MLBAKER.ORG PRESENTS

PMATH 764

Introduction to Algebraic Geometry

Dr. Ruxandra Moraru • Spring 2013 (1135) • University of Waterloo

Disclaimer: These notes are provided *as-is*, and may be incomplete or contain errors.

Contents

Administrative

- Email: `moraru@uwaterloo.ca`.
- Office: MC 5170.
- Course webpage: `https://learn.uwaterloo.ca`.
- Prerequisites: PMATH 345 or equivalent (you have some background in polynomials, rings, and a bit of field theory).
- Away at conference May 30 – June 6, so 3 lectures will be missed: May 31, June 3, and June 5. Makeup lectures 4:30 – 5:20 on the following Fridays: May 24, July 5, July 19.
- Vladimir Voevodsky is giving a talk at the Symbolic Logic Meeting on Wednesday, May 8, 10:20 – 11:10. QNC 1501.

Introduction

We are concerned with solving systems of polynomial equations in several variables:

$$p_1(x_1, \ldots, x_m) = 0$$
$$\vdots$$
$$p_n(x_1, \ldots, x_m) = 0.$$

We study the properties of the set of solutions. "Algebraic geometry" means we are only considering zero sets of polynomials. If you're just doing complex geometry, you may allow yourself to have systems with transcendental functions. However, because we want to stay in this particular realm of objects, all the maps or equivalences we construct will be using only polynomials or rational functions. In differential geometry, you might allow smooth functions. When describing these objects, you allow yourself in differential geometry to use smooth functions as opposed to just polynomial or rational functions.

We will first describe algebraic varieties (zero sets of polynomials) and focus, particularly, on plane curves. A plane curve is just sitting inside affine 2-space, described by a polynomial in two variables. Geometric properties: tangent lines, intersection of these curves, etc. but we will do everything algebraically.

After this we will look at projective space and projective varieties: gives us a way of compactifying the objects we're working with. Because projective space is compact (over $\mathbb{C}$, at least), we'll be able to make much stronger statements when it comes to intersection theory in particular. We'll be looking at projective curves. An important theorem is Bézout's theorem: if you have two curves in the projective plane that are given by two polynomial equations, then these two curves will intersect in a finite number of points which is the product of the degrees of the polynomials.

Towards the end of the course we'll look at divisors and Jacobians of curves (in particular of elliptic curves) and we'll be using these divisors to describe the group law on the cubic, which is a very important tool even in cryptography. That's more or less the outline of the topics.

1 Affine algebraic sets

1.1 Affine space and algebraic sets

Let k be a field (not necessarily algebraically closed).

1.1 Definition. We define

$$\mathbb{A}^n(k) = \mathbb{A}^n = \{(a_1, \ldots, a_n) : a_i \in k \text{ for all } i = 1, \ldots, n\} = \text{affine } n\text{-space}.$$

For example $\mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$, etc. $\mathbb{A}^1(k)$ is called the **affine line**, and $\mathbb{A}^2(k)$ is called the **affine plane**.

1.2 Definition. $k[x_1, \ldots, x_n]$ is the **polynomial ring** in n variables over k. If $f \in k[x_1, \ldots, x_n]$ then we set

$$V(f) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n(k) : f(a_1, \ldots, a_n) = 0\}$$

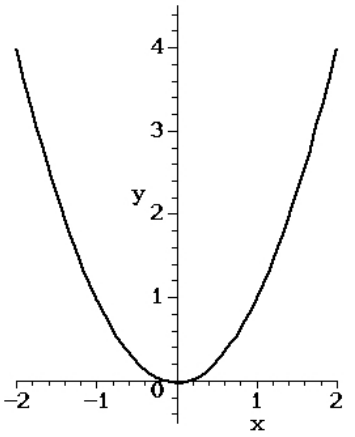
which is called the **set of zeros** of f. We will call the set of zeros of a single non-constant polynomial a **hypersurface**.

1.3 Example. We have:

1. In $\mathbb{R}$, we have
$$V((x-2)(x+5)) = \{2, -5\}.$$
More generally, if $f \in \mathbb{R}[x]$, then
$$V(f) = \{\text{set of roots of } f\}.$$
Note that $V(f)$ may be empty. For example, $V(x^2+1) = \varnothing$ in $\mathbb{R}$, even though $V(x^2+1) = \{\pm i\}$ in $\mathbb{C}$.

2. In $\mathbb{Z}_p$ for p a prime[1] then by Fermat's Little Theorem,
$$V(x^p - x) = \mathbb{Z}_p.$$

3. A hypersurface in $\mathbb{A}^2$ is called an **affine plane curve**. For example, in $\mathbb{R}^2$, $V(y - x^2)$ is a parabola:



On the other hand, in $\mathbb{Q}^2$, $V(x^2+y^2-1)$ is the set of rational points on the unit circle $x^2+y^2=1$ in $\mathbb{R}^2$. This is an infinite set because the unit circle admits a rational parametrisation:
$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$
coming from stereographic projection (whenever $t \in \mathbb{Z}$ we get a rational point on the circle).

The circle is an example of a *rational curve* (i.e. curves that can be "parametrised by rational functions").

4. A hypersurface in $\mathbb{A}^3$ is called an **affine surface**. For example, in $\mathbb{R}^3$,
$$V(xyz) = V(x) \cup V(y) \cup V(z) = \text{union of the coordinate planes in } \mathbb{R}^3.$$

1.4 Definition. More generally, for any $S \subseteq k[x_1, \ldots, x_n]$, we define

$$V(S) := \{p \in \mathbb{A}^n : f(p) = 0 \text{ for all } f \in S\} = \bigcap_{f \in S} V(f).$$

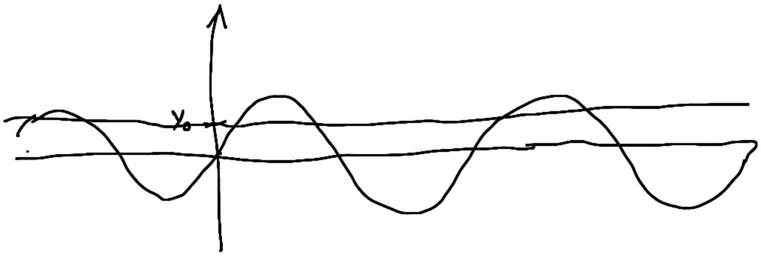
If $S = \{f_1, \ldots, f_m\}$ is a finite set of polynomials, we write $V(f_1, \ldots, f_m)$ rather than $V(\{f_1, \ldots, f_m\})$.

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

1.6 Example. We have:

[1] Of course by $\mathbb{Z}_p$ we mean $\mathbb{Z}/p\mathbb{Z}$, *not* some lame inverse limit you may be thinking of...

1. $\mathbb{A}^n = V(0)$ is an algebraic set. Also, $\varnothing = V(1)$ is an algebraic set.
2. In $\mathbb{R}^2$, $V(y - x^2, x - y + 2) = V(y - x^2) \cap V(x - y + 2) = \{(-1, 1), (2, 4)\}$. [DIAGRAM OF TWO GRAPHS].
3. In $\mathbb{A}^n$, if $(a_1, \ldots, a_n) \in \mathbb{A}^n$,
$$\{(a_1, \ldots, a_n)\} = V(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$$
so any point in $\mathbb{A}^n$ is an algebraic set.
4. Not all subsets of $\mathbb{A}^n$ are algebraic. Indeed consider
$$C := \{(x, y) : y = \sin x\} \subseteq \mathbb{R}^2.$$
Then C is not algebraic.



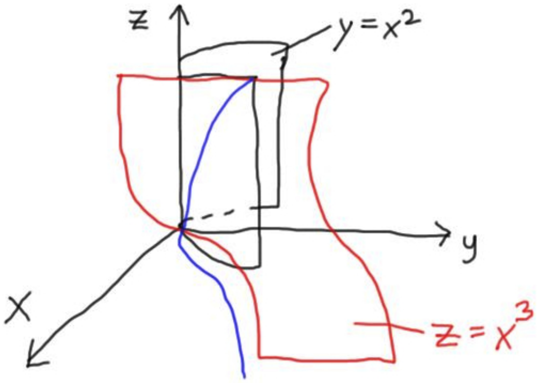
Suppose instead that C is algebraic, so that $C = V(S)$ for some $S \subseteq k[x, y]$. Since $C \subsetneq \mathbb{R}^2 = V(0)$ there must exist at least one $0 \neq f_0 \in S$. Also,
$$C = V(S) = \bigcap_{f \in S} V(f) \subseteq V(f_0).$$
Moreover since $\mathbb{R}$ is infinite, there exists a y_0 $(-1 < y_0 < 1)$ such that $f_0(x_0, y_0) \neq 0$ for some x_0. Otherwise, we would have $f_0 \equiv 0$. Set $g(x) = f_0(x, y_0) \in \mathbb{R}[x]$. Thus $V(g)$ is at most a finite set of points. Also,
$$\underbrace{C \cap V(y - y_0)}_{\substack{\text{intersection of } y = \sin x \\ \text{with } y = y_0}} \subseteq V(g)$$
which is at most a finite set of points.

Course webpage: `http://www.math.uwaterloo.ca/~moraru`

1.7 Exercise. In general, suppose that C is an affine plane curve and L is a line (i.e. the zero set of a degree 1 polynomial in $k[x, y]$), then $L \cap C$ is a finite set of points, or $L \subseteq C$. More generally, any algebraic set in $\mathbb{A}^n$ intersects a line, which it does not contain, in a finite set of points.

However, note that in $\mathbb{A}^n$, for $n \geq 2$, algebraic sets may intersect in an infinite number of points.

1.8 Example. Is the twisted cubic
$$T := \{(t, t^2, t^3) : t \in \mathbb{R}\} \subseteq \mathbb{R}^3$$
algebraic?



Yes. Here $(x, y, z) = (t, t^2, t^3)$ means $y = x^2$ and $z = x^3$ so that $T = V(y - x^2, z - x^3)$, the intersection of the surfaces $y = x^2$ and $z = x^3$.

1.9 Example (THE CLASSIFICATION OF ALGEBRAIC SETS IN $\mathbb{A}^1(k)$). The algebraic sets in $\mathbb{A}^1$ are $\mathbb{A}^1$, $\varnothing$, and finite sets of points.

Proof. $\mathbb{A}^1 = V(0)$, $\varnothing = V(1)$, and for a finite set of points $\{b_1, \ldots, b_m\}$,

$$\{b_1, \ldots, b_m\} = V((x - b_1)(x - b_2) \cdots (x - b_m)).$$

So these are all algebraic. Conversely, suppose that $X \subseteq \mathbb{A}^1$ is algebraic. Then $X = V(S)$ for some $S \subseteq k[x]$. If $S = \varnothing$ or $\{0\}$, then $V(S) = \mathbb{A}^1$. Let us then assume that S has at least one polynomial $f \not\equiv 0$. Then

$$X = V(S) \subseteq V(f) = \{\text{finite \# of roots}\}$$

since $f \in k[x]$. So $X \subseteq \{b_1, \ldots, b_m\}$ where b_i are the roots of f. So X is a finite set of points. □

1.10 Proposition. We have:

1. If $S \subseteq T \subseteq k[x_1, \ldots, x_n]$ then $V(T) \subseteq V(S)$.
2. If $I = \langle S \rangle$ (the ideal generated by S), then $V(S) = V(I)$. That is, *every algebraic set is the zero set of an ideal.*

Proof. We have:

1. Let $p \in V(T)$. Then by definition, $f(p) = 0$ for every $f \in T \supseteq S$, so $f(p) = 0$ for every $f \in S$. So $p \in V(S)$.
2. Since $S \subseteq \langle S \rangle = I$, we have $V(I) \subseteq V(S)$. Conversely, let $p \in V(S)$. Then, if $g \in I = \langle S \rangle$, then $g = a_1 f_1 + \ldots + a_m f_m$ with $a_i \in k[x_1, \ldots, x_n]$ and $f_i \in S$. Thus,

$$g(p) = \sum_{i=1}^{m} a_i \underbrace{f_i(p)}_{=0} = 0.$$

So $p \in V(I)$ hence $V(S) \subseteq V(I)$. □

1.11 Definition. A commutative ring R is called **Noetherian** if every ideal of R is finitely generated.

In particular we have the following.

1.12 Theorem (HILBERT BASIS THEOREM). If R is Noetherian, then $R[x_1, \ldots, x_n]$ is Noetherian.

1.13 Corollary. $k[x_1, \ldots, x_n]$ is Noetherian.

Proof. k is a field, so it is trivially Noetherian. □

1.14 Corollary. Any algebraic set in $\mathbb{A}^n$ is the zero set of a finite set of polynomials.

Proof. Let $X \subseteq \mathbb{A}^n$ be algebraic. Then, $X = V(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$. So $X = V(\langle S \rangle)$. But $\langle S \rangle = \langle g_1, \ldots, g_m \rangle$ for some $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$. So $X = V(g_1, \ldots, g_m)$. □

1.15 Remark. This implies, in particular, that any algebraic set is the intersection of a finite number of hypersurfaces: if $X = V(g_1, \ldots, g_m)$, then

$$X = \bigcap_{i=1}^{m} V(g_i)$$

with each $V(g_i)$ a hypersurface (codimension 1).

1.16 Proposition (PROPERTIES OF ALGEBRAIC SETS). We have:

1. If $\{I_\alpha\}$ is any collection of ideals in $k[x_1, \ldots, x_n]$, then

$$V\left(\bigcup_{\alpha} I_\alpha\right) = \bigcap_{\alpha} V(I_\alpha)$$

so the intersection of any collection of algebraic sets is algebraic.

2. $V(fg) = V(f) \cup V(g)$, for any $f, g \in k[x_1, \ldots, x_n]$. More generally, if I, J are ideals in $k[x_1, \ldots, x_n]$ then

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

where $IJ := \langle \{fg : f \in I \text{ and } g \in J\} \rangle = \{\sum f_i g_i : f_i \in I, g_i \in J\}$. So a finite union of algebraic sets is algebraic.

3. $\varnothing$ and $\mathbb{A}^n$ are algebraic.

Proof. Exercise. □

1.17 Remark. We have:

1. Properties 1 to 3 tell us that the algebraic sets are the closed sets of a topology called the **Zariski topology**. This topology is not Hausdorff.
2. It is important that in property 2 we only have a finite union of algebraic sets. For example consider $\mathbb{Z} \subseteq \mathbb{R}$. This is not algebraic, but $\mathbb{Z}$ is an infinite (countable) union of its points.
3. If k is finite, then all subsets of $\mathbb{A}^n(k)$ are algebraic since they are finite unions of points, which are algebraic.

1.18 Definition. We define the **Zariski topology** on $\mathbb{A}^n$ by taking the open subsets to be the complements of algebraic sets. This is a topology by properties (1) to (3) above.

Moreover, any algebraic set $X \subseteq \mathbb{A}^n$ can be endowed with the **induced topology** whose open subsets are of the form $X \cap U$, where U is open in $\mathbb{A}^n$.

1.19 Example (Zariski topology on $\mathbb{A}^1(k)$ for k infinite). We have seen that the algebraic sets in $\mathbb{A}^1$ are $\varnothing, \mathbb{A}^1$ and finite sets $\{b_1, \ldots, b_m\}$. So the open sets in the Zariski topology are therefore $\mathbb{A}^1$, $\varnothing$, $\mathbb{A}^1 - \{b_1, \ldots, b_m\}$.

Note that the open sets are quite "big" and so the topology is not Hausdorff.

1.20 Definition. A topology is **Hausdorff** if, given any 2 points p and q, there exist open sets U_p and U_q such that $p \in U_p$, $q \in U_q$, and $U_p \cap U_q = \varnothing$ (i.e. the topology **separates points**).

Note that any metric topology (for example that on $\mathbb{R}$) obviously separates points.

However, in the Zariski topology, any open set U_p containing p looks like $U_p = \mathbb{A}^1 - \{p_1, \ldots, p_m\}$ with $p_i \neq p$, and any open set U_q containing q is of the form $U_q = \mathbb{A}^1 - \{q_1, \ldots, q_t\}$ with $q_j \neq q$ so that $U_p \cap U_q \neq \varnothing$.

In $\mathbb{R}^2$, $U = \mathbb{R}^2 - V(y - x^2)$ is open: [diagram of parabola].

One can show that the Zariski topology is not Hausdorff for all $\mathbb{A}^n(k)$ if k is infinite.

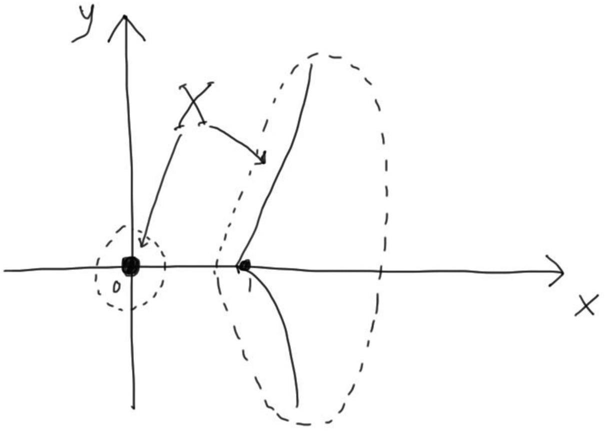
1.21 Remark (connectedness). A subset X of a topological space Y is called **connected** if it cannot be expressed as the disjoint union of two relatively open subsets in X.

A subset of $\mathbb{R}^n$ or $\mathbb{C}^n$ that is connected in the Zariski topology may not be connected in the metric topology.

1.22 Example. Note that

$$X = V(y^2 - \underbrace{x^2(x-1)}_{\geq 0 \text{ only if } x \geq 1}) \subseteq \mathbb{R}^2$$

is not connected in the metric topology, but connected in the Zariski topology.



1.2 Ideals

Recall that to any ideal I of $k[x_1, \ldots, x_n]$ we can associate an algebraic set $X = V(I)$. Conversely, given any set $X \subseteq \mathbb{A}^n$, we can define the following ideal.

1.23 Definition. For $X \subseteq \mathbb{A}^n$,

$$I(X) := \{f \in k[x_1, \ldots, x_n] : f(p) = 0 \text{ for all } p \in X\}$$

is called the **ideal of** X.

1.24 Example. We have:

1. In $\mathbb{A}^1$,
   - $I(\varnothing) = k[x]$.
   - $I(\{b_1, \ldots, b_m\}) = \langle (x - b_1) \cdots (x - b_m) \rangle$.
   - $I(\mathbb{A}^1) = \begin{cases} \langle 0 \rangle & \text{if } k \text{ is infinite} \\ \langle x^{p^n} - x \rangle & \text{if } k \text{ has } p^n \text{ elements with } p \text{ prime.} \end{cases}$

2. In $\mathbb{A}^2$,

   $$I(\{(a, b)\}) = \langle x - a, y - b \rangle.$$

   Indeed, $k[x, y]/\langle x - a, y - b \rangle \cong k$, which is a field. Thus $\langle x - a, y - b \rangle$ is maximal in $k[x, y]$. This forces $I(\{(a, b)\}) = \langle x - a, y - b \rangle$ because $I(\{(a, b)\}) \neq k[x, y]$ since $1 \notin I(\{(a, b)\})$.

   Alternatively, just pick anything in $I(\{(a, b)\})$. Because it must vanish at the point (a, b), it's not hard to show that it must be a combination of $x - a$ and $y - b$.

1.25 Proposition (Properties). We have:

1. If $X \subseteq Y \subseteq \mathbb{A}^n$, then $I(Y) \subseteq I(X)$.
2. If $S \subseteq k[x_1, \ldots, x_n]$, then $S \subseteq I(V(S))$ (or if I is an ideal in $k[x_1, \ldots, x_n]$, then $I \subseteq I(V(I))$).

   If $X \subseteq \mathbb{A}^n$, then $X \subseteq V(I(X))$. But one doesn't always have equality.
3. $V(I(V(S))) = V(S)$ for any $S \subseteq k[x_1, \ldots, x_n]$, and $I(V(I(X))) = I(X)$ for any $X \subseteq \mathbb{A}^n$.

1.26 Example. We have:

1. $I = \langle x^2 + 1 \rangle$ in $\mathbb{R}[x]$. Then $I \neq \mathbb{R}[x]$ since $1 \notin I$. Also, $V(I) = \varnothing$ and $I(V(I)) = \mathbb{R}[x] \supsetneq I$.

   Often, when trying to find counterexamples, use a field that's not algebraically closed. Algebraic geometry over $\mathbb{R}$ is very important, so it's a good thing to build such intuition.
2. $X = (0, 1) \subsetneq \mathbb{R}$. Then $I(X) = \langle 0 \rangle$, since polynomials in one variable only have a finite number of roots, and elements of the ideal must vanish on all of $(0, 1)$. Thus $V(I(X)) = V(\langle 0 \rangle) = \mathbb{R} \supsetneq X$.

Proof. We prove #3.

3. By #2 part 2,

   $$\underbrace{V(S)}_{=X} \subseteq V(I(\underbrace{V(S)}_{=X}))$$

   Also, by #2 part 1, $S \subseteq I(V(S))$, so by properties of zero sets,

   $$V(I(V(S))) \subseteq V(S)$$

   and therefore $V(S) = V(I(V(S)))$. Idem for second property. □

We will see a one-to-one correspondence between algebraic sets and *radical* ideals.

1.27 Remark. If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal such that $I = I(X)$ for some $X \subseteq \mathbb{A}^n$, then $I = I(V(I))$.

But, we have seen that $I \subsetneq I(V(I))$ for a random ideal $I \subseteq k[x_1, \ldots, x_n]$. For example $I = \langle x^2 + 1 \rangle = \mathbb{R}[x]$ so $I \subsetneq I(V(I)) = \mathbb{R}[x]$.

1.28 Definition. Let $X \subseteq \mathbb{A}^n$ and $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. We define $\overline{X}$ to be the **closure of** X **in the Zariski topology** (that is, the smallest algebraic set containing X).

We define $\overline{I}$, the **closure of** I, to be the smallest ideal in $k[x_1, \ldots, x_n]$ containing I that is the ideal of a set of points in $\mathbb{A}^n$. If $I = \overline{I}$, we'll say that the ideal is **closed**.

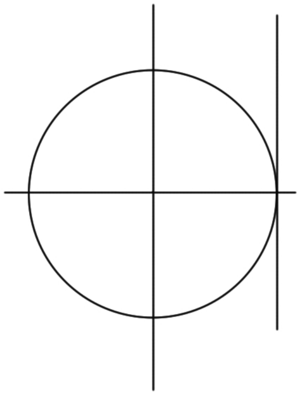
1.29 Lemma. $\overline{X} = V(I(X))$ and $\overline{I} = I(V(I))$.

Proof. We prove the first claim. We know that $X \subseteq V(I(X))$, and if Y is any algebraic set containing X, say $Y = V(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$, then $X \subseteq Y = V(S)$, so

$$V(I(X)) \subseteq V(I(V(S))) = V(S) = Y. \qquad \square$$

1.30 Example. We have:

1. Let $X = (0,1) \subseteq \mathbb{R}$. Then, $I(X) = (0)$ and $\overline{X} = \overline{(0,1)} = V(I(X)) = V(0) = \mathbb{R}$.
2. If k is infinite and X is an infinite subset of $\mathbb{A}^1(k)$, then $\overline{X} = \mathbb{A}^1(k)$, so *infinite subsets of* $\mathbb{A}^1(k)$ *are dense.*
3. Let $I = \langle x^2 + y^2 - 1, x - 1\rangle \subseteq \mathbb{R}[x, y]$. Then $V(I) = \{(1, 0)\}$:



So, $\overline{I} = I(V(I)) = I(\{(1, 0)\}) = \langle x - 1, y\rangle \supsetneq I$ since $y \notin I$.

On the assignment, we saw that an algebraic set intersected with a line (which is not contained in the set) never yields an infinite set of points. Is there a way of testing whether an ideal $I \subseteq k[x_1, \ldots, x_n]$ is the ideal of a set of points? We'll see that if $I = I(X)$ for some $X \subseteq \mathbb{A}^n$, then I is *radical.*

1.31 Definition. Let R be a ring and $I \subseteq R$ be an ideal. We define the **radical** of I by

$$\sqrt{I} = \mathrm{Rad}(I) := \{a \in R : a^n \in I \text{ for some } n > 0\}.$$

Also, I is called **radical** if $I = \sqrt{I}$.

1.32 Lemma. $I = \sqrt{I}$ if and only if whenever $a^n \in I$ for some $n > 0$, we have $a \in I$.

Proof. Suppose that $I = \sqrt{I}$. Let $a \in R$ be such that $a^n \in I$ for some $n > 0$. Then by definition, $a \in \sqrt{I} = I$.

Conversely, suppose that whenever $a^n \in I$ for some $n > 0$ we have $a \in I$. Since $I \subseteq \sqrt{I}$, we just need to check that $\sqrt{I} \subseteq I$. Let $a \in \sqrt{I}$. Then, $a^n \in I$ for some $n > 0$. But then $a \in I$ by hypothesis. $\square$

1.33 Example. We have:

1. Examples of radical ideals:

   (i) *Prime ideal*: Suppose that I is prime and $a \in R$ is such that $a^n \in I$ for some $n > 0$. Then $a^n = a^{n-1} \cdot a \in I$, and since I is prime, we get that $a^{n-1} \in I$ or $a \in I$. Continuing this process of decomposition some number of times, we will find that $a \in I$.

   Alternatively, note that I is radical iff R/I lacks nilpotents and I is prime iff R/I is an integral domain. Since any integral domain clearly lacks nilpotents, any prime ideal is radical.

   (ii) $I = \langle x^2 + 1\rangle \subseteq \mathbb{R}[x]$. Since $x^2 + 1$ is irreducible and $\mathbb{R}[x]$ is a PID, then $I = \langle x^2 + 1\rangle$ is prime and so radical.

   (iii) $I = \langle x - a, y - b\rangle \subseteq \mathbb{R}[x, y]$. Then I is maximal, hence prime, hence radical.

2. Examples of ideals that are *not* radical:

   (i) $I = \langle x^2 + y^2 - 1, x - 1\rangle$, so that $V(I) = \{(1, 0)\}$ but $I(V(I)) = \langle x - 1, y\rangle \supsetneq I$ (the idea is that since I not the ideal of a set of points, it is likely not radical). Well, note that

   $$y^2 = (x^2 + y^2 - 1) - (x + 1)(x - 1) \in I,$$

   but $y \notin I$, so I is not radical.

1.34 Theorem. Let $I \subseteq k[x_1, \dots, x_n]$. Then, if $I = I(X)$ for some $X \subseteq \mathbb{A}^n$, I is radical.

Proof. Let $f \in k[x_1, \dots, x_n]$ such that $f^n \in I = I(X)$ for some $n > 0$. Then,

$$f^n(p) = \underbrace{f(p) \cdots f(p)}_{n \text{ times}} = 0,$$

for all $p \in X$. But $f(p) \in k$, where k is a field and therefore has no zero divisors, so $f(p) = 0$, for all $p \in X$. Thus, $f \in I(X) = I$, so $I = I(X)$ is radical. □

1.35 Remark. We have:

1. If $I \subseteq k[x_1, \dots, x_n]$ is an ideal that is not radical, then I is not the ideal of a set of points.
2. The converse of the theorem may be false: a radical ideal may not be the ideal of a set of points.

   1.36 Example. $I = \langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$ is radical, but $I \subsetneq I(V(I))$ and so is not the ideal of a set of points.

Note carefully that the counterexample is over a field that is *not* algebraically closed.

1.37 Theorem (Hilbert's Nullstellensatz). Suppose that k is algebraically closed and $I \subseteq k[x_1, \dots, x_n]$ is an ideal. Then

$$I(V(I)) = \sqrt{I}.$$

1.38 Corollary. If k is algebraically closed and $I \subseteq [x_1, \dots, x_n]$ is an ideal, then $I = I(X)$ for some $X \subseteq \mathbb{A}^n$ if and only if $I = \sqrt{I}$.

Proof. We saw that if $I = I(X)$ then I is radical (i.e. $I = \sqrt{I}$).

Conversely if $I = \sqrt{I}$, then $I = I(V(I))$ (since $I(V(I)) = \sqrt{I}$ by the Nullstellensatz). □

Office hours tomorrow (16 May): 3 – 3:30pm and 4:30 – 6pm.

The usual grading scheme is 40% assignments and 60% final exam. However if you want to do a presentation it will be changed to 40% assignments, 40% final exam, 20% presentation.

The proof of the Nullstellensatz will appear later.

The goal of the class is to study geometric objects from an algebraic point of view. We saw that algebraic sets correspond to radical ideals (and vice versa, at least under the hypothesis of algebraic closure). Here is a recap:

- If X is algebraic, then $X = V(I(X))$.
- If I is the ideal of a set of points, $I = I(V(I))$.
- $\overline{X} = V(I(X))$, the closure of X (X is algebraic if $X = \overline{X}$).
- $\overline{I} = I(V(I))$, the closure of I ($I \subseteq \overline{I}$ and we call I *closed* if $I = \overline{I}$).
- Furthermore, if $I = I(X)$ for some $X \subseteq \mathbb{A}^n$, then I is radical. The Nullstellensatz told us that we have the converse when the field is algebraically closed ($k = \overline{k}$), so in this case $I = I(X)$ *if and only if* I is radical. This is because $\sqrt{I} = I(V(I)) = \overline{I}$.

1.39 Remark. In general, if k is not necessarily alg. closed, we have $I \subseteq \sqrt{I} \subseteq \overline{I}$ and may have that $\sqrt{I} \subsetneq I(V(I))$. Indeed, $I \subseteq \sqrt{I}$ by def. of $\sqrt{I}$, and if $f \in \sqrt{I}$ then $f^m \in I$ for some $m > 0$. Then, for all $p \in V(I)$, $f^m(p) = 0$ means that

$$\underbrace{f(p)}_{\in k} \cdots f(p) = 0$$

and hence $f(p) = 0$, so $f \in I(V(I))$, thus $\sqrt{I} \subseteq I(V(I))$.

1.40 Remark. In view of the maps $X \mapsto I(X)$ and $V(J) \leftarrow\!\shortmid J$, we have the following 1:1 correspondence.

$$\{X \subseteq \mathbb{A}^n \text{ alg.}\} \longleftrightarrow \{\text{closed ideals in } k[x_1, \dots, x_n]\}.$$

If k is alg. closed, then we can replace "closed" by "radical":

$$\{X \subseteq \mathbb{A}^n \text{ alg.}\} \longleftrightarrow \{\text{radical ideals in } k[x_1, \dots, x_n]\}.$$

An algebraic set X maps to $I(X)$, which then goes to $V(I(X)) = X$ since X is algebraic. Similarly if J is closed (i.e. ideal of a set of sets), then it gets mapped to $V(J)$, which subsequently gets mapped to $I(V(J)) = J$.

If k is alg. closed, then J is closed if and only if J is radical. So, we get the second correspondence.

