MATH 137, SPRING 2020

WITH BROOKE ULLERY

CONTENTS

PRELIMINARIES

These notes were taken during the spring semester of 2020 in Harvard's Math 137, *Algebraic Geometry*. The course was taught by Dr. Brooke Ullery and transcribed by Julian Asilis. The notes have not been carefully proofread and are sure to contain errors, for which Julian takes responsibility. Corrections are welcome at `asilis@college.harvard.edu`.

1. INTRODUCTION, ALGEBRAIC SETS

Some introductory texts on algebraic geometry can sacrifice content for form, focusing on convincing you that algebraic geometry is cool and pretty instead of teaching you very much about it. We'll place more priority on content, really getting into the heart of algebraic geometry. For that next couple weeks that'll mean that we'll be talking about curves.

Before we get there, let's talk a bit about what algebraic geometry *is* and the kinds of questions that it can help answer. Roughly speaking, algebraic geometry (AG) is the study of geometric objects called *varieties*. Varieties are (locally) defined by polynomial equations in k^n, where k is a field. So we might write

$$V = \{(a_1, \ldots, a_n) \in k^n | f_i(a_1, \ldots, a_n) = 0\} \subseteq k^n$$

where the f_i are elements of $k[x_1, \ldots, x_n]$.

Example 1.1. Varieties include conics in $\mathbb{R}^2$ like $V_1 = \{(x,y)|x^2+4y-1=0\}$, which is an ellipse. Or $V_2 = \{(x,y)|x^2-y^2-1=0\}$, which is a hyperbola. In each of these examples we only looked at the zeroes of a single polynomial, but keep in mind that we're allowed to look at the shared zeroes of an arbitrary collection of polynomials.

Roughly speaking, varieties give us a dictionary between geometry and algebra, whereby questions concerning the geometry of a curve can be translated into questions at the level of commutative algebra. Varieties need not live in k^n, but it'll turn out that we can often translate things to k^n.

What kinds of questions can we ask about varieties? For V a variety, it is sensible to ask about:

(a) Singularity theory - what kind of geometry does V have near a point? Cusps, etc. How to find a "smooth model" of a variety?
(b) Intersection theory - how do varieties intersect? In the plane, a line and a conic can intersect in 0, 1, or 2 points. This includes making precise notions like multiplicity.
(c) Number theory - counting rational points in a variety. This includes Diophantine problems, like asking what the rational solutions to $x^n + y^n = 1$ are. Geometrically, this translates to asking what the corresponding variety in $\mathbb{Q}^2$ looks like.
(d) Embedding questions - given a variety V, is there an embedding $V \hookrightarrow k^n$? If so, what's the smallest n such that an embedding exists? Is there an embedding $V \hookrightarrow \mathbb{P}^n$? If there is, V is called a *projective variety*
(e) Points imposing conditions on polynomials - how many polynomials pass of degree n pass through k points? E.g. if $p_1, \ldots, p_5 \in \mathbb{R}^2$, which conics contain them? It turns out that all sets of 5 points are contained in some conic, and most are contained in a unique conic.

Now let's really get into things. For the moment, we'll consider fields k which are *algebraically closed*, meaning all polynomials in $k[x]$ have zeroes in k (or, equivalently, surject onto k). By induction, this implies that any element of $k[x]$ has all its roots in k and is the product of linear factors.

Example 1.2. $\mathbb{C}$ is famously algebraically closed but $\mathbb{R}$ is not: x^2+1 has no real roots.

Definition 1.3. *Affine n-space*, denoted $\mathbb{A}^n_k$ or $\mathbb{A}^n$, is the set of n-tuples of elements of k. It is not endowed with such structure as an origin or the structure of a vector space.

We'll be thinking of polynomials as functions from $\mathbb{A}^n_k$ to k, as well as being elements of a (polynomial) ring.

Definition 1.4. A *conic* is the zero set of a quadratic polynomial $g(x,y) = ax^2 + bxy + cy^2 + dx + ey + f$.

Definition 1.5. Let $S \subseteq k[x_1, \ldots, x_n]$ be a set of polynomials. Then $V(S)$ is the set of common zeroes of the elements of S. More explicitly,

$$V(S) = \{p \in \mathbb{A}^n | f(p) = 0 \ \forall f \in S\}.$$

Moreover, $X \subseteq \mathbb{A}^n$ is an *algebraic set* if $X = V(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$.

Proposition 1.6. *Let $S \subseteq k[x_1, \ldots, x_n]$ and $I = (S)$. Then $V(S) = V(I)$.*

Proof. Clearly $V(S) \supseteq V(I)$. In the other direction, a zero of $f_1, \ldots, f_n$ is also a zero of $\alpha_1 f_1 + \cdots + \alpha_n f_n$. □

So we need only worry about algebraic sets arising from ideals of polynomial rings (since they all do!). Using only definition, we can prove a few more basic properties of $V(-)$.

Proposition 1.7. *The following hold for $V(-)$ as defined above:*

(1) It's inclusion reversing: $I \subseteq J$ implies $V(I) \supseteq V(J)$.
(2) If $\{I_\alpha\}$ is a collection of ideals, then $\cap_\alpha V(I_\alpha) = V(\cup_\alpha I_\alpha)$. So algebraic sets are closed under arbitrary intersection.
(3) If $f, g \in k[x_1, \ldots, x_n]$ then $V(f) \cup V(g) = V(fg)$. More generally, $V(I) \cup V(J) = V(IJ)$ for I, J ideals. So algebraic sets are closed under finite unions.
(4) $V(0) = \mathbb{A}^n$, and $V(1) = \emptyset$. And $V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$, so any finite set is algebraic.

Remark 1.8. The third claim of the above proposition cannot be made stronger: algebraic sets are not in general closed under infinite unions. More importantly, the above propositions tell us that algebraic sets behave like closed sets in topological spaces (contain $\mathbb{A}^n$ and $\emptyset$, closed under arbitrary intersections and finite unions).

Definition 1.9. $X \subseteq \mathbb{A}^n$ is *Zariski closed* if X is an algebraic set. A *Zariski open* set is the complement of a Zariski closed set.

The Zariski open sets form the Zariski topology on affine space, which is always strictly coarser than the Euclidean topology.

2. Radical ideals, Irreducibility, Noetherian rings

Last time we talked about how to move from polynomial to algebraic sets in affine space using the $V(-)$ function. Today we'll talk about how we can move in the other direction, from points of affine space to polynomials over the appropriate field.

Again let k be an algebraically closed field, $R = k[x_1, \ldots, x_n]$, and $X \subseteq \mathbb{A}^n$.

Definition 2.1. The *ideal* of X, $I(X)$, is the set of polynomials in R that vanish on X.

This might look like an inverse to $V(-)$, but unfortunately this isn't quite so.

Example 2.2. Let $X = \mathbb{Z} \subseteq \mathbb{A}^1_{\mathbb{C}}$. Then $V(I(X)) = V(0) = \mathbb{A}^1 \neq X$. Perhaps more interestingly, let $J = (y, y - x^2) \subseteq \mathbb{C}[x, y]$. Then $V(J) = V(y) \cap V(x^2) = \{(0, 0)\}$, and $I(V(J)) = (x, y) \neq J$.

