Algebraic geometry

Shing Tak Lam

May 21, 2023

Contents

Throughout, we work over the complex numbers.

1 Affine varieties

1.1 Affine varieties

Definition 1.1 (affine n-space)

Affine n-space over $\mathbb{C}$ is the set[a]

$$\mathbb{A}^n = \mathbb{C}^n$$

[a]Basically, we want the set, but not the vector space structure.

Notation 1.2. When n is clear, we write $\mathbb{C}[\mathbf{X}] := \mathbb{C}[X_1, \ldots, X_n]$

Definition 1.3 (vanishing locus, affine variety)
Let $S \subseteq \mathbb{C}[\mathbf{X}]$ be any subset. The vanishing locus of S is given by

$$\mathbb{V}(S) = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for all } f \in S\}$$

An affine variety is any set of the form $\mathbb{V}(S)$ for some $S \subseteq \mathbb{C}[\mathbf{X}]$.

Theorem 1.4. Let $S \subseteq \mathbb{C}[\mathbf{X}]$ be any subset. Then

(i) Let $I = \langle S \rangle$ be the ideal generated by S. Then $\mathbb{V}(I) = \mathbb{V}(S)$.

(ii) There exists a finite subset $\{f_j\} \subseteq S$ such that $\mathbb{V}(I) = \mathbb{V}(S)$.

Proof. (i) follows from basic properties of ideals.

(ii) We already have that $\mathbb{V}(S) = \mathbb{V}(I)$ by (i). By the Hilbert basis theorem, we have a finite set $\{h_1, \ldots, h_r\}$ of generators for I. Therefore, we have a finite subset $\{f_1, \ldots, f_m\} \subseteq S$, and $g_{ij} \in \mathbb{C}[\mathbf{X}]$, such that

$$h_i = \sum_{j=1}^{m} g_{ij} f_j$$

Therefore $\{f_j\}$ are also a set of generators for I. Hence $\mathbb{V}(S) = \mathbb{V}(f_1, \ldots, f_m)$. □

Proposition 1.5.

(i) if $S \subseteq T$, then $\mathbb{V}(T) \subseteq \mathbb{V}(S)$,

(ii) $\mathbb{V}(0) = \mathbb{A}^n$ and $\mathbb{V}(1) = \varnothing$,

(iii) for any family of ideals I_j, we have that

$$\bigcap_j \mathbb{V}(I_j) = \mathbb{V}\left(\sum_j I_j\right)$$

(iv) $\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cap J)$

Proof. (i) and (ii) are obvious. For (iii), notice that by definition,

$$\bigcap_j \mathbb{V}(I_j) = \mathbb{V}\left(\bigcup_j I_j\right)$$

and $\sum_j I_j$ is ideal generated by $\bigcup_j I_j$. Finally, for (iv), by defintion we have that

$$\mathbb{V}(I) \cup \mathbb{V}(J) \subseteq \mathbb{V}(I \cap J)$$

For the reverse containment. Suppose $P \in \mathbb{V}(I \cap J)$, and $P \notin \mathbb{V}(I)$. Then there exists $g \in I$ such that $g(P) \neq 0$. Moreover, for all $f \in J$, $fg \in I \cap J$, so $fg(P) = 0$. Therefore, we must have that $f(P) = 0$, so $P \in \mathbb{V}(J)$. □

Definition 1.6 (irreducible)
A variety V is irreducible if it cannot be written as a union

$$V = V_1 \cup V_2$$

of proper subvarieties.

Proposition 1.7. Every affine variety V is a finite union of irreducible varieties.

Proof. If V is irreducible we are done. Otherwise, we can write $V = V_1 \cup V_1'$. If V_1, V_1' are both unions of irreducible varieties, then we are done. If not, then we can write $V_1 = V_2 \cup V_2'$. Repeating this, we get

$$V = V_0 \supsetneq V_1 \supsetneq V_2 \supsetneq \dots$$

Suppose $V_j = \mathbb{V}(I_j)$. Define

$$W = \bigcap_j V_j = \mathbb{V}\left(\sum_j I_j\right)$$

Now $I = \sum_j I_j$ is finitely generated, as $\mathbb{C}[X]$ is Noetherian. Therefore, $I = \sum_{j \le N} I_j$ for some N, as the ascending chain stabilises. Therefore, we must have that

$$W = \bigcap_{j \le N} V_j$$

so the descending chain stabilises. $\square$

Proposition 1.8. Let V be a variety. A minimal decomposition $V = \bigcup V_i$ into a finite union of distinct irreducible varieties is unique up to reordering.

1.2 Topology

Definition 1.9 (Zariski topology)
The Zariski topology on $\mathbb{A}^n$ is the topology where the closed sets are affine varieties on $\mathbb{A}^n$.

Definition 1.10 (Euclidean topology)
The Euclidean topology on $\mathbb{A}^n$ is the topology coming from the metric topology on $\mathbb{C}^n$.

Proposition 1.11. Every Zariski closed subset is Euclidean closed. In addition, every Zariski open dense subset is Euclidean dense.

1.3 Nullstellensatz

Theorem 1.12 (Weak Nullstellensatz)**.** Let $I \subsetneq \mathbb{C}[X]$ be a proper ideal. Then $\mathbb{V}(I)$ is nonempty.

Proof is in section 5. . $\square$

Definition 1.13 (ideal of a variety)
Let V be an affine variety. Then the ideal

$$I(V) = \{f \in \mathbb{C}[\mathbf{X}] \mid f(P) = 0 \text{ for all } P \in V\}$$

is called the ideal of V.

Proposition 1.14. Let $V \subseteq \mathbb{A}^n$ be a variety.

(i) if $V = \mathbb{V}(S)$, then $S \subseteq I(V)$. In particular, $I(V)$ is the largest ideal of functions that vanish on V,

(ii) $V = \mathbb{V}(I(V))$,

(iii) two varieties V, W are equal if and only if $I(V) = I(W)$.

Proof. By definition. □

Proposition 1.15. $V \subseteq W$ if and only if $I(W) \subseteq I(V)$.

Proof. Suppose $V \subseteq W$, then $I(W) \subseteq I(V)$ follows from definition. Conversely, if $V \nsubseteq W$, then we can choose $P \in V \setminus W$. Since $P \notin \mathbb{V}(I(W))$, there exists $f \in I(W)$ such that $f(P) \neq 0$. In particular, $f \notin I(V)$. □

Proposition 1.16. A variety $V \subseteq \mathbb{A}^n$ is irreducible if and only if $I(V)$ is prime.

Proof. We have seen that $I(V_1 \cup V_2) = I(V_1 \cap V_2)$. Now suppose V was reducible. Then we can write $V = V_1 \cup V_2$ as a nontrivial union, then

$$V_1 \nsubseteq V_2 \nsubseteq V_2$$

Let $I_j = I(V_j)$, then $I(V) = I_1 \cap I_2$, and by the previous proposition, $I_1 \nsubseteq I_2 \nsubseteq I_1$. We can therefore find

$$f_1 \in I_1 \setminus I_1 \quad \text{and} \quad f_2 \in I_2 \setminus I_1$$

Then $f_i \notin I(V)$, but $f_1 f_2 \in I_1 \cap I_2 = I(V)$. So $I(V)$ is not prime.
Conversely, suppose $f_1 f_2 \in I(V)$, with neither $f_1, f_2 \in I(V)$. Then we can define

$$V_i = V \cap \mathbb{V}(f_i) = \{P \in V \mid f_i(P) = 0\}$$

Since $f_i \notin I(V)$, $V_i \neq V$. Then

$$P \in V \implies f_1(P) f_2(P) = 0 \implies P \in V_1 \cup V_2$$

Hence $V = V_1 \cup V_2$. □

Definition 1.17 (radical of an ideal)
Let $I \trianglelefteq \mathbb{C}[\mathbf{X}]$, then define the radical of I by

$$\sqrt{I} = \{f \in \mathbb{C}[\mathbf{X}] \mid \text{ there exists an integer } m > 0 \text{ such that } f^m \in I\}$$

Proposition 1.18.

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

Proof. By definition. □

Theorem 1.19 (Hilbert's strong Nullstellensatz)**.** Let $I \subseteq \mathbb{C}[\mathbf{X}]$, $V = \mathbb{V}(I)$. Then

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

Corollary 1.20. If $\mathbb{V}(I) = \mathbb{V}(J)$, then $\sqrt{I} = \sqrt{J}$.

1.4 Morphisms of affine varieties

Definition 1.21 (coordinate ring)

The coordinate ring, or ring of regular functions of V is defined as the quotient

$$\mathcal{O}(V) = \mathbb{C}[V] = \frac{\mathbb{C}[\mathbf{X}]}{I(V)}$$

Proposition 1.22. Each element (i.e. coset) in $\mathbb{C}[V]$ gives a well defined function on V.

Proof. $f, g \in \mathbb{C}[\mathbf{X}]$ restricts to the same function on V if and only if $f - g$ vanishes on V, i.e. $f - g \in I(V)$. □

Morally, each element in $\mathbb{C}[V]$ is a coset, or a function $V \to \mathbb{C}$. But when convenient, we may want to think of them by their representatives as polynomials.

Corollary 1.23. $V \subseteq \mathbb{A}^n$ is irreducible if and only if $\mathbb{C}[V]$ is an integral domain.

Definition 1.24 (morphism)

Let $V \subseteq \mathbb{C}^n$, $W \subseteq \mathbb{C}^m$ be varieties. A regular map, or morphism from V to W is a map

$$\varphi : V \to W$$

such that there exists $f_1, \ldots, f_m \in \mathbb{C}[V]$, such that

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

The set of morphisms from V to W is $\mathrm{Mor}(V, W)$.

Proposition 1.25. If $\varphi : V \to W, \psi : W \to Z$ are morphisms, then $\psi \circ \varphi : V \to Z$ is a morphism.

Proof. The composition of polynomials is a polynomial. □

Definition 1.26 (isomorphism)

An isomorphism of affine varieties is a morphism with a 2-sided inverse.

Definition 1.27 (pullback)

Suppose $g \in \mathbb{C}[W]$, $\varphi : V \to W$ is a morphism. Then the pullback of g by φ is[a]

$$\varphi^* g = g \circ \varphi \in \mathbb{C}[V]$$

[a] Formally, we need to check that this is actually an element of $\mathbb{C}[V]$. But this is immediate if we take a representative $\tilde{g} \in \mathbb{C}[Y_1, \ldots, Y_m]$ for g, then $g \circ \varphi$ gives us the same function as $\tilde{g}(\varphi_1(\mathrm{X}), \ldots, \varphi_m(\mathrm{X})) \in \mathbb{C}[X_1, \ldots, X_n]$.

Proposition 1.28. The pullback map $\varphi^* : \mathbb{C}[W] \to \mathbb{C}[V]$ is a $\mathbb{C}$-algebra homomorphism.

Proof. Clear from definitions. □

Theorem 1.29. Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ be varieties. Then the map $\varphi \mapsto \varphi^*$ defines a bijection

$$\mathrm{Mor}(V, W) \leftrightarrow \{\mathbb{C}\text{-algebra homomorphisms } \mathbb{C}[W] \to \mathbb{C}[V]\}$$

Proof. Let $x_1, \ldots, x_n \in \mathbb{C}[V]$ be the coordinate functions on V, $y_1, \ldots, y_m \in \mathbb{C}[W]$ be the coordinate functions on W.

Injectivity: Suppose $P \in V$, $\varphi \in \mathrm{Mor}(V, W)$. Then we have that

$$\varphi(P) = (y_1(\varphi(P)), \ldots, y_m(\varphi(P))) = (\varphi^* y_1(P), \ldots, \varphi^* y_m(P))$$

Therefore, the $\mathbb{C}$-algebra homomorphism φ^* determines φ.

