# Algebraic Geometry

April 24, 2024

## Contents

### Lectures

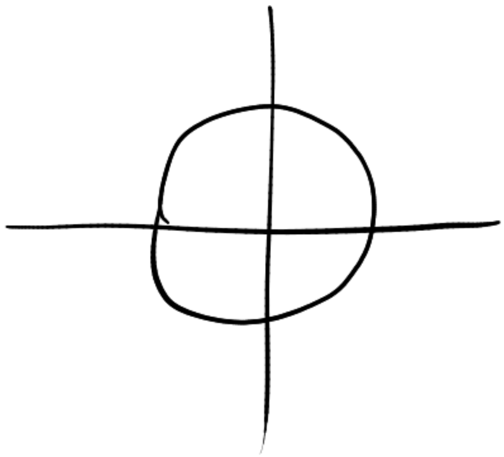
Start of lecture 1

**What is Algebraic Geometry?**

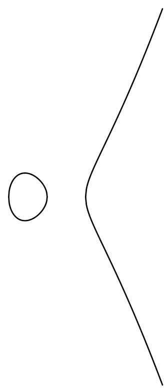
Study of solution sets to systems of polynomial equations.

For example:

- $\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$



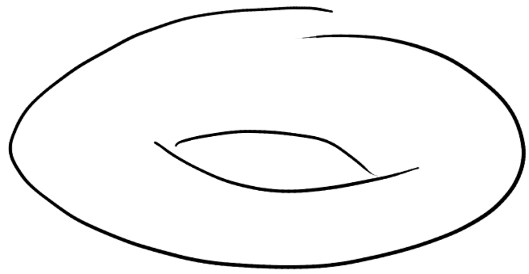
- $\{(x,y) \in \mathbb{R}^2 \mid y^2 = x^3 - x\}$



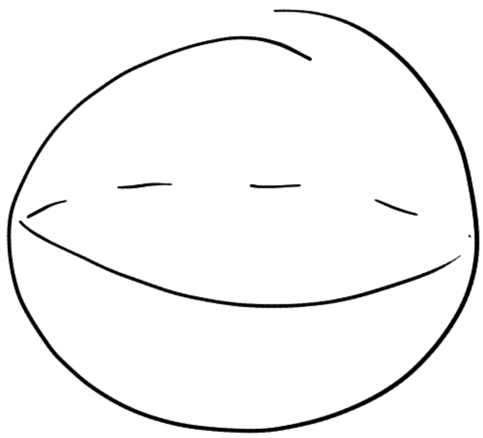
We could look for solutions over $\mathbb{C}$:

$$\{(x,y) \in \mathbb{C}^2 \mid y^2 = x^3 - x\}$$

'Looks like' a torus with one point removed.



$\mathbb{R}^3$: $x^2 + y^2 + z^2 = 1$



$\{(x, y, z) \in \mathbb{C}^3 \mid x^3 + y^3 + z^3 = 1\} = X$. $X$ contains 27 lines:

$$9 \text{ lines} : \begin{cases} x = -\xi^j y \\ z = \xi^k \end{cases}$$

$$9 \text{ lines} : \begin{cases} x = -\xi^j z \\ y = \xi^k \end{cases}$$

$$9 \text{ lines} : \begin{cases} y = -\xi^j z \\ x = \xi^k \end{cases}$$

(where $\xi = e^{2\pi i/4}$).

# 1 Affine Varieties

## 1.1 Basic setup

Fix a field $\mathbb{K}$.

**Definition** (Affine $n$-space)**.** Affine $n$-space over $\mathbb{K}$ is $\mathbb{A}^n = \mathbb{K}^n$.

**Definition** (Zero set)**.** Let $A := \mathbb{K}[X_1, \dots, X_n]$, $S \subset A$ a subset. Define

$$\begin{aligned} Z(S) &:= \text{“zero set of } S\text{”} \\ &= \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid f(a_1, \dots, a_n) = 0 \ \forall f \in S\} \end{aligned}$$

**Proposition.** Basic properties of the zero set:

(a) $Z(\{0\}) = \mathbb{A}^n$.

(b) $Z(A) = \emptyset$.

(c) $Z(S_1 \cdot S_2) = Z(S_1) \cup Z(S_2)$ where

$$S_1 \cdot S_2 = \{f \cdot g \mid f \in S_1, g \in S_2\}.$$

(d) Let $I$ be an index set and suppose for each $i \in I$, we are given $S_i \subset A$. Then

$$\bigcap_{i \in I} Z(S_i) = Z\left(\bigcup_{i \in I} S_i\right).$$

*Proof.*

(a) Obvious

(b) Obvious

(c) If $p \in Z(S_1) \cup Z(S_2)$, then either $f(p) = 0 \ \forall f \in S_1$ or $g(p) = 0 \ \forall g \in S_2$. Thus $(f \cdot g)(p) = 0$ for all $f \in S_1$, $g \in S_2$. So $p \in Z(S_1 \cdot S_2)$.

Conversely, suppose $p \in Z(S_1 \cdot S_2)$, and suppose $p \notin Z(S_1)$. So there exists $f \in S_1$ with $f(p) \neq 0$. But $(f \cdot g)(p) = 0 \ \forall g \in S_2$ and $(f \cdot g)(p) = f(p) \cdot g(p)$, so $g(p) =$

$0\ \forall g \in S_2$. Thus $p \in Z(S_2)$. Thus $Z(S_1 \cdot S_2) \subseteq Z(S_1) \cup Z(S_2)$.

(d) If $p \in Z(S_1)\ \forall i$, then $p \in Z\left(\bigcup_{i \in I} S_i\right)$.

Conversely, if $p \in Z\left(\bigcup_{i \in I} S_i\right)$, then $p \in Z(S_i)\ \forall i$, so $p \in \bigcap_{i \in I} Z(S_i)$. □

**Moral:** This says that sets of the form $Z(S)$ form the closed sets of a topology on $\mathbb{A}^n$

**Moral:** This says that sets of the form $Z(S)$ form the closed sets of a topology on $\mathbb{A}^n$.

**Definition** (Algebraic subset)**.** A subset of $\mathbb{A}^n$ is *algebraic* (or *Zariski closed*) if it is of the form $Z(S)$ for some $S \subset A$.

**Definition** (Zariski open subset)**.** A *Zariski open subset* of $\mathbb{A}^n$ is a set of the form $\mathbb{A}^n \setminus Z(S)$ for some $S \subseteq A$. This defines the Zariski topology on $\mathbb{A}^n$.

**Example.**

(1) If $K = \mathbb{C}$, Zariski open or closed subsets are also open and closed in the "usual" topology.

(2) For any $\mathbb{K}$, consider $\mathbb{A}^1$, $A = \mathbb{K}[X]$, $S \subseteq \mathbb{K}[X]$ containing a non-zero element. Then $Z(S)$ is finite. So Zariski closed sets are $\mathbb{A}^1$ and all finite sets. Zariski open sets are $\emptyset$ and "co-finite sets".

**Recall:** If $A$ is a commutative ring, $S \subseteq A$ a subset, the *ideal generated by* $S$ is the ideal $\langle S \rangle \subseteq A$ given by

$$\begin{aligned}\langle S \rangle &= \left\{ \sum_{i=1}^{q} f_i g_i \mid q \geq 0, f_i \in S, g_i \in A \right\} \\ &= \text{the smallest ideal of } A \text{ containing } S\end{aligned}$$

**Lemma.** Let $S \subseteq A = \mathbb{K}[X_1, \ldots, X_n]$, $I = \langle S \rangle$. Then

$$Z(S) = Z(I).$$

*Proof.* If $p \in Z(S)$, $f_1, \dots, f_q \in S$, $g_1, \dots, g_q \in A$, then

$$\sum_{i=1}^{q} (f_i g_i)(p) = \sum_{i=1}^{q} \underbrace{f_i(p)}_{=0} g_i(p) = 0.$$

Thus $Z(S) \subseteq Z(I)$.

Conversely, since $S \subseteq I$, $Z(I) \subseteq Z(S)$. □

Start of lecture 2

**Definition** (Ideal of a set)**.** Let $X \subseteq \mathbb{A}^n$ be a subset. Define

$$I(X) = \{f \in A = \mathbb{K}[X_1, \dots, X_n] \mid f(p) = 0 \ \forall p \in X\}.$$

**Remark.** $I(X)$ is an ideal: if $f, g \in I(X)$, then $f + g \in I(X)$. If $f \in A$, $g \in I(X)$ then $f \cdot g \in I(X)$.

**Remark.** If $S_1 \subseteq S_2 \subseteq A$, then $Z(S_2) \subseteq Z(S_1)$. If $X_1 \subseteq X_2 \subseteq \mathbb{A}^n$, then $I(X_2) \subseteq I(X_1)$.

**Question:** Given an ideal $I$, what is the relationship between $I$ and $I(Z(I))$?

**Example.** $I = \langle x^2 \rangle \leq \mathbb{K}[X]$.

$$Z(I) = \{0\} \subseteq \mathbb{A}^1, \qquad I(Z(I)) = I(\{0\}) = \langle X \rangle \neq I.$$

**Definition** (Radical of an ideal)**.** Let $I \subseteq A$ be an ideal in a commutative ring $A$. The *radical* of $I$ is

$$\sqrt{I} := \{f \in A \mid f^n \in I \text{ for some } n > 0\}.$$

**Lemma.** $\sqrt{I}$ is an ideal.

*Proof.* Suppose $f, g \in \sqrt{I}$, say $f^{n_1}, g^{n_2} \in I$. Then

$$(f+g)^{n_1+n_2+1} = \sum_{i=0}^{n_1+n_2+1} \binom{n_1+n_2+1}{i} f^i g^{n_1+n_2+1-i}$$

For each $i$, either $i \geq n_1$ or $(n_1 + n_2 + 1) - i \geq n_2$. So each term lies in $I$, hence $(f+g)^{n_1+n_2+1} \in I$. Thus $f + g \in \sqrt{I}$. If $f \in \sqrt{I}$, $g \in A$, then $f^n \in I$ for some $n$, so $(fg)^n \in I$ so $fg \in \sqrt{I}$. □

**Proposition.**

(a) If $X \subseteq \mathbb{A}^n$ is algebraic, then

$$Z(I(X)) = X.$$

(b) If $I \subseteq A$ is an ideal, then

$$\sqrt{I} \subseteq I(Z(I)).$$

*Proof.*

(a) Since $X$ is algebraic, $X = Z(I)$ for some $I$. Certainly, $I \subseteq I(X)$ by definition of $Z$ and $I(X)$. Thus $Z(I(X)) \subseteq Z(I) = X$. But $X \subseteq Z(I(X))$ is obvious.

(b) Let $f^n \in I$. Then $f^n$ vanishes on $Z(I)$, and hence $f$ vanishes on $Z(I)$ also. So $f \in I(Z(I))$, hence $\sqrt{I} \subseteq I(Z(I))$. □

**Theorem** (Hilbert's Nullstellensatz)**.** Let $\mathbb{K}$ be an algebraically closed field. Then

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

*Proof.* Later. □

**Example.** $\mathbb{K} = \mathbb{R}$. $I = \langle X^2 + Y^2 + 1 \rangle \subseteq \mathbb{R}[X, Y]$. Then $Z(I) = \emptyset$, $I(Z(I)) = \mathbb{R}[X, Y] \neq \sqrt{I}$.

## 1.2 Irreducible Subsets

**Definition** (Irreducible subset)**.** Let $X$ be a topological space, and $Z \subseteq X$ a closed subset. We say $Z$ is *irreducible*, if $Z$ is non-empty, and whenever $Z = Z_1 \cup Z_2$ with $Z_1, Z_2$ closed in $X$, then either $Z = Z_1$ or $Z = Z_2$.

**Remark.** Bad notion in the Euclidean topology in $\mathbb{C}^n$. Only irreducible sets are points.

**Example.** $\mathbb{A}^1$ is irreducible as long as $\mathbb{K}$ is infinite.

**Definition** (Affine algebraic variety)**.** An *(affine algebraic) variety* in $\mathbb{A}^n$ is an irreducible algebraic set.

How do we recognize irreducible algebraic sets algebraically?

**Proposition.** If $X_1, X_2 \subseteq \mathbb{A}^n$, then

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

*Proof.* Since $X_1, X_2 \subseteq X_1 \cup X_2$, we have $I(X_1 \cup X_2) \subseteq I(X_1), I(X_2)$, so $I(X_1 \cup X_2) \subseteq I(X_1) \cap I(X_2)$.

Conversely, if $f \in I(X_1) \cap I(X_2)$, then $f \in I(X_1 \cup X_2)$. □

**Recall** (from GRM)**:** An ideal $P \subseteq R$ is *prime* if $P \neq R$ and whenever $f \cdot g \in P$, either $f \in P$ or $g \in P$.

**Lemma.** Let $P \subseteq A$ be a prime ideal, and let $I_1, \dots, I_n \subseteq A$ be ideals. Suppose $P \supseteq \bigcap_i I_i$. Then $p \supseteq I_i$ for some $i$. In particular, if $p = \bigcap_i I_i$, then $P = I_i$ for some $i$.

**Example.** $A = \mathbb{Z}$, $P = \langle p \rangle$, $p$ a prime number. Let $I_i = \langle n_i \rangle$. Then

$$\bigcap_i I_i = \langle \mathrm{lcm}(n_1, \dots, n_s) \rangle$$

Then $P \supseteq \bigcap_i I_i \iff p \mid \mathrm{lcm}(n_1, \dots, n_s)$, and the condition on the right implies that $p \mid n_i$ for some $i$.

*Proof.* Suppose $P \not\supseteq I_i$ for any $i$. Thus we can find $x_i \in I_i$, $x_i \notin P$. Then

$$\prod_{i=1}^n x_i \in \cap_{i=1}^n I_i \subseteq P,$$

so there exists $i$ with $x_i \in P$, a contradiction.

If $P = \bigcap_i I_i$, $P \subseteq I_i$ for each $i$ and since we know $I_i \subseteq P$ for some $i$, we have $P = I_i$ for that $i$. □

> **Proposition.** Let $\mathbb{K}$ be algebraically closed. Then an algebraic set $X \subseteq \mathbb{A}^n$ is irreducible if and only if $I(X) \subseteq A = \mathbb{K}[X_1, \dots, X_n]$ is prime.

Start of lecture 3

> **Proposition.** Let $\mathbb{K}$ be algebraically closed. Then an algebraic set $X \subseteq \mathbb{A}^n$ is irreducible if and only if $I(X)$ is prime.

*Proof.*

- $\Rightarrow$ If $f \cdot g \in I(X)$, then $X \subseteq Z(f \cdot g) = Z(f) \cup Z(g)$. Thus

$$X = (X \cap Z(f)) \cup (X \cap Z(f))$$

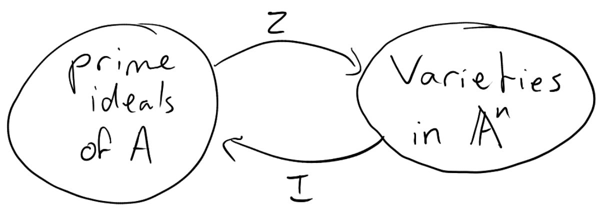
  By irreducibility of $X$ we can assume $X = X \cap Z(f)$, so $X \subseteq Z(f)$, so $f \in I(X)$.

- $\Leftarrow$ If $P \subseteq A = \mathbb{K}[X_1, \dots, X_n]$ is prime, suppose $Z(P) = X_1 \cup X_2$ with $X_1, X_2$ closed. Then

$$I(X_1) \cap I(X_2) = I(X_1 \cup X_2) = I(Z(P)) = \sqrt{P}.$$

  The last equality is by Hilbert's Nullstellensatz. But $\sqrt{P} = P$: if $f^n \in P$ then $f \in P$ by primality of $P$. Thus $I(X_1) \cap I(X_2) = P$, so by the lemma, $P = I(X_1)$ or $P = I(X_2)$. Thus $Z(P) = X_1$ or $Z(P) = X_2$. Thus $Z(P)$ is irreducible and $I(Z(P)) = P$. □

We now have a $1-1$ correspondence (if $\mathbb{K}$ is algebraically closed):



**Proposition.** Any algebraic set in $\mathbb{A}^n$ can be written as a finite union of varieties.

*Proof.* Let $\mathcal{R}$ be the set of all algebraic sets in $\mathbb{A}^n$ which can't be written as a finite union of varieties. If $\mathcal{R} \neq \emptyset$, I claim it has a minimal element. Otherwise there exists $X_1, X_2, X_3, \ldots \in \mathcal{R}$ with

$$X_1 \supsetneq X_2 \supsetneq X_3 \supsetneq \cdots$$

so

$$I(X_1) \subsetneq I(X_2) \subsetneq I(X_3) \subsetneq \cdots \subseteq A = \mathbb{K}[X_1, \ldots, X_n]$$

This contradicts $A$ being Noetherian (GRM).

Let $X \in \mathcal{R}$ be minimal. $X$ can't be irreducible, since then $X$ is itself a variety. Otherwise, we can write $X = X_1 \cup X_2$ with $X_1 \subsetneq X$, $X_2 \subsetneq X$ with $X_1, X_2$ algebraic. Then $X_1, X_2 \notin \mathcal{R}$, hence can be written as a union of irreducible sets. So $X$ can also be written as a finite union of irreducibles, so $X \notin \mathcal{R}$, contradiction. □

**Definition** (Irreducible components)**.** If $X = X_1 \cup \cdots \cup X_n$ with $X$, $X_i$ algebraic, $X_i$ irreducible and $X_i \not\subseteq X_j$ for any $i \neq j$, then we say $X_1, \ldots, X_n$ are the *irreducible components* of $X$.

**Example.**

(1) In $\mathbb{A}^2$, $A = \mathbb{K}[X_1, X_2]$, $X = \mathbb{Z}(X_1 \cdot X_2) = Z(X_1) \cup Z(X_2)$.

(2) More generally, $A = \mathbb{K}[X_1, \ldots, X_n]$ is a UFD. If $0 \neq f \in A$, we can write $f = \prod f_i^{a_i}$ with $f_i$ irreducible. Since $A$ is a UFD, $\langle f_i \rangle$ is prime. Thus $Z(f_i)$ is irreducible (assuming $\mathbb{K}$ is algebraically closed). Thus $Z(f) = Z(f_1) \cup \cdots \cup Z(f_s)$ is the irreducible decomposition of $Z(f)$.

(3) $Z(X_2^2 - X_1^3 + X_1)$ is irreducible.

## 1.3 Regular and rational functions

In Algebraic Geometry, polynomial functions are natural. Let $X \subseteq \mathbb{A}^n$ be an algebraic set. $f \in A = \mathbb{K}[X_1, \ldots, X_n]$. This gives a function $f : \mathbb{A}^n \to \mathbb{K}$, $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n) \in \mathbb{K}$. Then get $f|_X : X \to \mathbb{K}$.

If $f, g \in A$, and $f|_X = g|_X$, then $f \cdot$ vanishes on $X$. So $f \cdot g \in I(X)$.

So it is natural to think of $A/I(X)$ as being the set of polynomial functions on $X$.

**Definition** (Coordinate ring)**.** Let $X \subseteq \mathbb{A}^n$ be an algebraic set. The *coordinate ring* of $X$ is

$$A(X) := A/I(X)$$

(sometimes written $\mathbb{K}[X]$).

**Definition** (Regular function)**.** Let $X \subseteq \mathbb{A}^n$ be an algebraic set, $U \subseteq X$ an open subset. A function $f : U \to \mathbb{K}$ is *regular* if $\forall p \in U$, there exists an open neighbourhood $V \subseteq U$ of $p$ and functions $g, h \in A(X)$ with $h(q) \neq 0$ for any $q \in V$ and $f = \frac{g}{h}$ on $V$.

**Example.** Any $f \in A(X)$ defines a regular on $X$.

**Notation.** We write

$$\mathcal{O}_X(U) := \{f : U \to \mathbb{K} \mid f \text{ is regular}\}.$$

**Note.** $\mathcal{O}_X(U)$ is a ring if $f, g \in \mathcal{O}_X(U)$, then $f \pm g, f \cdot g \in \mathcal{O}_X(U)$. This is also a $\mathbb{K}$-algebra.

**Definition** (Algebra)**.** If $A$, $B$ are rings, then an $A$-algebra structure on $B$ is the data of a ring homomorphism $\varphi : A \to B$. This turns $B$ into an $A$-module via

$$a \cdot b := \varphi(a) \cdot b$$

So $\mathbb{K} \to \mathcal{O}_X(U)$ is given by $a \in \mathbb{K}$ being mapped to the constant function with value $a$.

