II Algebraic Geometry

Ishan Nath, Lent 2024

Based on Lectures by Prof. Mark Gross

October 3, 2024

Contents

1 Affine Varieties

1.1 Algebraic Sets

Our basic setup is as follows: we begin by fixing a field $\mathbb{K}$.

Definition 1.1. The *affine n-space* over $\mathbb{K}$ is

$$\mathbb{A}^n = \mathbb{K}^n.$$

Let $A = \mathbb{K}[x_1, \ldots, x_n]$, and $S \subseteq A$. Set

$$Z(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) = 0 \quad \forall f \in S\}.$$

Proposition 1.1.

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

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

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

Proof:

(a) and (b) are obvious.

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

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

(d) If $p \in Z(S_i)$ for all i, then $p \in Z(\bigcup S_i)$.

Conversely, if $p \in Z(\bigcup S_i)$, then $p \in Z(S_i)$ for all i.

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

Definition 1.2. A subset of $\mathbb{A}^n$ is *algebraic* if it is of the form $Z(S)$ for some $S \subseteq A$.

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 forms the *Zariski topology* on $\mathbb{A}^n$.

Example 1.1.

1. If $\mathbb{K} = \mathbb{C}$, the Zariski open or closed subsets are also open or closed in the "usual" topology.
2. For any $\mathbb{K}$, consider $\mathbb{A}^1$, and $S \subseteq K[x]$ containing a non-zero element. Then $Z(S)$ is finite.

   So the Zariski closed sets are $\mathbb{A}^1$ and all finite sets, so this is equivalent to the cofinite topology.

Recall that if A is a commutative ring and $S \subseteq A$ is a subset, the ideal generated by S is the ideal $\langle S \rangle \subseteq A$ given by

$$\langle S \rangle = \left\{ \sum_{i=1}^{q} f_i g_i \;\middle|\; q \geq 0, f_i \in S, g_i \in A \right\}.$$

This is the smallest ideal of A containing S.

Lemma 1.1. *Let $S \subseteq \mathbb{K}[x_1, \dots, x_n]$ and $I = \langle S \rangle$. Then*

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

Proof: If $p \in Z(S)$, let $f_1, \dots, f_q \in S$ and $g_1, \dots, g_q \in A$. Then

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

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

But conversely, since $S \subseteq I$, $Z(I) \subseteq Z(S)$. So $Z(S) = Z(I)$.

Definition 1.3. Let $X \subseteq \mathbb{A}^n$ be a subset. Define

$$I(X) = \{ f \in A = \mathbb{K}[x_1, \dots, x_n] \mid f(p) = 0 \quad \forall p \in X \}.$$

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

Moreover, if $S_1 \subseteq S_2 \subseteq A$, then $Z(S_2) \subseteq Z(S_1)$, and if $X_1 \subseteq X_2 \subseteq \mathbb{A}^n$, then $I(X_2) \subseteq I(X_1)$.

An intuitive thing to consider is the relationship between an ideal I and $I(Z(I))$.

Example 1.2.

Take $I = \langle x^2 \rangle \subseteq \mathbb{K}[x]$.

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

Definition 1.4. Let $I \subseteq A$ be an ideal in the commutative ring A. The *radical* of I is

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

Lemma 1.2. *$\sqrt{I}$ is an ideal.*

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

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

For each i, either $i \geq n_1$ or $n_1 + n_2 - i \geq n_2$. Therefore each term lies in I, hence $(f+g)^{n_1+n_2} \in I$. Hence $f + g \in \sqrt{I}$.

Now if $f \in \sqrt{I}$ and $g \in A$, then $f^n \in I$ for some n. So $(fg)^n = f^n g^n \in I$, so $fg \in \sqrt{I}$.

Proposition 1.2.

(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 ideal I. Certainly, $I \subseteq I(X)$, by definition of Z and $I(X)$. Thus $Z(I(X)) \subseteq Z(I) = X$. But we clearly have $X \subseteq Z(I(X))$.

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

Theorem 1.1 (Hilbert's Nullstellensatz)**.** *Let $\mathbb{K}$ be an algebraically closed field. Then*

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

Example 1.3.

Take $\mathbb{K} = \mathbb{R}$, and $I = \langle x^2 + y^2 + 1 \rangle \subseteq \mathbb{R}[x, y]$.

But now $Z(I) = \emptyset$, however $I(Z(I)) = \mathbb{R}[x, y] \neq \sqrt{I}$.

This shows why we need an algebraically closed field: sometimes the zero set cannot properly capture the detail of the algebra, for example if the variety has no solutions.

1.2 Irreducible Subsets

Definition 1.5. 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, then either $Z = Z_1$ or $Z = Z_2$.

Remark. This is a bad notion in the Euclidean topology in $\mathbb{C}^n$. The only irreducible sets are points.

Example 1.4.

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

Definition 1.6. An (affine, algebraic) *variety* in $\mathbb{A}^n$ is an irreducible algebraic set.

We are now interesting in recognizing irreducible algebraic sets algebraically.

Proposition 1.3. *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 that an ideal $P \subseteq A$ is *prime* if $P \neq A$, and whenever $f \cdot g \in P$, then either $f \in P$ or $g \in P$.

Lemma 1.3. *Let $P \subseteq A$ be prime, and $I_1, \dots, I_n \subseteq A$ be ideals. Suppose that $P \supseteq \bigcap I_i$. Then $P \supseteq I_i$ for some i. Moreover, if $P = \bigcap I_i$, then $P = I_i$ for some i.*

Example 1.5.

Take $A = \mathbb{Z}$, and $P = \langle p \rangle$ for p a prime number, and $I_i = \langle n_i \rangle$. Then,

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

Now note that

$$P \supseteq \bigcap_i I_i \iff p \mid \operatorname{lcm}(n_1, \dots, n_s) \iff p \mid n_i \text{ for some } i.$$

Proof: Suppose $P \not\supseteq I_i$ for any i. Then we can find $x_i \in I_i$ such that $x_i \notin P$. But now

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

so there exists $x_i \in P$, which gives a contradiction.

If $P = \bigcap I_i$, then $P \subseteq I_i$ for each i. We know that $I_i \subseteq P$ for some i, hence $P = I_i$ for some i.

Here's the main point.

Proposition 1.4. *Let 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.*

Proof:

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

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

so if X is irreducible, then without loss of generality, we can assume $X = X \cap Z(f)$, so $X \subseteq Z(f)$. Hence $f \in I(X)$.

$\impliedby$ If $P \subseteq A = \mathbb{K}[x_1, \dots, x_n]$ is prime, suppose $Z(P) = X_1 \cup X_2$ where X_1, X_2 are closed. Then

$$I(x_1) \cap I(X_2) = I(X_1 \cup X_2) = I(Z(P)) = \sqrt{P},$$

by Hilbert's Nullstellensatz. But note $\sqrt{P} = P$: if $f^n \in P$, then $f \in P$ by the primality of P. Therefore, $I(X_1) \cap I(X_2) = P$. So by our lemma, either $P = I(X_1)$ or $P = I(X_2)$, so $Z(P) = X_1$ or $Z(P) = X_2$.

We now have a one-to-one correspondence between prime ideals of A, and varieties in $\mathbb{A}^n$, given by our maps Z and I.

Proposition 1.5. *Any algebraic set in $\mathbb{A}^n$ can be written as a finite union of varieties.*

Proof: Let $\mathcal{S}$ be the set of all algebraic sets in $\mathbb{A}^n$ which cannot be written as a finite union of varieties. If $\mathcal{S} \neq \emptyset$, then I claim it has a minimal element with respect to inclusion. Otherwise, there exists $X_1, X_2, X_3, \ldots \in \mathcal{S}$ with

$$X_1 \supset X_2 \supset X_3 \supset \cdots,$$

and $X_i \neq X_{i+1}$. Now note that

$$I(X_1) \subset I(X_2) \subset I(X_3) \subset \cdots \subseteq A.$$

But note that $A = \mathbb{K}[x_1, \ldots, x_n]$ is Noetherian by Hilbert's basis theorem, so this is a contradiction.

Let $X \in \mathcal{S}$ be minimal. Now X is not irreducible, as otherwise X is itself a variety. Otherwise, we can write $X = X_1 \cup X_2$ with $X_1 \subset X, X_2 \subset X$ with X_1, X_2 algebraic. Thus $X_1, X_2 \notin \mathcal{S}$, hence they can be written as a union of irreducible sets, so X can also be written as a finite union of irreducibles, so $X \notin \mathcal{S}$, contradiction.

Definition 1.7. 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 1.6.

1. In $\mathbb{A}^2$, $A = \mathbb{K}[x_1, x_2]$. Then

$$X = Z(x_1 x_2) = Z(x_1) \cup Z(x_2).$$

2. More generally, $A = \mathbb{K}[x_1, \ldots, x_n]$ is a UFD. So for $0 \neq f \in A$, we write $f = \prod f_i^{a_i}$, with f_i irreducible. Since A is a UFD, $\langle f_i \rangle$ is prime.

Hence $Z(f_i)$ is irreducible, so

$$Z(f) = Z(f_1) \cup \cdots \cup Z(f_n)$$

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, and $f \in A = \mathbb{K}[x_1, \ldots, x_n]$. This gives a function $f : \mathbb{A}^n \to K$.

This naturally gives $f|_X : X \to \mathbb{K}$. Hence if $f, g \in A$ with $f|_X = g|_X$, then $f - g$ vanishes on X. So $f - g \in I(X)$. So it is natural to think of $A/I(X)$ as being the set of polynomial functions on X.

Definition 1.8. Let $X \subseteq \mathbb{A}^n$ be an algebraic set. The *coordinate ring* of X is

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

Definition 1.9. Let $X \subseteq \mathbb{A}^n$ be an algebraic set, and $U \subseteq X$ an open subset. A function $f : U \to \mathbb{K}$ is *regular* if for all $p \in U$ 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 $f = g/h$ on V.

A regular function is locally a rational function, but different points may require different representations.

Example 1.7.

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

Definition 1.10. We write

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

Note that $\mathcal{O}_X(U)$ is a ring, and it is also a vector space over $\mathbb{K}$. This makes it a $\mathbb{K}$-algebra.

Definition 1.11. If A, B are rings, then an A-algebra structure on B is the data of a ring homomorphism $\phi : A \to B$. This turn B into an A-module via

$$a \cdot b = \phi(a) \cdot b.$$

Hence $\mathbb{K} \to \mathcal{O}_X(u)$ is given by $a \in \mathbb{K} \mapsto$ the constant function with value a.

We have the following lemma:

Lemma 1.4. *For all X algebraic, if $\mathbb{K}$ is algebraically closed, then*

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

The proof will be given after Hilbert's Nullstellensatz.

Recall that, if A is an integral domain, then the *field of fractions* of A is

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

where we have

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

This is a field, as can be checked:

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'}, \qquad \frac{f}{g}\frac{f'}{g'} = \frac{ff'}{gg'}, \qquad \left(\frac{f}{g}\right)^{-1} = \frac{g}{f}.$$

If $X \subseteq \mathbb{A}^n$ is an affine variety, then $A(X) = A/I(X)$ is an integral domain, since $I(X)$ is a prime ideal.

Definition 1.12. If $X \subseteq \mathbb{A}^n$ is a variety, its *fraction field* is $K(X)$, the fraction field of $A(X)$. Elements of $K(X)$ are called *rational functions*.

Note that $g/h \in K(X)$ induces a regular function on $X \setminus Z(h)$.

1.4 Morphisms

Definition 1.13. A map $f : X \to Y$ between affine varieties is called a *morphism* if:

1. f is continuous in the induced Zariski topologies on X and Y (recall $Z \subseteq X \subseteq \mathbb{A}^n$ is closed in X if and only if it is closed in $\mathbb{A}^n$).
2. For all $V \subseteq Y$ open and $\phi : V \to \mathbb{K}$ a regular function,

$$\phi \circ f : f^{-1}(V) \to \mathbb{K}$$

is a regular function on $f^{-1}(V)$.

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

Moreover, we have

$$f^\#(a \cdot \phi) = a \cdot f^\#(\phi),$$

which gives a $\mathbb{K}$-algebra homomorphism.

