Eight Weeks of Algebraic Geometry

Dhruv Ranganathan[1]

These are a rough set of lecture notes for Part II Algebraic Geometry from Lent 2022, based on my handwritten notes from Lent 2020 and earlier notes from Tony Scholl.

Contents

1 Affine space and affine varieties **5**

2 An interlude: the two topologies on a variety **8**

3 Ideals from zero sets **9**

4 Maps between affine varieties **12**

5 Projective space **15**

6 Projective varieties **16**

7 Function theory on projective varieties **21**

8 Rational maps between projective varieties **23**

9 Singularities and tangent spaces **27**

10 Examples of theorems in algebraic geometry **32**

11 Geometry from the function field **33**

12 Hilbert's Nullstellensatz **35**

13 Algebraic curves and their local structure **36**

14 Maps between curves **39**

15 Divisors theory on curves **43**

16 Differentials on curves **46**

17 Differentials on plane curves **50**

18 The Riemann–Roch theorem and consequences **52**

[1]Comments and corrections to dr508@cam.ac.uk. Praise and presents to a.j.scholl@dpmms.cam.ac.uk

19 Equations for curves via Riemann–Roch **56**

Introduction

Algebraic geometry is a story about a duality:

$$\boxed{\{\text{Systems of Polynomial Equations}\} \leftrightarrow \{\text{Geometry of their Solution Sets}\}}$$

If we are given a polynomial system, we can form:

$$V = \{f_1 = \ldots = f_r = 0\},$$

with coefficients in a field k, and we obtain a subset $V \subset k^n$. A solution set of this form is called an affine algebraic variety. An algebraic variety will be a class of objects that locally look like such subsets. These include many familiar objects from elementary geometry. We also obtain an ideal

$$I := (f_1, \cdots, f_r) \subset k[X_1, \ldots X_n].$$

in the polynomial ring. The duality central to the subject is about the geometry of V and the algebra of the ring $k[\underline{X}]/I$.

A word about the field k.

(i) The vast majority of the results in this course are only true when k is an algebraically closed field. Modifications when k is not closed exist, but will take us too far afield.

(ii) A smaller subset of results in the course depend on k having characteristic zero, for example $\mathbb{C}$ or $\overline{\mathbb{Q}}$. By deep results in logic, if one fixes the cardinality of a field and the characteristic, there is only one field, so these are basically the only two examples.

(iii) Throughout these lectures, I will assume something stronger, namely that k is $\mathbb{C}$. The reason for this is to occasionally, though certainly not exclusively, use the ordinary Euclidean metric on $\mathbb{C}$ as a tool to study the geometric objects that will arise.

In comparison with standard courses, (ii) is a standard assumption but (iii) is slightly strong. In particular, your textbooks and other references will not assume this.

With this assumption, our duality is now between:

$$\boxed{R := \mathbb{C}[X_1, \ldots, X_n]/I \leftrightarrow V \subset \mathbb{C}^n.}$$

Our duality suggests basic questions that we will try to understand in this course:

(i) Is it possible to recover R directly from V?

(ii) Can we detect when V is a manifold, i.e. every point p in V has a Euclidean neighborhood in V homeomorphic to a ball, based only on the ring theory of R?

(iii) What is the right notion of *dimension* for sets such as V and what property of R does it reflect?

(iv) Is V compact as a topological space? The answer will depend on the topology, and we will discuss the different choices of topology. In the subspace topology of $\mathbb{C}^n$, with the usual metric, V will usually not be compact. One can ask: is it possible to find natural compactifications $\overline{V}$ such that $\overline{V}$ is locally an affine algebraic variety?

I'll give away the punchlines.

(i) The set V does not determine R but it gets close; this is known as Hilbert's Nullstellensatz.

(ii) It is possible to detect whether V is a manifold, and there is always a dense subset $U \subset V$ such that U is a manifold.

(iii) The dimension of V can be accessed via tangent spaces, a clever topology called the Zariski topology, or via Galois theory. The approaches will turn out to be equivalent.

(iv) We will produce compact topological spaces by using projective space and its geometry.

This should already give you a sense of what makes the subject both challenging and rewarding. We will steal ideas from topology, manifold theory, complex analysis, Galois theory, and most fundamentally, the theory of rings. However, will only ever use the simplest parts of these: nothing like a Cantor set or topolgists' sine curve will show up, the complex analysis will have no essential singularities or exponential functions but only polynomials, etc.

Algebraic geometry is full of rich examples. One of the primary motivations to study algebraic varieties is that it is a source of topological spaces, including interesting manifolds, that one can study. For examples:

(i) "Smooth" varieties of dimension 1 are all Riemann surfaces which connects algebraic geometry to complex analysis,

(ii) The geometry of surfaces inside 3-space are a classical object of study, just like surfaces in $\mathbb{R}^3$. However, everything will be complex and the 3-space will be a slightly more complicated object called $\mathbb{P}^3$.

(iii) The standard matrix groups, such as $GL(n, \mathbb{C})$, are naturally algebraic varieties, and are a rich source of examples.

These are among many other examples.

Learning Algebraic Geometry The subject is often considered challenging, but this is due to the interweaving nature of the mathematics above; it is likely the first time you will have encountered a situation where ideas from so many different areas have to be used in parallel. But it has pretty much always been challenging for everyone that ever learned it. It will be a course where I will need to state theorems that we will need to use but cannot prove; we will often rely on intuition based on topological ideas to try algebraic arguments; and geometry always requires a certain amount of leap before you learn. But the mathematics we are accessing has stood the test of time, and I genuinely believe it is worth the climb!

1 Affine space and affine varieties

Any algebraically closed field will work in what follows, but as noted above, we will always work over $\mathbb{C}$.

Definition 1.1. Affine n-space over $\mathbb{C}$ is the set

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

Its elements will be referred to as points and denoted by $P = (\underline{a}) = (a_1, \ldots, a_n)$. An affine subspace of $\mathbb{A}^n$: any subset of the form $v + U$, $v \in k^n$, $U \subset k^n$ a vector subspace.

The space $\mathbb{A}^n$ is the set on which $\mathbb{C}[X_1, \ldots, X_n]$ is naturally a ring of functions. I will often use the shorthand $\mathbb{C}[\underline{X}] = \mathbb{C}[X_1, \ldots, X_n]$ when the number n is clear. Given an element f in $\mathbb{C}[\underline{X}]$, we obtain a function:

$$\mathbb{A}^n \to \mathbb{C}.$$

The subset $\mathbb{C} \subset \mathbb{C}[\underline{X}]$ are referred to as the constant functions. We will be interested in the vanishing locus or zero set of functions of this form. It will be useful to have some basic facts about the ring at hand.

Proposition 1.2. *The polynomial ring satisifes the following properties.*

(i) The ring $\mathbb{C}[\underline{X}]$ is a unique factorization domain.

(ii) Every ideal $I \subset \mathbb{C}[\underline{X}]$ is finitely generated.

Remarks on the Proposition. The proof of the first statement is essentially identical to the proof of Gauss's Lemma.[2]. The second statement is called the Noetherian property of a ring. In fact, every module over the polynomial ring is also finitely generated. Moreover, if R is any quotient of the polynomial ring by an ideal, and J is an ideal in R, then J is also finitely generated.

We come to the main objects of interest.

Definition 1.3. Let $S \subset \mathbb{C}[\underline{X}]$ be any subset. The vanishing locus of S is given by

$$\mathbb{V}(S) = \{P \in \mathbb{A}^n \mid \forall f \in S,\ f(P) = 0\}$$

An affine variety or affine algebraic subset of $\mathbb{A}^n$ is any set of the form $\mathbb{V}(S)$, for some S as above.

Warning. The definition of variety and affine variety are *not* consistent in the literature. Several authors impose a further condition called *irreducibility*, which we will encounter shortly. There are good reasons for both conventions, but the main point is simply to be wary when you read textbooks.

Example 1.4. *Let us record numerous examples of algebraic varieties.*

(i) If $n = 1$ and $f \in \mathbb{C}[X]$ is nonzero, then $\mathbb{V}(f) = \{$zeros of $f\}$, a finite subset of $\mathbb{A}^1$. Conversely, if $V \subset \mathbb{A}^1$ is finite then $V = \mathbb{V}(f)$ with

$$f = \prod_{a \in V} (X - a).$$

Observe that several polynomials can have the same vanishing set; for example $(X - a)$ and $(X - a)^2$ vanish on the same subset. This will be important shortly.

[2] A well-written explanation of both may be found here `http://math.stanford.edu/~conrad/121Page/handouts/gausslemma.pdf`

(ii) A hypersurface is a variety of the form $\mathbb{V}(f) \subset \mathbb{A}^n$ where f is any non-constant polynomial. These encompass a large class of examples within them. if $V \subset \mathbb{A}^n$ is an affine subspace of dimension $n-1$, namely it is a translate of a linear subspace of dimension $n-1$, then by linear algebra it is a hypersurface.

(iii) It is often convenient to describe varieties parametrically. The affine twisted cubic is given by

$$C = \{(t, t^2, t^3) : t \in \mathbb{C}\} \subset \mathbb{A}^3.$$

It is the vanishing set

$$\{X_1 - X_2^2 = X_1 - X_3^3 = 0\} \subset \mathbb{A}^3.$$

(iv) As we will shortly see, a finite union of algebraic varieties is an algebraic variety. For example, in $\mathbb{A}^3$, take V to be the union of the three axes:

$$V = \{X_0 = X_1 = 0\} \cup \{X_1 = X_2 = 0\} \cup \{X_0 = X_2 = 0\}.$$

Find an explicit set of polynomials S such that $\mathbb{V}(S)$ is equal to V. This is called the spatial triple point.

(v) Consider the polynomial

$$f(\underline{X}) = X_1^2 + \cdots + X_{n+1}^2,$$

and consider the function

$$f : \mathbb{A}^{n+1} \to \mathbb{C}.$$

The level sets of this functions are all varieties. The vanishing locus of f, i.e. the preimage of 0, is called the ordinary double point. Although it may not seem believable right now, this is one of the richest and most informative examples in all of geometry!

Visualizing Algebraic Varieties. I have told you that we will assume the field over which we work is always algebraically closed, and in fact, I will always assume it is $\mathbb{C}$. Nevertheless, significant – but dangerous! – intuition is gained from looking at the pictures over $\mathbb{R}$. In order to help visualize varieties, I often use a computer or WolframAlpha. When n is 2 draw the real locus of the ordinary double point. Using a computer system, graph the affine twisted cubic.

Let us begin to explore how the ring theory interacts with these varieties.

Theorem 1.5. *Let V be the affine variety given by $\mathbb{V}(S)$ where S is any subset of the ring $\mathbb{C}[\underline{X}]$.*

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

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

Proof. For the statement (i), suppose $P \in \mathbb{A}^n$. Then then $f(P) = 0$ for all $f \in S$ and only if $f(P) = 0$ for all $f \in I$ by basic properties of ideals.

For the statement (ii), we already have the equality

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

by (i). We now apply the Hilbert basis theorem, and find $\{h_1, \ldots, h_r\}$ generators for I. The generators may not lie in S, but we can find a finite subset $\{f_1, \ldots, f_m\} \subset S$ and $g_{ij} \in k[\underline{X}]$ such that

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

. Therefore $\{f_j\}$ are also a set of generators for I, so $\mathbb{V}(S) = \mathbb{V}(\{f_j\})$ as demanded. □

A fundamental property about the relationship between the ideal I and its vanishing locus is that it is "order reversing": roughly speaking, as the ideal gets larger, the set of points where *all its functions* vanish gets smaller. These properties are formally spelled out in the next proposition.

Proposition 1.6. *Let S and T be subset of the polynomial ring $\mathbb{C}[\underline{X}]$. Then*

(i) If $S \subset T$ then $\mathbb{V}(T) \subset \mathbb{V}(S)$.

(ii) There is an equality $\mathbb{V}(0) = \mathbb{A}^n$; and $\mathbb{V}(\mathbb{C}[\underline{X}]) = \emptyset = \mathbb{V}(\lambda)$ for any non-zero λ in $\mathbb{C}$.

(iii) There is an equality $\bigcap_j \mathbb{V}(I_j) = \mathbb{V}(\sum_j I_j)$ for any family of ideals I_j.

(iv) There is an equality $\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cap J)$

Proof. The first two statements are trivial. For the statement (iii) we have $\bigcap \mathbb{V}(I_j) = \mathbb{V}(\bigcup I_j)$ by definition. To conclude, apply Theorem 1.1(i) above. For the statement (iv), we have already observed that

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

For the reverse containment, suppose P lies in $\mathbb{V}(I \cap J)$, and suppose $P \notin \mathbb{V}(I)$. Then there exists $g \in I$ with $g(P) \neq 0$. Moreover, for all elements $f \in J$, the product $fg \in I \cap J$ so $(fg)(P) = 0$. Therefore $f(P) = 0$ or in other words, $P \in \mathbb{V}(J)$. □

As a consequence, some varieties are unions of other varieties. It is useful to identify the "atomic" pieces of a variety.

Definition 1.7. A variety V is called <u>irreducible</u> if for every expression of V as a union

$$V = V_1 \cup V_2$$

either V_1 or V_2 is equal to V. A variety is <u>reducible</u> if it is not irreducible.

Example 1.8. *The variety $\mathbb{V}(X_1X_2) = 0 \subset \mathbb{A}^2$ is reducible as it is the union of two varieties, namely the set where $X_1 = 0$ and the set where $X_2 = 0$.*

On the other hand, showing that a variety is *irreducible* seems somewhat more difficult. We will come to this quite soon, but before that, let us justify why this is the right notion of "atomic".

Proposition 1.9. *Every affine variety V is a finite union of irreducible varieties.*

Proof. The proof technique is sometimes referred to as a "bisection" argument. If V is irreducible there is nothing to prove. If V is not irreducible, we can nontrivially write $V = V_1 \cup V_1'$. If both of V_1, V_1' are finite unions of irreducible varieties then again, there is nothing. It follows that V_1 can be written nontrivially as a union $V_2 \cup V_2'$. Continuing in this fashion, we are left with a chain

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

This infinite descending chain supposedly never stabilizes. However, the chain of varieties gives rise to an infinite ascending chain of ideals. Precisely, define

$$W = \bigcap_j V_j = V\left(\sum I_j\right).$$

The ideal $\sum I_j$ is finitely generated since the polynomial ring is Noetherian. It follows that $I = \sum_{j \leq N} I_j$ for some sufficiently large N, since the chain of ideals stabilizes. As a consequence, $W = \bigcap_{j \leq N} V_j$ and by a little basic set theory we see that chain terminates. □

In fact, the decomposition into irreducible pieces is essentially unique.

