

Algebraic Geometry

Amy Needham

January 2025

Contents

1	Motivating Examples and Introduction	2
1.1	The Projective Plane	3
2	Algebraic Varieties	4
3	Ideals and the Nullstellensatz	6
4	Coordinate Rings and Morphisms	7
5	Proof of Nullstellensatz	10
6	More Coordinate Rings	11
6.1	From Projective to Affine	15
6.2	Projective Nullstellensatz	16
7	Functions on Projective Varieties	17
7.1	Maps between Projective Varieties	18
8	Tangent Spaces, Singularities and Dimension	21
9	Structure of Algebraic Curves	25
10	Maps between Curves	27
11	Divisors on Curves	30
11.1	Bezout's Theorem	33
12	Differentials	34
13	Differentials on Plane Curves	36
13.1	Plane Cubics	36
14	Riemann-Roch Theorem	39
15	Equations of Curves	40

16 Elliptic Curves 41

17 More Consequences of Riemann Roch 42

1 Motivating Examples and Introduction

Algebraic geometry is the study of the relationship between algebraic (polynomial) equations on the one hand, and the geometry of their solution sets on the other

Example 1.1. Consider the polynomial in 2 variables $f(x, y) = x^2 + y^2 - 1$. Over $\mathbb{R}$, the solution set of this in $\mathbb{R}^2$ is just the unit circle. This has the following properties

1. It is dimension 1 as a real manifold
2. It is smooth everywhere
3. It is "irreducible"

On the algebraic side, $f(x, y) \in \mathbb{R}[x, y]$ and we have the following corresponding properties of the ideal it generates, $I = (f) \subset \mathbb{R}[x, y]$.

1. $\mathbb{R}[x, y]/I$ has transcendence degree 1
2. The "localisations" of $\mathbb{R}[x, y]/I$ are independent of choice of point
3. I is prime

Example 1.2. $x^n + y^n = z^n$. We look for non-trivial solutions over $\mathbb{Z}$ (Fermat's last theorem, at least for $n \geq 3$). Take $n = 2$.

$\{(x, y, z) \mid x^2 + y^2 = z^2\} \xrightarrow{\sim} \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\} \subset \mathbb{Q}^2$.

There is a nice parameterisation of this latter set. Let $P = (0, 1)$ and draw a line of slope t , L_t through P , letting Q_t be the other intersection of L_t with $x^2 + y^2 = 1$. $Q_t = (\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2}) \in \mathbb{Q}^2$ if $t \in \mathbb{Q}$.

Hence we get a bijection $t \longleftrightarrow (\frac{-2t}{1+t^2}, \frac{1-t^2}{1+t^2})$ giving a fully algebraic identification of the solution set in $\mathbb{Q}$

Remark. We notice the following from Example 1.2

1. We care about intersections!
2. We need mathematical structure for ideas like the set of lines through a point, or the tangent line, or maps between solution sets, or dimension, etc

Example 1.3. We have the Fundamental Theorem of Algebra: $p(z) \in \mathbb{C}[z]$ of degree $d > 0$ has exactly d zeros counting multiplicity. This set of zeros is nothing but the intersection of $y = p(x)$ and $y = 0$ in $\mathbb{C}^2$. The geometry of solution sets depends on where we are looking for solutions (eg. the FTA is false in $\mathbb{R}$)

Definition 1.1. We have a few definitions

1. Let $k \rightarrow L$ be an extension of fields. $x \in L$ is **algebraic** over k if there is non-zero $p_x(z) \in k[z]$ such that $p_x(x) = 0$. Otherwise x is **transcendental** over k .
2. L/K is **algebraic** if all elements of L are algebraic over K (For example $\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \mathbb{C}/\mathbb{R}, \mathbb{Q}\{\lambda \in \mathbb{C} \mid \exists k \geq 1 \text{ such that } \lambda^k = 1\}$)
3. Every field k has a (unique up to isomorphism) maximal algebraic extension $\bar{k}$ called its **algebraic closure**. $\bar{k}$ is itself **algebraically closed**, that is every non-constant $p(z) \in \bar{k}[z]$ has a root in $\bar{k}$. We write $k = \bar{k}$ for k algebraically closed

In this course, we will work over an algebraically closed k of characteristic 0 (eg. $\overline{\mathbb{Q}}, \mathbb{C}$)

1.1 The Projective Plane

FTA predicts that two lines in the plane intersect in a point (unless they're parallel). Idea: expand k^2 to add "points at infinity" where parallel lines intersect

Definition 1.2. The **projective plane**, denoted $\mathbb{P}_k^2 = \mathbb{P}^2$ is

$$\{(x, y, z) \in k^3 \setminus \{0\}\} / \{(x, y, z) \sim (\lambda x, \lambda y, \lambda z) \text{ for } \lambda \in k \setminus \{0\} \text{ and } x, y, z \in k\}$$

Denote $[(x, y, z)] = (x : y : z)$.

We have $k^2 \subset \mathbb{P}^2$ by $(x, y) \mapsto (x : y : 1)$ so the "points at infinity" are $\{(x : y : 0)\} \subset \mathbb{P}^2$. For fixed $(x_0 : y_0 : 0)$, we have $(x, y, z) \in (x_0 : y_0 : 0)$ if and only if $z = 0, yx_0 = xy_0$. There is nothing unique about the third component, and doing the same for the first and second gives a (very non-disjoint) covering of $\mathbb{P}^2$ by three copies of k^2 .

A line $ax + by + c = 0$ in k^2 doesn't have a well defined solution in $\mathbb{P}^2$, but its homogenisation $ax + by + cz = 0$ does, by considering multiplying (x, y, z) all by λ

Definition 1.3. A **projective plane curve** is $\{(x : y : z) \in \mathbb{P}^2 \mid F(x, y, z) = 0\}$ for some homogeneous polynomial F .

If $f(x, y) \in k[x, y]$ has **homogenisation** $z^{\deg(f)} f(\frac{x}{z}, \frac{y}{z}) = F(x, y, z)$ is homogeneous of some degree.

If $C = \{f(x, y) = 0\} \subset k^2$ and F the homogenisation of f , we say $\{(x : y : z) \mid F(x, y, z) = 0\}$ is the **projective closure** of C in $\mathbb{P}^2$. For a line, this is the addition of a point determined by the slope

2 Algebraic Varieties

Definition 2.1. Affine n -space over k is denoted by $\mathbb{A}_k^n$ and is k^n . A polynomial $f \in k[x_1, \dots, x_n]$ is also a function $\mathbb{A}^n \rightarrow k \cong \mathbb{A}^1$.

The **zero set**, or **vanishing locus** of a subset $S \subset k[x_1, \dots, x_n]$ is $Z(S) = \{P \in \mathbb{A}^n \mid f(P) = 0 \forall f \in S\}$

An **affine algebraic set** is any subset of $\mathbb{A}^n$ of the form $Z(S)$ for some S

Example 2.1. We have the following examples of affine algebraic sets

1. $\mathbb{A}^n = Z(0), \emptyset = Z(1)$
2. In $\mathbb{A}^2$, $Z(xy)$ is the union of the x and y axes, but in $\mathbb{A}^3$, $Z(xyz)$ is the union of the x, y, z planes. The axes in $\mathbb{A}^3$ are $Z(xy, xz, yz)$
3. If $f \in k[x_1, \dots, x_n]$ is a non-constant polynomial then $Z(f)$ is a **hypersurface**. If f is linear, it is a **hyperplane**
4. $\{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in k\}$ is called the **twisted cubic** in $\mathbb{A}^3$ equal to $Z(y - x^2, z - x^3)$. The twisted cubic is **non-planar** (not contained in any hyperplane)
5. Note that $Z(x) = Z(x^2)$

Proposition 2.1. Recall from GRM: $k[x_1, \dots, x_n]$ is Noetherian and is a UFD

Proof. IB GRM. □

Proposition 2.2. Let $S \subset k[x_1, \dots, x_n]$ be a set of polynomials.

1. If $I = (S)$ then $Z(I) = Z(S)$
2. There are $f_1, \dots, f_i \in S$ such that $Z(S) = Z(\{f_1, \dots, f_i\})$

Proof. For (1), clearly $Z(I) \subset Z(S)$.

For the other direction, if $P \in Z(S)$ and $f_1, \dots, f_k \in S$ and we have arbitrary $a_1, \dots, a_k \in k[x_1, \dots, x_n]$ then for $f = \sum_{i=1}^k a_i f_i$, $f(P) = \sum_{i=1}^k a_i(P) f_i(P) = 0$ so the other direction holds

For (2), I is generated by $g_1, \dots, g_s$ which are each a combination of finitely many elements of S . Call the union of all such $f_1, \dots, f_r$. Then $g_i \in (f_1, \dots, f_r)$ for each i , so $I = (f_1, \dots, f_r)$ and hence $Z(f_1, \dots, f_r) = Z(I) = Z(S)$ □

Remark. The association $I \mapsto Z(I)$ is **order-reversing** with respect to containment

Proposition 2.3. Affine algebraic sets satisfy the following properties

1. If $S \subset T \subset k[x_1, \dots, x_n]$ then $Z(T) \subset Z(S)$
2. $\mathbb{A}^n, \emptyset$ are affine algebraic sets

3. If $\{S_i\}_{i \in I}$ is a collection of subsets of $k[x_1, \dots, x_n]$, then $\bigcap_{i \in I} Z(S_i) = Z(\bigcup_{i \in I} S_i)$
4. If $S, T \subset k[x_1, \dots, x_n]$ then $Z(S) \cup Z(T) = Z(S \cdot T)$

Proof. (1), (2) are already proven, (3) is by definition. We prove (4).

Consider $P \in Z(S) \cup Z(T)$. If $fg \in S \cdot T$ then either f vanishes at P or g vanishes at P so $P \in Z(S \cdot T)$.

Conversely, if $P \in Z(S \cdot T)$ and $f \in S$ with $f(P) \neq 0$ (if no such element exists, then $P \in Z(S)$ so we are done) then as $f(P)g(P) = 0$ for all $g \in T$ we see $g(P) = 0$ for all $g \in T$ so we are done $\square$

Definition 2.2. The **Zariski topology** on $\mathbb{A}^n$ is the topology whose closed sets are the affine algebraic sets

Definition 2.3. A **distinguished open set** in $\mathbb{A}^n$ is any set $\mathbb{A}^n \setminus Z(f)$ for a single $f \in k[x_1, \dots, x_n]$. Any two open sets in the Zariski topology (not just distinguished) have dense intersection

From example sheet 1: Every Zariski open is a union of distinguished opens.

Example 2.2. We have some basic examples

1. In dimension 1, let $f(x) \in k[x]$. Then $Z(f)$ is one of finite, $\mathbb{A}^1$, $\emptyset$ so a distinguished open is a cofinite set (or $\mathbb{A}^1, \emptyset$), and hence we get the cofinite topology
2. Although $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ as sets, the product of the Zariski topology is not the Zariski topology (On Example sheet 1)
3. If $X \subset \mathbb{A}^n$ is an affine algebraic set, the Zariski topology on X is the subspace topology

Definition 2.4. A topological space X is **irreducible** if X can not be written as $X = X_1 \cup X_2$ with X_1, X_2 closed proper subsets. Otherwise, X is **reducible**. An irreducible affine algebraic set is called an **affine variety**

Example 2.3. We have 3 examples

1. $Z(xy) \subset \mathbb{A}^2$ is reducible
2. $\mathbb{A}^n$ is irreducible
3. If $f \in k[x_1, \dots, x_n]$ is irreducible, then $Z(f)$ is irreducible (to be proven soon)

3 Ideals and the Nullstellensatz

Definition 3.1. Suppose $X \subset \mathbb{A}^n$. The **ideal associated to X** , denoted $I(X)$ is $\{f \in k[x_1, \dots, x_n] \mid f(P) = 0, \forall P \in X\}$

Proposition 3.1. *We have the following properties of $X \mapsto I(X)$ for algebraic X . Let $X, Y \subset \mathbb{A}^n$ be affine algebraic*

1. *If $S \subset k[x_1, \dots, x_n]$ then $S \subset I(Z(S))$*
2. *We have $X = Z(I(X))$*
3. *$X = Y$ if and only if $I(X) = I(Y)$*
4. *We have $X \subset Y$ if and only if $I(Y) \subset I(X)$*

Proof. (1) is true by definition.

For (2), by definition $X \subset Z(I(X))$. We want to show $Z(I(X)) \subset X$.

Now $X = Z(S)$ for some set S , so $S \subset I(X)$ and therefore $Z(I(X)) \subset Z(S) = X$

(3) is immediate from (2)

For (4) the only if is true by definition. Suppose $I(Y) \subset I(X)$ and suppose $P \in X \setminus Y$, then by (2), $P \notin Z(I(Y))$ so there is $f \in I(Y)$ such that $f(P) \neq 0$, contradiction, so we are done $\square$

Proposition 3.2. *Any affine algebraic set is a finite union, unique up to order, of affine varieties*

Proof. Uniqueness up to ordering is on sheet 1.

Let X be affine algebraic, if X is irreducible, we are done

So assume $X = X_1 \cup X'_1$ not a finite union of varieties, labelled so X_1 is not a finite union of varieties. Then X_1 is reducible, so we may repeat this to get a strictly descending chain $X \supset X_1 \supset \dots \supset X_n \supset \dots$, so taking $I(\cdot)$ we have ideals $I(X) \subset I(X_1) \subset \dots \subset I(X_n) \subset \dots$ a strictly ascending chain. Contradiction, as $k[x_1, \dots, x_n]$ is Noetherian, so the ideal chain stabilises. $\square$

We therefore have $Z(\cdot), I(\cdot)$ providing a 1-1 map from affine algebraic subsets of $\mathbb{A}^n$ to ideals in $k[x_1, \dots, x_n]$, but I doesn't have full image (for example $(x^2) \notin \text{im}(I)$)

Proposition 3.3. *Suppose $X \subset \mathbb{A}^n$ is an affine algebraic subset. Then X is irreducible if and only if $I(X)$ is prime*

Proof. Suppose X is reducible, with $X = X_1 \cup X_2$ and X_1, X_2 proper closed subsets. Then $I(X) = I(X_1) \cap I(X_2)$.

We get some $f \in I(X_1) \setminus I(X_2), g \in I(X_2) \setminus I(X_1)$. Then $fg \in I(X)$ but $f, g \notin I(X)$

Suppose $I(X)$ is not prime, $f, g \notin I(X)$ such that $fg \in I(X)$.

Define $X_1 = X \cap Z(f)$ and $X_2 = X \cap Z(g)$. Now $X_1 \cup X_2 = X$ as $fg \in I(X)$, but neither is equal to X as $f, g \notin I(X)$ $\square$

Recall from GRM that I is prime if and only if $k[x_1, \dots, x_n]/I$ is an integral domain.

We postpone the proof of the following theorem

Theorem 3.1. (*Weak Nullstellensatz*) *The maximal ideals of $k[x_1, \dots, x_n]$ are those of the form $(x_1 - a_1, \dots, x_n - a_n)$ for $(a_1, \dots, a_n) \in k^n$*

Corollary 3.1.1. (*Also known as Weak Nullstellensatz*) *If $I \subset k[x_1, \dots, x_n]$ is a proper ideal, then $Z(I) \neq \emptyset$*

Proof. As $Z(I) \supset Z(\mathfrak{m})$ for some maximal $\mathfrak{m}$ and $Z(\mathfrak{m}) = \{(a_1, \dots, a_n)\}$ trivially $\square$

Remark. Note these are very false over $\mathbb{R}$, as $Z(x^2 + 1) = \emptyset$

Definition 3.2. Let I be an ideal. The **radical ideal** of I is

$$\sqrt{I} = \{f \in k[x_1, \dots, x_n] \mid f^m \in I \text{ for some } m > 0\}$$

. Notice $I \subset \sqrt{I}$ and $Z(I) = Z(\sqrt{I})$

Theorem 3.2. (*Hilbert's Nullstellensatz*) *Let $J \subset k[x_1, \dots, x_n]$ be an ideal. Then $\sqrt{J} = I(Z(J))$*

Proof. Note that $\sqrt{J} \subset I(Z(J))$ by definition.

Write $J = (f_1, \dots, f_r)$ and let $g \in I(Z(J))$.

Define the ideal $\tilde{J} = (f_1, \dots, f_r, x_{n+1}g - 1) \subset k[x_1, \dots, x_{n+1}]$.

Let $\tilde{P} \in Z(\tilde{J})$ then the projection P to the first n coordinates is in $Z(f_j)$ for $1 \leq j \leq r$, and so $g(\tilde{P}) = 0$, contradiction.