Start of lecture 4

Reminders:

- $X \subseteq \mathbb{A}^n$.
- $A(X) = A/I(X)$.

- We defined the notion of regular function on an open subset $U \subseteq X$.
- $\mathcal{O}_X(U) := \{f : U \to \mathbb{K} \mid f \text{ is regular on } U\}$

**Lemma.** $\mathcal{O}_X(X) = A(X)$.

*Proof.* Later (we will prove this after proving Hilbert's Nullstellensatz). □

Recall from GRM: Let $A$ be an integral domain. Then the *field of fractions* of $A$ (or *fraction field* of $A$) is

$$\left\{\frac{f}{g} \mid f, g \in A, g \neq 0\right\} / \sim$$

with $\frac{f}{g} \sim \frac{f'}{g'}$ if $fg' = f'g$.

We define addition and multiplication using:

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + gf'}{gg'} \qquad \frac{f}{g}\frac{f'}{g'} = \frac{ff'}{gg'}$$

and we observe that this is a field since

$$\left(\frac{f}{g}\right)^{-1} = \frac{g}{f}$$

is an inverse whenever $f \neq 0$.

**Remark.** If $X \subseteq \mathbb{A}^n$ is an affine variety, then $A(X) = A/I(X)$ is an integral domain. (This is because for any ring $R$ and ideal $P \subseteq R$, $R/P$ is an integral domain if and only if $P$ is prime – see GRM).

**Definition** (Function field)**.** If $X \subseteq \mathbb{A}^n$ is a variety, its *function field* is $K(X)$, the fraction field of $A(X)$. Elements of $K(X)$ are called *rational functions* on $X$. Note $\frac{g}{h} \in K(X)$ induces a regular function on $X \setminus Z(h)$.

## 1.4 Morphisms

**Definition** (Morphism)**.** A map $f : X \to Y$ between affine varieties is called a *morphism* if:

(1) $f$ is continuous in the induced Zariski topology on $X$ and $Y$ ($Z \subseteq X \subseteq \mathbb{A}^n$ is closed in $X$ if and only if it is closed in $\mathbb{A}^n$).

(2) $\forall V \subseteq Y$ be an open subset, $\varphi : V \to \mathbb{K}$ a regular function, we have that $\varphi \circ f : f^{-1}(V) \to \mathbb{K}$ is a regular function on $f^{-1}(V)$.

**Observation:** Let $f : X \to Y$ be a morphism. Then for any $\varphi \in A(Y)$, we get $\varphi \circ f : X \to \mathbb{K}$ a regular function. Assuming $\mathbb{K}$ is algebraically closed, $\mathcal{O}_X(X) = A(X)$, so $\varphi \circ f \in A(X)$. This gives a map $f^\# : A(Y) \to A(X)$. This is a $\mathbb{K}$-algebra homomorphism. We first check that it is indeed a ring homomorphism:

$$\begin{aligned} f^\#(\varphi_1 + \varphi_2) &= (\varphi_1 + \varphi_2) \circ f \\ &= \varphi_1 \circ f + \varphi_2 \circ f \\ &= f^\#(\varphi_1) + f^\#(\varphi_2) \\ f^\#(\varphi_1 \cdot \varphi_2) &= (\varphi \cdot \varphi_2) \circ f \\ &= (\varphi_1 \circ f) \cdot (\varphi_2 \circ f) \\ &= f^\#(\varphi_1) \cdot f^\#(\varphi_2) \\ f^\#(1) &= 1 \end{aligned}$$

Now we check multiplication by elements of $\mathbb{K}$. For $a \in \mathbb{K}$,

$$f^\#(a \cdot \varphi) = a \cdot f^\#(\varphi)$$

So this is a $\mathbb{K}$-algebra homomorphism.

**Theorem.** For $\mathbb{K}$ algebraically closed, there is a $1-1$ correspondence between morphisms $f : X \to Y$ and $\mathbb{K}$-algebra homomorphisms $f^\# : A(Y) \to A(X)$.

*Proof.* We have already constructed $f^\#$ from $f$. Suppose $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$. Then

$$A(X) = \frac{\mathbb{K}[X_1, \ldots, X_n]}{I(X)} \qquad A(Y) = \frac{\mathbb{K}[Y_1, \ldots, Y_m]}{I(Y)}$$

$$\mathbb{A}^n \supseteq X \underset{f}{\xrightarrow{(f_1, \ldots, f_m)}} Y \subseteq \mathbb{A}^m \underset{y_i}{\to} \mathbb{K}$$

$f_i = y_i \circ f$. Suppose given $f^\# : A(Y) \to A(X)$. Set $f_i = f^\#(\overline{y}_i)$ ($\overline{y}_i$ is the image of $y_i$ in $A(Y)$). We now define $f : X \to \mathbb{A}^m$ by $f(p) = (f_1(p), \ldots, f_m(p))$.

**Claim:** $f(X) \subseteq Y$.

Proof: Let $g \in I(Y)$, and $p \in X$. We need to show that $g(f(p)) = 0$. This will show $f(p) \in Y$. Consider the map

$$\mathbb{K}[Y_1, \ldots, Y_m] \to A(Y) \xrightarrow{f^\#} A(X)$$

$$Y_i \mapsto \overline{Y_i} \mapsto f_i$$

Thus

$$g(Y_1, \ldots, Y_m) \mapsto g(\overline{Y}_1, \ldots, \overline{Y}_m) \mapsto g(f_1, \ldots, f_m)$$

The right arrow uses $f^\#$ being a $\mathbb{K}$-algebra. The middle expression is the image of $g$ under quotient map, hence 0 since $g \in I(Y)$. Thus $g(f(p)) = g(f_1, \ldots, f_m)(p) = 0$.

Thus $f(X) \subseteq Y$. This completes the proof of the claim.

Note: If $\varphi \in A(Y)$, can write $\varphi = g(\overline{Y}_1, \ldots, \overline{Y}_m)$ and $f^\#(\varphi) = g(f_1, \ldots, f_m) = \varphi \circ f$.

**Claim:** $f$ is a morphism:

(1) *$f$ is continuous:* We will show $f^{-1}(Z)$ is closed for $Z \subseteq Y$ closed. Note $I(Z) \supseteq I(Y)$, so $\overline{I(Z)} = \frac{I(Z)}{I(Y)} \subseteq A(Y)$ is an ideal in $A(Y)$. Then define

$$Z(f^\#(\overline{I(Z)})) = \{p \in X \mid \varphi(p) = 0 \ \forall \varphi \in f^\#(\overline{I(Z)})\}$$

This is a closed subset of $X$ since it coincides with

$$Z(\pi_X^{-1}(f^\#(\overline{I(Z)})))$$

where $\pi_X : \mathbb{K}[X_1, \ldots, X_n] \to A(X)$. But

$$\begin{aligned} Z(f^\#(\overline{I(Z)})) &= \{p \in X \mid \psi \circ f = 0 \ \forall \psi \in \overline{I(Z)}\} \\ &= \{p \in X \mid f(p) \in Z\} \\ &= f^{-1}(Z) \end{aligned}$$

Thus $f^{-1}(Z)$ is closed.

(2) Let $U \subseteq Y$ be an open subset, $\varphi \in \mathcal{O}_Y(U)$. We need to show $\varphi \circ f : f^{-1}(U) \to \mathbb{K}$ is regular. Let $p \in f^{-1}(U)$, and let $V \subseteq U$ be an open neighbourhood of $f(p)$ for which we can write $f = \frac{g}{h}$, $g, h \in A(Y)$, $h$ nowhere vanishing on $V$. Then

$$\varphi \circ f|_{f^{-1}(V)} = \frac{g \circ f}{h \circ f} = \frac{f^\#(g)}{f^\#(h)}.$$

Now $f^\#(g), f^\#(h)$ lie in $A(X)$, and $f^\#(h) = h \circ f$ doesn't vanish on $f^{-1}(V)$. Thus $\varphi \circ f$ is regular. $\square$

Start of lecture 5

**Exercise:** Check that this gives a $1-1$ correspondence. We checked

$$f^\# \mapsto f \mapsto f^\#,$$

so it remains to check that

$$f \mapsto f^\# \mapsto f.$$

**Moral.** A morphism $f : \mathbb{A}^n \supseteq X \to Y \subseteq \mathbb{A}^m$ is given by choosing polynomial functions $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]$ and defining $f$ by

$$f(p) = (f_1(p), \dots, f_m(p)).$$

**Example.**

$$\begin{aligned} f : \mathbb{A}^1 &\to \mathbb{A}^2 \\ t &\mapsto (t, t^2) \end{aligned}$$

The image of this map is $Y = Z(X^2 - Y)$. This defines a morphism $f : \mathbb{A}^1 \to Y$. Then

$$\begin{aligned} f^\# : \frac{\mathbb{K}[X, Y]}{(Y - X^2)} &\to \mathbb{K}[t] \\ X &\mapsto t \\ Y &\mapsto t^2 \end{aligned}$$

This is an isomorphism!

**Definition** (Isomorphism of affine varieties)**.** Two affine varieties are *isomorphic* if there exist morphisms $f : X \to Y$, $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$, $f \circ g = \mathrm{id}_Y$.

**Theorem.** If $X, Y$ are affine varieties, then $X$ is isomorphic to $Y$ if and only if $A(X) \cong A(Y)$ as $\mathbb{K}$-algebra.

**Example.** $\mathbb{A}^1 \cong Z(X^2 - Y) \subseteq \mathbb{A}^2$.

**Remark.** A $\mathbb{K}$-algebra $\mathbb{A}$ is *finitely generated* if there exists a surjective $\mathbb{K}$-algebra homomorphism

$$\begin{aligned} \mathbb{K}[X_1, \ldots, X_n] &\to \mathbb{A} \\ X_i &\mapsto a_i \end{aligned}$$

i.e. every element of $A$ can be written as a polynomial in $a_1, \ldots, a_n$ with coefficients in $\mathbb{K}$. If $I$ is the kernel of this map then

$$A \cong \mathbb{K}[X_1, \ldots, X_n]/I.$$

SUppose further that $A$ is an integral domain. Then $I$ is a prime ideal of $\mathbb{K}[X_1, \ldots, X_n]$, so

$$A = A(X)$$

where $X = Z(I)$.

## 2 The proof of Hilbert's Nullstellensatz

**Goal:** We want to prove Hilbert's Nullstellensatz. That is, if $\mathbb{K}$ is algebraically closed, we want to show $I(Z(I)) = \sqrt{I}$.

**Definition** (Transcendental)**.** Let $F/\mathbb{K}$ be a field extension. We say an element $z \in F$ is *transcendental* over $\mathbb{K}$ if it is not algebraic, i.e. $\nexists f \in \mathbb{K}[X]$ with $f \neq 0$, $f(z) = 0$.

**Definition** (Algebraically independent elements)**.** We say $z_1, \dots, z_d \in F$ are *algebraically independent over* $\mathbb{K}$ if $\nexists f \in \mathbb{K}[X_1, \dots, X_d]$ with $f \neq 0$, $f(z_1, \dots, z_d) = 0$.

**Definition** (Transcendence basis)**.** A *transcendence basis* for $F/\mathbb{K}$ is a set $z_1, \dots, z_d \in F$ algebraically independent over $\mathbb{K}$ and such that $F$ is algebraic over $\mathbb{K}(z_1, \dots, z_d)$.

**Example.** If $X$ is a variety, $K(X)$ is a field extension of $\mathbb{K}$, and it usually has lots of transcendentals.

$$\begin{aligned} K(\mathbb{A}^n) &= \left\{ \frac{f}{g} \mid f, g \in \mathbb{K}[X_1, \dots, X_n], g \neq 0 \right\} / \sim \\ &= \mathbb{K}(X_1, \dots, X_n) \\ &= \text{field of rational functions in } X_1, \dots, X_n \end{aligned}$$

$X_1, \dots, X_n$ form a transcendence basis.

**Definition** (Finitely generated field extension)**.** If $F/\mathbb{K}$ is a field extension, we say $F$ is *finitely generated* over $\mathbb{K}$ if $F = \mathbb{K}(z_1, \dots, z_n)$ for some $z_1, \dots, z_n \in F$.

**Example.** $K(X)/\mathbb{K}$ is finitely generated. If $X \subseteq \mathbb{A}^n$, then $K(X)$ is the fraction field of $A(X) = \mathbb{K}[X_1, \dots, X_n]/I$ and hence $K(X)$ is generated by the images of $X_1, \dots, X_n$.

**Proposition.** Every finitely generated field extension $F/\mathbb{K}$ has a transcendence basis, and any two transcendence bases have the same number of elements.

Further, if $F = \mathbb{K}(z_1, \ldots, z_N)$, then there is a transcendence basis $\{Y_1, \ldots, Y_n\} \subseteq \{z_1, \ldots, z_N\}$.

*Proof.* Write $F = \mathbb{K}(z_1, \ldots, z_N)$. If $z_1, \ldots, z_n$ are algebraically independent, then $z_1, \ldots, z_n$ is a transcendence basis. If $z_1, \ldots, z_N$ are algebraic over $\mathbb{K}$, then the transcendence basis can be taken to be empty. Otherwise, assume $\{z_1, \ldots, z_d\}$ is a maximal subset of algebraically independent elements of $\{z_1, \ldots, z_n\}$. I claim $z_1, \ldots, z_d$ is a transcendence basis, i.e. $F$ is algebraic over $\mathbb{K}(z_1, \ldots, z_d)$. It is neough to show $z_j$ is algebraic of $\mathbb{K}(z_1, \ldots, z_d)$ for any $j > d$.

By assumption, $z_1, \ldots, z_d, z_j$ are *not* algebraically independent, i.e. there exists $f_j \in \mathbb{K}[X_1, \ldots, X_d, X_j]$ such that $f_j(z_1, \ldots, z_d, z_j) = 0$.

Write $f_j = \sum_I f_{ji}(X_1, \ldots, X_d) X_j^i$. Then

$$0 \neq f_j(z_1, \ldots, z_d, X) = \sum_i f_{ji}(z_1, \ldots, z_d) X^i \in \mathbb{K}(z_1, \ldots, z_d)[X]$$

(the polynomial is non-zero since $z_1, \ldots, z_d$ are algebraically independent). Then since $f_j(z_1, \ldots, z_d, z_j) = 0$, we have $z_j$ algebraic over $\mathbb{K}(z_1, \ldots, z_d)$. Thus $f$ is algebraic over $\mathbb{K}(z_1, \ldots, z_d)$, so $z_1, \ldots, z_d$ is a transcendence basis. Now suppose $z_1, \ldots, z_d$ and $w_1, \ldots, w_e$ are both transcendence bases. Suppose $d \le e$. First $w_1$ is algebraic over $\mathbb{K}(z_1, \ldots, z_d)$ since $w_1 \in F$. Then there exists a polynomial $f \in \mathbb{K}[X_1, \ldots, X_d, D_{d+i}]$ such that $f(z_1, \ldots, z_d, w_1) = 0$. This is obtained by clearing denominators of a polynomial $g \in \mathbb{K}(z_1, \ldots, z_d)[X_{d+1}]$ with $g(w_1) = 0$. Since $w_1$ is not algebraic over $\mathbb{K}$, $f$ must involve at least one of $X_1, \ldots, X_d$, say $X_1$. Thus $z_1$ is algebraic. So $z_1$ is algebraic over $\mathbb{K}(w_1, z_2, \ldots, z_d)$ (as witnessed by $f$). So $F$ is algebraic over $\mathbb{K}(w_1, z_2, \ldots, z_d)$. Repeat: $w_2$ is algebraic over $\mathbb{K}(w_1, \ldots, z_2, \ldots, z_d)$ and not algebraic over $\mathbb{K}(w_1)$. So one can find $0 neq g \in \mathbb{K}[X_1, \ldots, X_{d+1}]$ such that $g(w_1, z_2, \ldots, z_d, w_2) = 0$ and further $g$ involves one of $X_2, \ldots, X_d$: say it involves $X_2$. Thus $z_2$ is algebraic over $\mathbb{K}(w_1, w_2, z_3, \ldots, z_d)$. Continuing, eventually we find $F$ is algebraic over $\mathbb{K}(w_1, \ldots, w_d)$. But if $e > d$, then $w_e$ is algebraic over $\mathbb{K}(w_1, \ldots, w_d)$, contradicting $w_1, \ldots, w_e$ being a transcendence basis. □

Start of

lecture 6

**Lemma.** Let $M$ be a finitely generated $A$ module for $A$ a commutative ring $I \subseteq A$, $\phi : M \to M$ an $A$-module homomorphism such that

$$\phi(M) \subseteq I \cdot M = \langle a \cdot m \mid a \in I, \in M \rangle,$$

where $\langle \cdots \rangle$ represents the submodule of $M$ generated by those elements. Then there exists an equation

$$\phi^n + a_i \phi^{n-1} + \cdots + a_n \equiv 0$$

with $a_i \in I$. Interpretation: $a_i$ represents the homomorphism $m \mapsto a_i m$.

*Proof.* Let $x_1, \ldots, x_n \in M$ be a set of generators for $M$. Then each $\phi(x_i) \in I \cdot M$, so can write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} \cdot x_j$$

with $a_{ij} \in I$, i.e.

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij}) x_j = 0$$

So

$$\begin{pmatrix} \phi - a_{11} & -a_{12} & \cdots \\ -a_{21} & \phi - a_{22} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Multiplying by the adjoing matrix, we get

$$\det((\delta_{ij}\phi - a_{ij}))x_j = 0 \qquad \forall j$$

But $\det(\delta_{ij}\phi - a_{ij})$ is a degree $n$ polynomial in $\phi$ annihiliting each $x_j$, hence annihilating every element in $M$. The leading term in $\phi$ is $\phi^n$ and all other coefficients involve $a_{ij}$'s, hence lie in $I$. □

### Integrality

**Definition** (Integral element)**.** Let $A \subseteq B$ be integral domains. An element $b \in B$ is *integral* over $A$ if $f(b) = 0$ for a *monic* polynomial $f(X) \in A[X]$. (recall that monic means that the leading coefficient is 1).

**Proposition.** $b \in B$ integral over $A$ if and only if there is a subring $C \subseteq B$ containing $A[b]$ with $C$ a finitely generated $A$-module.

*Proof.*

$\Rightarrow$ Suppose $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. Then since $A[b]$ is generated as an $A$-module by $1, b, b^2, b^2, \ldots$. It is also generated by $1, \ldots, b^{n-1}$. So $A[b]$ is ginitely generated, and can take $C = A[b]$.

$\Leftarrow$ If $C$ is finitely generated, let $\phi : C \to C$ be given by $\phi(x) = b \cdot x$. Apply the above Lemma to the finitely generated $A$-module $C$ with $I = A$. We get $\phi^n + a_1 \phi^{n-1} \cdots + a_n \equiv 0$ or $b^n + a_1 b^{n-1} + \cdots + a_n$, acting by multiplication on $C$, is the zero map. Since $C$ is an integral domain, we have

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0$$

□

Start of lecture 7

**Lemma 1.** Let $A \le B$ be an inclusion of integral domains, and assume the fraction field $K$ of $A$ is contained in $B$. If $b \in B$ is algebraic over $K$, then there exists $p \in A$ non-zero such that $pb$ is integral over $A$.

*Proof.* Suppose $g \in K[X]$ with $g(b) = 0$, $g \neq 0$. By clearing denominators, we can assume $g \in A[X]$. Write

$$g(X) = a_N X^n + \cdots + a_0, \qquad a_n \neq 0, a_i \in A.$$

Note

$$a_N^{N-1} g = (a_N X)^n + a_{N-1}(A_N X)^{N-1} + a_{N-2} a_N \cdot (a_N X)^{N-2} + \cdots + a_0 a_N^{N-1}.$$

This is a monic polynomial in $a_N X$. Thus taking $X = b$, we thus have a monic polynomial killing $a_N b$. So $a_N b$ is integral over $A$ and we take $p = a_N$. □

**Lemma 2.** Let $A$ be a UFD with fraction field $K$. Then if $\alpha \in K$ is integral over $A$, we have $\alpha \in A$.