In general, we may ask how J and $I(V(J))$ compare. It's fairly easy to see that $J \subseteq I(V(J))$, but something stronger is true.

Definition 2.3. Let R be a ring and $I \subseteq R$ an ideal. The *radical* of I is $\text{rad}I = \{a \in R | a^n \in I, n \in \mathbb{N}\}$. An ideal I is *radical* if $I = \text{rad}I$.

Remark 2.4. In this class we'll assume that all rings are commutative.

Lemma 2.5. *$\sqrt{I}$ is a radical ideal.*

Proof. To see that $\text{rad}I$ is an ideal, suppose $a, b \in \text{rad}I$ meaning $a^n \in I$ and $b^m \in I$. Then $(a-b) \in \text{rad}I$ because $(a-b)^{n+m} \in I$. And $ca \in \text{rad}I$ because $(ca)^n = c^n a^n \in I$. To see that $\text{rad}I$ is radical, note that if $a \in \text{radrad}I$ then $a^n \in \text{rad}I$ so $a^{nm} \in I$ and thus $a \in \text{rad}I$. □

Proposition 2.6. *Let $R = k[x_1, \ldots, x_n]$*

a) If $J \subseteq R$ is an ideal, then $\text{rad}J \subseteq I(V(J))$.
b) If $X \subseteq \mathbb{A}^n$, then $X \subseteq V(I(X))$.

Proof. If $f \in \text{rad}J$ then $f^n \in J$ for some n and thus if $P \in V(J)$ then $f^n(P) = 0$. So $f(P) = 0$ and $f \in I(V(J))$. b) follows from definition. □

The following claims are left as exercises to check on your own.

Corollary 2.7. *I is inclusion-reversing, $I(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n)$, $I(X)$ is a radical ideal, and $V(I) = V(\text{rad}I)$.*

Example 2.8. Let's look at the cuspidal plane curve $X = \{(t^2, t^3)\} \subseteq \mathbb{A}^2_{\mathbb{C}}$. Is this an algebraic set? For $(x, y) \in X$, we have $x^3 - y^2 = 0$, so $X \subseteq V(x^3 - y^2)$. On the other hand, if $(a, b) \in V(x^3 - y^2)$ then choose t such that $t^2 = a$. Then $a^3 - b^2 = 0 \implies t^6 = b^2$. WLOG we can assume $b = t^3$ so indeed $(a, b) = (t^2, t^3) \in X$.
Now let $I = (x^2 + y^2, x^2 - y^2) \subseteq \mathbb{C}[x, y]$. What's $V(I)$? Geometrically, $V(I) = V(x^2 + y^2) \cap V(x^2 - y^2) = A \cap B$ for $A = V(x + iy) \cup V(x - iy)$ and $B = V(x + y) \cup V(x - y)$. By drawing two sets of perpendicular lines through the origin, we can see that $V(I) = \{(0, 0)\}$. Though it would've been easier to note that $I = (x^2, y^2)$ and $V(I) = V(\text{rad}I) = V(x, y) = \{(0, 0)\}$.

There's a notion in algebraic geometry like that of connectedness in topology, which allows us to decompose algebraic sets appropriately. It revolves around the notion of reducibility.

Definition 2.9. An algebraic set X is *reducible* if $X = X_1 \cup X_2$ where $X_1, X_2 \subsetneq X$ are algebraic sets. Otherwise X is *irreducible*.

Example 2.10. Let $L \subseteq \mathbb{A}^2$ be a line. Any $X \subsetneq L$ which is algebraic will consist of a finite set of points. So L is irreducible. On the other hand, $V(xy) = V(x) \cup V(y)$ is reducible while $V(x^2) = V(x) \cup V(x)$ is irreducible.

Definition 2.11. If $X = X_1 \cup \cdots \cup X_n$ for each X_i an irreducible algebraic set and $X_i \not\subset X_j$ the X_i are called the *irreducible components* of X.

It turns out that these decompositions always exist and are unique, though to show why we'll need to get into some algebra.

Definition 2.12. A (commutative) ring R is *Noetherian* if every ideal $I \subseteq R$ is finitely generated.

On the homework we'll show that there are several equivalent characterizations of the Noetherian property, some of which we list now.

Lemma 2.13. *R is Noetherian if and only if either of the following hold*

1) every strictly increasing chain of ideals terminates in finite time
2) every collection of ideals in R has a maximum with respect to inclusion

Proof. PSet 1 □

How can we bring this back to algebraic geometry? Via our function $I(-)$! The following claim explains what we mean.

Proposition 2.14. *$k[x_1, \ldots, x_n]$ is Noetherian $\iff$ every algebraic set in $\mathbb{A}^n$ is the intersection of finitely many hypersurfaces.*

That $k[x_1, \ldots, x_n]$ is Noetherian is a consequence of the Hilbert Basis theorem, which states that when R is Noetherian, $R[x]$ is as well.

3. Hilbert basis, Irreducible decomposition

Last time we talked about the Hilbert basis theorem, which states that $R[x]$ is Noetherian when R is Noetherian.

Corollary 3.1. *Any decreasing chain of algebraic sets terminates.*

Proof. Repeatedly using Hilbert basis, we have that $R[x_1, \ldots, x_n]$ is Noetherian. Passing through V and using the ascending chain condition formulation of the Noetherian condition gives the result. Recall that V is inclusion-reversing. □

Now we're ready to prove what we wanted to show last time about irreducible decompositions.

Theorem 3.2. *Let X be an algebraic set. Then*

a.) We can write $X = X_1 \cup \cdots \cup X_n$ where X_i is irreducible (i.e. cannot be written as a union of proper algebraic subsets)
b.) The above decomposition is unique

Proof. To decompose X, repeatedly write its components as unions of proper algebraic subsets. This procedure terminates by the above corollary. To see that it's unique, suppose $X_1 \cup \cdots \cup X_r = Y_1 \cup \cdots \cup Y_s$ are two irreducible decompositions. For each X_i, we have $X_i = \cup_{j=1}^{s} (Y_j \cap X_i)$. Since X_i is irreducible, one of these is all of X_i and thus $X_i \subseteq Y_j$ for some j. But similarly, $Y_j \subseteq X_k$ for some k, so $X_i \subseteq X_k$, producing contradiction. □

We've seen that algebraic sets give rise to ideals in polynomial rings via the I function; how does this look when the algebraic set is irreducible?

Proposition 3.3. *X is irreducible $\iff$ $I(X)$ is prime.*

Proof. Suppose X is reducible, meaning we can write $X = X_1 \cup X_2$. Then $I(X_1), I(X_2) \supsetneq I(X)$ by a question on PSet 1. Let $f_i \in I(X_i) \setminus I(X)$. Then $f_1 f_2 \in I(X)$, so $I(X)$ isn't prime. Now assume $I(X)$ is not prime. Then there exist $f, g \notin I(X)$ with $fg \in I(X)$. So $X \subseteq V(fg) = V(f) \cup V(g)$. But $X \not\subseteq V(f), V(g)$ so $X = (V(f) \cap X) \cup (V(g) \cap X)$. Thus X is reducible. □

We'll soon see that if J is prime then $V(J)$ is irreducible, as long as k is algebraically closed.

