supposed to be about. Examples: $y^2 = x(x-1)(x-\lambda)$ for $\lambda \in \mathbb{C}$. When $\lambda = 0$, get $y^2 = x^3 - x^2$ a cusp, and when $\lambda = 1$, get a nodal singularity (velocity always positive). Think $x = \frac{X_1}{X_0}$, $y = \frac{X_2}{X_0}$. Then homogenize to get

$$V_+(X_0X_2^2 - X_1^2(X_1 - X_0))$$

from $y^2 = x^2(x-1)$, $V_+(X_0X_2^2 - X_1^3)$ from $y^2 = x^3$ say, and $V_+(X_0X_2^2 - X_1(X_1 - X_0)(X_1 - 2X_0))$ from $y^2 = x(x-1)(x-2)$. In this last example, 2 can be replaced by any $\lambda \in \mathbb{C} \setminus \{0, 1\}$. Not that easy to show, but all irreducible plane cubic curves are isomorphic to one of these. Let's explain why $\lambda \in \mathbb{C} \setminus \{0, 1\}$ curve is not $\cong \mathbb{P}^1$.

Facts about $C = V_+(X_0X_2^2 - X_1(X_1 - X_0)(X_1 - \lambda X_0))$:

(1) C is nonsingular - this has to be a global question

(2) $U_0 \cap C$ is isomorphic to $X = V(y^2 - x(x-1)(x-2)) \in \mathbb{C}^2$

(3) The ring $\mathcal{O}(U_0 \cap C) = \mathcal{O}(X) = \mathbb{C}[x, y]/(y^2 - x(x-1)(x-2))$ is NOT a UFD.

Hence, it suffices to show that every open $U \subset \mathbb{P}^1$ gives $\mathcal{O}(U)$ a UFD. This fact would imply that $C \ncong \mathbb{P}^1$ by our definitions regarding morphisms of varieties. [This trick isn't really useable]. Here, non-unique factorization, recall is measured by the non-trivial *class group*. We know $\mathcal{O}(\mathbb{P}^1) = \mathbb{C}$ is a UFD. Let's prove the necessary fact about

$\mathbb{P}^1$. Well $\mathbb{P}^1 = \mathbb{C} \amalg \{\infty\}$ with coordinate $x = \frac{X_1}{X_0}$. Suppose $U = \mathbb{P}^1 \setminus \{\infty, t_1, \ldots, t_n\}$ is an open subset, then

$$\mathcal{O}(U) = \mathbb{C}[x, \frac{1}{(x-t_1)\cdots(x-t_n)}]$$

the localization of a UFD, namely $\mathbb{C}[x]$ so it's a UFD (you just get a few more constants). Now $U = \mathbb{P}^1 \setminus \{t_1, \ldots, t_n\}$ distinct, then $\infty \in U$, so

$$\mathcal{O}(U) = \mathbb{C}[y, \frac{1}{(y-s_1)\cdots(y-s_n)}]$$

where $y = \frac{x}{x-t_1}$, $s_i = \frac{t_i}{t_i - t_1}$; if $n = 0$, same as $\mathbb{C}$.

Now, we've seen that for $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{C})$, we get an automorphism $\mathbb{P}^1 \to \mathbb{P}^1$ by $[x_0 : x_1] \mapsto [ax_0 + bx_1 : cx_0 + dx_1]$ hence in affine coordinates we get

$$x = \frac{X_1}{X_0} \mapsto \frac{iX_0 + dX_0}{aX_0 + bX_1} = \frac{c + d\frac{X_1}{X_0}}{a + b\frac{X_1}{X_0}} = \frac{c + dx}{a + bx}$$

valid whenever this makes sense; so we've concluded that because $\mathbb{C}[x] = \mathcal{O}(\mathbb{P}^1 \setminus \{\infty\})$ that

$$\mathbb{C}[\frac{c+dx}{a+bx}] = \mathcal{O}(\overset{1}{\mathbb{P}} \setminus \{[b : -a]\}$$

(check) because by pulling back coordinate by the map.

To finish, we show that $R = \mathbb{C}[x, y]/(y^2 - x(x-1)(x-2))$ is NOT a UFD. There is a ring map $\mathbb{C}[x] \to R$ and every element of R can be written uniquely as $a + by$ with $a, b \in \mathbb{C}[x]$. Define the norm of $a + by$ to be

$$Nm(a + by) = (a + by)(a - by) = a^2 - b^2y^2 = a^2 - x(x-1)(x-2)b^2.$$

Because $(x, y) \mapsto (x, -y)$ is an automorphism of R, we see that it's in particular multiplicative (check). Hence the set of all $\{(a + by)(a - by)\}$ is stable. Note: if $Nm(\alpha)$ is a unit then α is a unit. If you divide a unit, you're a unit! Norm of non-zero things is non-zero, also. Unit has a norm that is also a unit! (not completely trivial). For example, $Nm(y) = -x(x-1)(x-2)$ and $Nm(x) = x^2$. If R was a UFD, then because $y^2 = x(x-1)(x-2)$ in R, we would get a prime element $f \in R$ dividing both y and x, then $Nm(f)$ divides $Nm(y)$ which is $-x(x-1)(x-2)$ and $Nm(f)$ divides $Nm(x)$ which is x^2 so $Nm(f) = cx$ or $Nm(f) = c$ for $c \in \mathbb{C}^*$, but f a unit would mean in this latter case that f can't be prime. Write $f = a + by$. The norm then is $Nm(f) = a^2 - y^2b^2$ so

$$a^2 - x(x-1)(x-2)b^2 = cx$$

but this forces $x \big| a$. Then look at the leading terms of a^2 and $x(x-1)(x-2)b^2$: they can't be equal to cancel and give cx as supposedly they do.$\square$.

15.2 Nonsingular curves

In affine space, $p \in X \subset \mathbb{C}^n$ a point on a quasi-affine curve, then by definition p is a nonsingular point of X iff $\exists f_1, \ldots, f_{n-1} \in I(X)$ such that

$$\operatorname{rank} \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_{n-1}}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \cdots & \frac{\partial f_{n-1}}{\partial x_n} \end{bmatrix} (p) = n - 1.$$

Note: this only depends on $I(X)$ and the point p. So we make shrink or enlarge X at will. In particular we may replace X by its Zariski closure. If $p \in X \subset \mathbb{C}^n$ is a nonsingular point on an algebraic curve then $X \cap B_\epsilon^{2n} \cong B_\epsilon^2$, that is, looking at a little ball of real dimension $2n$ in $\mathbb{C}^n$ intersected with curve gives a little disc from $\mathbb{C}$ around 0 say (in usual topologies). Hence smooth curves are complex 1-manifolds. Example: $y + yx + x^3 = 0$, $p = (0, 0)$, then

$$\{(x, y) \in \mathbb{C}^2 : y + yx + x^3 = 0 \ : \ |x|^2 + |y^2| < \epsilon\} \cong \text{disc}$$

Next lecture, will look closure at this with the implicit function theorem (holomorphic version).

16 March 11

Situation: $p \in C \subset \mathbb{C}^n$, C an algebraic curve, p a nonsingular point. Target: want to show $\exists$ a usual open neighborhood $p \in U \subset \mathbb{C}^n$ such that $C \cap U$ is homeomorphic to a disk, a ball in $\mathbb{C}$. What will come out of the proof will be <u>better</u> than a homeomorphism. We reduced this to "solving" a system of equations of the form $0 = x_k - \varphi_k(x_1, \ldots, x_n)$ for $1 \leq k \leq n-1$, where $\varphi_k \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes to order ≥ 2 at $(0, \ldots, 0)$ - i.e. there are no constant or linear terms. For $x \in \mathbb{C}^n$ set $||x|| = \max |x_i|$ (any norms induce the same topology).

Lemma 31 *for $\varphi(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ with no linear and constant terms $\exists C > 0$ such that*

$$|\varphi(x_1 + y_1, \ldots, x_n + y_n) - \varphi(x_1, \ldots, x_n)| < C||x|| \cdot ||y||$$

$\forall x, y \in \mathbb{C}^n$ with $||y|| \leq ||x|| \leq 1$.

Proof: look just at the monomials. Which monomials $x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n}$ can occur in the expansion? We know $\sum i_k + \sum j_k \geq 2$ and $\sum i_k \geq 1$. Then clearly because $||y|| \leq ||x|| \leq 1$ get $|x_1^{i_1} \cdots y_n^{j_n}| \leq ||x||||y||$ and let C be the sum of the absolute values of the coefficients of the monomials. $\square$

For example, $0 = x - \varphi(x, y)$, approximation number one: $x = \varphi(0, y)$, then $x = \varphi(\varphi(0, y), y)$, etc...[15]

[15] ???

Lemma 32 *Given $\varphi_1, \ldots, \varphi_n \in \mathbb{C}[x_1, \ldots, x_n]$ as in Lemma 1, pick $C > 0$ which works for each of them. Let $f_1, \ldots, f_{n-1} \in \mathbb{C}[z]$, $\epsilon > 0$, $k \geq 2$ such that*

(a) $|f_i(z)| \leq A|z|^2 \ \forall |z| < \epsilon$
(b) $|f_j(z) - \varphi_j(f_1(z), \ldots, f_{n-1}(z), z)| \leq B|z|^k \ \forall |z| < \epsilon$
(c) $A\,\epsilon^2 \leq 1$
(d) $B\,\epsilon^{k-1} \leq 1$
(e) $\epsilon \leq 1$

Then setting $g_j(z) = \varphi_j(f_1(z), \ldots, f_{n-1}(z), z)$ we have

(0) $|g - j - f_j| \leq B|z|^k \ \forall |z| < \epsilon$
(1) $|g_j| \leq (A + \epsilon^{k-2}\,B)|z|^2 \ \forall |z| < \epsilon$
(2) $|g_j - \varphi_j(g_1, \ldots, g_{n-1}, z)| \leq BC|z|^{k+1} \ \forall |z| < \epsilon$.

Proof: (0) and (1) are trivial from (b) and (a). To prove 2, apply Lemma from before to

$$|\varphi_j(f_1+\Delta_1, \ldots, f_{n-1}+\Delta_{n-1}, z) - \varphi_j(f_1, \ldots, f_{n-1}, z)| \leq C||(f_1, \ldots, f_{n-1}, z)|| \cdot ||(\Delta_1, \ldots, \Delta_{n-1}, 0)||.$$

Lemma from before applies because

$$1 \geq \epsilon \geq ||(f_1, \ldots, f_{n-1}, z)|| = ||z|| \geq B||z||^k \geq ||(\Delta_1, \ldots, \Delta_{n-1}, 0)||$$

which follows from (e), (c), (d), (b) respectively. But this is $\leq BC|z|^{k+1}$. $\square$

Start with $\varphi_1, \ldots, \varphi_{n-1}, C$ as in Lemma above. Also pick a C_0 such that $|\varphi_j(0, \ldots, 0, z)| \leq C_0|z|^2$ for $|z| \leq 1$ (find a C_0 for yourself as in Lemma twice before). Take $\epsilon = \min\{\frac{1}{2}, \frac{1}{2C}, \frac{1}{2C_0}\}$. Set $f_1^{(0)} = \cdots = f_{n-1}^{(0)} = 0$. By induction set $f_j^{(i)} = \varphi_j(f_1^{(i-1)}, \ldots, f_{n-1}^{(i-1)}, z)$. The I. H. is that (α)

$$|f_j^{(i)}(z)| \leq C_0(1 + \epsilon\,C + (\epsilon\,C)^2 + \cdots + (\epsilon\,C)^{i-1})|z|^2$$

and (β):

$$|f_j^{(i+1)}(z) - f_j^{(i)}| \leq C_0 C^i |z|^{i+2} \qquad \forall |z| < \epsilon\,.$$

The pretty part is that we've got the same ϵ! Proof by induction: $i = 0$ is trivial for (α), and for (β) this is true because $|\varphi_j(0, 0, \ldots, 0, z) - 0| \leq C_0|z|^2$. In Lemma 2(change number), check hypotheses: (e) is trivial, $A = C_0(1 + \epsilon\,C + \cdots + (\epsilon\,C)^{i-1})$, and $B = C_0 C^i$ and $k = i + 2$ Then we get $(a) A \cdot \epsilon^2 \leq 1$ works because $(1 + \epsilon\,C + \cdots + (\epsilon\,C)^{i-1}) \leq 2$. Also (d) we have $\epsilon^{i+1}\,C_0 C^i \leq 1$ since it's $(\epsilon\,C)^i(\epsilon\,C_0) \leq 1$. New A and B here; obvious from (2) of Lemma.

Conclusion: on the disk of radius a, the functions $f_j^{(i)}$ as $(i \to \infty)$ converge uniformly; $|Cz|^{i+2}$, $|C_z| \leq \frac{1}{2}$, $\sum \left(\frac{1}{2}\right)^n < \infty$ to a function f; and so we get $f_j = \varphi_j(f_1, \ldots, f_{n-1}, z)$ because φ_j is continuous, hence limit is special.

Black box: because convergence is uniform, the functions f_i are continuous but even holomorphic! Could be that given a differential equation, might find formal power series solution *different* from the ones you get from 5-times differentiating...

Addendum: $\exists\, \delta > 0$ such that $\forall |z| < \epsilon$, $\exists$ only one solution $y_1, \ldots, y_{n-1}$ of $0 = y_1 - \varphi_1(y_1, \ldots, z)$ up to $0 = y_{n-1} - \varphi_{n-1}(y_1, \ldots, y_{n-1}, z)$ when $|y_i| < \epsilon$. *Proof:* if there are any two y and y' solutions, then estimate $|\varphi(y_1, \ldots, y_{n-1}, z) - \varphi(y_1', \ldots, y_{n-1}', z)|$ using Lemma 1 from before (not actually this in our numbering). But this means $f_1, \ldots, f_{n-1}$ are unique (check) and

$$X \cap \{|x_i| < \epsilon, |x_n| < \delta\} = \{(f_1(z), \ldots, f_{n-1}(z), z) : \ |z| < \delta\}.$$

So $\exists!$ solution, but point-wise convergence shows that the *method* for getting the solution is unique.

Upshot: $p \in C \subset \mathbb{C}^n$ nonsingular point of an algebraic curve then $\exists$ a projection $\pi : \mathbb{C}^n \to \mathbb{C}$ and an open nbd U of p in $\mathbb{C}^n$ and an open nbd V of $\varphi(p)$ such that $C \cap U \cap \pi^{-1}(V) \to V$ is a homeomorphism whose inverse is given by *holomorphic functions*. For example, $\{y^2 - x = 0\} = C \to \mathbb{C}$ by $(x, y) \mapsto x$ is the wrong projection; $(x, y) \mapsto y$ works because (y^2, y) is holomorphic. Will have some points even if the curve where the projection is "wrong" - like $z \mapsto z^2$, in which case inverse is $z^{1/2}$.

17 March 23

17.1 Implicit Function Theorem.

Theorem 6 *(ImpFT) $p \in C \subset \mathbb{C}^n$ nonsingular point on a curve, then $\exists \Phi : \{z : |z| < 1\} \to C$ with $\Phi(0) = p$ and Φ given by $(g_1, \ldots, g_n)$ with each g_i holomorphic, at least one non-zero derivative, and Φ a homeomorphism of Δ disc $\{z : |z| < 1\}$ onto a usual open nbd of p in C.*

This implies C is a differentiable manifold because holomorphic functions are differentiable. Also other formulation:

Theorem 7 *$p \in C \subset \mathbb{C}^n$ a nonsingular point. Choose a linear projection $\pi : \mathbb{C}^n \to \mathbb{C}$ which does not collapse the tangent space to C at p (). Then $\forall$ sufficiently small $\epsilon > 0$, $\exists\, \delta > 0$ such that*

$$C \cap \{|x_i - p_i| < \epsilon : \ i = 1, \ldots, n\} \cap \pi^{-1}(\{z : |z| < \delta\}) \to \{z : |z| < \delta\}$$

is a homeomorphism whose inverse is given by holomorphic functions

Also ex: singularity people like: not smooth, maybe $y^2 = x^3$, and throw a ball S^3 around it, and look at its intersection with a curve. It's a knot or link! For example $\{y^2 = x^3\} \cap \{|y|^2 + |x|^2 = 1\}$ solved by $|t|^6 + |t|^4 = 1$ since parametrized by $y = t^3, x = t^2$ for $t \in \mathbb{C}$, and there's only one real $|t|$ positive satisfying this if 1 is small enough (hah). Then let $t = re^{i\theta}$ $\forall \theta$, $r = |t|$, some circle, then graphing should give a trefoil knot! Also in $xy = 0$, two discs meet at a point in $4d$, intersection should give the Hopf link - see homework. Now the next topic.