Proposition 1.10. *Let V be a variety. A minimal*[3] *decomposition $V = \cup V_i$ into a finite union of distinct irreducible varieties is unique up to ordering.*

Minimal here has the meaning that if $V = \cup V_i$ is a decomposition, no V_i should be contained in V_j for i not equal to j.

Proof. The proof is left as an exercise. The basic idea is to compare two decompositions by the following trick: take an irreducible component in the first decomposition and intersect it with each piece of the second decomposition. By using the irreducibility of this chosen component, one is quickly led to the conclusion of the proposition. □

Given this uniqueness, we can refer to the irreducible subvarieties V_i that occur in a decomposition of V as the irreducible components of V.

2 An interlude: the two topologies on a variety

The arguments of the previous section, especially involving intersections, unions, and irreducibility have a distinctly *topological* feel to them. It is convenient to formalize it.

We recall that a topology on a set X is a collection of subsets of X – "the topology" – which are declared to be open sets. The collection should not be arbitrary: (i) the empty set and X itself should be open; (ii) arbitrary unions of opens should be open; and (iii) finite intersections of opens should be open. By declaring a closed set to be the complement of an open set, one can equivalently specify a topology by describing its closed sets.

Definition 2.1. The Zariski topology on $\mathbb{A}^n$ is the topology whose closed sets are affine varieties in $\mathbb{A}^n$. If $V \subset \mathbb{A}^n$ is an affine variety, the Zariski topology on V is defined as the subspace topology for the Zariski topology on $\mathbb{A}^b$.

Proposition 1.6 shows that this is indeed a topology. Since we are working over $\mathbb{C}$, we have another option.

Definition 2.2. The Euclidean topology or analytic topology on $\mathbb{A}^n$ is the topology induced by the identification of $\mathbb{A}^n$ with $\mathbb{C}^n$, where the latter is given the metric topology for the standard metric on $\mathbb{C}^n$. If $V \subset \mathbb{A}^n$ the Euclidean topology on V is defined as the subspace topology for the Euclidean topology on $\mathbb{A}^n$.

Let us make a few basic observations to get a sense for how different these two topologies are.

Proposition 2.3. *The Zariski topology on $\mathbb{A}^1$ coincides with the cofinite topology. Affine space $\mathbb{A}^1$ is not Hausdorff in the Zariski topology, and non-compact in the Euclidean topology. Note that $\mathbb{A}^1$ is Hausdorff in the Euclidean topology; in the Zariski topology $\mathbb{A}^1$ every open cover of $\mathbb{A}^1$ has a finite subcover*[4].

The following statements hold for any affine variety $V \subset \mathbb{A}^n$.

(i) Every Zariski closed subset of V is Euclidean closed; the converse does not hold.

[3] The minimality condition was incorrectly dropped in lecture.

[4] We are being cagey here because the literature is inconsistent about what compact actually means: several authors include Hausdorff in the definition of compact, and instead use the term quasi-compact for general spaces having the finite subcover property.

(ii) Every Zariski open[5] *dense subset is dense in the Euclidean topology.*

(iii) A polynomial function f gives rise to a map

$$f : V \to \mathbb{A}^1.$$

The map is continuous in both Zariski and Euclidean topologies[6].

Proofs are not included, as these are statements to tune your intuition. The proofs may be considered non-examinable.

The topologies are both very useful: the Euclidean topology is where geometric intuition comes from, including all the pictures that algebraic geometers draw. The Zariski topology is a useful way to import general results from topology.

Important Warning Although set theoretically we can identify $\mathbb{A}^2$ and $\mathbb{A}^1 \times \mathbb{A}^1$, the Zariski topology on $\mathbb{A}^2$ is *not* the product topology for the Zariski topology on $\mathbb{A}^1$. For example, the set $\mathbb{V}(X_1 - X_2) \subset \mathbb{A}^2$ is Zariski closed, but not closed in the product Zariski topology.

3 Ideals from zero sets

In the discussion so far, varieties have been built from ideals in the polynomial ring. We now discuss the converse: how can we recover an ideal from only the data of an algebraic variety? The simplest version of this question considers the simplest variety, namely the empty set. We therefore must understand, what ideals I have the property that their vanishing set is *empty.*

Theorem 3.1 (Hilbert's Weak Nullstellensatz)**.** *Let $I \subsetneq \mathbb{C}[\underline{X}]$ be a proper ideal. Then the vanishing locus $\mathbb{V}(I)$ is nonempty.*

In particular, the only ideal that could possibly give rise to the empty set as a variety is the unit ideal. More generally, we want to understand, given two ideals I, J in $\mathbb{C}[\underline{X}]$, if

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

what can be said about the relationship between I and J? Note that the answer cannot be entirely straightforward: if $I = (f)$ and $J = (f^2)$, then their vanishing loci certainly coincide.

Let $V \subset \mathbb{A}^n$ be an affine variety. Consider the ideal

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

Proposition 3.2. *Let $V \subset \mathbb{A}^n$ be a variety as above.*

(i) If $V = \mathbb{V}(S)$ for some set $S \subset \mathbb{C}[\underline{X}]$, then $S \subset I(V)$. In particular, $I(V)$ is the largest ideal of functions that vanish on V.

(ii) There is an equality $V = \mathbb{V}(I(V))$.

(iii) Two varieties V and W are equal if and only if the ideal $I(V)$ and $I(W)$ are equal.

Proof. The statements follow immediately from the definitions. □

[5] The world open was dropped in lecture. The statement is false without this hypotheses. A counterexample is an infinite collection of points in $\mathbb{A}^1$, which is automatically Zariski dense.

[6] Precisely, place one of the two topologies on both source and target of f; for fun you can try to think about what happens when you mix and match different topologies on source and target, but there's not much to gain from this.

As a consequence, we obtain an injective map:

$$\boxed{\{\text{Affine varieties in } \mathbb{A}^n\} \hookrightarrow \{\text{Ideals in } \mathbb{C}[\underline{X}]\}}$$

obtained by sending V to $I(V)$. Since the $\mathbb{V}(-)$ construction is a left inverse by the proposition above, the map is injective.

The injection behaves well with respect to inclusions.

Proposition 3.3. *The containment $V \subset W$ holds if and only if $I(V) \supset I(W)$.*

Proof. The forward implication is obvious. If V is not contained in W we can choose P in $V \setminus W$. Since P is not in $\mathbb{V}(I(W))$, there exists f in $I(W)$ such that $f(P)$ is nonzero. In other words, f is not contained in $I(V)$. □

The injection also detects irreducibility.

Proposition 3.4. *A variety $V \subset \mathbb{A}^n$ is irreducible if and only if $I(V)$ is a prime ideal.*

Proof. We have seen that $I(V_1 \cup V_2) = I(V_1) \cap I(V_2)$. Now suppose that V were reducible and we write $V = V_1 \cup V_2$, as a nontrivial union. In particular,

$$V_1 \not\subset V_2 \not\subset V_1.$$

Let I_j be the ideal $I(V_j)$. Then $I(V) = I_1 \cap I_2$ and by the previous proposition, $I_1 \not\subset I_2 \not\subset I_1$. We can therefore find

$$f_1 \in I_1 \setminus I_2, \quad f_2 \in I_2 \setminus I_1.$$

Then $f_i \notin I(V)$ but

$$f_1 f_2 \in I_1 \cap I_2 = I(V),$$

so $I(V)$ not prime.

Conversely, suppose $f_1 f_2 \in I(V)$ with neither f_1 nor f_2 contained in $I(V)$. Then we define

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

Since f_i is not contained in $I(V)$, $V_i \neq V$. Then

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

hence $V = V_1 \cup V_2$. □

Given a function $f \in \mathbb{C}[\underline{X}]$, we can restrict the resulting function, initially defining

$$\mathbb{A}^n \to \mathbb{A}^1$$

to a variety $V \subset \mathbb{A}^n$. However, two functions f and g restrict to the same function on V if $f - g$ vanishes on V, i.e. if $f - g$ is contained in $I(V)$.

Definition 3.5. The coordinate ring or the ring of regular functions of V is defined as the quotient $\mathbb{C}[\underline{X}]/I(V)$. It is denoted $\mathcal{O}(V)$ or $\mathbb{C}[V]$.

The notation $\mathbb{C}[V]$ is more common when discussing the traditional theory of varieties, but it leads to a peculiar notational confusion if we were to use X to denote a variety.

Remark 3.6. Let $V \subset \mathbb{A}^n$ be a variety, fix a point P on it, and choose an element f in $\mathbb{C}[\underline{X}]$. There is a nice interpretation of the value of the function value $f(P)$. The point P can be written as $(\underline{a})$ and there is an associated ideal

$$\mathfrak{m}_P = \langle X_1 - a_1, \dots, X_n - a_n \rangle \subset \mathbb{C}[\underline{X}].$$

There is a quotient

$$\mathbb{C}[\underline{X}] \to \mathbb{C}[\underline{X}]/\mathfrak{m}_P = \mathbb{C}.$$

The elements f lies in the domain. The function value $f(P)$ is precisely the image of f in this quotient; indeed, in practice, the quotient means "plug in a_i for each X_i". Note that $\mathfrak{m}_P$ contains $I(V)$ so in fact, by the correspondence theorem in ring theory $\mathfrak{m}_P$ also determines an ideal in the coordinate ring $\mathbb{C}[V]$.

We can translate the link between primality and irreducibility into the language of coordinate rings.

Corollary 3.7. *A variety $V \subset \mathbb{A}^n$ irreducible iff $\mathbb{C}[V]$ is an integral domain.*

Remark 3.8. The ring $\mathbb{C}[V]$ does not remember the ideal $I(V)$ exactly. In order to recover $I(V)$ we also need the *quotient homomorphism*

$$\mathbb{C}[\underline{X}] \to \mathbb{C}[V].$$

We can recover $I(V)$ as the kernel. However, a given ring $\mathbb{C}[V]$ can be presented as a quotient in many different ways. For example, the ring $\mathbb{C}[X]$ can be presented as $\mathbb{C}[X,Y]/(Y)$. As you might imagine, it is essentially harmless to forget this data. In fact, this extra information is often more of a hindrance than anything else.

The weak form of the Nullstellensatz tells us that there is some chance that the variety $\mathbb{V}(I)$ contains a lot of information about I, in particular, it distinguishes I from the unit. The strong Nullstellensatz goes a step further.

Definition 3.9. Let $I \subset \mathbb{C}[X_1, \dots, X_n]$. Define the radical of I by

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

It is easy to see that this is also an ideal. An immediate observation is that for any ideal I

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

The strong form of the Nullstellensatz states that this is the only ambiguity.

Theorem 3.10 (Hilbert's Strong Nullstellensatz)**.** *Let $I \subset \mathbb{C}[\underline{X}]$ and let $V = \mathbb{V}(I)$. Then f lies in $I(V)$ if and only if f is contained in $\sqrt{I}$. That is,*

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

Corollary 3.11. *If ideals I and J have the same zero set then their radicals coincide.*

Remark 3.12. If I is not equal to its radical, then the quotient $R = \mathbb{C}[\underline{X}]/I$ contains nilpotent elements, i.e. nonzero elements r such that r^m is zero. From a function theory viewpoint this poses some intuitive confusion: at any point P of V, we have $f(P)^m = 0$. But $f(P)$ is an element in $\mathbb{C}$ so these functions take value zero everywhere, but they are not the zero functions. This is the reason we pass to the radical ideal before taking the quotient: we want[7] $\mathbb{C}[\underline{X}]/I$ to be a "ring of functions on V".

[7] In the interest of honesty, this is a pretty old fashioned viewpoint. Modern algebraic geometry takes these nipotents very seriously. But there is a huge technical burden in absorbing them into a geometric setup, called "scheme theory": the subject of the Part III course on this subject.

4 Maps between affine varieties

Let $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$. We want to understand an appropriate class of maps from V to W. There are two ways to look at this, both of which lead to the same conclusion. (i) Maps to W should be built out of functions on V, and therefore given by an m-tuple of elements in the coordinate ring of V that lands V inside W. (ii) Maps to W should be set theoretic maps from V to W that have the property that any polynomial on W induces a polynomial on V by precomposition (or "pullback").

Definition 4.1. A regular map or morphism from V to W is a map

$$\varphi : V \to W$$

such that there exist elements $f_1, \dots, f_m$ in $\mathbb{C}[V]$ such that

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

for all points P in V. The set of morphisms from V to W are denoted $\mathrm{Mor}(V, W)$.

Notice that a morphism is therefore just a set theoretic map from V to W that happens to arise in a nice way via polynomials. It is exactly paralle to how a variety is a set theoretic object that happens to arise in a nice way via polynomials. The key example to keep in mind is that the set of morphisms from V to $\mathbb{A}^1$ is precisely the coordinate ring $\mathbb{C}[V]$. We give some further examples of the kind of morphisms that arise in practice.

Example 4.2. *(i) A linear projection $\mathbb{A}^n \to \mathbb{A}^m$ is a morphism, as is any linear or affine transformation.*

(ii) If $V \subset W \subset \mathbb{A}^n$ are two affine varieties, the inclusion

$$V \hookrightarrow W$$

is a morphism.

(iii) The affine d-Veronese from $\mathbb{A}^1$ is the morphism $\mathbb{A}^1 \to \mathbb{A}^d$ given by

$$t \mapsto (t, t^2, \dots, t^d).$$

Proposition 4.3. *If $\varphi : V \to W$ is a morphism and $\psi : W \to Z$ is a morphism, then the composite map $V \to Z$ is also a morphism.*

Proof. Composition of polynomial functions is polynomial. □

Given this, we see that an isomorphism is a morphism with a 2-sided inverse.

The data of a morphism is in fact, purely ring theory data. If g is an element of $\mathbb{C}[W]$, and $\varphi \colon V \to W$ is any morphism, define the pullback $\varphi^* g = g \circ \varphi$ which is an element of $\mathbb{C}[V]$. It is straightforward to see that

$$\varphi^\star : \mathbb{C}[W] \to \mathbb{C}[V]$$

is a ring homomorphism that restricts to the identity on $\mathbb{C}$. This is called a $\mathbb{C}$-algebra homomorphism.

Theorem 4.4. *$V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$. Then $\varphi \mapsto \varphi^*$ defines a bijection*

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

Proof. Let $x_1, \dots x_n$ be the coordinate functions on V, namely the restrictions of the standard linear coordinate functions on $\mathbb{A}^n$. Similarly, let $y_1, \dots, y_m$ be the coordinate functions on W.

We first show injectivity of the association above. What has to be shown is that if we are given two set theoretic maps from V to W that happen to be morphisms, and if the corresponding algebra maps coincide, the set theoretic maps coincide. Suppose P lies on V. Then $\varphi(P)$ can be expressed as a tuple

$$\varphi(P) = (y_1(\varphi(P), \dots, y_m(\varphi(P)) = (\varphi^\star y_1(P), \dots, \varphi^\star y_m(P)).$$

Therefore, given two morphisms φ and ψ, if the corresponding algebra maps $\varphi^\star$ and $\psi^\star$ are equal, then $\varphi(P)$ and $\psi(P)$ are equal for all P in V.