*Proof.* If $\alpha \in K$ is integral over $A$, write $\alpha = \frac{a}{b}$, with $a, b$ having no commmon factor. We have $g\left(\frac{a}{b}\right) = 0$ for some monic polynomial $g$, say

$$g(X) = X^n + a_1 X^{n-1} + \cdots + a_n.$$

We have

$$\frac{a^n}{b^n} + a_1 \frac{a^{n-1}}{b^{n-1}} + \cdots + a_n = 0$$

in $K$. So

$$a^n + a_1 b a^{n-1} + \cdots + a_n b^n = 0$$

in $A$. So $b \mid a$, so $b$ must be a unit in $A$. Thus $\frac{a}{b} \in A$. □

**Lemma 3.** Let $A \leq B$ be integral domains, and $S \subseteq B$ the set of all elements in $B$ integral over $A$. Then $S$ is a subring of $B$.

*Proof.* If $b_1, b_2 \in S$, then $A[b_1]$ is a finitely generated $A$-module. Also, $b_2$ is integral over $A$, and hence is integral over $A[b_1]$. Thus $A[b_1][b_2] = A[b_1, b_2]$ is a finitely generated $A[b_1]$-module. Thus $A[b_1, b_2]$ -s a finitely generated $A$-module. Since $A[b_1 \pm b_2], A[b_1 \cdot b_2] \subseteq A[b_1, b_2]$, we have $b_1 \pm b_2, b_1 \cdot b_2 \in S$ by the proposition.

We also have $0, 1 \in S$ since $A \subset S$. □

**Lemma 4** (Hilbert's Nullstellensatz, Version 0)**.** Let $\mathbb{K}$ be an algebraically closed field, and $F/\mathbb{K}$ a field extension which is finitely generated as a $\mathbb{K}$-algebra (i.e. $\exists$ a surjective $\mathbb{K}$-algebra homomorphism $\mathbb{K}[X_1, \ldots, X_d] \to F$). Then $F = \mathbb{K}$.

*Proof.* Suppose $\alpha \in F$ is algebraic over $\mathbb{K}$, say with irreducible polynomial $f(X) \in \mathbb{K}[X]$. Then $f$ is linear since $\mathbb{K}$ is algebraically closed, hence of the form $c(X - \alpha)$. So $\alpha \in \mathbb{K}$.

Suppose we are given a surjective map

$$\begin{aligned} \mathbb{K}[X_1, \ldots, X_d] &\to F \\ x_i &\mapsto z_i \in F \end{aligned}$$

Then $z_1, \ldots, z_d$ generate $F$ as a field extension of $\mathbb{K}$. Assume $z_1, \ldots, z_e$ form a transcendence basis for $F/\mathbb{K}$. Note that if $F \neq \mathbb{K}$, we must have $e \geq 1$. Let $R = \mathbb{K}[z_1, \ldots, z_e] \leq F$ (note that this really is a polynomial ring since $z_1, \ldots, z_e$ are algebraically independent). Then $w_1 = z_{e+1}, \ldots, w_{d-e} = z_d$ are algebraic over $L = \mathbb{K}(z_1, \ldots, z_e)$. Let $S \leq F$ be the set of elements of $F$ integral over $R$. $S$ is a subring of $F$ by Lemma 3. By Lemma 1, there exists $p_1, \ldots, d_{d-e} \in R$ with $t_i := p_i w_i$ integral over $R$. In particular, $t_1 \in S$. Choose $\frac{f}{g} \in \mathbb{K}(z_1, \ldots, z_e) = L$, $f, g \in R$, with $f, g$ relatively prime. Then $g$ is relatively prime to $p_1, \ldots, p_{d-e}$. Here, we assume $e \geq 1$. Thus

$$p_1^{n_1} \cdots p_{d-e}^{n_{d-e}} \frac{f}{g} \notin \mathbb{K}[z_1, \ldots, z_e]$$

for any $n_1, \ldots, n_{e-d} \geq 0$. Since $z_1, \ldots, z_d$ generate $F$ as a $\mathbb{K}$-algebra there exists $q \in \mathbb{K}[X_1, \ldots, X_d]$ such that

$$\frac{f}{g} = q(z_1, \ldots, z_d) = q\left(z_1, \ldots, z_e, \underbrace{\frac{t_1}{p_1}}_{z_{e+1}}, \ldots, \underbrace{\frac{t_{d-e}}{p_{d-e}}}_{z_d}\right) \tag{$*$}$$

Let $n_j$ be the highest power of $X_{e+j}$ appearing in $q$. Multiplying by $\prod_j p_j^{n_j}$ clears denominators on RHS of $(*)$. So we have

$$p_1^{n_1} \cdots p_{d-e}^{n_{d-e}} \frac{f}{g} = q'(z_1, \ldots, z_e, t_1, \ldots, t_{d-e}) \tag{$**$}$$

The RHS of $(**)$ lies in $S$ as $z_1, \ldots, z_e \in S$, $t_1, \ldots, t_{d-e} \in S$. Thus LHS lies in $S$. But LHS lies in $\mathbb{K}(z_1, \ldots, z_e)$ and hence by Lemma 2, lies in $\mathbb{K}[z_1, \ldots, z_e]$, a contradiction. Thus $e = 0$, and $F$ is algebraic over $\mathbb{K}$, so $F = \mathbb{K}$ since $\mathbb{K}$ is algebraically closed. □

Start of lecture 8

**Theorem** (Nullstellensatz I)**.** Let $\mathbb{K}$ be algebraically closed. Then any maximal ideal $M \subset \mathbb{K}[X_1, \ldots, X_n]$ is of the form

$$M = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$$

for some $a_1, \ldots, a_n \in \mathbb{K}$.

*Proof.* Note we have an isomorphism

$$\begin{aligned} \frac{\mathbb{K}[X_1, \ldots, X_n]}{\langle X_1 - a_1, \ldots, X_n - a_n \rangle} &\xrightarrow{\cong} \mathbb{K} \\ X_i &\longmapsto a_i \end{aligned}$$

Recall $M \subseteq A$ is a maximal ideal if and only if $A/M$ is a field. Thus $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ is a maximal ideal.

Conversely, let $M \subseteq \mathbb{K}[X_1, \ldots, X_n]$ be a maximal ideal. Then

$$\frac{\mathbb{K}[X_1, \ldots, X_n]}{M} \cong F$$

for some field $F$ which is finitely generated as a $\mathbb{K}$-algebra by $X_1, \ldots, X_n$. Thus $F = \mathbb{K}$ by Lemma 4. We thus have an isomorphism

$$\varphi : \frac{\mathbb{K}[X_1, \ldots, X_n]}{M} \xrightarrow{\cong} \mathbb{K}.$$

Let $a_i = \varphi(X_i)$. Then

$$\varphi(X_i - a_i) = \varphi(X_i) - a_i = a_i - a_i = 0.$$

Thus $X_i - a_i \in M$ for each $i$. So

$$\langle X_1 - a_1, \dots, X_n - a_n \rangle \subseteq M.$$

But we have already seen that $\langle X_1 - a_1, \dots, X_n - a_n \rangle$ is maximal, so we must in fact have equality. $\square$

**Example.** $\langle X^2 + 1 \rangle \leq \mathbb{R}[X]$ is a maximal ideal, but $\langle X^2 + 1 \rangle \neq \langle X - a \rangle$ for any $a \in \mathbb{R}$.

**Theorem** (Nullstellensatz II)**.** Let $\mathbb{K}$ be algebraically closed, and $I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{K}[X_1, \dots, X_n]$. Then either:

(1) $I = \mathbb{K}[X_1, \dots, X_n]$, or

(2) $Z(I) \neq \emptyset$.

*Proof.* Suppose $1 \notin I$, i.e. not in case (1). Then there exists a maximal ideal $M \subseteq \mathbb{K}[X_1, \dots, X_n]$ with $I \subseteq M$. Thus $Z(M) \subseteq Z(I)$. Then by Nullstellensatz I, $M = \langle X_1 - a_1, \dots, X_n - a_n \rangle$, and hence $Z(M) = \{(a_1, \dots, a_n)\}$. So $Z(M) \neq \emptyset$, so $Z(I) \neq \emptyset$. $\square$

**Theorem** (Nullstellensatz III)**.** Let $\mathbb{K}$ be algebraically closed, $I \subseteq \mathbb{K}[X_1, \dots, X_n]$ an ideal. Then

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

*Proof.* $\sqrt{I} \subseteq I(Z(I))$ in any event.

Let $g \in \mathbb{K}[X_1, \dots, X_n]$. Define

$$V_g = Z(Zg(X_1, \dots, X_n) - 1) \subseteq \mathbb{A}^{n+1}$$

with coordinates $X_1, \dots, X_n, Z$. Projecting $V_g$ via $(X_1, \dots, X_n, Z) \mapsto (X_1, \dots, X_n)$ gives the set

$$D(g) := \mathbb{A}^n \setminus Z(g).$$

Now suppose $g \in I(Z(I))$. Then $D(g) \cap Z(I) = \emptyset$. If $I = \langle f_1, \dots, f_r \rangle$, consider $J = \langle f_1, \dots, f_r, Zg - 1 \rangle \subseteq \mathbb{K}[X_1, \dots, X_n, Z]$. Then $Z(J) = \emptyset$, so $J = \mathbb{K}[X_1, \dots, X_n, Z]$ by Nullstellensatz II.

Thus we can write

$$1 = \sum_i h_i(X_1, \dots, X_n, Z) f_i(X_1, \dots, X_n) + h(X_1, \dots, X_n, Z)(g(X_1, \dots, X_n)Z - 1)$$

with $h_i, h \in \mathbb{K}[X_1, \dots, X_n, Z]$. Substitute $Z = \frac{1}{g}$. We get

$$1 = \sum_i h_i \left( X_1, \dots, X_n, \frac{1}{g} \right) f_i(X_1, \dots, X_n).$$

Multiplying by a high power of $g$ clears denominators, giving:

$$g^N = h_i'(X_1, \dots, X_n) f_i \in I,$$

for some $h_i'$. Thus $g^n \in I$, so $g = \sqrt{I}$. □

Recall we need the proof of:

**Proposition.** If $X \subseteq \mathbb{A}^n$ is an affine variety, then $\mathcal{O}_X(X) = A(X)$.

**Lemma.** Let $f, g : X \to \mathbb{K}$ be regular functions on $X$ an affine variety, and suppose there exists open $U \subseteq X$ non-empty with $f|_U = g|_U$. Then $f = g$.

*Proof.* Consider the map $\varphi = (f, g) : X \to \mathbb{A}^2$. This is a morphism (exercise: check this!). Let $\Delta = \{(a, a) \in \mathbb{A}^2 \mid a \in \mathbb{K}\}$, $\Delta = Z(X - Y)$. Since $\varphi$ is continuous, $\varphi^{-1}(\Delta)$ is closed. But $U \subseteq \varphi^{-1}(\Delta)$, and $U$ is a dense subset of $X$ (otherwise $X = \overline{U} \cup X \setminus U$ is a union of two proper closed subsets, violating irreducibility of $X$). Thus $U \subseteq \overline{U} = X \subseteq \varphi^{-1}(\Delta)$, so $\varphi^{-1}(\Delta) = X$. □

*Proof of Proposition.* We know $A(X) \subseteq \mathcal{O}_X(X)$. So let $f : X \to \mathbb{K}$ be a regular function. So there exists an open cover $\{U_i\}$ of $X$ with $f$ is given on $U_i$ by $f|_{U_i} = \frac{g_i}{h_i}$, with $g_i, h_i \in A(X)$ and $h_i$ nowhere vanishing on $U_i$. Then

$$Z(\{h_i\}) = \bigcap_i Z(h_i) \leq \bigcap_i X \setminus U_i = X \setminus \bigcup_i U_i = \emptyset.$$

Thus $Z(\{h_i\}) = \emptyset$. Thus we can find $e_i \in A(X)$ (Remark: Pull back to $\mathbb{K}[X_1, \dots, X_n]$ and Nullstellensatz II to see this) such that $1 = \sum_i e_i h_i$. Note on $U_i \cap U_j$, $\frac{g_i}{h_i} = \frac{g_j}{h_j}$, so $g_i h_j = g_j h_i$ on $U_i \cap U_j$, so by the Lemma, $g_i h_j = g_j h_i$ on $X$. Thus $\frac{g_i}{h_i} = \frac{g_j}{h_j}$ in $K(X)$. Thus we have the equality in $K(X)$

$$f = \sum_i (e_i h_i) \left( \frac{g_i}{h_i} \right) = \sum_i g_i \in A(X)$$ □

Start of

lecture 9

**Remark.** In proof of previous propositions, we had a statement $Z(\{h_i\}) = \emptyset$, and hence by Nullstellensatz II, $1 \in \langle \{h_i\} \rangle$, and hence we can write $1 = \sum_{i \in I} e_i h_i$ for $I$ a finite index set.

## 3 Projective Varieties

**Definition** ($\mathbb{P}^n$)**.** Let $\mathbb{K}$ be a field. We define

$$\mathbb{P}^n = (\mathbb{K}^{n+1} \setminus \{(0, \dots, 0)\}) / \sim$$

where $(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n)$ for any $\lambda \in \mathbb{K}^\times := \mathbb{K} \setminus \{0\}$.

Alternatively, this is the set of one-dimensional sub-vector spaces of $\mathbb{K}^{n+1}$.

**Remark.** If $\mathbb{K} = \mathbb{R}$, then $\mathbb{P}^n = S^n / \sim$, with $x_n \sim -x$ ($S^n \subseteq \mathbb{R}^{n+1}$ is the unit sphere).

For arbitrary $\mathbb{K}$: Consider $\mathbb{P}^1$. For $(x_0 : x_1) \in \mathbb{P}^1$, if $x_1 \neq 0$, then

$$(x_0 : x_1) \sim \left(\frac{x_0}{x_1} : 1\right) \in \mathbb{A}^1$$

(since there is a unique representative with seconc coordinate 1). The missing points are of the form $(x_0 : 0) \sim (1 : 0)$. Thus we view $\mathbb{P}^1$ as

$$\mathbb{P}^1 = \mathbb{A}^1 \cup \{\underbrace{(1:0)}_{=\infty}\}.$$

This is the Riemann sphere if $\mathbb{K} = \mathbb{C}$.

Now $\mathbb{P}^2$: for $(x_0 : x_1 : x_2) \in \mathbb{P}^2$, if $x_2 \neq 0$, then

$$(x_0 : x_1 : x_2) \sim \left(\frac{x_0}{x_2} : \frac{x_1}{x_2} : 1\right) \in \mathbb{A}^2.$$

If $x_2 = 0$, we get a point $(x_0 : x_1 : 0) \in \mathbb{P}^1$. Thus

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$$

where $\mathbb{P}^1$ can be viewed as the 'line at infinity'.

Algebraic subsets of $\mathbb{P}^n$? When does $f(x_0, \dots, x_n) = 0$ make sense?

**Definition** (Homogeneous)**.** $f \in S = \mathbb{K}[x_0, \dots, x_n]$ is *homogeneous* if every term of $f$ is of the same degree, or equivalently,

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$$

for some $d \geq 0$, where $d$ is the *degree* of $d$.

**Example.** $x_0^3 + x_1x_2^2$ is homogeneous of degree 3. $x_0^3 + x_1^2$ is not homogeneous.

**Definition** (Zero set of $f$ in $\mathbb{P}^n$)**.** If $T \subseteq S$ is a set of homogeneous polynomials, define

$$Z(T) := \{(a_0, \dots, a_n) \in \mathbb{P}^n \mid f(a_0, \dots, a_n) = 0 \ \forall f \in T\}.$$

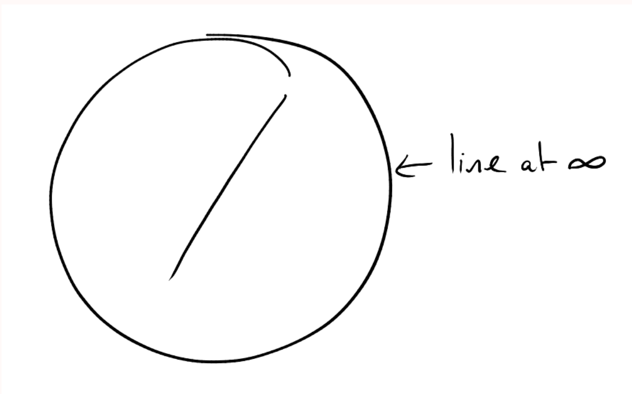
**Definition** (Homogeneous ideal)**.** An ideal $I \subseteq S$ is homogeneous if $I$ is generated by homogeneous polynomials.

**Definition** (Zero set of ideal)**.** For $I$ a homogeneous ideal, we define

$$Z(I) = \{(a_0, \dots, a_n) \in \mathbb{P}^n \mid f(a_0, \dots, a_n) = 0 \ \forall f \in I \text{ homogeneous}\}.$$

**Definition** (Algebraic subset of $\mathbb{P}^n$)**.** A subset of $\mathbb{P}^n$ is *algebraic* if it is of the form $Z(T)$ for some $T$.

**Example.** $Z(a_0x_0 + a_1x_1 + a_2x_2) \subseteq \mathbb{P}^2$, $a_0, a_1, a_2 \in \mathbb{K}$. In the $\mathbb{A}^2 \subseteq \mathbb{P}^2$ where $x_2 = 1$, we get the equation $a_0x_0 + a_1x_1 + a_2 = 0$. If $x_2 = 0$, we get the equation $a_0x_0 + a_1x_1 = 0$, which has the solution $(a_1 : -a_0) \in \mathbb{P}^1$ (assuming not both $a_0 = 0$, $a_1 = 0$, since otherwise just have $x_2 = 0$, the line at $\infty$)




**Exercise:** Check the algebraic sets in $\mathbb{P}^n$ form the closed sets of a topology on $\mathbb{P}^n$. This is the *Zariski topology* on $\mathbb{P}^n$.

**Definition** (Projective variety)**.** A *projective variety* is an irreducible closed subset of $\mathbb{P}^n$.

### The standard open affine cover of $\mathbb{P}^n$

Define $U_i \subseteq \mathbb{P}^n$ by
$$U_i = \mathbb{P}^n \setminus Z(x_i),$$
an open subset of $\mathbb{P}^n$. Note $\bigcup_{i=1}^n U_i = \mathbb{P}^n$. We have a bijection $\varphi_i : U_i \to \mathbb{A}^n$, given by
$$\varphi_1(x_0 : \dots : x_n) = \left(\frac{x_0}{x_i}, \dots, \widehat{\frac{x_i}{x_1}}, \dots, \frac{x_n}{x_i}\right)$$
(hat means this is omitted).

**Proposition.** With $U_i$ carrying the topology induced from $\mathbb{P}^n$, and $\mathbb{A}^n$ the Zariski topology, $\varphi_i$ is a homeomorphism.

*Proof.* Since $\varphi_i$ is a bijection, enough to show $\varphi_i$ identifies closed sets of $U_i$ with closed sets of $\mathbb{A}^n$. Can take $c = 0$, $\varphi = \varphi_0$, $U = U_0$. Let $S = \mathbb{K}[X_0, \dots, X_n]$, $S^h$ be the set of homogeneous polynomials in $S$. Let $A = \mathbb{K}[Y_1, \dots, Y_n]$. Define maps $\alpha : S^n \to A$, $\beta : A \to S^n$ by $\alpha(f(x_0, \dots, x_n)) = f(1, y_1, \dots, y_n)$. If $g \in A$ of degree $e$ (highest degree term is degree $e$), then define
$$\beta(g) = x_0^e g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$$
**Remark:** This is a process known as *homogenisation*. For example, $y_2^2 - y_1^3 - y_1 + y_1 y_2$ becomes
$$x_0^3\left(\frac{x_2^2}{x_0^2} - \frac{x_1^3}{x_0^3} - \frac{x_1}{x_0} + \frac{x_1 x_2}{x_0^2}\right) = x_0 x_2^2 - x_1^3 - x_0^2 x_1 + x_0 x_1 x_2.$$
under $\beta$.

If $Y \subseteq U$ is closed, then $Y$ is the intersection $\overline{Y} \cap U$ where $\overline{Y} \subseteq \mathbb{P}^n$ is a closed subset, which we can take to be the closure of $Y$. $\overline{Y} = Z(T)$ for some $T \subseteq S^h$. Let $T' = \alpha(T)$. Then $\varphi(Y) = Z(\alpha(T))$.