17.2 Resolving singularities

Examples: (A) $x^2 - y^2 + x^3 = 0$ the nodal cubic. Want to make another algebraic curve by adding a new function $z = \frac{y}{x}$ which separates the branches, is in $\mathbb{C}(C)$, and is integral over $\mathcal{O}(C)$ by

$$C^\nu = \{1 - z^2 + x = 0,\ y - xz = 0\}$$

in $\mathbb{C}^3$; these two imply $x^2 - y^2 + x^3 = 0$ by the way, and also $\mathcal{O}(C^\nu) = \mathbb{C}[x, y, z]/(1 - z^2+, y - xz) \cong \mathbb{C}[z]$ and $C^\nu \cong C$ as an algebraic curve.

Intermezzo: if C_1, C_2 are affine curves and $\mathcal{O}(C_1) \cong \mathcal{O}(C_2)$ as $\mathbb{C}$-algebras, then $C_1 \cong C_2$ as algebraic curves. *Proof:* look at ring of functions: $\mathcal{O}(C_1) = \mathbb{C}[x_1, \ldots, x_{n_1}]/I_1$, $\mathcal{O}(C_2) = \mathbb{C}[x_1, \ldots, x_{n_2}]/I_2$, then send $x_1 \mapsto f_1 \bmod I_2$ and $x_{n_1} \mapsto f_{n_1} \bmod I_2$ then check that the map $C_2 \to C_1$ by

$$b \cdot (b_1, \ldots, B_{n_2}) \mapsto (f_1(b_1, \ldots, b_{n_2}), \ldots, f_{n_1}(b_1, \ldots, b_{n_2}))$$

is a morphism and the inverse comes from inverse construction. Check; $h \in I$ then $h(f(\vec{b})) = 0$ but this is in I_2...

For the resolution of the cuspidal cubic, it's $\mathbb{C} = C^\nu \to C$ by $t = \frac{x}{y} \mapsto (t^3, t^2)$ giving $x^2 - y^3 = 0 \subset \mathbb{C}^2$. Now lets define what it means to resolve singularities on a curve.

Definition 26 *If $X \subset \mathbb{C}^n$ is an affine variety, then the function field is $\mathbb{C}(X)$ the fraction field of $\mathcal{O}(X)$.*

In the exercises you will show : if $U \subset X$ is non-empty affine open then restriction map $\mathcal{O}(X) \to \mathcal{O}(U)$ induces an isomorphism of fraction fields. Thus, for the function field, it is sufficient to know the small open U. So if X is any quasi-projective variety, then we DEFINE $\mathbb{C}(X)$ to be the fraction field of $\mathcal{O}(U)$ where $U \subset X$ is some non-empty affine open subvariety. This works because if you have $U, V \subset X$ both non-empty, then $U \cap V \neq \emptyset$ since X is irreducible $\Rightarrow \exists W \subset U \cap V$ an affine-open nonempty and by (*) get $\mathcal{O}(U) \to \mathcal{O}(W)$ and $\mathcal{O}(V) \to \mathcal{O}(W)$ induced isomorphisms and so $\mathbb{C}(U) \cong \mathbb{C}(V)$ (independent of choice).

For curves, let $\varphi : C_1 \to C_2$ be a non-constant morphism of algebraic curves, then choose $U_i \subset C_i$ nonempty affine open with $\varphi(U_1) \subset U_2$. Gives a map $\varphi^* \mathcal{O}(U_2) \hookrightarrow \mathcal{O}(U_1)$ the pull-back and hence $\varphi^* : \mathbb{C}(C_2) \to \mathbb{C}(C_1)$. Injectivity here comes from the fact that it's non-constant: uses closed subset of C... for general varieties say image is Zariski dense (?).

Lemma 33 *In situation above, the field extension $\mathbb{C}(C_2) \subset_{\varphi^*} \mathbb{C}(C_1)$ is **finite**.*

Proof: Recall that both $\mathbb{C}(C_1)$ and $\mathbb{C}(C_2)$ are finitely generated field extensions of transcendence degree 1 over $\mathbb{C}$. Pick $x_1, \ldots, x_n$ in $\mathbb{C}(C_1)$ which generate it as a field over $\mathbb{C}$; pick $t \in \mathbb{C}(C_2)$ which is transcendental over $\mathbb{C}$. Then we get

$$\mathbb{C} \subset \mathbb{C}(\varphi^* t) \subset \varphi^*(\mathbb{C}(C_2)) \subset \mathbb{C}(C_1)$$

where the first is purely transcendental of degree 1. This implies $\mathbb{C}(C_1) \supset \mathbb{C}(\varphi^* t)$ is algebraic and also generated by $x_1, \ldots, x_n$, hence it's finite so $\mathbb{C}(C_1) \supset \mathbb{C}(\varphi^* t)$ finite implies $\mathbb{C}(C_1) \supset \varphi^*(\mathbb{C}(C_2))$ finite. $\square$.

Definition 27 *The degree of φ is $[\mathbb{C}(C_1) : \mathbb{C}(C_2)]$. Also, φ is called birational if $\mathbb{C}(C_1) = \mathbb{C}(C_2)$, i.e. $\deg \varphi = 1$.*

Remark: if $\deg \varphi$ is n then for almost all $c_2 \in C_2$,

$$\#\{c_1 \in C_1 \text{ with } \varphi(c_1) = c_2\} = n.$$

Hopefully we'll do this later; recall fibres and degree of polynomials - you did a special case of this. NB: if φ is birational then $\exists U_2 \subset C_2$ open and non-empty such that $\varphi^{-1}(U_2) \to C_1$ is an isomorphism (non-trivial to prove).

Definition 28 *Let C be an algebraic curve. Then a resolution of singularities of C is a morphism $\nu : C^\nu \to C$ of algebraic curves such that*

(i) C^ν is non-singular

(ii) $C^\nu \to C$ is birational

(iii) ν is a proper map of underlying topological spaces

Note: (iii) prevents you from just using $C^\nu = C \setminus \{$ singular points $\}$. In algebraic geometry, this would mean finite, which we haven't defined yet.

Remarks: (a) resolutions always exist (will see this later) (b) sometimes, often, the map $\nu : C^\nu \to C$ is called the "normalization" of C because for curves the normalization gives a resolution! Next time: maps between non-singular curves.

Important distinction: for $\mathbb{P}^1$, we saw $\mathcal{O}(\mathbb{P}^1) = \mathbb{C}$. These regular functions are glued up functions on the opens. However, $\mathbb{C}(\mathbb{P}^1)$ is not the field of fractions of $\mathcal{O}(\mathbb{P}^1)$, but of $\mathcal{O}(U)$ for an *affine* open $U \subset \mathbb{P}^1$, so $\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(x)$.

18 March 25

18.1 Discrete Valuations

Now we're going to do something "really fun": discrete valuations. We are going to treat an algebraic curve in many ways. Suppose that $\alpha \in \mathbb{C}$, can define $\nu_\alpha : \mathbb{C}(x)^* \to \mathbb{Z}$, where $\mathbb{C}(x)^*$ are the units of the function field of $\mathbb{P}^1$, by

$$f \mapsto \text{ order of vanishing of } f \text{ at } x = \alpha.$$

So

$\nu_\alpha\left(\frac{P}{Q}\right) = \nu_\alpha(P) - \nu_\alpha(Q)$

$\nu_\alpha(x - \alpha) = 1$

$\nu_\alpha\left(\frac{x+\alpha+1}{(x-\alpha)^2}\right) = -2$
the valuation of the function 0 is ∞.

Here are some properties of ν_α:

(i) it is surjective
(ii) $\nu_\alpha(c) = 0$ for $c \in \mathbb{C}\setminus\{0\}$
(iii) $\nu_\alpha(fg) = \nu_\alpha(f) + \nu_\alpha(g)$
(iv) $\nu_\alpha(f+g) \geq \min\{\nu_\alpha(f), \nu_\alpha(g)\}$. Observe that strict inequality can occur: $1 = \nu_\alpha(x-\alpha) > \min\{\nu_\alpha(1), \nu_\alpha(x-\alpha-1)\} = 0$. It turns out that if the inequality is strict then f and g have the same order of vanishing.

Moreover we can also define $\nu_\infty : \mathbb{C}(x)^* \to \mathbb{Z}$ by $f \mapsto$ the order of vanishing of f at ∞. For a rational function $\nu_\infty\left(\frac{P}{Q}\right) = -\deg(P) + \deg(Q)$. Why? Just think that x^{-1} is a function that vanishes to order 1 at ∞, and write $P(x)/Q(x)$ in terms of x^{-1}. Check that the properties still hold for ν_∞. We can now generalize this:

Definition 29 *Let K be a field. A <u>discrete valuation</u> on K is a surjective map $\nu : K^* \to \mathbb{Z}$ such that (i) $\nu(fg) = \nu(f) + \nu(g)$ (ii) $\nu(f+g) \geq \min(\nu(f), \nu(g))$. If $K \supset k$ is an overfield, we say that ν is a discrete valuation of K over k, "K/k", if $\nu(c) = 0\ \forall c \in k \setminus \{0\}$.*

Proposition 6 *If ν is a discrete valuation on $\mathbb{C}(x)/\mathbb{C}$, then $\nu = \nu_\alpha$ for some ! $\alpha \in \mathbb{P}^1 = \mathbb{C} \amalg \{\infty\}$.*

The upshot of this: **points in $\mathbb{P}^1$ are in bijection with discrete valuations on $\mathbb{C}(\mathbb{P}^1)/\mathbb{C}$.** *Proof of proposition*: pick a ν some discrete valuation.

<u>Case 1</u>: $\exists P \in \mathbb{C}[x]$, $P \neq 0$ with $\nu(P) > 0$. Write $P = c\prod_{i=1}^m (x-\alpha_i)$, so $\nu(p) = \nu(c) + \sum_{i=1}^m \nu(x-\alpha_i) > 0$ and $\nu(c) = 0$, so $\Rightarrow \exists \alpha \in \mathbb{C}$ such that $\nu(x-\alpha) > 0$, say $\nu(x-\alpha) = n$. Let us now consider $\nu(x-\beta)$ for $\beta \neq \alpha$. Well

$$\nu(x-\beta) = \nu(x-\alpha+\alpha-\beta) \geq \min\{0, n\} \geq 0 \quad \forall \beta \in \mathbb{C}$$

but if $\nu(x-\beta) > 0$ for some $\beta \neq \alpha$, then $\nu(\beta-\alpha) = 0 = \nu(x-\alpha-(x-\beta)) \geq \min\{\nu(x-\alpha), \nu(x-\beta)\} > 0$ a contradiction. Now we know $\nu(x-\gamma) = n\delta_\gamma^\alpha$ is an indicator function. But any rational function is a product of linear terms, so

$$\nu(f) = \nu\Big(c\prod(x-\gamma)^{e_\gamma}\Big) = e_\alpha \nu(x-\alpha) = e_\alpha \cdot n = n \cdot \nu_\alpha(f)$$

by definition of ν_α. So $\nu = n\nu_\alpha$, but if $n > 1$, then ν is not surjective, so we must have $n = 1$ i.e. $v = v_\alpha$.

<u>Case 2</u>: $\forall P \in \mathbb{C}[x]$ with $P \neq 0$, $\nu(P) \leq 0$. Pick $\alpha \in \mathbb{C}$ with $n = \nu(x-\alpha)$ maximal ($n \leq 0$). Then $\nu(x-\beta) = \nu(x-\alpha) + \nu(\alpha-\beta) \geq \min(n, 0) = n$ but α maximal so $\nu(x-\beta) = n$ always. Then $\nu\left(\frac{P}{Q}\right) = [-\deg P + \deg Q] \cdot (-n) = (-n)\nu_\infty\left(\frac{P}{Q}\right)$

and again surjectivity implies $-n = 1$. $\square$

This says $\mathbb{P}^1$ is a nice algebraic curve: if you know its function field, you can find directly its points! We want to generalize this proposition to other nonsingular projective curves (this will take some work). Now we'll do some other algebra which is also fun.

18.2 Power Series

First, an example. Consider the power series ring $\mathbb{C}[[x]]$: it is a UFD with one prime element (x); everybody is $x^k \cdot$ unit, where the units are power series with $a_0 \neq 0$ which implies invertibility; it is a *local ring*[16] with maximal ideal (x); a domain; $\mathbb{C}[[x]]/(x) = \mathbb{C}$ so x is prime; also the Laurent series field $\mathbb{C}((x)) = \mathrm{Frac}(\mathbb{C}[[x]])$. Now if $f \in \mathbb{C}[[x]]$, $f = \sum a_i x^i$ is a unit if and only if $a_0 =$ "$f(0)$" $\neq 0$: to invert f, just take $f = a_0(1 + \frac{a_1}{a_0}x + \cdots) = a_0(1 + b_1 x + b_2 x^2 + \cdots)$ and call this right sum δ, then $f^{-1} = a_0^{-1}\frac{1}{1+\delta} = a_0^{-1}(1 - \delta + \delta^2 - \delta^3 + \cdots)$. Since $x \big| \delta \Rightarrow x^3 \big| \delta^3$, etc, so $\mathbb{C}((x)) = \mathbb{C}[[x]]\left[\frac{1}{x}\right]$; all we have to do is invert x! A Laurent series is a sum $\sum_{-\infty < i} a_i x^i$ (finitely many terms with negative exponent). Then $f \in \mathbb{C}((x))^* \Rightarrow f = x^k u$, $u \in \mathbb{C}[[x]]^*$, $k \in \mathbb{Z}$, the order of vanishing at $x = 0$. This gives a discrete valuation $\nu : \mathbb{C}((x)) \to \mathbb{Z}$ by $f = x^k u \mapsto \nu(f) = k$. Exercise: show that this is a discrete valuation. Check that $\mathbb{C}[[x]]^*$ are elements with valuation ≥ 0; $f \in (x)^m \Leftrightarrow \nu(f) \geq m$, or $a, b \in \mathbb{C}[[x]] \setminus \{0\}$ then a divides b in $\mathbb{C}[[x]]$ if and only if $\nu(b) \geq \nu(a)$.

18.3 Hensel's Lemma

Projecting a curve $C \to \mathbb{C}$, we want to look at the hard fibers - to zoom in so close that you don't have a function any more. We turn to Hensel's Lemma over a power series ring:

Lemma 34 *(Hensel) Let $f \in \mathbb{C}[[x]][T]$. Assume $f \bmod x = \overline{h} \cdot \overline{g}$ with $\overline{h}, \overline{g} \in \mathbb{C}[T]$ relatively prime. Then $f = h \cdot g$ for some $h, g \in \mathbb{C}[[x]][T]$ with $h \bmod x = \overline{h}$ and $g \bmod x = \overline{g}$.*

NB: we'll see in the proof that we can take g with $\deg_T(g) = \deg_T(\overline{g})$ for just one of the g, h. Counterexample to both: $f = xT^{100} + T(T-1)$, $\overline{g} = T$, $g = T$, $\overline{h} = T - 1$, $h = xT^{99} + T - 1$. There's another version of H's Lemma: solutions mod x not a double root then exists elements of $\mathbb{C}[[x]]$ a solution of f; means $\exists$ linear factor relatively prime to the rest...(?)

Proof of Lemma: We will show by induction. IH_n the induction hypothesis being $\exists h_n, g_n \in \mathbb{C}[[x]][T]$ such that $f \bmod x^n = h_n \cdot g_n$, $h_n \bmod x^n = h_{n-1} \bmod x^n$,

[16] From wikipedia: a ring R is local if it has any one of the following equivalent properties: (i) R has a unique maximal left ideal (ii) a unique maximal right one (iii) $1 \neq 0$ and the sum of any two non-units in R is a non-unit (iv) $1 \neq 0$ and $\forall x \in R$, either x or $1 - x$ is a unit (v) if a finite sum is a unit, then so are some of its terms (in particular the empty sum is not a unit, hence $1 \neq 0$).