We now prove surjectivity. Let $\lambda\colon \mathbb{C}[W] \to \mathbb{C}[V]$ be homomorphism. Each coordinate function y_i determines an element of $\mathbb{C}[V]$ via:

$$f_j = \lambda(y_j).$$

Assemble these together to get

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

We must now show that the image of V is contained in W, i.e. every polynomial in $I(W)$ vanishes on $\varphi(P)$ for all points P in W. Let g be a polynomial with m input variables. Since λ is a homomorphism we see that

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

It follows by plugging in at P, that if the polynomial g is contained in $I(W)$, then $g(f_1(P), \dots, f_m(P))$ vanishes. Equivalently, the point $\varphi(P)$ lies inside W. It is straightforward to check that λ coincides with $\varphi^\star$, so we obtain the required surjectivity. □

This gives us a way to quickly determine if there is an isomorphism between two varieties. For example, we see that the affine twisted cubic from earlier, the image

$$C = \{(t, t^2, t^3) : t \in \mathbb{C}\} \subset \mathbb{A}^3$$

is isomorphic as a variety to $\mathbb{A}^1$ by explicitly calculating the coordinate rings.

Here is a harder example that exhibits something very important.

Example 4.5. *Let V be the variety obtained by the union of three lines through the origin in $\mathbb{A}^2$: for concreteness, take them to be the two axes and the diagonal. Let W be the variety obtained by the union of the three axes in $\mathbb{A}^3$. In the Euclidean topology, these two varieties are homeomorphic. However, they are not isomorphic as affine varieties, because their coordinate rings are not isomorphic! This is the first sign that things are less flexible in algebraic geometry. There are a few ways to show this, but it will be easier once we introduce tangent spaces in a few lectures time.*

In various aspects of geometry and topology, we are often interested in functions that are only defined on some open set, but that may be undefined outside of that set. A typical example is the function $\frac{1}{z}$ in one complex variable, but "is infinite" at 0.

Definition 4.6. Let $V \subset \mathbb{A}^n$ be an irreducible affine variety. Its function field or field of rational functions or field of meromorphic functions is the fraction field

$$\mathbb{C}(V) := FF(\mathbb{C}[V]).$$

Its elements will be called rational functions or meromorphic functions. Let φ be a rational function. A point P of V is called regular if φ can be expressed as a ratio f/g with $g(P)$ nonzero.

A couple of notes about the notation and terminology. First, the notation is once again slightly dangerous when the variety is denoted X. Second, the word meromorphic here is used only in analogy. There may be more meromorphic functions in the sense of complex analysis, but it evokes the right intuition.

If a rational function φ can be expressed as f/g, then there is a partially defined function on the (open!) complement of $\mathbb{V}(g)$:

$$\varphi : V \setminus \mathbb{V}(g) \to \mathbb{C}.$$

It is useful to keep in mind that if V is irreducible, then every nonempty open subset is actually dense in the Zariski topology.

Example 4.7. *In $\mathbb{A}^1$, consider the rational function X_1^2/X_2. This is a function on the complement of the X_1-axis.*

Remark 4.8. Informally, we think of rational functions as being pairs (f, U) where f is a function and U is a nonempty open set in V subject to an equivalence relation. The equivalence relation states that two pairs (f, U) and (f', U') are the same if the functions agree on some smaller non-empty open set contained in both. In pithy terms: "functions defined on some open set".

Definition 4.9. Let V be an irreducible affine variety. The local ring at point P in V is

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

It is clear that this is a ring, but it is a very simple type of ring known as a local ring. A local ring is one that has a unique maximal ideal.

Proposition 4.10. *Let V and P be as above. The ring $\mathcal{O}_{V,P}$ has a unique maximal ideal given by*

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

Furthermore, the invertible elements in $\mathcal{O}_{V,P}$ are precisely those elements f such that $f(P)$ is nonzero.

The proof follows from the following lemma.

Lemma 4.11. *A ring R is a local ring if and only if $R \setminus R^*$ is an ideal. If so then $R \setminus R^*$ is the maximal ideal of R.*

Proof. Recall that in any ring, if $A \subset R$ is an ideal, then then A is a proper ideal if and only if A contains no units. Now suppose $\mathfrak{m} = R \setminus R^*$ is an ideal. By the previous sentence it is a maximal ideal and contains every proper ideal of R. It is therefore the unique maximal ideal of R.

Conversely, let $(R, \mathfrak{m})$ be a local ring. Then $\mathfrak{m} \subset R \setminus R^*$, and if $x \in R \setminus R^*$ then $(x) \neq R$ so $(x) \subset \mathfrak{m}$ by uniqueness. Therefore $\mathfrak{m} = R \setminus R^*$. We conclude. □

4.12 A quick review of the affine variety package

We have built a "local" geometric object with a good function theory. Our next task will be to build a "global" object. Exactly what is local and what is global only becomes clear with a bit of experience, but the manifold analogy is useful: locally we do linear algebra, and globally we have manifolds.

An affine variety $V \subset \mathbb{A}^n$ has a naturally associated ring of functions $\mathbb{C}[V]$. In fact, assuming V is irreducible, if we fix any open subset $U \subset V$ we have a larger ring R_U:

$$\mathbb{C}[V] \subset R_U \subset \mathbb{C}(V)$$

consisting of all the rational functions on V that are regular at all points of U. If $U \subset U'$ are open, then the functions in $R_{U'}$ can be restricted to R_U. This is good and should feel "geometric".[8] is a good sign for what we'll do next.

The next step will be to stitch together affine varieties to something larger.

5 Projective space

We will now introduce projective space $\mathbb{P}^n$, which will serve as a replacement for affine space $\mathbb{A}^n$. First, a word about why we would like this. The following are examples of statements that are true in projective geometry but fail in affine geometry.

(i) Every pair of distinct lines in $\mathbb{P}^2$ meet at a single point.

(ii) Let V be a projective variety in $\mathbb{P}^2$ defined by a polynomial of degree d. If V is a manifold, then V is an orientable surface of genus $\binom{d-1}{2}$.

(iii) More generally, Let V and V' be projective varieties in $\mathbb{P}^n$ defined by polynomials of the same degree. If V and V' are both manifolds, then V and V' are homeomorphic in the Euclidean topology.

(iv) Perhaps the most fundamental of these though: projective space in the Euclidean topology is a compact manifold, and every projective variety is a compact topological space in the Euclidean topology.

The statements about the Euclidean topology are not well-reflected in the Zariski topology, but if one also examines the ring theory side, there are versions of these facts that become visible. However, the additional sophistication required to do this honestly is significant.

We now begin in earnest, first with the set theoretic structure. Let U be a finite dimensional vector space over $\mathbb{C}$.

Definition 5.1. The projectivization of U is defined as

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

Define projective n-space to be

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

It is typical to index the coordinates on $\mathbb{C}^{n+1}$ by indices $0, \ldots, n$. A line in $\mathbb{C}^{n+1}$ is given by

$$\{(a_0t, a_1t, \ldots, a_nt) \mid t \in \mathbb{C}\}.$$

We will write $(a_0 : a_1 : \ldots : a_n)$ for corresponding element of $\mathbb{P}^n$. Thus

$$\boxed{\mathbb{P}^n = \{(a_0 : \cdots : a_n) \mid a_i \in k, \text{ not all } 0\}/\sim}.$$

where $(a_i) \sim (b_i)$ if and only if the tuples are non-zero scalar multiples of each other. In practice, the point here is that to name a point in $\mathbb{P}^n$, we must give $n+1$ complex numbers, not all zero, and be aware that there is ambiguity. The tuples $(1 : 1 : -1)$ and $(2 : 2 : -2)$ are actually the same point.

[8]This "association" can be dressed up in some fancy language. Precisely, we have attached a ring to every open set in such a way that inclusions of open sets give maps of rings. This is formalized by the notion of a sheaf and we have just defined the structure sheaf: it is precisely the data of this network of rings. We will not discuss further, despite the instructor's desire to.

A few elementary observations. We can decompose

$$\mathbb{P}^1 = \{(a_0 : a_1) \mid a_0 \neq 0\} \sqcup \{(a_0 : a_1) \mid a_0 \neq 0\} = \mathbb{A}^1 \cup \{pt\}.$$

The second equality follows because in the first set of the decomposition, we are allowed to divide out by a_0 to assume that it is equal to 1, and the only information left is $\frac{a_1}{a_0}$. As a consequence, we think of $\mathbb{P}^1$ as being $\mathbb{A}^1$ with a point at infinity. More generally, we can write

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

Inductively, we get a decomposition

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \ldots \sqcup \mathbb{A}^1 \sqcup \{pt\}.$$

We now place our two topologies on $\mathbb{P}^n$.

Definition 5.2. The Zariski (resp. Euclidean) topology on $\mathbb{P}^n$ is obtained as the quotient topology, for the subspace topology on $\mathbb{C}^{n+1} \setminus \{\underline{0}\}$, for the Zariski (resp. Euclidean) topology on $\mathbb{C}^{n+1}$.

The fact about projective space that underlies its nice properties, though we will never use it in this form, is the following. It provides important intuition.

Proposition 5.3. *Projective space $\mathbb{P}^n$ is compact for all n in the Euclidean topology.*

Proof. Notice that the unit sphere in $\mathbb{C}^{n+1}$ has a continuous surjective map onto $\mathbb{P}^n$. Since the image of a compact set is compact, the space is compact. □

Projective space $\mathbb{P}^n$ contains lots of "copies" of affine space $\mathbb{A}^n$ inside of it. There are infinitely many copies in fact, but we single out $n+1$ standard affine patches in terms of coordinates. Let

$$H_j = \{(a_i) \in \mathbb{P}^n \mid a_j = 0\}.$$

and

$$U_j = \mathbb{P}^n \setminus H_j = \{(a_i) \in \mathbb{P}^n \mid a_j \neq 0\}.$$

There is a natural set theoretic bijection:

$$(a_0 : \ldots : a_n) \mapsto (a_0/a_j, \ldots, a_{j-1}/a_j, a_{j+1}/a_j, \ldots a_n/a_j) = (a_0/a_j, \ldots, \widehat{a_j/a_j}, \ldots a_n/a_j)$$

where the hat symbol tells us to omit an entry. In the other direction

$$(b_1, \ldots, b_n) \mapsto (b_1, \ldots, b_i, 1, b_{i+1}, \ldots, b_n)$$

This reduces to the standard covering of the Riemann sphere $\mathbb{P}^1$ by two copies of $\mathbb{A}^1$. The projective plane $\mathbb{P}^2$ is often visualized as a triangle of lines in a big blob.

6 Projective varieties

If one views $\mathbb{P}^n$ as a replacement for $\mathbb{A}^n$, a projective variety should be the vanishing set of a collection of polynomial functions. However, this is delicate. The function theory of $\mathbb{P}^n$ is more subtle than it is in affine space. A polynomial in $\mathbb{C}[\underline{X}]$ is not a well-defined function. As an example, consider the polynomial $X_0 + 1$; it does not determine a function on $\mathbb{P}^1$, because the value depends on the chosen representative.

We begin by recording some basic terminology carefully.

Definition 6.1. A monomial is an element in $\mathbb{C}[\underline{X}]$ of the form $X_0^{d_0}X_1^{d_1}\cdots X_n^{d_n}$, for $d_i \geq 0$. A term is a nonzero multiple of a monomial. The degree of a term $c \cdot X_0^{d_0}X_1^{d_1}\cdots X_n^{d_n}$ is defined to be $\sum d_i$. A homogeneous polynomial is a sum of terms of degree d. It has a well-defined degree, equal to the degree of any of its constituent terms.

Every polynomial has a unique decomposition as a sum of homogeneous parts,

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

with $f_{[i]}$ homogeneous of degree i.

Lemma 6.2. *Let f be a homogeneous polynomial in $\mathbb{C}[X_0, \ldots, X_n]$. Suppose that $\underline{a} = (a_0, \ldots, a_n)$ is a tuple of complex numbers such that $f(\underline{a}) = 0$. Then*

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

for any nonzero complex numbers λ.

Proof. If f is homogeneous of degree d, then

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

The lemma is an immediate consequence. □

Corollary 6.3. *Let f be homogeneous of degree d. The set*

$$\mathbb{V}(f) = \{p \in \mathbb{P}^n : f(a) = 0, \text{ where } a \text{ is any representative of } p\} \subset \mathbb{P}^n$$

is well-defined.

In simple terms: the function value of f at a point of $\mathbb{P}^n$ is not well-defined, but the set where the function value is 0 is well-defined. The next step is to go from the vanishing of a single polynomial to the vanishing of an ideal. We need a definition.

Definition 6.4. An ideal $I \subset \mathbb{C}[\underline{X}]$ is homogeneous if it is generated by homogeneous polynomials, possibly of different degrees.

Homogeneous ideals are characterized by the following

Lemma 6.5. $I \subset \mathbb{C}[\underline{X}]$. *The following are equivalent.*

(i) The ideal I is homogeneous;

(ii) If f is any polynomial that is contained in I, then the homogeneous parts $f_{[r]}$ are contained in I for all r.

Proof. For (i) $\implies$ (ii): Let g_j be generators of I, homogeneous of degrees d_j. If

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

then we can split each h_j into homogenous pieces $h_{j[r]}$. Now we 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.

(ii) $\implies$ (i): This follows immediately from decomposing the generators of I. □

We can now confidently define the vanishing locus of a homogeneous ideal.

Definition 6.6. Let I be a homogeneous ideal. Define the vanishing locus of I to be

$$\mathbb{V}(I) = \{P = (a_i) \in \mathbb{P}^n \mid f((a_i) = 0 \ \forall f \in I\}.$$

A projective variety is a a subset $V \subset \mathbb{P}^n$ is the vanishing locus of a homogeneous ideal.

A couple of remarks on this definition. By the lemma, $\mathbb{V}(I)$ is the same if we add the condition "f homogeneous" into the definition above. Note also that if $f_1, \ldots, f_m$ is a set of homogeneous generators for I then $V(I)$ is the set of simultaneous zeros of the f_i.

The geometry of linear subspaces already provides interesting geometry.

Example 6.7. *(i) Let $U \subset \mathbb{C}^{n+1}$ be a vector subspace, then $\mathbb{P}(U) \subset \mathbb{P}^n$. If*

$$U = \left\{ \underline{v} \in \mathbb{C}^{n+1} \mid \sum_{i=0}^{n} a_i^{(j)} v_i = 0 \ \forall j \right\}$$

fo a subset $\{\underline{a}^{(j)} = (a_0^{(j)}, \ldots, a_n^{(j)}\} \subset \mathbb{C}^{n+1}$ then $\mathbb{P}(U) = \mathbb{V}(I)$ where I is the (homogeneous) ideal generated by the linear forms $F_j = \sum_i a_i^{(j)} X_i$. Conversely, any projective variety defined by linear homogeneous polynomials has this form. Note that $\mathbb{P}(U \cap V) = \mathbb{P}(U) \cap \mathbb{P}(V)$. As terminology, a projective linear space is the vanishing locus of an ideal generated by linear homogeneous polynomials.