Hence $Z(\tilde{J}) = \emptyset$, and so $1 \in \tilde{J}$ by weak nullstellensatz and so there are some $h_1, \dots, h_{r+1} \in k[x_1, \dots, x_{n+1}]$ with $\sum_{i=1}^r h_i f_i + h_{r+1}(x_{n+1}g - 1) = 1$. On the set where $x_{n+1}g = 1$, we have $\sum_{i=1}^r h_i(x_1, \dots, x_n, \frac{1}{g})f_i(x_1, \dots, x_n) = 1$. Clearing denominators of g , we get some $\sum_{i=1}^r \tilde{h}_i(x_1, \dots, x_n)f_i(x_1, \dots, x_n) = g^k$ and so $g \in \sqrt{J}$ as the left hand side is in J $\square$

4 Coordinate Rings and Morphisms

Corollary 4.0.1. *We have a bijective correspondence between affine algebraic subsets of $\mathbb{A}^n$ and radical ideals in $k[x_1, \dots, x_n]$ given by $I(\cdot), Z(\cdot)$*

Proof. We saw already $Z(I(X)) = X$ and $I(Z(J)) = \sqrt{J}$ by Nullstellensatz $\square$

Remark. This restricts to a correspondence of prime ideals to irreducible affine algebraic sets as prime ideals are radical

Definition 4.1. Let $X \subset \mathbb{A}^n$ be an affine algebraic set. We define the **co-ordinate ring** or the **ring of regular functions** on X to be denoted by $A(X) = k[x_1, \dots, x_n]/I(X)$ (also denoted as $\mathcal{O}_X, \mathcal{O}(X), k[X]$)

Recall from GRM that $A(X)$ is Noetherian

Remark. There is an algebraic description of evaluation at a point in an affine algebraic set $p = (p_1, \dots, p_n) \in X$ via the composition of natural maps $k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]/(x_1 - p_1, \dots, x_n - p_n) \cong k$ with the composition being ev_p . Call the maximal ideal $\mathfrak{m}_p = I(\{p\})$

So for $p \in X \subset \mathbb{A}^n$, $I(X) \subset \mathfrak{m}_p$, and the image of $\mathfrak{m}_p$ in $A(X)$ is the ideal of regular functions on X which vanish at p

Definition 4.2. Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ be affine algebraic sets. A **morphism** or a **regular map** from X to Y is $f: X \rightarrow Y$ such that there are $p_1, \dots, p_m \in A(X)$ with $f(P) = (p_1(P), \dots, p_m(P))$. We denote the set of morphisms from X to Y by $\text{Mor}(X, Y)$, and note that $\text{Mor}(X, \mathbb{A}^1) = A(X)$

Definition 4.3. Let $f: X \rightarrow Y$ be a morphism. Then the **pullback** of f is $f^*: A(Y) \rightarrow A(X)$ sending $g \in A(Y)$ to $g \circ f$

Definition 4.4. Let R be a commutative ring. A **commutative R -algebra** is a commutative ring A together with a ring homomorphism $\alpha_A: R \rightarrow A$. We omit α_A from our notation, and consider $R \subset A$. A key example is $k \hookrightarrow k[x_1, \dots, x_n]$

Definition 4.5. A **k -algebra homomorphism** of (commutative) k algebras A, B is a ring homomorphism $\phi: A \rightarrow B$ such that

$$\begin{array}{ccc} & k & \\ \swarrow & & \searrow \\ A & \xrightarrow{\phi} & B \end{array}$$

Proposition 4.1. *We have a few properties of morphisms*

1. *Morphisms are continuous with respect to the Zariski topology. The converse is trivially false (eg. e^x)*
2. *Morphisms are not necessarily closed*
3. *The composition of morphisms is a morphism*
4. *If f, g are morphisms then $(f \circ g)^* = g^* \circ f^*$*
5. *If $f: X \rightarrow Y$ is a morphism, then $f^*: A(Y) \rightarrow A(X)$ is a ring homomorphism which is the identity on k , and hence is a k -algebra morphism*

Proof. 1. If $Z = Z(g_1, \dots, g_r) \subset Y$ then

$$f^{-1}(Z) = \bigcap_{i=1}^r f^{-1}(Z(g_i)) = \bigcap_{i=1}^r Z(g_i \circ f) = Z(f^*g_1, \dots, f^*g_r)$$

so the preimage of closed is closed

2. Let $\pi_1: \mathbb{A}^2 \rightarrow \mathbb{A}^1$ by projection which sends $Z(xy - 1)$ to $\mathbb{A}^1 \setminus \{0\}$ which is not closed
3. By definition
4. Trivial
5. Trivial

□

Example 4.1. We have a few examples of morphisms

1. Let $n \geq m$ and $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^m$ the projection $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_m)$. This is a morphism and the pullback, $\pi^*: k[x_1, \dots, x_m] \rightarrow k[x_1, \dots, x_n]$ is given by $\pi^*(x_i) = x_i$ for $1 \leq i \leq m$ and hence the pullback map is the natural inclusion $k[x_1, \dots, x_m] \hookrightarrow k[x_1, \dots, x_n]$
2. Consider the map $f: \mathbb{A}^1 \rightarrow Z(y - x^2) \subset \mathbb{A}^2$ by $t \mapsto (t, t^2)$. Then $f^*: k[x, y]/(y - x^2) \rightarrow k[t]$ sending $x \mapsto t, y \mapsto t^2$ which is an isomorphism. More generally, the **affine d -Veronese embedding** of $\mathbb{A}^1$ to be the map $t \mapsto (t, \dots, t^d) \in \mathbb{A}^d$. The image is the **degree d Veronese curve**. For $d = 3$ the image is the twisted cubic.

Theorem 4.1. Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ be affine algebraic sets. Then $f \mapsto f^*$ defines a bijection from $\text{Mor}(X, Y)$ to k -algebra homomorphisms $A(Y) \rightarrow A(X)$

Proof. Let $x_1, \dots, x_n$ and $y_1, \dots, y_m$ be coordinates on $\mathbb{A}^n, \mathbb{A}^m$ respectively. A morphism $f: X \rightarrow Y$ is described by $(f_1, \dots, f_m)$ for some set of $f_i \in A(X)$. Then $f^*y_i = f_i$ so we can recover f from f^* and the map is injective. Suppose $\lambda: A(Y) \rightarrow A(X)$ is a k -algebra homomorphism. Then for each $1 \leq i \leq m$, let $f_i = \lambda(y_i)$ and define $f = (f_1, \dots, f_m): X \rightarrow \mathbb{A}^m$.

We claim $f(X) \subset Y = Z(I(Y))$ so we need to show that $g(f(P)) = 0$ for all $P \in X, g \in I(Y)$. $g(f(P)) = g(\lambda(y_1(P)), \dots, \lambda(y_m(P))) = \lambda(g(P)) = 0$ as $g \in I(Y) \subset \ker(\lambda)$. Finally note that by definition $f^* = \lambda$ so we are done □

Definition 4.6. A morphism $f: X \rightarrow Y$ is an **isomorphism** if f is bijective with f^{-1} an inverse morphism

Remark. Bijective morphisms are not necessarily isomorphisms. Consider $X = \mathbb{A}^1$ and $Y = \mathbb{A}^2 = Z(y^2 - x^3)$ (Y is called the **cuspidal cubic**). We can define $f: X \rightarrow Y, t \mapsto (t^2, t^3)$ which is a bijective morphism since $\frac{y}{x}$ is an inverse away from the origin. If this were a morphism, then there would be $g \in k[x, y]$ such that $g(t^2, t^3) = t$, but this is obviously impossible

Corollary 4.1.1. $f: X \rightarrow Y$ is an isomorphism if and only if $f^*: A(Y) \rightarrow A(X)$

Proof. Trivial □

There is an example in Example Sheet 1 Question 13

Remark. This is a very affine statement. The projective variety $\hat{\mathbb{C}}$, called the Riemann Sphere has only everywhere constant automorphisms by Liouville

5 Proof of Nullstellensatz

Definition 5.1. Let $R \subset S$ be rings. S is a **finitely generated R module** if there is $s_1, \dots, s_n \in S$ such that $S = Rs_1 + \dots + Rs_n$. It is a **finitely generated R algebra** if there is $s_1, \dots, s_n$ such that $S = R[s_1, \dots, s_n]$. $s \in S$ is **integral over R** if there is monic $f(x) \in R[x]$ with $f(s) = 0$

Proposition 5.1. *The following are equivalent for $s \in S$*

1. s is integral over R
2. $R[s]$ is a finitely generated R -module
3. There is a finitely generated R module $R' \subset S$ such that $R[s] = R'$

Proof. 1 implies 2: As s is integral, there are $r_0, \dots, r_{n-1}$ such that we have $s^n = r_{n-1}s^{n-1} + \dots + r_0$ so for all $k \geq n$, $s^k \in R + Rs + \dots + Rs^{n-1}$ so $R[s]$ is a finitely generated R module.

2 implies 3: Take $R' = R[s]$

3 implies 1: Write $R' = Rv_1 + \dots + Rv_n$. $sv_i \in R'$ so we can find $a_{ij} \in R$ such that $sv_i = \sum a_{ij}v_j$. Define $A = (a_{ij})_{1 \leq i, j \leq n}$ so that $Av = sv$ and $(A - sI)v = 0$ so $\det(A - sI) = 0$ so we are done $\square$

Corollary 5.0.1. *If $R \subset S$ are rings and S is a finitely generated R -algebra, if S is also a finitely generated R -module, then all elements of S are integral over R*

Proof. Trivial $\square$

Lemma 5.1. (Zariski's Lemma) *Suppose we have $k \subset K$ an extension of fields. If K is a finitely generated k -algebra then it is a finitely generated k -module*

Proof. (Postponed) $\square$

Proof. (Of Weak Nullstellensatz assuming Zariski's lemma). Note that $(x_1 - a_1, \dots, x_n - a_n) \subset k[x_1, \dots, x_n]$ is a maximal ideal, as evaluation shows its quotient is isomorphic to k . Suppose $\mathfrak{m} \subset k[x_1, \dots, x_n]$ is maximal so we have $k \hookrightarrow k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]/\mathfrak{m} = K$ and this is an embedding as it is not 0, hence K/k is a field extension. Call the whole map ϕ . K is a finitely generated k -algebra so by Zariski is a finitely generated k -module, hence is algebraic over k , so $K = k$ as k is algebraically closed. Therefore ϕ is a surjection. Define $a_i = \phi^{-1}(x_i \bmod \mathfrak{m})$ so $x_i - a_i \in \mathfrak{m}$ so we are done $\square$

Proposition 5.2. *Suppose $k \subset k(s)$, and s is transcendental over k . Then*

1. $k[s]$ is a UFD, containing an infinite set of pairwise coprime elements
2. If $t \in k(s)$ is integral over $k[s]$ then $t \in k[s]$

Proof. 1. $k[x] \rightarrow k[s]$ by $x \mapsto s$ has empty kernel has s is transcendental. Then $k[s]$ is a UFD by Gauss's Lemma. If we can only find finitely many pairwise coprime monic, irreducible elements, $p_1, \dots, p_k$ then $p_1 \dots p_k + 1$ is pairwise coprime to them all, contradiction

2. Write $t = \frac{p(s)}{q(s)}$ and suppose there are $f_0, \dots, f_{n-1} \in k[s]$ such that we have $\left(\frac{p}{q}\right)^n + f_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + f_0$ so $p^n = q(\dots)$ and hence as p, q coprime, q is constant so $t \in k[s]$

□

Proof. (Of Zariski's Lemma) We will induct on the number of generators of K as a k algebra.

Suppose $K = k[s]$ as a k -algebra. As K is a field, $\frac{1}{s} \in k[s]$ so s is algebraic, hence integral over k and K is a finitely generated k -module.

Assume Zariski holds for less than n generators and $K = k[s_1, \dots, s_n]$. Applying the inductive hypothesis to $K/k[s_1]$, K is a finitely generated $k(s_1)$ module. If s_1 is algebraic, we are done. So assume s_1 is transcendental over k . Each $s_i, 2 \leq i \leq n$ is algebraic over $k(s_1)$ so we have $f_{ij} \in k(s_1)$ such that we have $s_i^{n_i} + f_{i,n_i-1}s_i^{n_i-1} + \dots + f_{i,1}s_i + f_{i,0} = 0$. There is $f \in k[s_1]$ such that we may multiply by f^{n_i} and get that fs_i is integral with all coefficients in $k[s]$. Since the s_i generate the extension, every $h \in k(s_1) \subset K$, so there is an N such that $f^N h \in k[s_1][fs_2, \dots, fs_n]$ so $f^N h$ is integral over $k[s_1]$. Since $k[s_1]$ is integrally closed, $f^N h \in k[s_1]$. Choosing $h = \frac{1}{t}$ for t coprime to f , we get a contradiction. Hence s_1 is algebraic and we are done

□

6 More Coordinate Rings

Definition 6.1. Let $X \subset \mathbb{A}^n$ be an affine variety. Then the **function field** of X , denoted $k(X)$, is the fraction field of $A(X)$. The elements are called **rational functions** on X (for $k = \mathbb{C}$, sometimes called **meromorphic functions**). If $\phi \in k(X)$ can be represented as $\frac{f}{g}$ with $g \neq 0$ at $p \in X$ then we say ϕ is **regular** at p

Definition 6.2. If $\mathfrak{p}$ is a prime ideal in an integral domain R with field of fractions K then the **localisation** of R at $\mathfrak{p}$ is $R_{\mathfrak{p}} = \{\frac{a}{b} \in K \mid b \notin \mathfrak{p}\}$

Definition 6.3. Let X be an affine variety and $x \in X$. We define the **local ring** of X at x to be $\mathcal{O}_{X,x} = \{\phi = \frac{f}{g} \mid f, g \in A(X), g(x) \neq 0\}$. In other words, this is the localisation of $A(X)$ at the prime ideal of functions vanishing at x .

A **local ring** is a ring with a unique maximal ideal

Proposition 6.1. Let X be an affine variety and $x \in X$. Then the local ring $\mathcal{O}_{X,x}$ has a unique maximal ideal, $\mathfrak{m}_x = \{\phi \in \mathcal{O}_{X,x} \mid \phi(x) = 0\}$

Proof. For $\phi = \frac{f}{g} \in \mathcal{O}_{X,x}$ where $g(x) \neq 0$. This has a multiplicative inverse if and only if $f(x) \neq 0$ if and only if $\phi(x) \notin \mathfrak{m}_x$. Hence any proper ideal of $\mathcal{O}_{X,x}$ is contained in $\mathfrak{m}_x$. $\mathfrak{m}_x$ is an ideal so we are done.

□

Lemma 6.1. *If R is a Noetherian integral domain and $\mathfrak{p}$ is a prime ideal of R then the localisation of R at $\mathfrak{p}$ is Noetherian*

Proof. Suppose we have $I_1 \subset I_2 \subset I_3 \subset \dots$ a chain of ideals in $R_{\mathfrak{p}}$. The map $\phi: R \rightarrow R_{\mathfrak{p}}$ which sends $f \mapsto \frac{f}{1}$ gives a chain of ideals in R given as $\phi^{-1}(I_1) \subset \phi^{-1}(I_2) \subset \phi^{-1}(I_3) \subset \dots$ which stabilises, say $\phi^{-1}(I_n) = \phi^{-1}(I_{n+1})$. If there is $\frac{f}{g} \in I_{n+1}$, note that $g \notin \mathfrak{p}$ and $\frac{f}{1} \in I_{n+1}$ so $f \in \phi^{-1}(I_{n+1}) = \phi^{-1}(I_n)$ hence $\frac{f}{1} \in I_n$ so $\frac{f}{g} \in I_n$ as $g \notin \mathfrak{p}$ so is invertible so the upper chain stabilises $\square$

We can define for $U \subset X$ open, $\mathcal{O}_X(U) = \bigcap_{x \in U} \mathcal{O}_{X,x}$, the **ring of regular functions** on U

Lemma 6.2. $\mathcal{O}_X(X) = A(X)$

Proof. By $f \mapsto \frac{f}{1}$ we have $A(X) \subset \mathcal{O}_{X,x}$ for all $x \in X$. For the other inclusion, suppose $\phi \in \bigcap_{x \in X} \mathcal{O}_{X,x}$. Define an ideal $I_{\phi} = \{h \in A(X) \mid h\phi \in A(X)\}$. If I_{ϕ} is proper, it is contained in a maximal ideal so by the weak nullstellensatz, every function in I_{ϕ} vanishes at some $P \in X$. This is a contradiction as ϕ is regular at P , so we are done as $1 \in I_{\phi}$. $\square$

Example 6.1. It can happen that ϕ really requires more than one representation as $\frac{f}{g}$. One example is $\mathbb{A}^4$ with coordinates (x, y, z, w) , defining the algebraic set $X = Z(xw - yz)$. Let $\phi = \frac{x}{y}$. This is regular on $X \cap \{y \neq 0\}$. But in $k(X)$, $\phi = \frac{x}{y} = \frac{z}{w}$ which is regular when $W \neq 0$. Hence ϕ is actually regular on $X \cap (\{y \neq 0\} \cup \{w \neq 0\})$ which is strictly larger

Proposition 6.2. *Let $f: X \rightarrow Y$ be a Zariski continuous map of affine varieties. Then the following are equivalent*

1. f is a morphism
2. For all $x \in X$ and all $\phi \in \mathcal{O}_{Y,f(x)}$, $f^*\phi \in \mathcal{O}_{X,x}$

Proof. If f is a morphism and $\phi = \frac{g}{h}$ then $f^*\phi = \frac{g \circ f}{h \circ f}$ where $h \circ f \neq 0$ at x and so $f^*\phi \in \mathcal{O}_{X,x}$

Conversely, if $\phi \mapsto \phi \circ f$ induces a map $\mathcal{O}_{Y,f(x)} \rightarrow \mathcal{O}_{X,x}$ we have

$$f^*: \bigcap_{f(x) \in f(X)} \mathcal{O}_{Y,f(x)} \rightarrow \bigcap_{x \in X} \mathcal{O}_{X,x} = A(X)$$

so by restriction we get a map $f^*: A(Y) \rightarrow A(X)$. Evaluating f^* at $y_1, \dots, y_m$ the coordinates of $Y \subset \mathbb{A}^m$ gives f as a morphism. $\square$

Definition 6.4. Fix $n \geq 1$. **Projective n -space** over k is denoted by the notation $\mathbb{P}_k^n = \{(a_0, \dots, a_n) \in k^{n+1} \setminus \{0\}\} / \sim$ where $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ if there is $\lambda \in k^\times$ such that $a_i = \lambda b_i$. We denote $[(a_0, \dots, a_n)]$ by $(a_0 : \dots : a_n)$.