$g_n \bmod x^n = g_{n-1} \bmod x^n$, $\deg_T(h_n) \leq \deg_T(f) - \deg_T(\overline{g})$ and $\deg_T(g_n) \leq \deg_T(\overline{g})$ (also need starting case). If we can prove this, then we set $h = \sum a_i T^i$ for $i \leq \deg_T(f) - \deg_T(\overline{g})$ with $a_i \bmod x^n = i$th coefficient of $h_n \bmod x^n$; $g = \sum_{i<\deg_T(\overline{g})} b_i T^i$ with $b_i \bmod x^n = i$th coef of $g_n \bmod x^n$. For example, consider $h_1 = 1 + 1T$, $h_2 = (1 + x + x^2) + (1 + x^5)T$, ... WANT H_n OK MOD x^n (the garbage evens out), which would mean $f = g \cdot h$ because $\bmod x^n$ they are = for all $n \geq 1$. [Look up complete local rings...] Along the way, we have to control powers of T; since we have to end up having a polynomial. Prove now: IH_1: just take $h_1 = \overline{h}$ and $g_1 = \overline{g}$ but seen as elements of $\mathbb{C}[[x]][T]$. For $IH_n \to IH_{n+1}$, $f = b_n g_n + x^n r$ and $\deg_T(r) \leq \deg_T(f)$ since $\deg(h_n g_n) = \deg(h_n) + \deg(g_n) \leq \deg(f) - \deg(\overline{g}) + \deg(\overline{g}) = \deg(f)$. So we can write $r \bmod x = \overline{ag} + \overline{bh}$ for $\overline{a}, \overline{b} \in \mathbb{C}[T]$ such that $\deg_T(\overline{b}) < \deg(\overline{g})$ which implies $\deg_T(\overline{a}) \leq \deg_T(f) - \deg_T(\overline{g})$. Take $h_{n+1} = h_n - ax^n$ and $g_{n+1} = g_n - bx^n$, this works where a, b without the barre are in $\mathbb{C}[[x]][T]$. Then

$$h_{n+1}g_{n+1} = (h_n - x^n a)(g_n - x^n b) = h_n g_n - x^n(ag_n + bh_n) + x^{2n}ab = x^n(r - ag_n - bh_n) + x^{2n}ab \in (x^{n+1})$$

since this first term multiplied by x^n is 0 mod x by construction. $\square$

RMRK: the most general form of H's Lemma: a $f \in A[T]$, A is a local, complete ring with maximal idea $\mathfrak{m}$ and $f \bmod \mathfrak{m} = \overline{g} \cdot \overline{h}$ with $\gcd(\overline{g}, \overline{h}) = 1$, $\overline{g}, \overline{h} \in A/\mathfrak{m}[T]$ then $f = g \cdot h$ for $g, h \in A[T]$ such that $\overline{g} = g \bmod \mathfrak{m}$, $\overline{h} = h \bmod \mathfrak{m}$. A variant: $f \in A[T]$, $\overline{f} = f \bmod \mathfrak{m}$, $\overline{\alpha} \in A/\mathfrak{m}$, $\overline{f}(\overline{\alpha}) = 0$, $\overline{f}'(\overline{\alpha}) \neq 0$, then $\exists \alpha \in A$ such that (i) $f(\alpha) = 0$ and (ii) $\alpha \bmod \mathfrak{m} = \overline{\alpha}$ [take $\overline{g} = T - \overline{\alpha}$].

19 March 30

Last time, Hensel's Lemma: (i) $f \in \mathbb{C}[[x]][T]$ (ii) $f \bmod x = \overline{g}\overline{h}$ (iii) $\gcd(\overline{g}, \overline{h}) = 1 \Rightarrow$ can find $f = g \cdot h$ in $\mathbb{C}[[x]][T]$ and $\deg_T(g) = \deg_T(\overline{g})$. In analysis, we zoom in at a point and look at small balls; in algebra, we do this with power series. Idea: with the ring $\mathbb{C}[[x]]$ as the base curve, what curves can go over it?

Lemma 35 *Let $P(T) \in \mathbb{C}((x))[T]$ of degree $d \geq 2$. There exists an integer $q \geq 1$ such that p factors nontrivially over the field $\mathbb{C}((x^{1/q}))$.*

Note: given such a q, we have a diagram

$$\begin{array}{ccc} \mathbb{C}((x)) & \subset & \mathbb{C}((x^{1/q})) = \mathbb{C}((y)) \\ \uparrow & & \uparrow \\ \mathbb{C}[[x]] & \subset & \mathbb{C}[[x^{1/q}]] = \mathbb{C}[[y]] \end{array}$$

$$x \longrightarrow (x^{1/q})^q = y^q$$

where the map below is an injective ring map, and above $\mathbb{C}((x)) \hookrightarrow \mathbb{C}((y))$ is a finite extension of fields of degree q with basis $x^0 = 1, \ldots, x^{(q-1)/q}$. The Lemma

says that we can factor at the **cost** of adding $x^{1/q}$. Then HL: suffices to factor mod x; also applies to $y = x^{1/q}$. Assume P is monic (normalize leading coefficient). $P(T) = T^d + a_1 T^{d-1} + \cdots + a_d$ with $a_i \in \mathbb{C}((x))$. Now something clever:

$$x^{ed} P\Big(\frac{T}{x^e}\Big) = T^d + a_1 x^e T^{d-1} + a_2 x^{2e} T^{d-2} + \cdots + a_d x^{ed}.$$

When we go mod x, we want each coefficient in the power series ring, then divide by x want reducible. If e is huge, then all $a_i x^{e(d-i)}$: we need all coefficients in $\mathbb{C}[[x]]$ but not all divisible by x, lest when we go mod x we get $T^d = T \cdots T$ which isn't factorizable into two relatively prime parts. Set

$$-e = \min_{i=1,\ldots,d} \frac{\nu(a_i)}{i}$$

where ν over $\mathbb{C}[[x]]$ extends to $\mathbb{C}((x))$. This is equal to some $\frac{p}{q} \in \mathbb{Q}$ and is where we get our q. But since we are only trying to factor in $\mathbb{C}[[x^{1/q}]]$, let this be the q, and then over $\mathbb{C}((x^{1/q}))$ we have $x^{ed} P\Big(\frac{T}{x^e}\Big) = T^d + \sum_{i=1}^d (x^{ie} a_i) T^i = T^d + \sum_{i=1}^d b_i T^i$ such that $\forall i$ we have $b_i \in \mathbb{C}[[x^{1/q}]]$ and for at least one $i \in \{1, \ldots, d\}$ we have $b_i \bmod x^{1/q} \neq 0$. The valuation in y is q times the valuation in x (ν behaves like log): $\nu(b_i) = \nu(x^{ie} a_i) = ie + \nu(a_i) = i\big(\frac{\nu(a_i)}{i} + e\big)$. We want $e + \frac{\nu(a_i)}{i} \geq 0$ for all i and 0 for at least one i) so we conclude that $x^{ed} P\Big(\frac{T}{x^e}\Big) \mod x^{1/q} = T^d +$ at least oneterm cT^i for some $c \neq 0$ in $\mathbb{C}$. AND NOW YOU ARE STUCK! Because it could be that this factors as $(T - c)^d$.

Now we repair the damage on the spot using a special transformation. Step 1: make P monic.

Step 2: Tschirnhausen transformation applied to P, assume $P(T) = T^d + a_2 T^{d-2} + \cdots + a_d$ (achieved by $T \mapsto T \pm \frac{a_i}{d}$). Step 3: $-e = \min_{2 \leq i \leq d} \frac{\nu(a_i)}{i}$ and we get back to where we started and the coefficient of T^{d-1} is still 0. Claim: any $P = T^d + c_2 T^{d-2} + \cdots + c_d \in P[T]$ such that $c_i \neq 0$ for some i has factorization $\overline{p} = \overline{g} \cdot \overline{h}$ nontrivial with $\gcd(\overline{g}, \overline{h}) = 1$. Then apply HL over $\mathbb{C}[[x^{1/q}]]$ this ring to get $x^{ed} P\Big(\frac{T}{x^e}\Big) = H \cdot W$ so P factors non-trivially too. $\square$

Lemma 36 *Any $P \in \mathbb{C}((x))[T]$ factors completely over $\mathbb{C}[[x^{1/q}]]$ for some $q \geq 1$.*

Pf: Start with P; P is linear, then we're done; if $\deg P \geq 2$, then apply the previous lemma, and the pieces strictly decrease in degree. $\square$

The moral of the story: **we can fully describe the algebraic closure of the field $\mathbb{C}((x))$: it is the union over all qs of $\mathbb{C}((x^{1/q}))$.** More generally, given $K \subset L$ a field extension, how to recognize if $L = \overline{K}$? Well, L has to be an algebraic

extension, and so we check that every polynomial in K factors in L. Now you don't have to check for this in L! Consider the fundamental group π_1 of a field without zero, (draws picture), it's $\mathbb{Z}$. Well

$$Gal\Big(\overline{\mathbb{C}((x))}/\,\mathbb{C}((x))\Big) = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/n\,\mathbb{Z}\,.$$

The Galois group is the profinite completion of the integers (the inverse limit on the right is taken via divisibility).[17]

Proposition 7 *Any finite extension $\mathbb{C}((x)) \subset K$ of fields is obtained by adjoining a qth root of x where $q = [K : \mathbb{C}((x))]$.*

Proof: Step 1: By the previous Lemma, $K \subset \mathbb{C}((x^{1/r}))$ for some r.

Step 2: $Gal\big(\,\mathbb{C}((x^{1/r}))/\,\mathbb{C}((x))\big) = \mathbb{Z}/r\,\mathbb{Z}$ containing σ a generator. Then $\sigma(x^{1/r}) = e^{\frac{2\pi i}{r}} \cdot x^{1/r}$ then we get $\sigma^l(x^{1/r}) = e^{\frac{2\pi i e}{r}} x^{1/r}$ we get all of them. Step 3: All subgroups of cyclic groups are cyclic, hence by Galois correspondence, $Gal(K/\,\mathbb{C}((x)))$ is cyclic. □

Proposition 8 *Let $\mathbb{C}[[x]] \subset A$ be a finite extension of rings such that A is reducible (i.e., if $a \in A$ nilpotent then $a = 0$). Then $\exists!$ ring extension $A \subset B$ such that*

(i) $B \cong \mathbb{C}[[y_1]] \times \cdots \times \mathbb{C}[[y_r]]$ for some r and $x \mapsto (y_1^{e_1}, \ldots, y_r^{e_r})$ for some $e_1, \ldots, e_r \geq 1$ (really the qs from before).

(ii) $A[1/x] \cong B[1/x]$; he mentions "away from the puncture – think Spec"

(iii) compute B from A: B is the integral closure of A in $A[1/x]$ which is also the integral closure of $\mathbb{C}[[x]]$ in $A[1/x]$

Definition 30 *(i)If $A \subset R$ is a ring extension, then the integral closure of $A \subset R$ is $A' = \{f \in R : f$ is integral over $A\}$; it is an A-subalgebra of R.*

(ii) We say A is integrally closed in R iff $A = A'$

(iii) if A is a domain, we say A is a normal domain iff A is integrally closed in its fraction field

Algebraic Fact: if $K \subset R$ is a finite ring extension, K a field, R is reduced, then R is a finite product of fields (look at annihilator...). Can finally prove the proposition:

Proof: $\mathbb{C}[[x]] \subset A$ is finite and A is reduced; then invert x: $\mathbb{C}((x)) \hookrightarrow A[1/x]$ is finite and $A[1/x]$ is reduced. Check that A reduced $\Rightarrow A[1/x]$ reduced. Projection to factors, so by the fact, $A[1/x] = L_1 \times \cdots \times L_k$ is a finite product of fields L_i. By the previous proposition, $\mathbb{C}((x)) \subset L_i \cong \mathbb{C}((y_i))$ with $y_i^{e_i} = x$. Then check if $B :=$integral closure of $\mathbb{C}[[x]]$ in $A[1/x]$, which is explicitly given above $B = \mathbb{C}[[y_1]] \times \cdots \times \mathbb{C}[[y_r]]$

[17] "What just happened?" moment number 5453

with $x = (y_1^{e_1}, \ldots, y_r^{e_r})$. Amounts to showing that the integral closure in $X \times Y$ is the product of integral closures; also look at integral closure in $\mathbb{C}((y_i))$ is itself. Since A was assumed finite over $\mathbb{C}[[x]]$, every element of it is integral over $\mathbb{C}[[x]]$ (previous algebraic fact) so $A \subset B$. Then also $B =$ int closure of A (easy - do it). $\square$

What we would like / what will this do for us: at a horrible singularity, have a resolution $C^\nu \to C \to \mathbb{C} \subset \mathbb{P}^1$ and this smoothing out corresponds to $B \to A$ a ring extension. Will get actual power series rings at each point up here, and $\sum e_i = \deg$ of $C \to \mathbb{P}^1$....

20 April 1 - Jarod Alper

20.1 Motivation

$\mathbb{C}$ is a complex curve, potentially has singularities - useful to find resolution of singularities, that is, find smooth curve $C^\nu \to C$ with morphism that is birational (is an isomorphism restricted to an open set in C^ν). For example, nodal and cuspidal cubics - almost everywhere bijections. We can study C by studying C^ν. Now, the algebra behind this.

20.2 Normal rings

Definition 31 *An integral domain A with fraction field $ffA = K$ is normal or integrally closed if $\forall x \in K$ such that $\exists$ a monic polynomial $P(t) \in A[t]$ such that $P(x) = 0$, then $x \in A$.*

For example $\mathbb{C}[x]$ is integrally closed (use the fact that it is a UFD).

Proposition 9 *A a UFD $\Rightarrow$ A normal.*

Proof: Let $x \in K$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in A$. If $x \notin A$, write $x = \frac{f}{g}$ where $\exists p/g$, $p \not| f$ in lowest terms (uses the fact that A is a UFD). Then replace this into the monic polynomial:

$$\left(\frac{f}{g}\right)^n + a_{n-1}\left(\frac{f}{g}\right)^{n-1} + \cdots + a_0 = 0$$

and clearing denominators with g^n gives $f^n + a_{n-1}gf^{n-1} + \cdots a_0 g^n = 0$. Now since $p|g$, p divides the expression above besides f^n, but then $p|f^n \Rightarrow p|f$ since p is prime, a contradiction.$\square$

Definition 32 *A an integral domain with Frac$(A) = K$, then if A is not normal, take the integral closure of A as $\tilde{A} = \{x \in K : \exists \{a_i\} \subset A$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0\}$.*

Facts:
(i) $\tilde{A}$ is a ring
(ii) $\text{Frac}(\tilde{A}) = K$
(iii) $\tilde{A}$ is normal.
Some examples:
(1) $A = \tilde{A}$ if A is integrally closed.

(2) From the cuspidal cubic $V(y^2 - x^3) \subset \mathbb{C}^2$. What is the integral closure of $\mathbb{C}[x, y]/(y^2 - x^3)$? Well $K = \text{Frac}(A) = \mathbb{C}(y/x)$ by $\left(\frac{y}{x}\right)^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x$ and $\left(\frac{y}{x}\right)^3 = \frac{y^3}{x^3} = \frac{y^3}{y^2} = y$, so this field contains x and y. The element $\frac{y}{x}$ satisfies $T^2 - x = 0$ but $y/x \notin A$. Now $A \subset \mathbb{C}\left[\frac{y}{x}\right] \subset \tilde{A}$ then conclude $\mathbb{C}[\frac{y}{x}] = \tilde{A}$ because it is integrally closed. Indeed, for $t = \frac{y}{x}$, $\mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$ and this is isomorphic to our ring $\mathbb{C}[x, y]/(x^3 - y^2)$.

(3) For $A = \mathbb{C}[x, y]/(y^2 - x^2(x+1))$ the nodal cubic, if you complete the ring at the origin, you get a power series ring in two variables (...). $\text{Frac}(A) = \mathbb{C}(t)$ where $t = \frac{y}{x}$, for $t^2 = \left(\frac{y}{x}\right)^2 = \frac{x^2(x+1)}{x^2} = x + 1$ so $x = t^2 - 1$ and also $t^3 = \left(\frac{y}{x}\right)^3 = \frac{x^2(x+1)y}{x^3} = y + \frac{y}{x}$ implies $y = t^3 - t$. Then $t \in \text{Frac}(A)$ satisfies $P(t) = T^2 - (x+1)$ and so $A \subset \mathbb{C}[y/x] = \tilde{A}$ corresponds to $\mathbb{C}^1 \to V(y^2 - x^2(x+1)) \subset \mathbb{C}^2$ by $t \mapsto (t^2 - 1, t^3 - t)$ and we see that $f^{-1}(0, 0) = \{1, -1\}$. Turns out **two curves are birational iff they have the same function field**.

(4) Let $A = \mathbb{C}[x, y]/(y^2 - x(x + 1)(x + 2)$ be a smooth cubic. But $\text{Frac}(A) = \mathbb{C}(x, y)/(y^2 - x(x + 1)(x + 2))$ cannot be written as a fraction field in one variable. It is an elliptic curve of **genus** 1. Is A integrally closed? Amazing fact: $V(I) \subset \mathbb{C}^n$ **is nonsingular iff** $\mathbb{C}[x_1, \ldots, x_n]/I$ **is normal.**, which tells us this is normality is a *local* question.

20.3 A finiteness proof

Suppose $V(I)$ is singular, then $\tilde{A}$ the integral closure of $\mathbb{C}[x_1, \ldots, x_n]/I$: is $\tilde{A}$ finitely generated as a $\mathbb{C}$-algebra? If yes, then $\tilde{A} = \mathbb{C}[y_1, \ldots, y_n]/J \subset \text{Frac}(A)$ is a "resolution of singularities". It turns out that the answer is YES! Great, but requires work. This is the motivation for the next half-hour.