Surjectivity: Let $\lambda : \mathbb{C}[W] \to \mathbb{C}[V]$ be a $\mathbb{C}$-algebra homomorphism. Then each coordinate function y_i pull back to an element of $\mathbb{C}[V]$ via

$$f_i = \lambda(y_i)$$

Combine these to define a map

$$\varphi = (f_1, \ldots, f_m) : V \to \mathbb{A}^m$$

First, we must show that $\varphi(V) \subseteq W$. Let $g \in \mathbb{C}[Y_1, \ldots, Y_m]$, then as λ is a homomorphism,

$$g(f_1, \ldots, f_m) = g(\lambda(y_1), \ldots, \lambda(y_m)) = \lambda(g)$$

Therefor, if we evaluate the above at $P \in V$, and $g \in I(W)$, then $g(f_1(P), \ldots, f_m(P)) = 0$. Hence $\varphi(P) \in W$. Furthermore, it follows from the definition of φ that $\lambda = \varphi^*$. □

Definition 1.30 (function field, rational functions, regular)

Let $V \subseteq \mathbb{A}^n$ be an irreducible affine variety. It's function field, or field of rational functions, is the fraction field

$$\mathbb{C}(V) = \mathrm{Frac}(\mathbb{C}[V])$$

Elements of $\mathbb{C}(V)$ are called rational functions. $\varphi \in \mathbb{C}(V)$ is regular at a point P if we can write $\varphi = f/g$, with $f, g \in \mathbb{C}[V]$, $g(P) \neq 0$.

Morally, we can think of rational functions in a very similar way to germs in Riemann surfaces. Consider the set of pairs (f, U), where $f : U \to \mathbb{C}$ is a rational function[1], and U is a nonempty open subset of V. We say that $(f, U) \simeq (f', U')$ if $f = f'$ on some nonempty open set $V \subseteq U \cap U'$.

This intuition makes sense, since nonempty open subsets of an irreducible variety are dense.

[1] In the sense that $f = g/h$ on U, where $g, h \in \mathbb{C}[V]$.

Definition 1.31 (local ring)

Let V be an irreducible affine variety. The local ring at a point $P \in V$ is

$$\mathcal{O}_{V,P} = \{f \in \mathbb{C}(V) \mid f \text{ regular at } P\}$$

Definition 1.32 (local ring)

A local ring[a] R is a ring which has a unique maximal ideal.

[a]Yes this is the same name as above... Hopefully it should be clear from context what we mean.

Lemma 1.33. A ring R is a local ring if and only if $R \setminus R^\times$ is an ideal. If so, then $R \setminus R^\times$ is the unique maximal ideal of R.

Proof. Suppose $R \setminus R^\times$ was an ideal. Then any ideal properly containing it must contain a unit, so it is the whole ring. Hence it must be a maximal ideal. On the other hand, if $mfa \trianglelefteq R$ is a proper ideal, then it must be contained in $R \setminus R^\times$, so it is the unique maximal ideal.

Conversely, suppose R is a local ring, with unique maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} \subseteq R \setminus R^\times$. Now suppose $x \in R \setminus R^\times$. Then $\langle x \rangle \neq R$, so $\langle x \rangle \subseteq \mathfrak{m}$, since if not, then $\mathfrak{m} + \langle x \rangle$ would be a proper ideal containing $\mathfrak{m}$. Therefore, $\mathfrak{m} = R \setminus R^\times$. □

Definition 1.34 (maximal ideal of a variety at a point)

Let V be an irreducible affine variety, $P \in V$, the maximal ideal of $\mathcal{O}_{V,P}$ is

$$\mathfrak{m}_{V,P} = \{f \in \mathcal{O}_{V,P} \mid f(P) = 0\}$$

Corollary 1.35. $\mathcal{O}_{V,P}$ is a local ring.

2 Projective varieties

Notation 2.1. When clear, we will write $\mathbb{C}[\mathbf{X}] = \mathbb{C}[X_0, \dots, X_n]$.

2.1 Projective space

Definition 2.2 (projectivisation)

Let U be a finite dimensional U-vector space. Then the projectivisation of U is

$$\mathbb{P}(U) = \{\text{lines in } U \text{ through } 0\}$$

Definition 2.3 (projective space)

Then projective n-space is

$$\mathbb{P}^n = \mathbb{P}(\mathbb{C}^{n+1})$$

Notation 2.4. We will index the coordinate son $\mathbb{C}^{n+1}$ by $0, \ldots, n$. Then a line in $\mathbb{C}^{n+1}$ is given by $\{(a_0 t, a_1 t, \ldots, a_n t) \mid t \in \mathbb{C}\}$. We will write $(a_0 : a_1 : \cdots : a_n)$ for the corresponding point in $\mathbb{P}^n$.

Proposition 2.5.

$$\mathbb{P}^n = \frac{\mathbb{C}^{n+1} \setminus 0}{\sim}$$

where $x \sim y$ if there exists $\lambda \in \mathbb{C}^\times$ such that $x = \lambda y$.

Proposition 2.6. We have a decomposition

$$\mathbb{P}^n = \{(a_0 : \cdots : a_n) \mid a_0 \neq 0\} \sqcup \{(a_0 : \cdots : a_n) \mid a_0 = 0\} = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$$

which gives us a decomposition

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \underbrace{\mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^1 \sqcup \{\mathrm{pt}\}}_{=\text{things at } \infty}$$

Definition 2.7 (Euclidean, Zariski topology)

The Zariski and Euclidean topologies on $\mathbb{P}^n$ are the ones induced from the Zarski and Euclidean topologies on $\mathbb{C}^{n+1}$.

$$\mathbb{C}^{n+1} \xrightarrow{\text{subspace}} \mathbb{C}^{n+1} \setminus 0 \xrightarrow{\text{quotient}} \frac{\mathbb{C}^{n+1} \setminus 0}{\sim} = \mathbb{P}^n$$

Definition 2.8 (standard affine patch)

The j-th standard affine patch of $\mathbb{P}^n$ is

$$U_j = \big\{(a_0 : \cdots : a_n) \in \mathbb{P}^n \mid a_j \neq 0\big\}$$

Proposition 2.9. $U_j = \mathbb{A}^n$.

Proof. Without loss of generality $a_j = 1$. Then the natural map gives us the identification. □

Proposition 2.10. We have an action of $\mathrm{GL}_{n+1}(\mathbb{C})$ on $\mathbb{P}^n$, by acting on lines in $\mathbb{C}^{n+1}$. The normal subgroup of scalar matrices $\mathbb{C}^\times$ acts trivially, and so we have an action on $\mathbb{P}^n$ by the projective general linear group

$$\mathrm{PGL}_{n+1}(\mathbb{C}) = \frac{\mathrm{GL}_{n+1}(\mathbb{C})}{\mathbb{C}^\times}$$

2.2 Projective varieties

Definition 2.11 (homogeneous polynomial)

A homogeneous polynomial of degree d is a sum of monomials of degree d.

Definition 2.12 (homogeneous parts)
For a polynomial $f \in \mathbb{C}[X]$, we there exists a unique decomposition

$$f = \sum_i f_{[i]}$$

with $f_{[i]}$ homogeneous of degree i. We call $f_{[i]}$ the degree i homogeneous part of f.

Lemma 2.13. Let $f \in \mathbb{C}[X]$ be homogeneous, $a = (a_0, \dots, a_n) \in \mathbb{C}^{n+1}$ such that $f(a) = 0$. Then for any $\lambda \in \mathbb{C}$,

$$f(\lambda a_0, \dots, \lambda a_n) = 0$$

Proof. Suppose f has degree d. Then

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n)$$

□

Corollary 2.14. Let f be homogeneous of degree d, then

$$\mathbb{V}(f) = \{p \in \mathbb{P}^n \mid f(a) = 0 \text{ where } p = (a_0 : \dots : a_n)\}$$

is well defined.

Definition 2.15 (homogeneous ideal)
An ideal $I \trianglelefteq \mathbb{C}[X]$ is homogeneous if it is generated by homogeneous polynomials, not necessarily of the same degree.

Lemma 2.16. Let $I \trianglelefteq \mathbb{C}[X]$, then I is homogeneous if and only if for any $f \in I$, $f_{[r]} \in I$ for all r.

Proof. Suppose I is homogeneous. Let $I = \langle g_1, \dots, g_k \rangle$, with $d_j = \deg(g_J)$. If

$$f = \sum_j h_j g_j \in I$$

,

then we can plit each h_j into homogeneous parts $h_{j[r]}$. Then we can see that $h_{j[r]} g_j \in I$, so $f = \sum f[r]$, with

$$f_{[r]} = \sum_j h_{j[r-d_j]} g_j \in I$$

homogeneous of degree r, where we define $f_{[k]} = 0$ for $k < 0$. For the converse, we can decompose the generators of I. □

Definition 2.17 (vanishing locus, projective variety)
Let I be a homogeneous ideal, then define the vanishing locus of I to be

$$\mathbb{V}(I) = \{p = (a_i) \in \mathbb{P}^n \mid f(a_i) = 0 \text{ for all } f \in I\}$$

A projective variety is a subset of $\mathbb{P}^n$ of the form $\mathbb{V}(I)$.

Proposition 2.18. Suppose $V = \mathbb{V}(I) \subseteq \mathbb{P}^n$, let $V_0 = V_0 \cap U_0 \subseteq \mathbb{A}^n$. Then $V_0 = \mathbb{V}(I_0)$, where

$$I_0 = \{F(1, Y_1, \dots, Y_n) \mid F \in I \text{homogeneous}\}$$

Definition 2.19 (homogenisation)
For $f \in \mathbb{C}[Y_1, \dots, Y_n]$ with total degree d, we define the homogenisation of f to be

$$f^h(X_0, \dots, X_n) = X_0^d f(X_1/X_0, \dots, X_n/X_0) \in \mathbb{C}[\mathbf{X}]$$

which is a homogeneous polynomial of degree d. The homogenisation of an ideal I is

$$I^h = \langle f^h \mid f \in I \rangle$$

Definition 2.20 (projective closure)
Identifying $\mathbb{A}^n = U_0 \subseteq \mathbb{P}^n$. Let $V = \mathbb{V}(I) \subseteq \mathbb{A}^n$ be an affine variety. Then the projective variety

$$V^h = \mathbb{V}(I^h)$$

is called the projective closure of V.

Proposition 2.21.

1. $V^h \cap \mathbb{A}^n = V$,
2. V^h is the Zariski closure of $V \subseteq A_n \subseteq \mathbb{P}^n$.

Definition 2.22 (homogeneous vanishing ideal)
Let V be a projective variety. Then define

$$I^h(V) = \{f \in \mathbb{C}[\mathbf{X}] \mid f \text{ homogeneous and vanishes on } V\}$$

Theorem 2.23 (Projective Nullstellensatz).

(i) if $\mathbb{V}(I) = \varnothing$, then $\langle X_0^m, \dots, X_n^m \rangle \leq I$ for some $m > 0$,

(ii) if $V = \mathbb{V}(I) \neq \varnothing$, then $I^h(V) = \sqrt{I}$.

Proof. We reduce to the affine case, which will be proved in section 5. Let I be a homogeneous ideal,

$$V_a = \mathbb{V}(I) \subseteq \mathbb{A}^{n+1} \quad \text{and} \quad V_p = \mathbb{V}(I) \subseteq \mathbb{P}^n$$

be the affine and projective varieties of I. Note that 0 is always a point in V_a. Furthermore, there is a natural quotient map

$$V_a \setminus \{0\} \twoheadrightarrow V_p$$

obtained by restricting the natural quotient map $\mathbb{C}^{n+1} \setminus 0 \twoheadrightarrow \mathbb{P}^n$. Therefore, V_p is empty if and only if $V_a \subseteq \{0\}$. The latter is true if and only if $\sqrt{I} \supseteq \langle X_0, \dots, X_n \rangle$. The second statement follows similarly. ☐

Definition 2.24 (open, closed subvarities)

Let V be a projective variety. If $W \subseteq V$, where W is a projective variety, we say W is a closed subvariety of V. Similarly, $V \setminus W$ is an open subvariety of V.