From now on, we look only at $\mathbb{K}$ algebraically closed. Assuming this, we get the following.

Theorem 1.2. *There is a one-to-one 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

$$A(X) = \frac{\mathbb{K}[x_1, \ldots, x_n]}{I(X)}, \qquad A(Y) = \frac{\mathbb{K}[y_1, \ldots, y_m]}{I(Y)}.$$

Suppose we are given $f^\# : A(Y) \to A(X)$. Set $f_i = f^\#(\bar{y}_i)$, where $\bar{y}_i$ is the image of y_i in $A(Y)$. Then we define $f : X \to \mathbb{A}^m$ by

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

We claim that $f(X) \subseteq Y$. Indeed, let $g \in I(Y)$, and $p \in X$. We need to show that $g(f(p)) = 0$. Consider the map

$$\mathbb{K}[y_1, \ldots, y_m] \to A(Y) \to A(X).$$

Then we have

$$g(y_1, \ldots, y_m) \mapsto g(\bar{y}_1, \ldots, \bar{y}_m) \mapsto g(f_1, \ldots, f_m).$$

Here it is important for $f^\#$ to be a $\mathbb{K}$-algebra homomorphism. Since $g \in I(Y)$, we get that $g(f_1, \ldots, f_m)(p) = 0$, i.e. $g(f(p)) = 0$. So $f(p) \in Y$.

Note that, if $\phi \in A(Y)$, we can write $\phi = g(\bar{y}_1, \ldots, \bar{y}_m)$ and $f^\#(\phi) = g(f_1, \ldots, f_m) = \phi \circ f$. Now we claim that f is a morphism.

First, we show f is continuous, by showing $f^{-1}(Z)$ is closed for $Z \subseteq Y$ closed. Note that $I(Z) \supseteq I(Y)$, so

$$\overline{I(Z)} = \frac{I(Z)}{I(Y)} \subseteq A(Y)$$

is an ideal in $A(Y)$. Then we can define

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

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,

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

So $f^{-1}(Z)$ is closed. Finally we show that f takes regular functions to regular functions. Let $U \subseteq Y$ be an open subset, $\phi \in \mathcal{O}_Y(U)$. then we need to show that $\phi \circ f : f^{-1}(U) \to \mathbb{K}$ 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 $\phi = g/h$, for $g, h \in A(Y)$. Then

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

Now $f^{\#}(g), f^{\#}(h)$ lie in $A(X)$, and $f^{\#}(h) = h \circ f$ does not vanish on $f^{-1}(V)$, as h does not vanish on V.

We can check this gives a one-to-one correspondence. We know that $f^{\#} \mapsto f \mapsto f^{\#}$, and we can check that $f \mapsto f^{\#} \mapsto f$.

The moral is that a morphism $f : X \to Y$ is given by choosing polynomial functions $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ and defining f by

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

Example 1.8.

Take $f : \mathbb{A}^1 \to \mathbb{A}^2$ by $t \mapsto (t, t^2)$. The image of this map is $Y = Z(x_1^2 - x_2)$, and this defines a morphism $f : \mathbb{A}^1 \to Y$.

Now the inverse map is

$$f^{\#} : \frac{\mathbb{K}[x_1, x_2]}{(x_2 - x_1^2)} \to \mathbb{K}[t]$$

by $f^{\#}(x) = t$, $f^{\#}(y) = t^2$. Then this is an isomorphism.

Definition 1.14. Two affine varieties X, Y 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 1.3. *If X, Y are affine varieties, then X is isomorphic to Y if and only if $A(X) \cong A(Y)$ as $\mathbb{K}$-algebras.*

As seen above, $\mathbb{A}^1 \cong Z(X^2 - Y) \subseteq \mathbb{A}^2$.

Remark. A $\mathbb{K}$-algebra A is *finitely generated* if there exists a surjective $\mathbb{K}$-algebra homomorphism $\mathbb{K}[x_1, \dots, x_n] \to A$ with $x_i \mapsto a_i$. Hence every element of A can be written as a polynomial in $a_1, \dots, a_n$ with coefficients in $\mathbb{K}$.

If I is the kernel of this map, then

$$A \cong \frac{\mathbb{K}[x_1, \dots, x_n]}{I}.$$

Suppose further that A is an integral domain. Then I is a prime ideal of $\mathbb{K}[x_1, \dots, x_n]$, so $A = A(X)$ where $X = Z(I)$.

2 Hilbert's Nullstellensatz

Our goal in this section is to prove, if $\mathbb{K} = \overline{\mathbb{K}}$, then

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

Definition 2.1. 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. there is no $f \in K[x]$ with $f \neq 0$, $f(z) = 0$.

Similarly, $z_1, \dots, z_d \in F$ are *algebraically independent* over $\mathbb{K}$ if there is no $f \in \mathbb{K}[x_1, \dots, x_d]$ such that $f \neq 0$, $f(z_1, \dots, z_d) = 0$.

A *transcendence basis* for $F/\mathbb{K}$ is a set $z_1, \dots, z_d \in F$, which are algebraically independent over $\mathbb{K}$, and such that F is algebraic over $\mathbb{K}[z_1, \dots, z_d]$.

Example 2.1.

If X is a variety, then $K(X)$ is a field over $\mathbb{K}$, and it usually has many transcendentals. For example,

$$K(\mathbb{A}^n) = \{f/g \mid f, g \in \mathbb{K}[x_1, \dots, x_n], g \neq 0\} = \mathbb{K}(x_1, \dots, x_n).$$

Then $x_1, \dots, x_n$ form a transcendence basis.

Definition 2.2. 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 2.2.

$K(X)/\mathbb{K}$ 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 2.1. *Every finitely generated field extension $F/\mathbb{K}$ has a transcendence basis, and any two transcendence bases have the same cardinality.*

Moreover, if $F = \mathbb{K}(z_1, \dots, z_N)$, then there is a transcendence basis $\{y_1, \dots, y_n\} \subseteq \{z_1, \dots, z_N\}$.

Proof: Write $F = \mathbb{K}(z_1, \dots, z_N)$. If these are algebraically independent, then $z_1, \dots, z_N$ is a transcendence basis. Also if they are algebraic over $\mathbb{K}$, then the transcendence basis can be taken to be empty.

After reordering, assume $\{z_1, \ldots, z_d\}$ is a maximal subset of algebraically independent elements of $\{z_1, \ldots, z_N\}$. Then we will show $\{z_1, \ldots, z_d\}$ is a transcendence basis, i.e F is algebraic over $\mathbb{K}(z_1, \ldots, z_d)$.

It is enough to show z_j is algebraic over $\mathbb{K}(z_1, \ldots, z_d)$ for any $j > d$. By assumption, $z_1, \ldots, z_d, z_j$ are not algebraically independent, so there exists $f_j \in \mathbb{K}[x_1, \ldots, x_d, x_j]$ such that $f_j(z_1, \ldots, z_d, z_j) = 0$.

Then consider the polynomial $F_j(x) = f_j(z_1, \ldots, z_d, x)$. This is a polynomial in $\mathbb{K}(z_1, \ldots, z_d)[x]$. Plugging in $x = z_j$, $F_j(z_j) = f_j(z_1, \ldots, z_d, z_j) = 0$. Also $F \neq 0$, as otherwise $F_j(z) = f_j(z_1, \ldots, z_d, z)$ would be an algebraic relation for $\{z_1, \ldots, z_d\}$, for all $z \in \mathbb{K}(z_1, \ldots, z_d)$. Hence $\{z_1, \ldots, z_d\}$ is indeed a transcendence basis.

Now suppose $z_1, \ldots, z_d$ and $w_1, \ldots, w_e$ are both transcendence bases. Suppose $d \leq e$. We will use the same idea as the Steinitz exchange lemma. First, as w_1 is algebraic over $\mathbb{K}(z_1, \ldots, z_d)$, there is a polynomial $f \in \mathbb{K}[x_1, \ldots, x_d, x_{d+1}]$ such that $f(z_1, \ldots, z_d, w_1) = 0$. This is obtained by clearing the denominators.

Since w_1 is not algebraic, f must involve at least some of $x_1, \ldots, x_d$. Thus we can suppose z_1 is algebraic over $\mathbb{K}(w_1, z_2, \ldots, z_d)$, hence F is algebraic over $\mathbb{K}(w_1, z_2, \ldots, z_d)$.

We now repeat this process. As w_2 is algebraic over $\mathbb{K}(w_1, z_2, \ldots, z_d)$, and not algebraic over $\mathbb{K}(w_1)$, we 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 furthermore g involves one of $x_2, \ldots, x_d$. Suppose it involves x_2, then z_2 is algebraic over $\mathbb{K}(w_1, w_2, z_3, \ldots, z_d)$, and hence F is algebraic over $\mathbb{K}(w_1, w_2, z_3, \ldots, z_d)$.

Continuing, eventually we find F is algebraic over $\mathbb{K}(w_1, \ldots, w_d)$. If $e > d$, this means w_e is algebraic over $\mathbb{K}(w_1, \ldots, w_d)$, contradicting the fact $\{w_1, \ldots, w_e\}$ is a transcendence basis.

Lemma 2.1. *Let M be a finitely generated A-module, for A a commutative ring. Let $I \subseteq A$ and $\phi : M \to M$ be an A-module homomorphism such that*

$$\phi(M) \subseteq I \cdot M = \{a \cdot m \mid a \in I, m \in M\}.$$

Then there exists an equation

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

with $a_i \in I$.

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 we can write

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

with $a_{ij} \in I$. Hence we have

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

where δ_{ij} is the usual Kronecker delta. Writing this out as a matrix,

$$\begin{pmatrix} \phi - a_{11} & -a_{12} & \cdots \\ -a_{21} & \phi - a_{22} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \end{pmatrix} = 0.$$

Multiplying by the adjoint matrix, we get

$$\det((\delta_{ij}\phi - a_{ij}))x_j = 0,$$

for all j. But $\det((\delta_{ij}\phi - a_{ij}))$ is a degree n polynomial in ϕ annihilating each x_j, hence it annihilates every element in M. Moreover the leading term in ϕ is ϕ^n, and all the other coefficients are elements in I.

2.1 Integrality

Definition 2.3. Let $A \subseteq B$ be integral domain. An element $b \in B$ is *integral* over A if $f(b) = 0$ for a monic polynomial $f(x) \in A[x]$

Proposition 2.2. *$b \in B$ is 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: Suppose $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. Then since $A[b]$ is generated as an A-module by $1, b, b^2, \ldots$, it is also generated by $1, b, \ldots, b^{n-1}$. In particular, it is finitely generated. Then we can just take $C = A[b]$.

On the other hand, if C is finitely generated, let $\phi : C \to C$ be the module homomorphism given by $\phi(x) = b \cdot x$. Applying the previous 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 $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, by plugging in 1.

Lemma 2.2. *Let $A \subseteq B$ 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 that $g \in A[X]$. Suppose that

$$g(x) = a_N x^N + \cdots + a_0,$$

for $a_N \neq 0$, $a_i \in A$. Then

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

This is a monic polynomial in $a_N x$. Substituting $x = b$, this gives a monic polynomial killing $a_N b$. So $a_N b$ is integral over A, and we take $p = a_N$.

Lemma 2.3 (Rational Root Theorem)**.** *Let A be a UFD with fraction field K. If $\alpha \in K$ is integral over A, we have $\alpha \in A$.*

Proof: If $\alpha \in K$ is integral over A, write $\alpha = a/b$, with a, b having no common factor. Say $g(\alpha) = 0$ for some monic polynomial α, with

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

Then we have

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

Multiplying out,

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

in A. So $b \mid a$, showing that b must be a unit in A. Thus $\alpha = a/b \in A$.

Lemma 2.4. *Let $A \subseteq B$ 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, hence over $A[b_1]$. So $A[b_1][b_2] = A[b_1, b_2]$ is a finitely generated $A[b_1]$-module.

From this, we can conclude that $A[b_1, b_2]$ is 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 $b_1 \pm b_2, b_1 \cdot b_2 \in S$.

Lemma 2.5 (Hilbert's Nullstellensatz, Version 0)**.** *Let $\mathbb{K}$ be an algebraically closed field, and $F/\mathbb{K}$ be a field extension which is finitely generated as a $\mathbb{K}$-module.*

Then $F = \mathbb{K}$.