Definition 33 *Let A be an integral domain with Frac$(A) = K$, and $K \subset L$ a field extension. Then take the integral closure of A in L: it is $B = \{x \in L : x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for $a_i \in A\}$.*

Facts:
(i) B is a ring
(ii) $\text{Frac}(B) = L$
(iii) B is integrally closed.

The example to keep in mind for

$$\begin{array}{ccc} K & \subset & L \\ \cup & & \cup \\ A & \subset & B \end{array}$$

is

$$\begin{array}{ccc} \mathbb{C}(x) & \subset & \mathbb{C}(y) \\ \cup & & \cup \\ \mathbb{C}[x] & \subset & \mathbb{C}[y] \end{array}$$

where $y^n = x$. Locally, all field extensions of $\mathbb{C}(x)$ do look like this, though $\exists$ non-cyclic extensions. What we're proving:

Theorem 8 *If A is a normal noetherian ring and $K = Frac(A) \subset L$ a field extension, then the integral closure B of A in L is a finite A-module.*

This is not the same as the original question! "Vague cloud": $C = V(I) \subset \mathbb{C}^n$ a curve, then $\exists\, \mathbb{C}[y] \subset \mathbb{C}[x_1, \ldots, x_n]/I$ such that it's finite (from Noether Normalization). But then the integral closure of $\mathbb{C}[x]$ in L we show to be finitely generated...

Proof: Let B be the integral closure of A in L. Since L is separable over K (since we are over $\mathbb{C}$) by the primitive element theorem, we can write $L = K(y)$ and can choose this $y \in B$ by clearing denominators. Let f be the minimal polynomial of y. A priori we know that $f \in K[T]$, but we claim that $f \in A[T]$, which we now show. Factor $f(T) = (T - y_1) \cdots (T - y_r)$ where $y = y_r$. Let $r = [L : K]$, then $1, y, y^2, \ldots, y^{r-1}$ is a basis for L/K. Since $y \in B$, it is integral over A, so sums and products of $y_1, \ldots, y_n$ are integral over A, but coefficients of $f[T]$ are also integral implies coefficients are in A. Recall from field theory there is a trace map $\mathrm{Tr} : L \to K$ that is K-linear, where $\mathrm{Tr}(y) = \sum y_i$ is the sum over the roots of the minimal polynomial. For $b \in B$, $\mathrm{Tr}(b) \in A$; taken with respect to fixed basis... Now

Lemma 37 *$Tr\left(\frac{y^i}{f'(y)}\right) = \delta_i^{n-1}$ where δ is the indicator function and $f'(y)$ is the algebraic derivative taken wrt y.*

This is a computation. Now, we know that $\frac{1}{f'(y)}, \frac{y}{f'(y)}, \ldots, \frac{y^{r-1}}{f'(y)}$ is a basis for L/K. Then write $A \subset A[T]/f =: C \subset B$. Show B is finite type by embedding it in something finite. Write

$$B^* = \{x \in L : \mathrm{Tr}(bx) \in A \ \forall b \in B\}$$

$$C^* = \{x \in L : \mathrm{Tr}(cx) \in A \ \forall c \in C\}$$

then $B \subset B^* \subset C^* \subset L$, and all we have to do is show C^* is a finite A-module. Now we claim: C^* is a free module over A given by the dual basis:

$$C^* = A\langle \frac{1}{f'(y)} \rangle \oplus \cdots \oplus A\langle \frac{y^{r-1}}{f'(y)} \rangle \subset L.$$

Proof of claim: It is clear that $\frac{y^i}{f'(y)} \in C^*$ for all i; check that $\mathrm{Tr}\left(y^j \frac{y^i}{f'(y)}\right) \in A$. The converse is what we need. Let $x \in C^*$. Write $x = c_1 \frac{1}{f'(y)} + \cdots + c_r \frac{y^{r-1}}{f'(y)}$ with $c_i \in K$. We want to show $c_i \in A$. Well, $\mathrm{Tr}(x) \in A$ picks out a coefficient $\Rightarrow c_n \in A$. Prove all $c_i \in A$ go by induction. Suffices to show $x' = x - c_n \frac{y^{n-1}}{f'(y)} \in D$ then $\mathrm{Tr}(yx') = c_{n-1} \in A$. Then we're done: C^* is a finite A-module, and then $B \subset C^*$ is too because A is noetherian.

21 April 6

"I'm excited: this is all going to work out!"

21.1 "Today's special"

Proposition 10 *Suppose we have a finite extension $C(x) \subset L$ (actually could be $\mathbb{C}[x]$ instead, whether the curve below is $\mathbb{C}$ or $\mathbb{P}^1$...). Write $L = \mathbb{C}(x)[y]/(P(y))$ where $P(T) \in \mathbb{C}(x)[T]$ is a monic irreducible polynomial (can always do this in characteristic 0 for finite separable extensions). Then*

(i) The ring $\hat{L}$ (completion) given by $\mathbb{C}((x))[y]/(P(y))$ (not necessarily a field) is reduced (the only nilpotent element is 0).

(ii) Set B = integral closure of $A = \mathbb{C}[x]$ in L and $\hat{B}$ = integral closure of $\hat{A} = \mathbb{C}[[x]]$ in $\hat{L}$. (In the last two lectures, we studied these operations). Then $\exists$ an A-algebra map $c : B \hookrightarrow \hat{B}$ with the property that it induces isomorphisms

$$B/x^n B \to \hat{B}/x^n \hat{B}$$

for all $n \geq 1$.

Though completions are a bit annoying, so we won't deal with them precisely, the moral here is that **integral closure commutes with completions**. Now, all sorts of things will magically turn out to be true!

Proof: Since P is irreducible, $\gcd(P, P') = 1$, so P has no multiple roots, and hence $P \cdot Q_1 + P' \cdot Q_2 = 1$ for some $Q_1, Q_2 \in \mathbb{C}(x)[T]$, and also $PQ_1 + P'Q_2 = 1$ for some $Q_1, Q_2 \in \mathbb{C}((x))[T]$ take images via $\mathbb{C}(x) \hookrightarrow \mathbb{C}((x))$. Hence P factors (since $K[T]$ a UFD for any field K) into pairwise distinct irreducible monics $P = P_1 \cdots P_r$, $P_i \in \mathbb{C}((x))[T]$. The pairwise distinct part uses $\gcd(P, P') = 1$ in $\mathbb{C}((x))[T]$. Interchanging y and t (sorry):

$$\mathbb{C}((x))[y]/(P(y)) \cong \mathbb{C}((x))[y]/(P_1(y)) \times \cdots \times \mathbb{C}((x))[y]/(P_r(y))$$

by the Chinese Remainder Theorem. Each $\mathbb{C}((x))[y]/(P_i(y))$ is a field because P_i is irreducible; hence because this is a product of fields, there are no nontrivial nilpotents, hence it is reduced, proving (i). Before we do (ii), let's make a diagram to keep things clear:

$$\begin{array}{ccc} L = \mathbb{C}(x)[y]/(P) & \xrightarrow{\varphi} & \mathbb{C}((x))[y]/(P) = \hat{L} \\ \uparrow & & \uparrow \\ B & \xrightarrow{c} & \hat{B} \\ \uparrow & & \uparrow \\ A = \mathbb{C}[x] & \longrightarrow & \mathbb{C}[[x]] = \hat{A} \end{array}$$

Now $\mathbb{C}(x) \subset L$ has a basis $1, y, \ldots, y^{d-1}$ where $d = \deg_T P$, and so does $\hat{L}$ over $\mathbb{C}((x))$, even though it is not a field. φ is injective ($L \subset \hat{L}$). Now $b \in B \Leftrightarrow b \in L$ and b integral over $A \Rightarrow \varphi(b) \in \hat{L}$ and $\varphi(b)$ integral over $\hat{A}$ because the monic polynomial g with coefficients in A that exists for b under φ gets sent $\varphi(g) = \hat{g}$ an isomorphism so $\varphi(b) \in \hat{B}$ by definition. Since φ is injective, c is injective. Now look at the isomorphism desired in (ii) - fix $n \in \mathbb{N}$. Claim: $c^{-1}(x^n\hat{B}) = x^nB$. This would show that the elements of B that map to 0 in $\hat{B}$ are only $0 \in B$ which would imply $B/x^nB \to \hat{B}/x^n\hat{B}$ is injective.

Proof of claim: $x^nB \subset c^{-1}(x^n\hat{B})$ is clear. Now to show $x^nB \supset c^{-1}(x^n\hat{B})$. Suppose $b \in B$ and $c(b) \in x^n\hat{B}$ that's to say $c(b) = x^n\hat{b}$. Show that $\hat{b} \in c(B)$ then show b is divisible by x^n. Show $\exists$ polynomial with monic coefficients in A such that $\frac{b}{x^n}$ satisfies it... have to show $b/x^n \in B$. Last time, Jarod proved B is a finite A-module. But A is a PID here, and by the classification of finite modules over a PID, we can see that since there is no torsion (B a domain) and only a free part we can write $B \cong A^{\oplus r}$ as an A-module. Why exactly $r = d$? Look at the rank

$$r = \operatorname{rank}_A(B) = \operatorname{rank}_{\mathbb{C}(x)} L = d.$$

Let P_b, not the same P as before, be $P_b = T^d + a_1T^{d-1} + \cdots + a_d$ be the characteristic polynomial of b acting on $B \cong A^{\oplus d}$ (of the matrix representation). Note that $a_1, \ldots, a_d \in A$. Then also $P_b(T)$ is the characteristic polynomial of b acting on L over $\mathbb{C}(x)$. Using the same basis for L and $\hat{L}$, then we see further that P_b is the characteristic polynomial of $c(b)$ acting on $\hat{L}$, which implies $P_b \in \hat{A}[T]$ is the char ply of $x^n\hat{b}$ which means each a_i is divisible by $x^{n \cdot i}$ in $\hat{A} = \mathbb{C}[[x]]$ (think). Then each a_i is divisible by $x^{n \cdot i}$ in $A = \mathbb{C}[x]$, and then $x^{-n}b$ satisfies a monic equation with coefficients in A (namely $x^{-n \cdot i}a_i$) which means $x^{-n}b \in B$. Note that we have to be careful because irreducible polynomials in B over $\mathbb{C}(x)$ may become reducible when passing to $\mathbb{C}((x))$. We're not done yet:

Final claim: if $\hat{b} \in \hat{B}$, then $\exists b \in B$ such that $c(b) = \hat{b} \bmod x^n\hat{B}$, which would give surjectivity of $B/x^nB \to \hat{B}/x^n\hat{B}$. First note that we can certainly find $b_1, \ldots, b_d \in B$ such that

$$x^NB \subset \hat{A}b_1 + \cdots + \hat{A}b_d \subset \hat{B}$$

for some large N. Indeed, take $b_i = x^{N_i}y^i$ for some suitably large N_i. $\hat{L}$ has basis $1, y, \ldots, y^{d-1}$. We know $\hat{B}\left[\frac{1}{x}\right] = \hat{L}$, and $\hat{B}$ is a finite module over $\hat{A}$, so take any finitely many generators (because we computed it two lectures ago) - huge power of x, denominators disappear; even higher, can write as a combo of the b_i. So say $\hat{B} = \hat{A}\hat{b_1} + \cdots + \hat{A}\hat{b_f}$ where f is some number (that we don't know is d yet) with $\forall i$ write $\hat{b_i} = \sum_{j=0}^{d-1} c_{ij}y^j$ with $c_{ij} \in \mathbb{C}((x))$. Then say $c_{ij} = x^{-k_{ij}}$ a unit of $\hat{A}$. Then pick $N = \max\{N_i\} + \max\{k_{ij}\}$ and check that this works. [We showed last time that $L \supset \mathbb{C}((x))$ is finite and reduced implies its $\mathbb{C}[[x]] \subset \mathbb{C}[[y_1]] \times \cdots \times \mathbb{C}[[y_r]]$ where $x \mapsto (y_1^{e_1}, \ldots, y_r^{e_r})$ the structure theorem for $\hat{B}$.] We're almost done proving the final claim: write $x^N\hat{b} = \sum \hat{a}_i b_i$ with $\hat{a}_i \in \mathbb{C}[[x]]$. Pick $a_i \in \mathbb{C}[x]$ very close to the power series $\hat{a}_i$, i.e. such that $a_i - \hat{a}_i \in x^{N+n}\hat{A}$. Then you get $x^N\hat{b} - \sum a_i b_i = x^{N+n}\hat{r}$ for some $\hat{r} \in \hat{B}$, namely $\hat{r} = \sum \frac{(\hat{a_i}-a_i)}{x^N} b_i$. This implies by the previous claim that $b = x^{-N}\left(\sum a_i b_i\right) \in B$ and also $\hat{b} - b \in x^n\hat{B}$ as desired. $\square$.

21.2 Applications

What can we do with this??? Here's one nice application:

Proposition 11 *If $\mathbb{C}[x] \subset B$ is the integral closure of $\mathbb{C}[x]$ in a finite extension $\mathbb{C}(x) \subset L$, then every maximal ideal $\mathfrak{m}$ of B can be generated by two elements.*

Compare to maximal ideals in $\mathbb{C}[x]$ generated by one element. *Proof*: by the HNull, $B/\mathfrak{m} = \mathbb{C}$. Then this means $\mathbb{C}[x] \cap \mathfrak{m}$ is also a maximal ideal in $\mathbb{C}[x]$ ($\mathfrak{m}$ corresponds to a closed point on the curve). Then $\mathbb{C}[x] \cap \mathfrak{m} = (x - \alpha)$ for some $\alpha \in \mathbb{C}$ by the HN again. Change coordinates os that $\alpha = 0$ (THINK: apply an automorphism of $\mathbb{C}[x]$ by $x \mapsto x - \alpha$), and now $x \in \mathfrak{m}$. Then we know by today's special that

$$B/xB \cong \hat{B}/x\hat{B} \cong \mathbb{C}[y_1]/(y_1^{e_1}) \times \cdots \times \mathbb{C}[y_r]/(y_r^{e_r})$$

where the second equality came from two lectures ago. Note that truncating by a power of y_i is the same as if we did it in $\mathbb{C}[[y_i]]$ or $\mathbb{C}[y_i]$. Then also $\mathfrak{m}/xB \subset B/xB$ is maximal in here by the Third Isomorphism Thm, and so it corresponds to some maximal ideal over in the product of fields. So what are maximal ideals in this product of fields? Well, can have at most one idempotent $E_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ surviving, and has to put y_i in there, so each maximal ideal of RHS is of the form $\Big((1, \ldots, 1, y_i, 1 \ldots, 1)\Big)$ for some $1 \leq i \leq r$: quotient by this ideal gives $\mathbb{C}$ (call this element $\overline{b}$, then $\mathfrak{m}$ is generated by x and b where $b \mapsto \overline{b}$ in the quotient. $\square$

Next time we will show $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 1$ if and only if we have a "nonsingularity",and will link back to valuations. Again this is local (think saying $\epsilon^2 = 0$ to deal algebraically with infinitesimals...)

22 April 8

Review: what we have seen is a contravariant equivalence of categories of (G) affine algebraic curves and (A) $\mathbb{C}$-algebras B that are finitely generated domains of transcendence degree $\text{trdeg}_{\mathbb{C}}(ff(B)) = 1$ where $ff(B)$ is the fraction field. As a basic example of this, consider the category of (A) finite dimensional vector spaces over $\mathbb{C}$ in equivalence with (G) $\{\mathbb{C}^n \ : \ n \geq 0\}$ with morphisms given by linear maps: *this* is how we know every vector space has a basis. What follows are explicit illustrations of this correspondence in the various topics we have covered / will cover.

22.1 Ring of Regular Functions

Given $C \subset \mathbb{C}^n$ a Zariski closed subset, our functor $F : G \to A$ sends $C \mapsto \mathcal{O}(C) = \Gamma(C)$ the ring of regular functions on C (which are the coordinate ring of polynomials since C is closed in the ambient space). This functor sends a morphism

$$(\varphi : C_1 \to C_2) \mapsto (\varphi^* : \mathcal{O}(C_2) \to \mathcal{O}(C_1))$$

by the pullback which is contravariant. To show that it is an equivalence of categories, we have to show that each object / morphism is hit by a unique one from the LHS. To go back: if $B = \mathbb{C}[x_1, \ldots, x_n]/I$ take $C = V(I) \subset \mathbb{C}^n$ and if $\chi : B_2 \to B_1$ take the map $\varphi : C_1 \to C_2$ with $\varphi(a) = (h_1(a), \ldots, h_n(a))$ where $\chi(x_i) = h_i \bmod I(C_1)$... etc...

22.2 Noether normalization for curves

A curve C has a finite morphism $C \to \mathbb{C}$ if and only if, via our functor, any B as above has a copy of $A = \mathbb{C}[x] \to B$ an *embedding* such that B is finite over A. Note that this embedding is far from unique.