Definition 2.25 (irreducible)

We say that a projective variety V is irreducible if it cannot be written as $V = V_1 \cup V_2$ for proper closed subvarieties V_1, V_2 of V.

Proposition 2.26.

(i) every projective variety is a finite union of irreducible projective varieities,

(ii) V is irreducible if and only if $I^h(V)$ is prime.

Proof. (i) follows from the same proof as in the affine case. For (ii), notice if I homogeneous and not prime, then there exists homogeneous polynomials $F, G \notin I$ such that $FG \in I$.

To see this, as I is not prime, let $f, g \in \mathbb{C}[\mathrm{X}]$ be such that $f, g \notin I, fg \in I$. As $f, g \notin I$, we have r, s such that

$$f_{[0]}, \dots, f_{[r-1]} \in I, f_{[r]} \notin I \quad \text{and} \quad g_{[0]}, \dots, g_{[s-1]} \in I, g_{[s]} \notin I$$

Then we have that $(fg)_{[r+s]} \in I$, and

$$(fg)_{[r+s]} = f_{[r]}g_{[s]} + \text{ stuff in } I$$

So $f_{[r]}, g_{[s]} \notin I$, but $f_{[r]}g_{[s]} \in I$. With this, the same argument as in the affine case works. ☐

Proposition 2.27. Let $V \subseteq \mathbb{P}^n$ be irreducible, $W \subseteq V$ be a proper closed subvariety. Then $V \setminus W$ is dense in V.

Proof. Let $f \in \mathbb{C}[\mathrm{X}]$ be homogeneous, and vanishing on all of $V \setminus W$. As $W \neq V$, there exists $g \in I^h(W) \setminus I^h(V)$ by the projective nullstellensatz. Then fg vanishes on all of g. As $g \notin I^h(V)$, and $I^h(V)$ is prime, $f \in I^h(V)$. ☐

2.3 Rational maps

Definition 2.28 (function field, field of rational functions)

Let $V \subseteq \mathbb{P}^n$ be an irreducible variety, then the function field, or field of rational functions of V is defined as

$$\mathbb{C}(V) = \left\{ \frac{F}{G} \;\middle|\; F, G \in \mathbb{C}[\mathrm{X}] \text{ homogeneous of the same degree, } G \notin I^h(V) \right\} / \sim$$

where $F_1/G_1 \sim F_2/G_2$ if $F_1G_2 - F_2G_1 \in I^h(V)$.

Lemma 2.29. $\sim$ above is an equivalence relation.

Proof. Reflexivity and symmetry are obvious. Now suppose we have $F_1/G_1, F_2/G_2, F_3/G_3$ with $G_i \notin I^h(V)$, and

$$F_1G_2 - F_2G_1, F_2G_3 - F_3G_2 \in I^h(V)$$

Now consider $G_2(F_1G_3 - F_3G_1)$. Since $G_2 \notin I^h(V)$ and $I^h(V)$ os prime, it suffices to show that this is in $I^h(V)$. Equivalently, we want to show that this expression is zero in $\mathbb{C}[X]/I^h(V)$. In the quotient ring, we have

$$F_1G_2 = F_2G_1 \quad \text{and} \quad F_2G_3 = F_3G_2$$

Therefore, by substitution, we have that

$$F_1G_2G_3 - F_3G_1G_2 = F_2G_1G_3 - F_2G_1G_3 = 0 \in \mathbb{C}[X]/I^h(V)$$

□

Proposition 2.30. $\mathbb{C}(V)/\mathbb{C}$ is a finite extension of fields.

Proof. Suppose V is nonempty. Then there is a coordinate X_i which does not vanish identically on V, i.e. $X_i \notin I^h(V)$. By reordering coordinates, wlog X_0 does not vanish on V. But then it is clear that monomials with total degree zero, i.e.

$$X_0^{a_0} \cdots X_n^{a_n}$$

where $a_i \in \mathbb{Z}, \sum a_i = 0$ can be written in terms of X_i/X_0. So we are done. □

Corollary 2.31. Let $V \subseteq \mathbb{P}^n$ be an irreducible projective variety not contained in $\{X_0 = 0\}$. Let $V_0 = V \cap U_0$ be the affine variety in the 0-th affine patch.Then

$$\mathbb{C}(V) = \mathbb{C}(V_0)$$

Definition 2.32 (regular)
Let $\varphi \in \mathbb{C}(V)$ and $P \in V$. Then φ is regular at P if we can write $\varphi = F/G$ with $G(P) \neq 0$.

We can define the local ring and its maximal ideal as in the affine case. That is,

$$\mathcal{O}_{V,P} = \{f \in \mathbb{C}(V) \mid f \text{ is regular at } P\}$$
$$\mathfrak{m}_{V,P} = \{f \in \mathbb{C}(V) \mid f \text{ is regular at } P, f(P) = 0\}$$

Proposition 2.33. Suppose $V \subseteq \mathbb{P}^n$ is an irreducible projective variety not contained in $X_0 = 0$. Let $P \in V \cap U_0 = V_0$. Then we have an isomorphism

$$\mathcal{O}_{V,P} = \mathcal{O}_{V_0,P}$$

Proof. Follows from the isomorphism $\mathbb{C}(V) = \mathbb{C}(V_0)$. □

Definition 2.34 (rational maps)
Suppose V is an irreducible projective variety, then a rational map $\varphi : V \dashrightarrow \mathbb{P}^m$ is defined by

$$\varphi = (F_0, \ldots, F_m)$$

where $F_i \in \mathbb{C}[\mathrm{X}]$ homogeneous, not all F_i contained in $I^h(V)$. Furthermore, we say that $(F_i), (G_i)$ are the same[a] if $F_iG_j - F_jG_i \in I^h(V)$ for all i, j.

[a] i.e. a rational map is an equivalence class

By clearing denominators, we can also think about rational maps as an tuple $\varphi = (F_0 : F_1 : \cdots : F_m)$ where $F_i \in \mathbb{C}(V)$.

Definition 2.35 (regular point, domain, morphism)

A point $P \in V$ is a regular point of a rational map $\varphi : V \dashrightarrow \mathbb{P}^m$ if there exists a representative $\varphi = (G_0, \dots, G_m)$ such that $G_i(P) \neq 0$ for some i. That is, $\varphi(P)$ is a well defined point in $\mathbb{P}^n$.

The domain $\operatorname{dom}(\varphi)$ is the set of all regular points of φ. A rational map $\varphi : V \dashrightarrow \mathbb{P}^m$ is a morphism if $\operatorname{dom}(\varphi) = V$. In this case, we write $\varphi : V \to \mathbb{P}^m$.

Definition 2.36 ({rational map, morphism} between varieties)

If $W \subseteq \mathbb{P}^m$ is a projective variety, then a rational map (resp. morphism) is a rational map (resp. morphism) $\varphi : V \dashrightarrow \mathbb{P}^m$ (resp. $\varphi : V \to \mathbb{P}^m$) such that $\varphi(\operatorname{dom}(\varphi)) \subseteq W$.

Definition 2.37 (dominant)

A rational map $\varphi : V \dashrightarrow W$ is dominant of $\varphi(\operatorname{dom}(\varphi)) \subseteq W$ is dense in W.

Proposition 2.38. If φ is dominant, then for any rational map ψ, $\psi \circ \varphi$ is defined for any rational map ψ.

Proof. Let U be a dense open subset in $\operatorname{dom}(\varphi)$, U' an open subset in $\operatorname{dom}(\psi)$. Then let $U'' = U \cap \psi^{-1}(U')$. This is a nonempty open subset of V and the composition is well defined here. □

Definition 2.39 (birational)

Suppose $\varphi : V \dashrightarrow W$, $\psi : W \dashrightarrow V$ are rational maps, such that $\psi \circ \varphi, \varphi \circ \psi$ are well defined and equal to the identity maps of V, W respectively. Then we say that φ and ψ are birational.

Proposition 2.40. Rational maps are rational maps to $\mathbb{A}^1 \subseteq \mathbb{P}^1$. Therefore, given a dominant map $\varphi : V \to W$, we have a well defined pullback

$$\varphi^* : \mathbb{C}(W) \to \mathbb{C}(V)$$

where $\varphi^*(f) = f \circ \varphi$.

Theorem 2.41. Let V, W be irreducible varieties. Then V, W are birationally isomorphic if and only if there exists an isomorphism of fields $\mathbb{C}(V) \simeq \mathbb{C}(W)$.

2.4 Transformations, embeddings and products

Definition 2.42 (Veronese)

Let $F_0, \dots, F_m$ be the $m+1 = \binom{n+d}{d}$ degree d monomials in variables $X_0, \dots, X_n$. Then we have a natural morphism

$$v_d : \mathbb{P}^n \to \mathbb{P}^m$$

defined by $v_d(a) = (F_0(a), \dots, F_m(a))$.

Proposition 2.43. ν_d is an injective map, and $\nu_d(\mathbb{P}^n)$ is a projective variety isomorphic to $\mathbb{P}^n$.

Definition 2.44 (Segre embedding)
The Segre embedding is the map $\sigma_{mn} : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$, given by

$$\sigma_{mn}((x_i), (y_j)) = (x_i y_j)$$

In this case, we label the variables in $\mathbb{P}^{mn+m+n}$ as Z_{ij}, with $0 \leq i \leq m, 0 \leq j \leq n$.

Theorem 2.45. Let I be the ideal generated by

$$Z_{ij}Z_{pq} - Z_{iq}Z_{pj} \text{ for } i, p \in \{0, \dots, m\}, j, q \in \{0, \dots, n\}, i \neq p, j \neq q$$

and let $V = \mathbb{V}(I)$. Then $\sigma_{mn} : \mathbb{P}^m \times \mathbb{P}^n \to V$ is a bijection. Moreover, V is irreducible.

Proof. Clearly $\sigma_{mn} \subseteq V$. Now consider the affine piece

$$V_{00} = V \cap \{Z_{00} \neq 0\} \subseteq \mathbb{A}^{mn+m+n}$$

Then we have that $V_{00} = \mathbb{V}(I_{00})$, where after setting $Y_{ij} = Z_{ij}/Z_{00}$, we see that

$$I_0 0 = \left\langle Y_{ij} - Y_{i0}Y_{j0} \mid 1 \leq i \leq m, 1 \leq j \leq n \right\rangle$$

It then follows that it contains all $Y_{ij}Y_{pq} - Y_{iq}Y_{pj}$, and σ_{mn} defines an isomorphism $\mathbb{A}^m \times \mathbb{A}^n \to V_{00}$, with inverse

$$(Y_{ij}) \mapsto ((Y_{10}, \dots, Y_{m0}), (Y_{01}, \dots, Y_{0n}))$$

Since affine space is irreducible, and the product of irreducible affine varieties is irreducible, we have that V_{00} is irreducible. Repeating this for the other affine pieces gives us the result. $\square$

Definition 2.46 (product)
Suppose $V \subseteq \mathbb{P}^n$, $W \subseteq \mathbb{P}^m$ are projective varieties. Then we define the product to be

$$\sigma_{mn}(V \times W) \subseteq \mathbb{P}^{mn+m+n}$$

with the subspace topology.

Note the induced topology from above is *not* the product topology.