Example 3.4. Consider $f = y^2 + x^2(x-1)^2 \in \mathbb{R}[x, y]$. You can check that this polynomial is irreducible, so it's prime. But the zeroes of f are $\{(0,0), (1,0)\}$, which is reducible.

Now we turn to dimension: if $X \subseteq \mathbb{A}^n$ is an algebraic set, we can write $X \supseteq X_d \supsetneq \cdots \supsetneq X_0 \supsetneq \emptyset$. The maximal such d is the *dimension* of X.

Example 3.5. $\dim \mathbb{A}^1 = 1$. It's relatively easy to see that $\dim \mathbb{A}^n \geq n$, but it's pretty hard to show that it exactly equals n (though it does).

Equivalently, the dimension of a ring X equals the maximal length of an increasing chain of prime ideals containing $I(X)$.[1] Now let's look at the irreducible algebraic sets in $\mathbb{A}^2$. I claim that the following are irreducible:

1.) $\emptyset = V(1)$
2.) $\mathbb{A}^2 = V(0)$
3.) $(a, b) = V(x - a, y - b)$
4.) Plane curves of the form $V(f)$ for f irreducible.

To show that these are all the possibilities, it suffices to show the following.

Proposition 3.6. *If $f, g \in k[x, y]$ with no common factors then $V(f, g) = V(f) \cap V(g)$ is finite.*

Definition 3.7. For R an integral domain, the *field of fractions* of R is the set $\{\frac{a}{b} | a, b \in R, b \neq 0\}$ with $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = cb$.

Example 3.8. The field of fractions of $k[x_1, \ldots, x_n]$ is the textitfield of rational functions denote $k(x_1, \ldots, x_n)$.

Another tool which will be good to have our disposal is Gauss's theorem.

Theorem 3.9 (Gauss's theorem)**.** *For R a UFD with field of fractions K, then if f is irreducible in $R[x]$ it's also irreducible in $K[x]$.*

[1] I, like V, is inclusion-reversing.

Back to the previous proposition:

Proposition 3.10. *If $f, g \in k[x,y]$ with no common factors then $V(f,g) = V(f) \cap V(g)$ is finite.*

Proof. If f and g have no common factors in $k[x,y] = k[x][y]$, then by Gauss's theorem they don't have common factors in $k(x)[y]$. Since $k(x)$ is a field, $k(x)[y]$ is a PID. So $(f,g) = (h) \subseteq k(x)[y]$ for some h. Since h divides f and g, we have $(f,g) = 1$ and thus $rf + sg = 1$ for some $r, s \in k(x)[y]$. Clearing denominators, we have $af + bg = d$ in $k[x]$. Egh i missed the rest of the proof. □

4. Nullstellensatz

Last time we talked about classifying the irreducible algebraic sets in $\mathbb{A}^2$. We claimed that the irreducible algebraic sets take the form

1.) $\emptyset = V(1)$
2.) $\mathbb{A}^2 = V(0)$
3.) $(a,b) = V(x-a, y-b)$
4.) Plane curves of the form $V(f)$ for f irreducible.

We showed that these are all the possibilities, so it remains only to show that the plane curves of 4) are indeed irreducible.

Proposition 4.1. *If $f \in k[x,y]$ is irreducible then $I(V(f)) = (f)$, so $V(f)$ is irreducible.*

Proof. We know $(f)I(V(f))$. On the other hand, if $g \in I(V(f))$ then $V(f) \subseteq V(g)$. Since k is algebraically closed, we claim $V(f)$ is infinite. Without loss of generality, f has positive degree in x, so we can write $f = a_d(y)x^d + \cdots + a_1(y)x$. For each of the infinitely many $\alpha \in k$ such that $a_d(y)$ doesn't vanish, $f(x,\alpha)$ is a degree d polynomial so it has at least one root. Since there are infinitely many α for which this is the case, f has infinitely many roots. Since $V(f)$ is infinite and $V(f) \subseteq V(g)$, we have that $V(f,g)$ is infinite. So, by the theorem from last time, f and g have a common factor. Since f is irreducible, f divides g, as desired. □

So we've classified algebraic sets in $\mathbb{A}^2$ - cool. Let's pull back to some of the ideas we were talking about on the first day, in particular the idea of having a dictionary between algebra and geometry. So far we're equipped with the following tool

$$V : \{\text{ideals in } k[x_1, \ldots, x_n]\} \to \{\text{alg. sets in } \mathbb{A}^n_k\}$$

And we've seen that it's

- Inclusion-reversing: $I \subseteq JV(J) \subseteq V(I)$
- Surjective, by definition
- If X is algebraic, then $V(I(X)) = X$, so I is a right inverse to V.
- *Not* injective; for instance $V(x^2) = V(x)$
- $V(I) = V(\sqrt{I})$

It's now relatively natural to ask whether restricting to *radical ideals* turns V into a bijection between ideals and algebraic sets. The answer in general is no, if we allow k not to be algebraically closed.

Example 4.2. V doesn't inject out of radical ideals in $\mathbb{R}[x,y]$. (x^2+y^2) and (x,y) are prime and thus radical, but over $\mathbb{R}$ they have the same zero set.

Nullstellensatz says that as long k as *is* algebraically closed, however, V does restrict to a bijection from radical ideals in the polynomial ring to algebraic sets in affine space.

Theorem 4.3 (Hilbert's Nullstellensatz)**.** *Let k be algebraically closed and $I \subseteq k[x_1,\dots,x_n]$ an ideal. Then $I(V(I)) = \sqrt{I}$. In particular, V is bijective on radical ideals.*

In order to prove this we need some algebra we haven't seen yet as well as the weak Nullstellensatz, which is as follows:

Proposition 4.4 (Weak Nullstellensatz)**.** *If $k = \overline{k}$ and $I \subsetneq k[x_1,\dots,x_n]$ a proper ideal then $V(I) \neq \emptyset$.*

Proof. Pick a maximal ideal $\mathfrak{m} \supset I$. Then $V(\mathfrak{m}) \subseteq V(I)$. We make use of the result that when $k = \overline{k}$, the maximal ideals of $k[x_1,\dots,x_n]$ are exactly those of the form $(x_1 - a_1,\dots,x_n - a_n)$, though we won't prove this until next time. □

Now back to the OG Nullstellensatz.