22.3 Jarod's Lecture

(A): Given $A \subset B$ as in Noether normalization, the integral closure B' of B (or equivalently A) in $L = ff(B)$ is finite over B (or equivalently A). On the curves side this menas we get

$$C' \to C \to \mathbb{C} \qquad (*)$$

where $C \to \mathbb{C}$ is finite and $C' \to C$ is birational (same function field) and C' is a *normal* affine algebraic curve.

Definition 34 *An affine algebraic curve is <u>normal</u> iff $B = \mathcal{O}(C)$ is a normal domain, i.e. integrally closed in its fraction field $\mathbb{C}(C)$.*

Our goal is to show that C' is nonsingular; note that if C is already normal, then C' is C (this is our resolution of singularities C^ν).

22.4 Last Lecture

In (*), if C is normal, so $C = C'$ and $B = B'$, then $\forall n \geq 1$ $\exists$ an isomorphism $B/x^nB \to \hat{B}/x^n\hat{B}$ of $\mathbb{C}[x]$-algebras where $\hat{A} = \mathbb{C}[[x]] \subset \hat{B} \cong \mathbb{C}[[y_1]] \times \cdots \times \mathbb{C}[[y_r]]$ by $x \mapsto (y_1^{e_1}, \ldots, y_r^{e_r})$ and we also know $\hat{B}$ the integral closure of $\hat{A}$ in $\hat{L} = \mathbb{C}((x))[y]/(P(y))$ if $ff(B) = \mathbb{C}(C) = \mathbb{C}(x)[y]/(P(y))$.

Remark 1: Note that this also means $d = e_1 + \cdots + e_r$ where $d = \deg[\mathbb{C}(C) : \mathbb{C}(x)] = \deg\big(C \to \mathbb{C}\big)$. The rank of $\hat{B}$ as an $\hat{A}$-module is $e_1 + \cdots + e_r$ and on the other hand $\deg[\hat{L} : \mathbb{C}((x))] = \deg[P] = \deg[\mathbb{C}(C) : \mathbb{C}(x)]$.

Remark 2: The e_is will be called the **ramification indices** of the points of C lying above $0 \in \mathbb{C}$.

Remark 3: In the last proof, used x as a coordinate, but could've also done $x - \alpha$, hence this result holds $\forall$ points $\alpha \in \mathbb{C}$ (get e_i pieces ... etc). NB: the geometric picture of this we will see has to do with what sits above a disc $D \subset \mathbb{C}$: might have 3 disjoint holomorphic disks above... or say if $e_1 = 2, e_2 = e_3 = 1$, then we get three "disks" above, two y_2, y_3 of them map down to D by $z \mapsto z$ while the other maps down as $z \mapsto z^2$. The action on points is DUAL - careful! The power series are formal solutions -¿ don't worry outside a point, but proving normal curves are nonsingular, we then know from our earlier work that we do get disks locally (!!!).

22.5 Applications

Review: saw of this application 1 was $\forall$ NORMAL affine curves C and any maximal ideal $\mathfrak{m}$, $\mathfrak{m}$ can be generated by 2 elements. Now Application 2: with the assumptions as in App 1, then $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 1$. *Proof*: pick $A \subset B$ as before. After changing coordinates, see Remark 3, may assume that $\mathfrak{m} \cap A = (x) \subset A = \mathbb{C}[x]$. Then

$$B/x^2B \cong \hat{B}/x^2\hat{B} \cong \mathbb{C}[y_1]/(y_1^{2e_1}) \times \cdots \times \mathbb{C}[y_r]/(y_r^{2e_r})$$

by $x \mapsto (y_1^{e_1}, \ldots, y_r^{e_r})$. Then the ideal $\mathfrak{m}/x^2B \cong$ the ideal generated by $(1, \ldots, 1, y_i, 1, \ldots, 1) = \xi$. Think: then $\mathfrak{m}/\mathfrak{m}^2 \cong (\xi)/(\xi)^2 \cong (y_i)/(y_i^2)$ in $\mathbb{C}[y_i]/(y_i^{2e_i})$ and this has dimension 1 over $\mathbb{C}$.$\square$

Application 3: A normal affine algebraic curve is nonsingular.

Proof: It is enough to show the following proposition (Jacobian criterion): for $C \subset \mathbb{C}^n$ an affine curve, $p \in C$ corresponding to $\mathfrak{m} \subset B = \mathcal{O}(C)$, then p is a nonsingular point on C if and only if $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 1$. Warning: this algebraic RHS is considered the definition of nonsingular or smoothness in most algebraic geometry courses, not the rank condition on partials on the LHS. But we just saw this in app 2, so we'd be done! To prove this proposition, say $I(C) = (f_1, \ldots, f_t)$, then $\mathcal{O}(C) = \mathbb{C}[x_1, \ldots, x_n]/(f_1, \ldots, f_t)$. Now do an affine linear change of coordinates such that $p = (0, \ldots, 0)$. And this change of coordinates, we must note, doesn't

change rank. Then $f_i \in (x_1, \ldots, x_n)$ and $\mathfrak{m} = (x_1, \ldots, x_n)/(f_1, \ldots, f_n)$ hence we get $(x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2 \to \mathfrak{m}/\mathfrak{m}^2 = (x_1, \ldots, x_n)/(x_\alpha \cdot x_\beta, f_i)$ and also

$$(x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2 = \bigoplus_{i=1}^{n} \mathbb{C}\,\overline{x_i}$$

and so we can ask what is the kernel? Well $\sum_{i=1}^n \lambda_i \overline{x_i} \mapsto 0$, then $\sum \lambda_i x_i$, the linear terms of some $f \in I(C) = (f_1, \ldots, f_t)$ if and only if $\begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} \in I_{\mathfrak{m}}$ the matrix whose columns are $\frac{\partial f}{\partial x_j}(0)$ for $j = 1, \ldots, t$ so now want to show

$$\dim(\mathfrak{m}/\mathfrak{m}^2) = n - \operatorname{rank}\big[\frac{\partial f_i}{\partial x_j}(0)\big]$$

the COTANGENT SPACE (?). Now to prove that the rank of $\big[\frac{\partial f_i}{\partial x_j}(0)\big] \leq n - 1$ is true since $\mathfrak{m}/\mathfrak{m}^2 = 0 \Rightarrow \mathfrak{m} = \mathfrak{m}^2 \Rightarrow$ by NAKAYAMA there is some $f \in \mathfrak{m}$ such that $(1 + f)\mathfrak{m} = \mathfrak{m}$ which $\Rightarrow B$ has zerodivisors unless $\mathfrak{m} = 0$ but this is a contradiction since dim $= 1$ so $\mathfrak{m} \neq 0$. Generalization: rank $\leq n - d$ where d is the degree takes work... we won't do this because this is curves.

22.6 Unrelated ramble on Local Rings

Local rings, those which have exactly one maximal ideal. Now $S \subset A$, A a ring and S a multiplicative subset (closed under mult, contains identity) then picking denominators in S only, get

$$S^{-1}A = \{\frac{a}{s} : a \in A, s \in S\}/\sim$$

with equivalence $a/s = a'/s'$ if there is some $s'' \in S$ where $s'(as' - sa') = 0$ since this all isn't necessarily a domain. Then at a prime ideal $\mathfrak{p}$, we have

$$A\mathfrak{p} = (A - \mathfrak{p})^{-1} \cdot A$$

is always a local ring. Fulton: $p \in C$; then a local ring of C at p is $\mathcal{O}_p$ the germs of regular functions around p. This is

$$\mathcal{O}_p = \varinjlim \mathcal{O}(U)$$

where the direct limit is taken over all $p \in U \subset C$ open. The equivalence

$$\{(U, f) : p \in U \subset C \text{ open }, f \in \mathcal{O}(U)\}/\sim$$

where $(U, f) \sim (U', f') \Leftrightarrow \exists U'' \subset U \cap U'$ such that $f\big|_{U''} = f'\big|_{U''}$. Then if $p \in C$ with corresponding $\mathfrak{m} \subset B$ as before then

$$B_{\mathfrak{m}} \cong \mathcal{O}_p$$

which is to say that the local rings agree.

23 April 13

So, we saw that the normalization of an algebraic curve gives a nonsingular cirve, and the map is finite and birational. To prove that nonsingular $\Rightarrow$ normal will take work.

23.1 Valuations and Curves

We're avoiding local rings here. Also note that it turns out that any algebraic curve (more general definition) is a quasi-projective curve.

Definition 35 *Let C be a quasi-projective algebraic curve, and let $\nu : \mathbb{C}(C)^* \to \mathbb{Z}$ be a discrete valuation on $\mathbb{C}(C)/\mathbb{C}$. We say that ν is centered at $p \in C$ if $\exists$ an affine open neighborhood $p \in U \subset C$ such that*

(a) $\forall f \in \mathcal{O}(U)$, $f \neq 0$, we have $\nu(f) \geq 0$.

(b) $\forall f \in \mathcal{O}(U)$, $f \neq 0$ with $f(p) = 0$, then $\nu(f) > 0$.

For example, $C = \mathbb{C} = \mathbb{A}^1_{\mathbb{C}}$, then $\mathbb{C}(C) = \mathbb{C}(x)$, and ν_α is centered at α if $\alpha \in C = \mathbb{C}$ and ν_∞ is not centered at any point of $C = \mathbb{C}$. As a second example, $C = \mathbb{P}^1$, we have $\mathbb{C}(C) = \mathbb{C}(x)$ and ν_α is centered at α $\forall \alpha \in \mathbb{P}^1$.

Theorem 9 *Every discrete valuation of $\mathbb{C}(C)/\mathbb{C}$ is centered at at most one point of C. If C is projective, then every discrete valuation is centered at some point of C.*

Warning: it can happen that two different valuations are centered at the same point of C. For example, C the nodal cubic defined by $xy - (x^3 + y^3) = 0$, in this case $\mathcal{O}(C) = \mathbb{C}[x, y]/(xy - x^3 - y^3) \subset \mathbb{C}(t) = \mathbb{C}(C)$ by the map $x \mapsto \frac{t}{1+t^3}$, $y \mapsto \frac{t^2}{1+t^3}$ i.e. $y/x \mapsto t$. Here, ν_0 and ν_∞ on $\mathbb{C}(t)$ are both centered at $p = (0, 0)$ the nodal point. Will see that on a nonsingular curve we have a bijection between points and valuations. Also note that this doesn't happen when you look at the cuspidal cubic $y^2 - x^3 = 0$ because the normalization is a bijective map: look at see how many points are above the singular point.[18] Towards the proof of the theorem:

Lemma 38 *(0) If C is an affine curve and $\nu(f) \geq 0$ $\forall f \in \mathcal{O}(C) \subset \mathbb{C}(C)$, $f \neq 0$, then $\mathfrak{m} = \{f \in \mathcal{O}(C) : \nu(f) > 0\}$ is a maximal ideal of $\mathcal{O}(C)$ and corresponds to the unique point of C at which ν is centered.*

Check that this is an ideal (elementary: for example $x \in \mathfrak{m}$, $y \in \mathcal{O}(C)$, $\nu(xy) = \nu(x) + \nu(y) > 0$ because $\nu(x) > 0$ and $\nu(y) \geq 0$.) Actually, check that it is prime, and note that $\nu(1) = 0$ so $1 \notin \mathfrak{m}$. This prime ideal $\mathfrak{m}$ corresponds to a closed subvariety of an affine curve, so it's a point since the dimension must go down, hence it is maximal. This implies $\exists p \in \mathbb{C}$ such that $\mathfrak{m} = \{f \in \mathcal{O}(C) : f(p) = 0\}$ which implies ν is centered at p. If ν was also centered at $q \neq p$, then choose $f \in \mathcal{O}(C)$ with $f(p) \neq 0$, $f(q) = 0$, and you get $\nu(f) = 0$ a contradiction (actually have to look at $f\big|_U$ to get this contradiction...) $\square$

[18] Aside/review: note that $\mathcal{O}(\mathbb{P}^1) = \mathbb{C}$ but $\mathbb{C}(\mathbb{P}^1) = \mathbb{C}(x)$ because we have to look on affine opens.

Lemma 39 *(1) let C, ν, p, and $U \subset C$ be as in the definition above of "being centered at." If $V \subset U$ is an open affine and $p \in V$ then (a) $\nu(h) \geq 0$ $\forall h \in \mathcal{O}(V)$ and (b) $\nu(h) > 0$ $\forall h \in \mathcal{O}(V)$ with $h(p) = 0$.*

By an exercise, we can find an $f \in \mathcal{O}(U)$, $f(p) \neq 0$, with $U_f = \{q \in U : f(q) \neq 0\} = U \setminus V(f)$ we have $U_f \subset V \subset U$ and also the rings of functions

$$\mathbb{C}(C) \supset \mathcal{O}(U_f) \supset \mathcal{O}(V) \supset \mathcal{O}(U)$$

which is how we see that U and V have equal fraction fields. By lemma 0, we have $\nu(f) = 0$, hence $\nu\left(\frac{g}{f^n}\right) = \nu(g) \geq 0$ if $g \in \mathcal{O}(U)$ hence by (a) of Lemma 1 if $g(p) = 0$, $\nu(g/f^n) = \nu(g) > 0$ which proves part (b). $\square$

Lemma 40 *(2 - Geometric) For all quasi projective curves C and pairs of points $p, q \in C$, $\exists$ an affine open $U \subset C$ with $p, q \in U$.*

Remark: can also prove this with $p, q, r, s, \ldots, z \in C$ finitely man. For arbitrary abstract C this is harder to prove. *Proof of 2*: by definition, $C \subset \mathbb{P}^n$ is Zariski locally closed. Pick a linear form $\sum a_i X_i$ such that $p, q \notin V_+(\sum a_i X_i)$. Do a linear change of coordinates such that afterwards the new X_0 is the old $\sum a_i X_i$. Then we get $p, q \in U_0$ because both $p, q \notin V_+(X_0)$ are not in the hyperplane at ∞. Take $C' = C \cap U_0 \subset \mathbb{C}^n$ is now a quasi-affine curve with $p, q \in C'$. This reduces the lemma to the case where C is affine. In this case, write $\overline{C} = C \cup \{c_1, \ldots, c_N\}$ the Zariski closure of C in $\mathbb{C}^n$. Pick $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that $f(c_i) = 0 \forall i = 1, \ldots, N$ and $f(p) \neq 0$, $f(q) \neq 0$. Consider $U = C \setminus (C \cap V(f)) \subset \mathbb{C}^n \setminus V(f)$. By construction, $p, q \in U$, and $U \subset \mathbb{C}^n \setminus V(f)$ is closed and $\mathbb{C}^n \setminus V(f)$ is affine so U is closed in an affine which implies U is affine. Same trick works for more than two points...

Proof of Uniqueness part of Theorem: if centered at some point, can't be centered at another point. Say ν is a discrete valuation on $\mathbb{C}(C)/\mathbb{C}$. Say ν is centered at $p, q \in C$. By Lemma 2 can find an affine open $U \subset C$ with $p, q \in U$. Then there are $V, W \subset C$ such that $p \in V, q \in W$ and moreover V works for p in definition of centered at p and W works for q. By Lemma 1, may replace V, respectively W, by smaller affine open neighborhoods, then assume by uniqueness that $V, W \subset U$. And now we see V, W also work relative to U. So by Lemma 0 applied to U or V (?) we can conclude $p = q$.

Existence take $C \subset \mathbb{P}^n$ closed. If $C \subset V_+(X_i)$, then since $V_+(X_i) \cong \mathbb{P}^{n-1}$ we may lower n. Hence assume $C \not\subset V_+(X_i) \forall i$, then $\frac{X_1}{X_0}\big|_{C \cap U_0}$, $\ldots$, $\frac{X_n}{X_0}\big|_{C \cap U_0}$ are nonzero rational functions in $\mathbb{C}(C)^*$. If $\nu\left(\frac{X_i}{X_0}\big|_{C \cap U_0}\right) \geq 0$ $\forall i$ then $\nu(f) \geq 0$ $\forall f \in \mathcal{O}(C \cap U_0)$. Reason: any element of $\mathcal{O}(C \cap U_0)$ is a polynomial with complex coefficients in $\frac{X_i}{X_0}\big|_{C \cap U_0}$ (they're the coordinate functions on $U_0 \cong \mathbb{C}^n$). Then by Lemma 0, we see ν is centered at some point of $C \cap U_0$. What happens if one $\nu\left(\frac{X_i}{X_0}\big|_{C \cap U_0}\right) < 0$ for some i?