3 Singularities and tangent spaces

Definition 3.1 (tangent space of affine varieties)
Let $V \subseteq \mathbb{A}^n$ be a affine variety, $P \in V$. The tangent space to V at P is

$$T_{V,P} = \left\{ v \in \mathbb{C}^n \;\middle|\; \sum_{i=1}^{n} v_i \frac{\partial f}{\partial X_i}(P) = 0 \text{ for all } f \in I(V) \right\} \leq \mathbb{C}^n$$

Definition 3.2 (tangent space of projective varieties)
Let $V \subseteq \mathbb{P}^n$ be a projective variety, $P \in V$. Suppose $V_j = V \cap \{X_j \neq 0\}$ is an affine piece of V containing

P. Then define

$$T_{V,P} = T_{V_j,P}$$

where $T_{V_j,P}$ is the affine tangent space of the affine variety V_j at P.

Note that right now it is not clear that $T_{V,P}$ is well defined. However we will show that for different choices for j, the results are all naturally isomorphic[2].

Definition 3.3 (derivative)
Let $V \subseteq \mathbb{P}^n$, $W \subseteq \mathbb{P}^m$ be projective varieties, $\varphi : V \dashrightarrow W$ a rational map, $P \in \mathrm{dom}(\varphi)$. Assume wlog that $P \in V \cap U_0 = V \cap \mathbb{A}^n$, $\varphi(P) = Q \in W \cap U_0 = W \cap \mathbb{A}^m$, and we have a representative $\varphi = (F_0 : \cdots : F_m)$, where $F_j \in \mathbb{C}[\mathbf{X}]$ homogeneous. Set

$$f_j = \frac{F_j}{F_0}(1, X_1, \ldots, X_n) \in \mathbb{C}[X_1, \ldots, X_n]$$

Then define $\mathrm{d}\varphi_P : T_{V,P} \to \mathbb{C}^m$ by

$$\mathrm{d}\varphi_P(v) = \left(\sum_{i=1}^{n} v_i \frac{\partial f_j}{\partial X_i}(P)\right)_j$$

Proposition 3.4.

(i) $\mathrm{d}\varphi_P(T_{V,P}) \subseteq T_{W,\varphi(P)}$,

(ii) $\mathrm{d}\varphi_P$ depends only on φ, and not on the (F_i),

(iii) If $\psi : W \dashrightarrow Z$ is a rational map, with $\varphi(P) \in \mathrm{dom}(\psi)$, then $d(\psi \circ \varphi)_P = \mathrm{d}\psi_{\varphi(P)} \circ \mathrm{d}\varphi_P$,

(iv) if φ is birational, φ^{-1} regular at $\varphi(P)$, then $\mathrm{d}\varphi_P$ is an isomorphism.

Proof. (i) By the definition of the tangent space, we may replace V, W by the affine pieces $V \cap \mathbb{A}^n$ and $W \cap A^m$ repspectively. Let $Q = \varphi(P)$. Let $g \in I(W)$. Pulling back g with φ, we have that

$$h = g(f_1, \ldots, f_m)$$

and choose a representative of h in $\mathbb{C}(\mathbf{X})$. This is a rational function on V which is regular at P, and vanishes on the points of V where it is regular. That is, $h \in I(V)$. By the chain rule, we have

$$\frac{\partial h}{\partial X_i}(P) = \sum_j \frac{\partial g}{\partial Y_j}(Q) \frac{\partial f_j}{\partial X_i}(P)$$

Thus, if $v \in T_{V,P}$, then $\mathrm{d}\varphi_P(v) \in T_{W,Q}$, since we have that

$$\sum_i v_i \frac{\partial h}{\partial X_i}(P) = 0$$

(ii) If we choose another representation (F_j') for φ, then the corresponding rational functions f_j' will have the property that $f_j' - f_j$ vanishes on V when defined. So we have that $f_j' - f_j = p_j/q_j$, where $p_j \in I(V)$, $q_j \in \mathbb{C}[\mathbf{X}]$, $q_j(P) \neq 0$. Therefore, by the quotient rule, we have that

$$\frac{\partial f_j' - f_j}{\partial X_i}(P) = \frac{1}{q_j(P)} \frac{\partial p_j}{\partial X_i}(P)$$

as $p_j(P) = 0$. Therefore, if we choose $v \in T_{V,P}$, then

$$\sum_{i=1}^{n} v_i \frac{\partial f_j' - f_j}{\partial X_i}(P) = 0$$

[2]Most importantly, the will have the same dimension.

So $d\varphi_P$ is independent of the choice of the (F_j).
(iii) is just the chain rule, and (iv) follows from (iii). $\square$

Corollary 3.5. The tangent space of a projective variety is well defined.

Proof. Suppose $p \in U_i \cap U_j$. Then we have a birational map $\psi : U_i \dashrightarrow U_j$, induced by the identity map on $U_i \cap U_j$, and is defined at P. Therefore, we have a natural isomorphism $T_{V_i,P} \to T_{V_j,P}$. $\square$

Definition 3.6 (dimension, smooth, singular)
Let V be an affine or projective variety. Then

1. if V is irreducible, define $\dim(V) = \min\{\dim(T_{V,P} \mid P \in V)\}$,
2. if $P \in V$, V is irreducible, we say P is smooth if $\dim(T_{V,P}) = \dim(V)$, and P is singular otherwise.
3. if V is reducible, $\dim(V)$ is the maximum of the dimension of the irreducible components of V.

Theorem 3.7. The set of smooth points of V is a non-empty open subvariety.

Proof. Nonempty follows by definition. We can assume $V \subseteq \mathbb{A}^n$ is an affine variety, since we can look at the affine parts of a projective variety. Suppose $I(V) = \langle f_1, \ldots, f_m \rangle$. Then if $P \in V$,

$$T_{V,P} = \left\{ v \in \mathbb{C}^n \;\middle|\; \sum_i v_i \frac{\partial f_j}{\partial X_i}(P) = 0 \right\}$$

therefore, by some basic linear algebra,

$$\dim(T_{V,P}) = n - \operatorname{rank}\left(\frac{\partial f_j}{\partial X_i}\right)$$

Therefore, we have that for any $r \in \mathbb{N}$,

$$\{P \in V \mid \dim(T_{V,P}) \geq r\} = \left\{ P \;\middle|\; \operatorname{rank}\left(\frac{\partial f_j}{\partial X_i}\right) \leq n - r \right\}$$

is the closed subvariety generated by the $(n-r) \times (n-r)$ minors of the Jacobian matrix. $\square$

Corollary 3.8. Birational irreducible varieties have the same dimension.

4 Field theory

Definition 4.1 (transcendental)
Suppose L/K is a field extension, $\alpha \in L$ is transcendental over K if it is not the root of any nonzero polynomial in $K[X]$.

Definition 4.2 (algebraically independent)
Suppose L/K is a field extension, $S \subseteq L$ is algebraically independent over K if for all n, there is no nonzero polynomial $f \in K[X_1, \ldots, X_n]$ such that $p(s_1, \ldots, s_n) = 0$, $s_i \in S$.

Definition 4.3 (pure transcendental extension)
A field extension $K/\mathbb{C}$ is pure transcendental if

$$K = \mathbb{C}(x_1, \dots, x_n)$$

where $x_1, \dots, x_n$ are algebraically independent over $\mathbb{C}$.

Proposition 4.4. Let $K/\mathbb{C}$ be a finitely generated field extension. Then there exists a pure transcendental field extension $K_0 = \mathbb{C}(x_1, \dots, x_n)$ such that K/K_0 is finite[a]. Moreover, $K = K_0(y)$ for some $y \in K$.

[a] i.e. finite dimensional.

Proof. Suppose $K = \mathbb{C}(x_1, \dots, x_m)$. Then there is a maximal algebraically independent subset, which we can assume to be $\{x_1, \dots, x_n\}$. Define $K_0 = \mathbb{C}(x_1, \dots, x_n)$. Then each of $x_{n+1}, \dots, x_m$ is algebraic over K_0, so K/K_0 is finite. The final statement is just the primitive element theorem from Galois theory. $\square$

Proposition 4.5. Let $K = \mathbb{C}(x_1, \dots, x_n)$, with $x_1, \dots, x_n$ algebraically independent. Suppose x_{n+1} is algebraic over K. Then

$$I = \{g \in \mathbb{C}[X_1, \dots, X_{n+1}] \mid g(x_1, \dots, x_n, x_{n+1}) = 0\}$$

is a principal ideal of $\mathbb{C}[\mathbf{X}]$, generated by an irreducible $f \in \mathbb{C}[\mathbf{X}]$. Moreover, if f contains the variable X_i, then $\{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n\}$ are algebraically independent over $\mathbb{C}$.

Proof. As $x_1, \dots, x_n$ are algebraically independent, the subring $R = \mathbb{C}[x_1, \dots, x_n] \leq K$ is isomorphic to the polynomial ring $\mathbb{C}[X_1, \dots, X_n]$, which is a UFD. Let $h \in K[T]$ be the minimal polynomial of x_{n+1} over K. By definition, h is irreducible.

Now let $b = \operatorname{lcm}\{\text{denominators in coefficients of } h(T)\} \in R$. By Gauss' lemma[3], $f = bh$ is irreducible in $R[T]$. By the isomorphism above, we can think of $f \in \mathbb{C}[X_1, \dots, X_{n+1}]$.

We will now show that f generates the ideal I. Suppose we have $g \in \mathbb{C}[\mathbf{X}]$ such that $g(x_1, \dots, x_{n+1}) = 0$. Then in $K[T]$, $g(x_1, \dots, x_n, T)$ is divisible by $f(x_1, \dots, x_n, T)$. Applying Gauss' lemma[4], $f \mid g$ in $\mathbb{C}[x_1, \dots, x_n]$. So f generates the ideal I. $\square$

Corollary 4.6. Let V be any irreducible variety. Then V is birational to a hypersurface in $\mathbb{A}^{n+1}$, where $n = \dim(V)$.

Proof. Let $K = \mathbb{C}(V)$. By the above, $K = \mathbb{C}(x_1, \dots, x_{n+1})$, where $\{x_1, \dots, x_n\}$ are algebraically independent, x_{n+1} is algebraic over $\mathbb{C}(x_1, \dots, x_n)$. Then

$$K = \mathbb{C}(x_1, \dots, x_n) = \operatorname{Frac}\left(\frac{\mathbb{C}[X_1, \dots, X_{n+1}]}{\langle f \rangle}\right) = \mathbb{C}(\mathbb{V}(f))$$

$\square$

5 Proof of the Nullstellensatz

We prove the weak Nullstellensatz. Then proof of the Strong Nullstellensatz is non-examinable, hence omitted.

[3] Since f is primitive in $R[T]$ and irreducible in $K[T]$, it is irreducible in $R[T]$. We can assume f is primitive by minimality of b and the fact that h is monic.

[4] Since f is primitive, $f \mid g$ in $K[T]$ implies $f \mid g$ in R[T].

Theorem 5.1 (Weak Nullstellensatz). Every maximal ideal in $\mathbb{C}[\mathbf{X}]$ is of the form $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$, where $a_1, \ldots, a_n \in \mathbb{C}$. Moreover, if I is anu non-unit ideal, then $\mathbb{V}(I) \neq \varnothing$.

Proof. Every ideal of this form has $\mathbb{C}[\mathbf{X}]/I = \mathbb{C}$, so they are all maximal. Now suppose $\mathfrak{m} \trianglelefteq \mathbb{C}[\mathbf{X}]$ be a maximal ideal, $K = \mathbb{C}[\mathbf{X}]/\mathfrak{m}$. Then K is a field extension of $\mathbb{C}$. Write $a_i = X_i + \mathfrak{m}$. If $a_i \in \mathbb{C}$ for all i, then we re done, as the ideal is just $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

Otherwise, choose $t \in K \setminus \mathbb{C}$. As $\mathbb{C}$ is algebraically closed, t must be transcendental over $\mathbb{C}$. Let

$$U_m = \operatorname{span}_{\mathbb{C}} \left\{ a_1^{r_1} \cdots a_n^{r_n} \;\middle|\; r_i \geq 0, \sum r_i \leq m \right\} \leq \mathbb{C}$$

be the subspace of elements with exponenent at most m. Now as U_m is finite dimensional, $K = \bigcup_m U_m$ has countable dimension. However, the elements

$$\left\{ \frac{1}{t-c} \;\middle|\; c \in \mathbb{C} \right\}$$

are all $\mathbb{C}$-linearly independent. So we have uncountably many linearly independent elements. Contradiction.