Proof of original Nullstellensatz. We know $\sqrt{i} \subseteq I(V(I))$. Now let $I = (f_1,\dots,f_r)$ and $g \in I(V(I))$. Letting $R = k[x_1,\dots,x_n]$ and $S = k[x_1,\dots,x_{n+1}]$, we now define $J = (f_1,\dots,f_r, x_{n+1}g - 1) \subseteq S$. Now consider $V(J) \subseteq \mathbb{A}^{n+1}$. If $P \in V(J)$ then $f_i(P) = 0\ \forall i$ so $g(P) = 0$. So $x_{n+1}g - 1$ evaluated at P is not 0. So $V(J) = \emptyset$ and by the weak Nullstellensatz, $J = S$. Then $1 \in J$ and so $\sum a_i f_i + b(x_{n+1}g - 1) = 1$ for some $a_i, b \in S$. Now let N be the highest power of x_{n+1} appearing in the equation (in any term), and set $y = \frac{1}{x_{n+1}}$. Multiplying both sides by y^N and cancelling the x_{n+1}'s yields $\sum \tilde{a}_i f_i + \tilde{b}(g - y) = y^N$ where $\tilde{a}_1,\dots,\tilde{a}_r, \tilde{b} \in k[x_1,\dots,x_n,y]$. Substituting g for y, we get $g^N = F + 0 \in I$, and thus $g \in \mathrm{rad} I$. □

Corollary 4.5. *We can now start filling the dictionary between commutative algebra and algebraic geometry. Let $S = k[x_1,\dots,x_n]$. Then there are the following correspondences*

AG	*CA*
algebraic sets in $\mathbb{A}^n$	*radical ideals in S*
irreducible alg. sets	*prime ideals*
points in $\mathbb{A}^n$	*maximal ideals $(x_1 - a_1,\dots,x_n - a_n)$*
$\emptyset$	$(1) = S$
$\mathbb{A}^n$	(0)
inclusion of alg. sets	*(reverse) inclusion of ideals*
irreducible hypersurfaces	*irreducible polynomials, up to scaling*
algebraic subsets of $V(I)$	*radical ideals containing I (= radical ideals in S/I)*

Corollary 4.6. *For $k = \overline{k}$ and $I \subseteq k[x_1,\dots,x_n] = S$ an ideal, $V(S)$ is finite if and only if S/I is a finite dimensional k-vector space.*

Example 4.7. Let's apply the above corollary

1.) $k[x]$ has k-basis $1, x, x^2, \ldots$ and $V(0) = \mathbb{A}^1$, which is infinite.
2.) $k[x,y]/(x^2, y)$ has basis $1, x$ so dimension 2 and $V(x^2, y) = \{(0,0)\}$ is finite.
3.) $k[x,y]/(y, x(x-1))$ has basis 1,x and $V(y, x(x-1)) = \{(0,0), (1,0)\}$.
4.) $f \in k[x]$ has degree $d > 0$. Then $k[x]/(f)$ has basis $1, x, \ldots, x^{d-1}$.

Note that the dimension $\dim_k(S/I)$ is called the *length* of the corresponding scheme. And even though $V(x^2, y) = V(x, y)$, the two ideals define different schemes.

5. Module-finiteness, Ring-finiteness, and Integrality

I'm going to finish up what we were working on last time, i.e. corollaries to the Nullstellensatz.

Corollary 5.1. *For k algebraically closed and $I \subseteq k[x_1, \ldots, x_n] = S$ an ideal, then $V(I)$ is finite if and only if S/I is a finite-dimensional k-vector space.*

Proof. Assume $\dim_k(S/I) < \infty$ and let $P_1, \ldots, P_r \in V(I)$. Note that we can find $f_1, \ldots, f_r \in S$ such that $f_i(P_j) = \delta_i j$. We'd like to show that the $\overline{f_i}$'s are linearly independent in S/I. Let $\lambda_1, \ldots, \lambda_r \in k$ such that $\sum \lambda_i \overline{f_i} = 0$. Then $\sum \lambda_i f_i \in I$. Since $P_j \in V(I)$, then $\lambda_j = \sum \lambda_i f_i(P_j) = 0$. So all the $_i$ are 0 and the $\overline{f_i}$ are linearly independent. So $r \leq \dim_k(S/I) < \infty$ and $V(I)$ is finite.

Now suppose that $V(I) = \{P_1, \ldots, P_r\}$. For each $j \in \{1, \ldots, n\}$, define $f_j = (x_j - a_{1j}) \ldots (x_j - a_{rj})$ where a_{ij} is the jth coordinate of P_i. Note that $f_j(P_i) = 0$ for all i, j. So $f_j \in I(V(I)) = \sqrt{I}$. Then there exists an $N >> 0$ with $f_j^N \in I$ for all j. Then $\overline{f}_j^N = 0$. So $\overline{x_j}^{Nr}$ equals a k-linear combination of smaller powers of $\overline{x}_j$. Thus we can generate S/I as a vector space using finitely many monomials and $\dim_k(S/I) < \infty$. □

Now onto a bit of an algebra detour - recall that the step in the proof of the weak Nullstellensatz is that when $k = \overline{k}$, the maximal ideals of $k[x_1, \ldots, x_n]$ are exactly those which take the form $(x_1 - a_1, \ldots, x_1 - a_n)$. We'll need some algebra to tackle this.

Definition 5.2. M is a *finitely generated* R-module if there exist $m_1, \ldots, m_n \in M$ with $M = Rm_1 + \cdots + Rm_n$.

Definition 5.3. Suppose S is a ring with $R \subseteq S$ a subring. Then S is an R-module and in this case we'll call it an *R-algebra*.

Definition 5.4. If S is finitely generated as an R-module, then S is *finite over R*, or *module-finite* over R.

Now let $v_1, \ldots, v_n \in S$. We denote the subring generated by $R, v_1, \ldots, v_n$ in S by $R[v_1, \ldots, v_n]$. Roughly, this is the ring of "polynomials" in $v_1, \ldots, v_n$ with coefficients in R.

Definition 5.5. S is *ring-finite* over R, or a *finitely generated R-algebra*, if $S = R[v_1, \ldots, v_n]$ for some $v_1, \ldots, v_n \in S$.

Note that if $S = R[v_1, \ldots, v_n]$ then there's a natural surjection $R[x_1, \ldots, x_n] \twoheadrightarrow S$ with $x_i \mapsto v_i$.

Definition 5.6. $v \in S$ is *integral* over $R(\subseteq S)$ if there's a monic polynomial $f \in R[x]$ with $f(v) = 0$. S is *integral* over R if every $v \in S$ is.

You can check that

1) Module- and ring-finiteness are both transitive. Integrality is also transitive but harder to show - we'll see that on PSet 3
2) Module-finite implies ring-finite.

We'll see that the set of elements of S that are integral over R form a ring, called the *integral closure* of R in S. And if R is an integral domain, its integral closure (without reference to a bigger ring) is its integral closure in its field of fractions.

Example 5.7. Let's consider some examples of integrality:

1) $R[x]$ is ring-finite but not module-finite or integral over R.
2) $R[x]/(x^2) = R + Rx$ is module finite and integral over R.
3) $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2},]$ is not ring finite over $\mathbb{Q}$ (so it's not module-finite) but it is integral.

Next up is a proposition that we'll find really useful moving forward:

Proposition 5.8. *For $R \subseteq S$, S an integral domain, and $v \in S$, the following are equivalent:*

1) v is integral over R
2) $R[v]$ is module-finite over R
3) There's a subring $R' \subseteq S$ containing $R[v]$ that's module-finite over R.

Proof. (1) $\implies$ (2): If v is integral over R, then $v^n + a_1 v^{n-1} + \cdots + a_n = 0$ for appropriately $a_i \in R$. So $v^n \in R + Rv + \cdots + Rv^{n+1}$. So $R[v]$ is module-finite over R. For (2) $\implies$ (3), set $R' = R[v]$. For (3) $\implies$ (1), do some funky linear algebra $\square$

6. Fields, Affine varieties

Today we'll talk mostly about algebra, hoping to return to the geometry in the near future. Last time we talked about the equivalences between integrality of an element v, module-finiteness of the module $R[v]$ it gives rise to, and the existence of an $R' \subseteq S$ containing $R[v]$ that's module-finite over R.