Pick i such that this is minimal (most negative). Then look at

$$\frac{X_0}{X_i}\Big|_{C\cap U_i}, \ldots, \widehat{\frac{X_i}{X_i}\Big|_{C\cap U_i}}, \ldots, \frac{X_n}{X_i}\Big|_{C\cap U_i}$$

similarly as above, but now

$$\nu\Big(\frac{X_j}{X_i}\Big|_{C\cap U_i}\Big) = \nu\Big(\frac{X_j}{X_0}\big(\frac{X_i}{X_0}\big)^{-1}\Big|_{C\cap U_i\cap U_0}\Big) = \nu\big(\frac{X_j}{X_0}\big|_{C\cap U_0}\big) - \nu\big(\frac{X_i}{X_0}\big|_{C\cap U_0}\big) \geq 0$$

by choice of i. Why projective space is "compact" in a strong sense: every valuation has a center. This says you can take limits in some algebraic way...

24 April 15

24.1 Valuations and nonsingular curves: first a proposition

To prove:

Proposition 12 *Let $\mathbb{C} \subset R$ be a ring and $\mathfrak{m} \subset R$ an ideal. Assume (a) R is a Noetherian domain and (b) $R/\mathfrak{m} = \mathbb{C}$, in particular $\mathfrak{m}$ maximal and (c) $\dim_{\mathbb{C}}(\mathfrak{m}/\mathfrak{m}^2) = 1$ (cotangent space ... over residue field ...) . Then $\exists!$ (exactly one) discrete valuation ν on $K = ff(R)/\mathbb{C}$ such that*
(1) $\nu(f) \geq 0\ \forall f \in R \setminus \{0\}$ and
(2) $\nu(f) > 0\ \forall f \in \mathfrak{m}\setminus\{0\}$ which is to say "being centered at $\mathfrak{m}$".

We will prove this in steps, called Lemmas, with the notation in the proposition fixed.

Lemma 41 *(0) (another version of Nakayama's Lemma): If $I \subset R$ is an ideal and $\mathfrak{m}\, I = I$ then $I = 0$.*

Proof: As R is Noetherian, we see I is a finitely generated R-module, then by previous lemma (Nakayama), we can see $\mathfrak{m}\, I = I \Rightarrow \exists f \in \mathfrak{m}$ such that $(1+f)I = 0$; since $1 + f \neq 0$ and R a domain, we must have $I = 0$. $\square$ Pick $x \in \mathfrak{m}$ which generates $\mathfrak{m}\,/\,\mathfrak{m}^2$. Claim: x^n generates $\mathfrak{m}^n\,/\,\mathfrak{m}^{n+1}\ \forall n \geq 1$ (always the same x in what follows). *Proof of claim:* it suffices to show that if $f_1, \ldots, f_n \in \mathfrak{m}$, then $f_1 \cdots f_n \in Rx^n + \mathfrak{m}^{n+1}$. Write $f_i = a_i x + g_i$ with $g_i \in \mathfrak{m}^2$ and $a_i \in R$ (possible by our choice of x). Then $f_1 \cdots f_n = a_1 \cdots a_n x^n +$ terms of higher powers than n... $\square$

Claim: $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}\ \forall n \geq 0$. Well, $\mathfrak{m}$ is not the 0 ideal because $\dim(\mathfrak{m}\,/\,\mathfrak{m}^2) = 1$, but by Lemma 0, $\mathfrak{m}\cdot\mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m}^n \Rightarrow \mathfrak{m} = 0$ a contradiction.

Claim: $I = \bigcap_{n\geq 0} \mathfrak{m}^n = 0$. Well, will show $\mathfrak{m}\, I = I$ and then use Lemma 0, but the inclusion $\supset$ is hard, uses Artin-Rees, so a proof is outlined in the exercises (two versions). Now

Definition 36 *For $a \in R$, $a \neq 0$, $\nu_{\mathfrak{m}}(a) := \max\{n \mid a \in \mathfrak{m}^n\}$.*

Uses claim. Note $\nu_{\mathfrak{m}}(a) = n \Leftrightarrow a = cx^n + r$ with $c \in \mathbb{C}^*$ and $r \in \mathfrak{m}^{n+1}$. For $z \in K = ff(R)$, $z \neq 0$, set $\nu_{\mathfrak{m}}(z) = \nu_{\mathfrak{m}}(a) - \nu_{\mathfrak{m}}(b)$ whenever $z = \frac{a}{b}$ and $a, b \in R$ (compare to the p-adic valuation). Here x plays the role of the coordinate - "uniformizer"...

Claim: (1) $\nu_{\mathfrak{m}}$ is a discrete valuation. (2) if ν is a valuation on $K/\mathbb{C}$ such that $\nu(f) \geq 0\ \forall f \in R$, $\nu(f) > 0\ \forall f \in \mathfrak{m}\setminus\{0\}$, then $\nu = \nu_{\mathfrak{m}}$.

Proof of 1: if $a = cx^{n_1} + r_1$, $b = c_2x^{n_2} + r_2$ where $c_1, c_2 \in \mathbb{C}^*$, $r_1, r_2 \in \mathfrak{m}^{n+1}$, same x as before. So $\nu_{\mathfrak{m}}(a) = n_1$, $\nu_m(b) = n_2$, and

$$ab = c_1c_2x^{n_1+n_2} + c_1r_2x^{n_1} + c_2r_1x^{n_2} + r_1r_2$$

where the last three terms are in $\mathfrak{m}^{n_1+n_2+1}$. Then $\nu_{\mathfrak{m}}(ab) = n_1 + n_2 = \nu_{\mathfrak{m}}(a) + \nu_{\mathfrak{m}}(b)$. and also $a + b = c_1x^n + r_1 + c_2x^{n_2} + r_2 \in \mathfrak{m}^{\min(n_1,n_2)}$ which means $\nu_{\mathfrak{m}}(a + b) \geq \min(n_1, n_2) = \min(\nu_m(a), \nu_m(b))$. Surjectivity is clear because the valuation of x is 1. This proves 1.

Proof of 2: With arbitrary discrete valuations such that $\nu(f) \geq 0\ \forall f \in R\setminus\{0\}$ and $\nu(f) > 0$ for $f \in \mathfrak{m}\setminus\{0\}$. Then $t = \nu(x)$ for some t, and $s = \min\{\nu(g) : g \in \mathfrak{m}, g \neq 0\}$. By assumption $t, s > 0$, $t \geq s$. If $g \in \mathfrak{m}$, then $g = ax + \sum v_iw_i$ for $a \in R$, $v_i, w_i \in \mathfrak{m}$ because x generates $\bmod \mathfrak{m}^2$. If $s = \nu(y)$, $y \in \mathfrak{m}$ is an element where the minimum is attained, then $s = \nu(y) \geq \min\{\nu(ax), \nu\big(\sum v_iw_i\big)\} \geq \min\{t, \nu(v_i, w_i)\ \forall i|_1^n\}$ which is $\geq \min\{t, 2s\}$ which implies $s = t$. Now pick any $f \in R \neq 0$. Then we can write $f = cx^n + r$ for $c \in \mathbb{C}^*$, $r \in \mathfrak{m}^{n+1}$ so $\nu_{\mathfrak{m}}(f) = n$. Compute $\nu(f) \geq \min\{\nu(cx^n), \nu(r)\} = \min\{nt, \nu(r)\}$ but becase $r \in \mathfrak{m}^{n+1}$ and $s = t$ we get $\nu(r) \geq (n + 1)t$. General fact on discrete valuations: if $\nu(a) \neq \nu(b)$, then $\nu(a + b) = \min(\nu(a), \nu(b))$. We conclude that $\nu(f) = nt = n \cdot \nu_m(f)$ and by surjectivity we must have $n = 1$. $\square$ All of this comes from the fact that $\mathfrak{m}$ is virtually generated by 1 element.

24.2 Applications

Application 1Recall what we know about affine curves: normal $\Rightarrow$ nonsingular, and nonsingular curves are characterized by the property $\dim \mathfrak{m}\,/\,\mathfrak{m}^2 = 1$. If C is a nonsingular affine curve, then there are canonical bijections between

(i) discrete valutations on $\mathbb{C}(C)/\mathbb{C}$ such that $\nu(f) \geq 0\ \forall f \in \emptyset(C)$
(ii) discrete valuations on $\mathbb{C}(C)/\mathbb{C}$ which have a center on C
(iii) maximal ideals $\mathfrak{m} \subset \mathcal{O}(C)$
(iv) points of C.

We go about these by: (i) and (ii) from last lecture; (i) and (iii) from $\nu \mapsto \mathfrak{m} = \{f : \nu(f) > 0\}$ and also by Lemma 0 of last time (1 to 1 by today); (iii) to (iv) by

Hilbert's N and (ii) to (iv) by $\nu \mapsto$point of C where it is centered. Proof is by combining everything: note that the proposition with dimension $\dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 1$ does not apply to the cuspidal case; later, look at singularity with 1 point above in resolution. Application 2 If C is a nonsingular quasi-projective curve then discrete valuations on $\overline{\mathbb{C}(C)/\mathbb{C}}$ which have a center on C are in bijection with points on C (send a valuation to its center). Proof: well defined by last time, injective by uniqueness in proposition today, and why surjective? Point: it's in an affine, and with application 1 to $R = \mathcal{O}(U)$ and $\mathfrak{m} = \{f \in \mathcal{O}(U) : f(p) = 0\}$ we can say $\nu_{\mathfrak{m}}$ is a valuation on $\mathbb{C}(C)$ with center at p. For example, $\mathbb{C} = C$, don't get ν_∞. Application 3 C is a nonsingular projective curve, then discrete valuations on $\mathbb{C}(C)/\mathbb{C}$ are in bijection with points on C. By app II and any valuation has a center on a projective curve (last time). This is what says projective space is proper – completely wrong in higher dimensions!

25 April 20

Another lecture on valuations and singular curves. It's becoming inconvenient not to have this definition...

Definition 37 *Let X be a quasi-projective variety and $p \in X$ a point. The local ring of X at p is $\mathcal{O}_{X,p} = \mathcal{O}_p = \{f \in \mathbb{C}(X) : \exists p \in U \subset X$ affine open s.t. $f \in \mathcal{O}(U)\}$.*

Since $\mathrm{Frac}(\mathcal{O}(U)) = \mathbb{C}(X)$, on this open U take $\frac{f}{1}$. Silly remark: can make U as "small" as you like (hence local). Might as well assume affine (basis for topology).

Lemma 42 *$\mathcal{O}_p$ is a Noetherian local ring.*

Proof: if $f \in \mathcal{O}_p$, then I can evaluate f at p since f is a regular function on some nbd of p. I claim that $\mathcal{O}_p$ is a local ring with maximal ideal $\mathfrak{m}_p = \{f \in \mathcal{O}_p : f(p) = 0\}$. Algebraic fact: if R is a ring, $I \subset R$ an ideal, and if for any$f \in R$, $f \notin I \Rightarrow f$ invertible, then we must have R a local ring with maximal ideal I. By this algebraic fact, it suffices to check that $f \in \mathcal{O}_p$, $f \notin \mathfrak{m}$ yields f invertible. This is true because say $f \in \mathcal{O}(U)$. Then $U' = \{q \in U : f(q) \neq 0\} \subset U$ is open and affine and by assumption $p \in U'$, ($U' = U \setminus V(f)$ a localization), and $f^{-1} \in \mathcal{O}(U')$, hence $f^{-1} \in \mathcal{O}_p$ which is f invertible. Now to show $\mathcal{O}_p$ is Noetherian (sketch): pick any affine open $U \subset X$ with $p \in U$. Let $\mathfrak{m} = \{f \in \mathcal{O}(U) : f(p) = 0\} \subset \mathcal{O}(U)$ then check

$$\underset{p}{\mathcal{O}} = \{\frac{f}{g} : f, g, \in \mathcal{O}(U), g \notin \mathfrak{m}\},$$

hence by general algebraic fact which states that for given $(R, \mathfrak{p})$ with R Noetherian and $\mathfrak{p}$ a prime ideal, then $R_{\mathfrak{p}} = \{\frac{f}{g} : f, g \in R, g \notin \mathfrak{p}\}$ is Noetherian. $\square$

Example: $X = \mathbb{C}$, $p = 0 \in X = \mathbb{C}$, then $\mathcal{O}_p = \{\frac{f}{g} : f, g \in \mathbb{C}[x], g(p) \neq 0\}$. We tried to avoid these because they're not finitely generated; this contains $\frac{1}{x-\lambda}$ $\forall \lambda \neq 0$, so it's not finitely generated at all over $\mathbb{C}$ as an algebra - it sucks from a computational point of view, but is useful later on: $\mathbb{C}[[x]]$ is better ... it's also local ... easier: closed formula for this thing! Anyway, we're trying to get to the point where nonsingular $\Leftrightarrow$ normal...

Proposition 13 *If C is a nonsingular curve, pin$C$ and ν is a valuation on $\mathbb{C}(C)$ centered at p (one such one), then*

$$\underset{p}{\mathcal{O}} = \{f \in \mathbb{C}(C) : \nu(f) \geq 0\}$$

with maximal ideal

$$\mathfrak{m}_p = \{f \in \mathbb{C}(C) : \nu(f) > 0\}.$$

Before the proof of the proposition[19], let's first do a "might've made things less confusing if I said this earlier" Lemma:

Lemma 43 *If $p \in C$, C nonsingular curve, then $\exists$ arbitrarily small affine neighborhoods $p \in U \subset C$ of p such that the ideal $\mathfrak{m} = \{f \in \mathcal{O}(U) : f(p) = 0\} \subset \mathcal{O}(U)$ is generated by 1 element.*

Proof: By previous result, $\dim_{\mathbb{C}}(\mathfrak{m} / \mathfrak{m}^2) = 1$. Pick $x \in \mathfrak{m}$ which generates $\mathfrak{m} / \mathfrak{m}^2$. Then

$$\mathfrak{m} \cdot \Big(\mathfrak{m} /(x) \Big) = \mathfrak{m} /(x)$$

as $\mathcal{O}(U)$-modules because $(x) + \mathfrak{m}^2 = \mathfrak{m}$ by choice of x. Then by Nakayama's Lemma $\exists f \in \mathfrak{m}$ such that (*) $(1 + f)\,\mathfrak{m} /(x) = 0$ so $\forall g \in \mathfrak{m}$, $(1 + f)g$ is divisible by x in $\mathcal{O}(U)$. This means that if we set $p \in U' = \{q \in U : (1 + f)q \neq 0\}$ affine open set in U and $\mathfrak{m}' = \{g \in \mathcal{O}(U') : g(p) = 0\}$, then actually $\mathcal{O}(U') = \mathcal{O}(U)_{1+f}$ a principle localization, and $\mathfrak{m}' = \mathfrak{m}_{1+f} = \{\frac{g}{(1+f)^n} : g \in \mathfrak{m}\}$ and now from (*) you conclude that $\mathfrak{m}' = (x)$ inside $\mathcal{O}(U')$. NB: before $mI = I$ in a domain could use Nakayama's Lemma that way; here, we're in $\mathfrak{m} /(x)$ - this happens in $\mathcal{O}(U)/(x)$ which is not in general a domain. For Nakayama's Lemma we have two cases: either apply it in a domain or when we're in a local ring.

Example: $\mathbb{C}[x, y]/(y^2 - x(x - 1)(x - 2))$. Here $\mathfrak{m} = (x, y)$ a point; can't be generated by 1 element globally, but $\mathfrak{m} / \mathfrak{m}^2$ is generated by y (smallest order of vanishing). Ish, look at real picture, see that tangent space at $x = 0$, y has non-zero derivative on this curve. To prove $\mathfrak{m}$ can't be generated by one element, have to do more work. But what would be an open subset where it **is** generated by one element? Second attempt: maybe y generates it? $y = 0$ on $(1, 0)$ and $(2, 0)$ also: note that in $\mathcal{O}(U')$ which is

$$\Big[\mathbb{C}[x, y]/(y^2 - x(x - 1)(x - 2)) \Big]_{(x-1)(x-2)}$$

allowing inverting $x - 1$ and $x - 2$, we see then that $\mathfrak{m} = (y)$ exactly what happens in proof. Not that easy to see but it's true. The way to find an open where you can do this is to pick a generator of $\mathfrak{m} / \mathfrak{m}^2$ then look where the element is 0, and invert some elements.

[19] Aside: example $X = \mathbb{C}, p = 0$, any $f \in \mathbb{C}(x)$ is $f = c \prod_{i=1}^{n} (x - \lambda_i)^{e_i}$ for $c \in \mathbb{C}$, $\lambda_i \in \mathbb{C}$ pairwise distinct, and $e_i \in \mathbb{Z}$. Then $\nu_0(f)$ is the order of vanishing at 0 is 0 if $\lambda_i \neq 0$ $\forall i$ or it is e_i if some $\lambda_i = 0$. And here $f \in \mathcal{O}_0 \Leftrightarrow \nu(f) \geq 0$.