Now suppose I is a non-unit ideal. Then there exists a maximal ideal $\mathfrak{m}$ such that $I \supseteq \mathfrak{m} \subseteq \mathbb{C}[\mathbf{X}]$, so $\mathbb{V}(I) \supseteq \mathbb{V}(\mathfrak{m}) \neq \varnothing$. ☐

6 Algebraic curves

6.1 Curves

Definition 6.1 (curve)

A curve is a (projective or affine) variety of dimension 1.

Unless otherwise specified, by curve we will mean "smooth projective irreducible 1-dimensional variety". Furthermore, when we say a curve C, where $C = \mathbb{V}(I) \subseteq \mathbb{P}^n$, we will often drop the $\subseteq \mathbb{P}^n$ and study curves up to isomorphism.

Proposition 6.2. Let C be a curve, $D \subsetneq C$ be a proper subvariety. Then D is a finite set of points.

Proof. Suffices to prove this for affine irreducible curves $V \subseteq \mathbb{A}^n$. If $W \subsetneq V$ is an irreducible subvariety, we will show that W is a point. By the Nullstellensatz, we have that $I(V) \subsetneq I(W)$. Suppose for contradiction that W is not a point. Then $\mathbb{C}[W] \neq \mathbb{C}$. Choose $t \in \mathbb{C}[W] \setminus \mathbb{C}$. Then t must be transcendental over $\mathbb{C}$.

The inclusion map $\varphi : W \hookrightarrow V$ induces an algebra homomorphism $\varphi^* : \mathbb{C}[V] \twoheadrightarrow \mathbb{C}[W]$[5]. Let $y \in (\varphi^*)^{-1}(t)$. Now choose $x \in \mathbb{C}[V]$ nonzero with $\varphi^*(x) = 0$. Now x, y are algebraically independent in $\mathbb{C}(V)$, as t is transcendental. Contradiction, since $\dim(V) = 1$ implies that the transcendence degree of $\mathbb{C}(V)$ is 1.

Therefore, we have that $\mathbb{C}[W] = \mathbb{C}$, so W is a point. ☐

Lemma 6.3 (Nakayama). Let R be a ring, M be a finitely generated R-module, $J \trianglelefteq R$ be an ideal. Then

(i) if $JM = M$, then there exists $r \in J$ such that $(1 + r)M = 0$.

(ii) if $N \leq M$ is a submodule such that $JM + N = M$, then there exists $r \in J$ such that $(1 + r)M \subseteq N$.

Proof. Some nonexaminable commutative algebra. ☐

Theorem 6.4. Suppose V is an irreducible curve, $P \in V$ is a smooth point. Then the ideal $\mathfrak{m}_{V,P} \trianglelefteq \mathcal{O}_{V,P}$

[5] The fact that this map is surjective comes from the definition of $\mathbb{C}[V]$ and $\mathbb{C}[W]$ as quotients.

is principal.

Proof. Suppose that P lies in an affine patch $V_0 \subseteq \mathbb{A}^n$ of $V \subseteq \mathbb{P}^n$. By a change of coordinates, wlog $P = (0, \dots, 0) \in \mathbb{A}^n$. Then we have that

$$\begin{aligned}
\mathbb{C}[V_0] &= \frac{\mathbb{C}[X_1, \dots, X_n]}{I(V_0)} = \mathbb{C}[x_1, \dots, x_n] \quad \text{where} \quad x_i = X_i \mod I(V_0) \\
\mathcal{O}_P := \mathcal{O}_{V_0,P} &= \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{C}[V_0], g \notin \langle x_1, \dots, x_n \rangle \right\} \\
\mathfrak{m}_P := \mathfrak{m}_{V_0,P} &= \left\{ \frac{f}{g} \;\middle|\; f, g \in \mathbb{C}[V_0], f \in \langle x_1, \dots, x_n \rangle, g \notin \langle x_1, \dots, x_n \rangle \right\} \\
&= x_1\mathcal{O}_p + \dots + x_n\mathcal{O}_p
\end{aligned}$$

More generally, if $J \trianglelefteq \mathcal{O}_P$ is any ideal, then $f/g \in J \iff f \in J$, since g is a unit in $\mathcal{O}_p$. So we can write

$$J = \left\{ \frac{f}{g} \;\middle|\; f \in J \cap \mathbb{C}[V_0], g \in \mathbb{C}[V_0], g(P) \neq 0 \right\}$$

Hence by the Hilbert basis theorem, J is finitely generated.

Since P is smooth, $T_{V,P}$ is a line in C^n. By a change of coordinates, we can assume wlog $T_{V,P} = \{x_2 = \dots = x_n = 0\}$. We will now show that $\mathfrak{m}_p = (x_1)$.

Since $T_{V,P}$ is cut out by linearisations of polynomials in $I(V_0)$, and $X_2, \dots, X_n$ are such lienarisations, we must have $f_2, \dots, f_n \in I(V_0)$ such that

$$f_j = X_j - h_j$$

where h_j has no terms of degree < 2. So in $\mathcal{O}_P$, we have

$$x_j = h_j(x_1, \dots, x_n) \in \left\langle x_1^2, x_1x_2, \dots, x_n^2 \right\rangle = \mathfrak{m}_P^2$$

Therefore, we have that

$$\mathfrak{m}_P = \sum_{j=1}^{n} x_i\mathcal{O}_P = x_1\mathcal{O}_P + \mathfrak{m}_P^2$$

Applying (ii) of Nakayama's lemma, with $R = \mathcal{O}_P, J = \mathfrak{m}_P, N = (x_1)$ gives the required result. □

Definition 6.5 (local parameter)
Suppose P is a smooth point of V, then any generator π_P of $\mathfrak{m}_{V,P}$ is called a local parameter, or local coordinate of P.

Corollary 6.6. Let $V = \mathbb{V}(f) \subseteq \mathbb{A}^2$ be an irreducible affine plane curve, $P \in V$ be a smooth point of V. Then the function $V \to \mathbb{C}$ given by

$$Q \mapsto X(Q) - X(P)$$

is a local parameter at P if and only if $\frac{\partial f}{\partial Y}(P) \neq 0$.

Proof. Same as the theorem. □

Corollary 6.7. Let P be a smooth point of a curve V. Then there exists a surjective group homomorphism $v_p : \mathbb{C}(V)^\times \to \mathbb{Z}$ such that

$$\mathcal{O}_{V,P} = \{0\} \cup \left\{ f \in \mathbb{C}(V)^\times \mid v_p(f) \geq 0 \right\}$$
$$\mathfrak{m}_{V,P} = \{0\} \cup \left\{ f \in \mathbb{C}(V)^\times \mid v_p(f) > 0 \right\}$$

and if $f \in \mathbb{C}(V)^\times$, then for any local parameter π_P, we can write

$$f = u\pi_P^{v_P(f)}$$

where $u \in \mathcal{O}_{V,P}^\times = \mathcal{O}_{V,P} \setminus \mathfrak{m}_{V,P}$.

Proof. Let π_P be a local parameter at P. Then $\mathfrak{m}_P^n = \langle \pi_P^n \rangle$ for all n. Now notice that we have a descending chain of ideals,

$$\mathcal{O}_P = \mathfrak{m}_P^0 \geq \mathfrak{m}_P^1 \geq \mathfrak{m}_P^2 \geq \dots$$

Let

$$J = \bigcap_n \mathfrak{m}_P^n$$

be the limit of this descending chain. In the proof of the previous theorem, we have seen that J is finitely generated. Furthermore, notice that

$$\mathfrak{m}_P J = \pi_P J = J$$

Hence by Nakayama's lemma, $J = 0$. Therefore, for any $f \in \mathcal{O}_P$, there exists $n \geq 0$ such that $f \in \mathfrak{m}_P^n \setminus \mathfrak{m}_P^{n+1}$. We define $v_P(f) = n$. Now notice that this means that $f = c\pi_P^n$ for some $c \in \mathcal{O}_P$. But $f \notin \mathfrak{m}_P^{n+1}$ implies that $c \in \mathcal{O}_p \setminus \mathfrak{m}_P = \mathcal{O}_P^\times$.

Now suppose $f \in \mathbb{C}(V)^\times \setminus \mathcal{O}_P$. We can write $f = g/h$, with $g, h \in \mathcal{O}_P$[6]. By the above, we can write $g = u\pi_P^k, h = v\pi_P^\ell$, where $u, v \in \mathcal{O}_P^\times$. moreover, since $f \notin \mathcal{O}_P$, $k < \ell$. So we have that

$$\frac{1}{f} = \pi_P^{\ell-k}\frac{v}{u} \in \mathcal{O}_P$$

For such f, define $v_P(f) = -v_P(1/f)$. The fact that v is a homomorphism is clear from definitions. □

Definition 6.8 (valuation)
The homomorphism $v_P : \mathbb{C}(V)^\times \to \mathbb{Z}$ is called the valuation at P.

Corollary 6.9. Let V be an irreducible curve, $P \in V$ smooth, $f \in \mathbb{C}(V)$. Then at least one of f, f^{-1} is regular at P.

Proof. At least one of $v_P(f), v_P(1/f) = -v_P(f)$ is nonnegative. □

Corollary 6.10. Let V be a smooth curve. Then any rational map $\varphi : V \dashrightarrow \mathbb{P}^m$ is a morphism.

Proof. By reordering coordinates, we can assume wlog that $\varphi(V)$ is not contained in $\{X_0 = 0\}$. So we can write

$$\varphi = (G_0 : \dots : G_m) = (1 : g_1 : \dots : g_m) \text{ where } g_j = \frac{G_j}{G_0} \in \mathbb{C}(V)$$

[6] This is obvious in the affine case, and in the projective case, we can assume wlog that P is in $\{X_0 \neq 0\}$. Then we can write $f = G/H$, where $G, H \in \mathbb{C}[\mathbf{X}]$ are homogeneous polynomials of degree d. Then $f = (G/X_0^d)/(H/X_0^d)$ is a ratio of elements of $\mathcal{O}_P$.

If all $g_j \in \mathcal{O}_P$, then we are done. Otherwise, let $t = \min_j \left\{ v_P(g_j) \right\}$. Now notice that $\min_j \left\{ v_P(\pi_P^{-t} g_j) \right\} = 0$. Therefore,

$$\varphi = (\pi_P^{-t} : \pi_P^{-t} g_1 : \cdots : \pi_P^{-t} g_m)$$

is regular at P. □

6.2 Degree and ramification

Proposition 6.11. Let $\varphi : V \to W$ be a nonconstant morphism of irreducible, *possibly singular* curves. Then

(i) for all $Q \in W$, $\varphi^{-1}(Q)$ is finite,

(ii) the map φ induces an inclusion of function fields $\varphi^* : \mathbb{C}(W) \hookrightarrow \mathbb{C}(V)$ which makes $\mathbb{C}(V)$ a finite extension of $\mathbb{C}(W)$.

Proof. (i) $\varphi^{-1}(Q)$ is a closed subvariety of V, and as φ is not constant, it is not all of V. Hence it must be a finite set of points.