Corollary 6.1. *The set of elements of S that are integral over R is a subring of S, called the integral closure of R in S.*

Proof. If a, b are integral over R then $R[a]$ is module-finite over R and b is integral over $R[a]$. So $R[a, b]$ is module-finite over $R[a]$ and, by transitivity, thus over R. Setting $R' = R[a, b]$, we have that R' is module-finite over R. Setting $v = ab$ or $v = a \pm b$, we have by the proposition that v is integral over R. $\square$

Corollary 6.2. *Suppose S is ring-finite over R. Then S is module-finite over R if and only if it is integral over R.*

Proof. First suppose S is module-finite over R and fix $a \in S$. Then $R[a] \subseteq S$ so a is integral over R and, since a was arbitrary, S is integral over R. Now suppose S is integral over R; we write $S = R[v_1, \ldots, v_n]$. Note that $R[v_1]$ is module-finite over R, and let us assume that $R[v_1, \ldots, v_k]$ is module-finite over R. Then v_{k+1} is integral over $R[v_1, \ldots, v_k]$, so $R[v_1, \ldots, v_{k+1}]$ is module finite over $R[v_1, \ldots, v_k]$ and thus over R. We've completed the inductive argument. □

Now we'll pivot slightly to fields - if $K \subseteq L$ are fields, we write $K(v_1, \ldots, v_n)$ to mean the field of fractions of $K[v_1, \ldots, v_n]$. Equivalently, it's the smallest field in L containing K and $v_1, \ldots, v_n$.

Definition 6.3. L is a *finitely generated* field extension of K if $L = K(v_1, \ldots, v_n)$ for some $v_i \in L$. L is *algebraic* over K if all elements of L are algebraic over K.

Example 6.4. $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}(\sqrt{5})$ is an algebraic extension of $\mathbb{Q}$. In fact, it's module-finite over $\mathbb{Q}$. $\mathbb{Q}(\pi)$, on the other hand, is not algebraic over $\mathbb{Q}$.

Remark 6.5. If $K \subseteq L$ are fields, then the algebraic elements of L over K form a subfield of L.

Proposition 6.6. *$k(x)$ is a finitely-generated field extension, but it's not ring-finite over k.*

Proof. Suppose $k(x) = k[v_1, \ldots, v_n]$. Then there exists $b \in k[x]$ such that $bv_i \in k[x]\ \forall v_i$. Now choose $c \in k[x]$ irreducible that doesn't divide b. We can write $\frac{1}{c}$ as a k-linear combination of monomials in the v_i. Then there exists $N >> 0$ such that $\frac{b^N}{c} \in k[x]$, producing contradiction. □

Proposition 6.7. *$k[x] \subseteq k(x)$ is its own integral closure.*

Proof. Let $z \in k(x)$ be integral over $k[x]$. Then $z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0$ with the $a_i \in k[x]$. We can write $z = \frac{f}{g}$ for $f, g \in k[x]$ relatively prime. Multiplying through by g^n, we get that $f^n + a_{n-1}f^{n-1}g + \cdots + a_0 g^n = 0$. So g divides f^n and $g \in k$. □

Theorem 6.8. *Let $K \subseteq L$ be fields. If L is ring-finite over K, then L is module-finite (and thus algebraic) over K.*

Proof. Eh, zoned out during this proof. □

Theorem 6.9. *If k is algebraically closed and $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ is a maximal ideal then $m = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_i \in k$.*

Proof. Let $L = R/\mathfrak{m}$, and note $k \subseteq L$. L is ring-finite over k, as $L = k[\overline{x}_1, \ldots, \overline{x}_n]$. If $z \in L$ then $f(z) = 0$ for some $f \in k[x]$. But k is algebraically closed, so $z \in k$ and thus $L = k$. □

We're done with the algebra, so let's move back to the algebra.

Definition 6.10. An *affine variety* is an irreducible algebraic set. So affine varieties in $\mathbb{A}^n$ correspond to prime ideals in $k[x_1, \ldots, x_n]$.

What should functions between varieties look like?

Definition 6.11. For $V \subseteq \mathbb{A}^n$ a variety a function $f : V \to k$ is a *polynomial function* or *regular function* on V if there exists $F \in k[x_1, \ldots, x_n]$ with $f = F|_V$.

Definition 6.12. The ring of regular functions on V is called the *coordinate ring* of V, denoted $\Gamma(V)$.

Example 6.13. $\Gamma(\mathbb{A}^n) = k[x_1, \ldots, x_n]$

7. Regular functions

Last time we talked about coordinate rings on algebraic sets, which are functions from the algebraic set to the field which come from restrictions of polynomials from greater affine space.

For instance, for $V = V(y - x^2)$, we have that y and x^2 are the same function on V, so inside $\Gamma(V)$, they're the same. What about $V = V(xy - 1) \subseteq \mathbb{A}^2$. Is $\frac{1}{y}$ regular? Yes, because $xy = 1 \implies x = \frac{1}{y}$. So x and $\frac{1}{y}$ are the same function of V and $\frac{1}{y}$ is indeed regular on V.

In general, if $V \subseteq \mathbb{A}^n$ is an algebraic set, we have a map $k[x_1, \ldots, x_n] \twoheadrightarrow \Gamma(V)$ given by restriction which gives rise to an isomorphism $\Gamma(V) \simeq k[x_1, \ldots, x_n]/I(V)$. This is sometimes given as the definition of the coordinate ring, but that's not a great way to think about it - it conceals what's going on and obstructs you from thinking about $\Gamma(v)$ as a collection of functions, rather than a ring.

Remark 7.1. $\Gamma(V)$ is ring-finite over k. Furthermore, if V is a variety, then $\Gamma(V)$ is an integral domain.

Definition 7.2. A *subvariety* of $V \subseteq \mathbb{A}^n$ is a variety $W \subseteq \mathbb{A}^n$ such that $W \subseteq V$.

So, expanding slightly our dictionary between AG and CA, we have that subvarieties of V correspond to prime ideals in $\Gamma(V)$ – as those are prime ideals containing $I(V)$, by the above definition of the coordinate ring – and points of V correspond to maximal ideals in $\Gamma(v)$.

We have $R \twoheadrightarrow \Gamma(V) \twoheadrightarrow \Gamma(W)$ given by restriction maps. $\overline{f} \in \Gamma(V)$ is in the kernel of the rightmost map iff $\overline{f}$ vanishes on W meaning $\overline{f} \in I_V(W)$. So

$$\begin{aligned}\Gamma(W) &\simeq \Gamma(V)/I_V(W) \\ &\simeq (R/I(V))/(I(W)/I(V))\end{aligned}$$

Definition 7.3. Let $V \subseteq \mathbb{A}^n$, $W \in \mathbb{A}^m$ be algebraic sets. A function $\phi : V \to W$ is a *regular map* if there are $T_1, \ldots, T_m \in k[x_1, \ldots, x_n]$ such that for all $a = (a_1, \ldots, a_n) \in V$, $phi(a) = (T_1(a), T_2(a), \ldots, T_m(a))$.