Now we can prove the proposition. Want to show $\mathcal{O}_p = \{f \in \mathbb{C}(C) : \nu(f) \geq 0\}$ where ν is centered at p. Now, RHS doesn't depend on the curve: just on valuations and function field. The LHS is defined in an arbitrarily small neighborhood of the point: also affine and maximal ideal generated by one element. By previous results, we may "replace" C to be C' an affine neighborhood of p such that $\mathfrak{m} = \{f \in \mathcal{O}(C') : f(p) = 0\}$ is generated by a single element $x \in \mathfrak{m}$. Then $\nu(x) = 1$ by $\nu = \nu_{\mathfrak{m}}$ in previous Lemma. Described this valuation explicitly! Also $\nu(f) > 0 \Leftrightarrow f \in \mathfrak{m} \Leftrightarrow x$ divides f (because now it's generating the ideal!). So any $f \in \mathcal{O}(C)$ can be written as $f = x^{\nu(f)}\tilde{f}$ where $\tilde{f}(p) \neq 0$. Now prove the proposition! Pick $f \in \mathbb{C}(C)$. Write $f = g/h$ with $g, h \in \mathcal{O}(C)$. Write $g = x^{\nu(g)}g'$, $h = x^{\nu(h)}h'$, then $h'(p) \neq 0 \Rightarrow h'$ is invertible in some open neighborhood of p. So then $\nu(f) \geq 0 \Rightarrow \nu(g) - \nu(h) \geq 0$ which means $f = x^{\nu(g)-\nu(h)}g' \cdot (h')^{-1}$ is regular on some neighborhood of p which means $f \in \mathcal{O}_p$. Converse: $f \in \mathcal{O}(U')$ for some $p \in U' \subset U$, then by previous Lemma, $\nu(f) \geq 0$. $\square$ Note that we didn't prove $\mathfrak{m}_p = \{f \in \mathbb{C}(C) : \nu(f) > 0\}$ but the proof is similar.

IDEA: instead of thinking of functions, think of $\mathbb{C}(C)$ and a collection of opens $\mathcal{O}(U)$ and how they sit in $\mathbb{C}(C)$...

Corollary 11 *if C is a nonsingular curve and $U \subset C$ is open, then*

$$\mathcal{O}(U) = \bigcap_{p \in U} \mathcal{O}_p$$

as subsets of $\mathbb{C}(C)$.

This is true because we can find both equal to

$$\{f \in \mathbb{C}(C) : \nu_p(f) \geq 0 \ \ \forall p \in U\}.$$

Of course, ν_p is the unique valuation whose center is $p \in C$. Regular functions locally look like the quotient of polynomials: this is *exactly our definition!* Proof: one equality is by proposition; the inclusion $\mathcal{O}(U) \subset \bigcap_p \mathcal{O}_p$ is clear. Conversely, if $f \in \mathbb{C}(C)$, I get $\forall p \in U$ open affine regular $U_p \subset U$ a nbd of p such that $f \in \mathcal{O}(U_p)$ so all of these regular functions $f : U_p \to \mathbb{C}$ agree on overlaps (Exercise!) $\square$ Just building theory, it's hard to do examples - goal is this theorem:

Theorem 10 *Let L be a finitely generated field extension over $\mathbb{C}$ of transcendence degree 1. Then $\exists$ a projective nonsingular curve C with the following properties:*

(i) $\mathbb{C}(C) \leftrightarrow L$

(ii) points of C $\leftrightarrow$ discrete valuations on $L/\mathbb{C}$

(iii) topology on $C \leftrightarrow$ closed sets are finite sets of valuations (or all or none)

(iv) $\mathcal{O}(U) \leftrightarrow \bigcap_{v \in U} \mathcal{O}_v = \{f \in L : \nu(f) \geq 0\}$.

In particular, exists at most one up to isomorphism such nonsingular projective curve (bijections give morphisms). Given $\mathbb{C}, x, y, p(x,y) \in \mathbb{C}[x,y]$ irreducible, then can make $L = f.f.\,\mathbb{C}[x,y]/(p)$ and then find curve. Don't know yet that $\forall$ curves not just affine we can desingularize: that's what we'd get. It looks like one category is the same as another ... but we haven't talked about the morphisms here...

26 April 22

Corollary 12 *A nonsingular affine curve C is normal.*

Recall, we already know the converse. Sketch of proof: pick $C \to \mathbb{C}$ finite (Noether normalization) and let $C' \to C$ be a normalization. Then discrete valuations on $\mathbb{C}(C)/\,\mathbb{C}$ with center on C is equal to $\{\nu \text{ s.t. } \nu(f) \geq 0 \ \forall f \in \mathcal{O}(C)\}$ which is equal to $\{\nu : \quad \nu(f) \geq 0 \forall f \in \mathcal{O}(C')\}$, which we want to say is equal to all valuations on $\mathbb{C}(C')/\,\mathbb{C}$ with center on C'. Get desired equality by

$$\mathcal{O}(C) = \bigcap_{p \in C} \mathcal{O}_p = \bigcap_{\text{vals as above}} \mathcal{O}_\nu = \bigcap_{p \in C'} \mathcal{O}_p = \mathcal{O}(C')$$

hence $C = C'$ is equal to its normalization, hence it's normal; note that we used $\mathbb{C}(C) = \mathbb{C}(C')$.

Now prove this theorem we stated last time:

Theorem 11 $\forall$ *finitely generated field extensions $\mathbb{C} \subset L$ with $trdeg_{\mathbb{C}} L = 1$, $\exists$ a nonsingular projective curve C with $\mathbb{C}(C) = L$ and moreover (of course ! up to isomorphism:)*

(i) points of C $\leftrightarrow$ all ν on $L/\,\mathbb{C}$
(ii) topology $\leftrightarrow$ cofinite topology
(iii) $\mathcal{O}(U)$ $\leftrightarrow_{=} \bigcap_{\nu \in U} \mathcal{O}_\nu$ where $\mathcal{O}_\nu = \{f \in L : \nu(f) \geq 0\}$.

Proof: have done everything but existence (there's a version of this with functorality). For existence, pick $\mathbb{C}(x) \subset L$ as before; then picture $A = \mathbb{C}[x]$, $A' = \mathbb{C}[x^{-1}] = \mathbb{C}[y]$, and $A'' = \mathbb{C}[x, x^{-1}]$, in their corresponding B, B', B'' integral closures in L. We saw in the exercises that $B'' \cong B_x \cong B'_y$. The intersection $B \cap B'$ is the curve corresponding to B'': the projective nonsingular model. By Jarod's Theorem, finitely generated algebras over $\mathbb{C}$ correspond to curves: domains with transcendence degree 1; B'': open part of two affine curves (if you know abstract scheme theory, this would be obvious). Pick generators $b_1 = x, b_2, \ldots, b_r \in B$ which generate B as a $\mathbb{C}$-algebra. Pick $b'_1 = y, b'_2, \ldots, b'_s$ generators, and choose n large enough such that $x^n b'_j \in B$, $y^n b_i \in B'$ for all i, j. Consider homogeneous variables/coordinates

$$X_0, X_1, Y_1, \ldots, Y_r, Z_1, \ldots, Z_s$$

in $\mathbb{P}^{r+s+1}$. Define a graded ideal $I \subset \mathbb{C}[X_0, X_1, Y_1, \ldots, Z_s]$ by the rule

$$F \in I \Leftrightarrow F(1, x^n, b_1, \ldots, b_r, x^n b'_1, \ldots, x^n b'_s) = 0 \text{ in } B' \text{ or in } L.$$

Set $C = V_+(I) = \bigcap_{F \in I} V_+(F)$. By some algebra, I is finitely generated; won't prove this. Then YOU prove $C \cap (\mathbb{P}^{r+s+1} \setminus V_+(X_0)) = C \cap U_0 \cong$ an affine curve with coordinate ring B. This works because we're looking in an algebraic set in $\mathbb{C}^{r+s+1}$ defined by kernel of

$$\mathbb{C}[x_1, y_1, \ldots, y_r, z_1, \ldots, z_s] \to B$$

surjective by $x_1 \mapsto x^n$, $y_i \mapsto b_i$ and $z_j \mapsto b'_j x^n$ are all in B! Then you prove $C \cap U_1$ is cong to an affine whose coordinate ring is B'. Because first coordinates become $\frac{1}{x^n}, \frac{1}{x^n} b_1, \ldots, \frac{1}{x^n} b_r, b'_1, \ldots, b'_s$ all in B'. Third thing: $C \cap V_+(X_0) \cap V_+(X_1) = \emptyset$. This is tricky: use b_i, b'_j integral over $\mathbb{C}[x^n]$ (it's irreducible - the intersection of two irreducibles) and here $C = (C \cap U_0) \cup (C \cap U_1)$ is nonsingular.

Example: hyperelliptic curve $z^2 = \prod_{i=1}^{2g+2}(x - \lambda_i)$ write $\lambda_i \in \mathbb{C}$ pairwise distinct, I mean $L = \mathbb{C}(x)[z]/(z^2 - \prod_{i=1}^{2g+2}(x - \lambda_i))$. Scratch work, with $y = \frac{1}{x}$, we get

$$\big(\frac{z}{x^{g+1}}\big)^2 = \prod (1 - y\lambda_i)$$

and so

$$B' = \mathbb{C}[y, \frac{z}{x^{g+1}}]/\Big(\big(\frac{z}{x^{g+1}}\big)^2 - \prod(1 - \lambda_i y)\Big)$$

now take in construction of the proof $b_1 = x$, $b_2 = z$, $b'_1 = y = x^{-1}$, $n = g + 1$ works; procedure tells us to take $X_0, X_1, Y_1, Y_2, Z_1, Z_2$ given by $1, x^{g+1}, x, z, x^n y, x^n \frac{z}{x^{g+1}}$ which is $1, x^{g+1}, x, z, x^g, z$. Now procedure is to consider ALL homogeneous polynomials in $X_0, X_1, Y_1, Y_2, Z_1, Z_2$ which give relations between the $1, x^{g+1}, x, z, x^g, z$. In particular, $Y_2 - Z_2 = z - z = 0$, so we can eliminate Z_2 (it's expressible in terms of Y_2). Relabel the variables for now: $X_0 = 1$, $X_1 = x$, $X_2 = x^g$, $X_3 = x^{g+1}$, $X_4 = z$. Look at homogeneous equations here: $X_0 X_3 - X_1 X_2 = 0$: our curve is in the hypersurface given by this equation. To figure out all equations is quite hard;

$$X_0^{2g} X_4^2 - \prod_{i=1}^{2g+2} (X_1 - \lambda_i X_0) = 0$$

is the main one. Also (*) $X_1^g - X_0^{g-1} X_2 = 0$, or $X_1^{g+1} - X_0^g X_3 = 0$, or $X_2^{g+1} - X_0 X_3^g = 0$ etc. Figure out each equation of degree d (combinatorial). Also need

$$X_3^{2g} X_4^2 - \prod_{i=1}^{2g+2} (X_3 - \lambda_i X_2) = 0.$$

For example, $X_1 X_3^{g-1} - X_2^g = 0$ is dual to (*). Now when $X_2 \neq 0$, get $\cong \mathbb{C}[\frac{X_1}{X_2}]$, and when $X_3 \neq 0$, get $\cong \mathbb{C}[\frac{X_2}{X_3}]$. ... argument looking at degrees ... what you have to do abstractly using integrality ...

27 April 27: Guest Lecture - Andrew Obus

Question: what do projective smooth connected curves look like as topological spaces in the standard complex topology? What we know:

- Any point on a nice curve has a neighborhood homeomorphic to an open disc in $\mathbb{C}$ (consequence of the implicit function theorem in Homework 8)
- Hence, should appear to be a real 2-dimensional surface
- They are smooth
- *Orientable*: exists a consistent continuous choice of "clockwise" on the tangent space at each point (intrinsic definition - see manifolds course). Why? $\forall p \in C$, look at affine open patch $p \in U \subset C$, well this lives in some $\mathbb{A}^n = \mathbb{C}^n$, and the tangent space T_pC is a 1-dimensional complex line, which is 2-real dimensions, and the rotation v to $-iv$ by multiplication by $-i$ is a 90 degree clockwise rotation. We can see that this is consistent because for any two points $p, q \in C$, there is an affine patch containing p and q, and then the transition from v on p and q on q is given by a matrix $GL(\mathbb{C}, n)$ which commutes with multiplication by $-i$.
- Also compact: closed subsets of $\mathbb{P}^N$ which is compact and Hausdorff in the standard topology (remember its a quotient of S^{2N+1} in $\mathbb{C}^{N+1}$).

Upshot: C a compact, orientable, smooth surface implies by topology (end of Munkres) that any one of this is Σ_g for some $g \in \mathbb{N}$ (genus / genera; like lemma/lemata). In light of the equivalence of categories from past lecture, note that given any $g \in \mathbb{N}$, there $\exists$ an ∞ number of algebraic function fields that are non-isomorphic that give the same Σ_g...

Question: given equations for a curve, can we calculate how many holes are in its associated complex space?

Theorem 12 *If $C \subset \mathbb{P}^2$ is a smooth plane curve defined by a degree d homogeneous polynomial then*

$$g(C) = \frac{(d-1)(d-2)}{2}.$$

We won't prove this fully. This is true only when the curve can be embedded in $\mathbb{P}^2$. We will prove this for $d = 1, 2, 3$, i.e. $g = 0, 0, 1$.

27.1 Case $d = 1$:

We get $\mathbb{P}^1 \subset \mathbb{P}^2$ and $\mathbb{C}\,\mathbb{P}^1 \cong S^2$ which implies $g = 0$.

27.2 Case $d = 2$:

A generic quadratic is

$$aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0.$$

Claim: by completing the square, we can eliminate all the cross terms by a substitution, but first we would need a substitution making sure $a, b, c \neq 0$. Then we get

$aX^2 + bY^2 + cZ^2 = 0$, but by scaling we can assume $a, b, c \in \{0, 1\}$. If $a = b = c = 0$ then we don't get a curve. If 2 of the a, b, c are 0, then we get a line, which is not reduced (double line - scheme theory to come) as in $x^2 = 0$. If one of them is 0, we get $X^2 + Y^2 = 0$, which is $(X + iY)(X - iY) = 0$ the union of two lines; at their intersection, we will not get a smooth point. Thus, we are left with the only possibility: $X^2 + Y^2 + Z^2 = 0$: indeed, all smooth conics are isomorphic to this! Hence, we can pick and conic like this and look at it! Choose C to be defined by $X^2 - YZ = 0$ (verify its smooth on your own). Claim: $f : \mathbb{P}^1 \to C$ is an isomorphism for $f : [s : t] \mapsto [st : s^2 : t^2]$. Note that we avoid $[0 : 0 : 0]$ and that this point lives on the variety. This is an isomorphism with inverse $[x : y : z] \mapsto [x : z]$ whenever $[x : y : z] \neq [0 : 1 : 0]$, i.e., on $U_0 \cup U_2$ and also $[x : y : z] \mapsto [y : x]$ for $[x : y : z] \neq [0 : 0 : 1]$, i.e. on $U_0 \cup U_1$, which gets everything. Indeed, on the overlaps we have $\frac{y}{x} = \frac{x}{z}$ (check yourself that this is true, and that the compositions give identities both ways). Now $C = \mathbb{P}^1$ hence $g(C) = 0$.

As an aside, note that there is something called "arithmetic genus" which holds for curves even when it isn't smooth...carrying on

27.3 Case $d = 3$:

C: defined by

$$aX^3 + bY^3 + cZ^3 + dX^2Y + eXY^2 + fX^2Z + gXZ^2 + hY^2Z + IYZ^2 + jXYZ = 0.$$

Claim: any smooth plane cubic is isomorphic to one given by the equation of the form

$$Y^2Z = X(X - Z)(X - \lambda Z) \qquad \text{for some} \quad \lambda \in \mathbb{C} \setminus \{0, 1\}.$$

If $Z = 1$, then on that patch $U_z \subset \mathbb{P}^2$ this is $y^2 = x(x-1)(x-\lambda)$ - "Weierstrass form".

Pf sketch: admit that any smooth cubic has an **inflection point** - a point where the tangent line is of order 3. This is a statement about partials vanishing: the intersection of the curve of partials vanishing with the original curve must have intersection by Bezout's Theorem. Actually, can phrase this inflection property about the ideal you get: it has to do with the length of the ideal (should be 3)... Anyway, consider $\mathrm{Aut}(\mathbb{P}^n)$, which is $\mathbb{P}GL^{n+1}$ (this is $n + 2$ transitive) for $n = 2$. Then it is a fact that

1) $\forall p, q_1 \mathbb{P}^2$ $\exists$ an isomorphism of $\mathbb{P}^2$ taking p to q (transitivity) - given by 3×3 matrices.

2) for a point $p \in \mathbb{P}^2$ and two lines l_1, l_2 through p, there exists an isomorphism of $\mathbb{P}^2$ taking l_1 to l_2 and fixing p. Hence, we can assume that the inflection point of C is $[0 : 1 : 0]$ with tangent line $z = 0$. Claim: $b = 0$: on line $z = 0$, we are left with $aX^3 + dX^2 + eX$ when $y = 1$, but we need inflection point of order 3, so $d = e = 0$ (sketchy...).