(ii) Since $\dim(V) > 0$, V is infinite. So by (i), $\varphi(V)$ is also infinite. Thus, it is a dense subset of W. Therefore, φ is dominant, so $\varphi^* : \mathbb{C}(W) \to \mathbb{C}(V)$ is well defined and injective. Let $t \in \mathbb{C}(W) \setminus \mathbb{C}$, and set $x = \varphi(t)$. Since $\mathbb{C}(V)/\mathbb{C}$ is finitely generated, and finite over the degree 1 transcendental extension $\mathbb{C}(X)/\mathbb{C}$, it must also be finite over the intermediate extension $\varphi^*(\mathbb{C}(W))$. □

Definition 6.12 (degree)

Let $\varphi : V \to W$ be a non constant morphism of irreducible curves. Then the degree of φ is

$$\deg(\varphi) = [\mathbb{C}(V) : \varphi^* \mathbb{C}(W)]$$

Definition 6.13 (ramification degree)

Suppose $P \in V, Q = \varphi(P) \in W$ are smooth points. Define the ramification degree of $\varphi : V \to W$ at P to be

$$e_P = e(\varphi, P) = v_P(\varphi^* \pi_Q)$$

where π_Q is any local parameter for W at Q.

Definition 6.14 (quasiprojective variety)

A quasiprojective variety U is a Zariski open subset of a projective variety $V \subseteq \mathbb{P}^n$.

We can define irreducibility, rational functions, rational maps and morphisms for quasiprojective varieties in the same way as for projective varieties.

Proposition 6.15. The projection map[a] $\mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$ is a closed map.

[a] Where we consider $\mathbb{P}^n \times \mathbb{A}^m \subseteq \mathbb{P}^n \times \mathbb{P}^m$ is a quasiprojective variety, and the topology on $\mathbb{P}^n \times \mathbb{P}^m$ is the one coming from the Segre embedding.

Proof. Omitted. □

Proposition 6.16. Let $\varphi : V \to W$ be a morphism of quasiprojective varieties, and suppose V is projetcive. Then φ is closed.

Proof. First of all, we can factorise φ as

$$V \longrightarrow \Gamma_\varphi = \{(P, \varphi(P) \mid P \in V\} \longrightarrow W$$

Now notice that the diagonal $\Delta \subseteq W \times W$ is closed[7]. Then $\Gamma_\varphi = (\varphi \times \mathrm{id})^{-1}(\Delta)$ is a closed set[8]

Since $V \subseteq \mathbb{P}^n$ is closed, suffices to show $\mathbb{P}^n \times W \to W$ is a closed map. Moreover, if W is covered by affines U_i, it suffices to show that $\mathbb{P}^n \times U_i \to U_i$ is closed. But now notice that each U_i is a closed subset of $\mathbb{A}^m$, and the result follows from the previous proposition. □

Corollary 6.17. Let $\varphi : V \to W$ be a non constant morphism between irreducible projective, not necessarily smooth, curves. Then φ is surjective.

Proof. $\mathrm{im}(\varphi)$ is a closed subvariety, and it is not a point, so it must be all of W. □

Theorem 6.18 (finiteness theorem for curves)**.** Suppose V, W smooth projective curves, $\varphi : V \to W$ a morphism, then for any $Q \in W$,

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

Furthermore, for all but finitely many $P \in V$, we have $e_P = 1$.

Proof. Omitted[9]. □

Corollary 6.19. Let V be a smooth projective irreducible curve, $f \in \mathbb{C}(V)^\times$. Then

(i) if f is regular for all $P \in V$, then f is constant,

(ii) the set of P such that $v_P(f) \neq 0$ is finite, and $\sum_{P \in V} v_P(f) = 0$.

Proof. Consider the morphism $\varphi : V \to \mathbb{P}^1$ given by

$$\varphi = (1 : f)$$

Now $\varphi(P) = (0 : 1)$ if and only if f is not regular at P. Therefore, if f is regular at all P, then it can't be surjective, so it must be constant.

(ii) We can assume wlog that f is non constant. Let $t = X_1/X_0$. This is a local coordinate at the point $0 = (1 : 0) \in \mathbb{P}^1$. Now notice that $\varphi^*(t) = t \circ \varphi = f$. Therefore, if $f(P) = 0$, then $e_P = v_P(\varphi^*(t)) = v_P(f)$. Similarly, $1/t = X_0/X_1$ is a local parameter near $\infty = (0 : 1) \in \mathbb{P}^1$, and if $f(P) = \infty$, then

$$e_P = v_P(\varphi^*(1/t)) = -v_P(f)$$

Finally, if $\varphi(P) \neq 0, \infty$, then $v_P(f) = 0$, so by the finiteness theorem,

$$\deg(\varphi) = \sum_{P \in \varphi^{-1}(p)} v_P(f) = -\sum_{P \in \varphi^{-1}(\infty)} v_P(f)$$

and the result follows. □

Morally, the number of zeros and poles of a rational function are the same, and most points are neither.

[7] Recall $W \times W$ has the topology from the Segre map, *not* the product topology

[8] In the ambient $\mathbb{P}^n \times \mathbb{P}^m$.

[9] In Dhruv's notes he says that we prove the "Furthermore ..." sentence later on. One way would be to derive this as a corollary to Riemann-Hurwitz, but as the proof of Riemann-Roch is omitted, it's not clear that this is not circular.

On the other hand we prove this theorem in the Riemann surfaces setting, called the valency theorem.

7 Divisors

From now on, curve = "smooth projective irreducible curve"

7.1 Divisors

Definition 7.1 (divisor)
Let V be a curve, then the set of divisors on V is

$$\mathrm{Div}(V) = \bigoplus_{P \in C} \mathbb{Z} \cdot [P]$$

where a divisor $D \in \mathrm{Div}(V)$ is a finite integer linear combination $\sum n_P[P]$.

Definition 7.2 (degree of a divisor)
The degree of a divisor $D = \sum n_P[P]$ is

$$\deg(D) = \sum n_P \in \mathbb{Z}$$

$\deg : \mathrm{Div}(V) \to \mathbb{Z}$ is a homomorphism, and we write

$$\mathrm{Div}^0(V) = \ker(\deg)$$

for the degree zero divisors.

Definition 7.3 (valuation of a divisor)
If $D = \sum n_P[P]$, we write $v_P(D) = n_P$.

Definition 7.4 (rational functions poles bounded by D)
Let D be a divisor on a curve V. Then the space of rational functions with poles bounded by D is

$$L(D) = \{f \in \mathbb{C}(V) \mid \forall P \in V, v_P(f) + v_P(D) \geq 0\}$$

That is, if $n_P \geq 0$, then f has a pole of order at most n_P at P. If $n_P < 0$, then f has a zero of order at least $|n_P|$ at P.

Definition 7.5 (divisor of a function)
Let $f \in \mathbb{C}(V)^\times$ be a nonzero rational function. The divisor of f is

$$\mathrm{div}(f) = \sum_{P \in V} v_P(f)[P]$$

Divisors of this form are called principal divisors. We write $\mathrm{Prin}(V)$ for the set of principal divisors.

Proposition 7.6. $\mathrm{Prin}(V)$ is a subgroup of $\mathrm{Div}^0(V)$.

Proof.

$$\deg(\mathrm{div}(f)) = \sum_{P \in V} v_P(f) = 0$$

by the finiteness theorem. Furthermore, $\mathrm{div}(f) + \mathrm{div}(g) = \mathrm{div}(fg)$, so it is a subgroup. □

Definition 7.7 (class group)

The class group of V is

$$\mathrm{Cl}(V) = \frac{\mathrm{Div}(V)}{\mathrm{Prin}(V)}$$

Definition 7.8 (linearly equivalent)

Divisors D and D' are linearly equivalent if $D - D' \in \mathrm{Prin}(V)$. That is, they give the same class in the class group.

Definition 7.9 (hyperplane section)

Let $V \subseteq \mathbb{P}^n$ be a curve, L be a homogeneous linear function, $V \not\subseteq \mathbb{V}(L)$. Then the hyperplane section of V by $\mathbb{V}(L)$ is

$$\mathrm{div}(L) = \sum_{P \in V} n_P[P] \quad \text{where} \quad n_P = v_P\left(\frac{L}{X_i}\right) \quad \text{for } i \text{ such that } X_i(P) \neq 0$$

Proposition 7.10. The hyperplane section is well defined. That is, it does not depend on i. Furthermore, all $n_P \geq 0$.

Proof. If $X_i(P), X_j(P) \neq 0$, then

$$v_P\left(\frac{L}{X_i}\right) - v_P\left(\frac{L}{X_j}\right) = v_P\left(\frac{X_j}{X_i}\right) = 0$$

Furthermore, $L/X_i \in \mathcal{O}_P$, so $v(L/X_i) \geq 0$. □

Proposition 7.11. Let V be a curve, L, L' linear homogeneous polynomials, neither vanishing on all of V. Then

$$\mathrm{div}(L) - \mathrm{div}(L) = \mathrm{div}(L/L')$$

In particular, $\mathrm{div}(L)$ and $\mathrm{div}(L')$ are linearly equivalent, so $\deg(\mathrm{div}(L)) = \deg(\mathrm{div}(L'))$.

Proof. By definition. □

Definition 7.12 (degree of a curve)

Let $V \subseteq \mathbb{P}^n$ be a curve. Then the degree of V is

$$\deg(V) = \deg(\mathrm{div}(L))$$

for any L with $V \not\subseteq \mathbb{V}(L)$.

Definition 7.13 (effective divisor)

A divisor $D = \sum n_P[P]$ is effective if $n_P \geq 0$ for all P. Wr write this as $D \geq 0$.

Proposition 7.14.
$$L(D) = \{f \in \mathbb{C}(V) \mid f = 0 \text{ or } \operatorname{div}(f) + D \geq 0\}$$

Proof. By definitions. □

Proposition 7.15. $L(D)$ is a complex vector space.

Proof. If f, g are nonzero rational functions, then $v_P(f+g) \geq \min\{v_P(f), v_P(g)\}$, so $L(D)$ is closed under addition. It is clearly closed under scalar multiplication. □

Notation 7.16. We write $\ell(D) = \dim(L(D))$.

Proposition 7.17. Let D be a divisor on V. Then

(i) if $\deg(D) < 0$, then $L(D) = 0$,

(ii) if $\deg(D) \geq 0$, then $\ell(D) \leq \deg(D) + 1$,

(iii) for any $P \in V$, $\ell(D) \leq \ell(D - [P]) + 1$.

In particular, $L(D)$ is always finite dimensional.

Proof. (i) If $L(D) \neq 0$, then for $0 \neq f \in L(D)$, $E = \operatorname{div}(f) + D \geq 0$. But then this means that $\deg(D) = \deg(E) \geq 0$. (iii) Let $n = v_P(D)$. Then define $\mathrm{ev}_P : L(D) \to \mathbb{C}$ by $\mathrm{ev}_P(f) = (\pi_P^n f)(P)$. This is a linear map, and the kernel is $L(D-P)$. Hence by rank nullity, $\ell(D-P) \geq \ell(D) - 1$. (ii) If $d = \deg(D) \geq 0$, we see that

$$\ell(D) \leq \ell(D - (d+1)[P]) + d + 1 = d + 1$$

since $\deg(D - (d+1)[P]) < 0$, so $\ell(D - (d+1)[P]) = 0$. □

Proposition 7.18. If D, E are linearly equivalent divisors on a curve, then $\ell(D) = \ell(E)$.