Note that a regular function f on V determines a regular map $V \to \mathbb{A}^1$.

Definition 7.4. For $\phi : V \to W$, define $\phi^* : \Gamma(W) \to \Gamma(V)$ defined by $\phi^*(g) = g \circ \phi$ to be the *pullback* of ϕ.

Remark 7.5. If $\phi : V \to W$ and $\psi : W \to X$, then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

The identity pulls back to itself (with different domain/codomain), so we've proven that Γ is a contravariant functor from the category of algebraic sets and regular maps to that of finitely-generated, reduced ($\sqrt{(0)} = (0)$) k-algebras.

Example 7.6. If $X \subseteq \mathbb{A}^n$ and $f : X \to \mathbb{A}^n$ is the corresponding inclusion, then $f^*(x_i) = \overline{x_i} \subseteq \Gamma(x)$. So the map is just the quotient.

Proposition 7.7. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be algebraic sets. There's a one-to-one correspondence between regular maps $V \to W$ and k-algebra homomorphisms $\Gamma(W) \to \Gamma(V)$.*

Proof. Sort of tedious. □

So turning a map into its k-algebra homomorphism retains all information, which is a remarkably strong statement.

8. Regular maps

Last time we talked about regular maps - as always, a regular map is an *isomorphism* if it has a two-sided inverse. On the homework we'll see that this is a stronger condition than bijectivity.

Corollary 8.1. *$\phi : V \to W$ is an isomorphism if and only if $\phi^* : \Gamma(W) \to \Gamma(V)$ is an isomorphism.*

Proof. $\phi \circ \psi = \text{id} \iff (\phi \circ \psi)^* = \psi^* \circ \phi^* = \text{id}$, by Proposition 7.7. □

Example 8.2. Consider $\phi : \mathbb{A}^1 \to V(y - x^2) = V$ defined by $t \mapsto (t, t^2)$. Then $\phi : V \to \mathbb{A}^1$ defined by $(x, y) \mapsto x$ is regular and equals the inverse of ϕ, so ϕ is an isomorphism.
An alternative solution would have been to check that $\phi^* : k[x, y]/(y - x^2) \to k[t]$ defined by $x \mapsto t$ and $y \mapsto t^2$ is an isomorphism.

Lemma 8.3. *Let $\phi : V \to W$ be a regular map and $X \subseteq W$ algebraic. Then*

a.) $\phi^{-1}(X)$ is algebraic
b.) If $X \subseteq \phi(V)$ and $\phi^{-1}(X)$ is irreducible, then X is irreducible.

Proof. a.) $X = V(f_1, \ldots, f_r) = V(f_1) \cap \ldots \; capV(f_r)$, so $\phi^{-1}(X) = \cap \phi^{-1}(V(f_i))$ and $\phi^{-1}(V(f_i)) = \{a \in V | f_i(\phi(a)) = 0\}$. So $\phi^{-1}(V(f_i)) = \{a \in V | \phi^*(f_i)(a) = 0\} = V(\phi^*(f_i))$.

b.) Suppose $X = A \cup B$ for A, B algebraic. Then $\phi^{-1}(X) = \phi^{-1}(A) \cup \phi^{-1}(B)$. Without loss of generality, $\phi^{-1}(A) = \phi^{-1}(X)$ and $A = X$.

□

Now we'll talk about injectivity and surjectivity.

Proposition 8.4. *Suppose that V and W are algebraic. If $\psi : V \to W$ is regular and surjective, then ϕ^* is injective.*

Proof. If $f \in \Gamma(W)$ with $\phi^*(f) = 0$, then $V \twoheadrightarrow W \xrightarrow{f} k$ so $f = 0$. □

The converse here doesn't hold, due to the structure of these regular maps - i.e. it is in general not possible for two maps to coincide one all but one arbitrary part of the domain.

Definition 8.5. Lete $\phi : V \to W$ be regular. ϕ is *dominant* if $\overline{\phi(V)} = W$. Equivalently, $I(\phi(V)) = I(W)$.

Proposition 8.6. *$\phi : V \to W$ is regular if and only if ϕ^* is injective.*

Proof. Suppose ϕ^* is injective, and let $f \in I(\phi(V))$. If $\phi^*(f) = 0$ then $f \in I(W)$ (or $\overline{f} = 0$). Now assume ϕ is dominant and $\overline{f} \in \Gamma(W)$. If $\phi^*(\overline{f}) = 0$. then $f \in I(\phi(V)) = I(W)$ and thus $\overline{f} = 0$. □

Proposition 8.7. *$\Phi^* : \Gamma(W) \to \Gamma(V)$ is surjective if and only if ϕ is an isomorphism onto its image.*

Proof. Omitted. □

Now we'll talk about rational functions, which resemble meromorphic functions from complex analysis (while elements of the coordinate ring resembles holomorphic functions).

Definition 8.8. Let $\emptyset \neq V \subseteq \mathbb{A}^n$ be a variety, with $\Gamma(V)$ an integral domain. The *field of rational functions* on V, denoted $k(V)$ is the field of fractions of $\Gamma(V)$,

Example 8.9. In $V(xy - z^2) \subseteq \mathbb{A}^3$, $\frac{x}{z}$ is the same rational function as $\frac{z}{y}$.

Definition 8.10. A rational function $f \in k(V)$ is *defined* or *regular* at $p \in V$ if $\exists g, h \in \Gamma(V)$ such that $f = \frac{g}{h}$ and $h(p) \neq 0$.

In the above case, $f = \frac{x}{z} = \frac{z}{y}$ is defined if $z \neq 0$ or $y \neq 0$.

Definition 8.11. Let $f \in k(V)$ and $p \in V$. Then p is a *pole* of f if f is not defined at p.

Definition 8.12. The set of poles of a rational function is an algebraic subset of V.

Proof. Suppose $V \subseteq \mathbb{A}^n$ and $f \in k(V)$. Now let $J_f = \{g \in \Gamma(V) | gf \in \Gamma(V)\}$. J_f is an ideal, and we'd like to show that $V(J_f) =$ pole set of f. And p is not a pole of f iff there exist $a, b \in \Gamma(V)$ with $\frac{a}{b} = f$ and $b(p) \neq 0$. And that holds iff there exist $b \in J_f$ with $b(p) \neq 0$. And that occurs exactly when $p \notin V(J_f)$, so we're done. □

9. Local rings

Today we'll talk a bit about local rings at points.

Definition 9.1. Let $p \in V$ for V a variety. Then $\mathcal{O}_p(V) \subseteq k(V)$ is the set of rational functions on V that are defined at p, called the *local ring* of V.

Recall that $k(V)$ is the field of fractions of $\Gamma(V)$. Note $k(p) = k$, and that in general this won't equal $\mathcal{O})p(V)$ (a function out of V isn't determined by what it does at p).