Check:
$$\begin{aligned} f(a_0 : \dots : a_n) = 0, (a_0 \neq 0) &\iff f\left(f, \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) = 0 \\ &\iff (\alpha(f))\left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) \\ &\iff \alpha(f)(\varphi(a_0, \dots, a_n)) = 0 \end{aligned}$$

Start of lecture 10

Still to prove that if $W \subseteq \mathbb{A}^n$ is closed, then $\varphi^{-1}(W) \subseteq U = U_0$ is closed. We have $W = Z(T')$ for some set $T' \subseteq A = \mathbb{K}[Y_1, \ldots, Y_n]$. Then

$$\varphi^{-1}(W) = Z(\beta(T')) \cap U$$

($\beta$ is homogenisation as mentioned earlier). Indeed, if $g \in T'$,

$$\begin{aligned} g(b_1, \ldots, b_n) = 0 &\iff \beta(g)(1, b_1, \ldots, b_n) = 0 \\ &\iff \beta(g)(\varphi^{-1}(b_1, \ldots, b_n)) = 0 \end{aligned}$$

□

**Example.** $f : \mathbb{P}^1 \to \mathbb{P}^3$.

$$f(u : t) = (u^3, u^2t, ut^2, t^3)$$

which is well-defined. The image of this map is called the *twisted cubic* (recall Example Sheet 1).

**Claim:** This is a projective variety.

Proof: Consider the homomorphism

$$\begin{aligned} \phi : \mathbb{K}[X_0, \dots, X_3] &\to \mathbb{K}[u, t] \\ X_0 &\mapsto u^3 \\ X_1 &\mapsto u^2t \\ X_2 &\mapsto ut^2 \\ X_3 &\mapsto t^3 \end{aligned}$$

Let $I = \ker \varphi$. If $g \in I$, then $g$ vanishes on the image of the map $f$. Thus $\mathrm{Im}(p) \le Z(I)$.

Conversely, note that

$$X_0X_3 - X_1X_2, X_1^2 - X_0X_2, X_2^2 - X_1X_3 \in I.$$

Let $p = (a_0 : a_1 : a_2 : a_3) \in Z(I)$. 4 cases:

- $a_0 \neq 0$. So take $a_0 = 1$.

  $$a_3 - a_1a_2 = 0, \qquad a_1^2 - a_2 = 0, \qquad a_2^2 - a_1a_3 = 0.$$

  Then $p = (1, a_1, a_2^2, a_1^3) = f(1 : a_1)$. Thus $p \in \mathrm{Im}(f)$.

Similarly check cases $a_1 \neq 0$, $a_2 \neq 0$ and $a_3 \neq 0$. The conclusion is $p \in \mathrm{Im}(f)$ in all 4 cases, so $\mathrm{Im}\, f \supseteq Z(I)$. Therefore $Z(I) = \mathrm{Im}\, f$. Thus the twisted cubic is an algebraic set.

**Exercise:** Given $X \subseteq \mathbb{P}^n$ an algebraic, define its *ideal* $I(X)$ to be the ideal in $S = \mathbb{K}[X_1, \dots, X_n]$ generated by homogeneous polynomials vanishing on $X$. Then show that $X$ is irreducible if and only if $I(X)$ is prime.

For the twisted cubic, $X = \mathrm{Im}(F)$, $I(X) = I = \ker(\varphi)$. But

$$\frac{\mathbb{K}[X_0, \dots, X_3]}{\ker \varphi}$$

is a subring of the integral domain $\mathbb{K}[u, t]$. Hence it is an integral domain, hence $\ker \varphi$ is prime. Therefore $X$ is a projective variety.

**Definition** (Projective regular function)**.** Let $X \subseteq \mathbb{P}^n$ be a projective variety. A *regular function* on $U \subseteq X$ open is a function $f : U \to \mathbb{K}$ such that for every $p \in U$, there exists an open neighbourhood $V \subseteq U$ of $p$ and $g, h \in S$ homogeneous of the same degree with $h$ nowhere vanishing on $V$, and with $f|_V = \frac{g}{h}$.

**Definition** (Quasi-variety)**.** A *quasi-affine variety* is an open subset of an affine variety.

A *quasi-projective variety* is an open subset of a projective variety.

These types of varieties also have (the same) notion of regular functions.

A *variety* means an affine, quasi-affine, projective or quasi-projective variety.

**Definition** (Morphism between varieties)**.** A *morphism* $\varphi : X \to Y$ between varieties is a continuous function $\varphi$ such that $\forall V \subseteq Y$ open, $f : V \to \mathbb{K}$ regular, $f \circ \varphi : \varphi^{-1}(U) \to \mathbb{K}$ is regular.

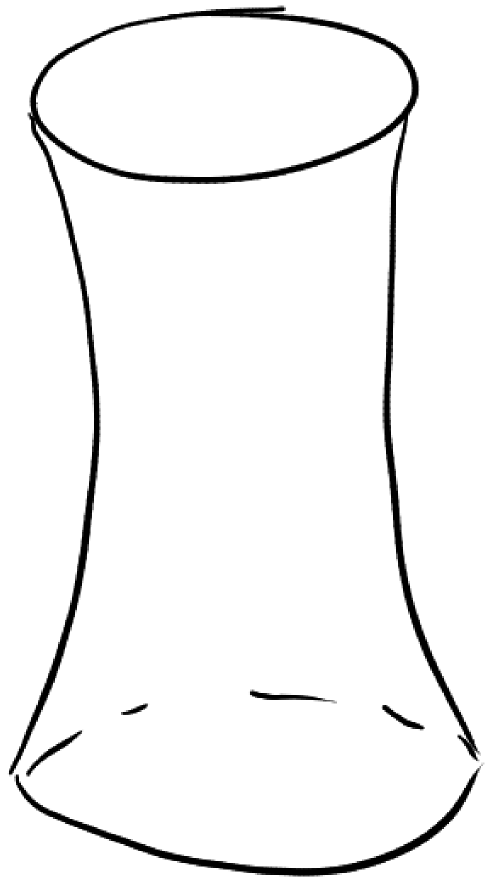
**Remark.** If $X$ is projective, then in fact

$$\mathcal{O}_X(X) = \{X \to \mathbb{K} \text{ regular}\}$$

is $\mathbb{K}$. Thus finding morphisms from a projective variety becomes much harder, and this is a lot of what Algebraic Geometry is about.

### Example

Let $Q \subseteq \mathbb{P}^3$ be given by $Z(xy - zw)$. This is a quadric surface



**Important feature:** For $(a:b) \in \mathbb{P}^1$, $Q$ contains the line

$$ax = bz, by = aw$$

(if $a \neq 0$, can take $a = 1$, $(bz)y - z(by) = 0$, if $a = 0$, $z = 0$, $y = 0$, so $xy - zw = 0$). This gives a family of lines in $Q$ parametrized by $(a:b) \in \mathbb{P}^1$> We also have $ax = bw$, $by = az$ for $(a:b) \in \mathbb{P}^1$ contained in $Q$.

If we take a line from one family and a line from the other, they meet at one point:

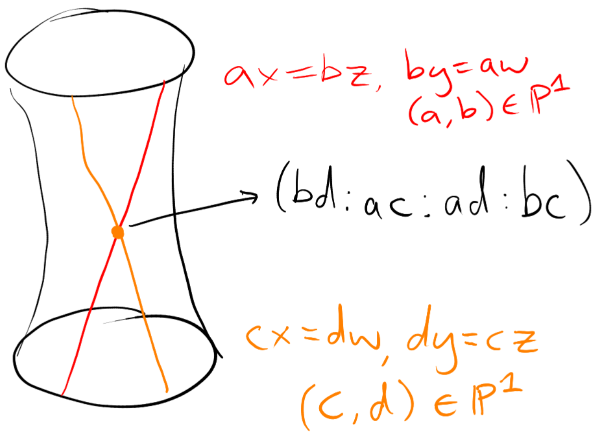
$$ax = bz, by = aw$$

$$cx = dw, dy = cz$$

has a unique solutoin up to scaling: $(bd, ac, ad, bc)$.

Start of

lecture 11




This suggests we define a map $\Sigma : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$,

$$\Sigma((a:b),(c:d)) = (bd:ac:ad:bc)$$

**Claim:** $\Sigma$ is a bijection with $Q = Z(xy - zw)$.

*Proof.* Note $(bd)\cdot(ac) - (ad)\cdot(bc) = 0$, so $\Sigma$ has image in $Q$. Injection: suppose $a, c \neq 0$, so

$$\Sigma((1:b),(1:d)) = (bd:1:d:b)$$

so clearly injective on the set where $a, c \neq 0$. If $a = 0$,

$$\Sigma((0:b),(c:d)) = (bd:0:0:bc) = (d:0:0:c)$$

doesn't coincide with any of the previous points and is injective on the locus where $a = 0$. If $a = c = 0$,

$$\Sigma((0:1),(0:1)) = (1:0:0:0)$$

If $a \neq 0$, $c = 0$,

$$\Sigma((a:b),(0:1)) = (b;0:a:0)$$

so $\Sigma$ is injective.

Surjective: Suppose $(a_0 : a_1 : a_2 : a_3) \in Q$, i.e. $a_0a_1 - a_2a_3 = 0$. If $a_0 \neq 0$, can take $a_0 = 1$, so $a_1 = a_2a_3$. So

$$(a_0 : a_1 : a_2 : a_3) = (1 : a_2a_3 : a_2 : a_3) = \Sigma((a_2:1),(a_3:1))$$

Similar arguments work in the charts where $a_1 \neq 0$, $a_2 \neq 0$ or $a_3 \neq 0$. □

**Moral.** $\mathbb{P}^1 \times \mathbb{P}^1$ is not a projective variety, but can be given a variety structure by identifying it with $Q$, i.e. closed sets of $\mathbb{P}^1 \times \mathbb{P}^1$ are of the form $\Sigma^{-1}(Z)$ for $Z \subseteq Q$ closed.

**Exercise:** Check this is not the product topology on $\mathbb{P}^1 \times \mathbb{P}^1$.

regular functions on $U = \Sigma^{-1}(V)$ for $V \subseteq Q$ open, are functions on $U$ of the form $\varphi \circ \Sigma$ with $\varphi : V \to \mathbb{K}$ regular.

A generalisation:

The *Segre embedding* is the map

$$\Sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$$

given by

$$\Sigma((x_0 : \cdots : x_n), (y_0 : \cdots : y_m)) = (x_i y_j)_{\substack{0 \le i \le n \\ 0 \le j \le m}}$$

**Theorem.** $\Sigma$ is injective and its image is an algebraic variety.

Thus $\mathbb{P}^n \times \mathbb{P}^m$ acquires the structure of an algebraic variety.

**Theorem.** If $X \subseteq \mathbb{P}^n$, $Y \subseteq \mathbb{P}^m$ are projective varieties, then $\Sigma(X, Y)$ is a projective variety in $\mathbb{P}^{(n+1)(m+1)-1}$.

**Moral.** This allows us to thin of $X \times Y$ as a projective variety.

**Remark.** We can also think of the geometry of $\mathbb{P}^n \times \mathbb{P}^m$ by thinking about *bihomogeneous* polynomials in $\mathbb{K}[x_0, \dots, x_n, y_0, \dots, y_m]$, i.e. polynomials $f$ satisfying

$$f(\lambda x_0, \dots, \lambda_n x_n, \mu y_0, \dots, \mu y_m) = \lambda^d \mu^e f(x_0, \dots, x_n, y_0, \dots, y_m).$$

We say $f$ is bidegree $(d, e)$. $f = 0$ makes sense as an equation in $\mathbb{P}^n \times \mathbb{P}^m$.

**Remark.** If $X$ and $Y$ are quasi-projective, $X \subseteq \overline{X} \subseteq \mathbb{P}^n$, $Y \subseteq \overline{Y} \subseteq \mathbb{P}^m$, then $X \times Y \subseteq \overline{X} \times \overline{Y}$ defines an open subset of $\overline{X} \times \overline{Y}$ (check!). This allows us to view $X \times Y$ as a quasi-projective variety.

**Example: The blowup of $\mathbb{A}^n$**

By the Remark, $\mathbb{A}^n \times \mathbb{P}^{n-1}$ is a quasi-projective variety.

Let

$$X = Z(\{x_i y_j - x_j y_i \mid 1 \leq i < j \leq n\}) \subseteq \mathbb{A}^n \times \mathbb{P}^{n-1}.$$

Let $\varphi : X \to \mathbb{A}^n$ be given by

$$\varphi((x_1, \dots, x_n), (y_1 : \dots : y_n)) = (x_1, \dots, x_n),$$

the projection. This is a morphism.

**Observations:**

(1) If $p \in \mathbb{A}^n \setminus \{0\}$, then $\varphi^{-1}(p)$ consists of one point.

*Proof.* Let $p = (a_1, \dots, a_n)$, say $a_1 \neq 0$. If

$$((a_1, \dots, a_n), (b_1 : \dots : b_n)) \in \varphi^{-1}(p),$$

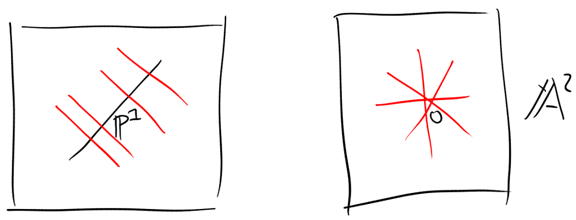
then for $j \neq i$, $a_i b_j - a_j b_i = 0$, or $b_j = \frac{a_j}{a_i} b_i$. So $b_1, \dots, b_n$ are completely determined up to scaling. Taking $b_i = a_i$, we see

$$\varphi^{-1}(p) = \{((a_1, \dots, a_n), (a_1 : \dots : a_n))\}. \qquad \square$$

Defining $\psi : \mathbb{A}^n \setminus \{0\} \to X$ by $\psi(a_1, \dots, a_n) = ((a_1, \dots, a_n), (a_1 : \dots : a_n))$ is an inverse to $\varphi|_{X \setminus \varphi^{-1}(0)} : X \setminus \varphi^{-1}(0) \to \mathbb{A}^n \setminus \{0\}$.

(2) $\varphi^{-1}(0) = \{0\} \times \mathbb{P}^{n-1}$

(3) The points of $\varphi^{-1}(0)$ are in $1-1$ correspondence with the lines through the origin in $\mathbb{A}^n$. $n = 2$ picture:




Start of

lecture 12

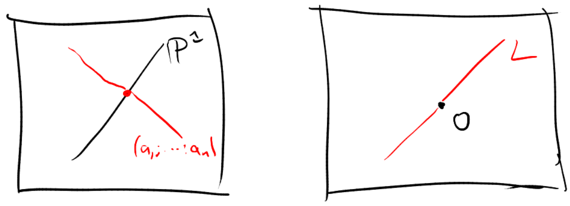
*Proof.* A line through 0 can be parametrised by $l : \mathbb{A}^1 \to \mathbb{A}^n$,

$$l(t) = (a_1 t, \dots, a_n t)$$

for some $a_1, \dots, a_n$ not all 0. For $t \neq 0$,

$$\begin{aligned} \varphi^{-1}(a_1 t, \dots, a_n t) &= ((a_1 t, \dots, a_n t), (a_1 t : \cdots : a_n t)) \\ &= ((a_1 t, \dots, a_n t), (a_1 : \cdots : a_n)) \end{aligned}$$

Thus the lift of $L \setminus \{0\}$ is given parametrically by $t \mapsto ((a_1 t, \dots, a_n t), (a_1 : \cdots : a_n))$, $\mathbb{A}^1 \setminus \{0\} \to \varphi^{-1}(\mathbb{A}^n \setminus \{0\}) \subseteq X$. This extends to all of $\mathbb{A}^1$ and also $\overline{\varphi^{-1}(L \setminus \{0\})}$ is the image of this parametrisation.




□

(4) $X$ is irreducible.

*Proof.* $X = (X \setminus \varphi^{-1}(0)) \cup \varphi^{-1}(0)$. The first set being homeomorphic to $\mathbb{A}^n \setminus \{0\}$, and hence is irreducible. (An open subset of an irreducible space is irreducible). But every point of $\varphi^{-1}(0)$ is in the closure of $X \setminus \varphi^{-1}(0)$, by the proof of (3), so $X \setminus \varphi^{-1}(0)$ is dense in $X$.

**Claim**: If $U \subseteq X$ is a dense open set and $U$ is irreducible, then $X$ is irreducible.

Proof: If $X = Z_1 \cup Z_2$, $Z_1, Z_2$ closed, then $U = (Z_1 \cap U) \cup (Z_2 \cap U)$, so $U = Z_1 \cap U$ say. So $U \subseteq Z_1$, so $\overline{U} \subseteq Z_1$. But $\overline{U} \subseteq Z_1$. But $\overline{U} = X$ by density of $U$. SO $Z_1 = X$.

Thus the blowup $X$ is irreducible. □

**Definition** (Blowing up)**.** If $Y \subseteq \mathbb{A}^n$ is a closed subvariety with $0 \in Y$, we define the *blowing up* of $Y$ at 0 to be

$$\tilde{Y} := \overline{\varphi^{-1}(Y \setminus \{0\})} \subseteq X,$$

where $X = Z(\{x_i y_j - x_j y_i \mid 1 \leq i < j \leq n\}) \subseteq \mathbb{A}^n \times \mathbb{P}^{n-1}$, $\varphi : X \to \mathbb{A}^n$ is given by projection of the first $n$ coordinates.

### Example

Let $Y \subseteq \mathbb{A}^2$ be given by

$$Y = Z(\underbrace{x_2^2 - (x_1^3 + x_1^2)}_{x_2^2 - x_1^2(x_1+1)})$$

$X \subseteq \mathbb{A}^2 \times \mathbb{P}^1$, $x_1 y_2 - x_2 y_1 = 0$. Work in two coordinate patches:

$$U_1 = \{y_1 \neq 0\}, \qquad U_2 = \{y_2 \neq 0\}$$

In $U_2$, we set $y_2 = 1$, and the equation for $X$ becomes $x_1 = x_2 y_1$. Then

$$\varphi^{-1}(Y) \cap U_2 = Z(x_2^2 - (x_1^3 + x_1^2), x_1 - x_2 y_1) \subseteq \mathbb{A}^2 \times \mathbb{A}^1 = \mathbb{A}^3.$$

This is isomorphic to

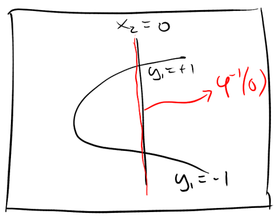
$$Z(x_2^2 - (x_2^3 y - 1^3 + x_2^2 y_1^2)) \subseteq \mathbb{A}^2.$$

In terms of coordinate rings,

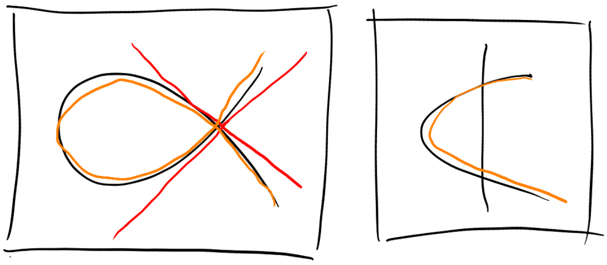
$$\frac{\mathbb{K}[x_1, x_2, y_1]}{\langle x_2^2 - (x_1^3 + x_1^2), x_1 - y_1 x_2 \rangle} \cong \frac{\mathbb{K}[x_2, y_1]}{\langle x_2^2 - (x_2^3 y_1^2 + x_2^2 y_1^2) \rangle}$$

Note

$$x_2^2 - (x_2^2 y_1^2 + x_2^2 y_1^2) = x_2^2(1 - x_2 y_1^2 - y_1^2)$$




Noet $\varphi^{-1}(0) \cap U_2 = Z(x_2)$. The blowup $\tilde{Y} \cap U_2 = \overline{\varphi^{-1}(Y \setminus \{0\})} \cap U_2$ is now given by the equation $1 - x_2 y_1^2 - y_1^2$ in $\mathbb{A}^2$ $(x_2, y_1)$.



For thoroughness, we will also consider $\tilde{Y} \cap U_1$, where $y_1 = 1$, $x_2 = x_1 y_2$, so can eliminate $x_2$ from equation to get

$$x_1^2 y_2^2 - (x_1^3 + x_1^2) = x_1^2(y_2^2 - x_1 - 1)$$

$\tilde{Y} \cap U_1$ has equation $y_2^2 - x_1 - 1 = 0$.

### Rational maps

**Definition** (Rational map)**.** Let $X, Y$ be varieties. Consider the equivalence relation on pairs $(U, f)$ where $U \subseteq X$ open, and $f : U \to Y$ a morphism, with $(U, f) \sim (V, g)$ if $f|_{U \cap V} = g|_{U \cap V}$.

**Exercise:** Check that this is an equivalence relation.

A *rational map* $f : X \dashrightarrow Y$ is an equivalence class of a pair.