Proof: Suppose $\alpha \in F$ is algebraic over $\mathbb{K}$, with irreducible polynomial $f(x) \in \mathbb{K}[x]$. Then f factors into linear factors over $\mathbb{K}$, as $\mathbb{K}$ is algebraic. So f is linear, and hence is of the form $c(x - \alpha)$. Thus $\alpha \in \mathbb{K}$.

Suppose we are given surjective map $\mathbb{K}[x_1, \dots, x_d] \to F$ surjective, where $x_i \mapsto z_i \in F$. Then $z_1, \dots, z_d$ generate F as a field extension of $\mathbb{K}$. Assume $z_1, \dots, z_e$ form a transcendence basis for $F/\mathbb{K}$.

Note if $F \neq \mathbb{K}$, then we must have $e \geq 1$. Let $R = \mathbb{K}[z_1, \dots, z_e] \subseteq F$. This is a polynomial ring, as $z_1, \dots, z_e$ are algebraically independent. Then $w_1 = z_{e+1}, \dots, w_{d-e} = z_d$ are algebraic over $L = \mathbb{K}(z_1, \dots, z_e)$.

Let $S \subseteq F$ be the set of elements of F integral over R. Then S is a subring of F. But now there exists $p_1, \dots, p_{d-e} \in R$, with $t_i = p_i w_i$ integral over R. In particular, $t_i \in S$.

Choose $f/g \in \mathbb{K}(z_1, \dots, z_e) = L$, with $f, g \in R$, f, g relatively prime, and g is relatively prime to $p_1, \dots, p_{d-e}$. Then $p_1^{n_1} \cdots p_{d-e}^{n_{d-e}} \cdot \frac{f}{g} \notin \mathbb{K}[z_1, \dots, z_e]$ for any $n_1, \dots, n_{d-e} \geq 0$. Here, don't think of f, g as polynomials, but rather elements of R.

But since $z_1, \dots, z_d$ generate F as a $\mathbb{K}$-algebra, there exists $q \in \mathbb{K}[x_1, \dots, x_d]$ such that

$$\frac{f}{g} = q(z_1, \dots, z_d) = q\left(z_1, \dots, z_e, \frac{t_1}{p_1}, \dots, \frac{t_{d-e}}{p_{d-e}}\right).$$

Let n_j be the highest power of x_{e+j} appearing in q. Multiplying by $\prod p_j^{n_j}$ clears the denominators of the right hand side, so we have

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

The right hand side lies in S as $z_1, \dots, z_e \in S$, $t_1, \dots, t_{d-e} \in S$, so the left hand side lies in S. But the left hand side lies in $\mathbb{K}(z_1, \dots, z_e)$, and thus lies in $\mathbb{K}[z_1, \dots, z_e]$, a contradiction.

Hence $e = 0$, so F is algebraic over $\mathbb{K}$, hence $F = \mathbb{K}$.

Now we can prove the "actual" Nullstellensatz.

Theorem 2.1 (Nullstellensatz I). *Let $\mathbb{K}$ be algebraically closed. Then any maximal ideal $m \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is of the form*

$$b = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$$

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

Proof: Note we have an isomorphism

$$\frac{\mathbb{K}[x_1, \ldots, x_n]}{\langle x_1 - a_1, \ldots, x_n - a_n \rangle} \to \mathbb{K},$$

by $x_i \mapsto a_i$. Note $m \subseteq A$ is a maximal ideal if and only if A/m is a field. This shows that $m = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is a maximal ideal.

Conversely, let $m \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be maximal. Then $\mathbb{K}[x_1, \ldots, x_n]/m = F$ is a field, which is generated as a $\mathbb{K}$-algebra by $x_1, \ldots, x_n$. Thus $F = \mathbb{K}$ by our previous lemma.

We thus have an isomorphism

$$\frac{\mathbb{K}[x_1, \ldots, x_n]}{m} \xrightarrow{\phi} \mathbb{K}.$$

Let $a_i = \varphi(x_i)$. Then $\phi(x_i - a_i) = \phi(x_i) - a_i = 0$, so $x_i - a_i \in m$. Hence $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq m$. Since the left hand ideal is maximal, we have equality.

Example 2.3.

This is false if our field is not algebraically closed. For example, $\langle x^2 + 1 \rangle$ is a maximal ideal in $\mathbb{R}[x]$, but of course $\langle x^2 + 1 \rangle \neq \langle x - a \rangle$ for any $a \in \mathbb{R}$.

Here is another form.

Theorem 2.2 (Nullstellensatz II). *Let $\mathbb{K}$ be algebraically closed, and $I = \langle f_1, \ldots, f_r \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Then either:*

1. $I = \mathbb{K}[x_1, \ldots, x_n]$, *or*
2. $Z(I) \neq \emptyset$.

Proof: Suppose $1 \notin I$, i.e. we are not in the first case. Then there exists a maximal ideal $m \subseteq \mathbb{K}[x_1, \ldots, x_n]$, with $I \subseteq m$.

But then $Z(m) \subseteq Z(I)$, and since $m = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, we have $Z(m) = \{(a_1, \ldots, a_n)\}$. So $Z(m) \neq \emptyset$, hence $Z(I) \neq \emptyset$.

Here we actually go.

Theorem 2.3 (Nullstellensatz III)**.** *Let $\mathbb{K}$ be algebraically closed, $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ an ideal. Then*

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

Proof: One direction we have already seen: $\sqrt{I} \subseteq I(Z(I))$.

Let $g \in \mathbb{K}[x_1, \ldots, x_n]$. Define

$$V_g = Z(zg(x_1, \ldots, x_n) - 1) \subseteq \mathbb{A}^{n+1},$$

with coordinates $x_1, \ldots, x_n, z$. If we project V_g via $(x_1, \ldots, x_n, z) \mapsto (x_1, \ldots, x_n)$, we get 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 $I = \langle f_1, \ldots, f_r \rangle$, consider $J = \langle f_1, \ldots, f_r, zg - 1 \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n, z]$. Then $Z(J) = \emptyset$, so $J = \mathbb{K}[x_1, \ldots, x_n, z]$ by our previous version of the Nullstellensatz. So we can write

$$1 = \sum_{i=1}^{n} h_i f_i + h(gz - 1),$$

with $h_i, h \in \mathbb{K}[x_1, \ldots, x_n, z]$. Substitute $z = 1/g$, to get

$$1 = \sum_{i=1}^{n} h_i(x_1, \ldots, x_n, 1/g) f_i(x_1, \ldots, x_n).$$

Multiplying by a high power of g clears the denominators, giving

$$g^N = \sum_{i=1}^{n} h_i'(x_1, \ldots, x_n) f_i \in I.$$

Thus $g^N \in I$, so $g \in \sqrt{I}$.

Recall we need the proof of the lemma 1.4. For this, we need the following.

Lemma 2.6. *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 $\phi = (f, g) : X \to \mathbb{A}^2$. This is a morphism. Let $\Delta = \{(a, a) \in \mathbb{A}^2 \mid a \in \mathbb{K}\}$. Then $\Delta = Z(x - y)$.

Since ϕ is continuous, $\phi^{-1}(\Delta)$ is closed. But $U \leq \phi^{-1}(0)$, 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. Hence $U \subseteq \overline{U} = X \subseteq \phi^{-1}(0)$, so $\phi^{-1}(0) = X$.

We are now ready to prove the proposition.

Proof: We know $A(X) \subseteq \mathcal{O}_X(X)$. So let $f : X \to \mathbb{K}$ be a regular function, i.e. there exists an open cover $\{U_i\}$ of X with f 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 in U_i. Then

$$Z(\{h_i \mid i \in I\}) = \bigcap_i Z(h_i) \subseteq \bigcap_i (X \setminus U_i) = X \setminus \left(\bigcup_i U_i\right) = \emptyset.$$

Thus $Z(\{h_i\}) = \emptyset$. We can now pull back to $\mathbb{K}[x_1, \dots, x_n]$ and use Hilbert's second Nullstellensatz to get

$$1 = \sum_i e_i h_i.$$

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 our previous lemma, $g_i h_j = g_j h_i$ on X. Hence $\frac{g_i}{h_i} = \frac{g_j}{h_j}$ on $K(X)$. Thus we have the equality in $K(X)$

$$f = \sum_i (e_i h_i) f = \sum_i (e_i h_i) \frac{g_i}{h_i} = \sum e_i g_i \in A(X).$$

Remark. U_i and U_j always intersect, as they are dense sets: if not, $\overline{U_i}$ and $X \setminus U_i$ form a proper closed union of X.

In essence open subsets of affine varieties are always dense, and this makes the

Zariski topology interesting!

3 Projective Varieties

Definition 3.1. 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 $\lambda \in \mathbb{K}^\times$. Alternatively, this is the set of one-dimensional sub-vector spaces of $\mathbb{K}^{n+1}$.

Remark. If $\mathbb{K} = \mathbb{R}$, then $\mathbb{P}^n = S^n/\sim$, where $x \sim -x$.

For arbitrary $\mathbb{K}$, we look at $\mathbb{P}^1$. For an arbitrary element $(x_0 : x_1) \in \mathbb{P}^1$, if $x_1 \neq 0$, then we have

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

since there is a unique representative with the second coordinate 1. The missing points are of the form $(x_0 : 0) \sim (1 : 0)$. Thus we view $\mathbb{P}^1 = \mathbb{A}^1 \cup \{(1, 0)\}$, where we can view the point $(1, 0)$ as ∞. This is the Riemann sphere if $\mathbb{K} = \mathbb{C}$.

Now $\mathbb{P}^2$ consists of elements of the form $(x_0 : x_1 : x_2) \in \mathbb{P}^2$. 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 $(x_0 : x_1 : 0) \in \mathbb{P}^1$. So $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$, where we view $\mathbb{P}^1$ as the line at infinity.

As we did for $\mathbb{A}^n$, we now look to define a topology via algebraic subsets of $\mathbb{P}^n$. But we cannot just define it as the zeros of a polynomial $f(x_0, \dots, x_n)$, as then we may have two equivalent points not being in the same algebraic set.

Definition 3.2. $f \in S = \mathbb{K}[x_0, \dots, x_n]$ is *homogeneous* if every term of f is 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.

Example 3.1.

$x_0^3 + x_1 x_2^2$ is homogeneous of degree 3, whereas $x_0^3 + x_1^2$ is not homogeneous.

Definition 3.3. If $T \subseteq S$ is a set of homogeneous polynomials, define

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

An ideal $I \subseteq S$ is *homogeneous* if I is generated by homogeneous polynomials. For I a homogeneous ideal, we define

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

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

Example 3.2.

Take $Z(a_0x_0+a_1x_1+a_2x_2) \subseteq \mathbb{P}^2$, for $a_0, a_1, a_2 \in \mathbb{K}$. In $\mathbb{A}^2 \subset \mathbb{P}^2$ 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 $a_0 = a_1 = 0$, as then we just have $x_2 = 0$, the line at infinity.

We can check that the algebraic set in $\mathbb{P}^n$ form the closed sets of a topology on $\mathbb{P}^n$. This is again the *Zariski topology* on $\mathbb{P}^n$.

Definition 3.4. A *projective variety* is an irreducible closed subset of $\mathbb{P}^n$.

Define $U_i \subseteq \mathbb{P}^n$ to be $U_i = \mathbb{P}^n \setminus Z(x_i)$. This is an open subset of $\mathbb{P}^n$, and moreover

$$\bigcup_{i=0}^{n} U_i = \mathbb{P}^n.$$

We have a bijection $\phi_i : U_i \to \mathbb{A}^n$ by

$$\phi_i(x_0 : \ldots : x_n) = \left(\frac{x_0}{x_i}, \ldots, \widehat{\frac{x_i}{x_i}}, \ldots, \frac{x_n}{x_i}\right).$$

This is the *standard open affine cover* of $\mathbb{P}^n$.

Proposition 3.1. *With U_i carrying the topology induced from $\mathbb{P}^n$ and $\mathbb{A}^n$ the Zariski topology, ϕ_i is a homeomorphism.*

Proof: Since ϕ_i is a bijection, it suffices to show ϕ_i identifies closed sets of U_i with closed sets of $\mathbb{A}^n$. We take $i = 0$, $\phi = \phi_0$ and $U = U_0$.