Proposition 9.2. *$\mathcal{O}_p(V)$ is a subring of $k(V)$.*

Proof. $\frac{a}{b}, \frac{c}{d} \in \mathcal{O}_p(V)$ such that $b(P), d(P) \neq 0$. Then $b(P)d(P) \neq 0$. So products and differences are in $\mathcal{O}_P(V)$. □

Proposition 9.3. *$\Gamma(V) = \cap_{p \in V} \mathcal{O}_p(V)$ for V a variety.*

Proof. We know $\subseteq$ (via $f \mapsto \frac{f}{1}$). Now note that if $f \in \cap \mathcal{O}_p(V)$, then f has no poles. So if $J_f = \{g \in \Gamma(V) | gf \in \Gamma(V)\}$, then $V(J_f) =$ set of poles $= \emptyset$. So $1 \in J_f$, by Weak Nullstellensatz, and $f \in \Gamma(V)$. □

If $f \in \mathcal{O}_p(V)$, then we can evaluate at p in a way which is well-defined. This gives rise to a homomorphism $\mathcal{O}_p(V) \to k$ defined by $f \mapsto f(p)$. And $k \subseteq \mathcal{O}_p(V)$ maps to itself, so evaluation is a surjection. The kernel of this map is then maximal, and it's called the *maximal ideal of V at p*. It's defined $\mathfrak{m}_p(V) = \{\text{non-units of } \mathcal{O}_p(V)\} = \{\frac{g}{1} | g \in I_V(p)\}$.

Definition 9.4. A ring R is a *local ring* if it satisfies the following equivalent conditions:

1) The set of non-units in R is an ideal.
2) R has a unique maximal ideal

Example 9.5. $\mathbb{C}[x]$ isn't a local ring. $x + 1$ and x are both non-units, so non-units don't form an ideal.

Example 9.6. $R = \{\frac{a}{b} \in k(x) | a, b \in k[x], \text{b has nonzero constant term}\}$ is a local ring with maximal ideal $(\frac{x}{1})$. In fact, $R = \mathcal{O}_0(\mathbb{A}^1)$.

Proposition 9.7. *$\mathcal{O}_p(V)$ is Noetherian.*

Proof. Let $I \subseteq \mathcal{O}_p(V)$. Consider $J = I \cap \Gamma(V)$, whic is an ideal of $\Gamma(V)$. $\Gamma(V)$ is Noetheerian, so $J = (f_1, \ldots, f_r) \subseteq \Gamma(V)$. Now let $f \in I \subseteq \mathcal{O})p(V)$. We have $f = \frac{a}{b}$ for $a, b \in \Gamma(V), b(p) \neq 0$. So $bf = a \in I \cap \Gamma(V) = J$. So $bf = a_1 f_1 + \cdots + a_r f_r$ for appropriate $a_i \in \Gamma(V)$. Then $f = (\frac{a_1}{b}) f_1 + \cdots + (\frac{a_r}{b}) f_r$. So $I(\frac{f_1}{1}, \ldots, \frac{f_r}{1})$. □

Let $\phi : V \to W$ be a regular map of varities, and consider $\phi^* : \Gamma(W) \to \Gamma(V)$. Can we extend ϕ^* to $k(W)$? If so, there's only one possible map: $\frac{g}{h} \mapsto \frac{\phi^*(g)}{\phi^*(h)}$. But if $h \in \ker(\phi^*)$, this doesn't work.

Instead, let $p \in V$ and set $Q = \phi(p)$. Let $h \in \Gamma(W)$ such that $h(Q) \neq 0$. Then $V \to W \xrightarrow{h} k$ defined by $P \mapsto Q \mapsto h(Q) \neq 0$ is $\phi^*(h)$. So if $\frac{g}{h}$ is defined at Q, with $h(Q) = 0$, this process works. This gives rise to a well-defined map, so ϕ^* induces a morphism $\mathcal{O}_Q(W) \to \mathcal{O}_P(V)$. If $\frac{g}{h} \in \mathfrak{m}_Q(W)$, then $g(Q) = 0$. Thus $\phi^*(\frac{g}{h}) \in \mathfrak{m}_P(V)$. So $\mathfrak{m}_Q(W)$ gets mapped into $\mathfrak{m}_P(V)$.

For the rest of the class, we'll talk about affine plane curves. In fact, we'll spend the next couple weeks using the theoretical tools we've developed to study plane curves. Recall that an irreducible affine plane curve $C \subseteq \mathbb{A}^2$ corresponds to an ideal $(f) \subseteq k[x,y]$ for f irreducible. However, we also want to consider reducible plane curves with multiple component. If $f, g \in k[x,y]$ and $(f) = (g)$, then $f = \lambda g$ for nonzero $\lambda \in k$.

Definition 9.8. An *affine plane curve* is an equivalence class of non-constant polynomials in $k[x,y]$ with $f \sim g \iff f = \lambda g$ ($\lambda \neq 0$).

Note that $V(x) = V(x^2)$ but $x \not\sim x^2$. If $f = \prod f_i^{e_i}$ for the f_i irreducible. The f_i are the *components* of f and the e_i are their *multiplicities*.

Definition 9.9. p is a *simple point* or *smooth point* if $f_x(p) \neq 0$ pr $f_y(p) \neq 0$. In this case the tangent line is $f_x(p)(x-a) + f_y(p)(y-b) = 0$. A point that's not simple is *multiple or singular.*

10. Homogeneous polynomials, multiplicities

Today we'll spend more time talking about affine place curves, which you'll recall is a non-constant polynomial up to scaling.

Definition 10.1. For f a plane curve and $p \in f$, P is a smooth point if $f_x(P) \neq 0$ or $f_y(P) \neq 0$.

Here $f_z = \frac{\partial}{\partial z} f$.

Example 10.2. Let $f = y^2 - x^3 + x$, over $\mathbb{C}$. Then $f_x = 1 - 3x^2$ and $f_y = 2y$ are singular at $(\pm\frac{\sqrt{3}}{3}, 0)$. But they're not in $V(f)$, so f is nonsingular.

Example 10.3. Consider the cusp $g = y^2 - x^3$. Then $g_x = -3x^2$ and $g_y = 2y$, meaning g is singular at $(0,0)$.

Example 10.4. Take $h = (x^2+y^2)^2 + 3x^2y - y^3$. We have $h_x = 2x(2x^2 + 2y^2 + 3y)$ and $h_y = 4y(x^2+y^2) + 3(x^2 - y^2)$. It turns out that these are both 0 if and only if $x, y = 0$.

Definition 10.5. $F \in k[x_1, \ldots, x_n]$ is *homogeneous* or a *form* of degree d if it can be written as the sum of monomials of degree d.

As an edge case, we consider 0 to be a form of degree d for all d. We can *dehomogenize* F, with respect to x_n, by setting $f = F(x_1, \ldots, x_{n-1}, 1) \in k[x_1, \ldots, x_{n-1}]$. This is the the same as taking the image of F in $k[x_1, \ldots, x_n]/(x_n - 1) \simeq k[x_1, \ldots, x_{n-1}]$.

If $f \in k[x_1, \ldots, x_n]$ is a polynomial of degree d, we can write $f = f_0 + \cdots + f_d$ with f_i a (possible 0) form of degree i and $f_d \neq 0$.

Definition 10.6. The *homogenization* of f is defined $F = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \cdots + f_d \in k[x_1, \ldots, x_{n+1}]$

Example 10.7. Let $F = x^2z + y^2z + xz^2 + z^3$. Dehomogenizing with respect to z gives $x^2 + y^2 + x + 1$. Homogenizing then gives $x^2 + y^2 + xz + z^2 \neq F$. So these are not in general inverses.