1.3 Irreducible algebraic sets

1.41 Definition. Let $X \subseteq \mathbb{A}^n$ be an alg. set. Then X is called **irreducible** if $X \neq \varnothing$ and X cannot be written as

$$X = X_1 \cup X_2$$

with both X_1, X_2 algebraic sets not equal to X. Otherwise X is called **reducible**.

1.42 Example. We have:

1. If k is infinite, $\mathbb{A}^1$ is irreducible since $\mathbb{A}^1 \neq \varnothing$ and any proper algebraic subset of $\mathbb{A}^1$ is either $\varnothing$ or a finite set of points. So, if $\mathbb{A}^1 = X_1 \cup X_2$, with X_1, X_2 algebraic and $\neq \mathbb{A}^1$, this forces X_1 and X_2 to be finite sets of points (otherwise $X_1 = \varnothing$ and $X_2 = \mathbb{A}^1$ or vice versa). But this is a contradiction if k is infinite.

   On the other hand, if k is finite, then k is reducible.

2. Let $X = V(xy) \subseteq \mathbb{A}^2$. Then X is reducible because $X = V(x) \cup V(y)$ and these are both algebraic and $\neq X$.

   Note that $I(\mathbb{A}^1) = \langle 0 \rangle$ (a prime ideal) and $I(V(xy)) = \langle xy \rangle$ (not prime since $xy \in \langle xy \rangle$ but $x, y \notin \langle xy \rangle$).

1.43 Theorem. Let $X \subseteq \mathbb{A}^n$ be an algebraic subset. Then X is irreducible if and only if $I(X)$ is prime.

Proof. ($\rightarrow$) Suppose that X is irreducible. Let $f, g \in k[x_1, \ldots, x_n]$ be such that $fg \in I(X)$. Therefore $f(p)g(p) = 0$ for every $p \in X$, so that $X \subseteq V(fg) = V(f) \cup V(g)$. Thus,

$$X = (X \cap V(f)) \cup (X \cap V(g))$$

and these are both algebraic, so $X = X \cap V(f)$ or $X = X \cap V(g)$ since X is irreducible. If $X = X \cap V(f)$, then $X \subseteq V(f)$, so f must vanish at every point in X, so $f \in I(X)$. Similarly, if $X = X \cap V(g)$, $g \in I(X)$. Thus $I(X)$ is prime.

($\leftarrow$) Suppose that $I(X)$ is prime and that $X = X_1 \cup X_2$ with X_1, X_2 algebraic sets. Then

$$I(X) = I(X_1) \cap I(X_2)$$

(trivial proof: if $f \in I(X)$, then $f(p) = 0$, for all $p \in X = X_1 \cup X_2$ so $f \in I(X_1) \cap I(X_2)$ thus $I(X) \subseteq I(X_1) \cap I(X_2)$. If $f \in I(X_1) \cap I(X_2)$, $f(p) = 0$ for all $p \in X_1$, and $f(q) = 0$ for all $q \in X_2$, so $f(p) = 0$ for all $p \in X = X_1 \cup X_2$ thus $f \in I(X)$ thus $I(X_1) \cap I(X_2) \subseteq I(X)$).

If $I(X) = I(X_1)$ then $X = V(I(X)) = V(I(X_1)) = X_1$. Otherwise, $I(X) \subsetneq I(X_1)$ so there exists $f \in I(X_1)$ such that $f \notin I(X)$. Then, let us show that $I(X) = I(X_2)$, so that $X = X_2$ by the same argument as before. To see this, let $g \in I(X_2)$. Then,

$$fg \in I(X_2) \text{ and } fg \in I(X_1) \text{ since } f \in I(X_1)$$

thus $fg \in I(X_1) \cap I(X_2) = I(X)$, so $g \in I(X)$ by primality of $I(X)$, so

$$I(X_2) \subseteq I(X) \implies I(X_2) = I(X)$$

since $I(X) = I(X_1) \cap I(X_2)$. □

As a consequence, we have the following 1:1 correspondence:

$$\{\text{irreducible algebraic sets in } \mathbb{A}^n\} \leftrightarrow \{\text{prime ideals in } k[x_1, \ldots, x_n]\}$$

1.44 Definition. An **affine variety** (or **algebraic variety** or simply **variety**) is an irreducible algebraic set.

Thus, algebraic varieties correspond to prime ideals.

1.45 Example. We have:

1. If k is infinite (in particular, alg. closed), then $\mathbb{A}^n$ is irreducible (i.e. a variety) since $I(\mathbb{A}^n) = \langle 0 \rangle$, which is prime (note that $\langle 0 \rangle$ is always prime in $k[x_1, \ldots, x_n]$ for a field k, but we may have $I(\mathbb{A}^n) \supsetneq \langle 0 \rangle$ if k is finite).

2. Any point $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ is irreducible since $I(\{p\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal hence prime.

We'll see that the same way any integer can be decomposed as a product of powers of primes, any algebraic set can be decomposed as a finite union of irreducible sets.

1.46 Example. If k is infinite, then $\mathbb{A}^n$ is irreducible because $I(\mathbb{A}^n) = \langle 0 \rangle$. But if k is finite then $\mathbb{A}^n$ is the (finite) union of its points, so it's a finite union of algebraic sets, so $\mathbb{A}^n$ is reducible.

1.47 Theorem. If k is infinite, $I(\mathbb{A}^n) = \langle 0 \rangle$.

Proof. Clearly $\langle 0 \rangle \subseteq I(\mathbb{A}^n)$. Need to check that any $f \in I(\mathbb{A}^n)$ must be identically zero. If $n = 1$, then $f \in k[x]$ and $f(x) = 0$, for all $x \in \mathbb{A}^1 = k$ which is infinite, thus f has an infinite number of roots, so $f \equiv 0$. Suppose that it's true for all positive integers up to $n - 1$. Then, $f \in k[x_1, \ldots, x_n] = k[x_1, \ldots, x_{n-1}][x_n]$ so that

$$f(x_1, \ldots, x_n) = a_0(x_1, \ldots, x_{n-1}) + a_1(x_1, \ldots, x_{n-1})x_n + \ldots + a_m(x_1, \ldots, x_{n-1})x_n^m.$$

Also, $f(x_1, \ldots, x_n) = 0$ for all points $(x_1, \ldots, x_n) \in \mathbb{A}^n$. Let us fix $s_1, \ldots, s_{n-1} \in k$. Then,

$$g(x_n) := f(s_1, \ldots, s_{n-1}, x_n) = a_0(s_1, \ldots, s_{n-1}) + a_1(s_1, \ldots, s_{n-1})x_n + \ldots + a_m(s_1, \ldots, s_{n-1})x_n^m = 0, \quad \forall x_n \in k.$$

This implies $g \equiv 0$, so that $a_j(s_1, \ldots, s_{n-1}) = 0$, for all j and $s_1, \ldots, s_{n-1} \in k$. By induction we obtain $a_j \equiv 0$ for all j, so that $f \equiv 0$. □

1.48 Remark. If k is finite, then $I(\mathbb{A}^n) \neq \langle 0 \rangle$ since it contains $x_i^{p^\ell} - x_i$ for every i, where p is the prime such that $k = \mathbb{F}_{p^\ell}$. Thus

$$x_i(x_i^{p^\ell - 1} - 1) \in I(\mathbb{A}^n) \text{ for all } i, \text{ but } x_i, x_i^{p^\ell - 1} - 1 \notin I(\mathbb{A}^n) \implies I(\mathbb{A}^n) \text{ is not prime.}$$

We now want to talk about decomposition into irreducible sets. We first start with the following.

1.49 Theorem. Any algebraic set $X \subseteq \mathbb{A}^n$ is a finite union of irreducible algebraic sets.

Proof. Suppose instead that X is not a finite union of irreducible algebraic sets. In particular, X is not irreducible and $X = X_1 \cup X_1'$ with either X_1 or X_1' not a finite union of irreducible algebraic sets. Suppose that it is X_1. Then X_1 is not irreducible and $X_1 = X_2 \cup X_2'$ with X_2 or X_2' not a finite union of irreducible algebraic sets. Continuing this, we get a strict descending chain of algebraic sets:

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \ldots$$

and hence a strict ascending chain of ideals in $k[x_1, \ldots, x_n]$:

$$I(X) \subsetneq I(X_1) \subsetneq I(X_2) \subsetneq \ldots$$

Note that $I(X_i) \neq I(X_j)$ because otherwise $X_i = V(I(X_i)) = V(I(X_j)) = X_j$, but we know this is false. Similarly $I(X) \neq I(X_1)$. However, this contradicts the fact that $k[x_1, \ldots, x_n]$ is Noetherian. □

1.50 Question. If $X = X_1 \cup \ldots \cup X_m$ with each X_i irreducible algebraic, is the set of X_i's unique? No, because if $Y \subseteq X$ is any irreducible algebraic set, then $X = X_1 \cup \ldots \cup X_m \cup Y$ with all of the sets in the union irreducible.

However, we have the following.

1.51 Lemma. If $Y \subseteq \mathbb{A}^n$ is irreducible algebraic, and $Y \subseteq X_1 \cup \ldots \cup X_m$ with each X_i an algebraic set, then $Y \subseteq X_j$ for some j.

Proof. If $Y \subseteq X_1 \cup \ldots \cup X_m$, then $Y = (Y \cap X_1) \cup \ldots \cup (Y \cap X_m)$ where each $Y \cap X_i$ is algebraic. Thus, $Y = Y \cap X_j$ for some j, since Y is irreducible. Thus $Y \subseteq X_j$ for some j. □

1.52 Definition. Let $X \subseteq \mathbb{A}^n$ be an algebraic set. If we write

$$X = X_1 \cup \ldots \cup X_m$$

where each X_i is an irreducible algebraic set and $X_i \not\subseteq X_j$ for all $i \neq j$, we call $X_1 \cup \ldots \cup X_m$ the **(irredundant) decomposition** of X into irreducible algebraic sets.

Note that this decomposition always exists, since any algebraic set can be written as $X_1 \cup \ldots \cup X_m$ with X_i irreducible, and if $X_{i_0} \subseteq X_1 \cup \ldots \cup X_m$ for some i_0 ($1 \leq i_0 \leq m$), then $X_{i_0} \subseteq X_j$ for some j, so we can throw it out because it does not contribute non-trivially to the union.

1.53 Proposition. Every algebraic set has a unique irredundant decomposition into irreducible algebraic sets.

Proof. We have already seen that the decomposition exists, so we just need to check uniqueness. Let $X \subseteq \mathbb{A}^n$ be algebraic, and suppose that

$$X = X_1 \cup \ldots \cup X_m = Y_1 \cup \ldots Y_r$$

irredundantly. Let's show that $X_i = Y_j$ for all i, j.

$$X_i \subseteq X = Y_1 \cup \ldots \cup Y_r$$

but X_i is irreducible, so this forces $X_i \subseteq Y_j$ for some j, by the lemma. Similarly

$$Y_j \subseteq X = X_1 \cup \ldots \cup X_m$$

but Y_j is irreducible, so $Y_j \subseteq X_{i_0}$ for some i_0 by the lemma. Then, $X_i \subseteq Y_j \subseteq X_{i_0}$ thus $X_i = X_{i_0}$ because the decomposition is irredundant. Thus $X_i = Y_j$. Similarly any Y_j must be equal to some X_i. □

1.54 Example. Consider $X = V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subseteq \mathbb{C}^2$. Then,

$$y^4 - x^2 = (y^2 - x)(y^2 + x)$$

and

$$y^4 - x^2y^2 + xy^2 - x^3 = (y^2 - x^2)(y^2 + x)$$

which means that

$$X = V(y^2 + x) \cup V(y^2 - x, y^2 - x^2)$$

where $V(y^2 + x)$ is irreducible (by argument below). Moreover

$$V(y^2 - x, y^2 - x^2) = \{(0,0), (1,1), (1,-1)\}$$

so that

$$X = V(y^2 + x) \cup \cancel{\{(0,0)\}} \cup \{(1,1)\} \cup \{(1,-1)\}$$

where we remove $(0,0)$ since $(0,0) \in V(y^2 + x)$. We claim that this is the irredundant decomposition of X:

$$X = V(y^2 + x) \cup \{(1,1)\} \cup \{(1,-1)\}.$$

Office hours: Tomorrow 3:00 – 3:45pm and Friday 1 – 2:30pm (only this week)

Lectures on May 24, July 5, July 19: 3:30 – 5:20pm in MC 4064 (OR replace July 19 by June 7).

Notice that points are certainly irreducible, and moreover we have $V(y^2 + x)$ is irreducible since

$$I(V(y^2 + x)) = \sqrt{(y^2 + x)} = (y^2 + x)$$

(the first equality is from the Nullstellensatz since $\mathbb{C}$ is algebraically closed; the second is since $(y^2 + x)$ is prime because $y^2 + x$ is irreducible, so it's radical). Thus,

$$I(V(y^2 + x)) = (y^2 + x) \text{ prime} \implies V(y^2 + x) \text{ is irred.}$$

Therefore, $V(y^2 + x)$, $\{(0,0)\}$, $\{(1,1)\}$, $\{(1,-1)\}$ are all irreducible. Note that $(0,0) \in V(y^2 + x)$ so that we can get rid of $\{(0,0)\}$.

1.55 Example. If k is algebraically closed and $f = f_1^{r_1} \cdots f_m^{r_m}$ with f_i an irreducible polynomial in $k[x_1, \ldots, x_n]$, for all i, then

$$V(f) = V(f_1) \cup \ldots \cup V(f_m)$$

and each $V(f_i)$ is irreducible (because by the Nullstellensatz $I(V(f_i)) = \sqrt{(f_i)} = (f_i)$ which is prime).

1.56 Remark. We have seen if k is alg. closed, then there is a 1:1 correspondence between alg. sets in $\mathbb{A}^n$ and radical ideals in $k[x_1, \ldots, x_n]$. Let I be a radical ideal in $k[x_1, \ldots, x_n]$. Then, $X = V(I)$ is alg. and can be written as

$$X = X_1 \cup \ldots \cup X_m$$

with each X_i an irred. alg. set. So

$$I(X) = I(X_1) \cap \ldots \cap I(X_m) \tag{*}$$

with each $I(X_i)$ a prime ideal. The expression (*) is the **primary decomposition** of the radical ideal $I(X) = I$ (X alg.).

1.4 Classification of irreducible algebraic subsets in $\mathbb{A}^2$

If k is finite, then the only irreducible alg. subsets of $\mathbb{A}^2$ are single points (since irred. alg. are non-empty). Let us then assume that k is infinite. We want to show that the only irred. alg. sets are single points, $\mathbb{A}^2$, and sets of the form $V(f)$ (with f irreducible and $V(f)$ infinite).

1.57 Remark. If k is not algebraically closed, then $V(f)$ may be finite even if $f = f(x, y)$ is irreducible in $k[x, y]$.

1.58 Example. $f = x^2 + y^2(y-1)^2$ in $\mathbb{R}[x, y]$ has $V(f) = \{(0, 0), (0, 1)\}$. However, $f = x^2 + y^2(y-1)^2$ in $\mathbb{C}[x, y]$ has

$$V(f) = V(x - iy(y-1)) \cup V(x + iy(y-1))$$

which is infinite.

We first need to prove the following.

1.59 Proposition. If $f, g \in k[x, y]$ have no common factors, then $V(f, g)$ has at most a finite number of points.

Proof. Note $f, g \in k[x, y] = k[x][y]$. Since f and g don't have common factors in $k[x][y]$, they don't have common factors in $k(x)[y]$. Otherwise, there exist $s, t \in k(x)[y]$ with $sf + tg = d$. If $m = \operatorname{lcm}(\text{denom. of } s, t, d)$ then

$$\underbrace{(ms)}_{\in k[x,y]} f + \underbrace{(mt)}_{\in k[x,y]} g = md \in k[x, y],$$

contradicting the fact that f and g don't have common factors in $k[x, y]$.

Now, $k(x)[y]$ is a PID since $k(x)$ is a field, so there are $\tilde{s}, \tilde{t} \in k(x)[y]$ such that $\tilde{s}f + \tilde{t}g = 1$ (because f and g don't have common factors). Again, if $\tilde{m} = \operatorname{lcm}(\text{denom. of } \tilde{s}, \tilde{t})$ and $a = \tilde{m}\tilde{s}$, $b = \tilde{m}\tilde{t}$, we have

$$af + bg = \tilde{m} = \tilde{m}(x)$$

with $\tilde{m} \in k[x]$ (since the denom. are polynomials in $k[x]$). Let $(x_0, y_0) \in V(f, g)$. Then

$$0 = a\underbrace{f(x_0, y_0)}_{0} + b\underbrace{g(x_0, y_0)}_{0} = \tilde{m}(x_0)$$

so x_0 is the zero of a polynomial in 1 variable, so there are only a finite number of possibilities for x_0. In the same way, we prove by writing $k[x, y] = k[y][x]$ that there exist only finitely many possibilities for y_0. Thus $V(f, g)$ has at most a finite number of points. □

It is clear from the proof that this does not extend at all to higher dimensions.

1.60 Corollary. If $f \in k[x, y]$ is irreducible and X is an infinite alg. subset of $V(f)$, then $I(X) = \langle f \rangle$. In particular, $X = V(f)$ and $V(f)$ is irreducible.

Proof. Since $X \subseteq V(f)$, then f vanishes on all of X, so $f \in I(X)$, so $\langle f \rangle \subseteq I(X)$. Suppose that there exists $g \in I(X)$ such that $g \notin \langle f \rangle$. So, g is not a multiple of f, and, since f is irreducible, this means that f and g don't have common factors. Thus, $V(f, g)$ is at most a finite set of points. But, $f, g \in I(X)$ so $X \subseteq V(f, g)$ and X is infinite. So this is a contradiction. Hence, for all $g \in I(X)$, we have $g \in \langle f \rangle$ so $I(X) = \langle f \rangle$.

Also, we have that $X = V(I(X))$ since X is algebraic, but we said $V(I(X)) = V(\langle f \rangle) = V(f)$. And if we set $X = V(f)$ then $I(V(f)) = I(X) = \langle f \rangle$ which is prime since f is irreducible. So $V(f)$ is irreducible. □

1.61 Theorem (Classification of irred. alg. sets in $\mathbb{A}^2$). Suppose that k is infinite. Then, the irred. alg. sets in $\mathbb{A}^2$ are:

(i) $\mathbb{A}^2$

(ii) $\{(a, b)\}$ for $(a, b) \in \mathbb{A}^2$

(iii) $V(f)$ where $f \in k[x, y]$ is irred. and $V(f)$ is an infinite set.

Proof. We have already seen that $\mathbb{A}^2$ and $\{(a, b)\}$ are irred. alg. sets. Let X be an irred. alg. set other than $\mathbb{A}^2$ or a singleton $\{(a, b)\}$. Note that $X \neq \varnothing$ since it is irreducible. Moreover X is infinite, for otherwise it would be either a singleton or reducible. Finally $I(X)$ is prime by irreducibility of X, and $I(X) \neq (0)$ for otherwise $X = V(I(X)) = \mathbb{A}^2$ because X is alg.

Then, there exists $0 \neq f \in I(X)$ and we can assume that f is irreducible (otherwise, pick any irred. factors of f, which must also be in $I(X)$ because $I(X)$ is prime). Then,

$$\underbrace{X}_{\text{infinite}} \subseteq \underbrace{V(f)}_{\text{irred.}}$$

thus $X = V(f)$ by the corollary above. □

1.6 Proof of Hilbert's Nullstellensatz

We have seen that if $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then

$$I \subseteq \sqrt{I} \subseteq I(V(I))$$

1.62 Theorem (Hilbert's Nullstellensatz). If k is alg. closed, then

$$\sqrt{I} = I(V(I)).$$

The theorem relies on the following technical fact.

Recall that if k and K are two fields such that $k \subseteq K$, then K is called an **extension of** k. Also, K is said to be **algebraic** over k if every element of K is the zero of a polynomial in $k[t]$. Finally, k is **algebraically closed**, which we denote $k = \overline{k}$, if every algebraic extension of k is equal to k.

1.63 Fact (Zariski lemma?). Let k be a field and K be such that

$$K = k[y_1, \ldots, y_m] \qquad \text{(finitely generated } k\text{-algebra)}$$

for some $y_1, \ldots, y_m \in K$. Note that there may be relations among the y_i. Then if K is a field, then K is algebraic over k. In particular, if $k = \overline{k}$ then $K = k$.

1.64 Example. Take $k = \mathbb{R}$ and $K = \mathbb{R}[x]/(x^2+1) = \mathbb{R}[\overline{x}]$ with $\overline{x^2+1} = 0 \iff \overline{x}^2 = -1$. Then, K is a field because (x^2+1) is maximal. In fact $K = \mathbb{R}[\overline{x}] = \mathbb{C}$, which is alg. over $\mathbb{R}$.

1.65 Theorem (Weak Nullstellensatz). If $k = \overline{k}$, then every maximal ideal of $R := k[x_1, \ldots, x_n]$ is of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $(a_1, \ldots, a_n) \in \mathbb{A}^n$.

Proof. Let M be any maximal ideal in R. Then R/M is a field. So,

$$R/M = k[x_1, \ldots, x_n]/M = k[\overline{x_1}, \ldots, \overline{x_n}],$$

where $\overline{x_i}$ is the congruence class of $x_i \pmod{M}$. By the above fact, we must have $R/M = k$. Suppose that $\overline{x_i} = a_i$ with $a_i \in k$. Then

$$\overline{x_i - a_i} = \overline{x_i} - a_i = 0$$

thus $x_i - a_i \in M$, for all $i = 1, \ldots, n$. Hence

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq M$$

but $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal, so $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

So, under the hypothesis of algebraic closure, *the only maximal ideals in the polynomial ring are the ideals of points.*

1.66 Corollary. If $k = \overline{k}$ and I is an ideal in $k[x_1, \ldots, x_n]$ such that $V(I) = \varnothing$, then $I = k[x_1, \ldots, x_n]$.

Proof. Suppose instead that $I \subsetneq k[x_1, \ldots, x_n]$. Then $I \subseteq M$ for some maximal ideal $M \subsetneq k[x_1, \ldots, x_n]$. By the Weak Nullstellensatz, $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $(a_1, \ldots, a_n) \in \mathbb{A}^n$. So, $I \subseteq \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ and

$$(a_1, \ldots, a_n) \in V(I) = \varnothing,$$

a contradiction. So $I = k[x_1, \ldots, x_n]$. □

We now prove the Nullstellensatz. "Nullstellen" means "zeroes" and "satz" means "locus".

Proof of Hilbert's Nullstellensatz. We know that $\sqrt{I} \subseteq I(V(I))$. Let us show the other inclusion. It is enough to show that if $g \in I(V(I))$ then $g^m \in I$ for some $m > 0$.

Let $g \in I(V(I))$. Suppose that $I = \langle f_1, \dots, f_r \rangle$. Then,

$$V(f_1(x_1, \dots, x_n), \dots, f_r(x_1, \dots, x_n), x_{n+1}g(x_1, \dots, x_n) - 1) = \varnothing.$$

Indeed, if $(a_1, \dots, a_{n+1}) \in V(f_1, \dots, f_r, x_{n+1}g - 1)$, then

$$f_i(a_1, \dots, a_n) = 0, \qquad \forall i$$

thus $(a_1, \dots, a_n) \in V(f_1, \dots, f_r) = V(I)$, and $g(a_1, \dots, a_n) = 0$ because $g \in I(V(I))$. So, $x_{n+1}g(x_1, \dots, x_n) - 1$ evaluated at $(a_1, \dots, a_n, a_{n+1})$ gives

$$a_{n+1}\underbrace{g(a_1, \dots, a_n)}_{0} - 1 = -1 \neq 0,$$

a contradiction. Then, by the corollary,

$$\langle f_1, \dots, f_r, x_{n+1}g - 1 \rangle = k[x_1, \dots, x_{n+1}].$$

In particular

$$1 = p_1(x_1, \dots, x_{n+1})f_1(x_1, \dots, x_n) + \dots + p_r(x_1, \dots, x_{n+1})f_r(x_1, \dots, x_n) + p_{r+1}(x_1, \dots, x_{n+1})(x_{n+1}g(x_1, \dots, x_n) - 1)$$

Replacing $x_{n+1} = 1/g$ in the expression, we get

$$1 = p_1(x_1, \dots, x_n, 1/g)f_1 + \dots + p_r(x_1, \dots, x_n, 1/g)f_r + 0.$$

Multiplying by a high enough power of $g(x_1, \dots, x_n)$ to clear the denominators, we get

$$g^s = \widetilde{p_1}(x_1, \dots, x_n)f_1 + \dots + \widetilde{p_r}(x_1, \dots, x_n)f_r \in \langle f_1, \dots, f_r \rangle = I. \qquad \square$$

Idea of proof of Zariski's lemma. Induction on $m = 1$. If $m = 1$, then $K = k[a_1]$ is a field. So $\frac{1}{a_1} \in k[a_1]$. Thus $\frac{1}{a_1} = f(a_1)$ for some $f(t) \in k[t]$. In particular,

$$a_1 f(a_1) - 1 = 0$$

and a_1 is the root of the polynomial $tf(t) - 1 \in k[t]$.

For $m = 2$: $K = k[a_1, a_2] = k[a_1][a_2] = k(a_1)[a_2]$ is a field. By the case $m = 1$, K is algebraic over $k(a_1)$. If we show that $k(a_1)$ is algebraic over k, then K is algebraic over k (by "transitivity of algebraicity": $k \subseteq k(a_1) \subseteq K$). Then show that a_1 is alg. over k to obtain that $k(a_1)$ is alg. over k. □

2 Affine varieties

Let us assume from now on that k is infinite. Also, any alg. set is assumed to be in $\mathbb{A}^n$.

We have seen that an affine (algebraic) variety is an irreducible alg. set. Moreover, the ideal of a variety is prime. This means that if X is any variety, $k[x_1, \dots, x_n]/I(X)$ is an integral domain.

2.1 Coordinate rings

2.1 Definition. Given a variety X, the quotient ring

$$\Gamma(X) := \frac{k[x_1, \dots, x_n]}{I(X)}$$

is called the **coordinate ring of** X. Other notations include $k[X]$ or $A(X)$.

2.2 Definition. A function $f : X \to k$ is called a **polynomial function** if there exists $F \in k[x_1, \dots, x_n]$ such that $f(p) = F(p)$ for all $p \in X$.

Note that two distinct polynomials $F, G \in k[x_1, \dots, x_n]$ may determine the same polynomial function on X, in which case

$$F(p) = f(p) = G(p), \quad \forall p \in X \iff F - G \in I(X).$$

Consequently,

$$\Gamma(X) := k[x_1, \dots, x_n]/I(X)$$

can be interpreted as the set of all polynomial functions on X.

2.3 Example. We have:

1. If $X = \{p\}$, then $\Gamma(X) = k$. Indeed, $I(X) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ if $p = (a_1, \dots, a_n)$, so that
$$\Gamma(X) = \frac{k[x_1, \dots, x_n]}{\langle x_1 - a_1, \dots, x_n - a_n \rangle} = k.$$
2. If $X = \mathbb{A}^n$ then $\Gamma(X) = k[x_1, \dots, x_n]$ since $I(X) = (0)$, so that
$$\Gamma(X) = \frac{k[x_1, \dots, x_n]}{(0)} = k[x_1, \dots, x_n].$$
3. Let $X = V(y - x^2) \subseteq \mathbb{A}^2$. Then
$$\Gamma(X) = \frac{k[x, y]}{\langle y - x^2 \rangle} = k[\overline{x}, \overline{y}] \text{ (with } \overline{y} = \overline{x}^2) = k[\overline{x}].$$
[DIAGRAM OF PARABOLA].
4. Let $X = V(xy - 1) \subseteq \mathbb{A}^2$. Then
$$\Gamma(X) = \frac{k[x, y]}{\langle xy - 1 \rangle} = k[\overline{x}, \overline{y}] \text{ (with } \overline{xy} = 1) = k[\overline{x}, \overline{x}^{-1}]$$
(the ring of Laurent polynomials).

2.4 Remark. Note that

- $\Gamma(\mathbb{A}^1) = k[t]$.
- $\Gamma(V(y - x^2)) = k[\overline{x}] \cong k[t]$ so $V(y - x^2) \cong \mathbb{A}^1$
- $\Gamma(V(xy - 1)) = k[\overline{x}, \overline{x}^{-1}] \ncong k[t]$ (not true here; we'll see this later).

2.5 Remark. We have the following "dictionary" between geometry and algebra (assume $k = \overline{k}$).

Geometry	**Algebra**
$\mathbb{A}^n$	$k[x_1, \dots, x_n]$
$X \subseteq \mathbb{A}^n$ algebraic	a radical ideal $I(X)$
$X \subseteq \mathbb{A}^n$ irreducible algebraic	a prime ideal $I(X)$
a point	a maximal ideal

Similarly, for a variety $X \subseteq \mathbb{A}^n$,

Geometry	**Algebra**
X	$\Gamma(X)$
$Y \subseteq X$ algebraic	$I_X(Y) = I(Y) \pmod{I(X)}$ radical
$Y \subseteq X$ irreducible algebraic	$I_X(Y)$ prime
a point in X	a maximal ideal in $\Gamma(X)$

Assignment 2: due Friday June 7.

Assignment 3: due Friday June 14.

Let X be a variety (i.e. irred. alg. set) in $\mathbb{A}^n$. Since X is irreducible, $I(X)$ is prime and

$$\Gamma(X) = \frac{k[x_1, \dots, x_n]}{I(X)},$$

the coordinate ring of X (set of all polynomial functions on X), is a *domain.* But $\Gamma(X)$ has more structure.

2.6 Proposition. $\Gamma(X)$ is Noetherian.

Proof. We use the fact that, if R is a ring and $I \subseteq R$ is an ideal, then any ideal J in R/I is of the form $J = \pi(J')$ for some ideal $J' \subseteq R$, where $\pi : R \to R/I$ is the natural projection map ($r \mapsto \overline{r}$) such that $I \subseteq J'$.

Let $J_1 \subseteq J_2 \subseteq \ldots \subseteq J_r \subseteq \ldots$ be an ascending chain of ideals in $\Gamma(X) = k[x_1, \ldots, x_n]/I(X)$. Then for all i, there exists an ideal J_i' in $k[x_1, \ldots, x_n]$ that contains $I(X)$ and we have

$$J_1' \subseteq J_2' \subseteq \ldots J_r' \subseteq \ldots$$

Since $k[x_1, \ldots, x_n]$ is Noetherian, this ascending chain must terminate. So there exists i_0 such that

$$J_r' = J_{i_0}' \qquad \forall r \geq i_0.$$

Therefore $J_r = \pi(J_r') = \pi(J_{i_0}') = J_{i_0}$ for all $r \geq i_0$. So $\Gamma(X)$ is Noetherian. □

2.2 Polynomial maps

Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two varieties.

2.7 Definition. A map $\varphi : X \to Y$ is called **polynomial** if there exist polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that

$$\varphi(x) = (f_1(x), \ldots, f_m(x))$$

for all $x \in X$ (and $\varphi(X) \subseteq Y$).