Then let $S = \mathbb{K}[x_0, \ldots, x_n]$, S^h the set of homogeneous polynomials in S, and $A = \mathbb{K}[x_1, \ldots, x_n]$. Define maps $\alpha : S^h \to A$ and $\beta : A \to S^h$ by $\alpha(f(x_0, \ldots, x_n)) = f(1, x_1, \ldots, x_n)$, and if $g \in A$ is of degree e, define

$$\beta(g) = x_0^e g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

This is a process known as *homogenisation*, for example if we take $x_2^2 - x_1^3 - x_1 + x_1x_2$, the homogenisation is

$$x_0^3\left(\frac{x_2^2}{x_0^2} - \frac{x_1^3}{x_0^3} - \frac{x_1}{x_0} + \frac{x_1x_2}{x_0^2}\right) = x_0x_2^2 - x_1^3 - x_0^2x_1 + x_0x_1x_2.$$

If $Y \subseteq U$ is closed, Y is the intersection $\bar{Y} \cap U$, where $\bar{Y} \subseteq \mathbb{P}^n$ is a closed subset, which we can take to be the closure of Y. Now $\bar{Y} = Z(T)$ for some $T \subseteq S^h$, and let $T' = \alpha(T)$. We will show

$$\phi(Y) = Z(\alpha(T)).$$

We can check that

$$\begin{aligned} f(a_0 : \dots : a_n) = 0 &\iff f\left(1, \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) = 0 \\ &\iff \alpha(f)\left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right) = 0 \\ &\iff \alpha(f)\phi(a_0 : \dots : a_n) = 0. \end{aligned}$$

We need to prove that if $W \subseteq \mathbb{A}^n$ is closed, then $\phi^{-1}(W) \subseteq U = U_0$ is closed. We have $W = Z(T')$ for some set $T' \subseteq A = \mathbb{K}[y_1, \dots, y_n]$. We will show

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

Indeed, if $g \in T'$,

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

Example 3.3.

Take $f : \mathbb{P}^1 \to \mathbb{P}^3$, by

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

The image of this map is called the twisted cubic. Now we claim that this is a projective variety.

Indeed, consider the homomorphism

$$\phi : \mathbb{K}[x_0, \dots, x_3] \to \mathbb{K}[u, t],$$

by $x_0 \mapsto u^3$, $x_1 \mapsto u^2t$, $x_2 \mapsto ut^2$ and $x_3 \mapsto t^3$. Let $I = \ker \phi$. If $g \in I$, then g vanishes on the image of the map f. Thus $\mathrm{Im}(f) \subseteq Z(I)$.

Conversely, note that $x_0x_3 - x_1x_2$, $x_1^2 - x_0x_2$, $x_2^2 - x_1x_3 \in I$. Now let $p = (a_0 : a_1 : a_2 : a_3) \in Z(I)$. Then we have four cases.

If $a_0 \neq 0$, we can take $a_0 = 1$. Then $a_3 - a_1a_2 = 0$, $a_1^2 - a_2 = 0$ and $a_2^2 - a_1a_3 = 0$. Then $p = (1, a_1, a_1^2, a_1^3) = f(1 : a_1)$. So $p \in \mathrm{Im}(f)$.

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

Given $X \subseteq \mathbb{P}^n$ an algebraic set, define its *ideal* $I(X)$ to be the ideal in $S = \mathbb{K}[x_0, \dots, x_n]$, generated by homogeneous polynomials which vanish on X.

Then X is irreducible if and only if $I(X)$ is prime. For the twisted cubic $X = \mathrm{Im}(f)$, we indeed have $I(X) = I = \mathrm{Ker}\, \phi$. But $\mathbb{K}[x_0, \dots, x_3]/\operatorname{Ker}\phi$ is a subring of the integral domain $\mathbb{K}[u, t]$, hence is an integral domain, so $\mathrm{Ker}\, \phi$ is prime. Therefore X is a projective variety.

Definition 3.5. Let $X \subseteq \mathbb{P}^n$ be an affine 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 $f|_V = g/h$.

Definition 3.6. 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 action of regular functions. A variety will henceforth refer to any of an affine, quasi-affine, projective or quasi-projective variety.

Definition 3.7. A morphism $\phi : X \to Y$ between varieties is a continuous function ϕ such that, for all $V \subseteq Y$ open, $f : V \to \mathbb{K}$ regular,

$$f \circ \phi : \phi^{-1}(V) \to \mathbb{K}$$

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 morphism from a projective variety becomes harder, and this is a lot of what algebraic geometry is about.

Example 3.4.

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

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

$$ax = bz, \qquad by = aw.$$

Indeed if $a \neq 0$, we can take $a = 1$, and the $xy - zw = (bz)y - z(by) = 0$. If $a = 0$, then $y = z = 0$ so $xy - zw = 0$. This gives a family of lines in Q parametrized by $(a : b) \in \mathbb{P}^1$.

We also have $ax = bw, by = az$ another family of lines.

If we take a line from one family and a line from the other, they meet at one point. Indeed, $ax = bz$, $by = aw$, $cx = dw$ and $dy = cz$ has a unique solution up to scaling: $(bd : ac : ad : bc)$.

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

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

We claim that Σ is a bijection with $Q = Z(xy - zw)$. First note that $(bd) \cdot (ac) - (ad)(bc) = 0$, so indeed $\operatorname{Im} \Sigma \subseteq Q$.

Now we show that it is an injection. First suppose that $a, c \neq 0$. Then

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

which is injective on the set where $a, c \neq 0$. If $a = 0$, then

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

which does not coincide with the previous point and recovers $(c : d)$. If $a = c = 0$, then

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

If $a \neq 0, c = 0$, then we get

$$\Sigma((a : b)(0 : 1)) = (b : 0 : a : 0).$$

So Σ is injective. To prove it is surjective, suppose that $(a_0 : a_1 : a_2 : a_3) \in Q$, i.e. $a_0 a_1 - a_2 a_3 = 0$. If $a_0 \neq 0$, we can take $a_0 = 1$, so $a_1 = a_2 a_3$. Hence

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

A similar thing works in the case when a_2, a_3 or $a_4 \neq 0$.

Remark. $\mathbb{P}^1 \times \mathbb{P}^1$ is not a priori a variety, but it 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. We can check that 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 $\phi \circ \Sigma$ with $\phi : V \to \mathbb{K}$ regular.

We can generalise this notion. The *Segre embedding* is the map

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

where

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

Then we have the following:

Theorem 3.1. *Σ is injective and its image is an algebraic variety.*

Thus $\mathbb{P}^n \times \mathbb{P}^m$ acquires the structure of an algebraic variety. Another thing we can show is:

Theorem 3.2. *If $X \subseteq \mathbb{P}^n$, $Y \subseteq \mathbb{P}^n$ are projective varieties, then $\Sigma(X \times Y)$ is a projective variety.*

The proofs are given in the attached handout. This allows us to think of $X \times Y$ as a projective variety.

We can also think of the geometry of $\mathbb{P}^n \times \mathbb{P}^m$ by thinking about bihomogeneous polynomials in

$$\mathbb{K}[x_0, \ldots, x_n, y_0, \ldots, y_m],$$

i.e. polynomials f satisfying

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

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

If X and Y are quasi-projective, i.e. $X \subseteq \bar{X} \subseteq \mathbb{P}^n$, $Y \subseteq \bar{Y} \subseteq \mathbb{P}^n$, then $X \times Y \subseteq \bar{X} \times \bar{Y}$ defines an open subset of $\bar{X} \times \bar{Y}$. This allows us to view $X \times Y$ as a quasi-projective variety.

Example 3.5. (Blowup of $\mathbb{A}^n$)

By the above, $\mathbb{A}^n \times \mathbb{P}^{n-1}$ is a quasi-projective variety, as $\mathbb{A}^n$ is an open subset of $\mathbb{P}^n$. Take coordinates $x_1, \ldots, x_n$ for $\mathbb{A}^n$, and $y_1, \ldots, y_n$ for $\mathbb{P}^{n-1}$. Then let

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

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

$$\phi((x_1, \ldots, x_n)(y_1 : \ldots : y_n)) = (x_1, \ldots, x_n),$$

the projection onto $\mathbb{A}^n$. This is a morphism. We make a couple of observations:

1. If $p \in \mathbb{A}^n \setminus \{0\}$, then $\phi^{-1}(p)$ consists of one point. Indeed, let $p = (a_1, \ldots, a_n)$ with, say, $a_i \neq 0$. If

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

then for $j \neq i$, $a_i b_j - a_j b_i = 0$, so $b_j = a_j b_i / a_i$. So $b_1, \ldots, b_n$ are completely determined up to scaling. If we take $b_i = a_i$ for all i, then we see that

$$\phi^{-1}(p) = \{((a_1, \ldots, a_n)(a_1 : \ldots : a_n))\}.$$

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

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

3. The points of $\phi^{-1}(0)$ are in one-to-one correspondence with lines through the origin in $\mathbb{A}^n$.

For $n = 2$ we have the following picture: instead of taking $\mathbb{A}^2$, we somehow replace the origin with a copy of $\mathbb{P}^1$.

We prove the third statement. A line L through the origin can be parametrized by $\ell : \mathbb{A}^1 \to \mathbb{A}^n$, such that $\ell(t) = (a_1 t, \ldots, a_n t)$ for some $a_1, \ldots, a_n$ not all 0. For $t \neq 0$,

$$\begin{aligned} \phi^{-1}(a_1 t, \ldots, a_n t) &= ((a_1 t, \ldots, a_n t)(a_1 t : \ldots : a_n t)) \\ &= ((a_1 t, \ldots, a_n t)(a_1 : \ldots : a_n)). \end{aligned}$$

This is the lift of $L \setminus \{0\}$, which is given parametrically by

$$t \mapsto ((a_1 t, \ldots, a_n t)(a_1 : \ldots : a_n)).$$

This takes $\mathbb{A}^1 \setminus \{0\}$ to $\phi^{-1}(\mathbb{A}^0 \setminus \{0\}) \subseteq X$. This extends to all of $\mathbb{A}^1$, and also $\overline{\phi^{-1}(L \setminus \{0\})}$ is the image of this parametrisation.

Finally, we can show that X is irreducible. Indeed $X = (X \setminus \phi^{-1}(0)) \cup \phi^{-1}(0)$. The first set we showed is homeomorphic to $\mathbb{A}^n \setminus \{0\}$, and hence is irreducible (an open subset of an irreducible space is irreducible). But every point in $\phi^{-1}(0)$ is in the closure of $X \setminus \phi^{-1}(0)$ by the proof of property 3, so $X \setminus \phi^{-1}(0)$ is dense in X.

Now I claim if $U \subseteq X$ is a dense open set and U is irreducible, then X is irreducible. Indeed if $X = Z_1 \cup Z_2$ for Z_1, Z_2 closed, then $U = (Z_1 \cap U) \cup (Z_2 \cap U)$. These are closed in U under the induced topology, so as U is irreducible, we may assume $U = Z_1 \cap U$. So $U \subseteq Z_1$, hence $\bar{U} \subseteq Z_1$. But since $\bar{U} = X$, by the density of U we have $X = Z_1$.

Thus the blow-up of X is irreducible.

The blow-up is a useful tool.

Definition 3.8. 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 $\hat{Y} = \overline{\phi^{-1}(Y \setminus \{0\})} \subseteq X$.

Example 3.6.

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

$$Y = Z(x_2^2 - (x_1^3 - x_1^2)).$$

This has something interesting going on at the origin: it intersects it twice. The blow up lives in $X \subseteq \mathbb{A}^2 \times \mathbb{P}^1$, and is the zero set of $x_1 y_2 - x_2 y_1 = 0$.