**Example.** If $X$ is affine, $\varphi = \frac{f}{g} \in K(X)$, then we have a morphism $\varphi : X \setminus Z(g) \to \mathbb{A}^1$. This defines a rational morphism to $\mathbb{A}^1$.

Start of lecture 13

**Definition** (Birational map)**.** A *birational map* is a rational map $f : X \dashrightarrow Y$ with a rational inverse $g : Y \dashrightarrow X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$ as rational maps.

**Remark.** We can't always compose rational maps. Suppose given $f : X \dashrightarrow Y$, $g : Y \dashrightarrow Z$, $f : U \to Y$, $g : V \to Z$. If $f(U) \subseteq Y \setminus V$, we can't compose. If this is not the case, then $f^{-1}(Y \setminus V) \subsetneq U$ is a proper subset of $U$, and then $g \circ f : U \setminus f^{-1}(Y \setminus V) \to Z$ defines a rational map $g \circ f : X \dashrightarrow Z$. Note the ability to compose may depend on the representative for $f, g$.

**Remark.** One can show that if $f : X \dashrightarrow Y$ is a birational map, then $\exists U \subseteq X$, $V \subseteq Y$ such that $f$ is defined on $U$, $f(U) \subseteq V$ and $f : U \to V$ is an isomorphism.

**Definition** (Birationally equivalent)**.** We say varieties $X, Y$ are *birationally equivalent* if there exists a birational map $f : X \dashrightarrow Y$. Equivalently, $\exists U \subseteq X$, $V \subseteq Y$ open subsets with $U \cong V$.

**Example.** $\varphi : X \to \mathbb{A}^n$, the blow up of $\mathbb{A}^n$ at $0 \in \mathbb{A}^n$. This is a birational map (morphism) since it induces an isomorphism $\varphi : \varphi^{-1}(\mathbb{A}^n \setminus \{0\}) \to \mathbb{A}^n \setminus \{0\}$. $\varphi^{-1} : \mathbb{A}^n \dashrightarrow X$ is not a morphism, only defined on $\mathbb{A}^n \setminus \{0\}$.

**Definition** (Dominant)**.** We say that $f : X \dashrightarrow Y$ is a *dominant* rational map if whenever $\tilde{f} : U \to Y$ is a representative for $f$, then $f(U)$ is dense in $Y$.

**Definition** (Function field of a variety)**.** The *function field* of a variety $X$ is

$$K(X) = \{(U, f) \mid f : U \to \mathbb{K} \text{ is a regular function}\}/\sim,$$

where $(U, f) \sim (V, g)$ if $f|_{U \cap V} = g|_{U \cap V}$. In particular, if $X$ is affine variety, then this is the field of fractions of $A(X)$. If $f$ is dominant, we obtain

$$\begin{aligned} f^{\#} : K(Y) &\to K(X) \\ (V, \varphi) &\mapsto (f^{-1}(V) \cap U, \varphi \circ f) \end{aligned}$$

Note $f^{-1}(V) \cap U$ is non-empty since $V \cap f(U) \neq \emptyset$ by density of $f(U)$.

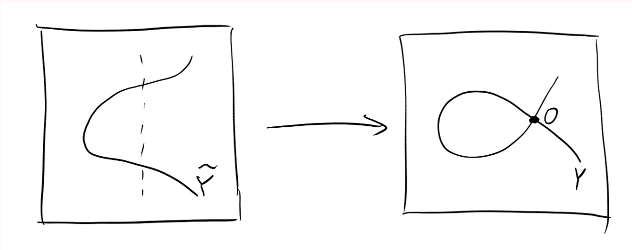
**Note.** If $f : X \dashrightarrow Y$ is a birational map, with birational inverse $g : Y \dashrightarrow X$, each are dominant since they induce isomorphisms between open subsets. Thus we get

$$f^{\#} : K(Y) \to K(X), \qquad g^{\#} : K(X) \to K(Y)$$

inverse maps, so $K(X) \cong K(Y)$.

**Fact:** If $K(X) \cong K(Y)$, then $X$ and $Y$ are birational to each other, i.e. $\exists f : X \dashrightarrow Y$ birational.

**Example.** $0 \in Y \subseteq \mathbb{A}^n$, $\tilde{Y} \to Y$ the blow up of $Y$ at $0$ is a birational morphism:



# 4 Tangent spaces, singularities and dimension

**Recall:** Gvien an equation $f(X_1, \dots, X_n) = 0$ in $\mathbb{R}^n$, $X$ the solution set, $p \in X$, the tangent space to $X$ is the orthogonal complement to $(\nabla f)(p)$, i.e. the tangent space to $X$ at $p$ is

$$T_pX := \left\{ (v_1, \dots, v_n) \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^{n} v_i \frac{\partial f}{\partial x_i}(p) = 0 \right\}.$$

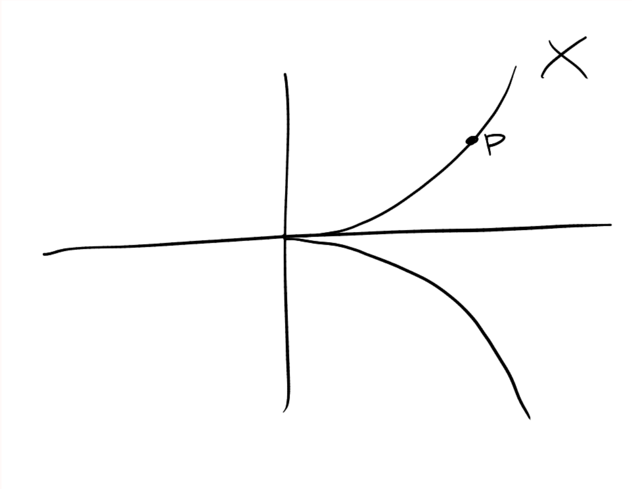
This is a vector subspace of $\mathbb{R}^n$.

**Definition** (Tangent space)**.** If $X \subseteq \mathbb{A}^n$ is an affine variety with $I = I(X) = \langle f_1, \dots, f_r \rangle$, $f_1, \dots, f_r \in \mathbb{K}[X_1, \dots, X_n]$, then we define, for $p \in X$ the tangent space to $X$ at $p$ by

$$T_pX = \left\{ (v_1, \dots, v_n) \in \mathbb{K}^n \;\middle|\; \sum_{i=1}^{n} v_i \frac{\partial f_j}{\partial x_i}(f) = 0, 1 \leq j \leq r \right\}.$$

The derivative is defined using the standard differentiation rules for polynomials.

**Example.** $I = \langle x_2^2 - x_1^3 \rangle \subseteq \mathbb{K}[x_1, x_2]$, $X = Z(I)$, $p = (a_1, a_2)$.




$$T_pX = \{(v_1, v_2) \in \mathbb{K}^2 \mid v_1(-3a_1^2) + v_2(2a_2) = 0\}$$

$$\dim_{\mathbb{K}} T_pX = \begin{cases} 1 & p \neq (0,0) \\ 2 & p = (0,0) \end{cases}$$

(assuming $\operatorname{char} \mathbb{K} \neq 2, 3$).

**Definition** (Dimension of an affine variety)**.** Let $X \subseteq \mathbb{A}^n$ be an affine variety. Then the *dimension* of $X$ is

$$\dim X = \min\{\dim_{\mathbb{K}} T_pX \mid p \in X\}.$$

We say $X$ is *singular* at $p$ if $\dim_{\mathbb{K}} T_pX > \dim X$.

**Lemma.** $\{p \in X \mid \dim_{\mathbb{K}} T_pX \geq K\}$ is a closed subset of $X$.

*Proof.*

$$T_pX = \ker \underbrace{\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_r}{\partial x_1} & \cdots & \frac{\partial f_r}{\partial x_n} \end{pmatrix}}_{\mathbb{K}^n \to \mathbb{K}^r}$$

where $I(X) = \langle f_1, \ldots, f_r \rangle$. But $\dim \ker M + \operatorname{rank} M = n$ (rank-nullity). So

$$\begin{aligned} \dim T_p X \geq K &\iff n - \operatorname{rank} \geq K \\ &\iff \operatorname{rank} \leq n - K \end{aligned}$$

If $A$ is an $r \times n$ matrix, then $\operatorname{rank}(A) \geq k+1$ if and only if there is a $(k+1) \times (k+1)$ submatrix of $A$ whose determinant is non-zero. So $\operatorname{rank} J \leq n - k$ if and only if all $(n-k+1) \times (n-k+1)$ minors (determinants of $(n-k+1) \times (n-k+1)$ matrices) vanish. Thus the set:

$$\{p \in X \mid \dim T_p X \geq k\} = Z(f_1, \ldots, f_r, \text{ all } (n-k+1) \times (n-k+1) \text{ minors of } J).$$

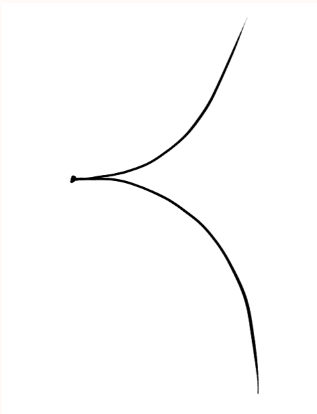
Hence this set is closed. □

Start of lecture 14

**Recall:** $p \in X$ is singular if $\dim_{\mathbb{K}} T_p X > \dim X = \inf\{\dim T_p X\}$.

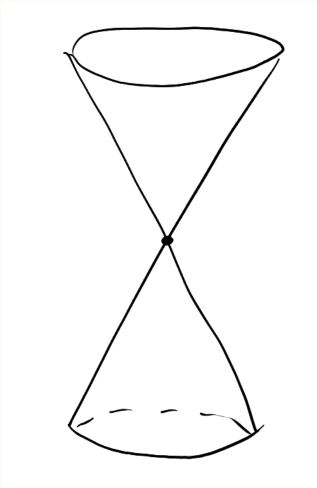
The above lemma tells us that the set of singular points of $X$ is a *proper* closed subset.

**Example.** $y_2 - x^3 = 0$, $J = (2y, -3x^2)$



vanishes when $x = y = 0$.

**Example.** $x^2 + y^2 - z^2 = 0$, $J = (2x, 2y, -2z)$, vanishing at the origin.



**Intrinsic characterisation of the tangent space**

Let $X$ be an affine variety. For $p \in X$, define $\varphi_p : A(X) \to \mathbb{K}$ to be the $\mathbb{K}$-algebra homomorphism given by $\varphi_p(f) = f(p)$.

**Definition** (Derivation centred at $p$)**.** A *derivation centred at* $p$ is a map $D : A(X) \to \mathbb{K}$ such that

(1) $D(f + g) = D(f) + D(g)$

(2) $D(fg) = \varphi_p(f)D(g) + D(f)\varphi_p(g)$ (the RHS can also be written as $f(p)D(g) + g(p)D(f)$). (Leibniz rule).

(3) $D(a) = 0$ for $a \in \mathbb{K}$.

Denote $\mathrm{Der}(A(X), p)$ to be the set of derivations centred at $p$.

**Note.** $\mathrm{Der}(A(X), p)$ is a $\mathbb{K}$-vector space (check $D_1 + D_2$, $aD$ are derivations if $D_1, D_2, D$ are derivations).

**Theorem.** $T_pX \cong \mathrm{Der}(A(X), p)$ as $\mathbb{K}$-vector spaces for $p \in X$.

*Proof.* Given $(v_1, \ldots, v_n) \in T_pX$, so if $I(X) = \langle f_1, \ldots, f_r \rangle$, $\sum_i v_i \frac{\partial f_j}{\partial x_i}(p) = 0$ for all $j$. Define

$$\mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}f \qquad\qquad \mapsto \sum_i v_i \frac{\partial f}{\partial x_i}(p)$$

This vanishes on elements of $I(X)$, which are of the form $f = \sum_{j=1}^r g_j f_j$ for $g_j \in \mathbb{K}[x_1, \ldots, x_n]$. Then

$$\begin{aligned} f &\mapsto \sum_{i=1}^n v_i \left( \sum_{j=1}^r \left( \frac{\partial f_j}{\partial x_i} \cdot g_j + \frac{\partial g_j}{\partial x_i} f_j \right)(p) \right) \qquad (f_j(p) = 0 \text{ for all } j, \text{ since } p \in X) \\ &= \sum_{i,j} \left( v_i \frac{\partial f_j}{\partial x_i} g_j(p) \right) \\ &= \sum_j g_j(p) \left( \sum_i v_i \frac{\partial f_j}{\partial x_i}(p) j \right) \\ &= 0 \end{aligned}$$

Thus we get a well-defined $\mathbb{K}$-linear map

$$D_r : \frac{\mathbb{K}[x_1, \ldots, x_n]}{I(X)} = A(X) \to \mathbb{K}.$$

Check easily that this is a derivation. Given $D \in \operatorname{Der}(A(X), p)$, define $v_i = D(x_i)$. By repeated use of the Leibniz rule,

$$D(f) = \sum_{i=1}^n v_i \frac{\partial f}{\partial x_i}(p).$$

Example:

$$\begin{aligned} D(x_1 x_2) &= D(x_1) \cdot x_2(p) + x_1(p) D(x_2) \\ &= v_1 x_2(p) + v_2 x_1(p) \\ &= v_1 \frac{\partial(x_1 x_2)}{\partial x_1}(p) + v_2 \frac{\partial(x_1 x_2)}{\partial x_2}(p) \end{aligned}$$

Thus $D(f_j) = \sum_i v_i \frac{\partial f_j}{\partial x_i}(p)$, but $f_j \in I(X)$, so $D(f_j) = 0$. Thus $\sum_i v_i \frac{\partial f_f}{\partial x_i}(p) = 0$ for all $j$, so $(v_1, \ldots, v_n) \in T_pX$. □

**Remark.** Singular points and tangent spaces are intrinsic to affine varieties.

**Definition** (Local ring)**.** Let $X$ be a variety, $p \in X$. We define the *local ring* to $X$ at $p$ to be

$$\mathcal{O}_{X,p} = \{(U, f) \mid U \text{ is an open neighbourhoof of } p,\ f : U \to \mathbb{K} \text{ a regular function}\}/\sim$$

where $(U, f) \sim (V, g)$ if $f|_{U \cap V} = g_{U \cap V}$. This is a subring of $K(X)$, the field of fractions.

**Example.**

(1) $X \subseteq \mathbb{A}^n$ is an affine variety,

$$\mathcal{O}_{X,p} = \left\{ \frac{f}{g} \in K(X) \;\middle|\; g(p) \neq 0, f, g \in A(X) \right\}.$$

(2) $X \subseteq \mathbb{P}^n$ a projective variety. Then

$$\mathcal{O}_{X,p} = \left\{ \frac{f}{g} \;\middle|\; {}^{f,g \in \mathbb{K}[x_1,\ldots,x_n]/I(X), g(p) \neq 0,}_{f,g \text{ homogeneous of the same degree}} \right\}$$

which is a subring of

$$K(X) = \left\{ \frac{f}{g} \mid {}^{f,g \in \mathbb{K}[x_0,\ldots,x_n]/I(X), g \neq 0}_{f,g \text{ homogeneous of the same degree}} \right\}$$

**Remark.** The definition of $\mathcal{O}_{X,p}$ makes it intrinsic, i.e. not dependent on the embedding.

**Remark.** $\mathcal{O}_{X,p}$ is a ring ($(U, f) + (V, g) = (U \cap V, f|_{U \cap V} + g|_{U \cap V})$ etc). We define

$$m_p = \{(U, f) \in \mathcal{O}_{X,p} \mid f(p) = 0\}.$$

This is an ideal, and every element of $\mathcal{O}_{X,p} \setminus m_p$ is invertible. Thus $m_p$ is the *unique* maximal ideal of $\mathcal{O}_{X,p}$.

**Definition** (Local ring)**.** A ring $A$ with a unique maximal ideal is called a *local ring*.

Start of

lecture 15

**Theorem.** If $X \subseteq \mathbb{A}^n$ is an affine variety then $T_pX \cong (m_p/m_p^2)^*$ where $V^*$ is the dual of the $\mathbb{K}$-vector space $V$.

*Proof.* Note that there is an isomorphism

$$\begin{aligned} \mathcal{O}_{X,p}/m_p &\to \mathbb{K} \\ f &\mapsto f(p) \end{aligned}$$

This map is surjective since constants are regular functions, and injective by definition of $m_p$. Thus we can define the $\mathbb{K}$-vector space on $m_p/m_p^2$ by identifying $\mathbb{K}$ with $\mathcal{O}_{X,p}/m_p$, and

$$(f + m_p) \cdot (g + m_p^2) = (f \cdot g + m_p^2).$$

We will show $\mathrm{Der}(A(X), p) \cong (m_p/m_p^2)^*$. Given $D \in \mathrm{Der}(A(X), p)$, we define

$$\varphi_D : m_p/m_p^2 \to \mathbb{K}$$

defined as follows: for $f, g \in A(X)$, $g(p) \neq 0$, $f(p) = 0$, $(X \setminus Z(g), \frac{f}{g}) \in m_p\mathcal{O}_{X,p}$. Set

$$\begin{aligned} \varphi_D\left(\frac{f}{g}\right) &= \text{“}D\left(\frac{f}{g}\right)\text{”} \\ &= \frac{g(p)D(f) - f(p)D(g)}{g(p)^2} \\ &= \frac{D(f)}{g(p)} \end{aligned}$$

since $f(p) = 0$. Note if $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in m_p$, then

$$\varphi_D\left(\frac{f_1f_2}{g_1g_2}\right) = \frac{f_2(p)}{g_2(p)} \cdot \varphi_D\left(\frac{f_1}{g_1}\right) + \frac{f_1(p)}{g_1(p)}\varphi_D\left(\frac{f_2}{g_2}\right) = 0.$$

Thus $\varphi_D(m_p^2) = 0$, so we obtain a well-defined map $\varphi_D : m_p/m_p^2 \to \mathbb{K}$.

Conversely, if given $\varphi : m_p/m_p^2 \to \mathbb{K}$, $p = (a_1, \dots, a_n) \in X \subseteq \mathbb{A}^n$. Note $x_i - a_i \in m_p$ for all $i$, and we define

$$D_\varphi(x_i - a_i) = \varphi(x_i - a_i).$$

This is sufficient to determine $D_\varphi$ as before. ∎

**Example.** Suppose $X = \mathbb{A}^n$, $p = 0$. Then

$$m_p/m_p^2 = \underbrace{(x_1, \dots, x_n)}_{\subseteq \mathbb{K}[x_1,\dots,x_n]} / (x_1, \dots, x_n)^2$$

(exercise).

**Definition** (Zariski tangent space)**.** If $X$ is any variety, and $p \in X$, then the *Zariski tangent space* to $X$ at $p$ is

$$T_p X = (m_p/m_p^2)^*,$$

where $m_P \subseteq \mathcal{O}_{X,p}$ is the maximal ideal.

**Theorem.** Any variety has an open cover by affine varieties (i.e. open subsets isomorphic to affine varieties).

**Note.** If $X \subseteq \mathbb{P}^n$ is projective, $\{U_i \cap X \mid 0 \le i \le n\}$ ($U_i = \mathbb{P}^n \setminus Z(x_i)$) is a cover of $X$ by affines.

*Proof.* Consider the most general case where $X$ is a quasi-projective variety, $X \subseteq \mathbb{P}^n$. Each $U_i \cap X$ is a quasi-affine variety. So enough to show each quasi-projective variety is covered by affine varieties. Let $p \in X \subseteq \mathbb{A}^n$. Will find an affine neighbourhood of $p$ in $X$. Then $\overline{X} \subseteq \mathbb{A}^n$, the closure, is an affine variety, and $Z = \overline{X} \setminus X$ is closed in $\overline{X}$. Choose $f \in I(Z)$ with $f(p) \neq 0$. Then $\langle f \rangle \subseteq I(X)$, so $Z(f) \supseteq Z(I(Z)) = Z$, so $p \in \overline{X} \setminus Z(f) \subseteq \overline{X} \setminus Z = X$. But $\overline{X} \setminus Z(f)$ can be identified with the closed subset of $\mathbb{A}^{n+1}$ given by $Z(I(\overline{X}), yf - 1)$ as in Example Sheet 1. □

**Remark.** The definition of dimension of singular points goes through unchanged with the Zariski tangent space.

$$\dim X = \inf\{\dim T_p X \mid p \in X\}.$$

$p \in X$ is singular if $\dim X < \dim T_p X$. By applying the above theorem, in fact the set of singular points of an arbitrary variety $X$ is closed in $X$. This also shows dimension and singularity are intrinsic to $X$.