2.8 Remark. $f_1, \ldots, f_m$ are uniquely determined by φ up to elements in $I(X)$.

2.9 Example. We have:

1. Polynomial functions $f : X \to k = \mathbb{A}^1$ are polynomial maps.
2. Any affine map $\mathbb{A}^n \to \mathbb{A}^m$, $x \mapsto A(x) + \vec{b}$ where $A : \mathbb{A}^n \to \mathbb{A}^m$ is a linear map and $\vec{b} \in \mathbb{A}^m$ (so, the composition of a linear map and a translation).

   If A is invertible (when $n = m$) then the affine map is called an **affine change of coordinates**.
3. $X = V(y - x^2) \subseteq \mathbb{A}^2 \to \mathbb{A}^1$ by $(x, y) \mapsto x$. [DIAGRAM OF PARABOLA WITH PROJECTION LINE]. This is a polynomial map, with polynomial inverse

   $$\varphi^{-1} : \mathbb{A}^1 \to X \subseteq \mathbb{A}^2, \qquad t \mapsto (t, t^2).$$

4. $X = V(y^2 - x^3) \subseteq \mathbb{A}^2$ [DIAGRAM OF CUSP CURVE WITH SINGULARITY]. This is a surjective polynomial map, but it does not have a polynomial inverse.

   Indeed, suppose that φ has a polynomial inverse. Then there exists $\psi : X \subseteq V(y^2 - x^3) \to \mathbb{A}^1$ by $(x, y) \mapsto p(x, y)$ with $p(x, y) \in k[x, y]$. In particular,

   $$t = \psi \circ \varphi(t) = \psi(t^2, t^3) = p(t^2, t^3)$$

   Since $p(x, y) \in k[x, y]$, we can write it as:

   $$p(x, y) = a_0 + a_1 x + a_2 y + a_3 x^2 + a_4 xy + \ldots$$

   so,

   $$t = p(t^2, t^3) = \underbrace{a_0}_{\text{deg } 0 \text{ in } t} + \underbrace{a_1 t^2 + a_2 t^3 + a_3 t^4 + \ldots}_{\text{deg } \geq 2 \text{ in } t}$$

   and since the right-hand side has *no linear term*, this is impossible. Hence φ has no polynomial inverse.

2.10 Proposition. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two varieties. Also, let $\varphi : X \to Y$ be a polynomial map. Then,

(i) For any alg. set $Z \subseteq Y$, $\varphi^{-1}(Z) \subseteq X$ is an alg. set. That is, φ is continuous in the Zariski topology.

(ii) $\overline{\varphi(X)}$ is irreducible in $\mathbb{A}^m$.

Proof. Let $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_m)$ be ambient coordinates in $\mathbb{A}^n$ and $\mathbb{A}^m$, respectively. Also, suppose that $\varphi = (f_1, \ldots, f_m)$ for some $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$.

(i) Let $Z \subseteq Y$ be alg. Then, $Z = V(g_1, \dots, g_r)$ for some $g_1, \dots, g_r \in k[y_1, \dots, y_m]$. I claim that

$$\varphi^{-1}(Z) = V(g_1 \circ \varphi, \dots, g_r \circ \varphi).$$

Indeed,

$$\begin{aligned} p \in \varphi^{-1}(Z) &\iff \varphi(p) \in Z \\ &\iff g_i(\varphi(p)) = (g_i \circ \varphi)(p) = 0 \text{ for all } i \ (1 \leq i \leq r) \\ &\iff p \in V(g_1 \circ \varphi, \dots, g_r \circ \varphi). \end{aligned}$$

Finally, note that

$$g_i \circ \varphi = g_i(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \in k[x_1, \dots, x_n]$$

for all i, so $\varphi^{-1}(Z)$ is algebraic.

(ii) Let us show that $\overline{\varphi(X)}$ is irred. in $\mathbb{A}^m$. Suppose that $\overline{\varphi(X)} = V_1 \cup V_2$ with V_1 and V_2 algebraic. Then, let's verify that $\overline{\varphi(X)} = V_1$ or V_2. Note that

$$X = \varphi^{-1}(\overline{\varphi(X)}) = \varphi^{-1}(V_1 \cup V_2) = \varphi^{-1}(V_1) \cup \varphi^{-1}(V_2)$$

Then, since $\varphi^{-1}(V_1)$ and $\varphi^{-1}(V_2)$ are algebraic (by (i)) and X is irreducible (since it's a variety), we have $X = \varphi^{-1}(V_1)$ or $X = \varphi^{-1}(V_2)$. If $X = \varphi^{-1}(V_i)$, then

$$\varphi(X) \subseteq V_i \implies V_1 \cup V_2 = \overline{\varphi(X)} \subseteq \overline{V_i} = V_i \text{ (since } V_i \text{ is algebraic)} \implies \overline{\varphi(X)} = V_i. \qquad \square$$

2.11 Remark. We have:

(i) Can use (i) to determine whether or not a set is algebraic. That is, if one can express $X \subseteq \mathbb{A}^n$ as the preimage of an algebraic set in $\mathbb{A}^m$ under a polynomial map, then X is algebraic.

(ii) Can use (ii) to determine whether an algebraic set is irreducible. That is, if one can express an algebraic set $Z \subseteq \mathbb{A}^m$ as $\overline{\varphi(X)}$ for some polynomial map $\varphi : X \to \mathbb{A}^m$ (with X a variety), then Z is irreducible.

2.12 Example. Consider the polynomial map

$$\det : M_{n \times n}(k) = \mathbb{A}^{n^2} \to \mathbb{A}^1, \qquad A \mapsto \det A.$$

Then,

$$\mathrm{SL}(n, k) = \{A \in M_{n \times n}(k) : \det A = 1\} = \det{}^{-1}(1)$$

thus $\mathrm{SL}(n, k)$ is algebraic.

2.13 Example. Twisted cubic $V(y - x^2, z - x^3)$: is it irreducible?

$$\varphi : \mathbb{A}^1 \to V(y - x^2, z - x^3) \qquad t \mapsto (t, t^2, t^3)$$

is a polynomial map with $\varphi(\mathbb{A}^1) = V(y - x^2, z - x^3)$. Since $\mathbb{A}^1$ is a variety, this proves that $V(y - x^2, z - x^3)$ is irreducible and therefore a variety.

We therefore have 3 ways of testing irreducibility of an algebraic set $Z \subseteq \mathbb{A}^m$. Z is irreducible if and only if

(i) $I(Z)$ is prime

(ii) $k[x_1, \dots, x_m]/I(Z)$ is a domain

(iii) $Z = \overline{\varphi(X)}$ for some polynomial map $\varphi : X \to \mathbb{A}^m$ with $X \subseteq \mathbb{A}^m$ a variety

2.14 Definition. Two varieties $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ are said to be **isomorphic** if there exists an invertible polynomial map $\varphi : X \to Y$ whose inverse φ^{-1} is also a polynomial map. We then write $X \simeq Y$.

2.15 Example. We have:

1. $\varphi : X = V(y - x^2) \subseteq \mathbb{A}^2 \to \mathbb{A}^1$ given by $(x, y) \mapsto x$ is an isomorphism with polynomial inverse $\varphi^{-1} : \mathbb{A}^1 \to X$ given by $t \mapsto (t, t^2)$ [DIAGRAM OF PARABOLA PROJECTING DOWN ONTO x-AXIS]. Thus

$$X = V(y - x^2) \simeq \mathbb{A}^1.$$

2. $\varphi : \mathbb{A}^1 \to X = V(y^2 - x^3) \subseteq \mathbb{A}^2$ given by $t \mapsto (t^2, t^3)$. We saw that this is not an isomorphism because it does not admit a polynomial inverse. [DIAGRAM OF CURVE WITH "CUSP"].

   Question: Does an isomorphism between $\mathbb{A}^1$ and $X = V(y^2 - x^3)$ exist? We'll see that the answer is no because
   $$\Gamma(\mathbb{A}^1) = k[t] \not\simeq k[\overline{x}, \overline{y}] \text{ (with relation } \overline{y}^2 = \overline{x}^3) = \Gamma(X)$$
   where "$\not\simeq$" means "as k-algebras". This is an exercise.

3. An affine coordinate change is an affine transformation $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ given by $x \mapsto A(x) + \vec{b}$, with $A : \mathbb{A}^n \to \mathbb{A}^n$ an invertible linear map and $\vec{b} \in \mathbb{A}^n$. Note that φ has inverse $\varphi^{-1} : \mathbb{A}^n \to \mathbb{A}^n$ given by $x \mapsto A^{-1}(x) - A^{-1}(\vec{b})$, and φ and φ^{-1} are both polynomial maps (since A and A^{-1} can be represented by matrices).

Affine coordinate changes are special isomorphisms called **affine equivalences**.

2.16 Example. One can show that any **irreducible conic** in $\mathbb{R}^2$ (i.e. the zero set of an irreducible polynomial of degree 2) is affinely equivalent to

- $y^2 = x$ (parabola)
- $x^2 + y^2 = 1$ (circle)
- $x^2 - y^2 = 1$ (hyperbola)

2.17 Definition (PULLBACK). Let $\varphi : X \to Y$ be a polynomial map between two varieties X and Y. We define the **pullback along** φ by
$$\varphi^* : \Gamma(Y) \to \Gamma(X) \qquad \text{by} \qquad \overline{g} \mapsto \overline{g \circ \varphi}.$$
Is φ^* well-defined? That is, if $\overline{g} = \overline{g'}$ in $\Gamma(Y)$, do we have that $\overline{g \circ \varphi} = \overline{g' \circ \varphi}$ in $\Gamma(X)$? Suppose that $X \subseteq \mathbb{A}^n$ with ambient coordinates $x_1, \dots, x_n$ and that $Y \subseteq \mathbb{A}^m$ with ambient coordinates $y_1, \dots, y_m$. Then, if $\overline{g} = \overline{g'}$ in $\Gamma(Y) = k[y_1, \dots, y_m]/I(Y)$, then
$$g' = g + h, \qquad h \in I(Y).$$
Also,
$$g' \circ \varphi = g \circ \varphi + \underbrace{h \circ \varphi}_{=0} = g \circ \varphi$$
because for all $p \in X$, $\varphi(p) \in Y$, so that $h(\varphi(p)) = 0$. Therefore
$$\overline{g' \circ \varphi} = \overline{g \circ \varphi} \qquad \text{in} \qquad \Gamma(X) = \frac{k[x_1, \dots, x_n]}{I(X)}$$
thus φ^* is well-defined.

2.18 Remark (FUNCTORIALITY). We have:

(i) $(\mathrm{id}_X)^* = \mathrm{id}_{\Gamma(X)}$

(ii) $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$

(iii) Note that $\Gamma(X)$ is a k-algebra because it is a ring that admits a k-vector space structure. Then, $\varphi^* : \Gamma(Y) \to \Gamma(X)$ is a k-algebra homomorphism, i.e. φ^* is a k-linear ring homomorphism.

2.19 Remark. Since the pullback φ^* is a k-algebra homomorphism, it is enough to specify it on the generators $\overline{y_i}$ of $\Gamma(Y) = k[y_1, \dots, y_m]/I(Y) = k[\overline{y_1}, \dots, \overline{y_m}]$.

2.20 Example. $\varphi : \mathbb{A}^1 \to X = V(y^2 - x^3) \subseteq \mathbb{A}^2$ given by $t \mapsto (t^2, t^3)$. Then
$$\varphi^* : \Gamma(X) = k[\overline{x}, \overline{y}] \to \Gamma(\mathbb{A}^1) = k[t]$$
is given by
$$\overline{x} \mapsto \overline{x \circ \varphi} = t^2, \qquad \overline{y} \mapsto \overline{y \circ \varphi} = t^3$$

2.21 Remark. For two varieties X and Y, we will see that
$$X \simeq Y \iff \Gamma(X) \simeq \Gamma(Y) \text{ as } k\text{-algebras}.$$

We need to prove some things beforehand.

2.22 Proposition (FAITHFULNESS). If $\varphi : X \to Y$ and $\psi : X \to Y$ are polynomial maps and $\varphi^* = \psi^*$ then $\varphi = \psi$.

Proof. Let $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_m)$ be ambient coordinates in $\mathbb{A}^n$ and $\mathbb{A}^m$, respectively. Then $\varphi = (f_1, \ldots, f_m)$ and $\psi = (g_1, \ldots, g_m)$ for some $f_1, \ldots, f_m, g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$. Note that $f_i = y_i \circ \varphi$ and $g_i = y_i \circ \psi$. So, if $\varphi^* = \psi^*$, then

$$\overline{f_i} = \overline{y_i \circ \varphi} = \varphi^*(\overline{y_i}) = \psi^*(\overline{y_i}) = \overline{y_i \circ \psi} = \overline{g_i}$$

so f_i and g_i agree up to an element of $I(X)$ for all $i = 1, \ldots, m$, therefore $\varphi = \psi$. □

2.23 Proposition (FULLNESS). Let $\Phi : \Gamma(Y) \to \Gamma(X)$ be a k-algebra homomorphism. Then there exists $\varphi : X \to Y$ such that $\Phi = \varphi^*$.

Proof. Suppose that $\varphi : X \subseteq \mathbb{A}^n \to Y \subseteq \mathbb{A}^m$ given by $x = (x_1, \ldots, x_n) \mapsto (f_1(x), \ldots, f_m(x)) = (y_1, \ldots, y_m)$ is such that $\varphi^* = \Phi$. Then

$$\Phi(\overline{y_i}) = \varphi^*(\overline{y_i}) = \overline{y_i \circ \varphi} = \overline{f_i}. \tag{*}$$

So, if such a φ exists, we need (*) to hold. Let f_i be a representative of $\Phi(\overline{y_i})$ for all $i = 1, \ldots, m$, i.e. $\overline{f_i} = \Phi(\overline{y_i})$. Set $\varphi : X \subseteq \mathbb{A}^n \to \mathbb{A}^m$ by $x \mapsto (f_1(x), \ldots, f_m(x))$. Need to check the following:

(i) $\varphi(X) \subseteq Y$

(ii) $\varphi^* = \Phi$.

We now prove (i). Let $g \in k[y_1, \ldots, y_m]$. First note that

$$\Phi(\overline{g}) \underset{k\text{-alg hom}}{=} g(\overline{f_1}, \ldots, \overline{f_m}) = \overline{g \circ \varphi}.$$

Indeed, we have

$$g = \sum \underbrace{a_{r_1 \cdots r_m}}_{\in k} y_1^{r_1} \cdots y_m^{r_m}$$

and therefore,

$$\begin{aligned}
\Phi\left(\sum a_{r_1 \cdots r_m} \overline{y_1}^{r_1} \cdots \overline{y_m}^{r_m}\right) &= \sum a_{r_1 \cdots r_m} \Phi(\overline{y_1}^{r_1} \cdots \overline{y_m}^{r_m}) && k\text{-linearity} \\
&= \sum a_{r_1 \cdots r_m} \Phi(\overline{y_1})^{r_1} \cdots \Phi(\overline{y_m})^{r_m} && \text{ring hom.} \\
&= \sum a_{r_1 \cdots r_m} \overline{f_1}^{r_1} \cdots \overline{f_m}^{r_m} \\
&= g(\overline{f_1}, \ldots, \overline{f_m}) \\
&= \overline{\sum a_{r_1 \cdots r_m} f_1^{r_1} \cdots f_m^{r_m}} \\
&= \overline{g(f_1, \ldots, f_m)} = \overline{g \circ \varphi}.
\end{aligned}$$

To prove that $\varphi(X) \subseteq Y$, we need to check that $\varphi(x) \in Y$ for all $x \in X$, that is, $g(\varphi(x)) = 0$ for all $g \in I(Y)$, that is $g \circ \varphi \in I(X)$ for all $g \in I(Y)$, that is $\overline{g \circ \varphi} = 0$ in $\Gamma(X)$ if $\overline{g} = 0$ in $\Gamma(Y)$.

But, if $\overline{g} = 0$ in $\Gamma(Y)$, then

$$0 = \Phi(0) = \Phi(\overline{g}) = \overline{g \circ \varphi}. \qquad \checkmark$$

We now prove (ii). We wish to check that $\Phi = \varphi^*$. Enough to check that $\Phi(\overline{y_i}) = \varphi^*(\overline{y_i})$ for all $i = 1, \ldots, m$. But,

$$\Phi(\overline{y_i}) \underset{\text{def. of } f_i}{=} \overline{f_i} = \overline{y_i \circ \varphi} \underset{\text{def. of pullback}}{=} \varphi^*(\overline{y_i}).$$ □

2.24 Proposition. Let $\varphi : X \to Y$ be a polynomial map. Then φ is an isomorphism if and only if φ^* is an isomorphism of k-algebras in which case $(\varphi^*)^{-1} = (\varphi^{-1})^*$.

Proof. ($\to$) Suppose that φ has polynomial inverse $\varphi^{-1} : Y \to X$. Then, $\varphi \circ \varphi^{-1} = \mathrm{id}_Y$ and $\varphi^{-1} \circ \varphi = \mathrm{id}_X$. So,

$$(\varphi^{-1})^* \circ \varphi^* = (\varphi \circ \varphi^{-1})^* = (\mathrm{id}_Y)^* = \mathrm{id}_{\Gamma(Y)}$$

and similarly $\varphi^* \circ (\varphi^{-1})^* = \mathrm{id}_{\Gamma(X)}$ and so φ^* is iso with inverse $(\varphi^{-1})^*$. Note that $(\varphi^{-1})^*$ is a k-algebra homomorphism since it is the pullback of a polynomial map.

($\leftarrow$) If φ^* is an isomorphism of k-algebras with inverse Φ, then by the above proposition, $\Phi = \psi^*$ for some (unique!) polynomial map $\psi : Y \to X$. Let us show that $\psi = \varphi^{-1}$. Well,

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^* = \varphi^* \circ (\varphi^*)^{-1} = \mathrm{id}_{\Gamma(Y)} = (\mathrm{id}_Y)^*$$

and thus $\psi \circ \varphi = \mathrm{id}_Y$. Similarly, $\varphi \circ \psi = \mathrm{id}_X$. □

2.25 Corollary. $X \cong Y$ if and only if $\Gamma(X) \cong \Gamma(Y)$ as k-algebras.

Proof. $(\rightarrow)$ If there exists an isomorphism $\varphi : X \to Y$ then $\varphi^* : \Gamma(Y) \to \Gamma(X)$ is an isomorphism.

$(\leftarrow)$ If there exists a k-algebra isomorphism $\Phi : \Gamma(Y) \to \Gamma(X)$ then $\Phi = \varphi^*$ for some isomorphism $\varphi : X \to Y$. □

2.26 Example. Consider $X = V(xy - 1) \subseteq \mathbb{A}^2$. [DIAGRAM OF HYPERBOLA]. Is $X \cong \mathbb{A}^1$? Recall that $\Gamma(\mathbb{A}^1) = k[t]$ and $\Gamma(X) = k[\overline{x}, \overline{x}^{-1}]$. Suppose that $\Gamma(X) \cong \Gamma(\mathbb{A}^1)$ so there exists a k-algebra isomorphism $\Phi : \Gamma(X) = k[\overline{x}, \overline{x}^{-1}] \to k[t] = \Gamma(\mathbb{A}^1)$. In particular, Φ is a surjective ring homomorphism, so that $\Phi(1) = 1$. Thus,

$$\Phi(\overline{x}) \cdot \Phi(\overline{x}^{-1}) = \Phi(\overline{x} \cdot \overline{x}^{-1}) = \Phi(1) = 1.$$

Thus, $\Phi(\overline{x})$ and $\Phi(\overline{x}^{-1})$ are units in $k[t]$. Thus $\Phi(\overline{x}), \Phi(\overline{x}^{-1}) \in k$. Thus $\Phi(\Gamma(X)) = k \subsetneq k[t]$ which is a contradiction. Therefore, $\Gamma(X) \ncong \Gamma(\mathbb{A}^1)$, so in fact $X \ncong \mathbb{A}^1$.

2.27 Exercise. Consider $X = V(y^2 - x^3)$. We have $\Gamma(X) = k[\overline{x}, \overline{y}]$. In the assignment we will prove that $X \ncong \mathbb{A}^1$.

MC 2035 as of Monday, June 17.

2.28 Definition. Recall that a ***k*-algebra** is a ring with a k-vector space structure (e.g. $k[x_1, \dots, x_n]$ or $\Gamma(X)$ with X a variety).

Given a k-algebra A, it is called **finitely generated** if $\exists a_1, \dots, a_m \in A$ such that

$$A = k[a_1, \dots, a_m].$$

Equivalently, A is finitely generated if there exists a surjective k-algebra homomorphism $\varphi : k[x_1, \dots, x_m] \to A$, where $k[x_1, \dots, x_m]$ is the polynomial ring in m variables. [$A = \operatorname{Im}(\varphi) = k[\varphi(x_1), \dots, \varphi(x_m)] = k[a_1, \dots, a_m]$ with $a_i = \varphi(x_i)$.]

2.29 Proposition. Suppose that $k = \overline{k}$ and that A is a finitely generated k-algebra that is an integral domain. Then, there exists a variety X such that $A \cong \Gamma(X)$.

Proof. Since A is finitely generated, there exists a surjective homomorphism $\varphi : k[x_1, \dots, x_m] \to A$. Let $I = \ker \varphi$. Then, by first isomorphism theorem,

$$A \cong k[x_1, \dots, x_m]/I$$

which is a domain, thus I is prime. Set $X = V(I)$. Then, $I(X) = I(V(I)) = I$ since $k = \overline{k}$ and I is prime. Therefore, X is irreducible alg. subset of $\mathbb{A}^m$ with $\Gamma(X) = k[x_1, \dots, x_m]/I \cong A$. □

TABLE HERE

2.3 Rational functions

2.30 Definition. Let $X \subseteq \mathbb{A}^n$ be a variety. Then, $\Gamma(X)$ is a domain and so we can consider its field of fractions, which we will denote $k(X)$ and call the **function field of** X.

Note that an element $f \in k(X)$ may not be defined at every point on X. For example $f = \frac{1}{x}$ on $\mathbb{A}^1$, which is not defined at $x = 0$. However, if we consider $f = \frac{x^2}{x}$ on $\mathbb{A}^1$, this is not defined at $x = 0$, even though it is equal to $\frac{x}{1}$, for all $x \neq 0$, and $\frac{x}{1}$ is defined everywhere. So, we can extend $\frac{x^2}{x}$ to $\mathbb{A}^1$ by considering it equivalent to $\frac{x}{1}$.

2.31 Definition. A rational function $f \in k(X)$ is said to be **regular** at p (or **defined** at p) if f can be written as $\frac{a}{b}$ for some $a, b \in \Gamma(X)$ such that $b(p) \neq 0$. The **value** of f at p is defined to be $\frac{a(p)}{b(p)}$. The set of points where f is defined is called the **domain** of f, denoted $\operatorname{dom}(f)$. A point where f is not defined is called a **pole** of f and the set of all such points is called the **pole set** of f.

2.32 Example. We have:

1. Consider $f = \frac{x}{y}$ on $\mathbb{A}^2$. Then, the pole set of f on $\mathbb{A}^2$ is $\{(x, y) \in \mathbb{A}^2 : y = 0\}$. However, if we consider f on $X = V(x - y^2) \subseteq \mathbb{A}^2$, then in $\Gamma(X)$, $\overline{x} = \overline{y}^2$, so

$$\overline{f} = \frac{\overline{x}}{\overline{y}} = \frac{\overline{y}^2}{\overline{y}} = \overline{y}$$

so it is defined on all of X.

2. Let $f = \frac{(1-\overline{y})}{\overline{x}}$ on $X = V(x^2+y^2-1) \subseteq \mathbb{A}^2$. What is the pole set of f?

   If $\operatorname{char} k = 2$, then $x^2+y^2-1 = (x+y-1)^2$ and $X = V(x+y-1)$. So in $\Gamma(X)$, $\overline{x} = 1-\overline{y}$, thus
$$f = \frac{1-\overline{y}}{\overline{x}} = \frac{\overline{x}}{\overline{x}} = 1$$
   so it is defined on all of X.

   If $\operatorname{char} k \neq 2$, then we claim the pole set is $\{(0,-1)\}$. Note that the expression $\frac{1-\overline{y}}{\overline{x}}$ is defined everywhere except at points on X where $x = 0$, namely $(0,1)$ and $(0,-1)$.

   Consider $(0,1)$:
$$\frac{1-\overline{y}}{\overline{x}} = \frac{1-\overline{y}^2}{\overline{x}(1+\overline{y})} \overset{*}{=} \frac{\overline{x}^2}{\overline{x}(1+\overline{y})} = \frac{\overline{x}}{1+\overline{y}}$$
   which is defined at $(0,1)$ thus $(0,1)$ is not a pole; at * we have used that $\overline{x}^2 = 1-\overline{y}^2$ on X.

   Next consider $(0,-1)$: let's show that it is a pole. Assume instead that it is not a pole, so that there are $a, b \in \Gamma(X)$ such that $f = \frac{a}{b}$ and $b(0,-1) \neq 0$. So,
$$\frac{a}{b} = \frac{1-\overline{y}}{\overline{x}} \iff (1-\overline{y})b = \overline{x}a$$
   Evaluating at $(0,-1)$ we get
$$\underbrace{2}_{\neq 0}\underbrace{b(0,-1)}_{\neq 0} = a(0,-1)\cdot 0 = 0$$
   a contradiction. So $(0,-1)$ is a pole.

2.33 Proposition. Let X be an affine variety. Then the pole set of a rational function on X is an algebraic subset of X.

Proof. Let $f \in k(X)$. Then,
$$(\text{pole set of } f) = X \cap \left(\bigcap_{\substack{b \in k[x_1,\dots,x_n] \\ \text{s.t. } f = \frac{a}{b}}} V(b) \right)$$
which is algebraic since it is the intersection of algebraic sets. □

2.34 Corollary. $\operatorname{dom}(f) = X \setminus (\text{pole set of } f)$ is open in X.

2.35 Remark. If $\operatorname{dom}(f)$ is non-empty and closed in X, then $\operatorname{dom}(f) = X$. Indeed, if $\operatorname{dom}(f) \neq \varnothing$ and closed, then
$$X = \underbrace{\operatorname{dom}(f)}_{\text{closed}} \cup \underbrace{(X \setminus \operatorname{dom}(f))}_{\substack{\text{closed in } X \\ (\text{since } \operatorname{dom}(f) \text{ is open})}}$$
Since X is irreducible, we must have $\operatorname{dom}(f) = \varnothing$ or $X \setminus \operatorname{dom}(f) = \varnothing$, thus $X \setminus \operatorname{dom}(f) = \varnothing$ since we assumed $\operatorname{dom}(f) \neq \varnothing$. So $\operatorname{dom}(f) = X$.

We saw that polynomial functions are continuous in the Zariski topology on X. A similar result holds for rational functions on X.

2.36 Proposition. If $X \subseteq \mathbb{A}^n$ is a variety and $f \in k(X)$, then f is continuous with respect to the Zariski topology on $\operatorname{dom}(f)$ and the Zariski topology on $k \simeq \mathbb{A}^1$ (note: $f : X \to k \simeq \mathbb{A}^1$).

Proof. Exercise. □

2.37 Proposition. Let $X \subseteq \mathbb{A}^n$ be a variety. If $f \in k(X)$ is zero on a non-empty open set $U \subseteq X$, then f is zero on all X.

[Editor's note: $f^{-1}(\{0\})$ contains some non-empty open subset of X, but those are dense, so $\overline{f^{-1}(\{0\})}$ (which is equal to $f^{-1}(\{0\})$ by continuity of f) is everything. This can probably be made rigorous, and it's more elegant than what's below, which seems to try to avoid invoking continuity of rational functions.]

Proof. Choose $p \in U \neq \varnothing$. Since f is defined at p (because it is zero there), there exist $\overline{a}, \overline{b} \in \Gamma(X)$ with $b(p) \neq 0$ and $f = \overline{a}/\overline{b}$. Let $V = X \setminus V(b)$. Then V is open in X. Also $p \in U \cap V$ thus $U \cap V \neq \varnothing$ and open in X. Since X is irreducible, we have $\overline{U \cap V} = X$. Since $f = \overline{a}/\overline{b}$ and $b \neq 0$ on V and so on $U \cap V$, since $f \equiv 0$ on U, we must have that $a \equiv 0$ on $U \cap V$ and since polynomial functions are continuous in the Zariski topology, we see $a \equiv 0$ on $\overline{U \cap V} = X$ thus $f = \overline{0}/\overline{b} = 0$ and thus $f \equiv 0$ on X. □

2.38 Corollary (Identity theorem). If $f, g \in k(x)$ are such that $f = g$ on a non-empty open subset U of X, then $f = g$ on X.

Proof. Apply the proposition to $f - g$. □

2.39 Remark. The corollary tells us that rational functions are completely determined by their restriction to some open set.

2.4 Rational maps

2.40 Definition. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties. A map $\varphi : X \to Y$ such that

$$\varphi(x) = (f_1(x), \dots, f_m(x))$$

where $f_1, \dots, f_m \in k(X)$ is called a **rational map**. If $p \in X$ is such that f_i is defined at p, for all $i = 1, \dots, m$, then p is a **regular point of** φ. The set of all points where φ is defined is the domain of φ:

$$\mathrm{dom}(\varphi) = \mathrm{dom}(f_1) \cap \ldots \cap \mathrm{dom}(f_m) \implies \mathrm{dom}(\varphi) \text{ is open in } X.$$

2.41 Example. We have:

1. Rational functions $f : X \to k = \mathbb{A}^1$ are rational maps
2. Polynomial functions are rational maps
3. Let $X = V(y^2 - x^3) \subseteq \mathbb{A}^2$. Then,
$$\psi : X \to \mathbb{A}^1, \qquad (x, y) \mapsto y/x$$
is a rational map with poles at points on X where $x = 0$, i.e. at $(0, 0)$.

2.42 Definition. A rational map $\varphi : X \to Y$ is called **dominant** if $\overline{\varphi(X)} = Y$.

2.43 Example. The map $\varphi : X = V(y^2 - x^3) \subseteq \mathbb{A}^2 \to \mathbb{A}^1$, $(x, y) \mapsto y/x$ is dominant since $\varphi(X) = \mathbb{A}^1 - \{(0, 0)\}$ and $\overline{\varphi(X)} = \overline{\mathbb{A}^1 - \{0\}} = \mathbb{A}^1$.

Consider two rational maps $\varphi : X \to Y$ and $\psi : Y \to Z$. When can one compose ψ with φ? In order for $\psi \circ \varphi$ to be defined, need $\varphi(X) \cap \mathrm{dom}(\psi) \neq \varnothing$.