Remark. Viewing $(x_0, \dots, x_n) \in k^{n+1}$, we call x_i **homogeneous coordinates** on $\mathbb{P}^n$. They are not well defined functions alone, but the ratios $\frac{x_i}{x_j}$ are. The set of points $\{(x_0 : \dots : x_n) \in \mathbb{P}^n \mid x_0 \neq 0\}$ is well defined, as is its complement. The complement can be identified with $\mathbb{A}^n$ by sending $(x_0 : \dots : x_n)$ to $(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$. We therefore have a decomposition $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\text{pt}\}$. Similarly $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$. Similarly, $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$.

Definition 6.5. If $\mathbb{P}^n$ has homogeneous coordinates $x_0, \dots, x_n$, we define for $0 \leq i \leq n$, $U_i = \{(x_0, \dots, x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$ called a **standard affine patch** and $H_i = \mathbb{P}^n \setminus U_i$ is a **coordinate hyperplane**. Each $U_i \xrightarrow{\sim} \mathbb{A}^n$ and $\mathbb{P}^n = \bigcup_{i=0}^n U_i$.

Example 6.2. $n = 1, k = \mathbb{C}$. The projective line, $\mathbb{P}^1$ over $\mathbb{C}$, is the Riemann sphere. This is two copies of $\mathbb{C}$ with coordinates z, w respectively, glued along $z = \frac{1}{w}$ where $zw \neq 0$. We have $\mathbb{P}_{\mathbb{C}}^1 = \{(x_0, x_1) \mid x_0 x_1 \neq 0\} / \sim$. Now $z = \frac{x_1}{x_0}$ and $w = \frac{x_0}{x_1}$. We identify $\mathbb{P}^1 \setminus (1 : 0)$ and $\mathbb{P}^1 \setminus (0 : 1)$ with $\mathbb{C}$. When $k = \mathbb{C}$, $\mathbb{P}_{\mathbb{C}}^n$ comes with a natural quotient topology by definition.

Proposition 6.3. *With the Euclidean topology, $\mathbb{P}_{\mathbb{C}}^n$ is compact*

Proof. The quotient map $\mathbb{C}^{n+1} \setminus \{0\} \rightarrow \mathbb{P}^n$ is continuous by definition, and restricts to a surjective continuous map $S^{2n+1} \rightarrow \mathbb{P}^n$, and S^{2n+1} is compact. $\square$

Definition 6.6. The **Zariski topology** on $\mathbb{P}^n$ is the quotient of the Zariski topology on $\mathbb{A}^{n+1} \setminus \{0\}$. Hence $X \subset \mathbb{P}^n$ is closed if and only if $\pi^{-1}(X)$ is closed for $\pi : \mathbb{A}^{n+1} \setminus \{0\} \rightarrow \mathbb{P}^n$.

Example 6.3. For $n = 1$ we have a map $k^2 \setminus \{0\} \xrightarrow{\pi} \mathbb{P}^1$. Let $X \subset \mathbb{P}^1$. In example sheet 1, it is proven that the Zariski closed subsets of k^2 are $\emptyset, k^2$ and finite unions of curves and points. Restricting these to $k^2 \setminus \{0\}$ we get the same thing. We get $\emptyset, \mathbb{P}^1$ and the only curves in $k^2 \setminus \{0\}$ which contain lines through 0 are themselves lines through 0 (example sheet 1 question 6). Therefore the topology is cofinite.

Definition 6.7. A **monomial** in $k[x_1, \dots, x_n]$ is anything of the form $cx_0^{r_0} \dots x_n^{r_n}$ with $r_i \geq 0$ for all $0 \leq i \leq n$ and $c \in k$. The **degree** of the monomial is $d = r_0 + \dots + r_n$. A polynomial $f \in k[x_1, \dots, x_n]$ is **homogeneous** if all monomials of f have the same degree.

Lemma 6.3. *If $f \in k[x_1, \dots, x_n]$ is a homogeneous polynomial of degree d , then $Z(f)$ is a well defined subset of $\mathbb{P}^n$*

Proof. If f is homogeneous of degree d , then for all $\lambda \in k^\times$, we have that $f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$ and hence one side is zero if and only if the right is. $\square$

Definition 6.8. An **algebraic set** in $\mathbb{P}^n$ is any set of the form $Z(S)$ where S is a collection of homogeneous polynomials, not necessarily of the same degree.

We can use this to define a topology on $\mathbb{P}^n$ where the closed sets are the algebraic sets, and this is the same Zariski topology (example sheet 2)

Definition 6.9. An ideal $I \leq k[x_1, \dots, x_n]$ is **homogeneous** if it can be generated by homogeneous polynomials, not necessarily all of the same degree

Remark. Not all generating sets of homogeneous ideals are necessarily made of homogeneous polynomials. For example, $(x, x^3 + y^2) = (x, y^2)$

Lemma 6.4. Let $I \leq k[x_1, \dots, x_{n+1}]$ be an ideal. The following are equivalent

1. I is homogeneous
2. If $f \in I$ then the degree d part, f_d , is in I

Proof. (1) implies (2): If I is homogeneous, then $I = (f_1, \dots, f_s)$ where we have $\deg(f_i) = d_i$ and each f_i is homogeneous. Given $g \in I$, write $g = \sum_{i=1}^s h_i f_i$. Given any $d \geq 0$, we have $g_d = \sum_{i=1}^s (h_i)_{d-d_i} f_i \in I$ so we are done
(2) implies (1): The ideal is generated by the homogeneous parts of the generators. $\square$

As in the affine case, we have

Proposition 6.4. For homogeneous ideals $I_j \leq k[x_1, \dots, x_{n+1}]$ we have

1. If $I_1 \subset I_2$ then $Z(I_2) \subset Z(I_1)$
2. $\bigcap Z(I_j) = Z(\bigcup I_j)$
3. $Z(I_1) \cup Z(I_2) = Z(I_1 I_2)$

Proof. Trivial $\square$

Definition 6.10. A **projective variety** is an irreducible algebraic set in $\mathbb{P}^n$

Example 6.4. Suppose $f_1, \dots, f_r \in k[x_0, \dots, x_n]$ are linear homogeneous polynomials. Each $Z(f_i) \subset \mathbb{P}^{n+1}$ is a vector subspace, so $Z(f_1, \dots, f_r) \subset \mathbb{A}^{n+1}$ is too. Then $Z(f_1, \dots, f_r) \subset \mathbb{P}^n$ is a **projective linear space**. In $\mathbb{P}^2$, $Z(ax + by + cz)$ is parameterised by a projective line. For example, if $a \neq 0$ then $(b, -a, 0)$ and $(-c, 0, a)$ are distinct in $Z(ax + by + cz)$. The map $(t, u) \mapsto (bt - cu, -at, au)$ identifies this with $\mathbb{P}^1$

Example 6.5. Any element of $GL_{n+1}(k)$ induces a well defined map on $\mathbb{P}^n$ by the quotient construction. Multiplying by $\text{diag}(\lambda, \dots, \lambda)$ gives the identity map and hence $PGL_{n+1}(k)$ acts on $\mathbb{P}^n$, the projective linear group of automorphisms of $\mathbb{P}^n$

Remark. Varieties no longer need be irreducible (Lecturer notation change)

Definition 6.11. If $F \in k[x_0, \dots, x_n]$ is a non-constant homogeneous polynomial, then $Z(F) \subset \mathbb{P}^n$ is a **hypersurface** (some authors require irreducibility)

Example 6.6. The **Segre surface** is $F(x_0x_3 - x_1x_2) \subset \mathbb{P}^3$. The surface $\Sigma_{1,1}$ is built out of familiar objects. Consider the function of sets $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$ by $((t_0 : t_1), (u_0 : u_1)) \mapsto (t_0u_0 : t_0u_1 : t_1u_0 : t_1u_1)$ is a bijection into $\Sigma_{1,1}$. This identification defines $\mathbb{P}^1 \times \mathbb{P}^1$ as a projective variety and we will generalise this later.

Example 6.7. Consider $\mathbb{P}^1 \rightarrow \mathbb{P}^n$ by $(t, u) \mapsto (t^n : t^{n-1}u : \dots : u^n)$. This is a well defined map which is bijective onto its image, which is called the **rational normal curve** of degree n in $\mathbb{P}^n$. When $n = 3$, the curve $(t^3, t^2u, tu^2, u^3) \in \mathbb{P}^3$ is known as the **projective twisted cubic**. This is the zero locus of 3 quadratic polynomials in $k[x_0, \dots, x_3]$ and can't be written as the zero locus of any two polynomials (example sheet 2)

6.1 From Projective to Affine

For a projective variety $V \subset \mathbb{P}^n$, with $V = Z(I)$, we define the ideal $n \ k[x_1, \dots, x_n]$, called $I_0 = \{F(1, x_1, \dots, x_n) \mid F \in I\}$ which defines an affine variety $V_0 = Z(I_0)$. We call this **dehomogenisation**. Under the map $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ which is given by $(x_1, \dots, x_n) \mapsto (1 : x_1 : \dots : x_n)$, $V_0 = V \cap U_0$ where U_0 is the standard patch with $x_0 \neq 0$. If $V \subset \mathbb{A}^n$ is an affine variety, then $V \subset \mathbb{P}^n$ is not necessarily closed, but we can take its closure.

Definition 6.12. If $f \in k[x_1, \dots, x_n]$ the **homogenisation** of f is $F = x_0^{\deg(f)} f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$ is a homogeneous polynomial of the same degree, and $F(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$

Definition 6.13. For $V \subset \mathbb{A}^n$, $V = Z(I)$ we define I^* to be the ideal generated by all homogenisations of elements in I . Call $V^* = Z(I^*) \subset \mathbb{P}^n$. Then we have $V^* \cap U_0 = V$ and we call V^* the **projective closure** of V

V^* is the minimal projective variety containing V . If $V \subset Y$ is a projective variety, $Y = Z((F_1, \dots, F_s))$. Then each of these polynomials has dehomogenisation f_i of F_i which vanish along V . So $f_i \in I(V)$, and hence $F_i \in I^*$. So $I(Y) \subset I(V^*)$ so $V^* = Z(I(V^*)) \subset Z(I(Y)) = Y$

Example 6.8. The affine Fermat curve, $x^n + y^n = 1$, has homogenisation $x^n + y^n = z^n$ which cuts out a curve in $\mathbb{P}^2$. The points at infinity (ie where $z = 0$) are precisely those of the form $(1 : z : 0)$ where $z^n = -1$

Example 6.9. Consider $V \subset \mathbb{P}^2$ given by $V = Z(x_0x_2 - x_1^2)$. Its affine pieces are $Z(x_2 - x_1^2), Z(x_2x_0 - 1), Z(x_0 - x_1^2)$, so we can get both parabolae and hyperbolae

Example 6.10. Let F be homogeneous of degree 2 in $k[x_0, \dots, x_n]$. $Q = Z(F)$ is **quadric hypersurface**. By diagonalisation of quadratic forms, we can change coordinates so that this is identified with $Z(x_0^2 + \dots + x_r^2)$ where $r + 1$ is the rank of the form

6.2 Projective Nullstellensatz

Definition 6.14. Let $X \subset \mathbb{P}^n$. We define the **ideal of** X to be the ideal generated by homogeneous polynomials which vanish on X . The **affine cone** over X is $C(X) = \{(x_0, \dots, x_n) \mid (x_0 : \dots : x_n) \in X\} \cup \{0\}$

Proposition 6.5. *We have*

1. If $X_1 \subset X_2 \subset \mathbb{P}^n$ then $I(X_1) \supset I(X_2)$
2. If $X \subset \mathbb{P}^n$ is algebraic, then $Z(I(X)) = X$
3. For $J \in k[x_0, \dots, x_n]$ homogeneous such that $Z(J) \neq \emptyset$, we have that $I(Z(J)) = \sqrt{J}$
4. If J is a homogeneous ideal with $Z(J) = \emptyset$ then $J = k[x_0, \dots, x_n]$ or $\sqrt{J} = (x_0, \dots, x_n)$

Proof. 1 and 2 are the same as the affine case.

Suppose J is such an ideal as in 3. Then $C(Z(J)) \neq \emptyset$. By the affine nullstellensatz, we deduce that $I(Z(J)) = \sqrt{J}$

For 4, if $Z(J) = \emptyset$ then $Z(J)$ in $\mathbb{A}^n$ is either $\emptyset$ or $\{0\}$ and then the result follows by the affine nullstellensatz. $\square$

Definition 6.15. If V is a projective variety, and $W \subset V$ is also a projective variety, we say W is a **(closed) subvariety** of V , and $V \setminus W$ is an **open subvariety** of V . Open subvarieties of projective varieties (including when $W = \emptyset$) are called **quasi-projective varieties**

Proposition 6.6. *We have*

1. Every projective variety is a finite union of irreducible projective varieties
2. A projective variety X is irreducible if and only if $I(X)$ is prime

Proof. (1) is identical to the affine setting

(2) If X is reducible, then $\pi: C(X) \setminus \{0\} \rightarrow X$ gives that $C(X)$ is reducible so $I(X)$ is not prime by the affine version. If $I(X)$ is not prime then the cone $C(X) = V_1 \cup V_2$ is reducible with V_1, V_2 closed proper subsets. Then define the closed set $Z_i = Z(\{f(\lambda x_0, \dots, \lambda x_n) \mid f \in I(V_i), \lambda \in k^\times\})$ which by construction is the set of lines through 0 in V_i . Z_i is closed by definition and is a subset of V_i so is proper and for each line, it is contained in some V_i as $\mathbb{A}^1$ is irreducible, so $C(X) = Z_1 \cup Z_2$ as cones, and this passes to X via π , so done $\square$

Recall from example sheet 1 that open sets of irreducible affine varieties are Zariski dense (have intersection with any non-empty open set). A subset $S \subset X$ is Zariski dense in an algebraic set X if and only if every polynomial which vanishes on S vanishes on all of X

Proposition 6.7. *Let $X \subset \mathbb{P}^n$ be an irreducible projective variety and $Y \subset X$ a proper closed subvariety. Then $X \setminus Y$ is Zariski dense in X*

Proof. Let $f \in I(X \setminus Y)$. By projective nullstellensatz, $I(X) \subset I(Y)$ is a proper inclusion so we can find $g \in I(Y) \setminus I(X)$ so $fg \in I(X)$ and hence $f \in I(X)$ as $I(X)$ is prime $\square$

7 Functions on Projective Varieties

Definition 7.1. Let $X \subset \mathbb{P}^n$ be an irreducible projective variety. Then the **function field** or **field of rational functions** of X is

$$k(X) = \left\{ \frac{f}{g} \mid f, g \in k[x_0, \dots, x_n] \text{ are homogeneous of equal degree, } g \notin I(X) \right\} / \sim$$

where $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ if and only if $f_1g_2 - f_2g_1 \in I(X)$

$\sim$ is an equivalence relation. The first two axioms are clear. Suppose that $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$, $\frac{f_3}{g_3} \sim \frac{f_2}{g_2}$ so that $f_1g_2 - f_2g_1, f_3g_2 - f_2g_3 \in I(X)$. Since $I(X)$ is prime, $f_1g_3 - f_3g_1 \in I(X)$ if and only if $f_1g_3g_2 - f_3g_1g_2 \in I(X)$ which is equivalent to $f_2g_1g_3 - f_2g_3g_1 \in I(X)$ which holds.