(ii) By the discussion above, the set of projective linear spaces of $\mathbb{P}^n$ is in bijection with the set of linear subspaces in $\mathbb{C}^{n+1}$. Moreover, the group $GL(n+1, \mathbb{C})$ acts on $\mathbb{P}^n$ in the natural way. The normal subgroup of scalar matrices $\mathbb{C}^\star \subset GL(n+1, \mathbb{C})$ acts trivially. The quotient is denoted

$$PGL(n+1, \mathbb{C}) = GL(n+1, \mathbb{C})/\mathbb{C}^\star$$

and acts on $\mathbb{P}^n$ (very transitively).

The next most interesting class of examples comes from hypersurfaces; as in the affine, a projective hypersurface is a variety $V \subset \mathbb{P}^n$ defined by the vanishing of a single non-zero homogeneous polynomial equation.

Example 6.8. *The Segre surface in $\mathbb{P}^3$ is the hypersurface*

$$S_{11} = \mathbb{V}(X_0X_3 - X_1X_2) \subset \mathbb{P}^3.$$

In fact, S is built out of familiar objects. Consider the set theoretic map

$$\begin{aligned} \sigma_{11} : \mathbb{P}^1 \times \mathbb{P}^1 &\to \mathbb{P}^3 \\ ((a_0 : a_1), (b_0 : b_1)) &\mapsto (a_0b_0 : a_0b_1 : a_1b_0 : a_1b_1). \end{aligned}$$

A nice interpretation is as follows. First consider the map

$$\mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}^{2\times 2},$$

sending a pair of column vectors (v, w) to the matrix vw^T. The image is precise the set of rank 1 matrices[9]*. By linear algebra, it follows that the map σ_{11} is injective with image exactly S.*

[9]The instructor must record that they find this construction and the identification as the space of rank 1 matrices absolutely beautiful!

Important foreshadowing. Crucially, this gives us a way to construct products of projective spaces, and therefore products of projective varieties. This will be done carefully later on via the general form of the Segre embedding.

Just as $\mathbb{P}^n$ has $n+1$ copies of affine spaces $U_0, \ldots, U_n$, if $V \subset \mathbb{P}^n$ is a projective variety, it can be covered be affine pieces. Precisely, let $V = \mathbb{V}(I) \subset \mathbb{P}^n$. Let

$$I_0 = \{f = F(1, Y_1, \ldots, Y_n) \mid F \in I \text{ homogeneous}\} \subset \mathbb{C}[Y_1, \ldots, Y_n]$$

which is an ideal. Let $V_0 \subset \mathbb{A}^n$ be the affine variety defined by I_0. Then $V_0 = V \cap \mathbb{A}^n$ thinking of $\mathbb{A}^n$ as $U_0 \subset \mathbb{P}^n$, with coordinate functions $Y_1, \ldots, Y_n$.

Likewise, setting $X_j = 1$ defines an ideal I_j whose associated affine variety is $V \cap U_j$.

Let $V \subset \mathbb{A}^n$ be an affine variety. We may identify

$$\mathbb{A}^n = U_0 \subset \mathbb{P}^n.$$

Now view $V \subset \mathbb{P}^n$. Note that this subset is almost certainly not a projective variety, as it is typically not even Zariski closed. However, we can calculate its Zariski closure. There is a very concrete description of this.

Definition 6.9. Fix $f \in \mathbb{C}[Y_1, \ldots, Y_n]$ of total degree d. Define the homogenization to be

$$F(X_0, \ldots, X_n) := X_0^d f(X_1/X_0, \ldots, X_n/X_0) \in \mathbb{C}[\underline{X}]$$

is a homogeneous polynomial of degree d, not divisible by X_0, and $F(1, Y_1, \ldots, Y_n) = f$. Consider the homogeneous ideal I^* generated by all such F as f runs over $I(V)$. It is the ideal of a projective variety $V^* \subset \mathbb{P}^n$ with $V^* \cap \mathbb{A}^n = V$, called the projective closure of V.

Therefore a projective variety V has the property that every point has a Zariski open neighborhood that can be identified with an affine variety[10].

Let us look at a quick example on homogenization and dehomogenization.

Example 6.10. *Consider the projective variety $V \subset \mathbb{P}^2$ given by $\mathbb{V}(X_0X_1 - X_2^2)$. The three affine varieties that cover it are $V_0 \subset U_0$ given by*

$$\mathbb{V}(Y_1 - Y_2^2) \subset \mathbb{A}^2.$$

This is a standard parabola. The second patch $V_1 \subset U_1$ looks essentially the same. However, the third patch is given by

$$\mathbb{V}(Z_0Z_1 - 1) \subset \mathbb{A}^2$$

which is a rectangular hyperbola. Therefore the parabola and hyperbola are simply different affine patches of the same projective curve!

In fact, the linear algebra of quadratic forms gives complete control over quadratic hypersurfaces.

Theorem 6.11. *Let $Q \subset \mathbb{P}^n$ be a hypersurface $\mathbb{V}(f)$ where f is a homogeneous quadratic polynomial, i.e. a quadratic form. After a change of coordinates by an element of $PGL(n+1, \mathbb{C})$, the hypersurface Q is isomorphic to a a hypersurface of the form*

$$\mathbb{V}(X_0^2 + \cdots + X_r^2) \subset \mathbb{P}^n$$

where r is the rank of the qudratic form determined by f.

[10] In the world of manifolds, one can quickly define an abstract manifold as a topological space together with the property that locally it looks like a vector space. The ambient space quickly becomes unnecessary. In algebraic geometry, this is much trickier: one wants to define an abstract variety as a space that locally looks like an affine variety, but this is not straightforward. In fact, if one works hard enough to do this, one may as well do something significantly more general: define a scheme, a concept introduced by Alexander Grothendieck and his colleagues in the 1960s. This is the subject of the Part III course. However, the most beautiful and rich examples still tend to come from studying varieties!

Proof. The proof follows immediately from the theorem on diagonalization of quadratic and symmetric bilinear forms, treated in Part IB Linear Algebra. □

Note that the intersection and union properties seen for affine varieties continue to hold here. An intersection of projective varieties is cut out by the sum of the corresponding ideals, and a union of projective varieties is cut out by the intersection of the corresponding ideals. You should verify that these operations preserve the homogeneous property. The proofs are identical.

Let V be a projective variety and define $I^h(V)$ to be the ideal generated by all homogeneous polys vanishing on V. Then we have

Theorem 6.12 (Projective Nullstellensatz)**.** *(i) If $\mathbb{V}(I) = \emptyset$ then $I \supset (X_0^m, \ldots, X_n^m)$ for some $m > 0$.*

(ii) If $V = \mathbb{V}(I) \neq \emptyset$ then $I^h(V) = \sqrt{I}$.

Proof. We explain how to reduce to the affine case, which also gives a route to thinking about projective varieties in general. Let I be a homogeneous ideal. Let

$$V^a = \mathbb{V}(I) \subset \mathbb{A}^{n+1}, \quad V = \mathbb{V}(I) \subset \mathbb{P}^n$$

be the affine and projective vanishing sets of I. Note that $\underline{0}$ is always a point of V^a. There is a natural quotient map

$$V^a \setminus \{\underline{0}\} \to V$$

obtained by restricting the projection from $\mathbb{C}^{n+1} \setminus \{\underline{0}\}$ to $\mathbb{P}^n$. Therefore, V is empty if and only if V^a is a subset of $\underline{0}$. Therefore its radical must contain $(X_0, \ldots X_n)$. The second statement follows similarly. □

The affine case will be proved later in these lectures.

Let $V \subset \mathbb{P}^n$ be a projective variety. If $W \subset \mathbb{P}^n$ is a projective variety with $W \subset V$ we say that W is a <u>closed subvariety</u> of V, and that the complement $V \setminus W$ is an <u>open subvariety</u> of V. These satisfy same properties as open and closed sets in topology, parallel to the affine case.

Again, we say V is <u>irreducible</u> if $V \neq V_1 \cup V_2$ for proper closed subvarieties V_1 and V_2. The following basic proposition carries over again.

Proposition 6.13. *(i) Every projective variety is a finite union of irreducible projective varieties.*

(ii) V irreducible iff $I^h(V)$ is prime.

Proof. The first statement follows from an identical argument as the affine case. For the second, first notice the following key fact. If I is a homogeneous ideal which is not prime, can find homogeneous elements F, G not contained in I whose product FG is contained in I. Given this, the affine argument once again works. □

In both the projective and affine cases, it is good to get used to the idea that open sets are very large. Precisely, a subset $S \subset V$ is <u>Zariski dense</u> in V if, for $f \in \mathbb{C}[\underline{X}]$ homogeneous, if f vanishes on S then f vanishes on all of V. This is merely spelling out density in the Zariski topology.

Proposition 6.14. *Let $V \subset \mathbb{P}^n$ be irreducible and $W \subset V$ a proper closed subvariety. Then $V \setminus W$ is dense in V.*

Proof. Let $f \in \mathbb{C}[\underline{X}]$ be homogeneous, vanishing on $V \setminus W$. As $W \neq V$ there exists $g \in I^h(W) \setminus I^h(V)$. This follows from the projective Nullstellensatz. Then fg vanishes on all of V. As g is not contained in $I^h(V)$ which is a prime ideal, f is contained in $I^h(V)$. □

7 Function theory on projective varieties

The function theory on a projective variety is subtle, as we have already seen. Arbitrary polynomials do not give us functions on $\mathbb{P}^n$. Homogeneous polynomials have well-defined zero loci, but they too do not give functions: their value is only well-defined up to scalar multiplication.

The key to function theory on projective varieties is that a ratio of homogeneous polynomials of the same degree does have a well-defined value at a point, provided it has any value at all!

Definition 7.1. Let $V \subset \mathbb{P}^n$ be an irreducible variety. The function field or field of rational functions of V is defined as

$$\mathbb{C}(V) = \{F/G \mid F, G \in \mathbb{C}[\underline{X}] \text{ homogeneous of same degree, } G \notin I^h(V)\}/\sim$$

where $F_1/G_1 \sim F_2/G_2$ if and only if $F_1G_2 - F_2G_1$ is contained in the homogeneous ideal $I^h(V)$.

The fact that this relation is an equivalence relation is easy, but it uses the primality of the ideal!

Lemma 7.2. *The relation defined above is an equivalence relation.*

Proof. The reflexive and symmetric properties are clear. Now suppose that we have F_1/G_1, F_2/G_2, and F_3/G_3 with the G_i not vanishing on V and

$$F_1G_2 - F_2G_1, \quad F_2G_3 - F_3G_2.$$

are both contained in the homogeneous ideal $I(V)$. Now consider the expression $F_1G_3 - F_3G_1$. Multiply it by G_2 to get

$$F_1G_2G_3 - F_3G_1G_2.$$

Since G_2 is not in the ideal $I^h(V)$ and this ideal is prime, it will suffice to prove that that this expression is contained in $I(V)$. Equivalently, we can show that the expression is 0 in the quotient $\mathbb{C}[\underline{X}]/I(V)$. In the quotient, we have

$$F_1G_2 = F_2G_1, \quad F_2G_3 = F_3G_2.$$

By substitution of these expressions into the equation written above, we see that in the quotient

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

□

It is essentially immediate that the quotient above is a field, and therefore deserves this name.

Remark 7.3. Although we will not use it quite yet, there is more structure lurking here than one initially sees. The definition above examines homogeneous rational functions of total degree 0. For any integer d, one could examine a set $\mathbb{C}(V, d)$ of homogeneous rational functions of degree d. An object of this form would not be a field though, as it doesn't make sense to multiply two such! If f and g have degree d, then fg has degree $2d$. However, it does make sense to multiply a rational function of degree d by a rational function of degree 0, i.e. an element of $\mathbb{C}(V)$. In other words, the set $\mathbb{C}(V, d)$ of degree d is a vector space (or module) over $\mathbb{C}(V)$!

Proposition 7.4. *The field $\mathbb{C}(V)$ is a finitely-generated field extension of $\mathbb{C}$.*

The reader is warned that finitely generated as a field extension is not the same as finite generation as an algebra, since the former allows more operations, crucially, taking reciprocals. For example, $\mathbb{C}(x)$ is finitely generated as a field but not as a $\mathbb{C}$ vector space. In the proof that follows, it will be useful to remember that the subfield generated by a collection of elements is the smallest field containing those elements.

Proof. Assuming V is nonempty, there is some coordinate X_i that does not vanish on V. We can assume it is X_0 by reordering the coordinates. Then we claim that elements of the form X_i/X_0 generate $\mathbb{C}(V)$. Explicitly, this means that we must write degree 0 ratios of the form F/G in terms of these simple elements X_i/X_0. We immediately reduce to the case where F is a monomial, since if we can generate these, we can generate everything. But since fields contain reciprocals, it suffices to write a ratio of monomials of total degree 0 in terms of these X_i/X_0. The statement is now obvious. □

As a consequence, the calculation of the function field of a projective variety is no more difficult than the calculation of the function field of an affine variety.

Corollary 7.5. *Let $V \subset \mathbb{P}^n$ be an irreducible projective variety not contained in $\{X_0 = 0\}$. Let V_0 be the variety defined by the equations*

$$F(1, Y_1, \ldots, Y_n) = 0$$

where F ranges over homogeneous elements in $I^h(V)$. We view it as a subset of the affine space U_0. Then

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

The proof is a good exercise in tracking definitions, and is left to the diligent reader.

In the affine case we can think of rational functions as partially defined functions on the regular locus. In the projective case this continues to hold. The symbol V continues to denote an irreducible projective variety.

Definition 7.6. Let φ be an element of $\mathbb{C}(V)$ and P be a point of V. Then φ is regular at P if and only if φ can be expressed as F/G, with $G(P)$ nonzero. In this case, there is a partially defined function

$$V \setminus \{P : \varphi \text{ is not regular at } P\} \to \mathbb{C}.$$

The local ring $\mathcal{O}_{V,P}$ of V at P defined the same way as for affine varieties: it is the subring of $\mathbb{C}(V)$ consisting of those rational functions that are regular at P.