Proof. Say $D - E = \operatorname{div}(g)$. Then $f \mapsto fg$ defines a linear map $L(E) \to L(D)$, and $f \mapsto f/g$ defines the inverse map. □

7.2 Bezout's theorem

Definition 7.19 (hypersurface section of a morphism)
Suppose $\varphi : V \to \mathbb{P}^n$ any non constant morphism, G homogeneous of degree m, with $\operatorname{im}(\varphi) \nsubseteq \mathbb{V}(G)$. Then define

$$\operatorname{div}(G) = \sum_{P \in V} n_P[P] \quad \text{where} \quad n_p = v_P\left(\frac{\varphi^*(G)}{X_i^m}\right) \quad \text{where } X_i(P) \neq 0$$

Theorem 7.20 (weak Bezout). Let $V, W \subseteq \mathbb{P}^2$ be distinct smooth projective irreducible curves of degree m, n respectively. Then

$$|V \cap W| \leq mn$$

Proof. Suppose $V = \mathbb{V}(F), W = \mathbb{V}(G)$ where F, G are homogeneous polynomials of degree m, n respectively. We can replace G by any other homogeneous polynomial of degree m, since it will give a linearly equivalent divisor. Let $\iota : V \to \mathbb{P}^2$ be the inclusion map. Replacing G with L^n, where L is linear homogeneous, we see that

$$|\mathbb{V}(L) \cap V| \leq m = \deg(V)$$

and

$$\operatorname{div}(\iota^*(G)) = \sum_{P \in V \cap \mathbb{V}(G)} n_P[P]$$

But $\operatorname{div}(\iota^* G) = n\operatorname{div}(\iota^* L) = n\operatorname{div}(L)$, so $\deg(\operatorname{div}(\iota^* G)) = n \deg(\operatorname{div}(L)) = mn$. Furthermore, $n_P > 0$ if and only if G vanishes at P. $\square$

7.3 Differentials

Let $K/\mathbb{C}$ be a field extension.

Definition 7.21 (differential)
The space of differentials is

$$\Omega_{K/\mathbb{C}} = \frac{M}{N} = \frac{\operatorname{span}_K \{\delta x \mid x \in K\}}{\operatorname{span}_K \{\delta(x+y) - (\delta x + \delta y), \delta(xy) - (x\delta y + y\delta x), \delta a \mid x, y \in K, a \in \mathbb{C}\}}$$

and define the differential of $x \in K$ to be $\mathrm{d}x = \delta x \mod N$.

Proposition 7.22. $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$, $\mathrm{d}(xy) = x\mathrm{d}y + y\mathrm{d}x$, $\mathrm{d}a = 0$.

Definition 7.23 (exterior derivative)
The map $d : K \to \Omega_{K/\mathbb{C}}$ is called the exterior derivative.

Notation 7.24. We will write $\Omega_K = \Omega_{K/\mathbb{C}}$ as we are fixing the base field to be $\mathbb{C}$.

Definition 7.25 (derivation)
Let U be a K-vector space. A $\mathbb{C}$ linear map $D : K \to U$ is called a derivation of $D(xy) = xDy + yDx$.

Lemma 7.26 (universal properties of derivations)**.** A linear map $D : K \to U$ is a derivation if and only if there exists a K-linear map $\lambda : \Omega_K \to U$ such that

$$\begin{tikzcd} K \arrow[rr, "D"] \arrow[dr, "d"'] & & U \\ & \Omega_K \arrow[ur, "\lambda"'] & \end{tikzcd}$$

commutes.

Lemma 7.27. For any derivation D, we have That

$$D\left(\frac{x}{y}\right) = \frac{yDx - xDy}{y^2}$$

Proof. Expand $Dx = D(y(x/y))$ using Leibniz. □

Lemma 7.28. Let $f = \mathbb{C}(X_1, \ldots, X_n)$ be a rational function, $y = f(x_1, \ldots, x_n)$. Then

$$\mathrm{d}y = \sum_i \frac{\partial f}{\partial X_i}(x_1, \ldots, x_n)\mathrm{d}x_i$$

In particular, if $K = \mathbb{C}(x_1, \ldots, x_n)$, then Ω_K is spanned by $\mathrm{d}x_1, \ldots, \mathrm{d}x_n$.

Proof. Chain rule from calculus. □

Theorem 7.29. Let $K/\mathbb{C}(t)$ be finite, where t is trasncendental over $\mathbb{C}$. Then Ω_K is a 1-dimensional K-vector space, spanned by $\mathrm{d}t$.

Proof. First we consider the case $K = \mathbb{C}(t)$. By the leamma, Ω_K is spanned by $\mathrm{d}t$, so we need to show $\mathrm{d}t \neq 0$. By the universal property, suffices to show that a nonzero derivation exists. $\frac{\mathrm{d}}{\mathrm{d}t} : \mathbb{C}(t) \to \mathbb{C}(t)$ works.

In the general case, let $K_0 = \mathbb{C}(t), K = K_0(\alpha)$. Let $h \in K_0[X]$ be the minimal polynomial of α. As h is minimal, $h'(\alpha) \neq 0$. Therefore, by the lemma, $\mathrm{d}t, \mathrm{d}\alpha$ span Ω_K.

For $f \in K_0[X]$, write $D_t f = \frac{\partial f}{\partial t}$. Then by the chain rule, we have that

$$0 = \mathrm{d}(h(\alpha)) = (D_t h)(\alpha)\mathrm{d}t + h'(\alpha)\mathrm{d}\alpha$$

So Ω_K is spanned by $\mathrm{d}t$. Therefore, suffices to write sown a non-zero derivation $K \to K$.

First, define $D : K_0[X] \to K$ by

$$D(f) = D_t(f) \text{ if } f \in K_0 \tag{1}$$
$$D(X) = -\frac{(D_t h)(\alpha)}{h'(\alpha)} \tag{2}$$
$$D(X^n) = n\alpha^{n-1}D(X) \tag{3}$$

Then $D(h) = 0$, so D vanishes on $hK_0[X] \trianglelefteq K_0[X]$, so it gives us a derivation $D : K \to K$, with $Dt = 1$. □

7.4 Differentials on curves

Definition 7.30 (rational differentials)
Let V be a curve, then define

$$\Omega_V = \Omega_{\mathbb{C}(V)/\mathbb{C}}$$

Definition 7.31 (regular)
A differential $\omega \in \Omega_V$ is regular at $P \in V$ if

$$\omega = \sum_i f_i \mathrm{d}g_i$$

where $f_i, g_i \in \mathcal{O}_{V,P}$. Write $\Omega_{V,P}$ for the set of all regular differentials at P.

Remark 7.32. $\Omega_{V,P}$ is not a vector subspace of Ω_V.

Proposition 7.33. If $\omega \in \Omega_V$, then $\pi_P^k \omega \in \Omega_{V,P}$ for k sufficiently large.

Proof. Let k be such that $\pi_P^k f \in \mathcal{O}_{V,P}$ and ℓ be such that $\pi_P^\ell g \in \mathcal{O}_{V,P}$. Then

$$\begin{aligned}
\pi_P^{k+\ell+1} f \mathrm{d}g &= (\pi_P^k f)(\pi_P^{\ell+1} g) \\
&= (\pi_P^k f)(\mathrm{d}\big(\pi_P^{\ell+1} g\big) - (\ell+1)\pi_P^\ell g \mathrm{d}\pi_P) \\
&= \pi_P^k f\, \mathrm{d}\big(\pi_P^{\ell+1} g\big) - (\ell+1)(\pi_P^k f)(\pi_P^\ell g)\mathrm{d}\pi_P \in \Omega_{V,P}
\end{aligned}$$

□

Theorem 7.34. $\Omega_{V,P}$ is a free $\mathcal{O}_{V,P}$-module, generated by $\mathrm{d}\pi_P$, where π_P is a local coordinate at p. That is,

$$\Omega_{V,P} = \{ f \mathrm{d}\pi_P \mid f \in \mathcal{O}_{V,P} \}$$

Proof. Clearly we have that $\mathcal{O}_P \mathrm{d}\pi_P \subseteq \Omega_{V,P}$. Now given $f \in \mathcal{O}_P$, we can write it as

$$f = f(P) + \pi_P g \in \mathcal{O}_P = \mathbb{C} + \mathfrak{m}_P$$

Then by the Leibniz rule, we have that

$$\mathrm{d}f = g\mathrm{d}\pi_P + \pi_P \mathrm{d}g \in \mathcal{O}_P \mathrm{d}\pi_P + \pi_P \Omega_{V,P}$$

If we apply Nakayama's lemma, with $R = \mathcal{O}_P$, $J = \mathfrak{m}_P$, $M = \Omega_{V,P}$, $N = \mathcal{O}_P \mathrm{d}\pi_P$, we get that $\Omega_{V,P} = \mathcal{O}_P \mathrm{d}\pi_P$. Therefore, all we need to check is that $\Omega_{V,P}$ is a finitely generated $\mathcal{O}_P$ module. Choose an affine piece $V_0 \subseteq \mathbb{A}^n$ of V containing P, so $\mathbb{C}[V_0] = \mathbb{C}[x_1, \ldots, x_n]$, where the x_i generate $\mathbb{C}[V_0]$ as a $\mathbb{C}$-algebra. Now for $f \in \mathcal{O}_P$, then $f = g/h$ for polynomials g, h with $h(P) \neq 0$. Then by the quotient rule,

$$\mathrm{d}f = \sum \frac{h\frac{\partial g}{\partial X_i} - g\frac{\partial h}{\partial X_i}}{h^2}(x)\mathrm{d}x_i$$

Since $h(P) \neq 0$, the coefficient of $\mathrm{d}x_i$ is in $\mathcal{O}_P$. Therefore $\mathrm{d}x_1, \ldots, \mathrm{d}x_n$ generate $\Omega_{V,P}$ as a $\mathcal{O}_P$ module. □

Corollary 7.35. If π_P, π_P' are local parameters at P, then $\mathrm{d}\pi_P' = u\mathrm{d}\pi_P$, where $u \in \mathcal{O}_{V,P}^\times$.

Proof. Write $\mathrm{d}\pi_P' = u\mathrm{d}\pi_P, \mathrm{d}\pi_P = v\mathrm{d}\pi_P'$, then $uv = 1$. □

Corollary 7.36. Any $\omega \in \Omega_V$ can be written as $\omega = f\mathrm{d}\pi_P$ for some $f \in \mathbb{C}(V)$.

Proof. Let k be such that $\pi_P^k \omega \in \Omega_{V,P}$. Then we have that $\pi_P^k \omega = g\mathrm{d}\pi_P$ for some $g \in \mathcal{O}_{V,P}$. So $\omega = \pi_P^{-k} g \mathrm{d}\pi_P$. □

Definition 7.37 (valuation of a differential)
If $\omega \in \Omega_V$, $P \in V$, define

$$v_P(\omega) = v_P(f)$$

where $\omega = f d\pi_P$[a].

[a] Different choices of local parameters will give f which differ by a unit, so the valuation is the same.

Proposition 7.38. $v_P(\omega) \geq 0$ if and only of ω is regular at P.

Lemma 7.39. Let $\omega \in \Omega_V$ be a nonzero differential on a curve V. Then $v_P(\omega) = 0$ for all but finitely many $P \in V$.

Proof. $v_P(f) = 0$ for all but finitely many P[10]. □

Definition 7.40 (divisor)
The divisor of $\omega \in \Omega_V$ is

$$\text{div}(\omega) = \sum_{P \in V} v_P(\omega)[P]$$

Proposition 7.41. If ω, ω' are nonzero differentials on V, then $\text{div}(\omega) - \text{div}(\omega')$ is principal.

Proof. Since Ω_V is a 1-dimensional $\mathbb{C}(V)$ vector space, $\omega = f\omega'$ for some $f \in \mathbb{C}(V)$. Then $\text{div}(\omega) = \text{div}(f) + \text{div}(\omega')$. □

Definition 7.42 (canonical class)
The class of $\text{div}(\omega)$ in $\text{Cl}(V)$ for any nonzero $\omega \in \Omega_V$ is called the canonical class. We also call $D = \text{div}(\omega)$ a canonical divisor.