2.44 Proposition. If $\varphi : X \to Y$ is dominant, then $\varphi(X) \cap \mathrm{dom}(\psi) \neq \varnothing$.

Proof. If $\mathrm{dom}(\psi) = Y$ we are OK. Suppose that $\mathrm{dom}(\psi) \subsetneq Y$. This means in particular that $\mathrm{dom}(\psi)$ is proper open subset of Y and $Y \setminus \mathrm{dom}(\psi)$ is closed in Y. Suppose that $\varphi(X) \cap \mathrm{dom}(\psi) = \varnothing$. Then

$$\varphi(X) \subseteq Y \setminus \mathrm{dom}(\psi) \implies \overline{\varphi(X)} \subseteq \overline{Y \setminus \mathrm{dom}(\psi)} = Y \setminus \mathrm{dom}(\psi) \neq Y.$$

This is impossible since we assume φ to be dominant, so that $\overline{\varphi(X)} = Y$. Thus, $\varphi(X) \cap \mathrm{dom}(\psi) \neq \varnothing$. □

2.45 Definition. A dominant rational map $\varphi : X \to Y$ is **birational** or a **birational equivalence** if φ has an inverse rational map that is also dominant. In this case, X and Y are said to be **birationally equivalent** (or **birational**), denoted $X \sim Y$.

2.46 Example. We have:

1. Isomorphisms are birational equivalences.
2. Let $X = V(xy - 1) \subseteq \mathbb{A}^2$. The map $\varphi : X \to \mathbb{A}^1$ given by $(x, y) \mapsto x$ is a rational map, with rational inverse
$$\varphi^{-1} : \mathbb{A}^1 \to X, \qquad t \mapsto (1/t)$$
therefore $X \sim \mathbb{A}^1$.

2.47 Remark. We have:

1. $\Gamma(X) = k[\overline{x}, \overline{x}^{-1}]$ thus $k(X) = k(\overline{x}) \cong k(t) = k(\mathbb{A}^1)$ because $\Gamma(\mathbb{A}^1) = k[t]$.
2. φ is dominant since $\varphi(X) = \mathbb{A}^1 - 0$ thus $\overline{\varphi(X)} = \mathbb{A}^1$. φ^{-1} is only defined on $\mathbb{A}^1 - 0$ and $\varphi^{-1}(\mathbb{A}^1) = X$ implies φ^{-1} is dominant.

2.48 Definition. A variety X is called **rational** if $X \sim \mathbb{A}^m$ for some m.

2.49 Example. $X = V(xy - 1)$ is rational since $X \sim \mathbb{A}^1$.

As of Monday June 17, lectures are in MC 2035.

For a given rational map $\varphi : X \to Y$, can we define a pullback

$$\varphi^* : k(Y) \to k(X) \qquad f \mapsto f \circ \varphi?$$

Well,

- $f \circ \varphi$ needs to be defined, for all $f \in k(Y)$
- φ^* should be a homomorphism of fields and therefore injective.

Can always do it if $\varphi : X \to Y$ is dominant (that is, $\overline{\varphi(X)} = Y$). Indeed, set

$$\varphi^* : \Gamma(Y) \to k(X) \qquad \overline{a} \mapsto \overline{a \circ \varphi}$$

Then:

- φ^* is well-defined since φ is rational (so that $\overline{a \circ \varphi} \in k(X)$) and also $a \circ \varphi$ is defined (because φ is dominant).
- $\varphi^* : \Gamma(Y) \to k(X)$ is injective because $\overline{\varphi(X)} = Y$:

$$\varphi^*(\overline{a}) = 0 \implies \overline{a \circ \varphi} = 0 \text{ in } k(X) \implies a \circ \varphi = 0 \text{ on } X \implies a(\varphi(p)) = 0 \text{ for all } p \in X$$

and thus

$$a \in I(\varphi(X)) = I(\underbrace{V(I(\varphi(X)))}_{\overline{\varphi(X)}=Y}) = I(Y) \implies \overline{a} = 0 \text{ in } \Gamma(Y)$$

Now, we extend φ^* to $k(Y)$ as follows: $\varphi^* : k(Y) \to k(X)$ is given by

$$\frac{\overline{a}}{\overline{b}} \mapsto \frac{\varphi^*(\overline{a})}{\varphi^*(\overline{b})}$$

and here $\overline{b} \neq 0$ and $\varphi^*(\overline{b}) \neq 0$. This is an injective homomorphism.

We get the same "fully faithful functor" properties as for pullbacks of polynomial maps:

(i) $(\mathrm{id}_X)^* = \mathrm{id}_{k(X)}$.

(ii) If $\varphi : X \to Y$ and $\psi : Y \to Z$ are dominant rational maps, then

$$(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$$

and $\varphi^* : k(Y) \to k(X)$ is an injective k-algebra homomorphism.

(iii) If $\Phi : k(Y) \to k(X)$ is an injective k-algebra homomorphism, then there exists a unique dominant rational map $\varphi : X \to Y$ such that $\Phi = \varphi^*$.

These give:

2.50 Theorem. $X \sim Y$ if and only if $k(X) \cong k(Y)$ as k-algebras.

Proof. See notes. □

2.51 Example. $X = V(y^2 - x^3) \subseteq \mathbb{A}^2$. Then $X \sim \mathbb{A}^1$ because

$$\varphi : \mathbb{A}^1 \to X \qquad t \mapsto (t^2, t^3)$$

is a surjective polynomial map and therefore a dominant rational map. Moreover, φ has rational inverse

$$\varphi^{-1} : X \subseteq \mathbb{A}^2 \to \mathbb{A}^1 \qquad (x, y) \mapsto y/x$$

which is dominant (since $\varphi^{-1}(X) = \mathbb{A}^1 - 0$ thus $\overline{\varphi^{-1}(X)} = \mathbb{A}^1$).

Then, this gives the following isomorphism between $k(X) = k(\overline{x}, \overline{y})$ and $k(\mathbb{A}^1) = k(t)$:

$$(\varphi^{-1})^* : k(\mathbb{A}^1) = k(t) \to k(\overline{x}, \overline{y}) = k(X) \qquad t \mapsto \overline{t \circ \varphi^{-1}} = \frac{\overline{y}}{\overline{x}} \implies k(\overline{x}, \overline{y}) = k(\overline{y}/\overline{x}) \cong k(t).$$

2.52 Definition. A **quasi-affine variety** in $\mathbb{A}^n$ is an open subset U of a variety $X \subseteq \mathbb{A}^n$ (i.e. $U \subseteq X \subseteq \mathbb{A}^n$ and U is open).

Then:

- $\overline{U} = X$ since X is irreducible.
- $I(U) = I(\underbrace{V(I(U))}_{=\overline{U}}) = I(\overline{U}) = I(X)$ which is prime.
- Can define
$$\Gamma(U) := \frac{k[x_1, \dots, x_n]}{I(U)} \left(= \frac{k[x_1, \dots, x_n]}{I(X)} = \Gamma(X) \right) = \text{polynomial fcts on } U$$
and
$$k(U) = \text{fraction field of } \Gamma(U), \text{ defined since } \Gamma(U) \text{ is a domain} = \text{rational fcts on U}$$
Note that $k(U) = k(X)$.

2.5 Dimension

2.53 Definition. Let $X \subseteq \mathbb{A}^n$ be a variety. Then the **dimension** of X, denoted $\dim X$, is defined as the transcendence degree of $k(X)$ over k. Similarly, if $U \subseteq \mathbb{A}^n$ is a quasi-affine variety, then the **dimension** of U is defined as the transcendence degree of $k(U)$ over k, denoted $\dim U$.

2.54 Remark. If $U \subseteq X$ with X a variety in $\mathbb{A}^n$ then $k(U) = k(X)$, so that
$$\dim U = \dim X.$$

Therefore dimension is a local property.

Let us recall the definition and some properties of the transcendence degree. Let K be a field and k be a subfield of K.

2.55 Definition. A subset $U \subseteq K$ is **algebraically independent over** k if for all $n \geq 1$, and for all $0 \neq a \in k[t_1, \dots, t_n]$, we have
$$a(u_1, \dots, u_n) \neq 0$$
for every $u_1, \dots, u_n \in U$. A **transcendence basis of** K **over** k is an algebraically independent subset of K that is maximal with respect to inclusion.

2.56 Example. We have:

(i) $\varnothing \subseteq K$ is algebraically independent over k.

(ii) If $K = k$, then $\varnothing$ is a transcendence basis for K over k, i.e. of k over K, because any $\alpha \in k$ is such that $a(\alpha) = 0$ with $a(t) = t - \alpha \neq 0$ and $a(t) \in k[t]$.

(iii) If $K = k(x_1, \dots, x_n)$, then $\{x_1, \dots, x_n\}$ is a transcendence basis of K over k.

Proof. Well, $\{x_1, \dots, x_n\}$ is certainly algebraically independent because if $a \in k[t_1, \dots, t_n]$ is such that $a(x_1, \dots, x_n) = 0$ then $a = 0$. To show that $\{x_1, \dots, x_n\}$ is a maximal algebraically independent set over k, let $0 \neq u \in k(x_1, \dots, x_n)$. Then, $u = p/q$ for some $p, q \in k[x_1, \dots, x_n]$. Let $f \in k[t_1, \dots, t_{n+1}]$ be given by
$$f(t_1, \dots, t_n) = p(t_1, \dots, t_n) - t_{n+1}q(t_1, \dots, t_n).$$
Then, $f \neq 0$ and $f(x_1, \dots, x_n, u) = 0$ therefore $\{x_1, \dots, x_n, u\}$ is algebraically dependent, so that $\{x_1, \dots, x_n\}$ is maximal. □

2.57 Theorem. We have:

(i) every algebraically independent $U \subseteq K$ is contained in a transcendence basis. In particular, since $\varnothing$ is an algebraically independent set, K has at least one transcendence basis.

(ii) any two transcendence bases have the same cardinality.

2.58 Definition. The **transcendence degree** of K over k is the cardinality of any transcendence basis of K over k. It is denoted $\operatorname{trdeg}_k K$.

This is telling us points have dimension 0 (not surprising) and affine n-space has dimension n.

A few more problems will be posted. The next assignment is due in two weeks.

We assume $k = \overline{k}$.

2.59 Definition. Let $X \subseteq \mathbb{A}^n$ be a variety. The **dimension of** X is $\operatorname{trdeg}_k(X)$, denoted $\dim X$. If $Y \subseteq X$ is a subvariety of X, then the **codimension of** Y **in** X is

$$\operatorname{codim}_X Y := \dim X - \dim Y.$$

2.60 Example. We have:

1. If $K = k$, then $\varnothing$ is a transcendence basis for k over k. So,

$$\operatorname{trdeg}_k k = 0.$$

2. If $K = k(x_1, \dots, x_n)$, then $\{x_1, \dots, x_n\}$ is a transcendence basis for K over k. So

$$\operatorname{trdeg}_k k(x_1, \dots, x_n) = n.$$

2.61 Definition. A variety of dimension 1 is a **curve**, of dimension 2 is a **surface**, of dimension n is an n**-fold**.

We have a similar definition for quasi-affine varieties.

2.62 Example. We have:

1. $\dim \mathbb{A}^n = n$ since $k(\mathbb{A}^n) = k(x_1, \dots, x_n)$.
2. $\dim(\{\text{pt}\}) = 0$ since $k(\{\text{pt}\}) = k$ (because $\Gamma(\{\text{pt}\}) = k$).

$$\operatorname{codim}_{\mathbb{A}^n}\{\text{pt}\} = \dim \mathbb{A}^n - \dim\{\text{pt}\} = n - 0 = n.$$

2.63 Theorem. If Y is a proper subvariety of $X \subseteq \mathbb{A}^m$, then $\dim Y < \dim X$.

The following proof is fixed in the course notes.

Proof. Suppose that $\dim X = n$ and $(x_1, \dots, x_m)$ are coordinates in $\mathbb{A}^m$. Then any $(n+1)$ distinct coordinate functions $x_{i_1}, \dots, x_{i_{n+1}}$ are alg dep over X, i.e. $\{\overline{x_{i_1}}, \dots, \overline{x_{i_{n+1}}}\}$ is alg dep in $\Gamma(X)$. So, there exists $0 \neq a \in k[t_1, \dots, t_{n+1}]$ such that

$$a(\overline{x_{i_1}}, \dots, \overline{x_{i_{n+1}}}) = 0 \text{ in } \Gamma(X) \implies a(\overline{x_{i_1}}, \dots, \overline{x_{i_{n+1}}}) \in I(X) \subseteq I(Y) \text{ since } Y \subsetneq X$$

Therefore $a(\overline{x_{i_1}}, \dots, \overline{x_{i_{n+1}}}) = 0$ in $\Gamma(Y)$, implying $\{\overline{x_{i_1}}, \dots, \overline{x_{i_{n+1}}}\}$ is alg dep in $k(Y)$, and thus

$$\underbrace{\operatorname{trdeg}_k k(Y)}_{=\dim Y} < n+1 \implies \dim Y \leq n.$$

We want to show that in fact $\dim Y < n = \dim X$. Suppose instead that $\dim Y = n$. We'll see that this forces $Y = X$ because we'll have that

$$I(Y) = I(X)$$

so $Y = V(I(Y)) = V(I(X)) = X$ where the first and last equalities follow since X, Y are algebraic.

Since $\dim Y = n$ and $k(Y) = k(\overline{x_1}, \dots, \overline{x_m})$, there exist n of the $\overline{x_i}$ that are alg indep, say,

$$\overline{x_{i_1}}, \dots, \overline{x_{i_n}}.$$

Then, $\{\overline{x_{i_1}}, \dots, \overline{x_{i_n}}\}$ is also alg dep over X (otherwise, as we've just seen, if $\{\overline{x_{i_1}}, \dots, \overline{x_{i_n}}\}$ is alg dep over X, it is alg dep over Y). Since $\dim X = n$, if $0 \neq u \in \Gamma(X)$, the set $\{\overline{x_{i_1}}, \dots, \overline{x_{i_n}}, u\}$ is alg dep over X. So, there is $0 \neq a \in k[t_1, \dots, t_{n+1}]$ such that

$$a(x_{i_1}, \dots, x_{i_n}, u) = 0 \text{ in } k(X).$$

Note that $a(\overline{x_{i_1}}, \dots, \overline{x_{i_n}}, u) \in \Gamma(X)$, so that

$$a(\overline{x_{i_1}}, \dots, \overline{x_{i_n}}, u) \in I(X).$$

Since $I(X)$ is prime, can assume that a is irreducible. Also,

$$a(\overline{x_{i_1}},\ldots,\overline{x_{i_n}},u) = a_k(\overline{x_{i_1}},\ldots,\overline{x_{i_n}})n^k + \ldots + a_1(\overline{x_{i_1}},\ldots,\overline{x_{i_n}})u + a_0(\overline{x_{i_1}},\ldots,\overline{x_{i_n}}) = 0$$

therefore $a_0(\overline{x_{i_1}},\ldots,\overline{x_{i_n}}) \neq 0$ in $\Gamma(X)$, otherwise $a(\overline{x_{i_1}},\ldots,\overline{x_{i_n}},u)$ would be reducible.

Let us show that we must have $u \neq 0$ in $\Gamma(Y)$. Suppose instead that $u = 0$ in $\Gamma(Y)$. Then,

$$a_0(\overline{x_{i_1}},\ldots,\overline{x_{i_n}}) = a(\overline{x_{i_1}},\ldots,\overline{x_{i_n}}) = 0 \text{ on } Y.$$

But, a_0 is not the zero polynomial, since

$$a_0(\overline{x_{i_1}},\ldots,\overline{x_{i_n}}) \neq 0 \text{ in } \Gamma(X).$$

Thus $\overline{x_{i_1}},\ldots,\overline{x_{i_n}}$ are alg dep over Y, a contradiction. So, $u \neq 0$ in $\Gamma(Y)$. We thus have

$$u \neq 0 \text{ in } \Gamma(X) \implies u \neq 0 \text{ in } \Gamma(Y)$$

which is equivalent to

$$u \notin I(X) \implies u \notin I(Y)$$

which is equivalent to

$$u \in I(Y) \implies u \in I(X)$$

which is equivalent to

$$I(Y) \subseteq I(X).$$

Thus, $I(Y) = I(X)$ because $I(X) \subseteq I(Y)$ (since $Y \subsetneq X$). □

2.64 Corollary. Let X be a variety. Then $\dim X = 0$ if and only if $X = \{\text{pt}\}$.

Proof. We have already seen that $\dim\{\text{pt}\} = 0$. Suppose that $\dim X = 0$, but $X \neq \{\text{pt}\}$. Then, X has more than one point, implying that, if $p \in X$,

$$\underbrace{\{p\}}_{\text{irred.}} \subsetneq X \implies 0 = \dim\{p\} < \dim X = 0,$$

a contradiction. □

2.65 Example. Let X be an irreducible curve in $\mathbb{A}^2$, so that $X = V(f)$ with f an irreducible polynomial in $k[x,y]$. Then $\dim X = 1$. Indeed, $k(X) = k(\overline{x},\overline{y})$ with $\overline{x},\overline{y}$ satisfying the algebraic relation

$$f(\overline{x},\overline{y}) = 0.$$

Therefore $\{\overline{x},\overline{y}\}$ is algebraically dependent in $k(X)$. So $\dim X < 2$. But $\dim X > 0$, since X has more than one point. Thus $\dim X = 1$. Note $\operatorname{codim}_{\mathbb{A}^2} X = 2 - 1 = 1$.

In general, we have the following.

2.66 Theorem. Suppose $k = \overline{k}$. Let $f \in k[x_1,\ldots,x_n]$ be a non-constant irreducible polynomial. Then $\varnothing \neq V(f) \subsetneq \mathbb{A}^n$ and $V(f)$ is a subvariety of $\mathbb{A}^n$ of codimension 1, i.e. $\dim \mathbb{A}^n - \dim V(f) = 1$ thus $\dim V(f) = n-1$.

Proof. Let $X = V(f)$. Since f is non-constant at least one of x_i appears in the expression of f, say x_n. Then, $\overline{x_1},\ldots,\overline{x_{n-1}}$ are alg indep in $k(X)$. Indeed, if they are not, there is $0 \neq a \in k[t_1,\ldots,t_{n-1}]$ such that

$$a(\overline{x_1},\ldots,\overline{x_{n-1}}) = 0 \text{ in } k(X).$$

But $a(\overline{x_1},\ldots,\overline{x_{n-1}}) \in \Gamma(X)$, so that

$$a(\overline{x_1},\ldots,\overline{x_{n-1}}) = 0 \text{ in } \Gamma(X)$$

if and only if $a(x_1,\ldots,x_{n-1}) \in I(X) = I(V(f))$ which is $\langle f \rangle$ since $k = \overline{k}$ and f is irreducible. Thus $f \mid a(x_1,\ldots,x_{n-1})$ thus x_n must appear in the expression of $a(x_1,\ldots,x_{n-1})$ which is impossible.

So, $\{\overline{x_1},\ldots,\overline{x_{n-1}}\}$ is alg indep in $k(X)$. Hence,

$$\dim X \geq n-1.$$

Thus, since $X \subsetneq \mathbb{A}^n$,

$$n-1 \leq \dim X < \dim \mathbb{A}^n = n \implies \dim X = n-1.$$ □

What happens if we consider a hypersurface in a variety X other than $\mathbb{A}^n$? I.e. if f is a non-constant irreducible polynomial that is not constantly zero on X (i.e. $\overline{f} \neq 0$ in $\Gamma(X)$), do we have

$$\dim(X \cap V(f)) = \dim X - 1?$$

2.67 Example. Consider $X = V(y - x^2) \subseteq \mathbb{A}^2$. By the previous theorem, $\dim X = \dim \mathbb{A}^2 - 1 = 1$. Take $f = y - 1 \in k[x, y]$. Then

$$X \cap V(f) = \{(1, 1), (1, -1)\}$$

Even though $f = y - 1$ is irreducible, $X \cap V(f)$ is reducible. Nonetheless, the irreducible components of $X \cap V(f)$, namely $\{(1, 1)\}$ and $\{(-1, 1)\}$ have $\dim = 0$, so codim. 1 in X.

In general, we have:

2.68 Theorem. Let $k = \overline{k}$. Let $X \subseteq \mathbb{A}^n$ be an affine variety and $f \in k[x_1, \ldots, x_n]$ be an irreducible polynomial such that

$$0 \neq V(f) \cap X \neq X$$

(i.e. $\overline{f}$ is nonconstant in $\Gamma(X)$). Then each of the irreducible components of $V(f) \cap X$ has codimension 1 in X.

Proof. See course notes or Mumford's book. □

2.69 Remark. This result is the geometric version of Krull's principal ideal theorem.

So, this tells us that dimension for varieties behaves like dimension for linear systems. We have the following.

2.70 Corollary. If $Y \subsetneq X \subsetneq \mathbb{A}^n$ subvariety has codimension r in X, then there exist subvarieties $Y_0, \ldots, Y_r$ of X of codimension $0, 1, \ldots, r$ in X, resp., such that

$$Y = Y_r \subsetneq Y_{r_1} \subsetneq \ldots \subsetneq Y_1 \subsetneq Y_0 = X$$

(dimension jumps by 1 at each step).

Proof. Induction on r. If $r = 1$, then

$$Y = Y_1 \subsetneq Y_0 = X$$

(Y has codim 1 in X). If $r > 1$, since $Y \subsetneq X$, then $I(X) \subsetneq I(Y)$. Then there exists $f \in I(Y)$ such that $f \notin I(X)$. Since $I(Y)$ is prime we may assume that f is irreducible. Also, $Y \subseteq V(f)$ since $f \in I(Y)$, but

$$V(f) \cap X \neq X$$

because $f \notin I(X)$. So, by the previous theorem, every irreducible component of $V(f) \cap X$ has codimension 1 in X. But $Y \subseteq V(f) \cap X$ and Y is irreducible, so Y is contained in one of the irreducible components of $V(f) \cap X$, say Y_1.

$$Y \subsetneq Y_1 \subsetneq Y_0 = X$$

with Y_1 of codim 1 in Y_0. Repeat the process with Y and Y_1 etc., to get

$$Y = Y_r \subsetneq \ldots \subsetneq Y_1 \subsetneq Y_0 = X.$$ □

For topological spaces, it's the longest sequence of strict inclusions of irreducible closed subsets. That's how you define the dimension of a topological space.

2.71 Corollary (topological characterization of dimension). The dimension of an affine variety X is the largest integer d for which there exists a chain of subvarieties

$$\varnothing \neq X_0 \subsetneq X_1 \subsetneq X_2 \subsetneq \ldots \subsetneq X_{d-1} \subsetneq X_d = X$$

Proof. Apply above corollary to $Y = \{p\}$ where p is a point in X, and X. □

2.72 Definition. The **Krull dimension** of a ring R is defined as the length of the longest chain of prime ideals in R under strict inclusion in R.

In $\Gamma(X)$, prime ideals correspond to prime ideals in $k[x_1, \ldots, x_n]$ that contain $I(X)$. So, given a strict chain of prime ideals

$$(0) \subsetneq I_1 \subsetneq \ldots \subsetneq I_d$$

in $\Gamma(X)$, we have a corresponding strict chain of prime ideals in $k[x_1, \ldots, x_n]$,

$$I(X) \subsetneq J_1 \subsetneq \ldots \subsetneq J_d.$$

In turn, by taking zero sets, this corresponds to the strict chain of subvarieties of X:

$$\underbrace{V(J_d)}_{X_d} \subsetneq \underbrace{V(J_{d-1})}_{X_{d-1}} \subsetneq \ldots \subsetneq \underbrace{V(J_1)}_{X_1} \subsetneq X$$

Thus $\dim X$ is the Krull dimension of $\Gamma(X)$.

3 Local properties of affine varieties

Assume $k = \overline{k}$.

3.1 Local rings

3.1 Definition. Let X be a variety and $p \in X$. We define the **local ring of** X **at** p by

$$\mathcal{O}_p(X) := \{f \in k(X) : f \text{ is defined at } p\}.$$

So, $\mathcal{O}_p(X) \subseteq k(X)$ and $\Gamma(X)$ is a subring of $\mathcal{O}_p(X)$:

$$\Gamma(X) \subseteq \mathcal{O}_p(X) \subseteq k(X).$$

We also define the **maximal ideal of** X **at** p by

$$M_p(X) := \{f \in \mathcal{O}_p(X) : f(p) = 0\}.$$

3.2 Remark. Recall that a ring R is called **local** if it admits a unique maximal ideal.

Why is $M_p(X)$ maximal? Consider the evaluation homomorphism

$$\begin{aligned} \mathrm{ev} : \mathcal{O}_p(X) &\to k \\ f &\mapsto f(p). \end{aligned}$$

Then $M_p(X) = \ker(\mathrm{ev})$, so that

$$\frac{\mathcal{O}_p(X)}{M_p(X)} \cong k$$

which is a field, thus $M_p(X)$ is maximal. Also,

$$M_p(X) = \{f \in \mathcal{O}_p(X) : f \text{ is not a unit}\}.$$

This means $M_p(X)$ is the only maximal ideal in $\mathcal{O}_p(X)$, because no proper ideal of $\mathcal{O}_p(X)$ can contain units. We conclude that $\mathcal{O}_p(X)$ is a local ring and $M_p(X)$ is its maximal ideal.

The local rings $\mathcal{O}_p(X)$ capture local properties of a variety.

3.3 Theorem. $\mathcal{O}_p(X)$ is Noetherian.

Proof. Let $J \subseteq \mathcal{O}_p(X)$ be an ideal. Let us show that J is finitely generated. Since $\Gamma(X) \subseteq \mathcal{O}_p(X)$, we can consider $J \cap \Gamma(X)$, which is now an ideal in $\Gamma(X)$. But $\Gamma(X)$ is Noetherian, so that $J \cap \Gamma(X)$ is finitely generated:

$$J \cap \Gamma(X) = (f_1, \ldots, f_r), \qquad f_1, \ldots, f_r \in \Gamma(X).$$

Let $f \in J$. Let us show that $f = c_1 f_1 + \ldots + c_r f_r$ for $c_1, \ldots, c_r \in \mathcal{O}_p(X)$. Since $f \in J \subseteq \mathcal{O}_p(X)$, f is defined at p. Hence there exists $a, b \in \Gamma(X)$ such that $f = \frac{a}{b}$ and $b(p) \neq 0$. Thus, $bf = a$ with $a \in \Gamma(X)$ and $bf \in J$ since J is an ideal, so $bf \in J \cap \Gamma(X)$. Hence, $bf = a_1 f_1 + \ldots + a_r f_r$ for some $a_1, \ldots, a_r \in \Gamma(X)$, so

$$f = c_1 f_1 + \ldots + c_r f_r$$

with each $c_i = \frac{a_i}{b}$ and $b(p) \neq 0$. Thus $c_i \in \mathcal{O}_p(X)$. Hence J is generated by $f_1, \ldots, f_r$ in $\mathcal{O}_p(X)$. □

3.4 Definition. The **ring of regular functions on** X is defined by

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

recalling that all the $\mathcal{O}_p(X)$ are subrings of $k(X)$. $\mathcal{O}(X)$ is the set of functions that are defined (i.e. regular) at every $p \in X$. An element of $\mathcal{O}(X)$ is called a **regular function**. Clearly $\Gamma(X) \subseteq \mathcal{O}(X)$. In fact, we have the following.

3.5 Theorem. $\mathcal{O}(X) = \Gamma(X)$.

Proof. We just need to show that $\mathcal{O}(X) \subseteq \Gamma(X)$. Let $f \in \mathcal{O}(X)$ and define

$$J_f = \{g \in k[x_1, \dots, x_n] : \overline{g}f \in \Gamma(X)\}.$$

Note that J_f is an ideal of $k[x_1, \dots, x_n]$: it is clearly closed under addition, and if $g \in J_f$ and $h \in k[x_1, \dots, x_n]$, then $\overline{hg}f = \overline{h}(\overline{g}f) \in \Gamma(X)$. Moreover, $I(X) \subseteq J_f$ (because if $g \in I(X)$, then $\overline{g} = 0$). Hence,

$$V(J_f) \subseteq V(I(X)) \overset{*}{=} X$$

where (*) holds because X is algebraic. But J_f is the set of all possible denominators of a representation $\frac{a}{b}$ of f, so

$$V(J_f) = \left(\bigcap_{f=\frac{a}{b}} V(b)\right) \cap X = \text{pole set of } f.$$

However, f has no poles since it is regular and therefore defined at every point of X. Hence, $V(J_f) = \varnothing$, thus

$$k[x_1, \dots, x_n] = I(\varnothing) = I(V(J_f)) = \sqrt{J_f}$$

where we have used the Nullstellensatz in the last equality ($k = \overline{k}$). Hence in particular $1 \in \sqrt{J_f}$ so $1 \in J_f$. □

3.6 Remark (NOTATION). Let R, S be two rings with identity such that $R \subseteq S$. Let $I \subseteq R$ be an ideal. Then IS denotes the ideal in S generated by I. Of course, $I \subseteq IS$, but the inclusion may be strict.

Ideal structure of $\mathcal{O}_p(X)$

Since $\Gamma(X) \subseteq \mathcal{O}_p(X)$, we have the following correspondence between ideals in $\Gamma(X)$ and ideals in $\mathcal{O}_p(X)$:

$$I \mapsto I\mathcal{O}_p(X)$$
$$J \cap \Gamma(X) \hookleftarrow J$$

In general, this correspondence is not one-to-one. For example, suppose that $I \subsetneq \Gamma(X)$ is such that there exists $f \in I$ with $f(p) \neq 0$. Then since $f(p) \neq 0$, f is a unit in $\mathcal{O}_p(X)$, so that $I\mathcal{O}_p(X) = \mathcal{O}_p(X)$. Thus,

$$I \mapsto I\mathcal{O}_p(X) = \mathcal{O}_p(X)$$
$$I \neq \Gamma(X) = I\mathcal{O}_p(X) \cap \Gamma(X) \hookleftarrow I\mathcal{O}_p(X).$$

If we hope to get a one-to-one correspondence, we must only consider ideals I whose elements vanish at p. So, if $M_p = I(\{p\}) \subseteq \Gamma(X)$, we need $I \subseteq M_p$.

One can show that if $P \subseteq M_p \subseteq \Gamma(X)$ is prime, then $P\mathcal{O}_p(X) \cap \Gamma(X) = P$, giving a 1:1 correspondence between prime ideals in $\Gamma(X)$ contained in M_p and prime ideals in $\mathcal{O}_p(X)$. One can also use this 1:1 correspondence to show that $\Gamma(X)$ and $\mathcal{O}_p(X)$ have the same Krull dimension:

$$\dim X = \text{Krull dimension of } \mathcal{O}_p(X).$$

3.2 Multiple points and tangent lines

Affine plane curves

Recall that we defined a *plane curve* as the zero set in $\mathbb{A}^2$ of a polynomial $f \in k[x, y]$. If f is reducible, say

$$f = f_1^{m_1} \cdots f_r^{m_r}, \qquad f_1, \dots, f_r \text{ irreducible in } k[x, y],$$

then

$$V(f) = V(f_1) \cup \ldots \cup V(f_r).$$

This shows that we lose information by taking the zero set $V(f)$ of f. For example, $V(y^2) = V(y)$. However, it is useful in application to keep track of the multiplicites $m_1, \ldots, m_r$ if $\{f = 0\}$ represents the zero or the pole set of a rational function, or if $\{f = 0\}$ is the set of intersection of two varieties, etc. This motivates the following.