Proposition 7.7. *Assume $V \subset \mathbb{P}^n$ is a projective irreducible variety not contained in $\{X_0 = 0\}$. Let P be a point on V that is contained in the open subset V_0. Then there is an identification of local rings*

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

induced by the isomorphism

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

Proof. Exercise in the definitions; omitted. □

Remark 7.8. A slogan worth keeping in mind is that projective varieties do not have any interesting (non-constant) functions that are regular everywhere. In order to study them, these partially defined rational functions become much more important than in the affine case. The "reason" for this is clear: a projective variety is compact, and rational functions are polynomial ratios, and are therefore holomorphic whenever defined. If defined everywhere, we would get a holomorphic function on a compact domain, and therefore a bounded holomorphic function. By an extension of Liouville's theorem from complex analysis, there should not be any such. The honest proof of this requires more effort.

8 Rational maps between projective varieties

Just as we went from functions to partially defined functions, we can go from morphisms to partially defined morphisms, or rational maps. These will be denoted by a broken arrow, for example:

$$\mathbb{P}^n \dashrightarrow \mathbb{P}^m.$$

Let $F_0, \ldots F_m \in \mathbb{C}[\underline{X}]$ be homogeneous of same degree d. We may consider the map

$$\underline{F} = (F_0, \ldots, F_m) : \mathbb{C}^{n+1} \to \mathbb{C}^{m+1}$$

Proposition 8.1. *The map $\underline{F}$ descends to a map*

$$\varphi : \mathbb{P}^n \setminus \bigcap_j \mathbb{V}(F_j) \to \mathbb{P}^m,$$

with $\varphi(P)$ defined by choosing a representative $\underline{a} = (a_0, \ldots, a_n)$ for P and mapping it to the tuple $(F_0(\underline{a}) : \cdots : F_m(\underline{a}))$.

Proof. Note that all the F_j have the same degree d, so if we choose two representatives $\underline{a}$ and $\underline{a}'$ that are related by uniformly scaling by a complex number λ, then $\underline{F}(\underline{a})$ and $\underline{F}(\underline{a}')$ are related by uniformly scaling by λ^d. □

In order to avoid overcrowding notation, we denote these by

$$\varphi = (F_i) \colon \mathbb{P}^n \dashrightarrow \mathbb{P}^m.$$

The broken arrow indicates that the map is only partially-defined on its domain.

Let G be a nonzero homogeneous polynomial in $X_0, \ldots X_n$, and we are given $F_0, \ldots, F_m$ as above, then there is a map

$$G\underline{F} : \mathbb{P}^n \dashrightarrow \mathbb{P}^m.$$

This map is essentially the same, but the locus where it is undefined is potentially larger. On the common locus of definition, the map above agrees with φ defined previously. We will typically view these as the same rational map.

Since $\mathbb{C}[\underline{X}]$ is a unique factorization domain, there is a best representative for φ obtained by canceling all common factors out. However, this is is not a property we want to impose in general, so I will not stress this here.

We can now define rational maps from an irreducible projective variety $V \subset \mathbb{P}^n$. Let $F_0, \ldots, F_m$ be elements in $\mathbb{C}[\underline{X}]$ that are not all contained in $I^h(V)$. They determine a set theoretic mapping

$$V \setminus \cap_j \mathbb{V}(F_j) \to \mathbb{P}^m.$$

Two such pairs (F_j) and (G_j) are said to determine the same rational map if $F_j G_j - F_j G_i$ is contained in $I^h(V)$. A rational map is an equivalence class of mappings determined by polynomials as above.

Definition 8.2. A point $P \in V$ is said to be a regular point of a rational map $\varphi : V \dashrightarrow \mathbb{P}^m$ if there exists a representation of φ $(G_0, \ldots, G_m)$ such that $G_i(P)$ is nonzero for some index i. The domain of a rational map is the set of regular points. A rational map is a morphism if all points are contained in the domain.

Again, we stress that on an arbitrary V, different representatives may need to be used at different points and there may not be a "best possible" representation of the map. We see an explicit example of this below.

If $W \subset \mathbb{P}^m$ then a rational map $\varphi : V \dashrightarrow W$ is a rational map $\varphi : V \dashrightarrow \mathbb{P}^m$ such that the domain of φ is sent to W.

If every point of a rational map φ is regular, it is called a morphism and is written with the regular arrow rather than the broken arrow. It is an isomorphism if there is a morphism $\psi\colon W \to V$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity morphisms on W and V respectively.

Example 8.3. *A linear map is given by*

$$\varphi : \mathbb{P}^n \dashrightarrow \mathbb{P}^m$$

is given by any $(m+1) \times (n+1)$ matrix (a_{ij}). Concretely, φ is given by a tuple (F_j) with

$$F_j = \sum_i a_{ij} X_i.$$

If the matrix has rank $n+1 \leq m+1$ then φ is a morphism.

A rational map φ is a good source of m̌orphisms, via restricting. The following is a nice example.

Example 8.4 (Projection from a point)**.** *Consider the point $P = (0 : 0 : 1)$ in $\mathbb{P}^2$. A rational map projection from P*

$$\pi : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$$

is given by sending $(a_0 : a_1 : a_2)$ to the pair $(a_0 : a_1)$. The map is not defined at P. Now let $C \subset \mathbb{P}^2$ be the variety $\mathbb{V}(f_d)$ where f_d has degree d, and assume that P does not lie on C. By restriction, we get

$$\varpi : C \to \mathbb{P}^1.$$

This is a morphism, since it is defined everywhere. In order to understand this morphism well, fix a point q on $\mathbb{P}^1$ and describe the preimage (or fiber) of q in terms of f_d. Convince yourself that for almost all choices of q, the set $\varpi^{-1}(q)$ has size d.

Important Warning: If we restrict a rational map to a subvariety V that is entirely contained in its domain, we do indeed get a morphism on V. However, it is possible to restrict a rational map to a subvariety that has nonempty intersection with the domain and still end up with a morphism! We will see an example now.

Example 8.5 (Absolutely crucial!)**.** *Let C be the conic*

$$\mathbb{V}(X_0X_2 - X_1^2) \subset \mathbb{P}^2.$$

Consider the projection from the point $(0:0:1)$, which we notice lies on the curve C, to obtain

$$\pi : C \dashrightarrow \mathbb{P}^1$$

sending $(a_0 : a_1 : a_2)$ to $(a_0 : a_1)$. The map is determined by (X_0, X_1). At first sight, it appears that $(0:0:1)$ is not in the domain of π, but this is an illusion. ***We must look for other pairs*** *(F_0, F_1)* ***that determine the same rational map as*** *(X_0, X_1). If (F_0, F_1) is equivalent to (X_0, X_1) then we must have*

$$F_0X_1 - F_1X_0 \in I(C)^h.$$

The ideal is generated by $X_0X_2 - X_1^2$ and therefore, it makes sense to take $(F_0, F_1) = (X_1, X_2)$, since this is equivalent to (X_0, X_1). The latter pair of polynomials determines a rational map on which $(0:0:1)$ is clearly contained in the domain. It follows that

$$\pi : C \to \mathbb{P}^1$$

is in fact a morphism.

In fact, there is a strong statement that we can derive from this.

Proposition 8.6. *Let $C \subset \mathbb{P}^2$ be the vanishing locus $\mathbb{V}(f)$ where f is homogeneous of degree 2. If f is irreducible, then C is isomorphic to $\mathbb{P}^1$.*

Proof. We have seen that by changing coordinates, since f is irreducible, that we can assume $f = X_0X_2 - X_1^2$. By projection from the point $(0:0:1)$ we have a morphism

$$C \to \mathbb{P}^1.$$

For the inverse, consider the map

$$\mathbb{P}^1 \to \mathbb{P}^2$$

given by $(Y_0^2 : Y_0Y_1 : Y_1^2)$. It is straightforward to check that these are inverses. □

Aside from the technical definition of a rational map, in practice, it the important thing is that rational maps are set theoretic maps on dense open sets that arise via homogeneous polynomials.

We take a moment to record three Italian examples of rational maps and morphisms.

Example 8.7 (Cremona transformation)**.** *Consider the rational map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ determined by*

$$\kappa : (X_0 : X_1 : X_2) \mapsto (X_1X_2 : X_0X_2 : X_0X_1)$$

This can be thought of as the coordinate-wise reciprocal map. The Cremona map "sends lines to conics". Choose a line ℓ that is not given by the vanishing of any X_i. Consider the subset

$$\kappa(\mathrm{dom}\,\kappa \cap \ell) \subset \mathbb{P}^2.$$

This is the rational analogue of the "image". A simple and direct calculation shows that the closure of this set is a conic!

A classical construction of a morphism on $\mathbb{P}^n$ is the Veronese.

Example 8.8 (Veronese embeddings)**.** *Let $F_0, \ldots, F_m$ be the list of degree d monomials in variables $X_0, \ldots, X_n$. The number m is $\binom{n+d}{d} - 1$. There is a natural morphism*

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

sending $(\underline{a})$ to the tuple $(F_0(\underline{a}) : \cdots : F_m(\underline{a}))$. A straightforward but tedious calculation shows that the Veronese map is set theoretically injective and in fact $\nu_d(\mathbb{P}^n)$ is a projective variety isomorphic to $\mathbb{P}^n$.

The product of affine varieties is an affine variety, since $\mathbb{A}^m \times \mathbb{A}^n \simeq \mathbb{A}^{m+n}$ and if $V \subset \mathbb{A}^m$, $W \subset \mathbb{A}^n$ are varieties then

$$V \times W = V(I) \subset \mathbb{A}^{m+n},$$

where I is the ideal generated by polynomials $f(X_1, \ldots, X_m)$ for $f \in I(V)$ and $g(X_{m+1}, \ldots, X_{m+n})$ for $g \in I(W)$.

Critically, this does not extend to an isomorphism between $\mathbb{P}^m \times \mathbb{P}^n$ and $\mathbb{P}^{m+n}$. We have seen earlier how to view $\mathbb{P}^1 \times \mathbb{P}^1$ inside $\mathbb{P}^3$ as a projective variety. This generalizes as follows.

Example 8.9 (Segre embeddings)**.** *The Segre embedding is the map*

$$\begin{aligned}\sigma_{mn}\colon \mathbb{P}^m \times \mathbb{P}^n &\to \mathbb{P}^{mn+m+n}\\ ((x_i),(y_j)) &\mapsto (x_i y_j)\end{aligned}$$

where the $(m+1)(n+1)$ *variables in* $\mathbb{P}^{mn+m+n}$ *are labelled* Z_{ij}, $0 \le i \le m$, $0 \le j \le n$. *Note this is just a map of sets at the moment, though there is more that can be said. The nice geometry here is that, for each fixed* Q*, the map sending* P *to* $\sigma_{mn}(P,Q)$ *is a linear morphism* $\mathbb{P}^m \hookrightarrow \mathbb{P}^{mn+m+n}$*, and similarly for each fixed* P*.*

The discussion when $m = n = 1$ *involved the identification of the image as the set of rank* 1 *matrices of size* 2×2*. The interpretation there also generalizes, but requires the notion of a tensor product, which we do not assume. For those who are familiar with tensor products of vector spaces, we briefly indicate what is going on. It can be considered non-examinable. There is a natural map*

$$U \times U' \to U \otimes U',$$

sending a pair (u,u') *to* $u \otimes u'$*. The map is not linear, but it is bilinear, i.e. when a vector in a factor is fixed, the map is linear in the other factor. Passing to projective spaces gives the Segre map.*

The image of the Segre embedding is a projective variety.

Theorem 8.10. *The map* σ_{mn} *is a bijection between* $\mathbb{P}^m \times \mathbb{P}^n$ *and the projective variety* $V = V(I) \subset \mathbb{P}^{mn+m+n}$*, where* I *is the homogeneous ideal generated by polynomials*

$$Z_{ij}Z_{pq} - Z_{iq}Z_{pj}, \quad i,p \in \{0,\dots,m\},\ j,q \in \{0,\dots,n\},\ i \ne p,\ j \ne q.$$

Moreover the projective variety V *is irreducible.*

Proof. Clearly $\sigma_{mn}(\mathbb{P}^m \times \mathbb{P}^n) \subset V$. Consider the affine piece

$$V_{00} = V \cap \{Z_{00} \ne 0\} \subset \mathbb{A}^{mn+m+n}.$$

The inhomogeneous ideal I_{00} defining V_{00} is, after setting $Y_{ij} = Z_{ij}/Z_{00}$, generated by the polynomials

$$Y_{ij} - Y_{i0}Y_{j0}, \quad 1 \le i \le m,\ 1 \le j \le n$$

which contains automatically all the other elements $Y_{ij}Y_{pq} - Y_{iq}Y_{pj}$. It follows that σ_{mn} defines an isomorphism $\mathbb{A}^m \times \mathbb{A}^n \xrightarrow{\sim} V(I_{00})$ with inverse

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

Since affine space is irreducible, it follows that $V(I_{00})$ is also irreducible. Repeating this for the other affine pieces $\{Z_{ij} \ne 0\}$ gives the result. □

As a consequence of the partial definedness of rational maps, composition of rational maps is a slightly subtle issue. Suppose $\varphi\colon V \dashrightarrow W$, $\psi\colon W \dashrightarrow Z$ are rational maps. The composite $\psi \circ \varphi$ isn't always defined. The reason is simple: the image of φ could consist entirely of points at which ψ is not regular.

Definition 8.11. A rational map φ is dominant if $\varphi(\operatorname{dom}\varphi) \subset W$ is dense in W.

If φ is dominant, then $\psi \circ \varphi$ is defined for any rational map ψ. Indeed, let U denote a dense open subset in the domain of φ and let U' be an open subset in the domain of ψ. Then take U'' to be the intersection

$U \cap \psi^{-1}U'$. This is open in V and the composite is well-defined here. Since compositions of polynomials are polynomials, this partially defined composition is the identity.

If $\psi\colon W \dashrightarrow V$ is such that $\psi \circ \varphi$, $\varphi \circ \psi$ are defined and equal the identity maps of V, W respectively, then we say φ is birational (or a birational equivalence or birational isomorphism).

Obviously every isomorphism is a birational map, but there are a number of other important examples. The Cremona transformation is a more nontrivial example of a rational map.

Recall that rational functions are merely rational maps to $\mathbb{A}^1$, or to $\mathbb{C}$, so given a dominant map $\varphi : V \dashrightarrow W$, the composition above gives rise to

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

sending a rational function $f : W \dashrightarrow \mathbb{C}$ to the composition $f \circ \varphi : V \dashrightarrow \mathbb{C}$. A birational map gives rise to an isomorphism of function fields. In fact, we have the following theorem.

Theorem 8.12. *Let W, V be irreducible varieties. Then W, V are birationally isomorphic and only if there is an isomorphism of fields $\mathbb{C}(W) \simeq \mathbb{C}(V)$.*

This gives a direct connection between algebraic geometry and the algebra of fields. Algebraic varieties up to birational equivalence is merely field theory; that doesn't mean it is simple though!