**Alternative definitions of dimension (we won't prove stuff here)**

**Definition** (Transcendence degree)**.** If $F/\mathbb{K}$ is a finitely generated field extension, then the *transcendence degree* of $F/\mathbb{K}$, written $\mathrm{Trdeg}_{\mathbb{K}} F$ is the cardinality of any transcendence basis.

**Definition** (Krull dimension of a ring)**.** If $A$ is a ring, the *Krull dimension* of $A$ is the largest $n$ such that there exists a chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subseteq A.$$

**Definition** (Krull dimension of a topological space)**.** If $X$ is a topological space, the *Krull dimension of* $X$ is the largest $n$ such that there exists a chain of irreducible subsets

$$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \subseteq X.$$

Start of lecture 16

**Remark.** If $\mathbb{K}$ is algebraically closed, then $\dim \mathbb{K}[x_1, \ldots, x_n]$ agrees with the Krull dimension of $\mathbb{A}^n$. If $X \subseteq \mathbb{A}^n$ is an affine variety, then $\dim A(X)$ equals the Krull dimension of $X$ (check: there exists a $1-1$ correspondence between prime ideals of $A(X)$ and irreducible subsets of $X$).

**Theorem.** If $X$ is a variety, then

$$\dim X = \mathrm{Trdeg}_{\mathbb{K}} K(X) = \text{Krull dimension of } X = \text{Krull dimension of } \mathcal{O}_{X,p}$$

for $p \in X$.

*Proof.* "Dimension theory" – non-examinable proof. □

**Example.** In Example Sheet 1, we showed that if $X = Z(f) \subseteq \mathbb{A}^2$, then the clsoed subsets of $X$ are $X$ and finite subsets of $X$. Thus the Krull dimension of $X$ is 1.

## 5 Curves

**Definition** (Algebraic curve)**.** An *(algebraic) curve* is a variety $C$ with $\dim C = 1$.

**Definition.** Let $C \subseteq \mathbb{P}^n$ be a projective non-singular curve. We define $\operatorname{Div} C$ to be the free abelian group generated by the points of $C$. This is called the group of *divisors* of $C$.

An element of $\operatorname{Div} C$ is of the form $\sum_{i=1}^n a_i p_i$, $a_i \in \mathbb{Z}$, $p_i \in C$.

**Example.** Consider $C = \mathbb{P}^1$. An element of $K(C)$ is the raito $\frac{f(x_0,x_1)}{g(x_0,x_1)}$ where $f, g$ are homogeneous polynomials of the same degree. we can write

$$\frac{f}{g} = \frac{\prod_i (b_i x_0 - a_i x_1)^{m_i}}{\prod_j (d_j x_0 - c_j x_1)^{n_j}}$$

$\sum m_i = d = \sum n_j$. Let $P_i = (a_i : b_i)$, $Q_j = (c_j : d_j)$. $\frac{f}{g}$ has a zero of order $m_i$ at $P_i$ and a pole of order $n_j$ at $Q_j$. The divisors of zeroes and poles of $\frac{f}{g}$ is

$$\left(\frac{f}{g}\right) = \sum_i m_i P_i - \sum_j n_j Q_j.$$

**Definition** (Principal divisor)**.** We call a divisor $D \in \operatorname{Div} C$ *principal* if it is of the form $\left(\frac{f}{g}\right)$. Let $\operatorname{Prin} C \subseteq \operatorname{Div} C$ be the subgroup of principal divisors and define the *class group* of $C$ to be

$$\operatorname{Cl} C = \frac{\operatorname{Div} C}{\operatorname{Prin} C}.$$

**Example.** We see $\operatorname{Cl} \mathbb{P}^1 = \mathbb{Z}$.

**Goal:** Given any non-singular curve, $f \in K(X)$, want to define the order of 0 or pole at $p \in X$.

**Lemma.** Let $A$ be a ring, $M$ a finitely generated $A$-module and $I \subsetneq A$ an ideal such that $I \cdot M = M$. Then there exists $x \in A$ such that $x \equiv 1 \pmod{I}$ and $x \cdot M = 0$.

*Proof.* Recall if we have $\phi : M \to M$ an $A$-module homomorphism with $\phi(M) \subseteq IM$, then there exists $a_1, \ldots, a_n \in I$ such that

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0.$$

Take $\varphi$ to be the identity map. So this means multiplication by

$$1 + a_1 + a_2 + \cdots + a_n$$

is the zero homomorphism of $M$. Then taking this to be $x$, $x \equiv 1 \pmod I$ and $xM = 0$. □

**Theorem** (Nakayama's lemma)**.** Let $A$ be a local ring with maximal ideal $m$. Let $I \subseteq m$ be an ideal. Let $M$ be a finitely generated $A$-module. Then $I \cdot M = M$ implies $M = 0$.

*Proof.* There exists $x \in A$ with $x \cdot M = 0$ and $x \equiv 1 \pmod I$, so $x \equiv 1 \pmod m$. So $x \notin m$. But this implies $x$ is invertible: otherwise, $\langle x \rangle \neq A$ and hence $\langle x \rangle \subseteq m$. Then $M = x^{-1} \cdot (xM) = 0$. □

**Corollary.** Let $A$ be a local ring with maximal ideal $m$, $M$ a finitely-generated $A$-module, $I \subseteq m$ an ideal. Then if $M = IM + N$ for a submodule $N \subseteq M$, we have $M = N$.

*Proof.* Note $M/N$ satisfies

$$I\left(\frac{M}{N}\right) = \frac{IM + N}{N}.$$

If $M = IM + N$, we get $I\left(\frac{M}{N}\right) = \frac{M}{N}$, so $\frac{M}{N} = 0$. □

**Corollary.** Let $A$ be a local ring with $m$ its maximal ideal. Let $x_1, \ldots, x_n \in M$ be a set of elements of a finitely generated module $M$ such that the images $\overline{x}_1, \ldots, \overline{x}_n \in M/mM$ form a basis for $M/mM$ as an $A/m$-vector space. Then $x_1, \ldots, x_n$ generate $M$ as an $A$-module.

**Remark.** $A/m$ is a field since $m$ is maximal. Further, $M/mM$ is a vector space over $A/m$ via

$$(a + m)(\alpha + mM) = a\alpha + mM,$$

which is well-defined.

*Proof.* Let $N \subseteq M$ be the submodule of $M$ generated by $x_1, \dots, x_n$. Then the composition

$$N \hookrightarrow M \to M/mM$$

is surjective. Thus $M = N + mM$. So by the previous Corollary, $M = N$. $\square$

Start of lecture 17

**Corollary.** Let $C \subseteq \mathbb{P}^n$ be a non-singular projective curve. Then $m_p \subseteq \mathcal{O}_{C,p}$ is a principal ideal.

*Proof.* We begin by proving $\mathcal{O}_{C,p}$ is Noetherian. Replace $C$ by an open affine neighbourhood of $p \in C$, $C'$. This does not change $\mathcal{O}_{C,p}$, i.e. $\mathcal{O}_{C,p} = \mathcal{O}_{C',p}$. Then

$$\mathcal{O}_{C',p} = \left\{ \frac{f}{g} \;\middle|\; f, g \in A(C') = \frac{\mathbb{K}[x_1, \dots, x_n]}{I(C')} \right\} \subseteq K(C').$$

If $J \subseteq \mathcal{O}_{C',p}$, then

$$J = \left\{ \frac{f}{g} \;\middle|\; f \in A(C') \cap J, g \in A(C'), g(p) \neq 0) \right\} \subseteq \mathcal{O}_{C',p}.$$

Prove $\subseteq$: if $f/g \in J$, then $g \cdot \left(\frac{f}{g}\right) = f \in J$, so $f \in A(C') \cap J$. Prove $\supseteq$: if $f \in A(C') \cap J$, then $\frac{f}{g} = \frac{1}{g} \cdot f \in J$ (if $g(p) \neq= 0$).

Now $\mathbb{K}[x_1, \dots, x_n]$ is Noetherian by Hilbert's basis theorem. Hence $A(C') = \mathbb{K}[x_1, \dots, x_n]/I(C')$ is Noetherian. Hence $A(C') \cap J$ is finitely generated, and by the equation for $J$, the set of generators of $A(C')$ generate $J$ as an ideal in $\mathcal{O}_{C',p}$. Since $C$ is non-singular of dimension 1,

$$1 = \dim T_p C = \dim(m_p/m_p^2)^*.$$

Also, $\mathcal{O}_{C,p}/m_p \overset{\cong}{\to} \mathbb{K}$, $f + m_p \mapsto f(p)$. Thus $m_p/m_p^2$ is a 1-dimensional vector space over $\mathcal{O}_{C,p}/m_p$, hence by the previous Corollorary to Nakayama's lemma, $m_p$ is generated by the lift of a 1 element basis of $m_p/m_p^2$. Thus $m_p$ is principal (we need $m_p$ finitely generated here!). $\square$

**Remark.** Let $t \in m_p$ be a generator. We get a chain of ideals

$$\cdots \subseteq (t^3) \subseteq (t^2) \subseteq (t) = m_p \subset \mathcal{O}_{C,p}.$$

Notice if $(t^{k+1}) = (t^k)$, then $m_p \cdot (t^k) = (t^k)$. But then Nakayama's lemma tells us that $(t^k) = 0$. But $t^k \neq 0$ since $\mathcal{O}_{C,p}$ is an integral domain.

Also, consider $I = \bigcap_{k=1}^{\infty} (t^k)$. Clearly $t \cdot I = I$, so $m_p \cdot I = I$, so $I = 0$.

**Consequence:** If $f \in \mathcal{O}_{C,p} \setminus \{0\}$, then there exists a unique $\nu \geq 0$ such that $f \in (t^\nu)$ but $f \notin (t^{\nu+1})$. Define $\nu : \mathcal{O}_{C,p} \setminus \{0\} \to \mathbb{Z}$ by $\nu(f) = \nu$ as above.

**Remark.**

- $\nu(f \cdot g) = \nu(f) + \nu(g)$.
- $\nu(f + g) \geq \in \{\nu(f), \nu(g)\}$ with equality if $\nu(f) \neq \nu(g)$.

Can extend $\nu$ to a map

$$\nu : K(C) \setminus \{0\} =: K(C)^\times \to \mathbb{Z}$$

by

$$\nu\left(\frac{f}{g}\right) = \nu(f) - \nu(g).$$

$\nu$ is an example of a *discrete valuation*.

**Definition** (Discrete valuation)**.** Let $K$ be a field. A *discrete valuation* on $K$ is a function $\nu : K^\times \to \mathbb{Z}$ such that

(1) $\nu(f \cdot g) = \nu(f) + \nu(g)$.

(2) $\nu(f + g) \geq \min\{\nu(f), \nu(g)\}$ with equality if $\nu(f) \neq \nu(g)$.

**Definition** (Discrete valuation ring)**.** Given a discrete valuation, we define the corresponding *discrete valuation ring* (DVR) by

$$R = \{f \in K^\times \mid \nu(f) \geq 0\} \cup \{0\}$$

which is a subring of $K$. We also define

$$m = \{f \in K^\times \mid \nu(f) \geq 1\} \cup \{0\}.$$

Note $m$ is the unique maximal ideal of $R$: if $f \in R \backslash m$, then $\nu(f) = 0$, so $\nu(f^{-1}) = 0$, so $f^{-1} \in R$.

**Example.**

(1) $R = \mathcal{O}_{C,p} \subseteq K = K(C)$. $\nu$ the discrete valuation we defined.

(2) Let $p \in \mathbb{Z}$ be prime, $K = \mathbb{Q}$. Any rational number can be written as $\frac{a}{b}p^\nu$ with $(a,p) = 1$, $(b,p) = 1$. Then define

$$\nu_p\left(\frac{a}{b}p^\nu\right) = \nu.$$

This is a discrete valuation, with discrete valuation ring

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\right\}.$$

(3) $K = \mathbb{K}(x)$, $a \in \mathbb{K}$. Define

$$\nu\left((x-a)^\nu \frac{f}{g}\right) = \nu$$

where $f, g$ are relatively prime to $x - a$. Here the discrete valuation ring is $\mathcal{O}_{\mathbb{A}^1,a}$.

(4) Let $K = \mathbb{K}(x)$,

$$\nu\left(\frac{f}{g}\right) = \deg g - \deg f.$$

This is the "order of 0 at $\infty$".

**Setup:** $C \subseteq \mathbb{P}^n$ a projective non-singular curve. Each point $p \in C$ gives a discrete valuation $\nu_p : K(C)^\times \to \mathbb{Z}$ with discrete valuation ring $\mathcal{O}_{C,p}$. For $f \in K(C)^\times$, we define the divisor of zeroes and poles of $f$ to be

$$(f) := \sum_{p \in C} \nu_p(f) p$$

Next time: need to check that this is a finite sum!

Start of lecture 18

Let $C$ be a projective non-singular curve.

**Definition** (Divisor of zeroes and poles)**.** For $f \in K(C) \setminus \{0\}$, the *divisor of zeroes and poles* of $f$ is

$$(f) = \sum_{p \in C} \nu_p(f) \cdot p.$$

**Remark.** Note $f$ is represented on some open subset $U \subseteq C$ by $\frac{g}{h}$, $g, h$ homogeneous polynomials. We shrink $U$ by removing $Z(g), Z(h)$. Now, if $p \in U$, $f = \frac{g}{h} \in \mathcal{O}_{C,p}$ is a regular function with $f(p) \neq 0$, so $\nu_p(f) = 0$. Thus the sum defining $(f)$ is a sum over points of $C \setminus U$, which is a finite set.

(Here we use $\dim C = 1$, so that irreducible sets are $C$ and singleton sets).

**Definition** (Group of principal divisors)**.** The group of *principal divisors* on $C$ is

$$\operatorname{Prin} C = \{(f) \mid f \in K(C) \setminus \{0\}\}.$$

This is a subgroup since:

- $(f \cdot g) = (f) + (g)$
- $(f^{-1}) = -(f)$.

**Definition** (Divisor class group)**.** The *(divisor) class group* is

$$\operatorname{Cl} C := \frac{\operatorname{Div} C}{\operatorname{Prin} C}.$$

**Definition** (Linearly equivalent)**.** If $D, D' \in \operatorname{Div} C$ satisfy $D - D' = (f)$ for some $f \in K(C)^\times$, then we say $D$ is *linearly equivalent* to $D'$, and write

$$D \sim D'.$$

**Digression:** Extending morphisms to projective space. $C$ a projective non-singular curve, $\emptyset \neq U \subseteq C$ an open subset. $f_0, \ldots, f_n$ regular functions on $U$ without a common zero.

Then we obtian a morphism

$$\begin{aligned} f : U &\to \mathbb{P}^n \\ p &\mapsto (f_0(p) : \cdots : f_n(p)) \end{aligned}$$

**Theorem.** $f : U \to \mathbb{P}^n$ extends to a morphism $f : C \to \mathbb{P}^n$.

*Proof.* Suppose either $f_i$ has a pole at $p \in C$ (i.e. $\nu_p(f_i) < 0$) or all $f_i$ are zero at $p$. Let

$$m = \min\{\nu_p(f_i) \mid 0 \leq i \leq n\}.$$

Let $t$ be a local parameter at $p$, i.e. a generator of $m_p \subseteq \mathcal{O}_{C,p}$. So $\nu_p(t) = 1$. Then $\nu_p(t^{-m} f_i) = \nu_p(f_i) - m$. Thus $\nu_p(t^{-m} f_i) = 0$ for some $i$ and $\nu_p(t^{-m} f_j) \geq 0$. Thus $t^{-m} f_0, \ldots, t^{-m} f_n \in \mathcal{O}_{C,p}$, and these functions don't simultaneously vanish at $p$. Hence in some neighbourhood $V$ of $p$, we obtain a morphism $f_p : V \to \mathbb{P}^n$ given by $q \mapsto ((t^{-m} f_0)(p) : \cdots : (t^{-m} f_n)(p))$. This agrees with $f$ on $U \cap V$ by rescaling. □

**Proposition.** Let $f : X \to Y$ be a non-constant morphism between projective non-singular curves. Then

(1) $f^{-1}(q)$ is a finite set for all $q \in Y$

(2) $f$ induces an inclusion $K(Y) \hookrightarrow K(X)$ such that $[K(X) : K(Y)]$ is finite. We call $[K(X) : K(Y)]$ the *degree* of $f$.

*Proof.*

(1) $f^{-1}(q) \subseteq X$ is closed, and since $\dim X = 1$, either $f^{-1}(q)$ is finite, or $f^{-1}(q) = X$. The latter contradicts $f$ being non-constant.

(2) If $\varphi \in K(Y)$, then $\varphi$ defines a regular function on some open $U \subseteq Y$. $\varphi : U \to \mathbb{K}$. $\varphi \circ f$ makes sense provided $f(X) \nsubseteq Y \setminus U$. But $f(X)$ is irreducible (point set topology exercise), so $f$ is constant if $f(X) \subseteq Y \setminus U$. Thus $\varphi \circ f$ makes sense as a rational function on $X$. Thus $K(Y) \to K(X)$ exists and is automatically an injection since both are fields. Omit proof of finiteness. □

**Definition** (Degree of ramification)**.** Suppose $f : X \to Y$ is a non-constant morphism between projective non-singular curves. Let $p \in Y$, $m_p = (t) \subseteq \mathcal{O}_{Y,p}$, $t$ a local parameter. Let $q \in f^{-1}(p)$. Then $t \circ f \in \mathcal{O}_{X,q}$. Define

$$e_q := \nu_q(t \circ f),$$

the *degree of ramification* of $f$ at $q$.

**Theorem.** Let $f : X \to Y$ a non-constant morphism between projective non-singular curves. Then for $p \in Y$,

$$\sum_{q \in f^{-1}(p)} e_q = \deg f$$

is the degree of $f$.

*Proof.* Omitted, but the theorem statement is crucial. □

**Example.**

(1) $\operatorname{char} \mathbb{K} \neq 2$, $f : \mathbb{P}^1 \to \mathbb{P}^1$, $(u, v) \mapsto (u^2 : v^2)$. Setting $v = 1$, this gives a morphism $\mathbb{A}^1 \to \mathbb{A}^1$ given by $u \mapsto u^2$. If $p \in \mathbb{A}^1$, $t = u - p$ is a local parameter at $p$. $t \circ f = u^2 - p = (u - q)(u + q)$ where $q^2 = p$. Then $e_q = e_{-q} = 1$. We have $\deg f = e_q + e_{-q} = 2$.

(2) If $p = 0$, $f^{-1}(p) = \{0\}$, $e_0 = \nu_0(u^2) = 2$. Function fields, $K(\mathbb{P}^1) = \mathbb{K}(u)$, $\mathbb{K}(u) \to \mathbb{K}(y)$, $u \mapsto u^2$ degree 2.

(3) $\operatorname{char} \mathbb{K} = p$, $f : \mathbb{P}^1 \to \mathbb{P}^1$, $(u : v) \mapsto (u^p : v^p)$. Set $v = 1$, $u \mapsto u^p$. $f^{-1}(q) = \{r\}$ with $r^p = q$, $q \in \mathbb{A}^1$. Then $t = u - q$. $t \circ f = u^p - q = (u - r)^p$.

**Application:** Let $X$ be a projective non-singular curve, $f \in K(X)^\times$. This gives a morphism $U \to \mathbb{P}^1$ where $U$ is the open set in which $f$ is singular. This extends to $f : C \to \mathbb{P}^1$, non-constant as long as $f \notin \mathbb{K}$.

Start of lecture 19

Let $C$ be a projective non-singular curve, and $f \in K(C)^\times$. $f : C \to \mathbb{P}^1$, $p \mapsto (f(p) : 1)$, or writing $f = \frac{g}{h}$, $g, h$ homogeneous polynomials of the same degree, then $f : C \to \mathbb{P}^1$, $p \mapsto (g(p) : h(p))$.

Then

$$(f) = \sum_{p \in f^{-1}((0:1))} e_p p - \sum_{q \in f^{-1}((1:0))} e_q q.$$

Thus, if we define

$$\deg \sum_{p \in C} a_p p = \sum_{p \in C} a_p,$$

then $\deg(f) = \deg f - \deg f = 0$. Thus every principal divisor is degree 0.

Thus the homomorphism $\deg : \operatorname{Div} C \to \mathbb{Z}$ descends to $\deg : \operatorname{Cl} C \to \mathbb{Z}$, and this is surjective as $\deg p = 1$.