Proposition 7.1. Let $X \subset \mathbb{P}^n$ be an irreducible projective variety, and assume $X \not\subset \{x_0 = 0\}$. Then $X_0 = X \cap U_0$ is non-empty open and $k(X) = k(X_0)$

Proof. The map $\frac{f}{g} \rightarrow \frac{f(1, y_1, \dots, y_n)}{g(1, y_1, \dots, y_n)}$ is an isomorphism $\square$

Definition 7.2. Let $X \subset \mathbb{P}^n$ be an irreducible projective variety and $\phi \in k(X)$ and $p \in X$. Then ϕ is **regular** at p if there is a representative $\frac{f}{g}$ of ϕ with $g(p) \neq 0$. The **local ring** at p is $\mathcal{O}_{X,p} = \{\phi \in k(X) \mid \phi \text{ is regular at } p\}$

Proposition 7.2. Suppose $X \subset \mathbb{P}^n$ not contained in $\{x_0 = 0\}$. Let $p \in X_0$ where $X_0 = X \cap U_0$. Then $\mathcal{O}_{X,p} = \mathcal{O}_{X_0,p}$

Proof. Write $p = (1: p_1: \dots: p_n)$. The result is then by definition under the isomorphism of function fields $\square$

Example 7.1. If $k = \mathbb{C}$ and considering $\mathbb{P}_{\mathbb{C}}^1$ which is identified with the Riemann sphere. If $\phi \in \mathbb{C}(\mathbb{P}_{\mathbb{C}}^1)$ is regular everywhere, then we get a holomorphic map $\phi: \mathbb{C}_{\infty} \rightarrow \mathbb{C}$ which is necessarily constant by Liouville

Proposition 7.3. There are no non-constant rational functions on $\mathbb{P}^1$ which are regular at all points

Proof. If $\phi \in k(\mathbb{P}^1)$ with representative $\frac{f(x_0, x_1)}{g(x_0, x_1)}$ with no common factors, both of degree d . Then $f(1, x), g(1, x)$ have no common roots. If α is a root of g_1 and $\phi = \frac{h}{k}$ then $kf - hg = 0$ so evaluating at $(1, \alpha)$ we get $k(1, \alpha) = 0$ as $f(1, \alpha) \neq 0$, contradiction so $g(1, x)$ has no roots and $g(x_0, x_1) = cx_0^d$. But repeating this in the other coordinate, $g(x_0, x_1) = 1$ and so ϕ is constant $\square$

Corollary 7.0.1. $\mathbb{P}^n$ has no non-constant rational functions which are regular everywhere

Proof. If $\phi \in k(\mathbb{P}^n)$ is non-constant, there are $p, q \in \mathbb{P}^n$ with $\phi(p) \neq \phi(q)$. If $L \cong \mathbb{P}^1$ is the line containing p, q , then we get a non-constant regular function on $\mathbb{P}^1$, contradiction $\square$

7.1 Maps between Projective Varieties

If $F_0, \dots, F_m \in k[x_0, \dots, x_n]$ are all homogeneous of the same degree. Then $F = (F_0, \dots, F_m): k^{n+1} \rightarrow k^{m+1}$ descends to a map $F: \mathbb{P}^n \setminus \bigcap_{i=0}^m Z(F_i) \rightarrow \mathbb{P}^m$. For any homogeneous $G \in k[x_0, \dots, x_n]$, $(F_0G: \dots: F_mG)$ defines the same map on a smaller set. We know this is an issue more generally:

Example 7.2. Let $X = Z(xw - yz) \subset \mathbb{P}^3$. We get a well defined map $X \rightarrow \mathbb{P}^1$ by $(x: y: z: w) \mapsto (x: y) = (z: w)$.

Definition 7.3. Suppose $X \subset \mathbb{P}^n$ is an irreducible projective variety and let us have $F_0, \dots, F_m \in k[x_0, \dots, x_n]$ which are homogeneous of the same degree, not all in $I(X)$. Then we have a well defined map $F: X \setminus \bigcap_{i=0}^m Z(F_i) \rightarrow \mathbb{P}^m$. We say that F, G as above **determine the same rational map** if $F = G$ where both are defined. We call a **rational map** an equivalence class of such functions. We write $F: X \dashrightarrow \mathbb{P}^m$ for a rational map F

Remark. A simpler equivalent form of the condition ' F is equivalent to G ' is $F_i G_j - G_i F_j \in I(X)$ for all i, j

Definition 7.4. If $P \in X$, then F is **regular** at P if there is a representative $(F_0: \dots: F_m)$ with some $F_i(P) \neq 0$. The **domain** of F is the set of regular points and all other points are the **indeterminacy/indeterminate points** of F . A rational map is said to be a **morphism** if it is regular at all points of X , and we write $F: X \rightarrow \mathbb{P}^m$. If $F: X \dashrightarrow Y \subset \mathbb{P}^m$ for some algebraic Y then F is a **rational map** from X to Y , and similarly for **morphism**. A morphism $F: X \rightarrow Y$ is an **isomorphism** if there is an inverse morphism $G: Y \rightarrow X$ to F . A rational map is a **birational map** if it has a rational inverse

Example 7.3. If $F_0, \dots, F_m$ are degree 1 homogeneous polynomials in $k[x_0, \dots, x_n]$, we get a rational map $\mathbb{P}^n \dashrightarrow \mathbb{P}^m$ which is a morphism if and only if the corresponding matrix has trivial kernel (has rank $n + 1 \leq m + 1$)

Example 7.4. We have two critical examples

1. (Projection from a point) Suppose $P = (0: \dots: 0: 1)$. Then we can define **projection from P** (to the hyperplane $x_n = 0$) by

$$\pi: (x_0: \dots: x_n) \mapsto (x_0: \dots: x_{n-1})$$

This is not regular at P , as $k[x_0, \dots, x_n]$ is a UFD so we can't modify the F_i , but is regular at all other points. Suppose F is homogeneous of degree d in $k[x_0, \dots, x_n]$ and define $X = Z(F)$. If $P \notin X$, then $\pi|_X$ is a morphism $\pi|_X: X \rightarrow \mathbb{P}^{n-1}$. If we fix $a = (a_0: \dots: a_{n-1}) \in \mathbb{P}^{n-1}$ and consider its preimage, it will intersect X at exactly the points $(a_0: \dots: a_{n-1}: x_n)$

such that $F(a_0, \dots, a_{n-1}, x_n) = 0$. This polynomial has degree at most d in the variable x_n , so we have at most d such points
In particular if $n = 2$, $P = (0: 0: 1)$ and $X = Z(x_0x_2 - x_1^2)$. Now $\pi(x_0: x_1: x_2) = (x_0: x_1) \sim (F_1: F_2)$ if and only if

$$x_1F_0 - x_0F_1 \in (x_0x_2 - x_1^2)$$

so $(-x_1, x_2)$ gives a definition of π at P . $\pi|_X$ gives an isomorphism $Z(x_0x_2 - x_1^2) \cong \mathbb{P}^1$. This is an example of

Definition 7.5. Let $n, d \geq 1, N = \binom{n+d}{n} - 1$. Then $\nu_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$ given by $(x_0: \dots: x_n) \mapsto (x_0^d: x_0^{d-1}x_1: \dots: x_n^d)$ is the **degree d Veronese embedding of $\mathbb{P}^n$** . $\nu_d(\mathbb{P}^n)$ is a projective variety, and ν_d is an isomorphism onto its image

Remark. A homogeneous degree d polynomial F has its zero locus mapped to a hyperplane under the Veronese

2. Let $m, n \geq 1$ and $N = (n+1)(m+1) - 1$. The **Segre embedding** is $\sigma_{m,n}: \mathbb{P}^m \times \mathbb{P}^n \rightarrow \mathbb{P}^N$ by

$$((x_0: \dots: x_m), (y_0: \dots: y_n)) \mapsto (x_0y_0: x_0y_1: \dots: x_my_n)$$

We write z_{ij} for x_iy_j in the image of this embedding

Proposition 7.4. $\sigma_{m,n}$ is a bijection onto its image and the projection maps forming its inverse are morphisms.

The image, $\Sigma_{m,n} = \sigma_{m,n}(\mathbb{P}^m \times \mathbb{P}^n) = Z(I)$ is a projective variety with I generated by $(z_{ij}z_{pq} - z_{iq}z_{pj})$

I is prime, so $\Sigma_{m,n}$ is irreducible

Proof. $\Sigma_{m,n} \subset Z(I)$ is clear. Suppose that $(a_{00}: \dots: a_{mn}) \in Z(I)$. There is some i, j such that $a_{ij} \neq 0$, and assume $a_{ij} = 1$. Define $x = (x_0, \dots, x_m)$ by $x_p = a_{pj}$ and $y = (y_0: \dots: y_n)$ by $y_q = a_{iq}$. The image $(z_{00}: \dots: z_{mn})$ of (x, y) satisfies $z_{pq} = a_{pj}a_{iq} = a_{ij}a_{pq} = a_{pq}$ so equality holds $I = \ker(k[z_{00}, \dots, z_{mn}] \rightarrow k[x_0, \dots, x_m, y_0, \dots, y_n])$ by $z_{ij} \rightarrow x_iy_j$ so I is prime and $\Sigma_{m,n}$ is irreducible $\square$

Definition 7.6. Let $X \subset \mathbb{P}^m, Y \subset \mathbb{P}^n$ be projective varieties. The Zariski topology on $X \times Y$ is given by identifying it with $\sigma_{mn}(X \times Y)$

If $m = n = 1$, $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$ identifies $\mathbb{P}^1 \times \mathbb{P}^1$ with $Z(z_0, z_3 - z_1z_2)$. If we fix $P \in \mathbb{P}^1$ then $P \times \mathbb{P}^1, \mathbb{P}^1 \times P$ are closed curves in $Z(z_0, z_3 - z_1z_2)$ isomorphic to $\mathbb{P}^1$

A deeper statement is

Theorem 7.1. *Projective varieties are **complete** (ie. if X is a projective variety then for any algebraic variety Y , $X \times Y \xrightarrow{\pi_2} Y$ sends closed sets to closed sets)*

Proof. No Proof □

This is the algebraic geometry version of compactness.
Recall that $\mathbb{A}^1 \times \mathbb{A}^1 \rightarrow \mathbb{A}^1$ is not a closed map

Corollary 7.1.1. *Let $f: X \rightarrow Y$ be a morphism of projective varieties. Then f is a closed map*

Proof. The map $X \rightarrow X \times Y$ by $x \mapsto (x, f(x))$. This is closed, and so f as the composition of this with the projection onto the second factor, is closed □

Corollary 7.1.2. *Let X be an irreducible projective variety. Then all regular functions on X are constant*

Proof. $X \rightarrow \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ is closed, hence has image a finite union of points, hence has image a single point as X is irreducible. □

Definition 7.7. A rational map $f: X \dashrightarrow Y$ of irreducible projective varieties is **dominant** if $f(X)$ is dense in Y . A rational map is **birational** if it has rational inverse. In this case there are $U \subset X, V \subset Y$ which are open and dense such that $U \cong V$

Example 7.5. (Monomial maps) Take $A \in SL_n(\mathbb{Z})$ and define a rational map $h_A: \mathbb{A}^n \dashrightarrow \mathbb{A}^n$ by $(t_1, \dots, t_n) \mapsto (t_1^{a_{11}} \dots t_n^{a_{1n}}, \dots, t_1^{a_{n1}} \dots t_n^{a_{nn}})$. By definition, h_A is a morphism on $\mathbb{A}^n \setminus Z(t_1 \dots t_n)$. We can homogenise h_A to extend to a map $h_A: \mathbb{P}^n \dashrightarrow \mathbb{P}^n$, which is birational with inverse $h_{A^{-1}}$.

Example 7.6. (Cremona involution) In particular if $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ we get $h_A(t_1, t_2) = (\frac{1}{t_1}, \frac{1}{t_2})$ and so $h_A([t_0: t_1: t_2]) = [t_1 t_2: t_0 t_2: t_0 t_1]$

Remark. If $f: X \dashrightarrow Y, g: Y \dashrightarrow Z$ are rational maps, then $g \circ f$ is a rational map if we assume that f is dominant. In particular if $\phi: X \dashrightarrow Y$ is dominant and g is a rational function on Y , then $g \circ \phi$ is a rational function on X . Therefore a dominant rational map $\phi: X \dashrightarrow Y$ induces $\phi^*: K(Y) \rightarrow K(X)$ which is an injection

Theorem 7.2. *Let X, Y be varieties. The map $\phi \mapsto \phi^*$ is a bijection between the set of dominant rational maps and k extensions $k(Y) \hookrightarrow k(X)$*

Proof. (Non-examinable sketch) Without loss of generality, X, Y are affine. Suppose we have $i: k(Y) \rightarrow K(X)$. Consider the generators $\{y_j\}$ of $A(Y)$, with images $i(y_j) = \frac{a_j}{b_j}$ for $a_j, b_j \in A(X)$. These each define regular functions on $X \setminus \bigcup_j Z(b_j) = X'$ and so we obtain a map $A(Y) \rightarrow A(X')$, and hence we get a map $X' \rightarrow Y$, which is a rational map from X to Y and this inverse correspondence works. □

8 Tangent Spaces, Singularities and Dimension

Given a curve $C = Z(f)$ in $\mathbb{A}^2$, the tangent line at $(x_0, y_0) \in C$ is

$$\frac{\partial f}{\partial x}(x_0)(x - x_0) + \frac{\partial f}{\partial y}(y_0)(y - y_0) = 0$$

. More generally for $Z(f) \subset \mathbb{A}^n$, the linear subspace V at $P \in X$ obtained by linear terms is

$$V = \left\{ (x_1, \dots, x_n) \in \mathbb{A}^n \mid \sum_{i=1}^n \frac{\partial f}{\partial x_i}(P)(x_i - p_i) = 0 \right\}$$

We can verify that an affine line $L = \{(p_1 + tb_1, \dots, p_n + tb_n \mid t \in k)\}$ is contained in V if and only if $f(p_1 + tb_1, \dots, p_n + tb_n)$ vanishes to order greater than 1 at P . ie L is a tangent line to $Z(f)$ at P

Definition 8.1. Let $X \subset \mathbb{A}^n$ be an affine variety, $P \in X$. The **tangent space** to X at P is

$$T_{X,P} = \left\{ (v_1, \dots, v_n) \in k^n \mid \sum_{i=1}^n \frac{\partial f}{\partial x_i}(P)v_i = 0, \forall f \in I(X) \right\}$$

Example 8.1. If $X = Z(x + y + z^2 + xyz, x - 2y + z + x^2y^2z^3) \subset \mathbb{A}^3$ and $P = 0 \in X$, then

$$T_{X,0} = \{(v_1, v_2, v_3) \mid v_1 + v_2 = 0, v_1 - 2v_2 + v_3 = 0\}$$

which is a line in k^3 , parameterised by $(-t, t, 3t)$

Example 8.2. If $Y = Z(x + y + z^3 + xyz, x + y + x^2 + y^3 - 4z^5)$. Then $P = 0 \in Y$ and

$$T_{Y,0} = \{(v_1, v_2, v_3) \mid v_1 + v_2 = 0\}$$

is a plane in k^3

This are both curves, with different tangent space dimensions at the origin. Suppose $P \in X$, without loss of generality, by translating, $P = 0$. Then $T_{X,P}$ is generated by the linear parts of elements of $I(X)$. Now if $X = \mathbb{A}^n$ and $f(P) = 0$, ie $f \in \mathfrak{m}_P$. Consider df , the linear part of f . The map $f \mapsto df$ can be thought of as a map $\mathfrak{m}_P \rightarrow (T_{\mathbb{A}^n,0})^*$. The kernel of this map is $\mathfrak{m}_P^2$. We therefore have an identification $(T_{\mathbb{A}^n,0})^* \cong \mathfrak{m}_P / \mathfrak{m}_P^2$ (it is a lemma that the latter does not depend on whether it is viewed in $A(X)$ or $\mathcal{O}_{X,P}$). This is called the **cotangent space** to X at P

Proposition 8.1. Let $X \subset \mathbb{A}^n$ be an affine variety and $P \in X$. Then there is a natural isomorphism of vector spaces $(T_{X,P})^* \cong \mathfrak{m}_P / \mathfrak{m}_P^2$

Proof. We know that $T_{X,P} \subset k^n$, so taking duals we get a surjective map $(k^n)^* \rightarrow (T_{X,P})^*$ given by restriction. Again without loss of generality, $P = 0$. Composing restriction with $f \mapsto df$, we get a map $D: M \rightarrow (T_{X,P})^*$ where $M = (x_1, \dots, x_n)$. D is surjective. Suppose that $x \in MA(X)$ and $Df = 0$. Then df is a linear combination of linear parts of $I(X)$, so $f \in M^2$ and we are done. $\square$

Definition 8.2. If $X \subset \mathbb{P}^n$ is a projective variety and $P \in S$ then the **tangent space** to X at P is $T_{X_i,P}$ for any standard affine patch X_i of X containing P . We denote this $T_{X,P}$. By the previous proposition, this is well defined