Proof. We provide only an outline, leaving the relatively tedious by straightforward algebra to the reader. The proof can be considered non-examinable. Let $V \subset \mathbb{P}^n$ not contained in $\{X_0 = 0\}$, and $W \subset \mathbb{P}^m$ not contained in $\{Y_0 = 0\}$. Then we have seen that $\mathbb{C}(V) = \mathbb{C}(x_1, \ldots, x_n)$, where $x_i = X_i/X_0$. Similarly, $\mathbb{C}(W) = k = \mathbb{C}(y_1, \ldots, y_m)$, $y_j = Y_j/Y_0$. An isomorphism $\mathbb{C}(V) \simeq \mathbb{C}(W)$ identifies y_j with $f_j(\underline{x})$, for some rational functions f_j in n variables. Clear demoninators, and homogenize with respect to X_0, and we now obtain $m + 1$ homogenenous polynomials $F_j \in \mathbb{C}[\underline{X}]$ with

$$f_j(X_1/X_0, \ldots, X_n/X_0) = \frac{F_j(X_0, \ldots, X_n)}{F_0(X_0, \ldots, X_n)}$$

and $(F_0 : \cdots : F_m)$ therefore determines a rational map $V \dashrightarrow W$. By writing the x_i variables in terms of $\{y_j\}$ using the given isomorphism, we obtain a rational map in the other direction. It is straightforward to check that these are mutually inverses. □

9 Singularities and tangent spaces

We now import the notion of tangent spaces from classical geometry. We begin with the basic notions in the case of hypersurfaces only. Let $V = \mathbb{V}(f) \subset \mathbb{A}^n$ affine hypersurface, with f an irreducible polynomial. Choose a point $P = (a_i)$ on V. An affine line through P has the following form:

$$L = \{(a_1 + tb_1, \ldots, a_n + tb_n) \mid t \in \mathbb{C}\}, \quad 0 \neq \underline{b} \in \mathbb{C}^n$$

The intersection $V \cap L$ is then given by the set of points on this line on which f vanishes. Symbolically, we calculate:

$$0 = f(a_1 + tb_1, \ldots, a_n + tb_n) = g(t) = \sum_r c_r t^r.$$

The constant term is $c_0 = f(\underline{a}) = 0$, and the linear term is $c_1 = \sum_i b_i(\partial f/\partial X_i)(\underline{a})$. Certainly the polynomial $g(t)$ vanishes at $t = 0$ because P lies on $V \cap L$. The polynomial g has a zero of order larger than 1 at $t = 0$, i.e. L is tangent to V at P, if and only if the line L is contained in the affine subspace

$$T^{\text{aff}}_{V,P} = \mathbb{V}(g) \subset \mathbb{A}^n, \quad g = \sum_{i=1}^n (\partial f/\partial X_i)(P)(X_i - a_i).$$

Definition 9.1. The affine subspace $T^{\text{aff}}_{V,P}$ is the affine tangent space of V at P.

Therefore the subspace $T^{\text{aff}}_{V,P}$ is either an affine space of dimension $n-1$ or the entire space of $\mathbb{A}^n$. The point P is smooth or nonsingular in the first case, and is singular otherwise.

Example 9.2 (Nodal and cuspidal cubics)**.** *The first two classical examples of singular points occur for degree* 3 *curves in* $\mathbb{A}^2$*. The nodal cubic is an affine variety isomorphic to*

$$C = \mathbb{V}(Y^2 - X^2(X+1)).$$

The point $(0,0)$ *is singular by direct calculation. The cuspidal cubic or cusp is an affine variety isomorphic to*

$$C' = \mathbb{V}(Y^2 - X^3).$$

The calculation is essentially identical. The topological spaces of the real and complex parts can be useful to visualize.

There is also a projective version of course. Let $V = \mathbb{V}(F) \subset \mathbb{P}^n$, for $F \in \mathbb{C}[X_0, \ldots, X_n]$ homogeneous and irreducible.

Definition 9.3. The projective tangent space of V at $P = (a_0 : \ldots : a_n)$ is defined to be

$$T^{\text{proj}}_{V,P} = V(G) \subset \mathbb{P}^n, \quad G = \sum_{i=0}^{n} X_i(\partial F/\partial X_i)(\underline{a})$$

Two remarks are in order. First, though not absolutely immediate, the set $T^{\text{proj}}_{V,P}$ is a linear projective subspace that contains the point P. To see the containment, notice that we have a simple equality by elementary differentiation:

$$F(\underline{X}) = \deg(F)G(\underline{X}),$$

which is sometimes called Euler's formula. Second, there is a compatibility between tangent spaces and passing to affine patches of projective varieties. Specifically, assume $V \not\subset \{X_0 = 0\}$ and examine $V_0 = V \cap \mathbb{A}^n \subset \mathbb{A}^n$ be given by the given by $f(X_1, \ldots, X_n)$ where

$$F(X_0, \ldots, X_n) = X_0^{\deg F} f(X_1/X_0, \ldots, X_n/X_0).$$

By computing $\partial F/\partial X_i$ it follows that if $P \in V_0$ then $T^{\text{proj}}_{V,P} \cap \mathbb{A}^n = T^{\text{aff}}_{V_0,P}$.

The notions of smooth and singular point are made exactly as in the case of affine hypersurfaces. Uniformly, we can make the definition as follows.

Definition 9.4. A point P is a singular point if and only if all the partial derivatives $\partial f/\partial X_i$, $1 \leq i \leq n$, in the affine case, or $\partial F/\partial X_i$, $0 \leq i \leq n$, in the projective case, vanish at P. A point that is not singular is smooth. A hypersurface is smooth if all its points are smooth and a hypersurface is singular if it is not smooth.

The set of singular points is "small".

Proposition 9.5. *The set of smooth points of an irreducible hypersurface, i.e. the vanishing of a nonconstant polynomial, is a nonempty Zariski open subset.*

Proof. The set of singular points is exactly $V \cap \bigcap_i \mathbb{V}(\partial F/\partial X_i)$ which is a closed subvariety of V. If it were all of V then by Nullstellensatz, for each i the derivative $\partial F/\partial X_i$ would be contained in the ideal $I^h(V)$ which is principal and generated by (F). Since $\partial F/\partial X_i$ is homogeneous of degree smaller than $\deg F$, would then have $\partial F/\partial X_i = 0$ for all i. This implies that F is constant, which is a contradiction. $\square$

In simple terms, the set of smooth points is Zariski dense. There is a "meta" statement that the discussion above implies which we phrase as an example.

Example 9.6 (The variety parameterizing hypersurfaces)**.** *A hypersurface of degree d in $\mathbb{P}^n$ is given by the vanishing set of a non-zero homogeneous polynomial of degree d in $n+1$ variables. There are precisely $N = \binom{n+d}{d}$ monomials. A choice of N coefficients determines such a polynomial subject to (i) not all coefficients can be 0, and (ii) two equations determine the same hypersurface if and only if they are scalar multiples of each other.*

Therefore, there is a natural bijection

$$\{\textit{Hypersurfaces of degree } d \textit{ in } \mathbb{P}^n\} \leftrightarrow \mathbb{P}^{N-1}.$$

For examples, lines in $\mathbb{P}^2$ are in bijection with points of $\mathbb{P}^2$, while conics in $\mathbb{P}^2$ are in bijection with points of $\mathbb{P}^5$.

There is a very interesting subset:

$$\{\textit{Singular hypersurfaces of degree } d \textit{ in } \mathbb{P}^n\} \subset \{\textit{Hypersurfaces of degree } d \textit{ in } \mathbb{P}^n\}.$$

Identifying the right hand side with $\mathbb{P}^{N-1}$, the set of singular hypersurfaces is the set of coefficients in $\mathbb{P}^{N-1}$ such that, on the hypersurface determined by the coefficients, there is a common vanishing point for all the partial derivatives of that polynomial (again determined by those coefficients). As a challenge, can you prove that the set of singular hypersurfaces is a proper closed subset?

We now treat the case of a general variety. It is clearest to treat the tangent space as a <u>vector space</u> rather than an affine or projective space. In the case of affine hypersurfaces, we take the affine space and translate to the origin.

Definition 9.7. Let $V \subset \mathbb{A}^n$ be an affine variety, and let P be a point lying on V. We define the <u>tangent space to V at P</u> as

$$T_{V,P} = \left\{ \underline{v} \in \mathbb{C}^n \mid \sum_{i=1}^{n} v_i \frac{\partial f}{\partial X_i}(P) = 0 \ \forall f \in I(V) \right\} \subset \mathbb{C}^n$$

Let $V \subset \mathbb{P}^n$ a projective variety and P a point of V. Suppose $V_j = V \cap \{X_j \neq 0\}$ is an affine piece of V containing P. Define $T_{V,P} = T_{V_j,P}$ as above.

There is a minor issue worth flagging. The way we have defined things, a point P in projective variety has a tangent space for each choice of affine neighborhood V_j containing it. However, these are naturally isomorphic, and this is clarified in the remark following the next proposition. We will momentarily take this on faith, as the issue will become clarified in its appropriate context below.

We have obtained the tangent space at P by linearizing polynomials at P. We can do the same for maps between varieties. In what follows we abuse notation slightly in the following common manner. Recall that $\mathbb{P}^n$ is covered by affine spaces $U_0, \dots, U_n$ which are each natural identified with $\mathbb{A}^n$. Every point P in $\mathbb{P}^n$ is therefore contained in some U_i; when the precise index is unimportant, we write $\mathbb{A}^n \subset \mathbb{P}^n$ for an affine patch, rather than $U_i \subset \mathbb{P}^n$.

Let $V \subset \mathbb{P}^n$, $W \subset \mathbb{P}^m$ be projective varieties, and fix a rational map

$$\varphi \colon V \dashrightarrow W,$$

and P in the domain $\mathrm{dom}(\varphi)$. We will define a linear map $d\varphi_P \colon T_{V,P} \to T_{W,\varphi(P)}$ as follows. Assume that

$$P \in V \cap \mathbb{A}^n, \quad \varphi(P) = Q \in W \cap \mathbb{A}^m$$

and that $\varphi = (F_0 : \ldots : F_m)$ for homogeneous $F_j \in \mathbb{C}[\underline{X}]$. As noted above, we have abused the notation slightly, and written $\mathbb{A}^n$ and $\mathbb{A}^m$ for affine patches inside $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively.

Write

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

which represents a rational function on V, regular at P. We now define the derivative of φ or linearization of φ at P by the formula

$$\begin{aligned} d\varphi_P : T_{V,P} &\to \mathbb{C}^m \\ \underline{v} &\mapsto \left(\sum_{i=1}^{n} v_i \frac{\partial f_j}{\partial X_i}(P) \right)_j \end{aligned}$$

The map is evidently linear. The derivative has all the expected properties from geometry.

Proposition 9.8. *We maintain the notation above.*

(i) The derivative of a rational map sends the tangent space at P to the tangent space of $\varphi(P)$, i.e. $d\varphi_P(T_{V,P}) \subset T_{W,\varphi(P)}$.

(ii) The linear map $d\varphi_P$ depends only of φ, not on the polynomials (F_i) representing it.

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

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

Proof. (i) In order to verify the statement, we may replace V and W by the affine pieces $V \cap \mathbb{A}^n$ and $W \cap \mathbb{A}^m$. The tangent space to W at $\varphi(P)$ is cut out by the linearizations of the polynomials cutting out W. Therefore, consider a polynomual g in $I(W)$. Applying the map on function fields, we write $h = g(f_1, \ldots, f_m) \in \mathbb{C}(\underline{X})$ a rational function regular on V that is regular at P, and it vanishes on those points of V where it is regular. Then by the chain rule, we have the equality

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

so if $\underline{v} \in T_{V,P}$, we see that $d\varphi_P(\underline{v}) \in T_{W,Q}$.

(ii) If we take another representation (F_j') for φ then the corresponding rational functions $f_j' \in \mathbb{C}(\underline{X})$ will have the property that $f_j' - f_j$ vanishes on V wherever defined, so we have $f_j' - f_j = p_j/q_j$ where $p_j \in I(V)$ and $q_j \in \mathbb{C}[\underline{X}]$, with $q_j(P) \neq 0$. Then by applying the quotient rule and the fact that p_j lies in $I(V)$

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

Let $\underline{v} \in T_{V,P}$. Then the last equation shows that for every j

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

so the map $d\varphi_P$ is independent of the representation of φ.

(iii) This is now reduced to the statement of the chain rule from multivariable calculus.

(iv) The statement follows from (iii). ∎

Remark 9.9. We can now clarify the flagged point about the definition of the tangent space on a projective variety. First, given a point P in $\mathbb{P}^n$ contained in two different affine patches U_i and U_j, there is a natural birational map

$$U_i \dashrightarrow U_j$$

which is the identity on $U_i \cap U_j$ and defined at P. Therefore, there is a natural isomorphism between $T_{P,\mathbb{P}^n}$ on these two different affine patches, i.e. between $T_{U_i,P}$ and $T_{U_j,P}$. Now, given an irreducible variety V and a point P in V with $V_i = V \cap U_i$ and $V_j = V \cap U_j$, the tangent space $T_{V_i,P}$ is mapped isomorphically to $T_{V_j,P}$ under the natural isomorphism above between $T_{U_i,P}$ and $T_{U_j,P}$.

Definition 9.10. Let V be an affine or projective variety.

(i) If V irreducible define $\dim V = \min\{\dim T_{V,P} \mid P \in V\}$

(ii) If P lies on V and V is irreducible, we say P is <u>smooth</u> or <u>non-singular</u> if $\dim T_{V,P} = \dim V$, and is <u>singular</u> otherwise

(iii) For potentially reducible varieties, define $\dim V$ to be the maximum of the dimension of irreducible components of V.

Remark 9.11. The notion of dimension for varieties whose components have different dimensions is a very coarse invariant. For this reason, we have not defined the notion of smooth and singular points on varieties that are not irreducible. An ad-hoc definition that typically gives good answers is to declare any point that lies on multiple components to be singular, and then to treat the remainder of the points, which lie on a unique irreducible component, via the discussion for irreducible varieties. The reason that this is the right notion will take us on a detour without significant reward, so we omit it.

The set of singular points is always a "small set". We already saw this in the case of hypersurfaces.

Theorem 9.12. *The set of smooth points of V is a non-empty open subvariety.*

Proof. The non-emptiness is immediate from the definition. We can assume that $V \subset \mathbb{A}^n$ is affine; if V is projective, one may treat each affine pieces of V in turn, We further assume that $I(V)$ is generated by polynomials f_j. Then if $P \in V$,

$$T_{V,P} = \left\{ \underline{v} \in \mathbb{C}^n \mid \sum_i v_i (\partial f_j / \partial X_i)(P) = 0 \right\}$$

and so

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

and for any $r \in \mathbb{N}$,

$$\{P \in V \mid \dim T_{V,P} \geq r\} = \{P \mid \operatorname{rank}((\partial f_j/\partial X_i)(P)) \leq n - r\}$$

is the closed subvariety of V given by the $(n-r) \times (n-r)$ minors of the matrix of polynomials $(\partial f_j / \partial X_i)$. ☐

Since the locus where the minimum dimension is achieved is open and therefore dense we have the following corollary.