We work in two coordinate patches: $U_1 = \{y_1 \neq 0\}$, and $U_2 = \{y_2 \neq 0\}$. In U_2, we can set $y_2 = 1$ and the equation for X becomes $x_1 = x_2 y_1$. Then

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

This is isomorphic to $Z(x_2^2 - (x_2^3 y_1^3 + x_2^2 y_1^2)) \subseteq \mathbb{A}^2$. Indeed, in terms of coordinate rings

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

But note that the latter polynomial is $x_2^2(1 - x_2 y_1^3 - y_1^2)$. Note that $\phi^{-1}(0) \cap U_2 = Z(x_2)$. The blow up $\hat{Y} \cap U_2 = \overline{\phi^{-1}(Y \setminus \{0\})} \cap U_2$ is now given by the equation $1 - x_2 y_1^2 - y_1^2$ in $\mathbb{A}^2$. In particular, we gain two new points $(x_2, y_1) = (0, \pm 1)$.

For thoroughness, we also consider $\hat{Y} \cap U_1$, where $y_1 = 1$. Then $x_2 = x_1 y_2$, so we can eliminate x_2 from the equation to get $x_1^2 y_2^2 - (x_1^3 + x_1^2) = x_1^2(y_2^2 - x_1 - 1)$. So $\hat{Y} \cap U_1$ has equation $y_2^2 - x_1 - 1 = 0$. This is the same as in the previous blow-up.

3.1 Rational Maps

Let X, Y be varieties. Consider the equivalence relation on pairs (U, f) where $U \subseteq X$ is open, and $f : U \to Y$ is a morphism. Then

$$(U, f) \sim (V, g) \text{ if } f|_{U \cap V} = g|_{U \cap V}.$$

We can check that this is an equivalence relation.

Definition 3.9. A *rational map* $f : X \dashrightarrow Y$ is an equivalence relation of a pair.

Example 3.7.

If X is affine and $q = f/g \in K(X)$, then we have a morphism $\phi : X \setminus Z(g) \to \mathbb{A}^1$. This defines a rational map to $\mathbb{A}^1$.

Definition 3.10. A *birational map* is a rational map $f : X \dashrightarrow Y$ with a rational inverse $g : Y \to X$, such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$ as rational maps.

Remark. We cannot always compose rational maps. Suppose we are given $f : X \dashrightarrow Y$, $g : Y \dashrightarrow Z$ with $f : U \to Y$ and $g : V \to Z$.

If $f(U) \subseteq X \setminus V$, then we cannot compose. If this is not the case, then $f^{-1}(Y \setminus V) \subset U$ 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 that the ability to compose may depend on the representative for f, g. One can show that if $f : X \dashrightarrow Y$ is a birational map, then there 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 3.11. We say varieties X, Y are *birationally equivalent* if there exists a birational map $f : X \dashrightarrow Y$. Equivalent, there exists $U \subseteq X$, $V \subseteq Y$, open subsets with $U \cong V$.

Example 3.8.

Take $\varphi : X \to \mathbb{A}^n$, the blow-up of $\mathbb{A}^n$ at $0 \in \mathbb{A}^n$. This is a birational map since it induces an isomorphism $\varphi : \varphi^{-1}(\mathbb{A}^n \setminus \{0\}) \to \mathbb{A}^n \setminus \{0\}$.

However $\varphi^{-1} : \mathbb{A}^n \to X$ is not a morphism, and is only defined on $\mathbb{A}^n \setminus \{0\}$.

Remark. $f : X \dashrightarrow Y$ is a *dominant* rational map, i.e. if $U \xrightarrow{f} Y$ is a representative for f, then $f(U)$ is dense in Y.

Definition 3.12. 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 $f|_{U\cap V} = g|_{U\cap V}$. This is the field of fractions of $A(X)$ if X is affine.

If f is dominant, we obtain a map $f^\# : K(Y) \to K(X)$ by $(V,\varphi) \mapsto (f^{-1}(V) \cap U, \varphi \circ f)$. Note that $f^{-1}(V) \cap U$ is non-empty, since $V \cap f(U) \neq \emptyset$ by density of $f(U)$.

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

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

are inverse maps, so $K(X) \cong K(Y)$. In fact the converse is true: if $K(X) \cong K(Y)$, then X and Y are birational to each other.

Example 3.9.

Look at $0 \in Y \subseteq \mathbb{A}^n$, then $\hat{Y} \to Y$, the blow-up of Y at 0, is a birational morphism.

4 Tangent Spaces, Singularities and Dimension

Recall that given an equation $f(x_1, \dots, x_n) = 0$ in $\mathbb{R}^n$, where X is the solution set and $p \in X$, the tangent space to X is the orthogonal complement to $(\nabla f)(p)$, i.e. the tangent space to X at p is

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

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

Definition 4.1. If $X \subseteq \mathbb{A}^n$ is an affine variety with $I = I(X) = \langle f_1, \dots, f_r \rangle$, $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$ we define for $p \in X$, the *tangent space* to X at p by

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

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

Example 4.1.

Set $I = \langle x_2^2 - x_1^3 \rangle \subset \mathbb{K}[x_1, x_2]$, and $X = Z(I)$. Let $p = (a_1, a_2)$. Then

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

Then we see that $\dim_{\mathbb{K}} T_pX = 1$, unless $p = (0, 0)$ in which case it is 2.

Definition 4.2. 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 $\dim_{\mathbb{K}} T_pX > \dim X$ in X.

Lemma 4.1. *The set $\{p \in X \mid \dim_{\mathbb{K}} T_pX \geq k\}$ is a closed subset of X, for all k.*

Proof: The key property is rank-nullity. Note that T_pX is the null space of

$$\begin{pmatrix} \partial f_1/\partial x_1 & \cdots & \partial f_1/\partial x_n \\ \vdots & \ddots & \vdots \\ \partial f_r/\partial x_1 & \cdots & \partial f_r/\partial x_n \end{pmatrix},$$

where $I(X) = \langle f_1, \dots, f_r \rangle$. But the dimension of the null space plus the rank of the matrix is n, so

$$\dim T_pX \geq k \iff n - \text{rank} \geq k \iff \text{rank} \leq n - k.$$

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

But these minors are simply polynomial equations. Thus the set

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

Hence this set is closed.

Recall that $p \in X$ is singular if $\dim_K T_pX \geq \dim X$, which is the infimum of $\dim T_pX$. This lemma tells us that the set of singular points is a proper closed subset.

Example 4.2.

Look at $y^2 - x^3 = 0$. Then the Jacobian matrix is $(2y, -3x^2)$, which vanishes when $(x, y) = (0, 0)$.

Now consider the cone $x^2 + y^2 - z^2 = 0$. Then $J = (2x, 2y, -2z)$, vanishing at the origin.

Note we only care about where the Jacobian vanishes on the variety, not in the general space.

4.1 Intrinsic Characterization of the Tangent Space

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

Definition 4.3. A *derivation centred at* p is a map $D : A(X) \to \mathbb{K}$ such that:

(i) $D(f+g) = D(f) + D(g)$.

(ii) $D(f \cdot g) = \phi_p(f)D(g) + D(f)\phi_p(g)$.

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

Denote by $\text{Der}(A(X), p)$ to be the set of derivations centred at p. Note that $\text{Der}(A(X), p)$ is a $\mathbb{K}$-vector space.

Theorem 4.1. *$T_pX \cong \mathrm{Der}(A(X), p)$ as $\mathbb{K}$-vector spaces.*

Proof: Suppose $(v_1, \ldots, v_n) \in T_pX$, so if $I(X) = \langle f_1, \ldots, f_r \rangle$, then

$$\sum_{i=1}^{n} v_i \frac{\partial f_j}{\partial x_i}(p) = 0,$$

for all j. Define $\mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}$ by

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

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

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

since $f_j(p) = 0$ as $p \in X$. Thus we get a well-defined $\mathbb{K}$-linear map

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

We can check that this is a derivation. Now we want to generate tangent vectors from derivations.

Given $D \in \mathrm{Der}(A(X), p)$, define $v_i = D(x_i)$. By repeated use of the Leibniz rule,

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

For example, for $n = 2$,

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

Therefore we find

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

but $f_j \in I(X)$, so $D(f_j) = 0$. Hence

$$\sum_{i=1}^{n} v_i \frac{\partial f_j}{\partial x_i}(p) = 0$$

for all j, so $(v_1, \ldots, v_n) \in T_pX$.

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

Definition 4.4. Let X be a variety, and $p \in X$. We define the *local ring* to X at p to be

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

where $(U, f) \sim (V, g)$ if $f|_{U \cap V} = g|_{U \cap V} \subseteq K(X)$, the field of functions.

Example 4.3.

1. If $X \subseteq \mathbb{A}^n$ is an affine variety,
$$\mathcal{O}_{X,p} = \left\{ \frac{f}{g} \in K(X) \mid g(p) \neq 0, f, g \in A(X) \right\}.$$

2. If $X \subseteq \mathbb{P}^n$ is projective, then
$$\mathcal{O}_{X,p} = \left\{ \frac{f}{g} \mid f, g \in \frac{\mathbb{K}[x_1, \ldots, x_n]}{I(X)}, g(p) \neq 0, f, g \text{ hom, same degree} \right\},$$
as a subset of $K(X)$.

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

$$(U, f) + (V, g) = (U \cap V, f|_{U \cap V} + g|_{U \cap V}),$$

and multiplication defined similarly. We can 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 4.5. A ring A with a unique maximal ideal is called a *local ring*.

Theorem 4.2. *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 is surjective since constants are regular functions, and injective by the definition of m_p. Then we can define the $\mathbb{K}$-vector space structure 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 that $\operatorname{Der}(A(X), p) \subseteq (m_p/m_p^2)^*$. Given $D \in \operatorname{Der}(A(X), p)$, we define $\phi_D : m_p/m_p^2 \to \mathbb{K}$ as follows: for $f, g \in A(X)$, $g(p) \neq 0$ and $f(p) = 0$, with

$$\left(X \setminus Z(g), \frac{f}{g}\right) \in m_p \subseteq \mathcal{O}_{X,p},$$

we set

$$\phi_D\left(\frac{f}{g}\right) = D\left(\frac{f}{g}\right) = \frac{g(p)D(f) - f(p)D(g)}{g(p)^2} = \frac{D(f)}{g(p)},$$

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

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

Thus $\phi_D(m_p^2) = 0$, so we obtain a well defined map $\phi_D : m_p/m_p^2 \to \mathbb{K}$. Conversely, if we are given $\phi : m_p/m_p^2 \to \mathbb{K}$, for $p = (a_1, \ldots, a_n) \in X \subseteq \mathbb{A}^n$, note that $x_i - a_i \in m_p$ for all i. Then define

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

This is sufficient to determine D_ϕ as before.

Example 4.4.

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

$$\frac{m_p}{m_p^2} = \frac{(X_1, \ldots, X_n)}{(X_1, \ldots, X_n)^2}.$$

Definition 4.6. If X is any variety, the *Zariski tangent space* to X at p is

$$T_pX = (m_p/m_p^2)^*,$$

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

Theorem 4.3. *Any variety has an open cover by affine varieties.*

Note if $X \subseteq \mathbb{P}^n$ is projective, then $\{U_i \cap X \mid 0 \leq i \leq n\}$ is a cover of X by affine varieties.

Proof: Consider the most general case, where X is quasi-projective. Then each $U_i \cap X$ is quasi-affine, so it is enough to show that each quasi-affine variety is covered by affine varieties.

Let $p \in X$. We will find an affine neighbourhood of p in X. Then $\bar{X} \subseteq \mathbb{A}^n$, the closure, is an affine variety, and $Z = \bar{X} \setminus X$ is closed in $\bar{X}$. Choose $f \in I(Z)$ with $f(p) \neq 0$. Then $\langle f \rangle \subseteq I(X)$, so

$$Z(f) \subseteq Z(I(Z)) = Z,$$

so $p \in \bar{X} \setminus Z(f) \subseteq \bar{X} \setminus Z = X$.

But $\bar{X} \setminus Z(f)$ can be identified with the closed subset of $\mathbb{A}^{n+1}$ given by $Z(I(\bar{X}), yf - 1)$, as in the first example sheet.

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

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

and $p \in X$ 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 that the dimension, and singularity is intrinsic to X.

We can alternatively define dimension in the Zariski tangent space as follows.

Definition 4.7. if $F/\mathbb{K}$ is a finitely generated field extension, then the *transcendence degree* of $F/\mathbb{K}$, written as $\mathrm{trdeg}_K F$, is the cardinality of a transcendence basis.