More generally if $X \subset \mathbb{P}^n, Y \subset \mathbb{P}^m$ are projective varieties and $\phi: X \dashrightarrow Y$ is a dominant rational map with P in its domain. Restricting to affine patches containing $P, \phi(P)$, we can define a linear map $d\phi_P: T_{X,P} \rightarrow T_{Y,\phi(P)}$ by, if $\phi = (f_1, \dots, f_m)$, then $d\phi_P$, the **derivative** or **linearisation** of ϕ at P is the map $(v_1, \dots, v_n) \mapsto \left(\sum_{i=1}^n v_i \frac{\partial f_1}{\partial x_i}(P), \dots, \sum_{i=1}^n v_i \frac{\partial f_m}{\partial x_i}(P) \right)$

Proposition 8.2. *With the notation above,*

1. $d\phi_P(T_{X,P}) \subset T_{Y,\phi(P)}$
2. $d\phi_P$ is linear
3. $d\phi_P$ is independent of the choice of representative of ϕ
4. If $\psi: Y \dashrightarrow Z$ is dominant rational, then $d(\psi \circ \phi)_P = d\psi_{\phi(P)} \circ d\phi_P$
5. If ϕ is birational and ϕ^{-1} is regular at $\phi(P)$ then $d\phi_P$ is an isomorphism

Proof. 1. By definition, the image is an element of the tangent space at $\phi(P)$ if

$$\sum_{j=1}^m \left(\sum_{i=1}^n v_i \frac{\partial f_j}{\partial x_i}(P) \right) \frac{\partial g}{\partial y_j}(\phi(P)) = 0$$

for all $g \in I(Y)$. Considering ϕ^* on function fields, $h = g(f_1, \dots, f_m)$ is in $I(X)$. Since $(v_1, \dots, v_n) \in T_{X,P}$, this follows from the chain rule

2. By definition
3. Suppose $\phi = (f_1, \dots, f_m) = (f'_1, \dots, f'_m)$. Then $f_i - f'_i = \frac{p_i}{q_i}$ for $p_i \in I(X)$ and $q_i(P) \neq 0$. Then $\frac{\partial(f_j - f'_j)}{\partial x_i}(P) = \frac{\partial p_j}{\partial x_i}(P)/q_j$ so for $v \in T_{X,P}$, the linear sum of these differences (weighted by v_i) is 0, so done
4. Chain rule (normal version)
5. Immediate from 4

$\square$

Definition 8.3. Let X be an affine or projective variety. If X is irreducible define the **dimension** of X to be $\dim X = \min_{P \in X} \dim(T_{X,P})$. Further we say X is **smooth/non-singular** if $\dim T_{X,P} = \dim X$. Otherwise we say P is **singular**. If X is reducible, define the dimension of X to be the maximal dimension of its irreducible components. If X is reducible, and P lies only on a single irreducible component X_i then P is a smooth point of X if and only if it is a smooth point of X_i . Otherwise P is singular. In either case, X is smooth if it has no singular points

Example 8.3. $\dim \mathbb{A}^n = \dim \mathbb{P}^n = n$ and all points are smooth
 If $k = \mathbb{C}$ and $X = Z(f)$, $f \in \mathbb{C}[x_1, \dots, x_n]$ an irreducible hypersurface in $\mathbb{A}_{\mathbb{C}}^n$. For $P \in X$, the tangent space, $T_{X,P}$ is defined by the vanishing of the linear form coming from f expanded around P , so $T_{X,P}$ is either all of k^n (where the linear form is trivial) or an $n - 1$ dimensional linear subspace. The linear form is $(\frac{\partial f}{\partial x_1}(P), \dots, \frac{\partial f}{\partial x_n}(P))$ which is non-trivial if there is at least 1 non-vanishing partial. Without loss of generality, $\frac{\partial f}{\partial x_1}(P)$ doesn't vanish. The map $(x_1, \dots, x_n) \mapsto (f(x_1, \dots, x_n), x_2, \dots, x_n)$ has a Jacobian with non-zero determinant and so the inverse function theorem applies, so locally around P , X looks like a ball in $\mathbb{A}^{n-1}$

Tangent spaces for projective varieties actually need irreducibility to compute using affine patches

Example 8.4. $X = Z(xy) \subset \mathbb{P}^2$. $X \cap U_x = \{(1: 0: z) \mid z \in k\} \cong \mathbb{A}^1$ and $X \cap U_y = \{(0: 1: z) \mid z \in k\} \cong \mathbb{A}^1$ but

$$X \cap U_z = \{(0: y: 1) \mid y \in k\} \cup \{(x: 0: 1) \mid x \in k\} \cong \mathbb{A}^1$$

is a union of lines

If $Z(f) \subset \mathbb{A}^2$ and f has no linear terms then if $0 \in Z(f)$, it is automatically a singular point

Example 8.5. The **nodal cubic curve** is $Z(y^2 - x^2(x+1))$ and the **cuspidal cubic curve** is $Z(y^2 - x^3)$

Remark. The two curves of example 8.5 are not isomorphic, but looking at tangent spaces doesn't distinguish them. We need to consider $\mathfrak{m}/\mathfrak{m}^2, \mathfrak{m}^2/\mathfrak{m}^3, \dots$

Theorem 8.1. *Let X be an algebraic variety. The set of smooth points of X is an open dense subset*

Proof. Since the intersection set of distinct components is a proper closed subvariety of X , we can without loss of generality assume X is irreducible. We may further assume X is affine as $X \cap \mathbb{A}^n$ is open dense in X . Suppose that $I(X) = (f_1, \dots, f_r)$. If $P \in X$, then $T_{X,P}$ is the zero locus of all linearizations about P , $\dim T_{X,P} = n - \text{rank} \left(\frac{\partial f_i}{\partial x_j}(P) \right)$. The rank is computed by $(n - r) \times (n - r)$ minors of the matrix of polynomials $\left(\frac{\partial f_i}{\partial x_j}(P) \right)$ which can't all be in $I(X)$ for degree reasons $\square$

Corollary 8.1.1. *If X, Y are birational varieties, then $\dim X = \dim Y$*

Proof. Restrict $\phi: X \dashrightarrow Y$ to the smooth locus, and similarly with ϕ^{-1} to obtain isomorphisms of the tangent spaces which realise the dimension. $\square$

Definition 8.4. Given an extension of fields $K \leq L$, we say $x_1, \dots, x_n \in L$ are **algebraically independent** over K if there is no non-trivial polynomial $p \in k[t_1, \dots, t_n]$ such that $p(x_1, \dots, x_n) = 0$

Example 8.6. $k(\mathbb{A}^n)$ has n algebraically independent elements $k(Z(y^2 - x(x-1)(x+1)) \subset \mathbb{A}^2)$ is the function field of $k[x, y]/(y^2 - x(x-1)(x+1))$ has x, y be algebraically dependent, so $\{x\}, \{y\}$ are algebraically independent sets, but $\{x, y\}$ is not

If $K \leq L$ is finitely generated by $x_1, \dots, x_m$, we can find an algebraically independent subset of $\{x_1, \dots, x_m\}$, call it $\{x_{i_1}, \dots, x_{i_k}\}$ which has maximal size. Renaming these to $x_1, \dots, x_k$, we have $K \leq K(x_1, \dots, x_k) \leq L$ with the first extension **purely transcendental** and the latter extension algebraic. By the primitive element theorem, $L = K(x_1, \dots, x_k)(y)$ for a single $y \in L$. Any set $\{x_1, \dots, x_r\} \subset L$ which generate a pure transcendental extension called $K_0 = K(x_1, \dots, x_r)$ such that L/K_0 is finite is a **transcendence basis** for L/K

Definition 8.5. The **transcendence degree** of a finitely generated field extension L/K is the size of any transcendence basis

Proposition 8.3. *Let $K = k(x_1, \dots, x_n)$ with $x_1, \dots, x_n$ algebraically independent over k and $K \leq L$ is a field extension. If $x_{n+1} \in L$ is algebraic over K then $I = \{g \in k[t_1, \dots, t_n, t_{n+1}] \mid g(x_1, \dots, x_n, x_{n+1}) = 0\}$ is a principal ideal generated by some irreducible $f \in k[t_1, \dots, t_{n+1}]$. If f contains t_i , then $\{x_1, \dots, \hat{x}_i, \dots, x_{n+1}\}$ is an algebraically independent set over k*

Proof. Note that $k[t_1, \dots, t_n] \subset K$ is suitable for Gauss's lemma and $K[t]$ is a PID. I has a generator in $K[t]$ which gives an irreducible generator for I in the asserted ring. If $\{x_1, \dots, \hat{x}_i, \dots, x_{n+1}\}$ is algebraically dependent then there is some $g \in I$ which doesn't include t_i , but I is generated by a polynomial containing t_i contradiction $\square$

Corollary 8.1.2. *Transcendence degree is well defined*

Proof. No Proof $\square$

Lemma 8.2. *(Reduction to hypersurface) If X is an irreducible algebraic variety then X is birational to a hypersurface*

Proof. Find $K_0 = k(x_1, \dots, x_n)$ purely transcendental such that $k(X)/K_0$ is finite, with generator y . By the previous proposition, there is an irreducible $f \in k[x_1, \dots, x_n, y]$ such that $k[x_1, \dots, x_n, y] \cong k[x_1, \dots, x_n, y]/(f)$, which is the coordinate ring of a hypersurface in $\mathbb{A}^{n+1}$, and $k(X)$ is the function field of the left hand side, and the right hand side is the function field of the hypersurface, so X is birational to a hypersurface $\square$

Corollary 8.2.1. *For any algebraic irreducible variety X , $\dim X$ is the transcendence degree of $k(X)/k$, written $\text{trdeg}_k(k(X))$*

Proof. By the reduction lemma it suffices to prove it for hypersurfaces. If $P \in X$, then $T_{X,P}$ has dimension n or $n - 1$. On a Zariski open subset, it is $n - 1$. We have $k(X)$ is isomorphic to the function field of $k[x_1, \dots, x_n]/(f)$ for some irreducible f , which has $\text{trdeg} = n - 1$ since f is non-constant. $\square$

9 Structure of Algebraic Curves

Definition 9.1. A **curve** is a smooth, projective, irreducible variety of dimension 1 unless otherwise qualified

Example 9.1. We have a rich source of curves from hypersurfaces in $\mathbb{P}^2$ where $C = Z(f)$ for non-constant homogeneous $f \in k[x_0, \dots, x_2]$ of degree d . f is defined by $\binom{d+2}{2}$ coefficients. We can use the coefficients of f to identify the set of degree d hypersurfaces in $\mathbb{P}^2$ with $\mathbb{P}^{\binom{d+2}{2}-1}$. Reducibility of $Z(f)$ is a Zariski closed condition under this identification. Since there are irreducible polynomials of every degree (eg. $x^d + y^d + z^d$ as we work in characteristic 0 in this course), there is an open dense set of irreducible hypersurfaces. Inside $\mathbb{P}^{\binom{d+2}{2}-1} \times \mathbb{P}^2$ there is a closed subvariety which cuts out the relation $f(P) = 0$ where the first coordinate gives f and the second gives P . The vanishing of the partials are closed conditions, and hence curves and their smooth points cut out an open dense subset of $\mathbb{P}^{\binom{d+2}{2}-1} \times \mathbb{P}^2$, so as projective space is proper, the result descends to curves giving an open dense subset of $\mathbb{P}^{\binom{d+2}{2}-1}$.

Theorem 9.1. (*Generalised Eisenstein*) *Let R be an integral domain, $\mathfrak{p}$ a prime ideal of R , $f(x) = a_n x^n + \dots + a_0$ where $a_n \notin \mathfrak{p}, a_i \in \mathfrak{p}, a_0 \notin \mathfrak{p}^2$ for $0 \leq i \leq n-1$. Then if $f(x) = g(x)h(x) \in R[x]$ then one of g, h is constant*

Proof. Trivial $\square$

Example 9.2. $x^d + y^d + z^d \in k[x, y, z]$. Consider this as a polynomial in x over $k[y, z]$. Then $a_0 \in (x \pm y)$ for some choice of sign but $a_0 \notin (x \pm y)^2$ so it is irreducible

Example 9.3. $Z(x^d + y^d + z^d)$ is a smooth irreducible projective variety of dimension 1, so is a curve in $\mathbb{P}^2$

Remark. (Euler's homogeneous identity) If f is homogeneous of degree d in n variables, then $F(x_1, \dots, x_n) \cdot \deg f = \sum_{i=1}^n x_i \frac{\partial F}{\partial x_i}(x_1, \dots, x_n)$ as the formula is linear and it is clear for monomials

Proposition 9.1. *Let C be a curve and $D \subset C$ a proper closed subvariety. Then D is a finite union of points*

Proof. Without loss of generality, C is affine and D is irreducible. We know that $I(C) \subset I(D)$ is strict, so we have a surjective map with non-trivial kernel $\phi^*: A(C) \rightarrow A(D)$ induced by $D \hookrightarrow C$. So if D is not just a point, by Nullstellensatz, $A(D)$ strictly contains k , hence $k(D)$ contains a transcendental as k is algebraically closed. Clear denominators, and call this transcendental $t \in A(D)$ and choose $1 \neq x, y \in A(C)$ such that $\phi^*(x) = 1$ and $\phi^*(y) = t$ so x, y are algebraically independent in $A(C)$ and hence in $k(C)$, contradiction $\square$

Theorem 9.2. *If $P \in C$ is a smooth point of an irreducible projective variety of dimension 1, then the ideal $\mathfrak{m}_P \subset \mathcal{O}_P$ is principal*

Proof. We change variables to assume $P = 0$ and $T_{C,P} = \{x_2 = \cdots = x_n = 0\}$ where $C \subset \mathbb{A}^n$. So there are polynomials $f_2, \dots, f_n \in I(C)$ such that each $f_j = x_j + o(x)$. Hence in $\mathcal{O}_P$ we have $x_j = h_j \in \mathfrak{m}_P^2$ so $\mathfrak{m}_P = x_1\mathcal{O}_P + \mathfrak{m}_P^2$. We will use a powerful algebraic tool

Lemma 9.3. (Nakayama's Lemma) *Let R be a ring and M be a finitely generated R module and let $J \subset R$ be an ideal. Then*

1. *If $JM = M$ then there is $r \in J$ such that $(1 + r)M = 0$*
2. *If $N \subset M$ is a submodule such that $JM + N = M$, there is some $r \in J$ such that $(1 + r)M \subset N$*

Proof. (1) Write $M = y_1R + \cdots + y_nR$ with $y_i \in M = JM$. Write $y_i = \sum_j x_{ij}y_j$ for $x_{ij} \in J$. Let $X = (x_{ij})$ so that $(I - X)y = 0$. Multiplying by the adjugate of $I - X$, we get $\det(I - X)y = 0$, so $\det(I - X)y_i = 0$ for all $1 \leq i \leq n$ and $\det(I - X) = 1 + r$ for some $r \in J$

(2) Apply (1) to M/N and use correspondence theorem $\square$

Now we may apply Nakayama with $N = x_1\mathcal{O}_P \subset M = \mathfrak{m}_P = J$ for the ring $R = \mathcal{O}_P$. We get some $r \in \mathfrak{m}_P$ such that $(1 + r)M \subset N$. Since $r \in \mathfrak{m}_P$, $1 + r$ is a unit, so $M \subset N$ and $\mathfrak{m}_P = x_1\mathcal{O}_P$ $\square$

Corollary 9.3.1. *Let C be the affine plane curve (possibly singular) $Z(f) \subset \mathbb{A}^2$ and $P \in C$ be smooth. Then the function $C \rightarrow k$ sending $Q \mapsto x(Q) - x(P)$ is a local coordinate at P if $\frac{\partial f}{\partial y}(P) \neq 0$ (and similarly with the roles of x, y reversed)*

Proof. If $P = (0, 0)$ with tangent line $\{aX + bY = 0\}$, then the proof of the previous theorem shows that $Y \in X\mathcal{O}_P + \mathfrak{m}_P^2$ precisely when $\frac{\partial f}{\partial y} \neq 0$ and so in this case, $x - x(P)$ is a local coordinate at P . In the general case we just shift. $\square$

If a local parameter exists at P , then $\mathcal{O}_P$ is a discrete valuation ring

Corollary 9.3.2. *Suppose P is a smooth point of a possibly singular curve C . Then there exists a surjective homomorphism $\nu_P: k(C) \setminus \{0\} \rightarrow \mathbb{Z}$ called the **evaluation** at P which satisfies*

1. $\mathcal{O}_P = \{0\} \cup \{f \in k(C)^* \mid \nu_P(f) \geq 0\}$

$$2. \mathfrak{m}_P = \{0\} \cup \{f \in \mathcal{O}_P \mid \nu_P(f) > 0\}$$

$$3. \nu_P(x + y) \geq \min\{\nu_P(x), \nu_P(y)\} \text{ with equality if } \nu_P(x) \neq \nu_P(y)$$

(ie $\mathcal{O}_P$ is a **discrete valuation ring**). If $f \in k(X)^*$, then for any local parameter π_P at P , there is a unit $u \in \mathcal{O}_P^*$ such that $f = u\pi_P^{\nu_P(f)}$. $\nu_P(f)$ is called the **order of vanishing** at P