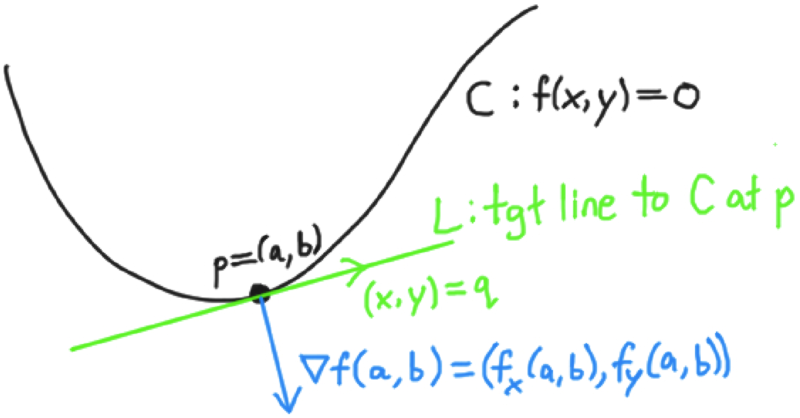
3.7 Definition. We define an **affine plane curve** to be an equivalence class of polynomials, where

$$f \sim g \iff f = \lambda g \text{ for some } \lambda \in k^*$$

(and *not* "$f \sim g \iff V(f) = V(g)$"). Of course, if f is irreducible, then $V(f)$ is a variety in $\mathbb{A}^2$.

Tangent lines

Let C be a curve given by the polynomial $f \in k[x, y]$, and $p = (a, b) \in C$ be a point.



Recall that the tangent line to C at $p = (a, b)$ is given by the equation

$$L : \nabla f(a, b) \cdot \underbrace{((x, y) - (a, b))}_{\overrightarrow{pq}} = 0 \iff \nabla f(a, b) \perp \overrightarrow{pq}$$

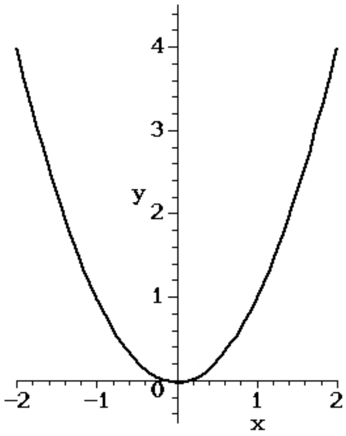
$$\iff L : f_x(a, b)(x - a) + f_y(a, b)(y - b) = 0.$$

L is a line if and only if $\nabla f(a, b) \neq 0$. Thus C has a tangent line at $p = (a, b)$ iff $\nabla f(a, b) \neq 0$.

3.8 Definition. In this case p is called a **smooth** (or **simple**) point of C. Otherwise (i.e. if $\nabla f(a, b) = 0$), the point $p = (a, b)$ is called **singular**. The curve C is called **smooth** if every point on C is smooth.

3.9 Example. We have:

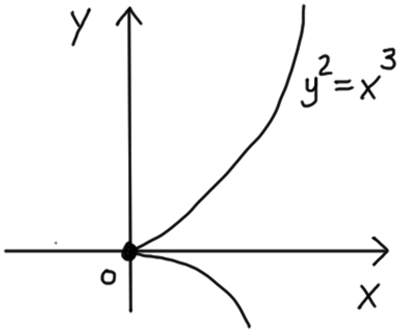
1. Let $C : f = y - x^2 = 0$.



In this case, C is smooth since

$$\nabla f = (f_x, f_y) = (-2x, 1) \neq (0,0) \text{ on } C.$$

2. Let $C : f = y^2 - x^3 = 0$ (the *cusp curve*).



Here,

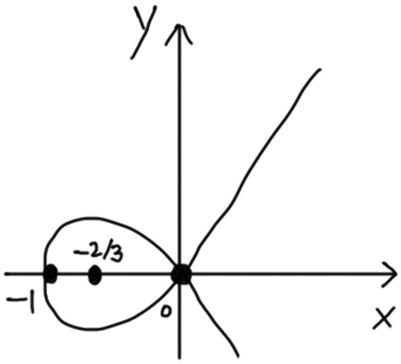
$$\nabla f = (-3x^2, 2y) = (0,0) \iff (x,y) = (0,0)$$

so $(0,0)$ is the only singular point on C.

3. Let $C : f = y^2 - x^3 - x^2 = 0$ (the *nodal curve*). We can rewrite it as

$$y^2 = x^2(x+1)$$

and $x^2 \geq 0$, and $x+1 \geq 0$ if $x \geq -1$.

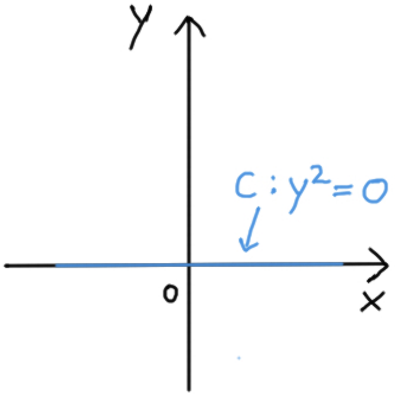


Here,

$$\nabla f = (-3x^2 - 2x, 2y) = (-x(3x+2), 2y) = (0,0) \text{ at } (0,0) \in C, (-2/3, 0) \notin C.$$

So $(0,0)$ is the only singular point on C.

4. Let $C : f = y^2 = 0$ (the *double line*).



Then

$$\nabla f = (0, 2y) = (0,0) \text{ at all points on } C.$$

So C is singular at every point.

3.10 Proposition. Let $C : f = 0$ be an affine plane curve. Then the set of all singular points of C is an algebraic subset of C, and must therefore consist of:

- a finite set of points,
- the union of a finite set of isolated points, and component(s) of C, or
- all of C.

Proof. We have

$$\begin{aligned}(\text{singular points of } C) &= \{p \in \mathbb{A}^2 : f(p) = 0 \text{ and } \nabla f(p) = 0\} \\ &= \{p : f(p) = 0, f_x(p) = 0, f_y(p) = 0\} \\ &= V(f, f_x, f_y)\end{aligned}$$

with $f_x, f_y \in k[x, y]$ since they are (formal) derivatives of polynomials. □

3.11 Definition. The **Zariski tangent space to C at** $p = (a, b)$ is defined as

$$T_p(C) := \{v \in \mathbb{A}^2 : \nabla f(a, b) \cdot v = 0\} \subseteq \mathbb{A}^2.$$

3.12 Remark. $T_p(C)$ is a vector space over k with origin $p = (a, b)$. Thus,

- $T_p(C) = \mathbb{A}^2$ iff p is a singular point of C, and
- $T_p(C)$ is a line iff p is a smooth point of C.

We therefore have the following.

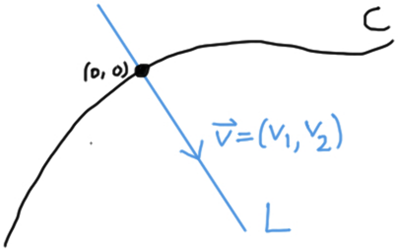
3.13 Theorem. $p \in C$ is smooth iff $\dim_k T_p(C) = 1$. Otherwise, $\dim_k T_p(C) = 2$.

Intersection multiplicity of a line L and a curve C

Let $C : f = 0$ be an affine plane curve (so that $f \in k[x, y]$) and $p \in C$ be a point. We may assume that $p = (0, 0)$ after translating the curve so that p coincides with $(0, 0)$ (or do a change of coordinates). Then since $(0, 0) \in C$, we have $f(0, 0) = 0$, so the polynomial f does not have a constant term:

$$f = \underbrace{ax + by}_{\text{deg. 1 part}} + \underbrace{cx^2 + dxy + ey^2}_{\text{deg. 2 part}} + \dots$$

Consider a line L in $\mathbb{A}^2$ that passes through $(0, 0)$, so that L intersects C in $(0, 0)$.



Since L is a line through $(0, 0)$, we can pick a direction vector (v_1, v_2) and write

$$L : v_2 x - v_1 y = 0 \qquad \text{or} \qquad L := \{(tv_1, tv_2) : t \in k\}.$$

3.14 Definition. The **intersection multiplicity of L with C at** $p = (0, 0)$ is defined as

$$I(p, L \cap C) := m_0,$$

where m_0 is a positive integer such that $f(tv_1, tv_2) = t^{m_0} g(t)$ and $g(0) \neq 0$.

3.15 Remark. We have:

- $m_0 \geq 1$ since $f(0, 0) = 0$.
- $m_0 = \infty$ if $f(tv_1, tv_2) = 0$ for all t (i.e. $L \subseteq C$).

- If L does not intersect C at p, we will set $m_0 = 0$.

3.16 Definition. If $I(p, L \cap C) \geq 2$ then L is a **tangent line of C at** p.

3.17 Example. Let

$$C : y - x^2 = f(x, y), \qquad p = (0, 0), \qquad L : x = 0, \text{ that is, } L = \{(0, t) : t \in k\}.$$

Then

$$f(0, t) = t = t \cdot \underbrace{1}_{g} \implies I(p, L \cap C) = 1.$$

On the other hand, if $L : y = 0$, that is $L = \{(t, 0) : t \in k\}$, then

$$f(t, 0) = -t^2 = t^2 \underbrace{(-1)}_{g} \implies I(p, L \cap C) = 2$$

so L is a tangent line to C at p.

3.18 Example. Let

$$C : y^2 - x^3 = f(x, y), \qquad p = (0, 0), \qquad L \text{ any line through the origin } \{(tv_1, tv_2) : t \in k\}.$$

Then

$$f(tv_1, tv_2) = t^2 v_2^2 - t^3 v_1^3 = t^2(v_2^2 - tv_1^3).$$

If $v_2 = 0$ (i.e. $L : y = 0$) then $I(p, L \cap C) = 3$. It is 2 otherwise, i.e. all lines in $\mathbb{A}^2$ through p are tangent to C at p.

3.19 Definition. A homogeneous polynomial $f \in k[x, y]$ is called an **ℓ-form** if it has degree ℓ.

One can write $f \in k[x, y]$ as (assuming $f(0, 0) \neq 0$ so that f has no constant term)

$$f = f_m + f_{m+1} + \ldots + f_d, \qquad \text{each } f_i \text{ an } i\text{-form}, \qquad m \geq 1.$$

We assume $f_m \neq 0$. We can write

$$f_i = a_0 x^i + a_1 x^{i-1} y + \ldots + a_i y^i$$

then

$$f_i(tv_1, tv_2) = t^i f_i(v_1, v_2) \implies f(tv_1, tv_2) = t^m[f_m(v_1, v_2) + tf_{m+1}(v_1, v_2) + \ldots + t^{d-m} f_d(v_1, v_2)].$$

Thus $I(p, L \cap C) \geq m$. Also if $f_m(v_1, v_2) = 0$ then by homogeneity $f_m(tv_1, tv_2) = 0$ for all t. Thus

$$\begin{aligned} L : \{(tv_1, tv_2) : t \in k\} \subset V(f_m) &\implies f_m \in I(L) = \langle v_2 x - v_1 y \rangle \\ &\implies (v_2 x - v_1 y) \mid f_m \\ &\implies (v_2 x - v_1 y) \text{ is a factor of } f_m. \end{aligned}$$

3.20 Definition. Define **multiplicity of C at** p to be the integer

$$m_p(C) := m = \text{smallest } i \text{ such that } f_i \neq 0.$$

The linear factors of f_m are called the **tangent directions** of C at p.

3.21 Remark. Note:

- If L is a line passing through $(0, 0) = p$ then $I(p, L \cap C) \geq m$.
- If L is a tangent direction then $f_m \equiv 0$ on L and so $I(p, L \cap C) \geq m + 1$.
- If f is smooth at $p = (0, 0)$ then $\nabla f(0, 0) \neq (0, 0)$. However if

$$f = f_m + f_{m+1} + \ldots + f_d$$

  is such that $m \geq 2$ then $\nabla f(0, 0) = (0, 0)$. Hence we must have $m = 1$. Then f_1 has only 1 factor (itself) and $L : f_1 = 0$ is the tangent line to C at p.

3.22 Example. We have:

- $C : f = y - x^2$, and $p = (0, 0) \in C$. $m_p(C) = 1$, so p is smooth and the tangent line is $y = 0$.

- $C : f = y^2 - x^3$, and $p = (0,0)$. $m_p(C) = 2$ thus p is singular. Tangent directions of C at p is $V(y)$ ("preferred tangent line").
- $C : f = y^2 - x^2 - x^3$, and $p = (0,0)$. $m_p(C) = 2$ so p is singular. Tangent directions: $V(x+y), V(y-x)$.
- $C : f = xy - 1$, $p = (1,1)$. Let $s = x - 1$, $t = y - 1$, so $p = (0,0)$ w.r.t. s and t. Then

  $$C : f = (s+1)(t+1) - 1 = st + s + t$$

  so $m_p(C) = 1$. Tangent line: $s + t = 0$ ie $x + y - 2 = 0$.

Pick $p = (0,0) \in \mathbb{A}^2$ so $M_p = \langle x, y \rangle$. Then $M_p^2 = \langle x^2, xy, y^2 \rangle$ and $M_p^3 = \langle x^3, x^2y, xy^2, y^3 \rangle$. So M_p/M_p^2 are the 1-forms. M_p^2/M_p^3 are the 2-forms. In general, M_p^m/M_p^{m+1} are the m-forms. Our goal is to obtain $(T_p(C))^* = M_p(C)/M_p^2(C)$. The idea we use is to get a homomorphism $\psi : M_p(C) \to (T_p(C))^*$ with $\ker \psi = M_p^2(C)$.

First note that if we consider $(0,0)$ to be the origin in $\mathbb{A}^2$ we now have a vector space and the following identification:

$$\text{1-forms} = \{a_1x + a_2y\} = \{\begin{bmatrix} a_1 & a_2 \end{bmatrix} : a_1, a_2 \in k\} = (\mathbb{A}^2)^* \implies M_p/M_p^2 = (\mathbb{A}^2)^*.$$

3.23 Definition. For $g \in k[x,y]$, we define the **differential of** g **at** $p = (0,0)$ by

$$d_pg = \frac{dg}{dx}(p) \cdot x + \frac{dg}{dy}(p) \cdot y \in k[x,y].$$

Under our identification,

$$d_pg = \begin{bmatrix} \frac{dg}{dx}(p) & \frac{dg}{dy}(p) \end{bmatrix} = \nabla g(p) \in (\mathbb{A}^2)^*$$

and $T_p(C) = \ker(d_pf)$, if C is given by f. Consider the map

$$\begin{aligned} d_p : k[x,y] &\to (\mathbb{A}^2)^* \\ g &\mapsto d_pg. \end{aligned}$$

Since $d_p\alpha = 0$ for all constants α, we can restrict d_p to M_p:

$$d_p : M_p \to (\mathbb{A}^2)^*.$$

Then d_p is linear and surjective because given $\begin{bmatrix} a_1 & a_2 \end{bmatrix} \in (\mathbb{A}^2)^*$ we have

$$\begin{bmatrix} a_1 & a_2 \end{bmatrix} = d_p(a_1x + a_2y).$$

Moreover, $\ker d_p = M_p^2$. Thus we have

$$M_p/M_p^2 = (\mathbb{A}^2)^*.$$

I think something was missed here. See the notes "Local properties of affine varieties" on LEARN, items 1.2.9 and 1.2.10.

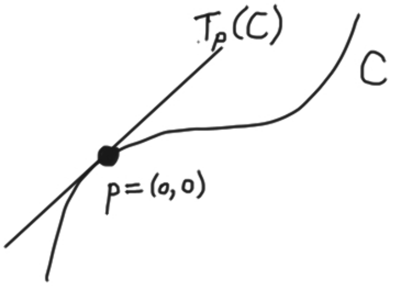
For C an affine plane curve,

$$(T_p(C))^* \cong \frac{M_p(C)}{M_p^2(C)}.$$

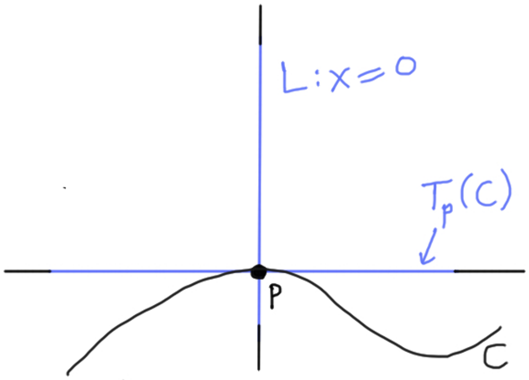
3.24 Theorem. p is smooth if and only if $M_p(C)$ is principal.

In this case, $M_p(C) = \langle \bar{t} \rangle$, where $t = 0$ is the equation of *any* line through p that is not tangent to C at p.

Proof. ($\to$) Assume p is smooth. By translating, we may assume $p = (0,0)$. Since p is a smooth point, C has a tangent line at p.



After possibly rotating the curve, we can assume that the tangent line to C at p is $y = 0$.



Consider the line $L : \{x = 0\}$. Then L is *not* tangent to C at p. First note that the maximal ideal corresponding to $p = (0, 0)$ in $k[x, y]$ is $M_p = \langle x, y\rangle$. So, $M_p(C) = \langle \overline{x}, \overline{y}\rangle$. Let us show that in fact,

$$M_p(C) = \langle \overline{x}\rangle.$$

If C is given by $f \in k[x, y]$, then since $p = (0, 0)$ is a smooth point of C,

$$f = f_1 + \ldots + f_d$$

with each f_i an i-form and $f_1 \neq 0$. Moreover, $f_1 = 0$ is the tangent line of C at p. So,

$$f = \underbrace{by}_{f_1} + \underbrace{cx^2 + dxy + ey^2}_{f_2} + \ldots + f_d, \qquad b \neq 0.$$

Then, we can write f as:

$$f = yg - x^2h,$$

where $g = b +$ (higher order multiples of y) $\in k[x, y]$ and $h = h(x) \in k[x]$ and so, since $\overline{f} = 0$ in $\Gamma(C)$ and also in $\mathcal{O}_p(C)$, we get

$$\overline{yg} = \overline{x}^2\overline{h}.$$

Moreover, $\overline{g} \in \mathcal{O}_p(C)$ since g is a polynomial and $\overline{g}(p) = b \neq 0$. Hence,

$$\overline{g} \text{ is a unit in } \mathcal{O}_p(C) \implies \overline{y} = \overline{x}^2\overline{g}^{-1}\overline{h} \implies M_p(C) = \langle \overline{x}\rangle \text{ and is thus principal.}$$

Note that if $ax + by = 0$ is any other line passing through $p = (0, 0)$ other than $y = 0$, then $a \neq 0$, so that

$$a\overline{x} + b\overline{y} = a\overline{x} + b(\overline{x}^2\overline{g}^{-1}\overline{h}) = \overline{x}(\underbrace{a + b\overline{x}\overline{g}^{-1}\overline{h}}_{=u})$$

with u a unit in $\mathcal{O}_p(C)$ since $u(p) = a \neq 0$. Thus $M_p(C) = \langle a\overline{x} + b\overline{y}\rangle$.

($\leftarrow$) Conversely, if the maximal ideal is principal, say $M_p(C) = \langle t\rangle$, then $M_p^2 = \langle t^2\rangle$ and $M_p/M_p^2 = \{at : a \in k\}$, a one-dimensional k-vector space. This implies that C is smooth at p. □

3.25 Definition. A local Noetherian ring with Krull dimension 1 whose maximal ideal is principal is called a **discrete valuation ring (DVR)**.

The above theorem can be written as:

$$p \text{ is smooth} \iff \mathcal{O}_p(C) \text{ is a DVR.}$$

3.26 Theorem. Let p be a smooth point on the affine plane curve C. Suppose $M_p(C) = \langle \overline{t}\rangle$. Then any $f \in \mathcal{O}_p(C)$ can be expressed as a unique power series in $\overline{t}$:

$$f := \sum_{i=0}^{\infty} a_i\overline{t}^i, \quad a_i \in k,$$

such that

$$f - (a_0 + a_1\overline{t} + \ldots + a_m\overline{t}^m) \in M_p^{m+1}(C), \quad \forall m.$$

This power series is called the **Taylor series expansion of** f. Note that this is a formal power series.

Proof. Note that $M_p^m(C) = \langle \bar{t}^m \rangle$, for all m. Also, we have

$$\frac{\mathcal{O}_p(C)}{M_p(C)} \cong \{f(p) \in k : f \in \mathcal{O}_p(C)\} \cong k$$

since, for all $f \in \mathcal{O}_p(C)$,

$$f - f(p) \in M_p(C) \implies f = \underbrace{f(p)}_{\in k} + (\underbrace{f - f(p)}_{\in M_p(C)}).$$

Moreover,

$$\frac{M_p^m(C)}{M_p^{m+1}(C)} \cong \{\alpha \bar{t}^m : \alpha \in k\} \cong k.$$

Indeed, note that if $f \in M_p^m(C) = \langle \bar{t}^m \rangle$ then $f = \bar{t}^m g$ for some $g \in \mathcal{O}_p(C)$. So,

$$f = \bar{t}^m (g(p) + (\underbrace{g - g(p)}_{\in M_p(C)}))$$

Since $g - g(p) \in M_p(C)$,

$$g - g(p) = \bar{t}h, \quad \text{for some } h \in \mathcal{O}_p(C).$$

Thus

$$f = \underbrace{g(p)}_{\in k} \bar{t}^m + \underbrace{\bar{t}^{m+1} h}_{\in M_p^{m+1}(C)} .$$

Existence: Let $f \in \mathcal{O}_p(C)$. Then

$$f = \underbrace{f(p)}_{a_0 \in k} + (\underbrace{f - f(p)}_{\in M_p(C)})$$

thus

$$f - f(p) = \bar{t} f_1 \qquad \text{for some } f_1 \in \mathcal{O}_p(C) \implies f = a_0 + \bar{t} f_1.$$

Similarly,

$$f_1 = \underbrace{f_1(p)}_{a_1} + \bar{t} f_2 \qquad \text{with } f_2 \in \mathcal{O}_p(C)$$

thus

$$f = a_0 + a_1 \bar{t} + \bar{t}^2 f_2 \implies f = a_0 + a_1 \bar{t} + a_2 \bar{t}^2 + \dots$$

and

$$f - (a_0 + a_1 \bar{t} + \ldots + a_m \bar{t}^m) = \bar{t}^{m+1} f_{m+1} \in M_p^{m+1}(C).$$

Uniqueness: enough to show that if $f = 0$ then all the a_i are 0. Assume that $f \equiv 0$. Then,

- $a_0 = f(p) = 0$ (since $f \equiv 0$)
- $M_p(C) \ni a_1 \bar{t} = -(f - (a_0 + a_1 \bar{t}))$ since $f \equiv 0$ and $a_0 = 0$. This is in $M_p^2(C)$.

Thus $a_1 = 0$ since

$$M_p(C)/M_p^2(C) = \{\alpha \bar{t} : \alpha \in k\}.$$

In general, if $i > 0$, then

$$a_i \bar{t}^i = -(f - (a_0 + a_1 \bar{t} + \ldots + a_i \bar{t}^i)) \in M_p^{i+1}(C)$$

and $M_p^i(C)/M_p^{i+1}(C) \cong \{\alpha \bar{t}^i : \alpha \in k\}$ so $a_i = 0$. □

Discrete valuation rings

3.27 Remark. Recall:

- $p \in C$ is smooth if and only if $\mathcal{O}_p(C)$ is a DVR (i.e. $M_p(C)$ is principal).
- If p is smooth, then $M_p(C) = \langle \bar{t} \rangle$ for any linear polynomial $t \in k[x, y]$ such that $p \in V(t)$ and $\{t = 0\}$ is not tangent to C at p.

3.28 Proposition. Suppose that $p \in C$ is smooth, so that $M_p(C) = \langle \bar{t} \rangle$. Then, for all $0 \neq z \in \mathcal{O}_p(C)$,

$$z = \bar{t}^m u,$$

with $m \in \mathbb{Z}^{\geq 0}$ and u a unit in $\mathcal{O}_p(C)$. Moreover, this decomposition is *unique.*

Proof. If z is a unit, set $n = 0$ and $u = z$. Otherwise $z \in M_p(C) = \langle \bar{t} \rangle$ so that $z = \bar{t} z_1$ with $z_1 \in \mathcal{O}_p(C)$. If z_1 is a unit, then $z = \bar{t}^1 \cdot z_1$ and we are done. Otherwise,

$$z_1 = \bar{t} z_2$$

with $z_2 \in \mathcal{O}_p(C)$, and so on. But,

$$(z_1) \subset (z_2) \subset (z_3) \subset \dots$$

Since $\mathcal{O}_p(C)$ is Noetherian, this ascending chain of ideals must terminate, so that

$$(z_i) = (z_m),$$

for some $m \in \mathbb{N}$, for all $i \geq m$. Then,

$$z_{m+1} = z_m u$$

with u a unit. Then $z = t^{m+1} u$.

Uniqueness: suppose that

$$z = \bar{t}^m u = \bar{t}^n v$$

with $m, n \in \mathbb{Z}^{\geq 0}$ and u, v units. Suppose that $n \geq m$. Then,

$$\bar{t}^m u - \bar{t}^n v = 0 \iff \bar{t}^m (u - \bar{t}^{n-m} v) = 0 \iff u - \bar{t}^{n-m} v = 0 \text{ since } \bar{t} \neq 0 \iff u = \bar{t}^{n-m} v$$

Now, $u(p), v(p) \neq 0$ since u, v are units, but $\bar{t}(p) = 0$. So we must have $n = m$ and $u = v$. □

3.29 Definition. Given a smooth point $p \in C$, a generator $\bar{t} \in \mathcal{O}_p(C)$ of $M_p(C)$ is called a **local parameter** (or **uniformisation parameter**).

Local parameters are unique up to a unit.

3.30 Definition. Let $0 \neq z \in \mathcal{O}_p(C)$. Given the decomposition $z = \bar{t}^m u$, we define

$$\mathrm{ord}_p^C(z) := m = \text{valuation of } z \text{ at } p.$$

In some sense this is giving you the order of vanishing of the function z at p. We also set $\mathrm{ord}_p^C(0) := \infty$. Thus, we have the following map:

$$\mathrm{ord}_p^C : \mathcal{O}_p(C) \to \mathbb{Z}^{\geq 0} \cup \{\infty\}, \qquad z \mapsto \mathrm{ord}_p^C(z)$$

called the **order function** (or the **discrete valuation map**).

3.31 Remark. We have:

(i) ord_p^C does not depend on the choice of local parameter $\bar{t}$.

(ii) $\mathrm{ord}_p^C(z) = \infty$ if and only if $z = 0$.

(iii) $\mathrm{ord}_p^C(z) = 0$ if and only if z is a unit in $\mathcal{O}_p(C)$.

(iv) $\mathrm{ord}_p^C(z_1 z_2) = \mathrm{ord}_p^C(z_1) + \mathrm{ord}_p^C(z_2)$.

(v) $\mathrm{ord}_p^C(z_1 + z_2) \geq \min\{\mathrm{ord}_p^C(z_1), \mathrm{ord}_p^C(z_2)\}$

Proof. Exercise. Properties (iv) and (v) come from the fact that $\mathrm{ord}_p^C(z)$ is the lowest power of $\bar{t}$ appearing in the Taylor series expansion of z, i.e.

$$z = \underbrace{a_m}_{\neq 0} \bar{t}^m + a_{m+1} \bar{t}^{m+1} + \dots = \bar{t}^m (\underbrace{a_m + a_{m+1} \bar{t}^1 + \dots}_{\text{unit}}).$$ □

Finally, the discrete valuation map can be extended to $k(C)$:

$$\operatorname{ord}_p^C : k(C) \to \mathbb{Z} \cup \{\infty\}, \qquad f = \frac{\overline{a}}{\overline{b}} \mapsto \operatorname{ord}_p^C(\overline{a}) - \operatorname{ord}_p^C(\overline{b}).$$

One can check that this is independent of the representation $\overline{a}/\overline{b}$ of f (exercise). Also,

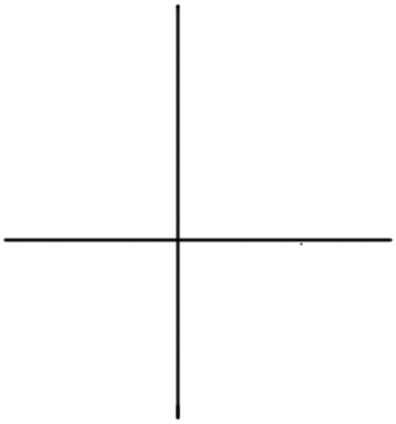
$$\mathcal{O}_p(C) = \{f \in k(C) : \operatorname{ord}_p^C(f) \geq 0\}$$
$$M_p(C) = \{f \in k(C) : \operatorname{ord}_p^C(f) > 0\}$$

(exercise).

Further properties of smoothness and ord_p^C

3.32 Lemma. Let C be an affine plane curve. If $p \in C$ is smooth, then p is contained in only one irreducible component of C.

3.33 Example. $C = V(xy) = V(x) \cup V(y)$.



Then the origin is singular.

Proof. If C is irreducible, we are done. Otherwise, if $C = V(f)$, then $f = gh$ for some nonconstant $g, h \in k[x, y]$. So,

$$C = V(g) \cup V(h).$$

Let $p \in V(g) \cap V(h)$, then p is singular. Indeed,

$$\nabla f(p) = (f_x(p), f_y(p)) = (0, 0)$$

because

$$f_x(p) = g_x(p)\cancel{h(p)} + \cancel{g(p)}h_x(p) = 0$$

and $f_y(p) = 0$ (similarly). In particular, if f_1, f_2 are irreducible factors of f and $p \in V(f_1) \cup V(f_2)$ then p is singular.

Thus, if p is smooth, p cannot be contained in more than one irreducible component of C. □

When studying smooth points on an affine curve, it is enough to look at the irreducible component containing them.

3.34 Proposition. Let C and C' be irreducible affine plane curves, and assume that there exists an isomorphism

$$\varphi : C \to C'.$$

Let $p \in C$ and set $p' = \varphi(p)$. Then C is smooth at p if and only if C' is smooth at p'. Moreover, $\varphi^* : k(C') \to k(C)$ maps $\mathcal{O}_p(C')$ isomorphically onto $\mathcal{O}_p(C)$ and $\operatorname{ord}_{p'}^{C'} = \operatorname{ord}_p^C \circ \varphi^*$. I.e. isomorphisms preserve smoothness and the order of vanishing of functions.

Proof. Since φ is an isomorphism,

$$\varphi^* : k(C') \to k(C)$$

is a field isomorphism. Note that since φ is a polynomial map, if $g \in \mathcal{O}_{p'}(C')$, then

$$\varphi^*(g) = g \circ \varphi$$

is defined at p so that

$$\varphi^*(\mathcal{O}_{p'}(C')) \subseteq \mathcal{O}_p(C)$$

In fact, $\varphi^*(\mathcal{O}_{p'}(C')) = \mathcal{O}_p(C)$ since φ has a polynomial inverse.