Definition 4.8. If A is a ring, the *Krull dimension* of A is the largest n such that there exists a chain of prime ideals

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

Definition 4.9. If X is a topological space, the *Krull dimension* of X is the largest n such that there exists a chain of irreducible subsets

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

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 $\dim A(X)$ is equal to the Krull dimension of X. We can check there is a one-to-one correspondence between prime ideals of $A(X)$ and irreducible closed subsets of X.

Theorem 4.4. *If X is a variety, then*

$$\dim X = \operatorname{trdeg}_{\mathbb{K}} K(X) = \textit{Krull dimension of } X = \textit{Krull dimension of } \mathcal{O}_{X,p},$$

for any $p \in X$.

Proof: This is by dimension theory. It is non-examinable.

Example 4.5.

In the first example sheet, we showed that if

$$X = Z(f) \subseteq \mathbb{A}^2,$$

then the closed subsets of X are X, and the finite subsets of X. Thus the Krull dimension of X is 1.

5 Curves

Definition 5.1. An (algebraic) *curve* is a variety C with $\dim C = 1$.

Definition 5.2. Let $C \subseteq \mathbb{P}^n$ be a projective non-singular curve. We define Div$C$ to be the free abelian group generated by points of C. This is called the group of *divisors* of C.

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

The point of this definition is as follows. Consider $C = \mathbb{P}^1$. An element of $K(C)$ is a ratio

$$\frac{f(x_0, x_1)}{g(x_0, x_1)},$$

where f, g are homogeneous polynomials of the same degree. We can factor

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

where $\sum m_i = \sum n_j = d$. Let $p_i = (a_i : b_i)$, and $q_j = (c_j : d_j)$. Then 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 f/g is

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

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

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

We can see that $\operatorname{Cl} \mathbb{P}^1 = \mathbb{Z}$.

In order for this definition to be sensible, for any non-singular curve $f \in K(X)$, we want to define the order of 0 of a pole at $p \in X$.

Lemma 5.1. *Let A be a ring, M a finitely generated A-module and $I \subset A$ an ideal such that $IM = M$. Then there exists $x \in A$ such that $x \equiv 1 \mod I$, and $xM = 0$.*

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 ϕ to be the identity map. This means multiplication by $1 + a_1 + a_2 +$

$\cdots + a_n$ is the zero homomorphism of M. Then taking this to be x, $x \equiv 1 \mod I$ and $xM = 0$.

Theorem 5.1 (Nakayama's Lemma)**.** *Let A be a local ring with maximal ideal m. Let $I \subseteq m$ be an ideal. Then for finitely generated M, $IM = M$ implies $M = 0$.*

Proof: As before, there exists $x \in A$ with $xM = 0$ and $x \equiv 1 \mod I$, so $x \equiv 1 \mod m$. Thus $x \notin m$. But this implies x is invertible, otherwise $\langle x \rangle \neq A$, and hence $\langle x \rangle \subseteq m$.

But then $M = x^{-1}(xM) = 0$.

Note all $x \in A \setminus m$ for a local ring A are invertible.

Corollary 5.1. *Let A be a local ring with maximal ideal m, M a finitely generated A-module, and $I \subseteq m$ an ideal. Then if $M = IM + N$ for a submodule $N \subseteq M$, we have $M = N$.*

Proof: Note that M/N satisfies

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

If $M = IM + N$, we get

$$I\left(\frac{M}{N}\right) = \frac{M}{N} \implies \frac{M}{N} = 0.$$

Corollary 5.2. *A is 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 $\bar{x}_1, \ldots, \bar{x}_n \in M/mM$ 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, since

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

is well-defined.

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

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

is surjective, so $M = N + mM$. By the previous corollary, $M = N$.

Corollary 5.3. *Let $C \subseteq \mathbb{P}^n$ be a non-singular projective curve. Then*

$$\{(U, f) \mid f(p) = 0\} = m_p \subseteq \mathcal{O}_{C,p}$$

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, say C'. This does not change $\mathcal{O}_{C,p}$. Then

$$\mathcal{O}_{C',p} = \left\{ \frac{f}{g} \mid f, g \in A(C') = \frac{\mathbb{K}[x_1, \dots, x_n]}{I(C')}, g(p) \neq 0 \right\} \subseteq K(C').$$

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

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

Indeed, one way is because if $f/g \in J$, then $g(f/g) = f \in J$, so $f \in A(C') \cap J$. Conversely, if $f \in A(C') \cap J$, then $f/g = 1/g \cdot f \in J$.

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 set of generators of $A(C') \cap J$ 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 the map $\mathcal{O}_{C,p}/m_p \to \mathbb{K}$ by $f + m_p \mapsto f(p)$. Thus m_p/m_p^2 is a one-dimensional vector space over $\mathcal{O}_{C,p}/m_p$, hence by the previous corollary 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!).

Remark. Let $t \in m_p$ be a generator. Then we get a chain of ideals

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

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

Also, consider

$$I = \bigcap_{k=1}^{\infty} (t^k).$$

Then clearly $t \cdot I = I$, so $m_p \cdot I = I$, hence $I = 0$.

Corollary 5.4. *If $f \in \mathcal{O}_{C,p} \setminus \{0\}$, there exists a unique $\nu \geq 0$ such that $f \in (t^\nu)$, $f \notin (t^{\nu+1})$.*

Definition 5.3. Define $\nu : \mathcal{O}_{C,p} \setminus \{0\} \to \mathbb{Z}$ by $\nu(f) = \nu$, as above.

We can show that ν satisfies the following:

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

We can extend ν to a map

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

by $\nu(f/g) = \nu(f) - \nu(g)$. ν is an example of a *discrete valuation*. It essentially tells us the order of the zero of f/g at p.

Definition 5.4. Let K be a field. A *discrete valuation* on K is a function $\nu : K^\times \to \mathbb{Z}$ such that:

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

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

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

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

a subring of K. Moreover, we can take $m = \{f \in K^\times \mid \nu(f) \geq 1\} \cup \{0\}$, which is the unique maximal ideal of R. If $f \in R \setminus m$, then $\nu(f) = 0$, so $\nu(f^{-1}) = 0$, and so $f^{-1} \in R$.

Example 5.1.

1. Take $R = \mathcal{O}_{C,p} \subseteq K = K(C)$. Then ν is the discrete valuation we defined.
2. Let $p \in \mathbb{Z}$ be prime, and $K = \mathbb{Q}$. Then any rational number can be written as $\frac{a}{b}p^\nu$, with $(a,p) = (b,p) = 1$. Then define

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

This is a discrete valuation, with discrete valuation ring

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

These are the p-adic valuation and p-adic integers, respectively.

3. Take $K = \mathbb{K}(x)$, and $a \in \mathbb{K}$. Then

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

where f, g are relatively prime to $x - a$. Here the DVR is $\mathcal{O}_{\mathbb{A}^1,0}$.

4. Let $K = \mathbb{K}(X)$, and define

$$\nu(f/g) = \deg g - \deg f.$$

This is the "order" of the zero at ∞.

The setup is follows: let $C \subseteq \mathbb{P}^n$ be a projective non-singular curve. Then each point $p \in C$ gives a valuation $\nu_p : K(C)^\times \to \mathbb{Z}$, with DVR $\mathcal{O}_{C,p}$. For $f \in K(C)^\times$, we define the divisor of zeros and poles of f to be

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

We need to check this is finite.

Note f is represented on some open subset $U \subseteq C$ by g/h, for homogeneous polynomials g, h. We shrink U by removing $Z(g)$, $Z(h)$. Now if $p \in U$, $f = g/h \in \mathcal{O}_{C,p}$ 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 the fact that $\dim C = 1$, so the irreducible sets are C and singleton sets.

Definition 5.5. The group of *principal divisors* on C is

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

This is a subgroup, as $(fg) = (f) + (g)$, and $(f^{-1}) = (-f)$.

The (divisor) *class group* is

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

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

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

Then we obtain a morphism $f : U \to \mathbb{P}^n$ by $p \mapsto (f_0(p) : \ldots : f_n(p))$.

Theorem 5.2. *$f : U \to \mathbb{P}^n$ 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's 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 the maximal ideal $m_p \subseteq \mathcal{O}_{C,p}$. So $\nu_p(t) = 1$. Then $\nu_p(t^{-m} f_i) = \nu_p(f_i) - m$, so $\nu_p(t^{-m} f_i) = 0$ for some i, and $\nu_p(t^{-m} f_j) \geq 0$. Thus $t^{-m} f_0, \ldots, t^{-m} f_p \in \mathcal{O}_{C,p}$ are regular functions which do not simultaneously vanish at p.

Hence in some neighbourhood V of p, we obtain a morphism $f_p : V \to \mathbb{P}^n$ by $q \mapsto ((t^{-m} f_0)(q), \ldots, (t^{-m} f_n)(q))$. This agrees with f on the intersection by rescaling, so gluing gives a morphism.

Proposition 5.1. *Let $f : X \to Y$ be a non-constant morphism between projective non-singular curves. Then:*

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

(ii) 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:

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

(ii) If $\phi \in K(Y)$, ϕ defines a regular function on some open $U \subseteq Y$, i.e. $\phi : U \to \mathbb{K}$.

Then $\phi \circ f$ makes sense, provided $f(X) \not\subseteq Y \setminus U$. But $f(X)$ is irreducible, so f is constant if $f(X) \not\subseteq Y \setminus U$. Thus $\phi \circ f$ makes sense as a rational function on X. Thus $K(Y) \to K(X)$ exists, and is automatically an injection since both are fields.

We omit the proof of finiteness (the idea is to look at the transcendence degrees; both are 1).

Definition 5.6. Suppose $f : X \to Y$ is a non-constant morphism between projective non-singular curves. Let $p \in Y$, $m_p = (t) \subseteq \mathcal{O}_{Y,p}$, where t is 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 5.3. *Let $f : X \to Y$ be as above. Then for $p \in Y$,*

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

is the degree of f.

The proof is omitted, however the theorem is crucial.

Example 5.2.

1. Suppose $\operatorname{char} \mathbb{K} \neq 2$, and take $f : \mathbb{P}^1 \to \mathbb{P}^1$ by $(u : v) \mapsto (u^2 : v^2)$. Setting $v = 1$, this gives a morphism $\mathbb{A}^1 \to \mathbb{A}^1$ by $u \mapsto u^2$.

   If $p \in \mathbb{A}^1$, then $t = u - p$ is a local parameter at p, and $t \circ f = u^2 - p = (u-q)(u+q)$ where $q^2 = p$, so $e_q = e_{-q} = 1$, hence $\deg f = e_q + e_{-q} = 2$.

   If $p = 0$, then $f^{-1}(p) = \{0\}$, and $e_0 = \nu_0(u^2) = 2$.

   Looking as function fields, letting $K(\mathbb{P}^1) = \mathbb{K}(u)$, then this map is $\mathbb{K}(u) \to \mathbb{K}(u)$ by $u \mapsto u^2$.

2. Look at $\operatorname{char} \mathbb{K} = 2$, and $f : \mathbb{P}^1 \to \mathbb{P}^1$ by $(u : v) \mapsto (u^p : v^p)$. Setting $v = 1$, this is $u \mapsto u^p$.

   Here $f^{-1}(q) = \{r\}$, where $r^p = q$ is unique. Then $t = u - q$, and $t \circ f = u^p - q = (u - r)^p$.

Let X be a projective non-singular curve, and $f \in K(X)^\times$. This gives a morphism $X \supseteq U \overset{(f,1)}{\to} \mathbb{P}^1$, where U is the open set on which f is regular.

This extends to $f : C \to \mathbb{P}^1$, non-constant as long as $f \notin \mathbb{K}$.

We can either extend by $p \mapsto (f(p) : 1)$ or $(g(p) : h(p))$, but both can be ill-defined, so we need to use our theorem from last time somewhere. Then note that

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

Thus if we define

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

then

$$\deg(f) = \deg f - \deg f = 0.$$

Thus every principal divisor is degree 0. So the homomorphism $\deg : \mathrm{Div} C \to \mathbb{Z}$ descends to $\deg : \mathrm{Cl} C \to \mathbb{Z}$, and this is surjective as $\deg p = 1$.