We often notationally define $\nu_P(0) = \infty$

Proof. Without loss of generality, C is affine. Write $\mathfrak{m}_P = (\pi_P)$ by the previous theorem. Consider the ideal $I = \bigcap_{n \in \mathbb{N}} \mathfrak{m}_P^n$. We claim $I = 0$. We have $\mathfrak{m}_P I = I$ and hence as $\mathcal{O}_P$ is Noetherian, I is finitely generated, by Nakayama, there is some $m \in \mathfrak{m}_P$ such that $(1 + m)I = 0$, and hence $I = 0$. Hence for any non-zero $f \in \mathcal{O}_P \setminus \{0\}$ there is some n such that $f \in \mathfrak{m}_P^n \setminus \mathfrak{m}_P^{n+1}$. Define $\nu_P(f) = n$. For arbitrary $f = g/h \in k(C)^\times$ with $g, h \in \mathcal{O}_P$, we define $\nu_P(f) = \nu_P(g) - \nu_P(h)$. We may then check that this is a well defined homomorphism to $\mathbb{Z}$ and 1, 2 are trivial. The remarks at the end follow similarly easily as we can do it for elements of $\mathcal{O}_P$. To prove 3, suppose $x = u\pi_P^m, y = v\pi_P^n$ for u, v units and $m, n \in \mathbb{Z}$. Then $x + y = u\pi_P^m + v\pi_P^n$ and without loss of generality $m \leq n$. Then $x + y = \pi_P^m(u + v\pi_P^{n-m})$ and the inequality follows as the latter term is regular, and if the two valuations are not equal, the latter term is a unit so the full result follows. $\square$

Remark. If P is a smooth point on a possibly singular curve C and $f \in k(C)^*$ then either f or $1/f$ is regular at P

Theorem 9.4. Let X be a curve and $\phi: X \dashrightarrow \mathbb{P}^m$ a rational map. Then ϕ is a morphism on X . In particular, birational curves are isomorphic

Proof. Without loss of generality choose coordinates so that $\phi(X) \not\subset \{x_0 = 0\}$. Write $\phi = (G_0 : \dots : G_m) = (1 : G_1/G_0 : \dots : G_m/G_0)$. If all of these are regular at P , then ϕ is regular at P . Otherwise, we can define the minimum of all the valuations, $t = \min\{\nu_P(G_i/G_0) \mid 1 \leq i \leq m\}$. Multiplying by π_P^{-t} , we get $\phi = (\pi_P^{-t} : \dots : \pi_P^{-t} G_m/G_0)$ which is a representation with at least one coordinate of zero valuation, all are non-negative so ϕ is regular at P . If ϕ is birational with inverse ψ then $\psi \circ \phi$ is a birational map which is the identity on an open dense subset $U \subset X$. ϕ, ψ extend to morphisms so it suffices to show that if $f: X \rightarrow X$ is a morphism which is the identity on U , then f is the identity on X . Consider the map $f \times \text{Id}_X: X \rightarrow X \times X$. This takes U into the diagonal, so takes $X = \bar{U}$ into the diagonal as the diagonal is closed so we are done. $\square$

10 Maps between Curves

Example 10.1. Let $C_d \subset \mathbb{P}^2$ be $C_d = Z(f_d)$ for f_d homogeneous of degree d and let $P \in \mathbb{P}^2$. Projection from P gives a morphism $C_d \rightarrow \mathbb{P}^1$. Smoothness is necessary: consider the nodal cubic $X = Z(y^2z - x^2(x + z))$. At $(0, 0, 1)$ it

crosses itself. Then projection $(x: y: z) \mapsto (x: y)$ can't be continuously defined at $(0: 0: 1)$

Proposition 10.1. *Suppose that $\phi: X \rightarrow Y$ is a non-constant homomorphism of possibly singular curves*

1. *For all $Q \in Y$, $\phi^{-1}(Q)$ is finite*
2. *$\phi^*: k(Y) \rightarrow k(X)$ is an inclusion which makes $k(X)$ a finite extension of $\phi^*(k(Y)) \cong k(Y)$*

Proof. 1. $\phi^{-1}(Q)$ is closed and hence is finite

2. $\phi(X)$ is dense in Y as $\phi(X)$ is infinite so ϕ is dominant and ϕ^* is injective. Let $t \in k(Y) \setminus k$. Then $x = \phi^*(t) \in k(X) \setminus k$. x is transcendental as k is algebraically closed, and so as $\text{trdeg}(k(X)) = 1$, $k(X)/\phi^*(k(Y))$ is a finite extension

□

Definition 10.1. The **degree** of $\phi: V \rightarrow W$ a non-constant map of curves is $\deg \phi = [k(v): \phi^*k(W)]$

Definition 10.2. Suppose $P \in V$ and $Q = \phi(P) \in W$, for $\phi: V \rightarrow W$ a non-constant map of curves, are smooth. The **ramification degree** of ϕ at P is $e_P = v_P(\phi^*\pi_Q)$ where π_Q is a local parameter at Q and v_P is the valuation associated to P on $k(V)^\times$. If $e_P = 1$ then ϕ is **unramified** at P , otherwise ϕ is **ramified** at P

Remark. $e_P = \min\{v_P(x) \mid x \in \phi^*(\mathfrak{m}_Q)\mathcal{O}_{V,P}\}$ where $\mathfrak{m}_Q$ is the unique maximal ideal of $\mathcal{O}_{W,Q}$ so e_P doesn't depend on choice of π_Q

If ϕ is an isomorphism then $\phi^*(\mathfrak{m}_Q)\mathcal{O}_{V,P} = \mathfrak{m}_P$ so $e_P = 1$ for all $P \in V$

Example 10.2. If we have $\phi: \mathbb{A}^1 \rightarrow \mathbb{A}^1$ corresponding to $\phi^*: k[x] \rightarrow k[x]$ by $x \mapsto x^d$. We have $e_0 = d$, as x is a local parameter at 0, and pulls back to x^d . We have $e_1 = 1$ as $x - 1$ is a local parameter, and this pulls back to $x^d - 1$ which has one factor of $x - 1$

Example 10.3. Let $E = Z(y^2 - x^3 + x)$ and $\phi: E \rightarrow \mathbb{A}^1$ by $(x, y) \mapsto x$. We have $\phi^*: k[x] \rightarrow k[x, y]/(y^2 - x^3 + x)$ defined by $x \mapsto x$. Let $P = (x_0, y_0) \in E$ with image $Q = x_0$. Then $e_P = v_P(\phi^*(x - x_0)) = v_P(x - x_0)$. When is $x - x_0$ a local parameter of $\mathcal{O}_{E,P}$? It is a local parameter exactly when $\frac{\partial f}{\partial y}(P) \neq 0$ where $f = y^2 - x^3 + x$, that is, when $2y = 0$ and hence $y = 0$ so $v_P(x - x_0) = 1$ if and only if $y_0 \neq 0$. We consider the case $y_0 = 0$. Then $x_0 \in \{0, \pm 1\}$. We see that $\frac{\partial f}{\partial x}(P) \neq 0$ and so y is a local parameter at P . We see from the defining equation $y^2 = x(x - 1)(x + 1)$ that $x - x_0 = uy^2$ for some unit $u \in \mathcal{O}_{E,P}^\times$, and so $e_P = 2$ in this case.

Theorem 10.1. *Let $\phi: V \rightarrow W$ is a non-constant map between irreducible projective possibly singular curves*

1. ϕ is surjective and for all but finitely many points $P \in V$, $e_P = 1$ (so ϕ is unramified at P)
2. If V, W are additionally smooth, then for all $Q \in W$,

$$\sum_{P \in \phi^{-1}(Q)} e_P = \deg \phi$$

Proof. We will only prove 1, no proof of 2 will be given. Since V is projective, completeness shows that $\phi(V) \subset W$ is closed. As the image is not finite as V is irreducible and ϕ is non-constant, it is therefore everything. We now prove that ϕ is unramified at all but finitely many points $P \in V$. Note that $e_P = 1$ if and only if $\phi^*(\mathfrak{m}_Q)\mathcal{O}_{V,P} = \mathfrak{m}_P$ where $Q = \phi(P)$. We may remove finitely many points from V, W , so we may assume they are affine: $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$. Now ϕ factors as $V \xrightarrow{(\text{id}, \phi)} V \times W \xrightarrow{\pi} W$. Since the first map is an isomorphism of varieties onto its image, we may assume $V \subset \mathbb{A}^{n+m}$ and ϕ is the restriction of the projection map onto $\mathbb{A}^m$. Suppose $P \in V$ and $Q = \phi(P) = (q_1, \dots, q_m)$. Then $\mathfrak{m}_Q = (y_1 - q_1, \dots, y_m - q_m)$ and so $e_P = 1$ if and only if we have that $(y_1 - q_1, \dots, y_m - q_m)\mathcal{O}_{V,P} = \mathfrak{m}_P$. By the primitive element theorem, $k(V) = k(W)[\alpha]$ for some $\alpha \in k(V)$. Away from the (finite set) of poles of α , $\mathfrak{m}_P = (y_1 - q_1, \dots, y_m - q_m, \alpha - \alpha(P))$ and so $e_P = 1$ if and only if we have that $\alpha - \alpha(P) \in \mathfrak{m}_Q\mathcal{O}_{V,P}$. α has minimal polynomial of the form

$$p(y_1, \dots, y_m, x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0$$

for $a_i \in k[y_1, \dots, y_m]$. This factors as $a_d \prod_{i=1}^d (x - \beta_i)$ in $\overline{k(W)}$. We can then consider $\text{disc}(p)$ which is in $k(W)$ by Galois theory. As in the examples before, away from the poles of all the a_i , the set of $\{P \in V \mid \text{disc}(p)(\phi(P)) \neq 0\}$ consists of unramified points, and includes all but finitely many points of V as if $\text{disc}(p) \in I(W)$ then $\gcd(p', p) \neq 1$, contradiction as p is irreducible $\square$

Remark. If we additionally remove the set $\{Q \in W \mid a_d(Q) = 0\}$, then Q has exactly d preimages in V under ϕ , all unramified, and so for the remaining $Q \in W$ we have $\sum_{\phi(P)=Q} e_P = \sum_{P_1, \dots, P_d} 1 = d = \deg \phi$

Corollary 10.1.1. *Let V be a curve, and $f \in k(V)^*$ a non-zero rational function. Then*

1. *If f is regular on V , then f is constant*
2. *The set of points P with $v_P(f) \neq 0$ is finite, and $\sum_{P \in V} v_P(f) = 0$*

Proof. Use $\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ to view f as a morphism $\phi: V \rightarrow \mathbb{P}^1$.

For (1), if f is regular then ϕ is not surjective (it doesn't hit infinity) so it is constant.

For (2), $v_P(f) \neq 0$ if and only if f vanishes at P or $1/f$ vanishes at P . Now $\phi^{-1}(0), \phi^{-1}(\infty)$ are finite by hypothesis. The statement is clear if f is constant, so assume f is non-constant. Then ϕ is non-constant. Let $t = \frac{x_1}{x_0}$ be a local

coordinate at $(1: 0)$. Now $\phi^*(t) = f$ so, if $\phi(P) = (1: 0)$, we know that the ramification index $e_P = v_P(\phi^*(t)) = v_P(f)$. Similarly at infinity, $\frac{1}{t} = \frac{x_0}{x_1}$ is a local coordinate at $(0: 1)$ so if $\phi(P) = \infty$, then $e_P = v_P(\phi^*(1/f)) = -v_P(f)$. Therefore

$$\begin{aligned} \sum_{P \in V} v_P(f) &= \sum_{\phi(P)=0} v_P(f) + \sum_{\phi(P)=\infty} v_P(f) \\ &= \sum_{\phi(P)=0} e_P - \sum_{\phi(P)=\infty} e_P \\ &= \deg \phi - \deg \phi \\ &= 0 \end{aligned}$$

□

11 Divisors on Curves

If V is a projective curve then the regular functions on V are the constants, but the rational functions on V , $k(V)$ is infinite dimensional as a k -vector space. Divisor theory will help us understand the larger space

Definition 11.1. A **divisor** on a curve V is a finite formal sum $\sum_{P \in V} n_P P$ with $n_P \in \mathbb{Z}$. The set of divisors is the abelian group generated by points of the curve, denoted $\text{Div}(V) = \bigoplus_{P \in V} \mathbb{Z}P$. The **degree** of $\sum_{P \in V} n_P P$ is $\sum_{P \in V} n_P \in \mathbb{Z}$. The map $\deg: \text{Div}(V) \rightarrow \mathbb{Z}$ is a group homomorphism with kernel $\text{Div}^0(V)$ and the set $\{P \in V \mid n_P \neq 0\}$ is the **support** of the divisor D

Definition 11.2. Let $f \in k(V)$ be a non-zero rational function. The **divisor** of f , $\text{div}(f) = \sum_{P \in V} v_P(f)P$. We know that $\deg \text{div}(f) = 0$. Any divisor of the form $\text{div}(f)$ is called a **principal divisor** on V . These form a subgroup of $\text{Div}(V)$ (respectively $\text{Div}^0(V)$) and the quotient of $\text{Div}(V)$ by the principal divisors is called the **divisor class group** (**Picard group**) of V (respectively the **degree zero divisor class group**). D, D' are **linearly equivalent** if there is a rational function f such that $D - D' = \text{div} f$. We write $D \sim D'$

Suppose that $f, g \in k(V)$ for a curve V . If $\text{div}(f) = \text{div}(g)$ then for all $p \in V$, $v_p(f) = v_p(g)$. So $v_p(f/g) = 0$ for all P , and $\text{div}(f/g) = 0$ hence f/g is constant as it is not surjective as a morphism to $\mathbb{P}^1$

Proposition 11.1. Any degree 0 divisor on $\mathbb{P}^1$ is principal, and so $\text{Cl}^0(\mathbb{P}^1) = 0$ and $\text{Cl}(\mathbb{P}^1) = \mathbb{Z}$

Proof. Suppose that D is a degree 0 divisor on $\mathbb{P}^1$, write the divisor in the form $D = \sum n_P P = n_\infty \infty + \sum_{P \in \mathbb{A}^1} n_P P$. We know that $n_\infty = -\sum_{P \in \mathbb{A}^1} n_P$. Construct the polynomial $f(t) = \prod_{P \in \mathbb{A}^1} (t - P)^{n_P}$ for coordinate $t = \frac{x_1}{x_0}$. Since $1/t$ is a local coordinate at $\infty = (0: 1)$, $v_\infty(f) = -\sum_{P \in \mathbb{A}^1} n_P = n_\infty$ as needed so we are done. □

Remark. If V is a curve and $\text{Cl}^0(V) = 0$, then for $P \neq Q$, $P - Q$ is a degree 0 divisor, and hence is $\text{div}(f)$ for some $f \in k(V)$. Hence f determines a morphism $\phi: V \rightarrow \mathbb{P}^1$ which is unramified at P with $\phi^{-1}(0) = P$, hence ϕ is a degree 1 morphism, and so is an isomorphism as $k(V) = k(\mathbb{P}^1)$.

Definition 11.3. Suppose $V \subseteq \mathbb{P}^n$ is a curve and consider a hyperplane given by $H = Z(l) \subseteq \mathbb{P}^n$ which doesn't contain V . The **hyperplane section** of V by H is $\text{div}(H) = \sum_{P \in V} n_P P$ where $n_P = \nu_P(l/x_i)$ for any $x_i(P) \neq 0$.