### Linear systems

**Definition** (Effective divisor)**.** Let $D \in \operatorname{Div} C$, $D = \sum_i n_i p_i$. We say $D$ is *effective* if $n_i \geq 0$ for all $i$. Define

$$\mathcal{L}(D) = \{f \in K(C)^\times \mid D + (f) \text{ is effective}\} \cup \{0\}.$$

**Lemma.** $\mathcal{L}(D)$ is a vector space.

*Proof.* $f \in \mathcal{L}(D)$ implies $cf \in \mathcal{L}(D)$ for $c \in \mathbb{K}$, $c \neq 0$, since $(f) = (cf) = (c) + (f)$. If $f, g \in \mathcal{L}(D)$, $f, g$ non-zero, $f + g \neq 0$, then

$$(f + g) = \sum_p \nu_p(f + g)p$$

and $\nu_p(f + g) \geq \min\{\nu_p(f), \nu_p(g)\}$. Thus if $D + (f)$, $D + (g)$ are effective, then so is $D + (f + g)$. □

**Theorem.** $\mathcal{L}(D)$ is a finite dimensional vector space and $\mathcal{L}(0) = \mathbb{K}$. Furthermore, $\dim_{\mathbb{K}} \mathcal{L}(D) \leq \deg D + 1$.

*Proof.* Induction on $\deg D$. If $\deg D < 0$, then there are no effective divisors linearly equivalent to $D$, so $\mathcal{L}(D) = 0$. Suppose $\deg D \geq 0$, write $D = \sum_i n_i p_i$ and pick $p \in C \setminus \{p_1, \ldots, p_n\}$. Consider the map

$$\lambda : \mathcal{L}(D) \to \mathbb{K}, \qquad f \mapsto f(p).$$

which makes sense since $\nu_p(f) \geq 0$ for $f \in \mathcal{L}(D)$, since otherwise the coefficient of $p$ in $D+(f)$ is negative. If $f \in \ker \lambda$, then $f \in m_p \subseteq \mathcal{O}_{C,p}$, so $\nu_p(f) \geq 1$. Thus $f \in \mathcal{L}(D-P)$. Note also $\mathcal{L}(D-D) \subseteq \mathcal{L}(D)$, since if $D - P + (f)$ is effective then so is $D - (f)$. Thus $\mathcal{L}(D-P) = \ker \lambda$, and $\frac{\mathcal{L}(D)}{\mathcal{L}(D-P)} \subseteq \mathbb{K}$. Thus $\dim_{\mathbb{K}} \mathcal{L}(D) \leq \dim \mathcal{L}(D-P) + 1$. Thus by induction, $\dim_{\mathbb{K}} \mathcal{L}(D) \leq \deg D + 1$.

Thus $\dim \mathcal{L}(0) \leq 1$, but $\mathbb{K} \subseteq \mathcal{L}(D)$ since $0 + (c) = 0$. So $\dim \mathcal{L}(0) = 1$. □

**Remark.** $\mathcal{L}(0) = \{f : C \to \mathbb{K} \text{ regular}\}$, and hence regular functions on $C$ are constant.

**Definition** (Complete linear system)**.** Given a divisor $D$, we define the *complete linear system associated* to $D$ to be

$$\begin{aligned} |D| &= \{D' \in \operatorname{Div} C \mid D' \text{ effective}, D' \sim D\} \\ &= \frac{\mathcal{L}(D) \setminus \{0\}}{\sim} \qquad\qquad (f \sim \lambda f) \\ &= \mathbb{P}(\mathcal{L}(D)) \end{aligned}$$

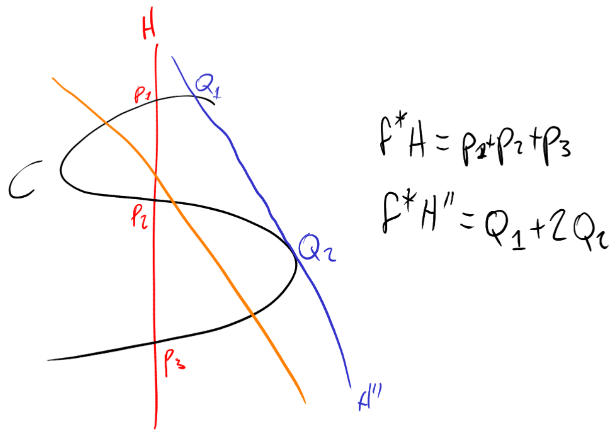
a projective space.

### Morphisms to projective space

Let $D$ be a divisor, $f_0, \dots, f_n \in \mathcal{L}(D)$ with not all $f_i$ being 0. This gives a morphism $f : C \to \mathbb{P}^n$, $p \mapsto (f_0(p) : \cdots : f_n(p))$.

**Definition** ($f^*H$)**.** Let $f : C \to \mathbb{P}^n$ be a morphism. Let $H \subseteq \mathbb{P}^n$ be a hyperplane with $f(C) \nsubseteq H$. We define $f^*H \in \operatorname{Div} X$ as follows. Let $H = Z(\varphi)$ with $\varphi$ a linear homogeneous polynomial and choose $\psi$ linear homogeneous so that $H' = Z(\psi)$ satisfies $f^{-1}(H) \cap f^{-1}(H') = \emptyset$. Define

$$f^*H = \sum_{p \in f^{-1}(H)} \nu_p \left( \frac{\varphi}{\psi} \circ f \right) p$$




**Remark.** This is independent of the choice of $\psi$. For example

$$\frac{\varphi}{\psi'} = \frac{\varphi}{\psi}\frac{\psi}{\psi'}.$$

**Relations to morphisms**

Let $f_0, \dots, f_n \in \mathcal{L}(D)$ to have the properties:

(1) The $f_i$ aren't all 0.

(2) $\forall p \in C$, $\exists a_0, \dots, a_n \in \mathbb{K}$ such that the coefficient of $p$ in $D + (\sum_i a_i f_i)$ is 0.

As above, we get a morphism $f : C \to \mathbb{P}^n$. Let $H \subseteq \mathbb{P}^n$ be given by an equation $\sum_i a_i x_i = 0$.

Start of lecture 20

**Theorem.** $f^*H = D + (\sum_i a_i f_i)$.

*Proof.* Let $p \in f^{-1}(H)$. Suppose the coefficient of $p$ in $D$ is 0. Let $\varphi = \sum_i a_i x_i$. Let $b_0, \dots, b_n$ be such that $p \notin Z(\sum_i b_i x_i)$. Let $\psi = \sum_i b_i x_i$. Then the coefficient of $p$ in $f^*H$ is

$$\nu_p\left(\frac{\varphi}{\psi} \circ f\right)$$

Necessarily, $f_0, \dots, f_n$ do not have a pole at $p$, since otherwise $D + (f_i)$ has a negative coefficient for $p$. Thus, $f_0, \dots, f_n$ are regular on a neighbourhood of $p$, so we can write

$f = (f_0 : \ldots : f_n)$ in this neighbourhood. Now

$$\nu_p\left(\frac{\varphi}{\psi} \circ f\right) = \nu_p\left(\frac{\sum_i a_i f_i}{\sum_i b_i f_i}\right) = \nu_p\left(\sum_i a_i f_i\right)$$

since $\sum_i b_i f_i$ is non-vanishing and regular at $p$. But $\nu_p\left(\sum_i a_i f_i\right)$ is the coefficient of $p$ in $D + \left(\sum_i a_i f_i\right)$. If $p$ appears in $D$ with coefficient $m<$ then

$$\nu_p\left(\sum_i b_i f_i\right) \geq -m$$

for any $b_0, \ldots, b_n \in \mathbb{K}$. There is also some choice of $b_0, \ldots, b_n$ with $\nu_p\left(\sum_i b_i f_i\right) = -m$ by assumption (2). In a neighbourhood of $p$, the morphism $f$ is given by

$$f = (t^m f_0 : \cdots : t^m f_n)$$

where $t$ is a local parameter at $p$. The coefficient of $p$ in $f^*H$ is

$$\nu_p\left(\underbrace{\frac{\sum_i a_i t^m f_i}{\sum_i b_i t^m f_i}}_{\nu_p = 0}\right) = \nu_p\left(\sum_i a_i t^m f_i\right) = m + \nu_p\left(\sum_i a_i f_i\right),$$

which is the coefficient of $p$ in $D + \left(\sum_i a_i f_i\right)$. Thus $f^*H = D + \left(\sum_i a_i f_i\right)$. □

Picture so far: $f_0, \ldots, f_n$ span a subspace $V \subseteq \mathcal{L}(D)$. This gives a linear subspace

$$\mathcal{D} = \frac{V \setminus \{0\}}{\mathbb{K}^1} = \mathbb{P}(V) \subseteq |D| = \mathbb{P}(\mathcal{L}(D)).$$

We call $\mathcal{D}$ the *linear system*.

**Definition** (Support of a divisor)**.** For a divisor $D = \sum_{i=1}^n a_i p_i$ with $a_i \neq 0$, we define the *support* of $D$ to be $\operatorname{Supp}(D) = \{p_1, \ldots, p_n\}$.

**Definition** (Base-point free)**.** We say $\mathcal{D} = \mathbb{P}(V)$ is *base-point free* if $\forall p \in C$, $\exists D' \in \mathcal{D}$ (where we identify $[f] \in D$ with $D + (f)$) with $p \notin \operatorname{Supp} D'$.

(This is assumption (2): $\forall p \in C$, there exists $b_0, \ldots, b_n$ such that $p \notin \operatorname{Supp}(D + (\sum_i b_i f_i)))$.

In this case, the theorem applies, and we obtain $f : C \to \mathbb{P}^n$ with the property that

$$\mathcal{D} = \{f^*H \mid H \subseteq \mathbb{P}^n \text{ hyperplane}\}.$$

**Converse:** Suppose $f : L \to \mathbb{P}^n$ is a morphism. Set $D = f^*Z(x_0)$. (Assume $f(C) \subseteq Z(x_0)$). Let $f_i \in K(C)$ be given by

$$r_i = \frac{x_1}{x_0} \circ f,$$

a rational function on $C$ which is regular on $C \setminus f^{-1}(Z(x_0))$. Then $f = (f_0 : f_1 : \cdots : f_n)$ on $C \setminus f^{-1}(Z(x_0))$ and hence $f$ is induced by the linear system $\mathcal{D} \subseteq |D|$, $\mathcal{D} = \mathbb{P}(V)$ with $V$ spanned by $f_0, \ldots, f_n \in \mathcal{L}(D)$.

By the previous theorem, $f^*Z(\sum_i a_i x_i) = D + (\sum_i a_i f_i) \in \mathcal{D}$. Note $\mathcal{D}$ is base-point free, since given $p \in C$, can find a hyperplane $H \subseteq \mathbb{P}^n$ with $f(p) \notin H$, so $p \notin \operatorname{Supp} f^*H$, while $f^*H \in \mathcal{D}$.

**Remark.** If $f : C \hookrightarrow \mathbb{P}^n$ is an embedding, then $f^*H$ can be viewed as "$H \cap C$ iwth multiplicaion", and

$$D = \{H \cap C \mid H \subseteq \mathbb{P}^n \text{ hyperplane}\}.$$

**Remark.** Can also pull-back hypersurfaces $H \subseteq \mathbb{P}^n$, with $H = Z(\varphi)$, $\varphi$ a homogeneous polynomial of degree $d$, as follows. For $p \in f^{-1}(H)$, choose a homogeneous polynomial $\psi$ which doesn't vanish at $f(p)$ and take the coefficient of $p$ in $f^*H$ to be

$$\nu_p\left(\frac{\varphi}{\psi} \circ f\right).$$

**Definition** (Degree of a curve morphism)**.** Let $f : C \to \mathbb{P}^n$ be a morphism, $L \subseteq \mathbb{P}^n$ a hyperplane, $f(C) \not\subseteq L$. The *degree of* $f$ is the degree of the divisor $f^*L$. This is well-defined since $f^*L$, $f^*L'$ are linearly equivalent and linearly equivalent divisors have the same defgree.

**Example.** Let $f : C \hookrightarrow \mathbb{P}^2$ identify $C$ with $Z(\varphi)$ where $\varphi$ has degree $d$. In this case, the degree of $f$ is $d$. (Check this: need to compare coefficients in $f^*L$ with the multiplicativity of zeroes of $\varphi|_L$).

**Theorem.** Let $f : C \to \mathbb{P}^n$ be a morphism. $H \subseteq \mathbb{P}^n$ a hypersurface with $f(C) \not\subseteq H$. $H = Z(\varphi)$. $\deg \varphi = e$. Then $\deg f^*H = (\deg f) \cdot e$.

*Proof.* Choose some $x_i$ such that $f(C) \not\subseteq Z(x_i)$. Then $\frac{\varphi}{x_i^e}$ is a rational function in $\mathbb{P}^n$ and $\frac{\varphi}{x_i^e} \circ f$ is a rational function on $C$. Assume $H \cap L \cap f(C) = \emptyset$. Then

$$\begin{aligned}\left(\frac{\varphi}{x_i^e} \circ f\right) &= \sum_{p \in f^{-1}(H)} \nu_p \left(\frac{\varphi}{x_i^e} \circ f\right) p - \sum_{p \in f^{-1}(L)} \left(\frac{x_i^e}{\varphi} \circ f\right) \\ &= f^*H - ef^*L\end{aligned}$$

Since the degree of a principal divisor is 0, we get $\deg f^*H = e \cdot \deg f^*L$. □

Start of lecture 21

**Remark.** This is known as Bézout's Theorem. This is usually expressed as follows:

Let $C, C' \subseteq \mathbb{P}^2$ be curves of degrees $d$ and $e$ respectively. Then the number of points in $C \cap C'$ (assuming $C \neq C'$) "counted with multiplicities" is $d \cdot e$.

For example, if $C$ is non-singular, $f : C \hookrightarrow \mathbb{P}^2$ an embedding, then $d = \deg f$ and $\deg f^*C' = d \cdot e$. So if $p \in C \cap C'$, its multiplicity is the coefficient of $p$ in $f^*C'$. If $C$ is singular, need a more subtle definition of multiplicity.

In general, given a divisor $D$ on a projective non-singular curve $C$, we would like to understand when $|D|$ induces an embedding $C$ in projective space.

In other words, suppose $|D|$ is base-point free, i.e. $\forall p \in C$, there exists $D' \in |D|$ with $p \notin \operatorname{Supp} D'$. Then by choosing $f_0, \dots, f_n \in \mathcal{L}(D)$ spanning $\mathcal{L}(D)$, we obtain a morphism $f = (f_: \cdots : f_n) : C \to \mathbb{P}^n$. When is this an embedding? We can alsu use a sub-linear system $\mathcal{D} = \mathbb{P}(V) \subseteq |D| = \mathbb{P}(\mathcal{L}(D))$ and choose $f_0, \dots, f_n \in V$ a spanning set.

**Theorem.** Suppose a linear system $\mathcal{D} \subseteq |D|$ is base-point free. Then the induced morphism $f : C \to \mathbb{P}^n$ is an embedding if and only if

(1) $\mathcal{D}$ separates points: i.e. $\forall P, Q \in C$ distinct, there exists a $D' \in \mathcal{D}$ such that $P \in \operatorname{Supp} D'$ and $Q \notin \operatorname{Supp} D'$. (This is equivalent to injectivity of $f$).

(2) $\mathcal{D}$ separates vectors: i.e. $\forall P \in C$, $\exists D' \in \mathcal{D}$ such that the coefficient of $P$ in $D'$ is 1.


**Definition** (Very ample divisor)**.** We say a divisor $D$ is *very ample* if $|D|$ induces an embedding into some projective space.

**Theorem.** $D$ is very ample if $\forall P, Q \in C$, not necessarily distinct, we have

$$\dim |D - P - Q| = \dim |D| - 2.$$

*Proof.* Recall $\dim |D| = \dim \mathcal{L}(D) - 1$. For any $P \in C$, we have a map $\mathcal{L}(D) \to \mathbb{K}$. This is constructed as follows. Suppose the coefficient of $P$ in $D$ is $n$. Then if $f \in \mathcal{L}(D)$, then $\nu_p(t^n \cdot f) = n + \nu_p(f) \geq 0$, where $t$ is a local parameter at $p$. So $t^n \cdot f \in \mathcal{O}_{C,p}$. Thus we define

$$\begin{aligned} ev_p : \mathcal{L}(D) &\to \mathbb{K} \\ f &\mapsto (t^n \cdot f)(p) \end{aligned}$$

If $f \in \ker(ev_p)$, we have $\nu_p(t^n \cdot f) \geq 1$, so $\nu_p(f) > -n$. Hence the coefficient of $p$ in $D = (f)$ is at least 1. Thus $(D - p) + (f)$ is effective, so $f \in \mathcal{L}(D - P)$. Conversely, if $f \in \mathcal{L}(D - P)$, $(D - P) + (f)$ is effective, so $\nu_p(f) \geq -n + 1$, so $\nu_p(t^n \cdot f) \geq 1$, so $f \in \ker(ev_p)$. Thus $\mathcal{L}(D - P) = \ker ev_p$. If $|D|$ is base-point free, then $ev_p : \mathcal{L}(D) \to \mathbb{K}$ is surjective $\forall p$ and conversely. So

$$\dim |D - P| = \dim \mathcal{L}(D - P) - 1 = \dim \mathcal{L}(D) - 2 = \dim |D| - 1$$

for all $p$ if and only if $|D|$ is base-point free. Now $|D|$ separates points and tangent vectors if and only if $|D - P|$ is base-point free $\forall p \in C$. Indeed, if $D' \in |D - P|$ does not have $Q$ in its support, then $D' + P$ separatest $P$ and $Q$ if $Q \neq P$. If $P = Q$, and $P \notin \operatorname{Supp} D'$, then $D' + P$ has coefficient 1 for $P$. Now

$$\dim |D - P - Q| = \dim |D - P| = 1$$

if and only if $|D - P|$ is base-point free so $|D|$ is very ample and base-point free if and only if

$$\dim |D - P - Q| = \dim |D - P| - 1 = \dim |D| - 2 \qquad \forall P, Q. \qquad \square$$

**Moral.** If we can control $\dim \mathcal{L}(D)$, then we know a lot about embeddings.

## 6 Differentials and the Riemann-Roch Theorem

**Definition** ($\Omega_{B/A}$)**.** Let $B$ be a ring and $A \subseteq B$ a subring. We define

$$\Omega_{B/A} = \frac{\text{free } B\text{-module generated by symbols } \mathrm{d}b \text{ for } b \in B}{\text{submodule } R \text{ of relations}}$$

where $R$ is the submodule with generators:

$$\begin{aligned} &\mathrm{d}(bb') - b\mathrm{d}b' - b'\mathrm{d}b && \forall b, b' \in B \\ &\mathrm{d}(b + b') - \mathrm{d}b - \mathrm{d}b' && \forall b, b' \in B \\ &\mathrm{d}a && \forall a \in A \end{aligned}$$

Start of lecture 22

**Example.** $\Omega_{\mathbb{K}[x]/\mathbb{K}}$ For $f \in \mathbb{K}[x]$, $\mathrm{d}f = f'(x)\mathrm{d}x$. Thus $\Omega_{\mathbb{K}[x]/\mathbb{K}}$ is the free $\mathbb{K}[x]$-module with one generator $\mathrm{d}x$.

Similarly $\Omega_{\mathbb{K}(x)/\mathbb{K}}$, $f \in \mathbb{K}(x)$, $\mathrm{d}f = f'(x)\mathrm{d}x$. Thus $\Omega_{\mathbb{K}(x)/\mathbb{K}}$ is the 1-dimensional vector space over $\mathbb{K}(x)$ with basis $\mathrm{d}x$.

**Proposition.** If $L/K$ is a separable algebraic field extension, then $\Omega_{L/K} = 0$.

A field extension $L/K$ is separable algebraic if everything in $L$ is a solution to some irreducible polynomial equation $f(x) = 0$ with $f(\alpha) \in K[X]$, and $f'(\alpha) \neq 0$, i.e. $\alpha$ is not a multiple root.