5.1 Linear Systems

Let $D \in \mathrm{Div} C$, so

$$D = \sum n_i \cdot p_i.$$

We say that 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 5.2. *$\mathcal{L}(D)$ is a vector space.*

Proof: Note that $f \in \mathcal{L}(D) \implies cf \in \mathcal{L}(D)$ for $c \in K, c \neq 0$ since $(f) = (cf)$.

If $f, g \in \mathcal{L}(D)$, where f, g are non-zero and $f + g \neq 0$, 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 5.4. *$\mathcal{L}(D)$ is a finite-dimensional vector space, and $L(0) = \mathbb{K}$. Furthermore, $\dim_{\mathbb{K}} \mathcal{L}(D) \leq \deg D + 1$, for $\deg D \geq 0$.*

Proof: We prove this by induction on $\deg D$. If $\deg D < 0$, there are no effective divisors linearly equivalent to D since $\deg(D + (f)) = \deg D < 0$, so $\mathcal{L}(D) = 0$.

Suppose that $\deg D \geq 0$, and write

$$D = \sum_{i=1}^{m} n_i p_i.$$

Pick $p \in C \setminus \{p_1, \ldots, p_m\}$. Consider the map

$$\begin{aligned} \lambda : \mathcal{L}(D) &\to \mathbb{K} \\ f &\mapsto f(p), \end{aligned}$$

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 $f \in \operatorname{Ker} \lambda$, 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 $\mathcal{L}(D - p) \subseteq \mathcal{L}(D)$, since if $D - p + (f)$ is effective, so is $D + (f)$. Thus $\mathcal{L}(D - p) = \operatorname{Ker} \lambda$, 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 the regular functions on C are constants.

Definition 5.7. Given a divisor D, we define the *complete linear system* associated to D to be

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

5.2 Morphisms to Projective Space

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

Definition 5.8. Let $f : C \to \mathbb{P}^n$ be a morphism. Let $H \subseteq \mathbb{P}^n$ be a hyperplane, with $f(C) \not\subseteq H$.

We define $f^*H \in \mathrm{Div}C$ as follows. Let $H = Z(\phi)$, with ϕ a linear homogeneous polynomial, and choose ψ linear homogeneous so that $H' = Z(\psi)$ satisfies

$$f^{-1}(H) \cap f^{-1}(H') = \emptyset.$$

Define

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

Insert cool diagram.

Remark. This is independent of the choice of ψ, as

$$\frac{\phi}{\psi'} = \frac{\phi}{\psi} \cdot \frac{\psi}{\psi'},$$

and the latter does not affect the coefficient of vanishing.

Now let's relate this to morphisms. Let $f_0, \ldots, f_n \in \mathcal{L}(D)$ be such that:

(i) the f_i aren't all 0,

(ii) for all $p \in C$, there exists $a_0, \ldots, a_n \in \mathbb{K}$ such that the coefficient of p in $D + (\sum a_i f_i)$ 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 $\sum a_i x_i = 0$.

Theorem 5.5. $f^*H = D + (\sum a_i f_i)$.

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

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

Necessarily, $f_0, \ldots, f_n$ do not have a pole at p, since otherwise $D + (f_i)$ has a negative coefficient for p. Thus, $f_0, \ldots, f_n$ are regular in a neighbourhood of p, so we can write $f = (f_0 : \ldots : f_n)$ in this neighbourhood. Now

$$\nu_p \left(\frac{\phi}{\psi} \circ f \right) = \nu_p \left(\frac{\sum a_i f_i}{\sum b_i f_i} \right) = \nu_p \left(\sum a_i f_i \right),$$

since $\sum b_i f_i$ is non-vanishing and regular at p. But this is precisely the coefficient of p in $D + (\sum a_i f_i)$.

If p appears in D with coefficient m, then

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

for any $b_0, \dots, b_n \in \mathbb{K}$. There is also some choice of $b_0, \dots, b_n$ with equality, by assumption.

In a neighbourhood of p, the morphism f is given by

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

where t is a local parameter of p. Thus the coefficient of p in f^*H is

$$\nu_p\left(\frac{\sum a_i t^m f_i}{\sum b_i t^m f_i}\right) = \nu_p\left(\sum a_i t^m f_i\right) = m + \nu_p\left(\sum a_i f_i\right),$$

which is the coefficient of p in $D + (\sum a_i f_i)$. Thus

$$f^*H = D + \left(\sum a_i f_i\right).$$

The picture so far: we know $f_0, \dots, f_n$ span a subspace $V \subseteq \mathcal{L}(D)$ .This gives a linear subspace

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

For a divisor $D = \sum a_i p_i$ with $a_i \neq 0$ and p_i distinct, we define the *support* of D to be

$$\mathrm{Supp}(D) = \{p_1, \dots, p_n\}.$$

We say $\mathcal{D}$ is *base-point free* if for all $p \in C$, there exists $D' \in \mathcal{D}$ with $p \notin \mathrm{Supp} D'$. This is the same as assumption (ii) in the above.

In this case, the theorem applies and we obtain $f : C \to \mathbb{P}^n$ with the property that $\mathcal{D} = \{f^*H \mid H \subseteq \mathbb{P}^n \text{ a hyperplane}\}$.

The converse is as follows. Suppose $f : C \to \mathbb{P}^n$ be a morphism. Set $D = f^*Z(x_0)$, assuming $f(C) \nsubseteq Z(x_0)$.

Let $f_1 \in K(C)$ be given by

$$f_1 = \frac{x_1}{x_0} \circ f,$$

which is a rational function on C regular on $C \setminus f^{-1}(Z(x_0))$. Then $f = (f_0 : f_1 : \dots : f_n)$ 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 $f_0, \ldots, f_n \in \mathcal{L}(D)$.

Also by the previous theorem, $f^*Z(\sum a_i x_i) = D + (\sum a_i f_i) \in \mathcal{D}$. Also $\mathcal{D}$ is base-point free, since given $p \in C$, we 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 '$H \cap C$ with multiplicity', and then $\mathcal{D} = \{H \cap C \mid H \subseteq \mathbb{P}^n \text{ a hyperplane}\}$.

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

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

Definition 5.9. 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 degree.

Example 5.3.

Let $f : C \hookrightarrow \mathbb{P}^2$ identify C with $Z(\phi)$, where ϕ has degree d. In this case, the degree of f is d.

To check this, we need to compare the coefficients in f^*L with the multiplicity of zeroes of $\phi|_L$.

Theorem 5.6. *Let $f : C \to \mathbb{P}^n$ be a morphism, $H \subseteq \mathbb{P}^n$ a hypersurface with $f(C) \not\subseteq H$, and $H = Z(\phi)$, where $\deg \phi = e$. Then $\deg f^*H = (\deg f) \cdot e$.*

Proof: Choose some x_i such that $f(C) \not\subseteq Z(x_i)$. Then ϕ/x_i^e is a rational function in $\mathbb{P}^n$, and

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

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

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

Let $C, C' \subseteq \mathbb{P}^2$ be curves of degree d and e respectively. Then the number o points in $C \cap C'$, assuming $C \neq C'$, calculated with multiplicity 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 $p = C \cap C'$, its multiplicity is the coefficient of p in f^*C'. If C is singular then we 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. for all $p \in C$, there exists $D' \in |D|$ with $p \notin \mathrm{Supp} D'$.

Then by choosing $f_0, \ldots, f_n \in \mathcal{L}(D)$ spanning $\mathcal{L}(D)$, we obtain a morphism $f = (f_0, \ldots, f_n) : C \to \mathbb{P}^n$. When is this an embedding?

We can also use a sub-linear system $\mathcal{D} = \mathbb{P}(V) \subseteq |D| = \mathbb{P}(\mathcal{L}(D))$, and choose $f_0, \ldots, f_n \in V$ a spanning set.

Theorem 5.7. *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:*

(i) *$\mathcal{D}$ separates points, i.e. for all $p, q \in C$ distinct, there exists a $D' \in \mathcal{D}$ such that $p \in \mathrm{Supp} D'$, and $q \notin \mathrm{Supp} D'$.*

(ii) *$\mathcal{D}$ separates tangent vectors, i.e. for all $p \in C$, there exists $D' \in \mathcal{D}$ such that the coefficient of p in D' is 1.*

Definition 5.10. We say a divisor D is *very ample* if D induces an embedding into some projective space.

We can rewrite the above as follows:

Theorem 5.8. *D is very ample if, for all $p, q \in C$, not necessarily distinct, we have*

$$\dim |D - p - q| = \dim |D| - 2.$$

Proof: Recall that $\dim |D| = \dim \mathcal{L}(D) - 1$. For any $p \in C$, we have a map $\mathcal{L}(D) \to \mathbb{K}$, which is constructed as follows.

Suppose the coefficient of p in D is n. Then if $f \in \mathcal{L}(D)$, then $\nu_p(t^n \cdot f) = n + \nu_p(f) \geq 0$ by definition of $\mathcal{L}(D)$, where t is uniformizing.

So $t^n f \in \mathcal{O}_{C,p}$, then we define

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

If $f \in \mathrm{Ker}(\mathrm{ev}_p)$, we have $\nu_p(t^n f) \geq 1$, so $\nu_p(f) > -n$. Hence the coefficient of p in $D + (f)$ is at least one, so $(D-p) + (f)$ is effective, so $f \in \mathcal{L}(D-p)$.

Conversely, if $f \in \mathcal{L}(D-p)$, then $(D-p)+(f)$ is effective, so $\nu_p(f) \geq -n+1$, and $\nu_p(t^n \cdot f) \geq 1$, so $f \in \mathrm{Ker}(\mathrm{ev}_p)$. Therefore $\mathcal{L}(D-p) = \mathrm{Ker}(\mathrm{ev}_p)$.

If $|D|$ is base-point free, then $\mathrm{ev}_p : \mathcal{L}(D) \to \mathbb{K}$ is surjective for all p, and conversely. So

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

for all p, if and only if $|D|$ is base-point free.

Now $|D|$ separates point and tangent vectors if and only if $|D-p|$ is base-point free for all $p \in C$. Indeed, if $D' = |D-p|$ does not have q in its support, then $D' + [$ separates p and q if $q \neq p$. If $p = q$, and $p \notin \mathrm{Supp} D'$, then $D' + [$ 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

$$\dim |D-p-q| = \dim |D-p| - 1 = \dim |D| - 2,$$

for all p, q.

The moral is, if we can control $\dim \mathcal{L}(D)$, then we know a lot about embeddings.

6 Differentials and Riemann-Roch

Definition 6.1. 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:

- $\mathrm{d}(bb') - b\,\mathrm{d}b' - b'\,\mathrm{d}b$, for all $b, b' \in B$.
- $\mathrm{d}(b + b') - \mathrm{d}b - \mathrm{d}b'$, for all $b, b' \in B$.
- $\mathrm{d}a$, for all $a \in A$.

Example 6.1.

Consider $\Omega_{\mathbb{K}[x]/\mathbb{K}}$. Then for $f \in \mathbb{K}[x]$, we find

$$\mathrm{d}f = f'(x)\,\mathrm{d}x.$$

Thus $\Omega_{\mathbb{K}[x]/\mathbb{K}}$ is the free $\mathbb{K}[x]$-module with one generator $\mathrm{d}x$.

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

Proposition 6.1. *If L/K is a separable algebraic field extension. Then*

$$\Omega_{L/K} = 0.$$

Here separable means everything in L is a solution to some irreducible polynomial equation $f(\alpha) = 0$ with $f(\alpha) \in K[x]$, and $f'(\alpha) \neq 0$.

Proof: Given $\alpha \in L$, $f(x) \in K[x]$ with $f(\alpha) = 0$, $f'(\alpha) \neq 0$, then

$$0 = f(\alpha) \implies 0 = d(f(\alpha)) = f'(\alpha)\,\mathrm{d}\alpha,$$

so $\mathrm{d}\alpha = 0$ since $f'(\alpha) \neq 0$.