Moreover, since φ^* maps units to units (because it is a field homomorphism), we have that φ^* maps $M_{p'}(C')$ isomorphically onto $M_p(C)$. In particular, if $M_{p'}(C') = \langle \overline{t}' \rangle$, then

$$M_p(C) = \langle \varphi^*(\overline{t}') \rangle$$

(and vice-versa). So, $\mathcal{O}_{p'}(C')$ is a DVR iff $\mathcal{O}_p(C)$ is a DVR. Finally, since $M_p(C) = \langle \varphi^*(\overline{t}') \rangle$, we see that

$$\mathrm{ord}_{p'}^{C'} = \mathrm{ord}_p^C \circ \varphi^*$$

(because $\overline{t} = \varphi^*(\overline{t}')$). □

We want to state one last property of ord_p^C.

3.35 Proposition. If $g_m \in k[x,y]$ is an m-form, then

$$g_m = h_1 \cdots h_m$$

where h_i are 1-forms for $i = 1, \ldots, m$.

Proof. We have

$$\begin{aligned} g_m &= a_0x^m + a_1x^{m-1}y + \ldots + a_my^m \\ &= x^m(a_0 + a_1(y/x) + \ldots + a_m(y/x)^m) \\ &= x^m(\alpha_1 - (y/x)) \cdots (\alpha_m - (y/x)), \text{ for some } \alpha_i, \in k \quad \text{since } k = \overline{k} \text{ and have a poly. expression in } s = y/x \\ &= (\alpha_1 x - y) \cdots (\alpha_m x - y) \end{aligned}$$

□

3.36 Proposition. Suppose that $p = (0,0) \in C$. If $g \in k[x,y]$ is such that

$$g = g_m + g_{m+1} + \ldots + g_r,$$

with g_i an i-form and $g_m \neq 0$, then we can write $g_m = h_1 \cdots h_m$, with h_j a 1-form, and

$$\mathrm{ord}_{(0,0)}^C(\overline{g}) \geq m.$$

Moreover,

$$\mathrm{ord}_p^C(\overline{g}) = m$$

iff each $h_j = 0$ is not tangent to C at p.

Proof. First note that $h_j(0,0) = 0$, for all $j = 1, \ldots, m$, so that $\overline{h_j} \in M_p(C) = \langle \overline{t} \rangle$ thus

$$\overline{h_j} = \overline{t}z \implies \mathrm{ord}_p^C(\overline{h_j}) \geq 1.$$

So,

$$\mathrm{ord}_p^C(\overline{g_m}) = \mathrm{ord}_p^C(\overline{h_1} \cdots \overline{h_m}) = \sum_{j=1}^m \underbrace{\mathrm{ord}_p^C(\overline{h_j})}_{\geq 1} \geq m.$$

Similarly, $\mathrm{ord}_p^C(\overline{g_i}) \geq i$, for all $i = m, \ldots, r$. Finally,

$$\mathrm{ord}_p^C(\overline{g}) \geq \min_{i=m,\ldots,r} \{\mathrm{ord}_p^C(\overline{g_i})\} = \mathrm{ord}_p^C(\overline{g_{i_0}}) \text{ (for some } m \leq i_0 \leq r) \geq i_0 \geq m.$$

Also,

$$\mathrm{ord}_p^C(\overline{g}) = m \iff \mathrm{ord}_p^C(\overline{g_m}) = m \iff \mathrm{ord}_p^C(\overline{h_j}) = 1 \qquad \forall j = 1, \ldots, m.$$

The only thing left to prove is that $\mathrm{ord}_p^C(\overline{h_j}) = 1$ if and only if $h_j = 0$ is not tangent to C at p. Suppose that C is given by the polynomial

$$f = f_1 + f_2 + \ldots + f_d.$$

Then, since C is smooth at p, $f_1 \neq 0$ and $f_1 = 0$ is the equation of the tangent line to C at p. Also, $\overline{f} = 0$ in $\mathcal{O}_p(C)$, so that

$$\overline{f_1} = -\overline{f_2} - \ldots - \overline{f_d}.$$

Thus $\text{ord}_p^C(\overline{f_1}) \geq 2$. Now, if $h_j > 0$ is tangent to C at p, then $h_j = \alpha f_1$, for some $\alpha \in k$. Thus,

$$\text{ord}_p^C(\overline{h_j}) = \text{ord}_p^C(\overline{\alpha}\overline{f_1})$$

$$\cancel{\text{ord}_p^C(\overline{\alpha})} + \text{ord}_p^C(\overline{f_1}) = \text{ord}_p^C(\overline{f_1}) \geq 2.$$

Where the cancellation occurs since $\overline{\alpha}$ is a unit in $\mathcal{O}_p(C)$. Thus, if $\text{ord}_p^C(\overline{h_j}) = 1$, we have that $h_j = 0$ is not tangent to C at p. Conversely, if $h_j = 0$ is not tangent to C at p, then $M_p(C) = \langle \underbrace{\overline{h_j}}_{\overline{t}} \rangle$ thus

$$\text{ord}_p^C(\overline{h_j}) = 1. \qquad \square$$

3.37 Remark. $M_p(C) = \langle \overline{t} \rangle$ iff $t = 0$ is not tangent to C at p.

3.3 Intersection multiplicity

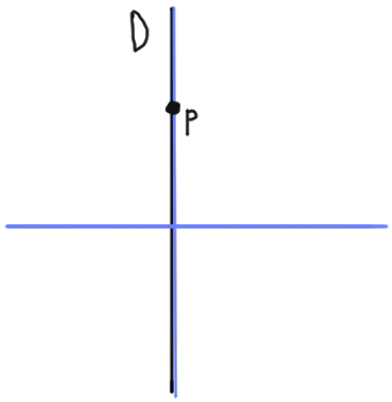
Let C and D be two affine plane curves.

3.38 Definition. We have

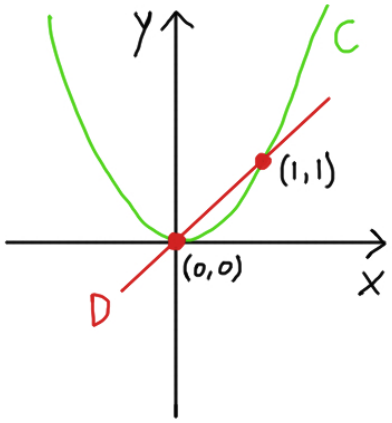
1. C and D **intersect properly** at $p \in \mathbb{A}^2$ if C and D don't have a common component that contain p.
2. C and D **intersect transversally** at $p \in \mathbb{A}^2$ if they are both smooth at p and have distinct tangent lines at p.

3.39 Example. We have

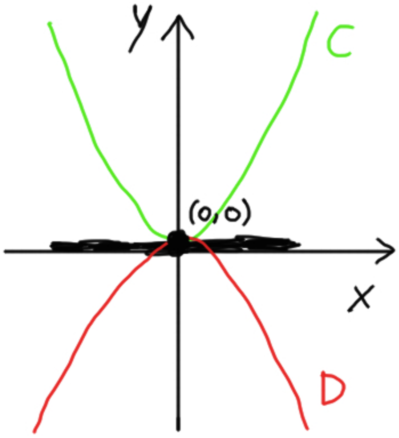
1. $C = V(x, y) = V(x) \cup V(y)$ and $D = V(x)$. Then for all $p \in V(x)$, $p \in C \cap D$, but C and D don't intersect properly at p.



2. $C = V(y - x^2)$ and $D = V(y - x)$. Then C and D intersect properly and transversally at $(0, 0)$ and $(1, 1)$.



3. $C = V(y - x^2)$ and $V(y + x^2)$



C and D intersect properly but not transversally at $p = (0, 0)$ since both C and D have tangent line $y = 0$ at $(0, 0)$.

Suppose that C is irreducible and smooth at $p \in C$. Then we define

$$I(p; C \cap D) := \operatorname{ord}_p^C(\overline{g})$$

where $D = V(g)$. This number $I(p; C \cap D)$ is called the **intersection multiplicity of C and D at p.**

3.40 Example. $C : f = y - x^2$ and $D : g = y^2 - x^3$. [diagram in binder]. Find pt in $C \cap D$:

$$y - x^2 = 0 \tag{1}$$

$$y^2 - x^3 = 0 \tag{2}$$

and substituting (1) into (2) gives $(x^2)^2 - x^3 = 0$ or equivalently $x^3(x - 1) = 0$, so $(0, 0)$ with multiplicity 3 and $(1, 1)$ with multiplicity 1. Find $I(p, C \cap D)$:

- $p = (0, 0)$: C is smooth at $(0, 0)$ with tangent line $y = 0$.

  Then, $M_{(0,0)}(C) = \langle \overline{x} \rangle$ (since $x = 0$ is not tangent to C at $(0, 0)$). Also,

  $$\overline{g} = \overline{y}^2 - \overline{x}^3 = \overline{x}^4 - \overline{x}^3$$

  since $\overline{y} = \overline{x}^2$ in $\mathcal{O}_{(0,0)}(C)$. Equivalently

  $$\overline{g} = \overline{x}^3 \underbrace{(\overline{x} - 1)}_{:=u}$$

  with $u(0, 0) = 1 \neq 0$ thus u is a unit in $\mathcal{O}_{(0,0)}(C)$, so

  $$I((0, 0), C \cap D) = \operatorname{ord}_{(0,0)}^C(\overline{g}) = 3.$$

- $p = (1, 1)$: C is smooth at $(1, 1)$ and $(x - 1) = 0$ is *not* tangent to C at $(1, 1)$. So,

  $$M_{(1,1)}(C) = \langle \overbrace{\overline{x} - 1}^{=\overline{t}} \rangle$$

  and

  $$\overline{g} = \overline{y}^2 - \overline{x}^3 = \overline{x}^4 - \overline{x}^3$$

  since $\overline{y} = \overline{x}^2$ in $\mathcal{O}_{(1,1)}(C)$, but this is equal to

  $$\underbrace{(\overline{x} - 1)}_{\overline{t}} \underbrace{(\overline{x}^3)}_{\overline{u}}$$

  thus $u := \overline{x}^3$ is a unit in $\mathcal{O}_{(1,1)}(C)$ (since $u(1, 1) = 1 \neq 0$). Thus $I((1, 1), C \cap D) = 1$.

There are some natural properties that one would expect intersection multiplicity to satisfy: suppose that C and D are affine plane curves. Then:

1. Intersection multiplicity is invariant under affine transformations.

2. $I(p, C \cap D) = \infty$ if and only if C and D have a common component containing p

3. If C and D intersect properly at p, then $I(p, C \cap D) < \infty$. Also, $I(p, C \cap D) = 0$ iff $p \notin C \cap D$.

4. $I(p, C \cap D) = 1$ if and only if C and D intersect transversally at p. Otherwise we have
$$I(p, C \cap D) \geq m_p(C)m_p(D)$$
(where if $p = 0$ and $C = V(f)$ with $f = f_m + \ldots + f_d$ then $m_p(C) = m$) with equality holding iff C and D don't have common tangent directions at p (the tangent directions of C at p are the lines $h_j = 0$ where $g_m = h_1 \cdots h_m$ with h_j a 1-form for all j).

5. Additivity: if $D = D_1 \cup D_2$, then
$$I(p, C \cap D) = I(p, C \cap V(g_1)) + I(p, C \cap V(g_2)).$$

6. If $D = V(g)$ and $E = V(h)$ with $\overline{g} = \overline{h}$ in $\Gamma(C)$, then
$$I(p, C \cap D) = I(p, C \cap E)$$

7. Symmetry:
$$I(p, C \cap D) = I(p, D \cap C).$$

Proof. For general proof see Fulton. But let's do it in the case where C irreducible and smooth at p. In this case, if $D = V(g)$, then
$$I(p, C \cap D) = \mathrm{ord}_p^C(\overline{g}).$$

1. Affine transformations are isomorphism and therefore preserve smoothness and the order function.

2. $I(p, C \cap D) = \infty$ if and only if $\mathrm{ord}_p^C(\overline{g}) = \infty$, if and only if $\overline{g} = 0$ in $\mathcal{O}_p(C)$, if and only if $g \in I(C) = \langle f \rangle$ (if $C = V(f)$), iff $f \mid g$, iff C is a component of D.

3. From 2), if C and D don't intersect properly at p, then C is a component of D and so $I(p, C \cap D) = \infty$.

   Also, $I(p, C \cap D) = 0$, iff $\mathrm{ord}_p^C(\overline{g}) = 0$, iff $\overline{g}(p) \neq 0$, iff $p \notin D = V(g)$, iff $p \notin C \cap D$ (since $p \in C$)

4. We have seen that p is a smooth point on C iff $m_p(C) = 1$. So, since C is smooth at p, we need to prove that
$$I(p, C \cap D) \geq m_p(D)$$
with equality holding iff no tangent direction to D at p is tangent to C at p. If $p = (0, 0)$ and $D = V(g)$ and $g = g_m + \ldots + g_d$ then we have seen that
$$I(p, C \cap D) = \mathrm{ord}_p^C(\overline{g}) \geq m = m_p(D)$$
with equality holding iff $h_j = 0$ is not tangent to C at p, for all linear factors $h_1, \ldots, h_m$ of g_m. In particular
$$I(p, C \cap D) = 1$$
if and only if ($m = 1$ (so that D is smooth at p) and the tangent line to D at p is not the tangent line to C at p), if and only if C and D intersect transversally.

5. If $D = V(g_1 g_2)$, then
$$I(p, C \cap D) = \mathrm{ord}_p^C(\overline{g_1 g_2}) = \mathrm{ord}_p^C(\overline{g_1}) + \mathrm{ord}_p^C(\overline{g_2}) = I(p, C \cap V(g_1)) + I(p, C \cap V(g_2))$$

6. If $D = V(g)$ and $E = V(h)$ with $\overline{g} = \overline{h}$ in $\Gamma(C)$ then
$$I(p, C \cap D) = \mathrm{ord}_p^C(\overline{g}) = \mathrm{ord}_p^C(\overline{h}) = I(p, C \cap E).$$

7. Symmetry: Suppose that $C = V(f)$ and $D = V(g)$. Then

   $$\operatorname{ord}_p^C(\overline{g}) = \dim_k \left(\frac{\mathcal{O}_p(\mathbb{A}^2)}{\langle f, g \rangle \mathcal{O}_p(\mathbb{A}^2)} \right).$$

   Indeed, if $\operatorname{ord}_p^C(\overline{g}) = m$, then $\overline{g} = \overline{t}^m u$ with $M_p(C) = \langle \overline{t} \rangle$ and u a unit in $\mathcal{O}_p(C)$. So,

   $$\frac{\mathcal{O}_p(C)}{\langle \overline{g} \rangle \mathcal{O}_p(C)} \overset{*}{=} \frac{\mathcal{O}_p(C)}{\langle \overline{t}^m \rangle \mathcal{O}_p(C)} = \{a_0 + a_1\overline{t} + \ldots + a_{m-1}\overline{t}^{m-1} : a_i \in k\} \simeq k^m$$

   where at (*) we use that $\langle \overline{g} \rangle = \langle \overline{t}^m \rangle$, and thus

   $$\operatorname{ord}_p^C(\overline{g}) = m = \dim_k \left(\frac{\mathcal{O}_p(C)}{\langle \overline{g} \rangle \mathcal{O}_p(C)} \right)$$

   Consider the following surjective homomorphism:

   $$\begin{array}{rcccll} \varphi : \mathcal{O}_p(\mathbb{A}^2) & \to & \mathcal{O}_p(C) & \to & \dfrac{\mathcal{O}_p(C)}{\langle \overline{g} \rangle \mathcal{O}_p(C)} & \\ \dfrac{a}{b} & \mapsto & \left(\dfrac{a}{b}\Big|_C \right) & \mapsto & \left(\dfrac{a}{b}\Big|_C \right) & \pmod{\overline{g}} \end{array}$$

   and

   $$\ker \varphi = \langle f, g \rangle \mathcal{O}_p(\mathbb{A}^2)$$

   and $\Gamma(C) = k[x, y]/\langle f \rangle$. □

Beginning of CUMC lectures (2013-07-10 and 2013-07-12).

In general, we have

3.41 Theorem. There exists a unique intersection number $I(p, C \cap D)$ defined for *all* points $p \in \mathbb{A}^2$, satisfying properties $1 - 7$.

If $C = V(f)$ and $D = V(g)$, then $I(p, C \cap D) = \dim_k(\mathcal{O}_p(\mathbb{A}^2)/\langle f, g \rangle \mathcal{O}_p(\mathbb{A}^2))$. In particular if C is smooth at p then

$$I(p, C \cap D) = \operatorname{ord}_p^C(\overline{g})$$

with $\overline{g} \in \mathcal{O}_p(C)$.

Proof. See Fulton. □

4 Projective varieties

4.1 Projective space and algebraic sets

4.1 Definition. Let k be any field and consider $\mathbb{A}^{n+1} := \mathbb{A}^{n+1}(k)$. The set of all lines in $\mathbb{A}^{n+1}$ passing through the origin $O = (0, 0)$ is called ***n*-dimensional projective space** (or **projective *n*-space**) and is denoted $\mathbb{P}^n(k)$ or $\mathbb{P}^n$ if k is understood.

Thus $\mathbb{P}^n = (\mathbb{A}^{n+1} - O)/\sim$ where $(x_1, \ldots, x_n) \sim (\lambda x_1, \ldots, \lambda x_n)$ for all $\lambda \in k^*$. (This equivalence tells us two points are equivalent if and only if they lie on the same line passing through the origin).

[DIAGRAM OF LINE WITH TWO EQUIVALENT POINTS]

Any two curves intersect at the point at infinity in projective space.

An element of $\mathbb{P}^n = (\mathbb{A}^{n+1} - O)/\sim$ is called a **point**. If $p \in \mathbb{P}^n$ is a point, then any $(n+1)$-tuple $(a_1, \ldots, a_{n+1}) \neq 0$ in the equivalence class of p is called a set of **homogeneous coordinates at** p. (p is a line in $\mathbb{A}^{n+1}$ through 0 and $(a_1, \ldots, a_{n+1})$ is any point on that line other than 0).

Equivalence classes are often denoted $p = [a_1 : \ldots : a_{n+1}]$ (homogeneous coordinates) to distinguish from affine coordinates.

Note: $[a_1 : \ldots : a_{n+1}] = [\lambda a_1 : \ldots : \lambda a_{n+1}]$ for all $\lambda \in k^*$.

Projective n-space can be covered by $(n+1)$ copies of $\mathbb{A}^{n+1}$. We will see that $\mathbb{P}^n$ is in fact n-dimensional. For $i = 1, \ldots, n$ let

$$U_i = \{[x_1 : \ldots : x_{n+1}] \in \mathbb{P}^n \mid x_i \neq 0\}.$$

Then

$$\mathbb{P}^n = \bigcup_{i=1}^{n} U_i$$

since for every $p = [x_1 : \ldots : x_{n+1}] \in \mathbb{P}^n$ at least one $x_i \neq 0$, so that $p \in U_i$. Also, if $p = [x_1 : \ldots : x_{n+1}] \in U_i$ so that $x_i \neq 0$, then

$$[x_1 : \ldots : x_{n+1}] = [x_1/x_i : \ldots : x_i/x_i : \ldots : x_{n+1}/x_i] = [x_1/x_i : \ldots : 1 : \ldots : x_{n+1}/x_i]$$

so

$$\left(u_1 = \frac{x_1}{x_i}, \ldots, u_{i-1} = \frac{x_{i-1}}{x_i}, u_i = \frac{x_{i+1}}{x_i}, \ldots, u_n = \frac{x_{n+1}}{x_i}\right) \implies U_i = \mathbb{A}^n.$$

4.2 Example. $\mathbb{P}^2 = (\mathbb{A}^3 - 0)/\sim$, $[x : y : z]$ (homogeneous coordinates).

$$\begin{aligned} U_x &= \{x \neq 0\} = \{[1 : y/x : z/x]\} = \{[1 : u : v] \mid u, v \in k\} = \{(u,v) \in \mathbb{A}^2\} \\ U_y &= \{y \neq 0\} = \{[x/y : 1 : z/y]\} \\ U_z &= \{z \neq 0\} = \{[x/z : y/z : 1]\} \end{aligned}$$

$\mathbb{A}^n$ can be thought of as a subset of $\mathbb{P}^n$:

$$\mathbb{A}^n \to \mathbb{P}^n = (\mathbb{A}^{n+1} - 0)/\sim, \qquad (b_1, \ldots, b_n) \mapsto [b_1 : \ldots : b_n : 1]$$

(or we could introduce the 1 in any other spot).

For each $i = 1, \ldots, n+1$,

$$H_i := \mathbb{P}^n \setminus U_i = \{[x_1 : \ldots : x_{n+1}] \in \mathbb{P}^n \mid x_i = 0\} = \text{hyperplanes}$$

since points in H_i look like $[x_1 : \ldots : x_{i-1} : 0 : x_{i+1} : \ldots : x_{n+1}]$ so that any x_j with $i \neq j$ can be zero.

Note that H_i can be identified with $\mathbb{P}^{n-1}$. In particular $H_\infty := H_{n+1}$ is called the **hyperplane at infinity** (so that $\mathbb{P}^n = U_{n+1} \cup H_\infty$).

$$\mathbb{P}^n = \underbrace{\{[x_1 : \ldots : x_n : 1]\}}_{\mathbb{A}^n} \cup \underbrace{\{[x_1 : \ldots : x_n : 0]\}}_{\mathbb{P}^{n-1}}$$

4.3 Example. We have:

1. $\mathbb{P}^0 = (\mathbb{A}^1 - 0)/\sim = \{\text{pt}\}$.
2. $\mathbb{P}^1 = U_2 \cup H_\infty = \mathbb{A}^1 \cup \mathbb{P}^0 = \mathbb{A}^1 \cup \{\text{pt}\} = A^1 \cup \{\infty\}$ is the 1-point compactification of $\mathbb{A}^1$. If $k = \mathbb{R}$, $\mathbb{P}^1(\mathbb{R}) = S^1$ (the circle). If $k = \mathbb{C}$ then $\mathbb{P}^1(\mathbb{C}) = S^2$ (the Riemann sphere).

$\mathbb{P}^1(\mathbb{R}) = (\mathbb{R}^2 - 0)/\sim$ (pick points unit one away).

4.4 Example. We have:

$$\mathbb{P}^2 = \underbrace{U_z}_{\{[x:y:1]\} = \mathbb{A}^2} \quad \cup \quad \underbrace{H_\infty}_{H_z = \{[x:y:0]\} = \mathbb{P}^1 \text{ (line)}} .$$

In $\mathbb{P}^2$, $H_\infty = \ell_\infty$ is the **line at infinity**,

$$\{[x : y : 0] \in \mathbb{P}^2\}.$$

4.5 Remark. Lines in $\mathbb{P}^2$ always intersect. Consider two parallel lines L, L' in $\mathbb{A}^2$,

$$\mathbb{A}^2 = U_z = \{[x : y : 1] \in \mathbb{P}^2\} = \{[u : v : 1] \in \mathbb{P}^2\}.$$

If L and L' are parallel, then they are given by equations of the form

$$\begin{aligned} au + bv + c &= 0 \qquad (*) \\ au + bv + c' &= 0 \end{aligned}$$

Also $L \neq L'$ if and only if $c \neq c'$. Now, if $U_z = \{z \neq 0\}$, then set $u = x/z$ and $v = y/z$. Substituting into the equations (*), we get

$$\begin{aligned} ax + by + cz &= 0 \\ ax + by + c'z &= 0 \end{aligned} \tag{**}$$

Solving the system (**), we get $(c - c')z = 0$ so $z = 0$ thus $ax + by = 0$. The solution is

$$\begin{aligned} x &= bt \\ y &= -at \\ z &= 0 \end{aligned}$$

so solutions of (**) lie on the line $\{(bt, -at, 0) \mid t \in k\} \subseteq \mathbb{A}^3$. Since this is a line through $0 \in \mathbb{A}^3$, it corresponds to the point "at infinity" $[b : -a : 0] \in \ell_\infty$.

4.6 Definition. Let $f \in k[x_1, \ldots, x_{n+1}]$. Then $p = [a_1 : \ldots : a_{n+1}] \in \mathbb{P}^n$ is a **zero of** f if and only if $f(\lambda a_1, \ldots, \lambda a_{n+1}) = 0$ for all $\lambda \in k^*$, in which case we write $f(p) = 0$.

4.7 Definition. For any $S \subset k[x_1, \ldots, x_{n+1}]$,

$$V_p(S) = \{q \in \mathbb{P}^n \mid f(q) = 0 \text{ for all } f \in S\}$$

is called the **zero set** of S in $\mathbb{P}^n$. Moreover, if $Y \subset \mathbb{P}^n$ is such that $Y = V_p(S)$ for some $S \subseteq k[x_1, \ldots, x_{n+1}]$ then Y is called a **projective algebraic set**.

4.8 Definition. Given $Y \subset \mathbb{P}^n$, define

$$I_p(Y) = \{f \in k[x_1, \ldots, x_{n+1}] \mid f(p) = 0 \text{ for all } p \in Y\}$$

to be the **ideal** of Y.

4.9 Remark. From now on, we will use I_a and V_a for the ideal of a set of points in $\mathbb{A}^m$ and for the zero set of polynomials in $\mathbb{A}^m$.

4.10 Lemma. Let $f \in k[x_1, \ldots, x_{n+1}]$ and $f = f_m + \ldots + f_d$ ($k = \overline{k}$), where f_i is an i-form for $i = m, \ldots, d$. Then, if $q \in \mathbb{P}^n$, $f(q) = 0$ if and only if $f_i(q) = 0$ for $i = m, \ldots, d$.

Proof. Suppose that $q = [a_1 : \ldots : a_{n+1}]$. Then

$$\begin{aligned} f(\lambda a_1, \ldots, \lambda a_{n+1}) &= f_m(\lambda a_1, \ldots, \lambda a_{n+1}) + \ldots + f_d(\lambda a_1, \ldots, \lambda a_{n+1}) \\ &= \lambda^m \underbrace{f_m(a_1, \ldots, a_{n+1})}_{\in k} + \ldots + \lambda^d \underbrace{f_d(a_1, \ldots, a_{n+1})}_{\in k} \text{ for all } \lambda \in k^*. \end{aligned}$$

This is a polynomial in λ. So $f(\lambda a_1, \ldots, \lambda a_{n+1}) = 0$ if and only if $f_m(\lambda a_1, \ldots, \lambda a_{n+1}) = \ldots = f_d(\lambda a_1, \ldots, \lambda a_{n+1}) = 0$ for all $\lambda \in k^*$ and for $i = m, \ldots, d$. □

Thus, if $f = f_m + \ldots + f_d \in k[x_1, \ldots, x_{n+1}]$ then

$$V_p(f) = V_p(f_m, \ldots, f_d)$$

and if $f \in I_p(Y)$ for $Y \subseteq \mathbb{P}^n$, then $f_i \in I_p(Y)$ for $i = m, \ldots, d$.

This gives us the following.

4.11 Proposition. We have:

(i) Every projective algebraic set is the zero set of a finite number of forms.

(ii) If $Y \subset \mathbb{P}^n$, then $I_p(Y)$ is generated by forms.

4.12 Definition. An ideal $I \subseteq k[x_1, \ldots, x_{n+1}]$ is called **homogeneous** if whenever $f = f_m + \ldots + f_d \in I$, then $f_i \in I$ for $i = m, \ldots, d$ (where f_i is an i-form).

By the above, we see that the ideal $I_p(Y)$ of any set of points $Y \subseteq \mathbb{P}^n$ is homogeneous. Moreover, one can show (as in the affine case) that $I_p(Y)$ is radical.

We have a correspondence

$$\text{proj. alg. sets in } \mathbb{P}^n \iff \text{homogeneous radical ideals in } k[x_1, \ldots, x_{n+1}]$$

4.13 Proposition. Let I and J be ideals in $k[x_1, \ldots, x_{n+1}]$. Then

(i) I is homogeneous if and only if I can be generated by forms.

(ii) If I and J are homogeneous then so are IJ, $I+J$, and $\sqrt{I}$.

(iii) Suppose I is homogeneous. Then I is prime if and only if whenever $f, g \in k[x_1, \ldots, x_{n+1}]$ are forms such that $fg \in I$, then $f \in I$ or $g \in I$.

Proof. We have:

(i) Assume that I is homogeneous, say $I = \langle f^1, \ldots, f^s \rangle$. Then, if $f^i = f^i_{m_i} + f^i_{m_i+1} + \ldots + f^i_{m_i+r_i}$ for all i, we have that each $f^i_{m_i+j} \in I$ (by definition), thus

$$I = \langle f^i_{m_i+j} : \text{all } i, j \rangle$$

thus I is generated by forms. Conversely, $I = \langle h^1, \ldots, h^s \rangle$ with each h^i_j a d_i-form. Let $f \in I$ such that $f = a^1 h^1 + \ldots + a^s h^s$ with $a_1, \ldots, a^s \in k[x_1, \ldots, x_{n+1}]$. Let $[f]_d$ be the homogeneous component of f of degree d. Then

$$\begin{aligned} [f]_d &= [a^1 h^1 + \ldots + a^s h^s]_d \\ &= [a^1 \underbrace{h^1}_{d_1\text{-form}}]_d + \ldots + [a^s \underbrace{h^s}_{d_s\text{-form}}]_d \end{aligned}$$

$$[a^1]_{d-d_1} h^1 + \ldots + [a^s]_{d-d_s} h^s \in \langle h^1, \ldots, h^s \rangle = I.$$

(ii) is an exercise; (iii) can be found in the official course notes. □

End of CUMC lectures

We saw that an ideal I is homogeneous if and only if I is generated by forms (that is, by homogeneous polynomials). In particular, ideals of subsets of $\mathbb{P}^n$ are homogeneous.

4.14 Example. We have:

1. $I = \langle x^2 \rangle$, $J = \langle x^2, y \rangle$ are homogeneous ideals.
2. $I = \langle x^2 + x \rangle$ is not homogeneous because $x \notin I$.

If I is a homogeneous ideal, then I is prime if and only if whenever f, g are two forms such that $fg \in I$ then either $f \in I$ or $g \in I$ (this is proved in the course notes). A projective algebraic set is simply the projective zero set of a set of polynomials. This will be irreducible if and only if its ideal is prime. To check this, you just need to use this property which makes things a lot easier.

We now introduce one more thing before we start going through all the properties that we've seen in the affine case, for the projective case.