*Proof.* Given $\alpha \in L$, $f(x) \in K[x]$ with $f(\alpha) = 0$, $f'(\alpha) \neq 0$, then $0 = f(\alpha)$ implies $0 = \mathrm{d}(f(\alpha)) = f'(\alpha)\mathrm{d}\alpha$, so $\mathrm{d}\alpha = 0$ since $f'(\alpha) \neq 0$. □

**Lemma.** Let $C$ be a curve, $p \in C$, and $t$ a local parameter for $C$ at $p$. Then

$$\Omega_{K(C)/\mathbb{K}} = K(C)\mathrm{d}t.$$

*Proof.* $t$ local parameter implies $t$ is not a constant function, and hence defines a non-constant map $t : C \to \mathbb{P}^1$, inducing a finite field extension $K(\mathbb{P}^1) = \mathbb{K}(t) \to K(C)$. This extension is separable (proof omitted, not required if $\operatorname{char} \mathbb{K} = 0$. The idea is that if the extension is not separable, then $\operatorname{char} \mathbb{K} \mid e_Q$ for all $Q \in C$. However, since $t$ is a local parameter at $p$, $e_p = 1$). If $\alpha \in K(C)$, then there exists $f \in \mathbb{K}(t)[x]$ such that $f(\alpha) = 0$, $f'(\alpha) = 0$. Write

$$f(x) = \sum_{i \geq 0} f_i(t) x^i$$

for some $f_(t) \in \mathbb{K}(t)$. Then

$$\begin{aligned} 0 = \mathrm{d}(f(\alpha)) &= \mathrm{d}\left(\sum_{i\geq 0} f_i(t)\alpha^i\right) \\ &= \left(\sum_{i \geq 0} f_i'(t)\alpha^i\right)\mathrm{d}f + \underbrace{\left(\sum_{i\geq} i f_i(t)\alpha^{i-1}\right)}_{=f'(\alpha)\neq 0}\mathrm{d}\alpha \end{aligned}$$

Thus we can solve for $\mathrm{d}\alpha$, getting $\mathrm{d}\alpha = g\mathrm{d}t \in K(C)\mathrm{d}t$. □

**Definition** $(\nu_p(\omega))$**.** Let $C$ be a projective non-singular curve, $\omega \in \Omega_{K(C)/\mathbb{K}}$, $p \in C$. We define $\nu_p(\omega)$ as follows. Let $t \in \mathcal{O}_{C,p}$ a local parameter and write $w = f\mathrm{d}t$ for $f \in K(C)$. Define

$$\nu_p(\omega) = \nu_p(f).$$

We define $\mathrm{div}(\omega) = \sum_{p\in C} \nu_p(\omega)p \in \mathrm{Div}\, C$. We say $\omega$ is regular at $p$ if $\nu_p(\omega) \geq 0$.

**Lemma.**

(1) $f \in \mathcal{O}_{C,p} \implies \nu_p(\mathrm{d}f) \geq 0$.

(2) If $t'$ is another local parameter at $p$, then $\nu_p(\mathrm{d}t') = 0$ and $\nu_p(f\mathrm{d}t') = \nu_p(f) + \nu_p(\mathrm{d}t')$ is independent of $t$.

(3) If $f \in K(C)$ and $\nu_p(f) \neq 0$ in $\mathbb{K}$ (i.e., $\mathrm{char}\,\mathbb{K} \mid \nu_p(f)$) then $\nu_p(\mathrm{d}f) = \nu_p(f) - 1$.

*Proof.*

(1) Let $p \in C \subseteq \mathbb{P}^n$, $p \in C \cap U_i$, where $U_i = \mathbb{P}^n \setminus Z(x_i)$. Work on $U_i \cap C$, where rational functions are just ratios of polynomials. If $f = g/h$, $h(p) \neq 0$, we have

$$\mathrm{d}f = \frac{h\mathrm{d}g - g\mathrm{d}h}{h^2} = \sum_i \gamma_i \mathrm{d}x_i$$

with $\gamma_i \in \mathcal{O}_{C,p}$. So

$$\nu_p(\mathrm{d}f) \geq \min\{\nu_p(\gamma_i\mathrm{d}x_i) 1 \leq i \leq n\} \geq \min\{\nu_p(\mathrm{d}x_i) \mid 1 \leq i \leq n\}.$$

Thus $\nu_p(\mathrm{d}f)$ is bounded below independently of $f$. Choose $f \in \mathcal{O}_{C,p}$ such that $\nu_p(\mathrm{d}f)$ is minimal, $t$ a local parameter at $p \in C$. Then $\nu_p(f - f(p)) \geq 1$, so can write $f - f(p) = tf_1$, for some $f_1 \in \mathcal{O}_{C,p}$. So

$$\begin{aligned} \mathrm{d}f &= \mathrm{d}(f - f(p)) \\ &= \mathrm{d}(ft_1) \\ &= f_1 \mathrm{d}t + t\mathrm{d}f_1 \end{aligned} \tag{$*$}$$

If $\nu_p(\mathrm{d}f) < 0$, note $\nu_p(f_1\mathrm{d}t) \geq 0$, and hence $(*)$ implies

$$\nu_p(\mathrm{d}f) = \nu_p(t\mathrm{d}f_i) = \nu_p(t) + \nu_p(\mathrm{d}f_1) = 1 + \nu_p(\mathrm{d}f_1).$$

So $\nu_p(\mathrm{d}f_1) < \nu_p(\mathrm{d}f)$. This contradicts the minimality of $\nu_p(\mathrm{d}f)$. Thus $\nu_p(\mathrm{d}f) \geq 0$.

(2) We may write $t' = u \cdot t$ for $u$ a unit, $u \in \mathcal{O}_{C,p}^\times$ (the group of units). Then $\mathrm{d}t' = u\mathrm{d}t + t\mathrm{d}u$. $\mathrm{d}u = g \cdot \mathrm{d}t$ for some $g$ with $\nu_p(g) \geq 0$ by (1). So

$$\mathrm{d}t' = \underbrace{(u + tg)}_{\nu_p = 0} \mathrm{d}t,$$

so $\nu_p(\mathrm{d}t') = 0$ by definition. If $f\mathrm{d}t = h\mathrm{d}t' = h(u + tg)\mathrm{d}t$, then

$$\nu_p(h(u + tg)) = \nu_p(h) + \nu_p(u + tg) = \nu_p(h).$$

Hence $\nu_p$ is independent of choice of $t$.

(3) Suppose $f = t^n u$ where $n = \nu_p(f)$, $u \in \mathcal{O}_{C,p}^\times$. Then $\mathrm{d}f = nt^{n-1}u\mathrm{d}t + t^n\mathrm{d}u$. If $\operatorname{char} \mathbb{K} \nmid n$, then

$$\nu_p(f) \geq \min\{\nu_p(nt^{n-1}u\mathrm{d}t), t^n\mathrm{d}u\} = \min\{n - 1, n\} = n - 1$$

and equality holds since $n \neq n - 1$. Thus $\nu_p(\mathrm{d}f) = \nu_p(f) - 1$. □

**Proposition.** If $\omega \in \Omega_{K(C)/\mathbb{K}}$, then $\nu_p(\omega) = 0$ for all but a finite number of $p$.

*Proof.* Omitted. □

Thus $\operatorname{div}(\omega) \in \operatorname{Div}(C)$.

Start of lecture 23

**Proposition.** Let $\omega, \omega' \in \Omega_{K(C)/\mathbb{K}}$. Then $\operatorname{div}(\omega)$ and $\operatorname{div}(\omega')$ are linearly equivalent.

*Proof.* For $t$ a local parameter at some point $p \in C$, $\omega = f\mathrm{d}t$, $\omega' = f'\mathrm{d}t$, then $\omega = \frac{f'}{f} \cdot \omega'$. Then

$$\mathrm{div}(\omega) = \mathrm{div}(\omega') + \left(\frac{f'}{f}\right). \qquad \square$$

**Definition** (Canonical class)**.** The *canonical class* of a projective non-singular curve $C$ is the linear equivalence class of $\mathrm{div}\,\omega$ in $\mathrm{Cl}\,C$, for any $0 \neq \omega \in \Omega_{K(C)/\mathbb{K}}$. We write the canonical class as $K_C$.

**Definition** (Genus)**.** The *genus* of $C$ is $\dim_{\mathbb{K}} \mathcal{L}(K_C)$.

If $\mathbb{K} = \mathbb{C}$ and we use the Euclidean topology rather than the Zariski topology, then this is the usual notion of genus!

**Example.** $C = \mathbb{P}^1$, $K(C) = \mathbb{K}(t)$, $t = x_0/x_1$. Note when $x_1 = 1$, $t = p_0$ is a local parameter for $C$ at $p_0 = (p_0 : 1) \in \mathbb{P}^1$. Thus $\mathrm{d}t = \mathrm{d}(t - p_0)$ and $\nu_{p_0}(\mathrm{d}(t - p_0)) = 0$. Thus $\nu_{p_0}(\mathrm{d}t) = 0$ for all $p_0 \in \mathbb{P}^1 \setminus Z(x_i)$. At $t = \infty$, look at $\mathbb{A}^1 = \mathbb{P}^1 \setminus Z(x_0)$, so $s = x_1/x_0$ is a local parameter at $q = (1 : 0)$. Note $t = s^{-1}$, so

$$\mathrm{d}t = \mathrm{d}(1/s) = -\frac{\mathrm{d}s}{s^2}$$

so $\nu_q(\mathrm{d}t) = -2$. So $K_C \sim -2q$ where $\sim$ means linearly equivalent. Thus $\mathcal{L}(K_C) = \mathcal{L}(-2q) = 0$. Thus

$$g(C) = \dim \mathcal{L}(K_C) = 0.$$

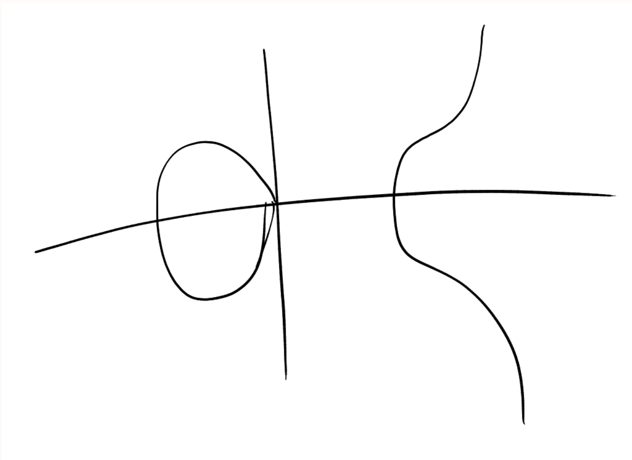
**Example.** Plane cubic

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

in $\mathbb{A}^2$ or

$$y^2 z = (x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z)$$

$\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$ distinct. $\omega = \frac{\mathrm{d}x}{y}$, $2y\mathrm{d}y = f'(x)\mathrm{d}x$.



so

$$\frac{2\mathrm{d}y}{f'(x)} = \frac{\mathrm{d}x}{y}.$$

In fact, $\mathrm{div}(\omega) = 0$. Hardest part: $q = (0 : 1 : 0)$. Thus $K_C \sim 0$, and $\mathcal{L}(K_C) = \mathcal{L}(0)$, so $g(C) = \dim \mathcal{L}(0) = 1$.

**Theorem** (Riemann-Roch Theorem)**.** Write $l(D) := \dim_{\mathbb{K}} \mathcal{L}(D)$ for $D \in \mathrm{Div}(C)$. Then

$$l(D) - l(K_C - D) = \deg D + 1 - g$$

where $g$ is the genus of $C$.

*Proof.* Omitted. This is far beyond the scope of this course; this theorem is not even proved in part III. □

Consequences:

(1) If $D = 0$ then $l(D) = 1$, so $1 - l(K_C) = 0 + 1 - g$ or $l(K_C) = g$, the definition of $g$.

(2) If $D = K_C$, then

$$\underbrace{l(K_C) - l(0)}_{=g-1} = \deg K_C + 1 - g$$

so $\boxed{\deg K_C = 2g - 2}$.

(3) If $\deg D > 2g - 2$, then $\deg K_C - D = 2g - 2 - \deg D, 0$. Thus $l(K_C - D) = 0$ and

$$\boxed{l(D) = \deg D + 1 - g}.$$

**Remark.** For $0 \le \deg D \le 2g - 2$, behaviour of $l(D)$ can be complicated and unpredictable.

(4) If $\deg D > 2g$, then $\forall P, Q \in C$,

$$l(D - P - Q) = l(D) - 2$$

by (3). Hence $|D|$ induces an embedding of $C$ in some $\mathbb{P}^n$.

**Example.** If $C$ has genus 0, then every positive degree divisor induces an embedding.

For example, if $P \in C$, $|P|$ is very ample, $l(P) = 2$, so we get an embedding of $C$ in $\mathbb{P}^1$. Thus $C \cong \mathbb{P}^1$.

**Example.** $g = 1$. If $\deg D = 3$, then $D$ is very ample, and $l(D) = 3+1-1 = 3$. So $|D|$ induces an embedding of $C$ in $\mathbb{P}^2$. Thus in particular $C$ is isomorphic to a curve of degree 3 in $\mathbb{P}^2$. Can show $C \cong Z(f)$ for some homogeneous polynomial of degree 3. More specifically, fix $P_0 \in C$, and embed using $|3P_0|$. Let $D \in \operatorname{Div} C$ be degree 0. Then

$$l(D + P_0) - l(K_C - D - P_0) = \deg(D + P_0) + 1 - g.$$

The second term of RHS is 0 since $\deg K_C - D - P_0 = -1$. Then since $\deg(D + P_0) = 1$ and $g = 1$, we get $l(D + P_0) = 1$. So there exists an effective divisor linearly equivalent to $D + P_0$, necessarily $D + P_0 \sim P$ for some $P \in C$. Thus $P - P_0 \sim D$. Note $P$ is unique: if $P - P_0 \sim P' - P_0$, then $P \sim P'$, so if $P \neq P'$, $\dim |P| \ge 1$, so $l(P) \ge 2$. But $l(P) = 1$ by Riemann-Roch Theorem.

Conclusion: every divisor class on $C$ of degree 0 can be represented uniquely by $P - P_0$ for some $P \in C$, i.e. $C \to \ker(\deg : \operatorname{Cl} C \to \mathbb{Z}))$, $p \mapsto p - p_0$ is a bijection. This gives a group structure on $C$, i.e. $P + Q = R$ for $P, Q, R \in C$ if

$$(P - P_0) + (Q - P_0) \sim R - P_0.$$

Geometric description: $P, Q \in C \overset{i}{\hookrightarrow} \mathbb{P}^2$. Let $L$ be the line joining $P$ and $Q$ (tangent line to $C$ at $P$ if $P = Q$). Then

$$\text{“}L \cap C\text{”} = i^*L = P + Q + S.$$

(possibly $S = P$ or $S = Q$). Now $P + Q + S \sim 3P_0$, or

$$(P - P_0) + (Q - P_0) + (S - P_0) \sim 0.$$

Next let $L'$ be the line joining $S$ with $P_0$. Then

$$\text{“}L' \cap C\text{”} = i^*L' = S + P_0 + R \sim 3P_0.$$

So $(S - P_0) + (R - P_0) \sim 0$ or $(S - P_0) \sim -(R - P_0)$. Thus

$$(P - P_0) + (Q - P_0) \sim (R - P_0)$$

so $P + Q = R$.

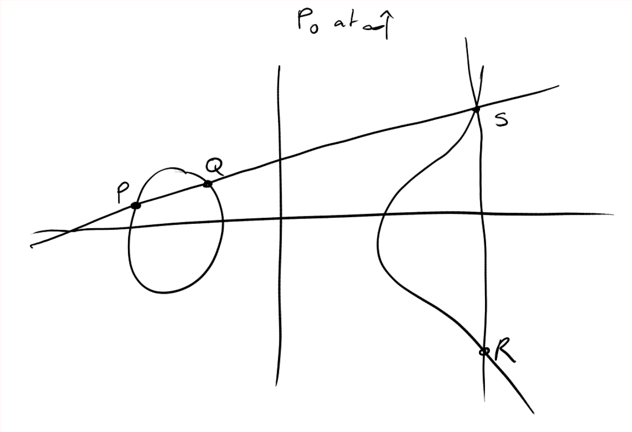
Start of

lecture 24

**Example.**

$$y^2 = (x - \lambda_1)(\lambda_2)(\lambda_3)$$

Take $P_0 = (0 : 1 : 0)$.




**Example.** Let $C$ have genus 2. Then $\deg K_C = 2g - 2 = 2$, $l(K_C) = 2$.

**Claim:** $|K_C|$ is base-point free, hence induces a morphism $f : C \to \mathbb{P}^1$.

**Lemma.** Let $C$ be a projective non-singular curve. If there exist $P, Q \in C$, $P \neq Q$, $P \sim Q$, then $C \cong \mathbb{P}^1$.

*Proof.* Consider the linear system $|P|$. Since $Q \in |P|$, $\dim |P| \geq 1$, so $l(P) \geq 2$. But we have an upper bound $\dim \mathcal{L}(D) \leq \deg D + 1 \leq 2$. Thus $l(P) = 2$. If $Q, R \in C$ then $\dim \mathcal{L}(P - Q - R) = 0$ since $\deg(P - Q - R) = 1$. Thus $|P|$ induces an embedding of $C$ into $\mathbb{P}^1$. So $C \cong \mathbb{P}^1$. □

*Proof of Claim.* If $|K_C|$ is not base-point free, then there exists $P \in C$ such that $l(K_C - P) = l(K_C) = 2$. Since $\deg K_C - P = 1$, this means there exists $Q, R \in |K_C - P|$, $Q \neq R$, with $Q \sim R$. Hence $C \cong \mathbb{P}^1$, contradiction, since $\mathbb{P}^1$ has genus 0. □

Thus if $g = 2$, we obtain a degree 2 morphism $f : C \to \mathbb{P}^1$ induces by $|K_C|$.

**Definition** (Hyperelliptic)**.** A projective non-singular curve $C$ is *hyperelliptic* if there exists a degree 2 morphism $f : C \to \mathbb{P}^1$.

Thus all genus 2 curves are hyperelliptic.

**Theorem.** Let $C$ be a projective non-singular curve of genus $g \geq 3$. Then either:

(1) $C$ is hyperelliptic, or

(2) $|K_C|$ induces an embedding $C \hookrightarrow \mathbb{P}^{g-1}$.

*Proof.* $|K_C|$ induces an embedding in $\mathbb{P}^{l(K_C)-1} = \mathbb{P}^{g-1}$ if and only if $\forall P, Q \in C$,

$$l(K_C - P - Q) = l(K_C) - 2 = g - 2.$$

In any event,

$$l(P + Q) - l(K_C - P - Q) = \deg(P + Q) + 1 - g = 3 - g.$$

Thus $|K_C|$ induces an embedding if and only if $l(P + Q) = 1$ for all $P, Q \in C$. Now suppose $|K_C|$ does not induce an embedding. Then there exist $P, Q \in C$ such that $l(P + Q) > 1$. If $l(P + Q) \geq 3$, then for $R \in C$, $l(P + Q - R) \geq 2$. So there exists $P_1, P_2 \in |P + Q - R|$ distinct. Thus $C \cong \mathbb{P}^1$ by the lemma, a contradiction. Thus $l(P+Q) = 2$. Note similarly $l(P+Q-R) = 1$ for all $R \in C$. Thus $|P+Q|$ is base-point free and induces a degree 2 morphism $f : C \to \mathbb{P}^1$. So $C$ is hyperelliptic. □

**Theorem** (Riemann-Hurwitz formula)**.** Let $f : X \to Y$ be a non-constant morphism between projective non-singular curves, with $\operatorname{char} \mathbb{K} = 0$ (or $K(Y) \subseteq K(X)$ is a separable field extension). Then

$$2 - 2g(X) = (\deg f)(2 - 2g(Y)) - \sum_{p \in X} (e_p - 1).$$

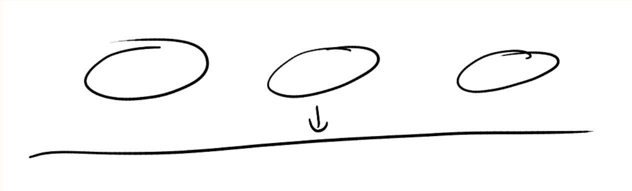
($e_p = \nu_p(t \cdot f)$ where $t$ is a local parameter at $f(p)$).

*Proof.* Omitted. □

**Example.** $X = C$ hyperelliptic, $Y = \mathbb{P}^1$, $Y = \mathbb{P}^1$, $f : C \to \mathbb{P}^1$ degree 2. Then

$$2 - 2g(C) = \underbrace{2 \cdot (2 - 2 \cdot 0)}_{4} - \sum_{p \in C} (e_p - 1).$$

Thus the number number of points $p \in C$ with $e_p > 1$ is $\sum_p (e_p - 1) = 2g(C) + 2$, $\deg g = \sum_{p \in f^{-1}(q)} e_p$.



# Index

Krull dimension 50