Definition 7.43 (genus)
Let V be a curve, K_V a canonical divisor of V. Then the genus of V is

$$g(V) = \ell(K_V)$$

where K_V is any canonical divisor on V.

Theorem 7.44. Let $V = \mathbb{V}(F) \subseteq \mathbb{P}^2$ be a plane curve of degree $d \geq 3$. Then $K_V = (d-3)H$, where H is the divisor of a hyperplane section.

Proof. **Step 1: Choosing an appropriate differential.** By a change of coordinates, wlog $(0:1:0) \notin V$. Let $x = X_1/X_0, y = X_2/X_0 \in \mathbb{C}(V)$. Let $f(X,Y) = F(1,X,Y)$, then $f(x,y) = 0$ in $\mathbb{C}(V)$. Differentiating this, we get

$$\frac{\partial f}{\partial X}(x,y)\mathrm{d}x + \frac{\partial f}{\partial Y}(x,y)\mathrm{d}y = 0$$

in Ω_V. We will consider the differential

$$\omega = \frac{\mathrm{d}x}{\frac{\partial f}{\partial Y}(x,y)} = -\frac{\mathrm{d}y}{\frac{\partial f}{\partial X}(x,y)}$$

[10] Dhruv's notes proves it for general $f\mathrm{d}g$, but we don't need to since we already know that $\omega = f\mathrm{d}\pi_P$ for some f.

Then suffices to show that $\mathrm{div}(\Omega) = (d-3)\mathrm{div}(X_0)$.

Step 2: Calculating in an affine patch. Here, we identify $U_0 = \mathbb{A}^2$. Let $P \in V \cap \mathbb{A}^2$. If $\frac{\partial f}{\partial Y}(P) \neq 0$, then $x - x(P)$ is a local parameter at P, so

$$v_P(\omega) = v_P\left(\frac{1}{\frac{\partial f}{\partial y}(P)}\right) = 0$$

Otherwise $\frac{\partial f}{\partial X}(P) \neq 0$, so $y - y(P)$ is a local parameter, and we also have $v_P(\omega) = 0$.

Step 3: Calculation at infinity[11]. Since we assumed that $(0:1:0) \notin V$, any point on V at infinity must be in $\{X_2 \neq 0\}$. On this open set, we can reparametrize the curve by $g(z, w) = 0$, where

$$z = \frac{X_0}{X_2} = \frac{1}{y}, \quad w = \frac{X_1}{X_2} = \frac{x}{y} \quad \text{and} \quad g(Z, W) = F(Z, W, 1)$$

Now consider the differential

$$\eta = \frac{\mathrm{d}z}{\frac{\partial g}{\partial Z}(z, w)} = -\frac{\mathrm{d}w}{\frac{\partial g}{\partial W}(z, w)}$$

The same argument as in step 2 shows that $v_P(\eta) = 0$ for any $P \in U_2$. But we have that $f(X, Y) = Y^d g(1/Y, X/Y)$. Differentiating this,

$$\frac{\partial f}{\partial X} = Y^{d-1}\frac{\partial}{\partial g}(W)(1/Y, X/Y)$$

and so we have that[12]

$$\omega = -\frac{\mathrm{d}y}{\frac{\partial f}{\partial X}(x, y)} = \frac{z^{-2}\mathrm{d}z}{y^{d-1}(\frac{\partial g}{\partial W}(z, w))} = z^{d-3}\eta$$

Therefore, if $X_2(P) \neq 0$, then $v_P(\omega) = (d-3)v_P(z) + v_P(\eta) = (d-3)v_P(z)$. Since $z = X_0/X_2$, $\mathrm{div}(\omega) = (d-3)\mathrm{div}(X_0)$ as claimed. □

Proposition 7.45. If $f(x, y) = 0$ is an affine equation for a smooth projective plane curve, with $\deg(f) \geq 3$, then

$$\left\{\frac{x^r y^s \mathrm{d}x}{\frac{\partial f}{\partial y}} \mid 0 \leq r + s \leq d - 3\right\}$$

is a basis for $L(K_V)$ for the representative $K_V = (d-3)H$, where H is the hyperplane at infinity.

Proof. Non-examinable, omitted. □

Corollary 7.46. If $d, d' \geq 2$ distinct integers, then no smooth plane curves of d, d' respectively can be isomorphic.

8 Riemann-Roch

Theorem 8.1 (Riemann-Roch)**.** Let V be a smooth projective irreducible curve, $g = g(V)$ and $K = K_V$ a canonical divisor. Then for any divisor D,

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

Proof. Omitted. □

[11] i.e. $X_0 = 0$

[12] $\mathrm{d}y = -z^{-2}\mathrm{d}y$ so the sign is correct.

Corollary 8.2. Let K be a canonical divisor on a curve V. Then $\deg(K) = 2g - 2$.

Proof. If we set $D = K$, we get $\ell(D) = \ell(K) = g$ and $\ell(K - D) = \ell(0) = 1$. □

Corollary 8.3. A smooth projective plane curve of degree d has genus $\frac{(d-1)(d-2)}{2}$.

Proof. The degree of K_V for a degree d plane curve with $d \geq 3$ is $(d-3)\deg(V) = d(d-3) = 2g - 2$. For the $d = 1, 2$ cases, $V \simeq \mathbb{P}^1$ and we can compute that $g(\mathbb{P}^1) = 0$. □

Corollary 8.4. If $\deg(D) > 2g - 2$, then $\ell(D) = 1 - g + \deg(D)$.

Proof. $\deg(K - D) < 0$, so $\ell(K - D) = 0$. □

Corollary 8.5. If $g(V) = 1$, and $\deg(D) > 0$, then $\ell(D) = \deg(D)$.

Proof. For $V = \mathbb{P}^1$, $\ell(D) = \deg(D) + 1$, $\ell(K) = 1$, result follows from Riemann-Roch. □

8.1 Elliptic curves

Definition 8.6 (Elliptic curve)
An elliptic curve is a pair $E = (V, P_0)$, where V is a genus 1 curve, $P_0 \in V$.

Definition 8.7 (group law)
Let $P, Q \in E$. By Riemann Roch, $\ell(P + Q - P_0) = 1$. Therefore there is a unique effective divisor of degree 1, i.e. a point R such that $P + Q - P_0 \sim R$. We define

$$P +_E Q = R$$

Theorem 8.8. $(E, +_E)$ is an abelian group with identity element P_0. Moreover, the map $\beta : P \mapsto [P - P_0] \in \mathrm{Cl}^0(E)$ is an isomorphism between E and the group $\mathrm{Cl}^0(E)$ of degree zero divisor classes on E.

Proof. **β is injective.** Suppose $\beta(P) = \beta(Q)$. Then $P - P_0 \sim Q - P_0$. So $P \sim Q$. However, $\ell(P) = 1$ by Riemann-Roch, so $P = Q$.

β is surjective. Say D has degree 0. $\ell(D + P_0) = 1$, so there exists P such that $D + P_0 \sim P$. Hence $[D] = \beta(P)$. □

8.2 Riemann-Hurwitz

Proposition 8.9. Let $\varphi : V \to W$ be a morphism of curves, $t \in \mathbb{C}(W)$ such that $\mathbb{C}(W)/\mathbb{C}(t)$ is finite. Then $\mathbb{C}(V)/\varphi^*\mathbb{C}(t)$ is finite, and Ω_V is generated by $\mathrm{d}\varphi^*(t)$.

Definition 8.10 (pullback of differentials)
Let $\omega = f\,\mathrm{d}t \in \Omega_W$. Then define

$$\varphi^*(\omega) = \varphi^*(f) d\varphi^*(t)$$

Lemma 8.11. Let $P \in V, Q = \varphi(P) \in W$, e_P be the ramification degree of φ at P, and π_P, π_Q local parameters at P, Q respectively. Then

$$v_P(\varphi^*(d\pi_Q)) = e_P - 1$$

More generally,

$$v_P(\varphi^* \omega) = e_P v_Q(\omega) + e_P - 1$$

Proof. Write $\omega = u\pi_Q^n d\pi_Q$, where $u \in \mathcal{O}_{V,P}^\times$. $\varphi^*(u)$ is a unit, so we can ignore it. By definition of e_P, we have that $\varphi^*(\pi_Q) = v \cdot \pi_P^{e_P}$, where v is a unit. Finally, we have that

$$\varphi^*(d\pi_Q) = d\big(\varphi^*(\pi_Q)\big) = v e_P \pi_P^{e_P - 1} d\pi_P$$

where the first equality comes from the definition of the pullback. □

Theorem 8.12. Let $\varphi : V \to W$ be a morphism of curves, then

$$2g(V) - 2 = \deg(\varphi)(2g(W) - 2) + \sum_{p \in V} (e_P - 1)$$

Proof. Let $\omega \in \Omega_W$ be a nonzero differential. Then

$$\begin{aligned}
2g(V) - 2 &= \deg(\mathrm{div}(\varphi^*(\omega))) \quad \text{by Riemann-Roch} \\
&= \sum_{P \in V} v_P(\varphi^*(\omega)) \quad \text{by definition} \\
&= \sum_{Q \in W} \sum_{P \in \varphi^{-1}(Q)} v_P(\varphi^* \omega) \\
&= \sum_{Q \in W} \sim_{P \in \varphi^{-1}(Q)} (e_P v_Q(\omega) + e_P - 1) \quad \text{by lemma} \\
&= \sum_{Q \in W} \left(\deg(\varphi) v_Q(\omega) + \sum_{P \in \varphi^{-1}(Q)} (e_P - 1) \right) \\
&= \deg(\varphi) \deg(\mathrm{div}(\omega)) + \sum_{P \in V} (e_P - 1) \\
&= \deg(\varphi)(2g(W) - 2) + \sum_{P \in V} (e_P - 1)
\end{aligned}$$

□

8.3 Morphisms associated to divisors

Definition 8.13 (morphism associated to a divisor)

Let V be a curve with $\ell(D) = n + 1 \geq 2$. Let $B = \{f_0, \ldots, f_n\}$ be a basis for $L(D)$. Then the morphism associated to D with respect to B is

$$\varphi_D : (f_0 : f_1 : \cdots : f_n) : V \to \mathbb{P}^n$$

We say that φ_D is an embedding if it is an isomorphism onto its image.

Notation 8.14. We say that a divisor D satisfies property $(\bigstar)$[a] if for every $P, Q \in V$, $\ell(D - P - Q) = \ell(D) - 2$.

[a] Dhruv did not name this

Theorem 8.15. The morphism φ_D associated to D is an embedding if and only if $(\bigstar)$ holds.

Proof. Omitted. □

Corollary 8.16. Suppose D is a divisor of degree $> 2g$. Then φ_D is an embedding.

Proof. By Riemann-Roch, D satisfies $(\bigstar)$. □

Corollary 8.17. Every curve of genus g can be embedded into $\mathbb{P}^m$ for some m depending only on g.

Proof. Let $m = \ell(2K_V)$ for $g \geq 3$ and $m = \ell(3K_V)$ for $g = 2$. □

Definition 8.18 (hyperelliptic curve)
A curve of genus $g > 1$ is hyperelliptic if there exists a degree 2 morphism $V \to \mathbb{P}^1$.

Theorem 8.19. A curve of genus $g \geq 2$ is hyperelliptic if and only if there exists a divisor D of V such that $\deg(D) = \ell(D) = 2$.

Proof. Omitted. □

Theorem 8.20. Suppose V is not hyperellipic. Then $\varphi_{K_V} : V \to \mathbb{P}^{g-1}$ is an embedding.

Proof. Suppose φ_{K_V} was not an embedding. Then K_V does not satisfy $(\bigstar)$. So there exists $P, Q \in V$ such that $\ell(K_V - P - Q) \geq g - 1$. But by Riemann-Roch, $\ell(P + Q) \geq 2$. □