Remark. 1. This is well defined as $x_i/x_j \in \mathcal{O}_P^\times$
 2. $n_P \geq 0$ for all P , as x_i doesn't have a pole at P
 3. If $H = Z(l), H' = Z(l')$ both don't contain V , then we can compute $\text{div}(H') - \text{div}(H) = \text{div}(l'/l)$ so all hyperplane sections are the same in $\text{Cl}(V)$. We call this the **hyperplane class**

Definition 11.4. The **degree** of $V \subset \mathbb{P}^n$ is $\deg V = \deg \text{div } H$ for any hyperplane H not containing V

Remark. This is not an isomorphism invariant, as isomorphisms need not send hyperplanes to hyperplanes. If $f: V \rightarrow W$ is an isomorphism of curves, $\text{Div}(V) \cong \text{Div}(W)$ and principal divisors are identified so $\text{Cl}(V) \cong \text{Cl}(W)$, however for example we can show that the twisted cubic in $\mathbb{P}^3$ has degree 3, but is isomorphic to $\mathbb{P}^1$. But a linear change of coordinates on $\mathbb{P}^n$ preserves degree as it preserves hyperplanes

If G is homogeneous of degree m and $V \subseteq \mathbb{P}^n$ we can similarly define a divisor $\text{div}(G) = \text{div}(Z(G)) = \sum n_P P$ for $n_P = \nu_P(G/x_i^m), x_i(P) \neq 0$, but this is just equivalent to $m \cdot \text{div}(H)$ as l^m is degree m

Example 11.1. Suppose $V \subseteq \mathbb{P}^2$. We claim there is a line not tangent to V at any point. Recall that we can identify the space of lines in $\mathbb{P}^2$ with $\mathbb{P}^2$ itself. The map sending P to the line tangent to V at P determines a morphism from V to $\mathbb{P}^2$. This image has dimension at most 1 and so there is at least 1 line not in the image, ie a line which is not tangent to V at any point. Linearly change coordinates to assume $\{x_0 = 0\}$ is such a line. Now $V = Z(f)$ for f homogeneous of degree d . Our tangency assumption implies $f(0, x_1, x_2)$ is a degree d homogeneous polynomial in 2 variables with no repeated linear factors. So there are exactly d points in $V \cap \{x_0 = 0\}$, and we know $\text{div}(\{x_0 = 0\}) = \sum_{P \in V \cap \{x_0 = 0\}} P$ and so $\deg V = \deg \text{div } H = d$

Remark. For a general choice of H , $|H \cap V| = d$

Definition 11.5. We say a divisor $D = \sum n_P P$ is **effective** if $n_P \geq 0$

Definition 11.6. Let $D = \sum n_P P$ be a divisor on a curve V . The **space of rational functions with poles bounded by D** is defined to be

$$\begin{aligned} L(D) &= \{f \in k(V) \mid \nu_P(f) + n_P \geq 0\} \\ &= \{f \in k(V) \mid f = 0 \text{ or } \text{div}(f) + D \text{ is effective}\} \end{aligned}$$

$f \mapsto \operatorname{div} f + D$ identifies $L(D)$ with the set of effective divisors which are equivalent to D

Remark. As $\nu_P(f + g) \geq \min\{\nu_P(f), \nu_P(g)\}$, we see $L(D)$ is a vector space over k

We summarise the definition as follows:

1. If $P \notin \operatorname{supp} D$, we require f is regular at P
2. If $n_P > 0$, then f has a pole of order at most n_P at P
3. If $n_P < 0$, f has a zero of order at least $-n_P$ at P

Example 11.2. If $V = \mathbb{P}^1$, write $(0: 1) = \infty$ and let $D = m(\infty)$ for $m > 0$. Write $x = x_1/x_0$. We see that $L(D)$ is spanned by $1, x, \dots, x^m$. So $L(D)$ picks out polynomials of degree at most m , and $\dim L(D) = m + 1$

Definition 11.7. We denote $l(D) = \dim L(D)$

Proposition 11.2. *If D is a divisor on V and*

1. $\deg D < 0$, then $l(D) = 0$
2. $\deg D \geq 0$, then $l(D) \leq \deg(D) + 1$
3. $P \in V$, $l(D) \leq l(D - P) + 1$

Proof. 1. If $\deg D < 0$ and $D' \sim D$, then $\deg D' < 0$ so D' is not effective

2. This is immediate by induction on the degree from 1, 3

3. Define $\operatorname{ev}_P: L(D) \rightarrow k$ by $f \mapsto (\pi_P^{n_P} f)(P)$ for a local parameter π_P at P . This is a well defined homomorphism with kernel

$$\{f \in L(D) \mid \nu_P(f) + n_P \geq 1\} = L(D - P)$$

The result follows by rank nullity. □

Proposition 11.3. *Suppose that $D, E \in \operatorname{Div}(V)$ such that $D \sim E$. Then $L(D) \cong L(E)$ and $l(D) = l(E)$*

Proof. If $D - E = \operatorname{div}(g)$ for some $g \in k(V)$ then consider $L(D) \rightarrow L(E)$ by $f \mapsto fg$.

To prove this is well defined, $f \in L(D)$ if and only if $f \in L(E + \operatorname{div}(g))$ if and only if $\operatorname{div}(g) + \operatorname{div}(f) + E \geq 0$ if and only if $\operatorname{div}(fg) + E \geq 0$ if and only if $fg \in L(E)$ and it is clearly a bijection as $g \mapsto g/f$ is an inverse □

11.1 Bezout's Theorem

Theorem 11.1. (*Weak Bezout for planar curves*) Any two distinct plane curves intersect and if their degrees are m, n respectively then they intersect in at most mn points

Proof. Let F, G be homogeneous forms in 3 variables of degree m, n respectively and call $C = Z(F), D = Z(G) \subseteq \mathbb{P}^2$. We have an effective divisor $\text{div}(G)$ which has the form $\sum_{P \in C \cap D} n_P P$.

Therefore we need to show that $1 \leq \deg \text{div}(G) \leq mn$.

We know that $\text{div } G \sim \text{div } L^n = n \text{div } L$ for any linear form L with $C \not\subseteq Z(L)$. It therefore suffices to show that $1 \leq \deg \text{div}(L) \leq m$. From example sheet 1, there is some $P \in C \cap L$ and as argued in example 11.1 we can choose L so that $\text{div } L = \sum_{P \in C \cap Z(L)} P$. Changing coordinates so that $L = x_0$, the result follows by the fundamental theorem of algebra $\square$

Remark.

1. For a general choice of F, G (or for general G and fixed F), $|C \cap D| = mn$
2. With the correct notion of multiplicity of C, D at an intersection point P , called $I(C \cap D, P)$, we have $\sum_{P \in C} I(C \cap D, P) = mn$.
In fact $I(C \cap D, P) = \nu_P(G/x_i^n)$ in $\mathcal{O}_{C,P}$. This is equal to $\dim_k \mathcal{O}_{\mathbb{A}^2, P}/(f, g)$ where f, g are dehomogenisations of F, G in coordinates with $P \in \mathbb{A}^2$

Definition 11.8. Let X be a projective variety of dimension m , the **degree** of $X \hookrightarrow \mathbb{P}^n$ is $|X \cap H_1 \cap \cdots \cap H_m|$ for general hyperplanes $H_1, \dots, H_m$ such that the intersection is finite (no proof of well definedness)

Theorem 11.2. (*Bezout for Hypersurfaces*). Let $X \subseteq \mathbb{P}^n$ be a projective variety, $F \in k[x_0, \dots, x_n]$ a homogeneous polynomial with $Z(F)$ not containing any component of X . Then $\deg X \cap Z(F) = \deg X \deg F$

Proof. No Proof $\square$

Corollary 11.2.1. There is no non-constant morphism $\mathbb{P}^2 \rightarrow \mathbb{P}^1$

Proof. Example sheet 3 $\square$

Theorem 11.3. If $f: \mathbb{P}^n \rightarrow \mathbb{P}^n$ is an isomorphism, then f is linear, ie we have $f(x) = Ax$ for some $A \in GL_{n+1}(k)$

Proof. If H is a hyperplane in $\mathbb{P}^n$ and $L \not\subseteq H$ is a line, then $\text{div}(H)$ on L is a point with coefficient 1, so has degree 1. So $\text{div}(f(H))$ on $f(L)$ has degree 1. So $f(H)$ and $f(L)$ have degree 1 by Bezout, so $f(H)$ is a hyperplane, as this holds for any general line. Applying this to $\{x_i = 0\} = H$ we get that $f(H) = \{a_{0i}x_0 + \cdots + a_{ni}x_n = 0\}$. Letting $A = (a_{ji})$, we get $f(x) = Ax$. Repeating for f^{-1} , it follows that $A \in GL_{n+1}(k)$ $\square$

12 Differentials

Let K/k be a field extension. A differential is to be a k -linear combination of symbols of the form $x dy$ with $x, y \in K$ such that

1. $d(\cdot)$ is linear
2. The Leibniz rule holds for $d(xy)$
3. $da = 0$ for $a \in k$

Definition 12.1. The **space of differentials**, $\Omega_{K/k} = \Omega_K$ is the quotient K vector space M/N where $M = \langle \delta x \mid x \in K \rangle$ and N is the subspace of M generated by

1. $\delta(x + y) - \delta x - \delta y$ where $x, y \in K$
2. $\delta(xy) - x\delta y - y\delta x$ where $x, y \in K$
3. δa where $a \in k$

For $x \in K$ define dx to be the coset $\delta x + N$. The map $d: K \rightarrow \Omega_{K/k}$ is the **exterior derivative**

Lemma 12.1. Suppose K/k is finitely generated as a field extension with transcendence basis $x_1, \dots, x_n$. Then if $f \in k(x_1, \dots, x_n)$ is a rational function in the x_i and $y = f(x_1, \dots, x_n)$ then $dy = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(x_1, \dots, x_n) dx_i$. So the set $\{dx_1, \dots, dx_n\}$ spans Ω_K and is in fact a basis

Proof. Linear independence is algebraic and will not be proven. The first part is an exercise. $\square$

Definition 12.2. Let V be a curve and $K = k(V)$. We write Ω_V for $\Omega_{K/k}$ and call this the space of **rational/meromorphic differentials** on V . A differential $\omega \in \Omega_V^\times$ is **regular** at $P \in V$ if we can express $\omega = \sum_i f_i dg_i$ with f_i, g_i regular at P .

If π_P is a local parameter at P , then π_P is transcendental over k and so $d\pi_P$ generates Ω_V and any differential can be written as $\omega = h d\pi_P$. h is not independent of choice of π_P

Definition 12.3. In the above setting, we define the **valuation** of a differential at a point to be $\nu_P(\omega) = \nu_P(h)$ for any choice of local parameter π_P . If $\nu_P(\omega) > 0$, we say ω **has a zero** at P , if $\nu_P(\omega) < 0$ we say ω **has a pole** at P . If $\omega \in \Omega_V^\times$ define $\text{div } \omega = \sum_{P \in V} \nu_P(\omega) P$

Definition 12.4. We denote $\Omega_{V,P} = \{\omega \in \Omega_V \mid \omega \text{ is regular at } P\}$

Proposition 12.1. $\Omega_{V,P} = \mathcal{O}_{V,P} d\pi_P$ for any local parameter π_P

Proof. $\supseteq$ is clear by definition. Since the partial of g/h is regular at P if and only if $h(P) \neq 0$, we see that the dx_i generate $\Omega_{V,P}$ over $\mathcal{O}_{V,P}$ so $\Omega_{V,P}$ is a finitely generated $\mathcal{O}_{V,P}$ -module. If $f \in \mathcal{O}_{V,P}$ then $df = d(f - f(P)) = d(\pi_P g)$ for some $g \in \mathcal{O}_{V,P}$, which is equal to $gd\pi_P + \pi_P dg \in \mathcal{O}_{V,P}d\pi_P + \mathfrak{m}_P\Omega_{V,P}$. By Nakayama, $\Omega_{V,P} \subseteq \mathcal{O}_{V,P}d\pi_P$ and we are done $\square$

Lemma 12.2. *Let $\omega \in \Omega_V$ be a non-zero differential on a curve V . Then $\nu_P(\omega) = 0$ for all but finitely many $P \in V$, and $\nu_P(\omega) \geq 0$ if and only if ω is regular at P*

Proof. Note that if $\omega, \omega' \in \Omega$ are non-zero, we can write $\omega = h d\pi_P, \omega' = h' d\pi_P$ so that

$$\begin{aligned} \nu_P(\omega + \omega') &= \nu_P(h + h') \\ &= \nu_P(h) + \nu_P(h') \\ &\geq \min\{\nu_P(h), \nu_P(h')\} \\ &= \min\{\nu_P(\omega), \nu_P(\omega')\} \end{aligned}$$

. For the first part, suppose that $g \in K(V)$ is non-constant and that $\omega = f dg$. Then for any $P \in V$, we have that $\nu_P(\omega) = \nu_P(f) + \nu_P(dg)$ and so it suffices to show that $\nu_P(dg) = 0$ for all but finitely many P . By the finiteness theorem for curves, if we consider g as a morphism from $V \rightarrow \mathbb{P}^1$, it has finitely many poles and finitely many ramified points. If $g(P) \neq \infty$ and t is a local coordinate at 0 on $\mathbb{P}^1$ then $t - g(P)$ is a local coordinate at $g(P)$, and if g is further unramified at P , then $g^*(t - g(P))$ is a local coordinate at P . We therefore have

$$\begin{aligned} \nu_P(dg) &= \nu_P(d(g - g(P))) \\ &= \nu_P(1) \\ &= 0 \end{aligned}$$

For the second part, the forward direction is clear. Assume that ω is regular at P , ie $\omega = \sum_i f_i dg_i$ with f_i, g_i regular at P . By the valuation inequality, it suffices to prove this for $f dg$ with f, g regular, and so it further suffices to prove $\nu_P(g) \geq 0$ for all $g \in \mathcal{O}_{V,P}^*$. We have

$$dg = d(g - g(P)) = d(\pi_P^n \cdot h)$$

where $n = \nu_P(g - g(P)), h \in \mathcal{O}_{V,P}^\times$. If $n = 1$ then $g - g(P)$ is a local coordinate and so $\nu_P(dg) = \nu_P(d(g - g(P))) = 0$. If $n > 1$, then

$$\begin{aligned} d(\pi_P^n \cdot h) &= \pi_P^{n-1} d(\pi_P \cdot h) + d(\pi_P^{n-1} \cdot h) \pi_P h \\ &= \pi_P^{n-1} d(\pi_P h) + (n-1) \pi_P^{n-1} h d\pi_P \end{aligned}$$

which has valuation $n-1$ and so $\nu_P(d(g - g(P))) \geq n-1 > 0$ and we are done. $\square$

Remark. We have proven that $\text{div } \omega$ is a divisor for any $\omega \in \Omega_V^*$

Definition 12.5. $\text{div } \omega$ is denoted by K_V , a **canonical divisor** for V

Lemma 12.3. For any non-zero differentials ω, ω' have the same divisor

Proof. As Ω_V is one dimensional, and so $\omega = f\omega'$ for some rational f and the result holds by definition $\square$

We call this class in $Cl(V)$ the **canonical class**

Remark. Everything we have done on differentials is isomorphism invariant as it was done on the level of function fields

Example 12.1. Let $V = \mathbb{P}^1$. We embed $\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ by $x \mapsto (1: x)$ and define $t = x_1/x_0$. Then $\omega = dt$ is a non-zero rational differential on $\mathbb{P}^1$. If $a \in \mathbb{A}^1$ then $t - a$ is a local parameter at a and $dt = d(t - a)$ has $\nu_a(dt) = 0$. At ∞ , $\frac{1}{t}$ is a local parameter and we have $d(\frac{1}{t}) = -t^{-2}dt$ and so $\nu_\infty(\omega) = \nu_\infty(t^{-2}) = -2$. Hence we have $\text{div } \omega = -2(\infty)$. This has negative degree, so is neither principal nor a hyperplane section

Definition 12.6. If V is a curve we define the **genus** to be $g(V) = l(K_V)$ where K_V is any element of the canonical class

Example 12.2. $g(\mathbb{P}^1) = l(-2(\infty)) = 0$ since the degree of $-2(\infty)$ is less than 0, and in general this agrees with topological genus for $k = \mathbb{C}$, but we will not prove this

13 Differentials on Plane Curves

13.1 Plane Cubics

Suppose $F(x_0, x_1, x_2) = x_0x_2^2 - \prod_{i=1}^3(x_1 - \lambda_i x_0)$ with $\lambda_1, \lambda_2, \lambda_3 \in k$ distinct. This distinctness gives us that $Z(F) = V$ is smooth and irreducible, hence a curve. We compute its genus. Dehomogenising with $x_0 = 1$, we get

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

where $y = x_2/x_0, x = x_1/x_0$. We therefore get

$$2ydy = g'(x)dx$$

in Ω_V . We choose

$$\omega = \frac{dx}{y} = \frac{2dy}{g'(x)}$$

and to compute the canonical divisor.

If $y(P) \neq 0$ then $x - x(P)$ is a local coordinate for $P \in V$ with $x_0 \neq 0$, and so $\nu_P(\omega) = \nu_P\left(\frac{dx}{y}\right)$. If $y(P) = 0$ then y is a local coordinate and as the λ_i are distinct, $g'(x(P)) \neq 0$ and so $\nu_P(\omega) = 0$.

Suppose $x_0 = 0$. Then we have the single point, $\infty = (0: 0: 1)$. Dehomogenising with respect to x_2 , we get

$$z - \prod_{i=1}^3 (t - \lambda_i z)$$

for $z = x_0/x_2 = 1/y, t = x_1/x_2 = x/y$. At $\infty, \nu_\infty(t - \lambda_i z) \geq 1$ so by the criterion for plane curves, t is a local parameter at infinity, so $\nu_\infty(t) = 1$ and $\nu_\infty(z) \geq 3$, so $\nu_\infty(t - \lambda_i z) = \nu_\infty(t) = 1$, and so $\nu_\infty(z) = 3$. Note also that $\nu_\infty(y) = -3, \nu_\infty(x) = -2$

Lemma 13.1. *If $h \in k(V)$ is a rational function on a curve and $\nu_P(h) \geq 1$ then $\nu_P(dh) = \nu_P(h) - 1$*

Proof. If $\nu_P(h) = 1$, this holds by definition, so assume $\nu_P(h) \geq 2, h = u\pi_P^n$ with $n = \nu_P(h)$. Then

$$\begin{aligned} dh &= u\pi_P d\pi_P^{n-1} = u\pi_P^{n-1}(n-1)d\pi_P + \pi_P^{n-1}d(u\pi_P) \\ &= \pi_P^{n-1}[u(n-1)d\pi_P + u d\pi_P + \pi_P du] \\ &= \pi_P^{n-1}[und\pi_P + \pi_P du] \end{aligned}$$

As u is regular at P , $\nu(du) \geq 0$ so that $\nu_P(\pi_P du) \geq 1$. We conclude that $\nu_P(dh) = n - 1$ as claimed $\square$

We know that $\nu_\infty(\frac{1}{x}) = 2$ so $\nu_\infty(d\frac{1}{x}) = 1$. Therefore $\nu_\infty(-\frac{1}{x^2}dx) = 1$. Since $\nu_\infty(\frac{1}{x^2}) = 4$ we deduce $\nu_\infty(dx) = -3$ and $\nu_\infty(\omega) = 0$. So the canonical divisor for the plane cubic is the zero divisor.