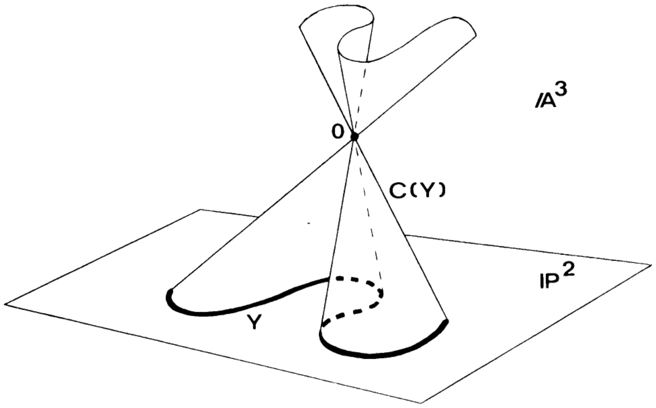
4.15 Definition (AFFINE CONE). Define the map

$$\theta : \mathbb{A}^{n+1} \setminus 0 \to \mathbb{P}^n$$

to be the projection map of the quotient. Given $Y \subset \mathbb{P}^n$, we define the **affine cone of** Y to be

$$C(Y) := \theta^{-1}(Y) \cup \{(0, \ldots, 0)\} \subseteq \mathbb{A}^{n+1}$$

(the whole point of introducing the affine cone is to get some nice set in projective space, so it would be practical to have the origin in there).



Here are some properties:

- Let $q = [a_1, \dots, a_{n+1}] \in \mathbb{P}^n$. Then $C(\{q\})$ is the line in $\mathbb{A}^{n+1}$ through 0 and $(a_1, \dots, a_{n+1})$.
- $C(\varnothing) = \{0\}$.
- $C(Y_1 \cup Y_2) = C(Y_1) \cup C(Y_2)$ for all $Y_1, Y_2 \subset \mathbb{P}^n$.
- $C(Y_1) = C(Y_2)$ if and only if $Y_1 = Y_2$, for all $Y_1, Y_2 \subset \mathbb{P}^n$.
- If $\varnothing \neq Y \subset \mathbb{P}^n$, then
$$I_p(Y) = I_a(C(Y)).$$
Note: we cannot have $Y = \varnothing$, since
$$I_p(\varnothing) = k[x_1, \dots, x_n] \qquad \text{and} \qquad \langle x_1, \dots, x_{n+1}\rangle = I_a(0)$$
- If $I \subset k[x_1, \dots, x_{n+1}]$ is a homogeneous ideal, such that $V_a(I) \neq 0$, then
$$C(V_p(I)) = V_a(I). \tag{*}$$
In particular, if $\varnothing \neq Y \subset \mathbb{P}^n$, then
$$C(Y) = V_a(I) \iff Y = V_p(I).$$
Note: we cannot consider ideals I for which $V_a(I) = \varnothing$ because the affine cone is never empty, so (*) could not hold.

  Proof. The inclusion $C(V_p(I)) \subset V_a(I)$ holds, because if $q = [a_1 : \dots : a_{n+1}] \in V_p(I)$, then $(\lambda a_1, \dots, \lambda a_{n+1}) \in V_a(I)$ for all $\lambda \in k^*$. Thus
$$C(\{q\}) \subset V_a(I).$$
Conversely, if $(a_1, \dots, a_{n+1}) \in V_a(I)$, then since I is generated by forms (since it is homogeneous) this means $(\lambda a_1, \dots, \lambda a_{n+1}) \in V_a(I)$ for all $\lambda \in k^*$. Thus $[a_1 : \dots : a_{n+1}] \in V_p(I)$, so $V_a(I) \subset C(V_p(I))$. □
- Also, if $\varnothing \neq Y \subset \mathbb{P}^n$, then
$$C(Y) = V_a(I) \qquad \text{for some homogeneous ideal } I \subset k[x_1, \dots, x_{n+1}]$$
if and only if (since $V_a(I) = C(V_p(I))$) $C(Y) = C(V_p(I))$, iff $Y = V_p(I)$.

We can use these properties to compute I_p, V_p and also to find properties of I_p, V_p.

4.16 Example (projective algebraic sets). We have

- $\varnothing = V_p(1) = V_p(\langle x_1, \dots, x_{n+1}\rangle)$
- $\mathbb{P}^n = V_p(0)$.
- If $q = [a : b] \in \mathbb{P}^1$. Then, $C(\{q\})$ will be the line in $\mathbb{A}^2$ through 0 and (a, b), in other words,
$$C(\{q\}) = V_a(bx - ay).$$

Thus, by our properties,

$$I_p(\{q\}) = I_a(C(\{q\})) = I_a(V_a(\underbrace{bx - ay}_{\text{irred.}})) = \langle bx - ay \rangle.$$

In general, if $q = [a_1 : \ldots : a_{n+1}] \in \mathbb{P}^n$, and a_i is a nonzero coordinate of q, then

$$\{q\} = V_p(a_i x_1 - a_1 x_i, \ldots, a_i x_{n+1} - a_{n+1} x_i)$$

thus points in $\mathbb{P}^n$ are projective algebraic sets.

- $Y = V_p(x - y, x^2 - yz) \subset \mathbb{P}^2$ is a proj. alg. set. Then

$$C(Y) = V_a(x - y, x^2 - yz) = \{(0, 0, s) : s \in k\} \cup \{(t, t, t) : t \in k\}$$

so $Y = \{[0 : 0 : 1]\} \cup \{[1 : 1 : 1]\}$.

4.17 Example (IDEALS). We have:

- $I_a(C(\mathbb{P}^n)) = I_p(\mathbb{P}^n) = (0) = I_a(\mathbb{A}^{n+1})$.
- $I_p(\varnothing) = k[x_1, \ldots, x_{n+1}]$, but note that both $V_p(k[x_1, \ldots, x_{n+1}])$ and $V_p(\langle x_1, \ldots, x_{n+1} \rangle)$ are $\varnothing$, so there is not a one-to-one correspondence between the ideals and the sets.
- $I_p([a_1 : \ldots : a_{n+1}]) = \langle a_i x_1 - a_1 x_i, \ldots, a_i x_{n+1} - a_{n+1} x_i \rangle$ with $a_i \neq 0$, because

$$I_p([a_1 : \ldots : a_{n+1}]) = I_a(C([a_1 : \ldots : a_{n+1}]))$$

(exercise).

We have the following one-to-one correspondence:

Geometry	**Algebra**
projective alg. set $\neq \varnothing$	homogeneous radical ideals other than $k[x_1, \ldots, x_{n+1}]$ and $\langle x_1, \ldots, x_{n+1} \rangle$

4.18 Proposition. The union of two proj. alg. sets is proj. alg., and any intersection of proj. alg. sets is proj. alg. Moreover, $\varnothing$ and $\mathbb{P}^n$ are proj. alg.

4.19 Definition. The **Zariski topology** on $\mathbb{P}^n$ is defined by taking the closed sets to be the proj. alg. sets.

4.20 Example. We have:

1. $H_i = \{x_i = 0\}$ is a projective algebraic set for all i (so a closed set in the Zariski topology). Thus,

$$U_i = \{x_i \neq 0\} = \mathbb{P}^n \setminus H_i$$

is open for all i.

$$\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i \implies \{U_i\}_{i=1}^{n+1} \text{ is an open cover of } \mathbb{P}^n.$$

2. We have seen that $\mathbb{A}^n$ can be identified with $U_{n+1} = \{x_{n+1} \neq 0\}$ as follows:

$$\mathbb{A}^n \ni (a_1, \ldots, a_n) \overset{\iota}{\mapsto} [a_1 : \ldots : a_n : 1] \in U_{n+1}.$$

This means that any subset $X \subseteq \mathbb{A}^n$ can be thought of as a subset of $\mathbb{P}^n$ by identifying X with its image $\iota(X) \subset U_{n+1} \subset \mathbb{P}^n$. We then define the **projective closure of X in $\mathbb{P}^n$** to be the smallest projective algebraic subset of $\mathbb{P}^n$ containing X. In other words, the projective closure of X in $\mathbb{P}^n$ is

$$\overline{\iota(X)}$$

that is, the closure of $\iota(X)$ in the Zariski topology.

3. $X = V_a(y^2 - x^3) \subseteq \mathbb{A}^2 = U_z = \{z \neq 0\}$. Then consider

$$Y = V_p(zy^2 - x^3)$$

noting that $zy^2 - x^3$ is the same as $y^2 - x^3$ when $z = 1$ (i.e. at points on U_z).

$$[x : y : z] = [x/z : y/z : 1] \text{ if } z \neq 0.$$

$$Y = (Y \cap U_z) \cup (Y \cap H_\infty) = \iota(X) \cup \{[0 : 1 : 0]\}$$

(the one-point compactification of $\iota(X)$). Moreover, Y is proj. alg. and must be the projective closure of X in $\mathbb{P}^2$ since it's simply $\iota(X) \cup \{\text{pt}\}$.

4.21 Definition. A non-empty closed subset of $\mathbb{P}^n$ is **irreducible** if it cannot be expressed as the union of two proper non-empty closed subsets. A **projective algebraic variety** is an irreducible proj. alg. set in $\mathbb{P}^n$ equipped with the induced Zariski topology.

As in the affine case, we have the following.

4.22 Proposition. Let $Y \subseteq \mathbb{P}^n$ be a proj. alg. set. Then, Y is irreducible iff $I_p(Y)$ is prime.

Proof. Since Y is proj. alg., $I_p(Y)$ is homogeneous. So, to prove that $I_p(Y)$ is prime, we just have to check that if $f, g \in k[x_1, \ldots, x_{n+1}]$ are two forms such that $fg \in I_p(Y)$, then $f \in I_p(Y)$ or $g \in I_p(Y)$. The rest of the proof is identical to the affine case (exercise). □

4.23 Proposition. Let $Y \subseteq \mathbb{P}^n$. Then:

1. Y is proj. alg. subset of $\mathbb{P}^n$ if and only if $C(Y)$ is alg. subset of $\mathbb{A}^{n+1}$.
2. Y is irred. proj. alg. subset of $\mathbb{P}^n$ if and only if $C(Y)$ is an irred. alg. subset of $\mathbb{A}^{n+1}$.
3. If Y is proj. alg., then it is the union of a finite number of projective alg. irred. subsets.

Proof. Recall that

- If $Y \neq \varnothing$, then
$$I_p(Y) = I_a(C(Y))$$
- If $I \subset k[x_1, \ldots, x_{n+1}]$ is a homog. ideal such that $V_a(I) \neq \varnothing$, then $C(V_p(I)) = V_a(I)$.

We have:

1 & 2. $Y \neq \varnothing$ is (irred.) proj. alg. iff $I_p(Y)$ is radical (prime), iff $I_a(C(Y))$ is radical (prime), iff $C(Y)$ is alg. (irred.)

$$Y = \varnothing \iff C(Y) = \{(0, 0, \ldots, 0)\} \text{ both alg. (irred.)}$$

1. Suppose that Y is proj. alg. Then, $Y = V_p(I)$ for some homogeneous ideal I. Consider
$$\begin{aligned} C(Y) &= C(V_p(I)) \\ &= V_a(I) \text{ affine alg. set} \\ &= \tilde{W}_1 \cup \ldots \cup \tilde{W}_r, \end{aligned}$$
for some alg. sets $\tilde{W}_i$ in $\mathbb{A}^{n+1}$ irred. But, since each $\tilde{W}_i$ is alg.,
$$\tilde{W}_i = V_a(I_a(\tilde{W}_i)) = C(V_p(I_a(\tilde{W}_i)))$$
and thus
$$C(Y) = \bigcup_{i=1}^{r} C(V_p(I_a(\tilde{W}_i))) = C\left(\bigcup_{i=1}^{r} V_p(I_a(\tilde{W}_i))\right)$$
which occurs iff
$$Y = \bigcup_{i=1}^{r} V_p(I_a(\tilde{W}_i)).$$
Finally, note that each $V_p(I_a(\tilde{W}_i))$ is a irred. since it is the cone of the irred. affine alg. $\tilde{W}_i$. □

4.24 Remark. We can define the **(irredundant) irreducible decomposition** of a proj. alg. set as in the affine case. Moreover, given a proj. alg. set $Y \subseteq \mathbb{P}^n$, if the irreducible decomposition of $C(Y)$ is
$$C(Y) = \tilde{W}_1 \cup \ldots \cup \tilde{W}_r,$$
then the irred. decomp. of Y is
$$Y = W_1 \cup \ldots \cup W_r$$
with $W_i = V_p(I_a(\tilde{W}_i))$.

4.25 Example. We have:

1. $(k = \overline{k})$. If $f \in k[x_1, \ldots, x_{n+1}]$ is a form, then
$$V_p(f) \text{ irred.} \iff C(V_p(f)) = V_a(f) \text{ is irreducible} \iff f \text{ is irreducible}$$

2. If $Y = V_p(xz^3 + y^2z^2 - x^3z - x^2y^2) \subseteq \mathbb{P}^2$ irreducible? Here f is a 4-form, and

$$\begin{aligned} f &= z^4 \left[\left(\frac{x}{z}\right) + \left(\frac{y}{z}\right)^2 - \left(\frac{x}{z}\right)^3 - \left(\frac{x}{z}\right)^2 \left(\frac{y}{z}\right)^2 \right] \\ &= z^4[u + v^2 - u^3 - u^2v^2] \\ &= z^4[u + v^2][1 - u^2] \\ &= z^4[u + v^2][1 - u][1 + u] \\ &= z^4 \left[\frac{x}{z} + \left(\frac{y}{z}\right)^2\right] \left[1 - \frac{x}{z}\right] \left[1 + \frac{x}{z}\right] \\ &= [xz + y^2][z - x][z + x] \end{aligned}$$

where $u = x/z$, $v = y/z$. And these are all irreducible. So

$$Y = V_p(xz + y^2) \cup V_p(z - x) \cup V_p(z + x)$$

is the irreducible decomposition.

$k = \overline{k}$. Let I be an ideal in $k[x_1, \dots, x_{n+1}]$.

Recall the affine Nullstellensatz:

- $V_a(I) = \varnothing$ iff $I = k[x_1, \dots, x_{n+1}]$
- $V_a(I) \neq \varnothing$ iff $I_a(V_a(I)) = \sqrt{I}$.

4.26 Proposition (Projective Nullstellensatz). We have:

(i) $V_p(I) = \varnothing$ iff there is $N \in \mathbb{N}$ such that I contains all forms of degree $\geq N$.

(ii) If $V_p(I) \neq \varnothing$, then $I_p(V_p(I)) = \sqrt{I}$.

Proof. We have:

(i) Note that

$$\begin{aligned} V_p(I) = \varnothing &\iff V_a(I) = \varnothing \text{ or } V_a(I) = (0, \dots, 0) \in \mathbb{A}^{n+1} \\ &\iff V_a(I) \subset \{(0, \dots, 0)\} \\ &\iff \underbrace{I_a(\{(0, \dots, 0)\})}_{=\langle x_1, \dots, x_{n+1}\rangle} \subset \underbrace{I_a(V_a(I))}_{=\sqrt{I}}. \\ &\iff \langle x_1, \dots, x_{n+1}\rangle \subset \sqrt{I}. \\ &\iff \exists\, N_1, \dots, N_{n+1} > 0 \text{ such that } x_i^{N_i} \in I \\ &\iff \text{all forms of degree} \geq N \text{ are in } I, \text{ where } N = \max\{N_1, \dots, N_{n+1}\}. \end{aligned}$$

(ii) $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \sqrt{I}$. □

4.2 Rational functions on projective varieties

4.27 Definition. Let $I \subset k[x_1, \dots, x_{n+1}]$ be a homogeneous ideal. A residue class in $k[x_1, \dots, x_{n+1}]/I$ is called an **m-form** if it contains an m-form. In particular 0-forms in $k[x_1, \dots, x_{n+1}]/I$ are called **constant**.

4.28 Proposition. Let I be a homogeneous ideal in $k[x_1, \dots, x_{n+1}]$. Every $\overline{f} \in k[x_1, \dots, x_{n+1}]/I$ may be expressed *uniquely* as $\overline{f} = \overline{f_0} + \dots + \overline{f_d}$ where $d = \deg f$ and $\overline{f_i}$ is an i-form for all i. Note that some of the $\overline{f_i}$ may be zero.

Proof. Let $\overline{f} \in k[x_1, \dots, x_{n+1}]/I$. Then if

$$f = f_m + \dots + f_d$$

with f_i an i-form, we have that

$$\overline{f} = \overline{f_m} + \dots + \overline{f_d}$$

is a sum of forms in $k[x_1, \dots, x_{n+1}]/I$. For uniqueness, suppose that we also have

$$\overline{f} = \overline{g_{m'}} + \dots + \overline{g_{d'}},$$

with g_j a j-form. Then

$$\sum_i (\overline{f_i} - \overline{g_i}) = 0,$$

where we set $f_i = 0$ if $i < m$ or $i > d$, and $g_i = 0$ if $i < m'$ or $i > d'$. Thus

$$\sum_i (f_i - g_i) \in I.$$

Since the homogeneous component of $\sum_i (f_i - g_i)$ of degree i_0 is $(f_{i_0} - g_{i_0})$ and I is homogeneous, we must have $(f_{i_0} - g_{i_0}) \in I$, for all i_0. Thus,

$$\overline{f_i} = \overline{g_i}, \ \forall i$$

thus the decomposition $\overline{f} = \overline{f_0} + \ldots + \overline{f_d}$ is unique. □

4.29 Definition. Let $Y \subseteq \mathbb{P}^n$ be a projective variety, so that

$$I_p(Y) = I_a(C(Y))$$

is prime and homogeneous.

(i) $\Gamma_H(Y) := k[x_1, \ldots, x_{n+1}]/I_p(Y) = \Gamma(C(Y))$ is called the **homogeneous coordinate ring of** Y, which is an integral domain.

(ii) The field of fractions of $\Gamma_H(Y)$ is denoted by $k_H(Y)$, and is called the **homogeneous function field of** Y. (Note that $k_H(Y) = k(C(Y))$.)

(iii) $k(Y) := \{\overline{f}/\overline{g} \mid \overline{f}, \overline{g} \in \Gamma_H(Y)$ are forms of the same degree$\}$ is called the **function field of** Y.

Note $k \subseteq k(Y) \subseteq k_H(Y) = k(C(Y))$.

But, unlike the affine case, may not have $\Gamma_H(Y) \subset k(Y)$ i.e. only the constant polynomials can be considered as functions on Y.

Indeed, let $\overline{f} \in \Gamma_H(Y)$, and suppose that $\overline{f} = \overline{f_0} + \ldots + \overline{f_d}$ with $\overline{f_i}$ an i-form for all i. Then, $\overline{f}$ can be considered as a function on Y iff

$$f(x_1, \ldots, x_{n+1}) = f(\lambda x_1, \ldots, \lambda x_{n+1}) = f_0(x_1, \ldots, x_{n+1}) + \ldots + \lambda^d f_d(x_1, \ldots, x_{n+1})$$

for all $\lambda \in k^*$ and for all $[x_1 : \ldots : x_{n+1}] \in Y$. This is true if and only if $f_i \equiv 0$ on Y for every $i > 0$, iff $\overline{f}$ is constant.

Similarly, if $\overline{f}, \overline{g} \in \Gamma_H(Y)$, then $z = \overline{f}/\overline{g}$ is a well-defined function on Y iff

$$\frac{f(x_1, \ldots, x_{n+1})}{g(x_1, \ldots, x_{n+1})} = \frac{f(\lambda x_1, \ldots, \lambda x_{n+1})}{g(\lambda x_1, \ldots, \lambda x_{n+1})}$$

for every $p = [x_1 : \ldots : x_{n+1}] \in Y$ with $\overline{g}(p) \neq 0$ and $\lambda \in k^*$, iff f and g are forms of the same degree, say m, since then

$$\frac{f_m(\lambda x_1, \ldots, \lambda x_{n+1})}{g_m(\lambda x_1, \ldots, \lambda x_{n+1})} = \frac{\lambda^m f_m(x_1, \ldots, x_{n+1})}{\lambda^m g_m(x_1, \ldots, x_{n+1})} = \frac{f_m(x_1, \ldots, x_{n+1})}{g_m(x_1, \ldots, x_{n+1})}$$

for all $p = [x_1 : \ldots : x_{n+1}] \in Y$ with $\overline{g}(p) \neq 0$ and for all $\lambda \in k^*$.

4.30 Definition. If $p \in Y$ and $z \in k(Y)$, we say that z is **regular** (or **defined**) at p if there exist forms $\overline{f}, \overline{g} \in \Gamma_H(Y)$ of the same degree such that $\overline{g}(p) \neq 0$ and $z = \overline{f}/\overline{g}$ in which case $z(p) = \overline{f}(p)/\overline{g}(p)$ is the value of z at p. Otherwise p is called a **pole of** f.

One proves, as in the affine case, that for any $z, z' \in k(Y)$,

(i) The domain of z (which consists of all points in Y where z is defined) is an open set in Y.

(ii) The pole set of z (which is the set of all poles of z) is a closed subset of Y.

(iii) (Identity Theorem) If $z = z'$ on an open set $U \subseteq Y$, then $z = z'$ as elements of $k(Y)$.

Consequently $k(Y) = k(U)$ for any open set $U \subseteq Y$. In particular

$$k(Y) = k(Y \cap U_i)$$

for every affine open set $U_i := \{x_i \neq 0\} = \mathbb{A}^n \subseteq \mathbb{P}^n$.

4.31 Definition. Let Y be a projective variety in $\mathbb{P}^n$. Then,

$$\mathcal{O}_p(Y) = \{z \in k(Y) \mid z \text{ is regular at } p\}$$

is the **local ring of Y at** p, and

$$M_p(Y) = \{z \in \mathcal{O}_p(Y) \mid z(p) = 0\}$$

is the **maximal ideal of Y at** p, and

$$\mathcal{O}(Y) = \bigcap_{p \in Y} \mathcal{O}_p(Y) = \{z \in k(Y) \mid z \text{ is regular for all } p \in Y\}$$

is the **ring of regular functions on** Y.

Unlike the affine case, we don't have $\mathcal{O}(Y) = \Gamma_H(Y)$. Instead we have:

4.32 Proposition. $\mathcal{O}(Y) = k$ (assuming $k = \overline{k}$).

Proof. Since $k(Y) \subseteq k(C(Y))$, we have that

$$\mathcal{O}(Y) \subseteq \mathcal{O}(C(Y)) = \Gamma(C(Y)) = \Gamma_H(Y).$$

But the only elements of $\Gamma_H(Y)$ that represent functions are the constants. □

4.33 Definition. Let $Y \subseteq \mathbb{P}^n$ be a variety. The **dimension of** Y is defined as

$$\dim Y := \operatorname{trdeg}_k k(Y).$$

4.34 Remark. Since $k(Y) \cong k(U)$, for all open sets $U \subseteq Y$, we have that $\dim Y = \operatorname{trdeg}_k k(U)$. And in particular, $\dim Y = \dim(Y \cap U)$ for all affine open sets $U_i = \{x_i \neq 0\} = \mathbb{A}^n$. Thus dimension is local.

4.35 Example. $\dim \mathbb{P}^n = \dim \mathbb{A}^n = n$.

Projective varieties of dimension 1, 2 and m are called **curves**, **surfaces**, and **m-folds** for $m \geq 3$. Also, a projective variety in $\mathbb{P}^n$ of dimension $(n-1)$ is called a **hypersurface**.

4.36 Remark. One can show that $\dim Y = \dim(C(Y)) - 1$ (exercise).

4.37 Definition. Let $Y \subseteq \mathbb{P}^n$ be an r-dimensional projective variety, and let $p \in Y$. If $Y = V_p(f_1, \ldots, f_s)$ for some forms $f_1, \ldots, f_s \in k[x_1, \ldots, x_{n+1}]$, then

$$\operatorname{Jac}(f_1, \ldots, f_s)(p) = \left(\frac{\partial f_i}{\partial x_j}(p)\right)_{\substack{i=1,\ldots,s \\ j=1,\ldots,n+1}}$$

and $T_pY = \ker \operatorname{Jac}(f_1, \ldots, f_s)(p)$ is the **Zariski tangent space** of Y at p.

Also, Y is **smooth at** p iff $\dim_k T_p(Y) = r = \dim Y$ iff $\operatorname{Jac}(f_1, \ldots, f_s)(p)$ has rank $(n+1)-r$. Finally, Y is **smooth** iff Y is smooth at every $p \in Y$.

One shows, as in the affine case, that

(i) $T_p(Y) = (M_p(Y)/M_p^2(Y))^*$, hence since $M_p(Y) \cong M_p(Y \cap U_i)$ for all $i = 1, \ldots, n+1$, smoothness is a local property.

(ii) If Y is a projective curve, then Y is smooth at p iff $\mathcal{O}_p(Y)$ is a DVR.

4.38 Example. Let $Y = V_p(f) \subseteq \mathbb{P}^2$ with $f(x,y,z) = axy + bxz + cyz \in k[x,y,z]$. Then Y is smooth iff $a, b, c \neq 0$.

Proof. We have

$$\operatorname{Jac}(f) = \nabla f = \begin{bmatrix} ay + bz & ax + cz & bx + cy \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}.$$

This means that

$$\begin{aligned} ay + bz &= 0 \\ ax + cz &= 0 \\ bx + cy &= 0 \end{aligned} \tag{*}$$

Suppose that one of a, b or c is 0, say $a = 0$. Then, the following are solutions of (*):

$$\begin{aligned} x &= ct \\ y &= -bt, \qquad t \in k \\ z &= 0 \end{aligned}$$

which is a line through $(0,0,0)$ in $\mathbb{A}^3$. Thus Y is singular at $[c : -b : 0] \in \mathbb{P}^2$. Note that Y has dimension 1. □

4.3 Rational maps

4.39 Definition. Let $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$ be projective varieties. A map $\varphi : X \to Y$ is called **rational** if it can be written as

$$\varphi(p) = [F_1(p) : \ldots : F_{m+1}(p)] \qquad \forall\, p \in X,$$

for some forms $F_1, \ldots, F_{m+1} \in k[x_1, \ldots, x_{n+1}]$ of the same degree (i.e. $\deg F_1 = \ldots = \deg F_{m+1}$). Also, φ is **regular at** p if it is defined at p, which means that $F_1(p), \ldots, F_{m+1}(p)$ cannot be simultaneously 0. If φ is not defined at p, then p is a **pole of** φ. If φ is defined at every point in X, then it is called **regular**. Finally, a rational map is called a **birational equivalence** if φ has a rational inverse φ^{-1}, in which case X and Y are **birational**, denoted $X \sim Y$. If φ and φ^{-1} are both regular, then they are called **isomorphisms**, and X and Y are **isomorphic**, denoted $X \simeq Y$.

4.40 Remark. We have:

(i) If $F_1, \ldots, F_{m+1} \in k[x_1, \ldots, x_{n+1}]$ are forms of the same degree, say d, then

$$\begin{aligned}[F_1(\lambda x_1, \ldots, \lambda x_{n+1}) : \ldots : F_{m+1}(\lambda x_1, \ldots, \lambda x_{n+1})] &= [\lambda^d F_1(x_1, \ldots, x_{n+1}) : \ldots : \lambda^d F_{m+1}(x_1, \ldots, x_{n+1})] \\ &= [F_1(x_1, \ldots, x_{n+1}) : \ldots : F_{m+1}(x_1, \ldots, x_{n+1})]\end{aligned}$$

so $\varphi = [F_1 : \ldots : F_{m+1}]$ is a well-defined map.

(ii) One can also define a rational map $\varphi : X \to Y$ as a map that can be written as $\varphi(p) = [h_1(p) : \ldots : h_{m+1}(p)]$ with $h_i \in k(X)$ for all i. But then $h_i = \overline{f_i}/\overline{g_i}$ with $\overline{f_i}, \overline{g_i}$ forms of the same degree. Clearing denominators,

$$[h_1(p) : \ldots : h_{m+1}(p)] = [F_1(p) : \ldots : F_{m+1}(p)]$$

where $F_i := g_1 \cdots g_{i-1} f_i g_i \cdots g_{m+1}$ are forms of the same degree.

(iii) As in the affine case, we can define the pullback of a rational map $\varphi : X \to Y$:

$$\varphi^* : k(Y) \to k(X) \qquad z \mapsto z \circ \varphi.$$

Also, $X \sim Y$ (birational) iff $k(X) \simeq k(Y)$ as k-algebras.

(iv) As in the affine case, smoothness is preserved under isomorphism.

4.41 Example. We have:

1. Let $h : X \to k$ be a rational function. Then $h = \overline{f}/\overline{g}$ with $\overline{f}, \overline{g} \in \Gamma_H(X)$ forms of the same degree. Then, set

$$\begin{aligned}\varphi : X &\to \mathbb{P}^1 \\ q &\mapsto [\overline{f}(q) : \overline{g}(q)]\end{aligned}$$

So, φ is a rational map. Thus any rational function $f : X \to k$ can be thought of as a rational map from X to $\mathbb{P}^1$.

2. Any invertible matrix $A \in \mathrm{GL}(n+1, k)$ defines an isomorphism of $\mathbb{P}^n$.

$$\begin{aligned}T : \mathbb{P}^n &\to \mathbb{P}^n \\ q &\mapsto Aq,\end{aligned}$$

called a projective coordinate change. Note: this is like an affine coordinate change, except that $\mathbb{P}^n$ consists of lines through the origin in $\mathbb{A}^{n+1}$, so the coordinate change cannot involve a translation.

3. Let $Y = V_p(xz - y^2) \subset \mathbb{P}^2$. Define

$$\begin{aligned}\varphi : \mathbb{P}^1 &\to Y \\ [u : v] &\mapsto [u^2 : uv : v^2]\end{aligned}$$

Since u, v cannot be simultaneously zero (because $[u : v] \in \mathbb{P}^1$), we have that u^2, uv, v^2 are not simultaneously zero, so that φ is regular at every point. Moreover, φ has the following rational inverse:

$$\begin{aligned}\varphi^{-1} : Y \subseteq \mathbb{P}^2 &\to \mathbb{P}^1 \\ [x : y : z] &\mapsto \begin{cases} [x : y] & x \neq 0 \\ [y : z] & z \neq 0 \end{cases}\end{aligned}$$

Let's check that φ^{-1} is well-defined: given $[x : y : z]$ with $x, z \neq 0$, need to show that $[x : y] = [y : z]$. But,

$$[x : y] \underset{z\neq 0}{=} [xz : yz] \underset{\text{on } Y,\ xz = y^2}{=} [y^2 : yz] \underset{y \neq 0 \text{ since } x,\, z \neq 0}{=} [y : z].$$

Moreover, φ^{-1} is regular at every point on Y, so φ is an isomorphism.

4. Let $Y = V_p(y^2z - x^3) \subseteq \mathbb{P}^2$, and define $\varphi : \mathbb{P}^1 \to Y$ by

$$[u : v] \mapsto [u^2v : u^3 : v^3].$$

Since u and v are not simultaneously zero, neither are u^3 and v^3, so φ is regular at every point.