Writing

$$hY^2Z + IyZ^2 + jXYZ = aX^3 + fX^2Z + gXZ^2 + cZ^3,$$

we can show that $h, a \neq 0$, since otherwise it factors when $a = 0$ and $h = 0$ gives us a singularity. By scaling, assume $h = a = 1$. Set $z = 1$ (in affine coordinates for simplicity) then complete the square in $y^2 + Iy + jxy = ax^3 + fx^2 + gx + c$ by $y \mapsto y - \frac{I}{2} - \frac{j}{2}x$, we end up getting

$$\begin{aligned} y^2 &= a'x^3 + f'x^2 + g'x + c' \\ y^2 &= (x - e_1)(x - e_2)(x - e_3) \end{aligned}$$

by smoothness we can show that e_1, e_2, e_3 are pairwise distinct (otherwise not smooth). Now setting $x = (e_2 - e_1)x' + e_1$ and $y = (e_2 - e_1)^{3/2}y'$ we get

$$(y')^2 = x'(x' - 1)(x' - \lambda)$$

where $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$ since all are pairwise not equal we get $\lambda \notin \{0, 1, \infty\}$. Projectivizing this, we get $Y'^2Z = X'Z(X' - Z)(X' - \lambda Z)$ as stated. The real content here to remember: any smooth cubic has an inflection point. $\square$

Fun part: now we have a relatively simple equation, let's see what this looks like. Well C defined by $y^2 = x(x - 1)(x - \lambda)$ on an affine patch ($[0 : 1 : 0]$ is point at ∞), we can project $f : C \to \mathbb{P}^1$ by $(x, y) \mapsto [x : 1]$ and $\infty \mapsto [1 : 0]$. This is not an isomorphism! Given $x \in \mathbb{A}^1 \amalg \{\infty\}$, there exist two square roots above in C, lest $x \in \{0, 1, \lambda, \infty\}$ given by $x_1 \pm \sqrt{x(x - 1)(x - \lambda)}$ obviously.

Claim: on $\mathbb{P}^1 \setminus (L_1 \cup L_2)$ where L_1 is the slit connecting 0 and ∞ and L_2 is the slit connecting 1 and λ, there exists a consistent choice of square root for $x(x-1)(x-\lambda)$. Idea of proof: problem of monodromy in $z \mapsto \sqrt{z}$ in complex case. Around the slit, we change sign twice, hence $(-1)^2 = 1$ is cool. Further, because $\pi_1(\mathbb{P}^1 \setminus (L_1 \cup L_2)) = \mathbb{Z}$, we took a generator of this, this is all we need to check (hand-wave).

Upshot: if we take $\mathbb{P}^1 \setminus (L_1 \cup L_2)$, then $C \setminus f^{-1}(L_1 \cup L_2)$ is two disconnected copies of $\mathbb{P}^1 \setminus (L_1 \cup L_2)$, one corresponding to each of the two consistent choices of square root. So to understand C, we have to know how these glue togetehr. By the homeomorphic ripping, we see that our two spheres with two slits rip off to form two halves of the torus (drawing argument) - hence $g(C) = 1$.

27.4 Remarks

First: in topology, $\mathbb{T}^2 \cong \mathbb{S}^1 \times \mathbb{S}^1$, and $\mathbb{S}^1 = \mathbb{R} / \mathbb{Z}$ is a group, so $\mathbb{T}^2$ has a group structure, so my **curve** has a group structure! If we choose the homeomorphism carefully, this gives a very natural geometric rule for the group structure on C [need to deal with Eisenstein series for this...] turns out cubic curves have group structure, while degree 5 and 6 do not (sketches group law for elliptic curve).

Second remark: can also prove $g(C) = 1$ using Hurwitz formula from topology; branch points + genus below gives you a formula for the curve upstairs (use simplicial decomposition and count simplices upstairs: this is very general and can be used for any curve...

Third remark: can do algebraic geometry over characteristic p fields... no good "complex space," but for arbitrary fields (algebraically closed fields) still can define genus of curves! But not as easy: there's a formula that agrees with that of curves over $\mathbb{C}$ and for smooth plane curves the formula $g(C) = \frac{(d-1)(d-2)}{2}$ still holds. This g is still an integer, not an element of $\mathbb{F}_2$ say. A lot of curves aren't smooth in $\overline{\mathbb{F}_2}$. You can use (i) the dimension of the vector space of global differential forms on the curve or (ii) sheaf cohomology [something about ideal class group in ring of integers to field of functions...]

28 April 29

Discussion of Exercise 12.5 omitted.

28.1 Impromptu discussion of the formula for genus of smooth plane curves

Proving $C \subset \mathbb{P}^2_{\mathbb{C}}$ nonsingular of degree d has genus $g(C) = \frac{(d-1)(d-2)}{2}$, there are several ways to do this. Here's a sketch of the standard idea: construct a finite map $C \to \mathbb{P}^1$ and count branch points; projection from a point in $\mathbb{P}^2$ to a line, $[X_0 : X_1 : X_2] \mapsto [X_1 : X_2]$ not defined at $[1 : 0 : 0]$ (the projection point). Almost everywhere you get the same number of points with multiplicity 1 preimage intersections, though for some you get tangent lines: if $p_0 \in \mathbb{P}^1$ lies on a tangent line through the projection point r, then typically you get $d - 1$ preimages, and the sequence of e_is is $(2, 1, 1, \ldots, 1)$. How many times does that happen? (discussion of existence of a general position projection source r omitted) Let C be a curve defined by $F_d(X_0, X_1, X_2) = 0$ smooth of course. On an affine piece $X_2 = 1$ say, this means counting when $F(x, t, 1)$ as a polynomial in x has a double root. This happens iff $\gcd\big(F(x,t,1), \frac{\partial F}{\partial x}(x,t,1)\big) \neq 1$ which happens iff $\mathrm{Res}_x\big(F(x,t,1), \frac{\partial F}{\partial x}(x,t,1)\big) = 0$. Looking at arbitrary equations $a_0x^d + a_1x^{d-1} + \cdots + a_d$ with derivative $da_0x^{d-1} + (d-1)_1x^{d-2} + \cdots + a_{d-1}$, we guess that if everything is in general position, since $\deg_t(a_i) \leq i$, we'd have

$$\deg_t \mathrm{Res}_x(F, \frac{\partial F}{\partial x}) = d(d-1).$$

If g is the number of holes, we get it by a triangulation of the surface

$$2 - 2g = V - E + F$$

the Euler characteristic, where V is the number of vertices, E the number of edges, and F the number of faces. For $\mathbb{P}^1 = \mathbb{S}^2$, we see we can triangulate with two triangles,

and $3-3+2=2$ hence $g=0$. Proving these things are independent of triangulation, do that later in life. Similarly for the torus, use gluing square and draw a diagonal to get $1-3+2=0$ so $g=1$ (fishy). Euler characteristic also shows up as the alternating sum of betti numbers in (co)homology. **It is the only invariant for these guys somehow**.[20] Why is it well defined, this "number of holes"? Not entirely obvious! Euler number of spaces is additive: $e(X \amalg Y) = e(X) + e(Y)$. For example, e of the open interval is -1, because it is e of the closed interval minus e of the boundary, i.e. $1-1-1=-1$. This can be generalized to more spaces...

Back to our curve: we have $\pi : C \to \mathbb{P}^1 \supset$ a finite set of points $d(d-1)$ of them which have $d-1$ points on the fibre. We want to look at what happens to the triangulation at edges and points: find triangulation of $\mathbb{P}^1$ whose vertices are these $d(d-1)$ points of interest, these p_0s. Between two such p, p' the preimages of the edges will be d different strands attached to $d-1$ points: i.e., corresponding to the partition $2,1,1,\ldots,1$ of d! Then we see it pulls back by π to a triangulation of C. Indeed, let v be the number of vertices on $\mathbb{P}^1$ and V the number of vertices on C, same for e, E and f, F:

$$\begin{aligned} +V &= d \cdot (v - d(d-1)) - (d-1) \cdot (d(d-1)) \\ -E &= d \cdot (e) \\ +F &= d \cdot (f) \end{aligned}$$

$$e(C) = d \cdot e(\mathbb{P}^1) - d^2(d-1) + d(d-1)^2 = 2d - d(d-1)$$

and $e(C) = 2-2g$ gives by algebraic juggling $2g = (d-2)(d-1)$ as desired. $\square$

Again, this is one of the many ways to do this. We need to get $(2,1,\ldots,1)$ and "simple branching".

28.2 Material: postlude

Given $\varphi : C_1 \to C_2$ a nonconstant map of nonsingular projective curves, we get $\mathbb{C}(C_2) \subset \mathbb{C}(C_1)$. Indeed, C_1 corresponds to valuations on $\mathbb{C}(C_1)$, and C_2 to valuations on $\mathbb{C}(C_2)$, and the map $v \mapsto v\big|_{\mathbb{C}(C_2)^*}$ restricts to a valuation. This is the basis for the proof of the functorial thing: the category of non-singular projective curves with **non-constant morphisms** is in anti-equivalence with finitely generated field extensions $\mathbb{C} \subset L$ with $\mathrm{trdeg}_{\mathbb{C}}(L) = 1$ by maps $C \mapsto \mathbb{C}(C)$, $(C_1 \to C_2)$ $mapsto(\mathbb{C}(C_2) \subset \mathbb{C}(C_1))$.

Another simple loose end: **ramification indices**! Let's look at them holomorphically. If $h : \{|z| < \delta\} \to C$ is holomorphic and $h(0) = 0$, then $\exists e \geq 1$ and $\exists g : \{|z| < \epsilon\} \to \mathbb{C}$ holomorphic with $0 < \epsilon < \delta$ and $\frac{\partial g}{\partial z}(0) \neq 0$ such that

$$h = g^e \qquad \text{on} \quad \{|z| < \epsilon\}.$$

[20] This sounds awesome.

Geometrically, $0 \mapsto 0$ for $\{|z| < \delta\} \to \mathbb{C}$ by h, then there is a subset of our original domain $\{|z| < \epsilon\}$ such that it is sent by g to some open in $\mathbb{C}$ where to map from this open back to $\mathbb{C}$ the target of h commutatively we get $z \mapsto z^e$. This is saying that up to coordinate change locally our projection looks like z^e this "twisting". We can characterize this integer e as the smallest integer such that $\frac{\partial^e h}{\partial z^e}(0) \neq 0$.

Proof sketch: write

$$h(z) = c_e z^e + c_{e+1} z^{e+1} + \cdots = z^e(c_e + c_{e+1} z^1 + \cdots)$$

and then take e^{th} root of u (we did an exercise at the formal level), and take $g = zu^{1/e}$. Then given a nonconstant map $\varphi : C_1 \to C_2$ of nonsingular projective curves, $p \in C_2$ with $\varphi^{-1}(p) = \{q_1, \ldots, q_r\}$ such that $\forall q_i$ $\exists$ small discs: morphisms are holomorphic locally on discs; get e_i for each q_i. These $e_1, \ldots, e_r$ are different from what we have done so far: before, the bottom curve was a $\mathbb{P}^1$. It turns out it's always true that the sum of the e_i is

$$\sum e_i = \deg \varphi = \deg[\mathbb{C}(C_1) : \mathbb{C}(C_2)]$$

for almost every p has $e_i = 1 \forall i$, i.e. $r = d$. But otherwise we get a *partition of the degree.*

For the exam: a lot of easy questions: make sure you know you're definitions. But of course, I'm always asking things that are tricky, so try not to get hung up.

29 6 May: Final Exam Review

The goal is to give lots of easy questions.

1. **When is a quasi-projective variety X nonsingular at a point p?** Pick an affine open neighborhood $U \subset X$, $U \hookrightarrow \mathbb{C}^n$ closed. If $\dim X = k$, let $f_1, \ldots, f_N \in \mathbb{C}[x_1, \ldots, x_n]$ generate the ideal of U. Look at the rank of the matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$: it should have rank $n - k$. Note that choosing the f_i to generate $I(U)$ is necessary, since choosing squares of these functions will cut out set theoretically the same thing but the Jacobian will vanish.

2. **What is the dimension of a variety?** Let X be a quasi-projective variety. Choose $U \subset X$ an affine open, $U \neq \emptyset$, and look at $\mathcal{O}(U)$ the ring of regular functions, and take its fraction field: this is $\mathbb{C}(X)$. Then $\text{trdeg}_{\mathbb{C}}(\mathbb{C}(X)) = \dim X$. Make a list of definitions and know them: on exam, something like "what is a function field? why is it well-defined?"

3. **What is a discrete valuation?** Let $K \subset L$ be an extension of fields. A discrete valuation on L/K is a surjective ring map $\nu : L^* \to \mathbb{Z}$ such that
(i) $\nu(f + g) \geq \min(\nu(f), \nu(g))$
(ii) $\nu(fg) = \nu(f) + \nu(g)$ (iii) $\nu\big|_{K^*} = 0$.

4. **What are the irreducible components of $V(x_1x_2, x_1x_3, x_2x_3) \subset \mathbb{C}^3$?** Must have at least two 0, hence elements are scalar multiples of $(1,0,0)$, $(0,1,0)$, $(0,0,1)$. It's the coordinate axes: $V(x_1,x_2) \cup V(x_1,x_3) \cup V(x_2,x_3)$.

5. **Find a finite projection of $C = V(xy+x+y+2)$ in $\mathbb{C}^2$ to $\mathbb{C}$.** We had a criterion for finiteness: projection to x iff written as a polynomial in y with coefficients in $\mathbb{C}[x]$ it's monic. Clearly here $xy+x+y+2 = (x+1)y+(x+2)$ isn't monic, so it won't work. By the affine change of coordinates $x = u+v$, $y = u-v$, our equation becomes $u^2+2u+(2-v^2)$ which is monic in u so project to v.

6. **Given an example of a Zariski closed curve $C \subset \mathbb{P}^3$ such that**

   (a) C is nonsingular. Lines are nonsingular, so take $V_+(X_2) \cap V_+(X_1)$. Have to go to affine pieces and check smoothness. If in some window there's no curve, the emptyset is nonsingular :). This set is $\{[*:0:0:*]\}$ check on U_0 and U_3.

   (b) C is singular. Find a curve in $\mathbb{C}^3$ that's singular and homogenize. Take $y^2 = x^3$ and $z = 0$ in $\mathbb{C}^3$.

   (c) C is nonsingular and C is not contained in $V_+(aX_0+bX_1+cX_2+dX_3)$ for any $(a,b,c,d) \in \mathbb{C}^4 \setminus 0$. This would take too much time to give on an actual test, but most things should satisfy this: take $y^2 - x = 0$, $z^3 - y = 0$ in $\mathbb{C}^3$, that is, the image of $\{(t^6,t^3,t)\}$ is a submersion (everywhere non-zero derivative).

7. **Give as a function of $a \in \mathbb{C}$ the number of intersection points of $V(xy-1)$ and $V(x^3+y^3+a)$.** Certainly $x = 0$ or $y = 0$ is not on $V(xy-1)$, so then $y = \frac{1}{x}$ can say $x^3 + \frac{1}{x^3} + a = 0$ so can write this as $x^6 + ax^3 + 1 = 0$. This is a quadratic in x^3, so $x^3 = \frac{-a \pm \sqrt{a^2-4}}{2}$. Hence there are six intersection points unless $a = \pm 2$, in which case there are three. Note that we aren't in the case $x = 0$.

8. **Give an example of a morphism $\mathbb{C}^2 \setminus \{0\} \to \mathbb{P}^1$ which does not extend to a morphism from $\mathbb{C}^2 \to \mathbb{P}^1$.** The quotient map $(a,b) \mapsto [a:b]$ works, since whatever $\pi((0,0)) \in \mathbb{P}^1$ is, separate it with another point, but the two lines $\pi((0,0))$ and $z \in \mathbb{P}^1$ are infinitely close to $(0,0)$. Can also say that by continuity, lines without $(0,0)$ that take constant values force $(0,0)$ to take every constant value, contradiction.

9. **Let C be a projective curve. Show $\mathcal{O}(C) = \mathbb{C}$.** This is sketchy: we wouldn't have this on the test, but this is a fact we should've shown earlier. A map $f : C \to \mathbb{C}$ in usual topology, domain is compact and image is compact set, so exist points that don't get hit. But, it happens to be true that morphisms that are non-constant must hit all but finitely many points.

10. **Let $X = V_+(X_0^2 + X_1^2 + X_2^2 + X_3^2) \subset \mathbb{P}^3_{\mathbb{C}}$. Does there exist a Zariski closed 1-dimensional curve $C \subset \mathbb{P}^3_{\mathbb{C}}$ such that $C \cap X = \emptyset$?** Ask Kyler for a solution. Uses 9.