Note that homogenization commutes with multiplication but not addition.

Proposition 10.8. *If $F \in k[x, y]$ is homogeneous and k algebraically closed, then F factors into a product of linear forms.*

Proof. $F = y^r G$ for $r \geq 0$ such that y doesn't divide g. The dehomogenization of G is $\alpha_i(x - \lambda_i)$ for $\alpha, \lambda_i \in k$. So $G = \alpha \prod_i (x - \lambda_i y)$ and $F = \alpha y_i^2 (x - \lambda_i y)$. □

Let f be a place curve and $p = (0, 0)$. Write $f = f_m + f_{m+1} + \cdots + f_{m+n}$ where f_i is a form of degree i and $f_m \neq 0$.

Definition 10.9. The *initial form* of f at $p = (0, 0)$ is $\text{in}(f) = f_m$. The *multiplicity* of f at p is $m_p(f) = \deg(\text{in}(f)) = m$.

Note that $(0, 0) \in V(f)$ if and only if $m_{(0,0)}(f) > 0$.

Proposition 10.10. *$p = (0, 0)$ is a simple point of f if and only if $m_p(f) = 1$.*

Proof. For $i \geq 0$, $(f_i)_x$ and $(f_i)_y$ are 0 or forms of degree $i - 1$. So $f_x(P) = (f_1)_x(p) + 0$ and $f_y(P) = (f_1)_y(p) + 0$. If $f_1 = ax + by$, then $f_x(p) = f_y(p) = 0$ if and only if $a = b = 0$. That occurs exactly when $f_1 = 0$. □

It's easy to check in this case – when $m_p(f) = 1$ – that f_1 is the tangent line to f at P. Now set $m = m_p(f)$. We can write $f_m = \prod L_i^{r_i}$, where r_i is the multiplicity of the tangent line and the L_i are distinct lines.

Definition 10.11. The L_i are *tangent lines* to f at $P = (0, 0)$. f_m is called the *tangent cone* to f at the origin. If f has $m = m_p(f)$ distinct tangeent lines at p, then p is an *ordinary* point of f.

An ordinary double point, i.e. point of multiplicity 2, is a *node*. Note that $\text{in}(gh) = \text{in}(g)\text{in}(h)$.

Now let $P = (a, b)$ and $T = \mathbb{A}^2 \to \mathbb{A}^2$ defined $T(x, y) = (x + a, y + b)$. We define $m_p(f) = m_{(0,0)}(T^*(f))$. If $L_i = \alpha x + \beta y$ is a tangent line to $T^*(f)$ at $(0, 0)$ with multiplicity e_i, then $\alpha(x - a) + \beta(y - b)$ is a *tangent line* to f at P.

11. DVRs

if it satisfies the following equivalent properties

1. R is Noetherian and local with principal maximal ideal
2. $\exists$ an irreducible $t \in R$ such that every nonzero $z \in R$ can be written uniquely as $z = ut^n$ for $n \geq 0$ and u a unit.

Proof. Suppose the first condition and, say $\mathfrak{m} = (t)$. Now suppose $ut^n = vt^m$ for u, v units and $n \geq m$. Then $v = ut^{n-m}$. Since t^{n-m} is a unit, then $n = m$ and $u = v$. Alternatively, let $z \in R$ be nonzero and z be a unit. Now let $z \in R$ be nonzero. If it's a unit, then $z = zt^0$. Otherwise, $z \in (t)$ and $z = z_1 t$. If z_1 is a unit, we're done. Otherwise, $z_1 = z_2 t$. If this process stops, we're done. If it doesn't, we get a chain of ideals $(z_1) \subseteq (z_2) \subseteq \dots$. Since R is Noetherian, $(z_n) = (z_{n+1})$ for some n and thus $z_{n+1} = vz_n$. That means $z_n(1 - vt) = 0$ so $vt = 1$, producing contradiction.

Now suppose we satisfy 2. $\mathfrak{m} = (t)$ consists exactly of non-units, so R is local. To see R is Noetherian, suppose $I \subseteq R$. Let $n \geq 0$ be the minimal integer such that $t^n \in I$. So $(t^n) \subseteq I$. If $z \in I$, then $z = ut^m$ and $t^m \in I$ with $m \geq n$. So $z \in (t^n)$ and $I = (t^n)$. □

for R. It's unique up to multiplication by a unit.

Remark 11.1. If R is a DVR with uniformizing parameter t, the nonzero ideals are of the form $(1) \supseteq (t) \supseteq (t^2) \supseteq \dots$

Example 11.2. Let $a \in \mathbb{A}^1$. Then $\mathcal{O}_a(\mathbb{A}^1) = \{\frac{f}{g} | \frac{f}{g} \in k(\mathbb{A}^1), g(a) \neq 0\}$. The maximal ideal consists of non-units, i.e. is the ideal $(x - a)$. So $\mathcal{O}_a(\mathbb{A}^1)$ is a DVR with uniform parameters $x - a$.

Example 11.3. The non-units in $\mathcal{O}_{(0,0)}(\mathbb{A}^2)$ are of the form $\frac{f}{g}$ with $f(0,0) = 0$. Then $\mathfrak{m}_{(0,0)} = (x, y)$ is not principal, so this isn't a DVR. In particular, we've shown that DVRs are PIDs.

Let R be a DVR, and fix a uniformizing parameter t. Let K be the field of fractions of R. If $\frac{f}{g} \in K$, then $f = ut^n$ and $g = vt^m$, so $\frac{f}{g} = (\frac{u}{v})t^{n-m}$. In fact, every non-zero $z \in K$ has a unique expression as ut^n for $u \in R$ a unit.

of z, denoted $\text{ord}(z)$. We define $\text{ord}(0) = -\infty$. You can check that order is independent of the choice of uniformizing parameter.

So $R = \{z \in K | \text{ord}(z) \geq 0\}$ and $\mathfrak{m} = \{z \in K | \text{ord}(z) \geq 1\}$. As an exercise, you can show that $\text{ord}(ab) = \text{ord}(a) + \text{ord}(b)$ and that $\text{ord}(a + b) \geq \min\{\text{ord}(a), \text{ord}(b)\}$.

Example 11.4. Set $R = \mathcal{O}_0(\mathbb{A}^1)$ with $\mathfrak{m} = (x)$, and let $M = (x^n)/(x^{n+1}) \subseteq R/(x^{n+1})$. This is a k-vector space, since $k \subseteq R$. And every $z \in M$ can be written $z = \frac{x^n}{f(x)}$ with $f(0) \neq 0$. Note that $f(x)x^n = f(0)x^n$ in M, since higher powers of x are 0. So $z = \frac{x^n}{f(x)} = \frac{x^n}{f(0)} = \frac{1}{f(0)}x^n$. So M is a 1-dimensional k-vector space.

More generally, let R be a DVR containing a field k such that the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism. Now let $t \in R$ be a uniformizing parameter. Now consider $z \in \mathfrak{m}^n$. $z = ut^n$ for u a unit, so the image of u in $R/\mathfrak{m}$ is nonzero.