We compute that $L(0) = \{f \in k(V) \mid \text{no poles}\} = k$ and so $l(K_V) = 1$ and this is the genus.

Remark. On the curve $x_0x_2 - \prod_{i=1}^3 (x_1 - \lambda_i x_0)$ we considered the projections to $x = (x_0: x_1)$ and $y = (x_0: x_2)$, with the former not defined at $\infty = (0: 0: 1)$, and so we deduce that $\infty \mapsto (0: 1)$ with ramification degree 2 by surjectivity, so $\nu_\infty(x) = -2$. Similarly $\infty \mapsto (0: 1)$ with ramification degree 3, so $\nu_\infty(y) = -3$, as we know x is degree 2, and y is degree 3

For a general plane curve we have

Theorem 13.2. *Let $V = Z(F) \subseteq \mathbb{P}^2$ be a smooth plane curve of degree $d \geq 3$. Then $K_V = (d - 3)H$ where H is the divisor of a hyperplane section*

Proof. Choose coordinates such that $(0: 1: 0) \notin V$. We dehomogenise with respect to $x = x_1/x_0, y = x_2/x_0$ to obtain $F(1, x, y) = f(x, y) = 0$, an affine curve. We take the exterior derivative to get

$$\frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = 0$$

. We therefore consider

$$\omega = dx / \frac{\partial f}{\partial y} = -dy / \frac{\partial f}{\partial x}$$

Let $H = \{x_0 = 0\}$. The same argument as before shows that $\text{div}(\omega)$ is supported in H . We dehomogenise F with respect to x_2 to get $g(z, w) = F(z, w, 1)$ where $z = x_0/x_2 = 1/y, w = x_1/x_2 = x/y$. Consider

$$\eta = dz/\frac{\partial f}{\partial w} = -dw/\frac{\partial f}{\partial z}$$

. The divisor of η is supported on $\{x_2 = 0\}$, not at any point in $P \in H \cap V$. We have

$$f(x, y) = F(1, x, y) = y^d F\left(\frac{1}{y}, \frac{x}{y}, 1\right) = y^d g\left(\frac{1}{y}, \frac{x}{y}\right)$$

Now

$$\frac{\partial f}{\partial x} = y^d \frac{\partial g}{\partial w}\left(\frac{1}{y}, \frac{x}{y}\right) \cdot \frac{1}{y} = \left(\frac{1}{z}\right)^{d-1} \frac{\partial g}{\partial w}(z, w)$$

. Similarly we have $y = 1/z$ and so $dy = -dz/z^2$. Therefore

$$\omega = -dy/\frac{\partial f}{\partial x} = \frac{-z^{-2}dz}{\left(\frac{1}{z}\right)^{d-1} \frac{\partial g}{\partial w}} = z^{d-3}\eta$$

Since $\nu_P(\eta) = 0$ for all $P \in H$, $\nu_P(\omega) = (d-3)\nu_P(x_0/x_2)$ and so $\omega = (d-3)H$ as claimed $\square$

Remark. So note that $\deg K_V = d(d-3)$ for a smooth plane curve

Proposition 13.1. *If $f(x, y) = 0$ is an affine equation for a smooth projective curve $V \subseteq \mathbb{P}^2$, and $\deg V \geq 3$. Then $\{x^r y^s \mid 0 \leq r+s \leq d-3, 0 \leq r, s\}$ provides a basis for $L(K_V)$*

Proof. By the previous theorem, all poles of any element of $L(K_V)$ are at infinity. We know that x, y generate $k(V)$ as a field, and so any element of $L(K_V)$ is polynomial in x, y . Therefore monomials $x^r y^s$ generate $L(K_V)$. By definition, as $x = x_1/x_0, y = x_2/x_0$, this has pole of order $r+s$, and so it suffices to show that $x^r y^s$ are linearly independent for $0 \leq r+s \leq d-3$. Any such non-trivial dependence would give us something of lower degree than f in the affine ideal, contradiction so we are done. $\square$

Corollary 13.2.1. *(Genus Degree formula for plane curves) If V is a smooth plane curve of degree $d \geq 3$, then $g(V) = \frac{(d-1)(d-2)}{2}$*

Proof. Trivial $\square$

Corollary 13.2.2. *There are infinitely many non-isomorphic curves*

Proof. As smooth curves of different degrees have different genera $\square$

14 Riemann-Roch Theorem

Theorem 14.1. (*Riemann-Roch*) Let V be a curve of genus g with canonical divisor K_V . Then for any divisor D on V ,

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

Proof. No Proof □

Remark. The right hand side is a ‘topological’ quantity and the left hand side is an ‘algebraic’ quantity

Corollary 14.1.1. (*Genus-Degree formula, another proof*)

Proof. Take $D = K_V$. Then Riemann-Roch says $l(K_V) - l(0) = 1 - g + \deg K_V$, or in other words $g - 1 = 1 - g + d(d - 3)$. Rearranging, the result follows □

Corollary 14.1.2. *If V is a curve then $\deg K_V = 2g - 2$*

Proof. Take $D = K_V$ in Riemann Roch, so $l(D) = g, l(K_V - D) = l(0) = 1$ □

Corollary 14.1.3. *Let D be a divisor with $\deg D > 2g - 2$ then $l(D) = 1 - g + \deg D$. In particular if $g = 1$, then $\deg D > 0$ implies $l(D) = \deg D$*

Proof. Trivial □

Consider a non-constant morphism of curves $\phi: V \rightarrow W$. This induces a map $\phi^*: k(W) \rightarrow k(V)$ which sends non-constant $t \in k(V)$ to some non-constant $\phi^*t \in k(V)$, and so Ω_W is generated by dt and Ω_V is generated by $d\phi^*t$. Given $\omega = fdt \in \Omega_W$, define $\phi^*\omega = \phi^*(f)d\phi^*t$

Lemma 14.2. *Let $P \in V$ with $\phi(P) = Q$. Let e_P be the ramification of ϕ at P , and π_P, π_Q local parameters at P, Q respectively. Then*

$$\nu_P(\phi^*\omega) = e_P \nu_Q(\omega) + e_P - 1$$

*. In particular, $\nu_P(\phi^*d\pi_Q) = e_P - 1$*

Proof. Now $\nu_P(\phi^*d\pi_Q) = \nu_P(1 \cdot d(\phi^*\pi_Q)) = e_P - 1$. For a general ω , write $\omega = u\pi_Q^{\nu_Q(\omega)}d\pi_Q$ where $u \in Q_{W,Q}^*$. Then

$$\phi^*\omega = (\phi^*u)\phi^*(\pi_Q)^{\nu_Q(\omega)}(d\phi^*\pi_Q)$$

and we know the valuation of each term, so the result follows □

Theorem 14.3. (*Riemann-Hurwitz*) Let $\phi: V \rightarrow W$ be a non-constant morphism of curves, and $\deg \phi = n$. Then

$$2g(V) - 2 = n(2g(W) - 2) + \sum_{P \in V} e_P - 1$$

Proof. Let $0 \neq \omega \in \Omega_W$, so $\phi^*\omega \in \Omega_V^\times$, so $\operatorname{div}(\phi^*\omega) = K_V$. By Riemann Roch, $\deg K_V = 2g(V) - 2$. So

$$\begin{aligned}
2g(V) - 2 &= \sum_{P \in V} \nu_P(\phi^*\omega) \\
&= \sum_{Q \in W} \sum_{\phi(P)=Q} \nu_P(\phi^*\omega) \\
&= \sum_{Q \in W} \sum_{\phi(P)=Q} (e_P \nu_Q(\omega) + e_P - 1) \\
&= \sum_{Q \in W} \deg(\phi) \nu_Q(\omega) + \sum_{P \in V} (e_P - 1) \\
&= \deg(\phi) \deg(\operatorname{div}(\omega)) + \sum_{P \in V} (e_P - 1) \\
&= n(2g(W) - 2) + \sum_{P \in V} (e_P - 1)
\end{aligned}$$

□

Corollary 14.3.1. *If V, W are curves and $g(V) < g(W)$ then any morphism $\phi: V \rightarrow W$ is constant*

Proof. Trivial

□

Corollary 14.3.2. *Let $X = V_1 \times V_2$ be a product of two curves of genus at least 1. Then X is a smooth projective surface with no lines (ie no subvariety isomorphic to $\mathbb{P}^1$)*

Proof. Take projections and apply Riemann-Hurwitz

□

15 Equations of Curves

Definition 15.1. Let V be a curve and D a divisor on V , with $l(D) = n+1 \geq 2$. Let $B = \{f_0, \dots, f_n\}$ be a basis for $l(D)$. The **morphism associated to D** with respect to the basis B is

$$\phi_D = (f_0 : \dots : f_n) : V \rightarrow \mathbb{P}^n$$

We say ϕ_D is an **embedding** if it is an isomorphism onto $\phi_D(V)$, in which case we say D is **very ample**

Remark. This morphism is non-constant as $l(D) > 1$, and a different choice of basis is just a linear change of coordinates on $\mathbb{P}^n$

Let $V \subseteq \mathbb{P}^m$ be a curve and $D = \operatorname{div} x_0$ be a hyperplane section. It can be shown that if $P \neq Q \in V$, then $l(D - P - Q) \leq l(D) - 2$, and in fact this holds for $P = Q$. From earlier we can even say that $l(D - P - Q) = l(D) - 2$. We say $L(D)$ **separates points** and **separates tangents**.

$$\forall P, Q \in V, l(D - P - Q) = l(D) - 2 \quad (*)$$

Theorem 15.1. ϕ_D is an embedding if and only if D satisfies $(*)$

Proof. No Proof □

Corollary 15.1.1. If $\deg D \geq 2g + 1$ then ϕ_D is an embedding

Proof. For $D, D - P - Q$, we have that

$$\begin{aligned} l(D) &= 1 - g - \deg D \\ l(D - P - Q) &= 1 - g - \deg(D - P - Q) \end{aligned}$$

□

Corollary 15.1.2. For fixed genus, if $g \geq 2$ there is some $m = m(g)$ such that mK_V is very ample

16 Elliptic Curves

Definition 16.1. An **elliptic curve** is a curve of genus 1, with a choice of basepoint $P_0 \in E$ written O_E

Suppose P, Q are on an elliptic curve (E, P_0) . The divisor $P + Q - P_0$ has degree 1 and so $l(P + Q - P_0) = 1$. Therefore there is an effective degree one divisor equivalent to $P + Q - P_0$, ie some $R \in E$ such that $P + Q - P_0 \sim R$. Distinct points on E are inequivalent since $E \not\cong \mathbb{P}^1$, and so R is unique. We call it $P \oplus_E Q = R$, ie $P + Q = R$

Theorem 16.1. The operation defined above makes E into an abelian group, with identity $O_E = P_0$. The map $P \mapsto [P - P_0] \in \text{Cl}^0(E)$ is an isomorphism of groups

Proof. It suffices to prove the second statement. Call the map β . If $P, Q \in E$, then

$$\beta(P + Q) = \beta(R) = [R - P_0] = [P + Q - P_0 - P_0] = \beta(P) + \beta(Q)$$

so β is a homomorphism. β is injective as if $\beta(P) = \beta(Q)$ then $P \sim Q$, so $P = Q$ as E is genus 1. It remains to prove β is surjective. Suppose D is a divisor of degree 0. $D + P_0$ has degree 1, and so $l(P_0 + D) = 1$ and so there is a point $P \in E$ such that $D + P_0 \sim P$, ie $D \sim P - P_0$ and $D = \beta(P)$ □

Remark. For any curve of positive genus $g > 1$, the map is injective and so there is an injection of the curve into a group, and it is a fact that the group is itself a projective variety of dimension g , called the **Jacobian** of V

We know that plane cubics have genus 1, and in fact we can show

Theorem 16.2. Let (E, P_0) be an elliptic curve then $3P_0$ provides an embedding of E into $\mathbb{P}^2$ as a plane cubic

Proof. Recall that $l(D) = \deg D$ if $\deg D > 0$, so mP_0 is an embedding if $m \geq 3$. We consider $L(mP_0)$. For $m = 3$, this has dimension 3 and contains constants, so has basis $1, x, y$ for some functions x, y where $1, x$ is a basis of $L(2P_0)$, so x induces a degree 2 morphism to $\mathbb{P}^1$ and y induces a degree 3 morphism to $\mathbb{P}^1$, by considering the preimage of infinity. So $(1: x: y): E \rightarrow \mathbb{P}^2$ is an embedding. Now $L(4P_0)$ has basis $\{1, x, y, x^2\}$, $L(5P_0)$ has basis $\{1, x, y, x^2, xy\}$ and $L(6P_0)$ contains those, and x^3, y^2 . There is therefore a linear relationship between these 7 functions $(1, x, x^2, y, xy, y^2, x^3)$ as $l(6P_0) = 6$ including both of y^2, x^3 by considering poles. Homogenising, we get a cubic equation, so $E \subseteq Z(F)$ for some cubic F . If this is smooth and reducible, its components have degree at most 2, and hence have genus 0, contradiction E is an isomorphism onto its image, and so onto a smooth component which can't have genus 0, so $Z(F)$ is irreducible and E maps onto $Z(F)$ $\square$

Remark. P_0 is the unique point of E sent to the line at ∞ . Changing coordinates, we may assume $P_0 \mapsto (0: 1: 0)$, and that the cubic has no yz^2 term (As P_0 is the unique point on $z = 0$, $F(x, y, 0)$ has a unique solution and therefore is x^3). Therefore

$$F: ay^2z = G(x, z)$$

which has the form

$$y^2z = \prod_{i=1}^3 (x - \lambda_i z)$$

Theorem 16.3. *Let $E = Z(F)$ with $F: y^2z - \prod_{i=1}^3 (x - \lambda_i z)$ is an elliptic curve with base point at infinity. Then $P + Q + R = \mathcal{O}_E$ holds if and only if P, Q, R are collinear*

Proof. Via $\beta: P \mapsto [P - P_0]$ we see that $P + Q + R = \mathcal{O}_E$ if and only if $P + Q + R \sim 3P_0$, which holds if and only if there is some rational function f with $\text{div } f = P + Q + R - 3P_0$. Now note that $f \in L(3P_0)$, so f is a linear combination of $1, x, y$ and so it is a linear form after homogenising with respect to z , so the zero set of f is precisely P, Q, R , so they are collinear if and only if such an f exists. $\square$

17 More Consequences of Riemann Roch

Definition 17.1. A curve V of genus $g \geq 2$ is **hyperelliptic** if there is some $\pi: V \rightarrow \mathbb{P}^1$ which is non-constant of degree 2

If V is hyperelliptic, consider the degree 2 divisor $D = \pi^*(\infty)$ of poles of π . The associated vector space $L(D)$ has dimension at least 2, as it contains constants and π . On the other hand, for $Q \in V$ we have $l(Q) = 1$ since V doesn't have a degree 1 map to $\mathbb{P}^1$. So as $l(D) \leq l(D - P) + 1$, we know $l(D) \leq 2$ and hence $l(D) = 2$

Proposition 17.1. *Let V be a curve of genus larger than 1 with an effective divisor of degree 2 on V with $l(D) = 2$. Then $\phi_D: V \rightarrow \mathbb{P}^1$ has degree 2 (and $\phi_V^*(\infty) = D$), so V is hyperelliptic. All genus 2 curves are hyperelliptic, and there are hyperelliptic curves of every genus*

Proof. Example sheet 4 □

Proposition 17.2. *ϕ_{K_V} is an embedding if and only if V is not hyperelliptic*

Proof. Suppose ϕ_{K_V} is not an embedding. Then there are P, Q on V such that $l(K_V - P - Q) \geq g - 1$. By Riemann Roch,

$$l(P + Q) = l(K_V - P - Q) + 1 - g + 2 \geq 2$$

Since $l(P + Q) \leq l(P) + 1 = 2$, it follows that $l(P + Q) = 2$, by proposition 17.1, V is hyperelliptic.

Conversely if V is hyperelliptic, then let $\pi: V \rightarrow \mathbb{P}^1$ have $D = \pi^*(\infty)$, and then $l(D) = 2, l(K_V - D) \geq g - 1$ working conversely □