Corollary 9.13. *Birational irreducible varieties have the same dimension.*

10 Examples of theorems in algebraic geometry

We have now developed sufficient technology to state a number of interesting theorems in algebraic geometry. Many of these theorems has been important corner stones in the subject. We will see some of them in the course, and will see shadows of some others. The section can be ignored for the purposes of an exam, but it should give you a sense of what questions are interesting in the subject.

Theorem 10.1. *A smooth and irreducible projective variety of dimension* 1 *is uniquely determined by its function field.*

The statement is false for surfaces. For example, $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ are birational, which you will prove on the second example sheet, but not isomorphic, though we haven't quite proved this.

There is much to say about the theory of algebraic curves. The most studied algebraic curves are the elliptic curves, which are the topic of the following theorem.

Theorem 10.2. *Let* $C \subset \mathbb{P}^2$ *be a smooth and irreducible variety cut out by a degree* 3 *polynomial. Then* C *admits a natural group structure:*

$$\oplus : C \times C \to C.$$

This is the "group law on the elliptic curve", and we will see this in the final lectures of the course. If the polynomial defining C has $\mathbb{Q}$ coefficients, then the set of $\mathbb{Q}$-points on C is a finitely generated abelian group by a remarkable theorem of Mordell. It is the starting point of the Birch–Swinnerton-Dyer conjecture

The study of the the class of birational "models" of a fixed variety of dimension 2 is a classical subject. The study in dimension 3 and larger is much more difficult, and of contemporary interest. The following will give you some intuition for how to think about birationality.

Theorem 10.3. *Every irreducible variety is birational to a projective hypersurface.*

The result is rather striking and beautiful, but surprisingly easy. It is the geometric incarnation of the primitive element theorem in Galois theory. The following similar sounding result is much more difficult.

Theorem 10.4. *Let* V *be an irreducible projective variety. There exists a smooth and irreducible projective variety* $\widetilde{V}$ *and a birational morphism*

$$\widetilde{V} \to V.$$

In particular, every irreducible variety is birational to a smooth and projective variety.

The theorem above was proved by Hironaka in the 1960s and is one of the most frequently used theorems in algebraic geometry. In algebraic geometry over fields of positive characteristic, the analogous result remains unavailable to this day.

A basic question in algebraic geometry is to determine a birational type of hypersurfaces. A variety is called <u>rational</u> if it is birational to projective space of some dimension. In Example Sheet II you will prove that all irreducible quadric hypersurfaces are rational. Rataionality of cubics is one of the most elementary, central, and challenging questions in algebraic geometry.

Theorem 10.5. *A smooth cubic hypersurface (i.e. surface) in* $\mathbb{P}^3$ *is rational. A surface of degree* $d \geq 4$ *in* $\mathbb{P}^3$ *is never rational. A smooth cubic hypersurface in* $\mathbb{P}^4$ *(i.e. a cubic threefold) is never rational. There exist smooth cubic hypersurfaces in* $\mathbb{P}^5$*, i.e. cubic fourfolds, that are rational.*

It is expected that there exist smooth cubic fourfolds that are not rational.

Another beautiful direction of study is the topology of complex algebraic varieties. The following result is within reach of the methods in the Part III course in algebraic geometry.

Theorem 10.6. *Let $V \subset \mathbb{P}^n$ be a smooth hypersurface with $n \geq 3$. Then V is simply connected in the Euclidean topology, i.e. $\pi_1(V) = 0$.*

As a very concrete consequence, this means that if $C \subset \mathbb{P}^2$ is a smooth projective variety cut out by an equation of degree $d \geq 3$, then $C \times C$ cannot be a hypersurface.

The following result from the 1950s uses Morse theory.

Theorem 10.7. *Let V be a smooth affine variety of dimension n. Then in the Euclidean topology the homology groups $H_i(V; \mathbb{Z})$ are 0 for $i > n$.*

Note that a smooth affine variety of dimension n has real dimension $2n$, so the result is surprising! In fact, the space V is homotopy equivalent to a simplicial complex of real dimension at most n.

Even simpler than simple connectedness are connectedness theorems. The following result is remarkable, and is due to Fulton–Hansen.

Theorem 10.8. *Let V and W be irreducible projective varieties in $\mathbb{P}^n$. If the inequality*

$$\dim V + \dim W > n$$

holds, then the intersection $V \cap W$ is connected.

Another direction of study is enumerative geometry. The starting point is one of the most famous results in the subject.

Theorem 10.9. *A smooth cubic surface in $\mathbb{P}^3$ contains precisely 27 straight lines. A general smooth quintic threefold in $\mathbb{P}^4$ contains 2875 straight lines and 609250 degree 2 curves.*

The result on cubic surfaces is provable using techniques we will have by the end of the course. The other two results are each significantly harder. The number of degree d curves on the quintic threefold above is known for all d. via mirror symmetry/string theory.

11 Geometry from the function field

We begin with some terminology. Let K be a finitely generated field extension of $\mathbb{C}$. A field of this form always arises by taking $\mathbb{C}[\underline{X}]/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ and then passing to its function field.

Recall that if $K \subset L$ are fields and α is an element of L, then α is transcendental over K if α is not the root of a nontrivial polynomial with coefficients in K. More generally if $S \subset L$ is a set of elements, then the elements of S are algebraically independent over K if they do not satisfy a non-trivial polynomial equation with coefficients in K.

The field $K/\mathbb{C}$ is a pure transcendental extension if $K = \mathbb{C}(x_1, \ldots, x_n)$ for $x_1, \ldots, x_n$ algebraically independent over $\mathbb{C}$. In other words, it is the fraction field of a polynomial ring.

Proposition 11.1. *Let $K/\mathbb{C}$ be a finitely generated field extension. Then there exists a pure transcendental sub-extension $K_0 = \mathbb{C}(x_1, \ldots, x_n) \subset K$ such that K/K_0 is finite. Moreover $K = K_0(y)$ for some $y \in K$.*

We will soon see that the integer n is unique. It will be referred to as the transcendence degree of K over $\mathbb{C}$.

Proof. The final statement is the primitive element theorem from Galois theory. We prove the first statement. Suppose K is generated by $x_1, \dots, x_m$. There is a maximal algebraically independent subset $\{x_i\}$. After relabeling it, we may write this set as $\{x_1, \dots, x_n\}$. Then each of $x_{n+1}, \dots, x_m$ is algebraic over $\mathbb{C}(x_1, \dots, x_n)$ so $K/\mathbb{C}(x_1, \dots, x_n)$ is finite. □

Proposition 11.2. *Let $K = \mathbb{C}(x_1, \dots, x_n)$ with $(x_1, \dots, x_n)$ algebraically independent, and let x_{n+1} be algebraic over K. Then*

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

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

In other words, $\mathbb{C}[x_1, \dots, x_{n+1}] = \mathbb{C}[\underline{X}]/I = \mathbb{C}[\underline{X}]/(f)$.

Proof. As $x_1, \dots, x_n$ are algebraically independent, the ring $R = \mathbb{C}[x_1, \dots x_n] \subset K$ is isomorphic to the polynomial ring $\mathbb{C}[X_1, \dots, X_n]$ so is a UFD. There exist polynomials in the ring $K[T]$ which have x_{n+1} as a root, and they form an ideal. Since $K[T]$ is a principal ideal domain, there is a unique generator $h(T)$ of this ideal whose leading coefficient is 1; it is the minimal polynomial from Galois theory.

Let b be the least common denominator of the coefficients of $h(T)$, which is an element in R. We know that bh is irreducible in $R[T]$ by Gauss's Lemma. Therefore $bh = f(x_1, \dots, x_n, T)$ for some irreducible $f \in \mathbb{C}[X_1, \dots, X_{n+1}]$.

We claim that this f generates the ideal in the proposition. Indeed, let g be an element of $\mathbb{C}[\underline{X}]$ such that $g(\underline{x})$ is 0. Therefore in the ring $K[T]$, the polynomial $g(x_1, \dots, x_n, T)$ is divisible by h. By once again applying Gauss's Lemma, we see that in fact f divides g. Therefore f must generate the ideal

For the last part, suppose $\{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{n+1}\}$ is not algebraically independent. Then there exists a polynomial g in the ideal I which does not involve X_i. However, we have shown that g is a nonzero multiple of f, so this is impossible. □

Corollary 11.3. *Let V be an irreducible variety. Then V is birational to a hypersurface.*

Proof. Let K be the function field $\mathbb{C}(V)$. By the discussion above we see that K is generated by elements $x_1, \dots, x_{n+1}$, where $x_1, \dots, x_n$ are algebraically independent, but x_{n+1} is algebraic over the pure transcendental $\mathbb{C}(x_1, \dots, x_n)$. The field K is the fraction field of the subring in K of polynomial expressions in $x_1, \dots, x_n$. By the discussion above, we see that we can write this subring as

$$K \supset \mathbb{C}[x_1, \dots, x_{n+1}] = \mathbb{C}[X_1, \dots, X_{n+1}]/(f),$$

where f is an irreducible polynomial; we remind the reader of the standard warning that $\mathbb{C}[x_1, \dots, x_{n+1}]$ is notation . Therefore K is the function field of $\mathbb{V}(f)$ and the result follows. □

We have already seen that birational varieties have the same dimension. We therefore have the following corollary.

Corollary 11.4. *Let W be an irreducible variety and let $V \subset \mathbb{A}^n$ be an affine hypersurface birational to W, with $V = \mathbb{V}(f)$ for f nonconstant. The dimension of W is equal to $n - 1$.*

In the language of field theory, the dimension of W is the transcendence degree of the field $\mathbb{C}(W)$.

12 Hilbert's Nullstellensatz

In this section we record the proof of Hilbert's Nullstellensatz in the case of affine varieties. The reduction of the projective statement to the affine statement has already been given.

We begin with the weak form of the result.

Theorem 12.1. *Every maximal ideal of $\mathbb{C}[\underline{X}]$ is of the form $(X_1 - a_1, \ldots, X_n - a_n)$ for $a_i \in \mathbb{C}$. Moreover, If I is a non-unit ideal in $\mathbb{C}[\underline{X}]$ then $\mathbb{V}(I)$ is non-empty.*

The most general form of the statement holds for polynomial rings over arbitrary algebraically closed fields. The uncountability of $\mathbb{C}$ offers a very slick proof, which we now outline. It is important for the proof to recognize if R is a quotient of the polynomial ring by an ideal, every element of R can be written as a $\mathbb{C}$-linear combination of monomial expressions in $a_1, \ldots, a_n$, where a_i is the image of X_i in R under the quotient. In more sophisticated language, the ring R is finitely generated as a $\mathbb{C}$-algebra.

Proof. It is clear that every ideal of the given form is maximal, since the quotient is automatically the field $\mathbb{C}$. Now let $\mathfrak{m} \subset \mathbb{C}[\underline{X}]$ be a maximal ideal, and consider the field K given by $\mathbb{C}[\underline{X}]/\mathfrak{m}$. Denote the coset $X_i + \mathfrak{m}$ by a_i. Then K is a field and every element of K can be obtained as a polynomial expression in the terms a_i with coefficients in $\mathbb{C}$. Now, if K is $\mathbb{C}$, then a_i must be in $\mathbb{C}$. In turn $X_i - a_i$ lie in $\mathfrak{m}$ and we conclude.

Otherwise, the containment $\mathbb{C} \subset K$ is strict. We can find $t \in K \setminus \mathbb{C}$. However since $\mathbb{C}$ is algebraically closed, the element t is transcendental over $\mathbb{C}$. Now let $U_m \subset K$ be the $\mathbb{C}$-vector subspace spanned by the products $\{a_1^{r_1} \cdots a_n^{r_n}\}$ with $\sum r_i \leq m$. Clearly the dimension of U_m is finite and and K is the union $\bigcup U_m$. Now $\{1/(t-c) \mid c \in \mathbb{C}\}$ are linearly independent over $\mathbb{C}$ (exercise!), so only finitely many of them can lie in each U_m. Therefore the number belonging to $K = \bigcup U_m$ is countable. As K is uncountable, we have a contradiction.

(ii) By the ascending chain condition for ideals, there exists a maximal ideal $\mathfrak{m}$ containing I. By the previous part, $\mathbb{V}(\mathfrak{m})$ is a point of $\mathbb{A}^n$, and therefore this point is contained in $\mathbb{V}(I)$. It follows that the vanishing set is nonempty. ☐

By the correspondence theorem in ring theory between ideals of quotients R/I and ideals of R that contain I we have the following corollary.

Corollary 12.2. *Let $V \subset \mathbb{A}^n$ be an affine variety and $\mathbb{C}[V]$ its coordinate ring. The maximal ideals of $\mathbb{C}[V]$ are in bijection with the points of V. If p is a point of V and $\mathfrak{m}_p$ is its associated maximal ideal, then evaluation at p gives a map*

$$\mathbb{C}[V] \to \mathbb{C}$$

which is naturally identified with the quotient

$$\mathbb{C}[V] \to \mathbb{C}[V]/\mathfrak{m}_p.$$

Remark 12.3. The corollary is conceptually clean, but in fact, it is more important than it initially seems. If you ask yourself the question, "what is the role of the prime ideals, rather than merely the maximal ideals?" you are led inevitably to the notion of a scheme.

The strong Nullstellensatz follows easily from the weak one, using a trick. The proof is non-examinable and will not be discussed in lecture, but is included for completeness.

Theorem 12.4. *Let V be an affine variety given by $\mathbb{V}(I)$. Then the ideal $I(V)$ coincides with the radical ideal of I.*

Proof. Let f be an element in $I(V)$. Consider the ideal $J \subset \mathbb{C}[X_1, \ldots, X_n, T]$ generated by the following elements:

(i) The elements if I under the obvious inclusion from $I(V)$ into $\mathbb{C}[X_1, \ldots, X_n, T]$.

(ii) The polynomial $1 - fT$.