Lemma 6.1. *Let C be a curve, $p \in C$, and t a local (uniformizing) parameter for C at p. Then*

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

Proof: Since t is a local parameter, it is not a constant functions, and thus defines a non-constant map $t : C \to \mathbb{P}^1$, inducing a finite field extension

$$\mathbb{K}(\mathbb{P}^1) = \mathbb{K}(t) \to K(C).$$

This extension is separable. The proof is omitted; for $\operatorname{char}\mathbb{K} = 0$ it is immediate. For positive characteristic, 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 $\alpha \in K(C)$, there exists $f \in \mathbb{K}(t)[x]$ such that $f(\alpha) = 0$, $f'(\alpha) \neq 0$. Write

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

for $f_i(t) \in \mathbb{K}(t)$. Then,

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

where $f'(\alpha) \neq 0$. So dividing, we can solve for $\mathrm{d}\alpha$, getting

$$\mathrm{d}\alpha = g\,\mathrm{d}t \in K(C)\,\mathrm{d}t.$$

Definition 6.2. Let C be a projective non-singular curve, and $\omega \in \Omega_{K(C)/\mathbb{K}}$, $p \in C$. We define $\nu_p(\omega)$ as follows: let $t \in \mathcal{O}_{C,p}$ be a local parameter, and write $\omega = f\,\mathrm{d}t$, for $f \in K(C)$. Define

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

We also define

$$\operatorname{div}(\omega) = \sum_{p \in C} \nu_p(\omega) \cdot p \in \operatorname{Div}C.$$

We say that ω is *regular* at p if $\nu_p(\omega) \geq 0$.

To show this is a sensible definition we need a few lemmas.

Lemma 6.2.

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

(ii) *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.*

(iii) *If $f \in K(C)$ and $\nu_p(f) \neq 0$ in $\mathbb{K}$, then $\nu_p(\mathrm{d}f) = \nu_p(f) - 1$.*

Proof: (i) We 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 $U_1 \cap C$, where rational functions are just ratios of polynomials. If $f = g/h$, $h(p) \neq 0$, we have

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

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

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

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 we can write $f - f(p) = tf_1$, for some $f_1 \in \mathcal{O}_{C,p}$, so

$$\mathrm{d}f = \mathrm{d}(f - f(p)) = \mathrm{d}(tf_1) = f_1\,\mathrm{d}t + t\,\mathrm{d}f_1.$$

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

$$\begin{aligned}\nu_p(\mathrm{d}f) &= \nu_p(\mathrm{d}f - f_1\,\mathrm{d}t) = \nu_p(t\,\mathrm{d}f_1)\\ &= \nu_p(t) + \nu_p(\mathrm{d}f_1) = 1 + \nu_p(\mathrm{d}f_1).\end{aligned}$$

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

(ii) Any two local parameters are related by a unit, so we may write $t' = u \cdot t$, for u a unit, $u \in \mathcal{O}^*_{C,p}$, the group of units in $\mathcal{O}_{C,p}$. Then,

$$\mathrm{d}t' = u\,\mathrm{d}t + t\,\mathrm{d}u,$$

and note $\mathrm{d}u = g \cdot \mathrm{d}t$ for some g with $\nu_p(g) \geq 0$, by the above. So

$$\mathrm{d}t' = (u + tg)\,\mathrm{d}t,$$

where $\nu_p(u + tg) = 0$, 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 note

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

So this is independent of choice of local parameter.

(iii) Suppose $f = t^n u$, where $n = \nu_p(f)$, $u \in \mathcal{O}^*_{C,p}$. 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. Hence $\nu_p(\mathrm{d}f) = \nu_p(f) - 1$.

Proposition 6.2. *If $\omega \in \Omega_{K(C)/\mathbb{K}}$, then $\nu_p(\omega) = 0$ for all but a finite number of p.*

The proof is omitted. Thus, $\operatorname{div}(\omega) \subseteq \operatorname{Div}(C)$.

Proposition 6.3. *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 $p \in C$, we have $\omega = f\,\mathrm{d}t$, $\omega\ = f'\,\mathrm{d}t$, so

$$\omega' = \frac{f'}{f} \cdot \omega,$$

and so we get

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

Definition 6.3. The *canonical class* of a proper, non-singular curve C is the linear equivalence class of $\operatorname{div}(\omega)$ in $\mathrm{Cl}C$, for any $0 \neq \omega \in \Omega_{K(C)/\mathbb{K}}$.

We write the canonical class as K_C.

Definition 6.4. The *genus* of C is $\dim_{\mathbb{K}} \mathcal{L}(K_C)$.

If $\mathbb{K} = \mathbb{C}$, any one uses the Euclidean topology rather than the Zariski topology, then this is the usual notion of genus.

Example 6.2.

Consider $C = \mathbb{P}^1$. Then $K(C) = \mathbb{K}(t)$, where $t = x_0/x_1$.

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

$p_0 \in \mathbb{P}^1 \setminus Z(x_1)$.

At $t = \infty$, we 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 that $t = s^{-1}$, so

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

so $\nu_q(\mathrm{d}t) = -2$. Thus $K_C \sim -2 \cdot q$. Thus $\mathcal{L}(K_C) = \mathcal{L}(-2q) = 0$, and so $g(C) = \dim \mathcal{L}(K_C) = 0$.

Example 6.3.

Consider the plane cubic, which in $\mathbb{A}^2$ is

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

and in $\mathbb{P}^2$ is

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

where $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K}$ are distinct. Take a differential

$$\omega = \frac{\mathrm{d}x}{y}.$$

Differentiating the equation for a plane cubic we get that

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

so

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

In fact $\mathrm{div}(\omega) = 0$. The hardest part is checking the point at infinity, $q = (0 : 1 : 0)$. Thus $K_C \sim 0$, and $\mathcal{L}(K_C) = \mathcal{L}(0) = \mathbb{K}$, so $g(C) = 1$.

6.1 Riemann-Roch

Write $\ell(D)$ for $\dim_{\mathbb{K}} \mathcal{L}(D)$ for $D \in \mathrm{Div} C$.

Theorem 6.1 (Riemann-Roch Theorem)**.**

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

where g is the genus of C.

As a corollary, we get the following:

- If $D = 0$, then $\ell(D) = 1$, so
$$1 - \ell(K_C) = 0 + 1 - g,$$
or $\ell(K_C) = g$, the definition of g.
- If $D = K_C$, then
$$\ell(K_C) - \ell(0) = \deg K_C + 1 - g,$$
so $\deg K_C = 2g - 2$.
- If $\deg D > 2g-2$, then $\deg(K_C - D) = 2g-2-\deg D < 0$, thus $\ell(K_C - D) = 0$, and
$$\ell(D) = \deg D + 1 - g.$$
- If $\deg D > 2g$, then for all $p, q \in C$,
$$\ell(D - p - q) = \ell(D) - 2,$$
by the above. Hence $|D|$ induces an embedding of C in some $\mathbb{P}^n$.

Remark. For $0 \leq \deg D \leq 2g - 2$, the behaviour of $\ell(D)$ can be complicated and unpredictable.

Example 6.4.

If C has genus 0, then every positive degree divisor induces an embedding. For example if $p \in C$, then $|p|$ is very ample, $\ell(p) = 2$, so we get an embedding of C in $\mathbb{P}^1$. Thus $C \simeq \mathbb{P}^1$.

Example 6.5.

Take $g = 1$. If $\deg D = 3$, then D is very ample, and $\ell(D) = 3 + 1 - 1 = 3$. So $|D|$ induces an embedding of C in $\mathbb{P}^2$.

Thus in particular C is isomorphic to a curve of degree 3 in $\mathbb{P}^2$. We can show that $C \simeq Z(f)$ for some homogeneous polynomial of degree 3.

More specifically, fix $p_0 \in C$, and embedding $|3p_0|$. Let $D \in \mathrm{Div} C$ be degree 0. Then,
$$\ell(D + p_0) - \ell(K_C - D - p_0) = \deg(D + p_0) + 1 - g,$$
which simplifies to $\ell(D + p_0) = 1$. So there exists an effective divisor linearly equivalent to $D + p_0$, which necessarily must be $D + p_0 \sim p$. Thus $p - p_0 \sim D$.

Moreover p is unique, as if $p - p_0 \sim p' - p_0$, then $p \sim p'$, so if $p \neq p'$, $\dim |p| = \geq 1$, so $\ell(p) \geq 2$. But $\ell(p) = 1$ by Riemann-Roch.

Hence every divisor class in C of degree 0 can be represented uniquely by $p - p_0$, for some $p \in C$. So

$$\begin{aligned} C &\to \mathrm{Ker}(\deg : \mathrm{Cl} C \to \mathbb{Z}) \\ p &\mapsto p - p_0 \end{aligned}$$

is a bijection. This gives a group structure on C. Hence we can say that $p + q = r$ for $p, q, r \in C$ if

$$(p - p_0) + (q - p_0) \sim (r - p_0).$$

Let's talk about this group structure a bit more, with a geometric description. Consider $p, q \in C \overset{i}{\hookrightarrow} \mathbb{P}^2$. Let L be the line joining p and q, tangent to C at p if $p = q$.

Then we can take the intersection $L \cap C$, which is formally $i^* L = p + q + s$. 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, which intersects at r. Then $s + p_0 + r \sim 3p_0$. So

$$(s - p_0) \sim -(r - p_0).$$

Therefore $(p - p_0) + (q - p_0) \sim (r - p_0)$, so $p + q = r$.

In terms of geometric description, we need a diagram. First take $y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$, taking $p_0 = (0 : 1 : 0)$.

The sum $p + q$ is first by taking the line through p, q to intersect again at s, then taking the intersection of the vertical line through s with the curve again to get $r = p + q$.

Example 6.6.

Let C have genus 2. Then

$$\deg K_C = 2g - 2 = 2,$$

so $\ell(K_C) = 2$. We claim that $|K_C|$ is base-point free, so induces a morphism $f : C \to \mathbb{P}^1$.

Lemma 6.3. *Let C be a projective non-singular curve. If there exists $p, q \in C$, $p \neq q$, $p \sim q$, then $C \cong \mathbb{P}^1$.*

Proof: Consider the linear system $|p|$. Since $q \in |p|$, $\dim |p| \geq 1$, so $\ell(p) \geq 2$. But we have an upper bound $\dim \mathcal{L}(D) \leq \deg D + 1$. So $\ell(p) = 2$.

Hence if $q, r \in C$, then $\dim \mathcal{L}(p - q - r) = 0$, since its degree is -1. Thus $|p|$ induces an embedding of C into $\mathbb{P}^1$, so $C \cong \mathbb{P}^1$.

We now return to our proof of the claim in the above example.

Proof: If $|K_C|$ is not base-point free, then there exists $p \in C$ such that $\ell(K_C - p) = \ell(K_C) = 2$.

However, since $\deg(K_C - p) = 1$, this says there exists $q, r \in |K_C - p|$, $q \neq r$ with $q \sim r$. Hence $C \cong \mathbb{P}^1$.

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

Definition 6.5. 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 6.2. *Let C be a projective non-singular curve of genus $g \geq 3$. Then either:*

- *C is hyperelliptic, or*
- *$|K_C|$ induces an embedding $C \hookrightarrow \mathbb{P}^{g-1}$.*

Proof: $|K_C|$ induces an embedding in $\mathbb{P}^{\ell(K_C)-1} = \mathbb{P}^{g-1}$ if and only if, for all $p, q \in C$,

$$\ell(K_C - p - q) = \ell(K_C) - 2 = g - 2.$$

In any event,

$$\ell(p + q) - \ell(K_C - p - q) = \deg(p + q) + 1 - g = 3 - g.$$

Thus $|K_C|$ induces an embedding if and only if $\ell(p + q) = 1$ for all $p, q \in C$.

Now suppose that K_C does not induce an embedding. Then there exists $p, q \in C$ such that $\ell(p + q) > 1$. If $\ell(p + q) \geq 3$, then for any $r \in C$, $\ell(p + q - r) \geq 2$, so there exists $p_1, p_2 \in |p + q - r|$ distinct. But then $C \cong \mathbb{P}^1$ by our lemma.

Thus $\ell(p+q) = 2$. Note similarly $\ell(p+q-r) = 1$, 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 6.3 (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:*

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

Example 6.7.

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

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

THus,

$$\sum_{p \in C} (e_p - 1) = 2g(C) + 2.$$

Therefore, $2g(C) + 2$ is the number of points $p \in C$ with $e_p > 1$, known as *branch points*.

Index