But, φ does not admit a regular inverse (i.e. φ is not an isomorphism). This is because if it were, then

$$Y \cap U_z = V_a(y^2 - x^3)$$

and φ would give an isomorphism between

$$\mathbb{A}^1 = \{[u : 1] \mid u \in k\} = \varphi^{-1}(Y \cap U_z),$$

which is impossible. Nonetheless, φ has the following rational inverse:

$$\begin{aligned} \varphi^{-1} : Y \subseteq \mathbb{P}^2 &\to \mathbb{P}^1 \\ [x : y : z] &\mapsto [y : x] \end{aligned}$$

thus $Y \sim \mathbb{P}^1$.

Note that

$$Y = \overbrace{(Y \cap U_z)}^{z=1} \cup \overbrace{(Y \cap H_\infty)}^{z=0} = V_a(y^2 - x^3) \cup \{[0 : 1 : 0]\}$$

is the projective closure of the cusp curve.

4.42 Proposition. Let C be a projective curve in $\mathbb{P}^n$, and let $\varphi : C \subseteq \mathbb{P}^n \to \mathbb{P}^n$ be a rational map. Then φ is regular at every smooth point of C.

Proof. Let p be a smooth point of C, so that $\mathcal{O}_p(C)$ is a DVR. Suppose that $M_p(C) = \langle t \rangle$. Moreover, assume that

$$\varphi(y) = [F_1(y) : \ldots : F_{m+1}(y)],$$

where $F_1, \ldots, F_{m+1}$ are forms of the same degree. Since F_i are forms, they are regular at p, so that $\overline{F_i} \in \mathcal{O}_p(C)$. Thus

$$\overline{F_i} = t^{m_i} u_i,$$

with $m_i \geq 0$ and u_i a unit in $\mathcal{O}_p(C)$, for all $i = 1, \ldots, m+1$. After possibly permuting the coordinates in $\mathbb{P}^m$, can assume that

$$m_1 \leq m_2 \leq \ldots \leq m_{m+1} (!).$$

So,

$$\varphi(p) = [t^{m_1}u_1 : \ldots : t^{m_{m+1}}u_{m+1}] = [u_1 : t^{m_2 - m_1}u_2 : \ldots : t^{m_{m+1} - m_1}u_{m+1}].$$

Now, $u_1(p) \neq 0$ since u_1 is a unit in $\mathcal{O}_p(C)$ thus φ is well-defined at p. □

4.43 Corollary. Let C and C' be smooth projective curves and let $\varphi : C \to C'$ be a birational equivalence. Then φ is an isomorphism.

Proof. φ is rational and has a rational inverse φ^{-1}. Since C and C' are smooth, by the proposition we have φ and φ^{-1} are regular at every point. □

5 Projective plane curves

From now on we only consider curves in $\mathbb{P}^2$.

5.1 Definition. Let $f \in k[x, y, z]$ be a non-constant form and consider the corresponding curve

$$C = V_p(f) \subseteq \mathbb{P}^2.$$

The **degree** of C is defined as the degree of f.

The local properties of C are given by restricting C to the affine open sets

$$U_x = \{x \neq 0\}, \qquad U_y = \{y \neq 0\}, \qquad U_z = \{z \neq 0\}$$

that cover $\mathbb{P}^2$, i.e. we study

$$\begin{aligned} C \cap U_x &= V_a(f(1, y, z)) \\ C \cap U_y &= V_a(f(x, 1, z)) \\ C \cap U_z &= V_a(f(x, y, 1)) \end{aligned}$$

In particular, if $q = [x_0 : y_0 : 1] \in C \cap U_z$, then the multiplicity of C at q is given by

$$m_q(C) = m_{(x_0,y_0)}(C \cap U_z) \qquad \text{(usual affine mult.)}$$

In particular, if q is a singular point, then (x_0, y_0) is a singular point of $C \cap U_z$, so

$$m_q(C) = m_{(x_0,y_0)}(C \cap U_z) \geq 2.$$

Intersection multiplicity is defined similarly. For example if C and D are projective plane curves and $q = [x_0 : 1 : z_0] \in C \cap D \cap U_y$ then

$$I(q, C \cap D) = I((x_0, z_0), (C \cap U_y) \cap (D \cap U_y)).$$

Note: since $k(C) \simeq k(C \cap U_x) \simeq k(C \cap U_y) \simeq k(C \cap U_z)$, these definitions are independent of the affine open (U_x, U_y, U_z) chosen.

5.2 Bézout's theorem

5.2 Theorem (Bézout). Let $C = V_p(f)$ and $D = V_p(g)$ be projective plane curves that do not have a common component. Then if C has degree m and D has degree n, C and D intersect in mn points counting multiplicity.

Note that $\deg C = \deg f = m$ and $\deg D = \deg g = n$. So the above reads

$$\sum_{q \in C \cap D} I(q, C \cap D) = mn = (\deg C)(\deg D).$$

5.3 Remark. We have:

1. The theorem tells us in particular that any two curves in $\mathbb{P}^2$ intersect in at least one point. Moreover, if C and D don't have a common component, the number of $\cap$ points is finite.
2. How does one find intersection points of curves in $\mathbb{P}^2$? If $C = V_p(f)$ and $D = V_p(g)$, to find $C \cap D$, solve the system

   $$\begin{aligned} f(x, y, z) &= 0 \\ g(x, y, z) &= 0 \end{aligned}$$

   or equivalently the two systems

   $$\begin{aligned} f(x, y, z) &= 0 \\ g(x, y, z) &= 0 \\ z &= 0 \end{aligned}$$

   (points on C and D on the line at infinity $\ell_\infty = \{z = 0\}$) and

   $$\begin{aligned} f(x, y, z) &= 0 \\ g(x, y, z) &= 0 \\ z &= 1 \end{aligned}$$

   (points on C and D away from ℓ_∞, that is, in $U_z = \{z \neq 0\}$). Discard $(0, 0, 0)$.

5.4 Example. Consider

$$\begin{aligned} f &= x^2 - y^2 + xz \\ g &= x + y \end{aligned}$$

Solve:

$$\begin{aligned} x^2 - y^2 + xz &= 0 \\ x + y &= 0 \\ z &= 0 \end{aligned}$$

so $y = -x$ and $z = 0$, thus we get one point: $[1 : -1 : 0]$ which is a point of intersection on the line at infinity. Note that we throw out $(0, 0, 0)$. Also

$$\begin{aligned} x^2 - y^2 + xz &= 0 \\ x + y &= 0 \\ z &= 1 \end{aligned}$$

so $y = -x = 0$ and $z = 1$. Thus we get only one point $[0 : 0 : 1]$. We find

$$C \cap D = \{[1 : -1 : 0], [0 : 0 : 1]\}$$

by Bézout's theorem, since $\deg C = \deg f = 2$ and $\deg D = \deg g = 1$, we cannot have more than $2 \cdot 1 = 2$ points of intersection counting multiplicity. This tells us in particular that we must have

$$I([1 : -1 : 0], C \cap D) = I([0 : 0 : 1], C \cap D) = 1.$$

Proof sketch of Bézout's theorem. Suppose that C and D don't have a common component. Then

- $C \cap D \neq \varnothing$
- $|C \cap D| < \infty$

which can be proved just by looking at the affine cone and figuring things out (Problem 2, Asmt 6). After an appropriate projective change of coordinates, we can assume that none of the intersection points lie on the line at infinity $\ell_\infty = \{z = 0\}$. So we can assume that

$$C \cap D \subset U_z = \{z \neq 0\}.$$

This means that $C \cap D$ can be obtained by solving the system of equations

$$\begin{aligned} f &= 0 \\ g &= 0 \\ z &= 1, \end{aligned}$$

i.e. $C \cap D = V_a(f(x, y, 1), g(x, y, 1))$. Hence for all $q \in C \cap D$,

$$I(q, C \cap D) = I(q, V_a(f(x, y, 1)) \cap V_a(g(x, y, 1))) = \dim_k \left(\frac{\mathcal{O}_q(\mathbb{A}^2)}{\langle f(x, y, 1), g(x, y, 1) \rangle \mathcal{O}_q(\mathbb{A}^2)} \right).$$

Need to show that

$$\sum_{q \in C \cap D} I(q, C \cap D) = mn.$$

But,

$$\sum_{q \in C \cap D} I(q, C \cap D) = \dim_k \left(\prod_{q \in C \cap D} \frac{\mathcal{O}_q(\mathbb{A}^2)}{\langle f(x, y, 1), g(x, y, 1) \rangle \mathcal{O}_q(\mathbb{A}^2)} \right)$$

The proof of Bézout's theorem now boils down to proving that this is a mn-dimensional k-vector space.

- Step 1: we have
$$\frac{k[x,y]}{\langle f(x,y,1), g(x,y,1)\rangle} \xrightarrow{\sim} \prod_{q\in C\cap D} \frac{\mathcal{O}_q(\mathbb{A}^2)}{\langle f(x,y,1), g(x,y,1)\rangle \mathcal{O}_q(\mathbb{A}^2)}$$
which, if we write $C\cap D = \{q_1,\ldots,q_\ell\}$,
$$\frac{\mathcal{O}_{q_1}(\mathbb{A}^2)}{\langle f,g\rangle \mathcal{O}_{q_1}(\mathbb{A}^2)} \times \ldots \times \frac{\mathcal{O}_{q_\ell}(\mathbb{A}^2)}{\langle f,g\rangle \mathcal{O}_{q_\ell}(\mathbb{A}^2)}$$

- Step 2:
$$\dim_k\left(\frac{k[x,y]}{\langle f(x,y,1), g(x,y,1)\rangle}\right) = mn.$$
because we mod out by f and g which have degree m and n respectively, so that any monomials of degree higher than m and n are annihilated. □

There are some immediate corollaries and applications of Bézout's theorem.

5.5 Corollary. We have
$$\sum_{q\in C\cap D} m_q(C)m_q(D) \le mn.$$

Proof. $I(q, C\cap D) \ge m_q(C)m_q(D)$ if C and D intersect properly at q. □

5.6 Corollary. If C and D intersect in mn distinct points, then these points are smooth on C and D, i.e. $m_q(C) = m_q(D) = 1$, for all $q\in C\cap D$.

Proof. If $|C\cap D| = mn$, then
$$mn \le \sum_{q\in C\cap D} \underbrace{m_q(C)}_{\ge 1}\underbrace{m_q(D)}_{\ge 1} \le mn$$
therefore
$$m_q(C)m_q(D) = 1, \qquad \forall q\in C\cap D$$
and thus $m_q(C) = m_q(D) = 1$ for all $q\in C\cap D$. □

5.7 Proposition. Any smooth projective plane curve is irreducible.

Proof. Suppose instead that $C = V_p(f)$ is reducible, so that $f = ab$ with a, b two forms of degree ≥ 1 and
$$C = \underbrace{V_p(a)}_{\neq\varnothing} \cup \underbrace{V_p(b)}_{\neq\varnothing}.$$

Then by Bézout's theorem,
$$V_p(a)\cap V_p(b) \neq \varnothing.$$

Fix $q\in V_p(a)\cap V_p(b)$. Then since $f = ab$,
$$m_q(C) = \underbrace{m_q(V_p(a))}_{\ge 1} + \underbrace{m_q(V_p(b))}_{\ge 1} \ge 2$$

the rest will be posted soon □

This has the following converse for curves of degree 2:

5.8 Proposition. Let C be an irreducible projective plane curve of degree 2. Then C is smooth.

Proof. Suppose instead that C is singular at q. Then $m_q(C)\ge 2$. Let q' be another point on C different from q.

[DIAGRAM ON CAMERA]

Let L be the line passing through q and q'. Since L is a line, $L = V_p(h)$ with h a 1-form and $\deg L = 1$. If L is not a component of C then by Bézout's theorem,
$$2 = (\deg C)(\deg L) \ge \sum_{q_0\in C\cap L} m_{q_0}(C)m_{q_0}(L) \ge \underbrace{m_q(C)}_{\ge 2}\underbrace{m_q(L)}_{\ge 1} + \underbrace{m_{q'}(C)}_{\ge 1}\underbrace{m_{q'}(L)}_{\ge 1} \ge 3$$
which is a contradiction. So L is a component of C, so C is not irreducible; again a contradiction which means that C is smooth. □

5.3 Divisors

Let C be a smooth projective plane curve.

5.9 Definition. A **divisor** on C is a formal sum of points

$$\sum_{p\in C} n_p p,$$

where $n_p \in \mathbb{Z}$ and all but finitely many n_p are zero.

5.10 Example. We have:

(i) $p-q$.

(ii) $2p+r-3q$.

Let $D=\sum_{p\in C} n_p p$ and $D'=\sum_{p\in C} n'_p p$ be two divisors. We define:

$$D+D' = \sum_{p\in C}(n_p+n'_p)p,$$

called the **sum** of D and D'. This is a well-defined divisor because only finitely many of the n_p and n'_p are nonzero.

5.11 Example. If $D=p-q$ and $D'=2p+r-3q$, then

$$D+D'=(p-q)+(2p+r-3q)=3p-4q+r.$$

Moreover if $n_p=0$ for all $p\in C$, we write $D=0$ and call it the **zero divisor**. The set of all divisors on C, denoted $\operatorname{Div}(C)$, is an abelian group where the inverse of $D=\sum_{p\in C} n_p p$ is

$$-D := \sum_{p\in C}(-n_p)p.$$

Finally, the **degree** of D is the sum

$$\deg(D)=\sum_{p\in C} n_p.$$

5.12 Remark. Note that non-zero divisors may have degree zero. For example if $p\neq q$ then consider

$$\deg(p-q)=0.$$

5.13 Definition. Let $g\in k[x,y,z]$ be a form. Then if $\overline{g}\neq 0$ in $\Gamma_H(C)$, we define the **divisor of** $\overline{g}$ to be

$$\operatorname{div}(\overline{g}) := \sum_{p\in C} \underbrace{\operatorname{ord}_p^C(\overline{g})}_{=n_p}\, p.$$

5.14 Remark. We have:

1. Note that since g is polynomial,
$$\operatorname{ord}_p^C(\overline{g})\geq 0$$
for all $p\in C$ and
$$\operatorname{ord}_p^C(\overline{g})=0 \iff g(p)\neq 0.$$
Thus the only points appearing in $\operatorname{div}(\overline{g})$ are the zeroes of $\overline{g}$ on C (with their respective multiplicities). So we can interpret $\operatorname{div}(\overline{g})$ as being the divisor of zeroes of $\overline{g}$ on C.

2. Since $\overline{g}\neq 0$ in $\Gamma_H(C)$, we have that $\overline{g}$ cannot vanish at every point in C and so C is not a component of $V_p(g)$, so C and $V_p(g)$ don't have a common component since C is irreducible. Then by Bézout's theorem,
$$\deg(\operatorname{div}(\overline{g})) = \sum_{q\in C\cap V_p(g)} \operatorname{ord}_p^C(\overline{g}) = \sum_{q\in C\cap V_p(g)} I(q, C\cap V_p(g)) = \deg(C)\cdot\deg(V_p(g)) = \deg(C)\cdot\deg(g).$$
Therefore,
$$\deg(\operatorname{div}(\overline{g}))=\deg(C)\deg(g)$$

and $\operatorname{div}(\overline{g})$ is the divisor of intersection points of C with $V_p(g)$ counting multiplicity.

$$= \sum_{q \in C \cap V_p(g)} I(q, C \cap V_p(g))q.$$

Thus, divisors of forms encode zeroes of polynomials on a variety *or* intersections of varieties. Here they're just points since we're on a curve, but in higher dimensions, divisors will be formal sums of hypersurfaces.

5.15 Example. We have:

1. If $g \equiv \alpha$, $\alpha \in k$ (i.e. a 0-form), then $\operatorname{div}(\overline{g}) = 0$.
2. Let $C = V_p(xy - z^2)$ and $g = x - y$. Then,

$$\deg(\operatorname{div}(g)) = (\deg C)(\deg g) = 2 \cdot 1 = 2$$

so the divisor can't contain more than 2 points (since all coefficients $n_p \geq 0$ here). Also,

$$C \cap V_p(x-y) = \{[1:1:1], [-1:-1:1]\}$$

thus by Bézout's theorem

$$I([1:1:1], C \cap V_p(x-y)) = I([-1:-1:1], C \cap V_p(x-y)) = 1$$

because there are 2 distinct intersection points. Thus,

$$\operatorname{div}(x-y) = [1:1:1] + [-1:-1:1]$$

5.16 Definition. A divisor $D = \sum_{p \in C} n_p p$ is called **effective** if $n_p \geq 0$, for every $p \in C$. We denote this by $D \geq 0$. Also, given two divisors D, D' we write $D \geq D'$ if and only if $D - D' \geq 0$.

5.17 Remark. If $D = \sum_{p \in C} n_p p$ and $D' = \sum_{p \in C} n'_p p$ then

$$D \geq D' \iff n_p \geq n'_p \quad \forall p \in C.$$

5.18 Example. We have:

(i) $D = p + 2q + r \geq 0$.

(ii) $D = -2p \ngeq 0$.

(iii) $\operatorname{div}(\overline{g}) \geq 0$, for any form $g \in k[x,y,z]$.

So, the divisor of any form is effective. Is the converse true?

Question: If $D \geq 0$, does there exist a form $g \in k[x,y,z]$ such that $D = \operatorname{div}(g)$?

Answer: No, if $\deg(C) \geq 2$.

If $\deg(C) = 1$, YES. In this case, because it's degree 1, $C = V_p(f)$ with f a 1-form. So C is a line. Let $D = p_1 + \ldots + p_m$ be a divisor on C. Consider the point p_i appearing in D. Let L_i be another line in $\mathbb{P}^2$ passing through p_i other than C. Then, $L_i = V(h_i)$ for some 1-form $h_i \in k[x,y,z]$ and $\overline{h_i} \neq 0$ in $\Gamma_H(C)$. Thus

$$\operatorname{div}(\overline{h_i}) \overset{*}{=} L_i \cap C = p_i$$

where (*) holds since $\deg(L_i) = \deg(C)$. This is possible for all $i = 1, \ldots, m$ and so, we get

$$\operatorname{div}(\underbrace{\overline{h_1 h_2} \cdots \overline{h_m}}_{m\text{-form}}) = p_1 + \ldots + p_m.$$

If $\deg(C) \geq 2$, NO. In this case, if g is an m-form such that $\overline{g} \neq 0$ in $\Gamma_H(C)$, we have:

$$\deg(\operatorname{div}(g)) = (\deg C)\underbrace{(\deg g)}_{=m} = m \deg(C) \geq 2m.$$

So, if $m = 0$ then $\operatorname{div}(\overline{g}) = 0$. If $m \geq 1$, then $\deg(\operatorname{div}(\overline{g})) \geq 2$. So, if D is a divisor on C of degree 1 (so that $D = p$ for some $p \in C$), we cannot have $D = \operatorname{div}(\overline{g})$ for some form $g \in k[x,y,z]$.

5.19 Definition. If $z \in k(C)$ is non-zero, we define the **divisor of** z by

$$\operatorname{div}(z) := \sum_{p \in C} \operatorname{ord}_p^C(z) p.$$

Recall that

$$\operatorname{ord}_p^C(z) > 0 \iff z \text{ has a zero at } p$$
$$\operatorname{ord}_p^C(z) = 0 \iff z \text{ is defined and nonzero at } p$$
$$\operatorname{ord}_p^C(z) < 0 \iff z \text{ has a pole at } p.$$

So, $\operatorname{ord}_p^C(z) \neq 0$ if and only if p is a zero or a pole of z. So the only points appearing in $\operatorname{div}(z)$ are the zeroes and poles of z of which there are only finitely many (since they form a proper algebraic subset of C). Thus, $\operatorname{div}(z)$ is a well-defined divisor.

Moreover, we have seen that if $z = \overline{g}/\overline{g'}$, where g and g' are forms of the same degree,

$$\operatorname{ord}_p^C(z) = \operatorname{ord}_p^C(\overline{g}) - \operatorname{ord}_p^C(\overline{g'})$$

(for any g, g' such that $z = \overline{g}/\overline{g'}$) so

$$\operatorname{div}(z) = \operatorname{div}(\overline{g}) - \operatorname{div}(\overline{g'}).$$

Also, we get that

$$\deg(\operatorname{div}(z)) = 0$$

(since $m = \deg(g) = \deg(g')$ and so $\deg(\operatorname{div}(\overline{g})) = \deg(\operatorname{div}(\overline{g'})) = (\deg C) \cdot m$). As a consequence:

5.20 Proposition. If $z \in k(C)$, then z has the same number of zeroes and poles (of course, counting multiplicity).

Finally, from the properties of the order function, we get:

- $\operatorname{div}(zz') = \operatorname{div}(z) + \operatorname{div}(z')$
- $\operatorname{div}(1/z) = -\operatorname{div}(z)$

for any two rational functions $z, z' \in k(C)$ (exercise).

We have just seen that the divisor of a rational function always has degree 0.

5.21 Definition. Let D be a divisor on C of degree 0. Then D will be called **principal** if $D = \operatorname{div}(z)$ for some $z \in k(C)$.

5.22 Definition. Denote

$$\operatorname{Div}^0(C) := \{D \in \operatorname{Div}(C) \mid \deg(D) = 0\}$$

and

$$P(C) := \{D \in \operatorname{Div}^0(C) \mid D = \operatorname{div}(z) \text{ for some } z \in k(C)\}$$

5.23 Remark. We have:

- $\operatorname{Div}^0(C)$ is a subgroup of $\operatorname{Div}(C)$ since if $D, D' \in \operatorname{Div}^0(C)$,

$$\deg(D + D') = \deg D + \deg D' = 0$$

- $P(C)$ is a subgroup of $\operatorname{Div}^0(C)$ since if $D, D' \in P(C)$ then $D = \operatorname{div}(z)$ and $D' = \operatorname{div}(z')$, for some $z, z' \in k(C)$. So,

$$D + D' = \operatorname{div}(zz') \in P(C).$$

5.24 Definition. We define the **divisor class group of** C by

$$\mathcal{C}\ell^0(C) := \frac{\operatorname{Div}^0(C)}{P(C)}.$$

We say that $D, D' \in \operatorname{Div}^0(C)$ are **linearly equivalent**, written $D \equiv D'$, if $D - D' \in P(C)$ (i.e. if D and D' are in the same equivalence class in $\mathcal{C}\ell^0(C)$.

We have that the divisor of any rational function on C has degree 0. Is the converse true? YES iff $\mathcal{C}\ell^0(C) = (0)$ (iff $\operatorname{Div}^0(C) = P(C)$).

5.25 Example. We have:

1. If $C = \mathbb{P}^1$ (i.e. $C = V_p(f)$ with f a 1-form) then $\mathcal{C}\ell^0(\mathbb{P}^1) = (0)$.

   Proof. Let $D \in \mathrm{Div}^0(\mathbb{P}^1)$. Then,

   $$D = p_1 + p_2 + \ldots + p_m - q_1 - q_2 - \ldots - q_m$$

   Suppose that $p_i = [a_i : b_i]$ and $q_i = [c_i : d_i]$. Then

   $$z = \frac{(b_1x - a_1y)\cdots(b_mx - a_my)}{(d_1x - c_1y)\cdots(d_mx - c_my)}$$

   has divisor equal to D. Thus $D \in P(C)$ and thus $\mathrm{Div}^0(C) = P(C)$. □

2. Suppose that C has degree 2. Let $D \in \mathrm{Div}^0(C)$ so that

   $$D = p_1 + p_2 + \ldots + p_m - q_1 - q_2 - \ldots - q_m$$

   If we can find $z_i \in k(C)$ with $\mathrm{div}(z_i) = p_i - q_i$, then $\mathrm{div}(z_1 \cdots z_m) = D$, showing that $\mathrm{Div}^0(C) = P(C)$ thus $\mathcal{C}\ell^0(C) = 0$. [see camera for diagram]. Let $r \in C$ that's not p_i or q_i. $L = V_p(h)$ and $L' = V_p(h')$ with h, h' 1-forms. By Bézout, since $\deg(C) = 2$,

   $$\mathrm{div}(\overline{h}) = L \cap C = r + p_i$$
   $$\mathrm{div}(\overline{h'}) = L' \cap C = r + q_i$$

   thus

   $$\mathrm{div}(\overline{h}/\overline{h'}) = (r + p_i) - (r + q_i) = p_i - q_i.$$

5.26 Theorem. If C is a smooth projective plane curve of degree ≥ 3, then:

$$(\exists z \in k(C) \text{ with } \mathrm{div}(z) = p - q) \iff p = q.$$

5.27 Corollary. $\mathcal{C}\ell^0(C) \neq \{0\}$ if $\deg(C) \geq 3$.

We have seen that birational smooth projective plane curves are in fact isomorphic. Moreover, it is clear from the definition that if $C \cong C'$, then $\mathcal{C}\ell^0(C) \cong \mathcal{C}\ell^0(C')$. We then have:

5.28 Corollary. If C is a smooth proj. plane curve of degree $d \geq 3$, then $C \not\sim P'$ (i.e. C is not rational).

Proof. Since $\deg(C) \geq 3$,

$$\mathcal{C}\ell^0(C) \not\cong \{0\} = \mathcal{C}\ell^0(\mathbb{P}^1) \implies C \not\sim \mathbb{P}^1.$$

□

Before proving the theorem, we first need the following lemma.

5.29 Lemma. Let C be a smooth projective plane curve. If $g, h \in k[x, y, z]$ are forms of possibly different degrees such that $\mathrm{div}(\overline{g}) \geq \mathrm{div}(\overline{h})$, then there exists a form $b \in k[x, y, z]$ such that $\overline{g} = \overline{b} \cdot \overline{h}$. This implies in particular that $\mathrm{div}(\overline{g}) = \mathrm{div}(\overline{b}) + \mathrm{div}(\overline{h})$.

Proof. After a possible coordinate change, we can assume that none of the points appearing in $\mathrm{div}(\overline{g})$ and $\mathrm{div}(\overline{h})$ are on ℓ_∞. Can assume that these points lie in $C \cap U_z$. Then for all $p \in C \cap U_z$, we have $p = [x_0 : y_0 : 1]$. Also, since $\mathrm{div}(\overline{g}) \geq \mathrm{div}(\overline{h})$, we have that

$$\mathrm{ord}_p^{C\cap U_z}(\overline{g(x,y,1)}) \geq \mathrm{ord}_p^{C\cap U_z}(\overline{h}(x,y,1)) \implies \mathrm{ord}_p^{C\cap U_z}\left(\frac{\overline{g(x,y,1)}}{\overline{h(x,y,1)}}\right) \geq 0.$$

Therefore,

$$\frac{\overline{g(x,y,1)}}{\overline{h(x,y,1)}}$$

is a rational function on $C \cap U_z$ that is defined and regular at every point in $C \cap U_z$, therefore

$$\frac{\overline{g(x,y,1)}}{\overline{h(x,y,1)}} \in \mathcal{O}(C \cap U_z) = \Gamma(C \cap U_z)$$

therefore

$$\frac{\overline{g(x,y,1)}}{\overline{h(x,y,1)}} = \overline{b_0(x,y)}$$

for some $b_0 \in k[x,y]$. Homogenize to get

$$g(x,y,z) = h(x,y,z)\underbrace{b_0(x,y,z)}_{=:\bar{b}}. \qquad \square$$

Proof of theorem. ($\leftarrow$) If $p = q$ implies $p - q = 0$ therefore pick $z = 1$; $\operatorname{div}(z) = 0$.

($\rightarrow$) Suppose that there exists $z \in k(C)$ such that $\operatorname{div}(z) = p - q$. Let $L = V_p(h)$, with h a 1-form, be a line through p. Then, by Bézout, $L \cap C$ consists of d points counting multiplicity (since $\deg L = 1$ and $\deg C = d$):

$$L \cap C = p + r_1 + \ldots + r_{d-1}$$

for some $r_i \in C$. Note that since $L = V_p(h)$, we have that $\operatorname{div}(\overline{h}) = L \cap C = p + r_1 + \ldots + r_{d-1}$. Suppose that $z = \overline{g}/\overline{g'}$, for some form $g, g' \in k[x,y,z]$ of the same degree. Then, $\operatorname{div}(z) = \operatorname{div}(\overline{g}) - \operatorname{div}(\overline{g'})$, so

$$\operatorname{div}(\overline{g'h}) = \operatorname{div}(\overline{g'}) + \operatorname{div}(\overline{h}) = (\operatorname{div}(\overline{g}) - \operatorname{div}(z)) + \operatorname{div}(\overline{h}) = \operatorname{div}(\overline{g}) + \underbrace{q + r_1 + \ldots + r_{d-1}}_{\geq 0} \geq \operatorname{div}(\overline{g}).$$

Thus by the Lemma, there exists a form $h' \in k[x,y,z]$ such that

$$(\overline{g'}h) = \overline{h'}g \implies \deg \overline{h'} = 1.$$

Thus, there exists a 1-form h' such that

$$\operatorname{div}(\overline{h'}) = \operatorname{div}(\overline{g'h}) - \operatorname{div}(\overline{g}) = q + r_1 + \ldots + r_{d-1}$$

Let $L' = V_p(h')$ which is a line in $\mathbb{P}^2$ passing through p.

- If $r_i = r_j$ for some i, j, then $L = L'$ since they pass through the same points.
- If $r = r_1 = \ldots = r_{d-1}$, then
  $$I(r, C \cap L), I(r, C \cap L') \geq 2$$
  thus L, L' are tangent lines to C at r. But C is smooth at r so C has a unique tangent line. Thus $L = L'$. Finally since $L = L'$, this forces
  $$p + r_1 + \ldots + r_{d-1} = q + r_1 + \ldots + r_{d-1} \implies p = q. \qquad \square$$

5.4 Elliptic curves

5.30 Definition. An **elliptic curve** is a smooth projective plane curve of degree 3 together with a distinguished point p_0. After a coordinate change, an elliptic curve C is of the form

$$y^2 z + b_1 xy + b_2 yz^2 = x^3 + a_1 x^2 z + a_2 xz^2 + a_3 z^3, \qquad p_0 = [0:1:0].$$

- $p_0 \in \ell_\infty$
- $\ell_\infty = V_p(z)$ is tangent to C at p_0 and $\operatorname{div}(z) = L \cap C = 3p_0$.

5.31 Proposition. Let (C, p_0) be an elliptic curve. Then:

1. If $(p - p_0) \in \mathcal{C}\ell^0(C)$, then $-(p - p_0) \equiv (t - p_0) \in \mathcal{C}\ell^0(C)$ for some $t \in C$
2. If $(p - p_0)(q - q_0) \in \mathcal{C}\ell^0(C)$ then $(p - p_0) + (q - q_0) \equiv t - p_0 \in \mathcal{C}\ell^0(C)$ for some $t \in C$.

Proof. We have:

1. $L = V_p(h)$. $\deg C = 3$. $L \cap C = p + p_0 + t = \operatorname{div}(h)$. Thus
   $$0 \equiv \operatorname{div}(h/z) = \operatorname{div}(h) - \operatorname{div}(z) = p + p_0 + t - 3p_0 = (p - p_0) + (t - p_0) \implies t - p_0 = -(p - p_0).$$
2. $L \cap C = p + q + r = \operatorname{div}(h')$ (haven't finished copying)

$\square$