Suppose we have a point $P = (a_1, \ldots, a_{n+1})$ in $\mathbb{V}(J)$. Then $f(a_1, \ldots, a_n) = 0$ since f is contained in I. However, additionally, we would have $1 - a_{n+1}f(\underline{a}) = 0$, which means there could not exist such a point. Therefore $V(J)$ is empty and by the Nullstellensatz above, J is the unit ideal $\mathbb{C}[\underline{X}, T]$. We can write the element 1 using the generators of the ideal J:

$$1 = \sum_{r=0}^{m} T^r h_r + (1 - fT)g$$

for some $h_r \in I$ and $g \in \mathbb{C}[\underline{X}, T]$. Now without any loss of generality, we can assume that m is at least the T-degree of g. Multiplying by f^m we have

$$f^m = \sum_{r=0}^{m} f^m T^r h_r + (1 - fT) f^m g(\underline{X}, T) = \sum_{r=0}^{m} f^{m-r} h_r (fT)^r + (1 - fT) g_1(\underline{X}, fT)$$

for some polynomial g_1. We now set $T = 1/f$ in this expression and therefore $f^m = \sum_{r=0}^{m} f^{m-r} h_r$, i.e. $f^m \in I$. □

13 Algebraic curves and their local structure

The basic theory of projective varieties has now been developed, and the next task is to see what this theory gives in the first case: algebraic varieties of dimension 1. By the discussion we have had, the dimension 1 can be interpreted as (i) the dimension of the tangent space at some (or by smoothness, every) point is 1, or (ii) that the function field is finite extension of the field $\mathbb{C}(t)$ of rational functions in 1 variable.

Important Convention on Terminology: Most frequently, we will discuss smooth, projective, irreducible curves. Therefore we adopt the convention that a curve is smooth, projective and irreducible of dimension 1 unless it is explicitly stated that the curve is singular, affine, or reducible.

Important Convention on Ambient Space: A projective curve by our definition comes as a subset $C \subset \mathbb{P}^n$. The ambient space will always be there, but note that it is certainly possible for $C \subset \mathbb{P}^n$ and $C' \subset \mathbb{P}^m$ to be isomorphic. The choice of ambient space will essentially never be important for us, so we will drop it from the notation.

Example 13.1. *We have a large supply of curves: take f_d to be a homogeneous degree d polynomial in X, Y, Z. If the coefficients are chosen generically, $\mathbb{V}(f_d)$ will be a smooth projective curve in $\mathbb{P}^2$. We will see that for distinct degrees $d, d' \geq 2$, smooth curves $\mathbb{V}(f_d)$ and $\mathbb{V}(f_{d'})$ will never be isomorphic. Therefore, even the geometry of $\mathbb{P}^2$ gives us infinitely many non-isomorphic curves. In fact, even if d and d' coincide, we can get non-isomorphic curves but this is not easy to show.*

We begin in earnest by understanding subvarieties of curves. Note that subvarieties are merely Zariski closed subsets.

Proposition 13.2. *Let C be a smooth projective irreducible curve and let $D \subset C$ be a proper closed subvariety. Then D is a finite union of points.*

Proof. It suffices to prove that if $V \subset \mathbb{A}^n$ is an irreducible affine curve, and if $W \subset V$ is a proper and irreducible subvariety, the W is a single point. We have a strict containment of $I(V)$inside $I(W)$ by the Nullstellensatz. Since $W \hookrightarrow V$ is a morphism, we have a homomorphism

$$\varphi^* \colon \mathbb{C}[V] = \mathbb{C}[\underline{X}]/I(V) \to \mathbb{C}[W] = \mathbb{C}[\underline{X}]/I(W)$$

obtained by restricting functions. If W is not a point, then $\mathbb{C}[W] \neq \mathbb{C}$. Now if t lies in $\mathbb{C}[W] \setminus \mathbb{C}$ then t is transcendental over $\mathbb{C}$. Now let x be a nonzero element of $\mathbb{C}[V]$ such that with $\varphi^*(x) = 0$, and let $y \in \mathbb{C}[V]$ with $\varphi^*(y) = t$. Then easy to see that x, y are algebraically independent. But this contradicts the fact that $\dim V = 1$. □

So now let $V \subset \mathbb{P}^n$ be an irreducible, possibly singular curve. We have the following basic structures associated to V. First, we have the function field $\mathbb{C}(V)$ of V. By the dimension 1 hypothesis on V, we know there exists $t \in \mathbb{C}(V)$ such that $\mathbb{C}(V)/\mathbb{C}(t)$ is a finite extension. The second structure we have is the local ring

$$\mathcal{O}_{V,P} = \mathcal{O}_P = \{f/g \mid g(P) \neq 0\} \subset \mathbb{C}(V)$$

at a point P in V. The unique maximal ideal $\mathfrak{m}_P$ is the set of elements on $\mathcal{O}_{V,P}$ that vanish at P.

Theorem 13.3. *If P is a smooth point of V then $\mathfrak{m}_P \subset \mathcal{O}_P$ is a principal ideal.*

Any π_P such that $\mathfrak{m}_P = (\pi_P)$ is called a local parameter at P.

Proof. Assume P lies in an affine piece $V_0 \subset \mathbb{A}^n$ of V and change coordinates to assume that $P = (0, \dots, 0)$. Then

$$\begin{aligned}
\mathbb{C}[V_0] &= \mathbb{C}[X_1, \dots, X_n]/I(V_0) = \mathbb{C}[x_1, \dots, x_n] \quad \text{where } x_i = \text{image of } X_i \\
\mathcal{O}_P &= \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[V_0],\ g \notin (x_1, \dots, x_n) \right\} \\
\mathfrak{m}_P &= \left\{ \frac{f}{g} \mid f \in (x_1, \dots, x_n),\ g \notin (x_1, \dots, x_n) \right\} \\
&= x_1 \mathcal{O}_P + \cdots + x_n \mathcal{O}_P
\end{aligned}$$

More generally, let $J \subset \mathcal{O}_P$ be any ideal, observe that a fraction f/g lies in J if and only if f lies in J. Indeed, in the ring $\mathcal{O}_P$ the element g is a unit. Therefore, we can write J in the form

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

and observe in particular that it is finitely generated by the Hilbert basis theorem.

As P is smooth, after change of coordinates we may identify

$$T_P = \{X_2 = \cdots = X_n = 0\}.$$

The main idea in the proof is to now show $\mathfrak{m}_P = (x_1)$. Since T_P is cut out by linearizations of polynomials in $I(V_0)$, and $X_2, \dots, X_n$ are such linearizations, it means there exist $f_2, \dots, f_n \in I(V_0)$ such that

$$f_j = X_j - h_j \quad (2 \leq j \leq n)$$

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

$$x_j = h_j(x_1, \dots, x_n) \in (x_1^2, x_1 x_2, \dots, x_n^2) = \mathfrak{m}_P^2, \quad (2 \leq j \leq n)$$

Thus

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

We now need to hope that this implies $\mathfrak{m}_P = (x_1)$.

Remark 13.4. The hope is reasonable geometrically: it is asking for a form of the inverse function theorem to hold. A form of the inverse function theorem does hold, and it is called Nakayama's Lemma. The statement will seem almost completely absurd at first, and may continue to do so for a long time. It is only after using the lemma a dozen times that one understands how and where to look for its use.

Lemma 13.5 (Nakayama's Lemma)**.** *Let R be a ring, let M a finitely generated R-module, and let $J \subset R$ be an ideal. Then:*

(i) If $JM = M$ the there exists an element r in J such that $(1 + r)M = 0$.

(ii) If $N \subset M$ be a submodule such that $JM + N = M$, then there exists r in J such that $(1+r)M \subset N$.

The result is belongs to commutative algebra, as does its proof. The proof will not be lectured and can be considered non-examinable. It is included for completeness in the notes.

Proof. (i) By the finite generation hypothesis, we have that $M = y_1R + \cdots + y_nR$, for elements y_i in $M = JM$. Then $y_i = \sum_{j=1}^{n} x_{ij}y_j$ with $x_{ij} \in J$. Let $X = (x_{ij})$, then have matrix equation $(I_n - X)\underline{y} = 0$. Multiply by adjugate of $(I_n - X)$ and we obtain $\det(I_n - X)f_i = 0\ \forall i$. Therefore $\det(I_n - X) = 1 + z$ for some $z \in J$ as claimed.

(ii) For this, simply apply (i) to the R-module M/N and use the correspondence theorems between submodules of modules and of their quotients. □

Returning to the proof of the theorem, we need now simply apply (ii) with

$$R = \mathcal{O}_P \supset J = \mathfrak{m}_P = M \supset N = (x_1).$$

□

The local parameter at a smooth point is not unique, but if π_P is one every other is of the form $u\pi_P$, $u \in \mathcal{O}_P^*$ a unit.

The proof gives a simple construction of local parameters in the situation of plane curves.

Proposition 13.6. *Let V be the affine plane curve $\mathbb{V}(f) \subset \mathbb{A}^2$ where f lies in $\mathbb{C}[X, Y]$. Let P be a smooth point on C. Then the function*

$$V \to \mathbb{C}$$

sending Q to $X(Q) - X(P)$ is a local parameter at P if and only if $(\partial f/\partial Y)(P) \neq 0$.

Proof. Simply run through the proof of the theorem above again; the $X(P)$ comes from the shift to the origin that happens at the start of the proof. □

The existence of local coordinates gives the crucial piece of structure that is the engine behind nearly every theorem on the geometry of curves. We think of this integer as the order of vanishing at the point P.

Corollary 13.7. *Let P be a smooth point of a (possibly singular but irreducible) curve V. Then there exists a surjective homomorphism $\nu_P \colon \mathbb{C}(V)^\star \to \mathbb{Z}$ (called the valuation at P) such that*

$$\mathcal{O}_P = \{0\} \cup \{f \in \mathbb{C}(V)^\star \mid \nu_P(f) \geq 0\}$$
$$\mathfrak{m}_P = \{0\} \cup \{f \in \mathbb{C}(V)^\star \mid \nu_P(f) > 0\}.$$

and if $f \in \mathbb{C}(V)^\star$ then for any local parameter π_P at P, we can write $f = \pi_P^{\nu_P(f)}u$ for some $u \in \mathcal{O}_P^\star$.

What is really going on here is that the ideals generated by π_P^n over all n filter the ring, and we're asking what the largest power is that contains a given element.

Proof. We know $\mathfrak{m}_P$ is principally generated and therefore is (π_P) for some local parameter. Therefore we also know that $\mathfrak{m}_P^n = (\pi_P^n)$. Now consider

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

As we saw in the previous proof, since $J \subset \mathcal{O}_P$ is an ideal it is finitely generated, and therefore we can see that

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

By applying Nakayama's Lemma again, we conclude that $J = 0$. Now for every f in $\mathcal{O}_P \setminus \{0\}$ there exists unique $n \geq 0$ such that $f \in \mathfrak{m}_P^n \setminus \mathfrak{m}_P^{n+1}$. Set $\nu_P(f) = n$. If f lies in $\mathbb{C}(V) \setminus \mathcal{O}_P$ then we claim that f^{-1} lies in $\mathcal{O}_P$. Indeed, writing f as a ratio g/h, by the discussion above we can write g and h respectively as $\pi_P^k u$ and $\pi_P^\ell u'$ where u and u' are units. Since f does not lie in $\mathcal{O}_P$, it follows that $k < \ell$. Now take reciprocals. Given this claim, we can now define $\nu_P(f) = -\nu_P(f^{-1})$. From the local ring property, we have $\mathcal{O}_P \setminus \mathfrak{m}_P = \mathcal{O}_P^*$ every nonzero element can be written as has $f = u\pi_P^n$, $n = \nu_P(f)$, where $u \in \mathcal{O}_P^*$. We have constructed the desired surjective homomorphism ν_P. □

By convention we write $\nu_P(0) = \infty$, so $\nu_P(f)$ is now defined for all rational functions. The construction is an instance of a general notion that arises everywhere in algebra and geometry. A discrete valuation ring or DVR is an integral domain with an element $t \neq 0$ such that every $0 \neq x \in R$ has a unique expression ut^n. A discrete valuation ring is a local principal ideal domain.

The local algebraic structure of curves has very concrete and useful consequences for geometry.

Corollary 13.8. *Let V be an irreducible curve, and let $f \in \mathbb{C}(V)$. If P is a smooth point of V, then one of f and f^{-1} is regular at P.*

Proof. An element f is regular at P if and only if its order of vanishing $\nu_P(f)$ is nonnegative. □

Corollary 13.9. *Let V be a projective nonsingular curve. Then any rational map $\varphi \colon V \dashrightarrow \mathbb{P}^m$ is a morphism.*

Proof. By reordering coordinates, we can assume that the image of φ isn't contained in $\{X_0 = 0\}$. Then we may write

$$\varphi = (G_0 : \ldots : G_m) = (1 : g_1 : \ldots : g_m)$$

with $g_i = G_i/G_0$ in $\mathbb{C}(V)$. If all $g_i \in \mathcal{O}_P$ then φ is regular at P. Otherwise let $t = \min\{\nu_P(g_i) \mid 1 \leq i \leq m\}$. This number is negative, but if we multiply through by a rational function the map is unchanged. Noticing that $\min\{\nu_P(\pi_P^{-t} g_i)\} = 0$, we conclude that $\varphi = (\pi_P^{-t} : \pi_P^{-t} g_1 : \cdots : \pi_P^{-t} g_m)$ is regular at P. □

14 Maps between curves

Now study morphisms between curves in more detail. They are extremely well-behaved, and easily accessible via field theory. Before beginning, let us record a couple of examples:

Example 14.1. *(i) Let $C_d \subset \mathbb{P}^2$ be a degree d smooth plane curve. Let P be a point in $\mathbb{P}^2$, either on or off C_d. Then projection from P gives rise to a morphism:*

$$C_d \to \mathbb{P}^1.$$

Note that what is a priori only a rational map is actually a morphism, due to the smoothness hypothesis and the results at the end of the previous section.

(ii) Consider the ring $R = \mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$. We can write R in the form $\mathbb{C}[\underline{X}]/I$ where I is some ideal. Therefore R determines an affine variety, and in fact a singular affine curve, up to isomorphism which we call C. In fact, we've seen this curve before; it's the <u>*cuspidal cubic*</u>*. The map of rings $R \to \mathbb{C}[t]$ then determines a morphism*

$$\mathbb{A}^1 \to C.$$

Visually, this is the map that takes the cusp and "pulls it taught" at the singular point. It is an example of a morphism that is actually injective and surjective but is not an isomorphism.

Proposition 14.2. *Let $\varphi\colon V \to W$ be a nonconstant morphism of irreducible, possibly singular curves.*

(i) For all $Q \in W$ the set $\varphi^{-1}(Q)$ is finite;

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

Proof. (i) $\varphi^{-1}(Q)$ is a closed subvariety of V, and therefore it is either V itself, or a finite set of points. Since the map is non-constant, it must be the latter.

(ii) The set V is infinite, since the dimension is positive. Now by (i) $\varphi(V)$ is infinite, therefore dense in W. Therefore φ is dominant and so $\varphi^*\colon \mathbb{C}(W) \to \mathbb{C}(V)$ is defined and automatically injective. Let $t \in \mathbb{C}(W) \setminus \mathbb{C}$, with $x = \varphi^*(t)$. Then since $\mathbb{C}(V)/\mathbb{C}$ is finitely generated and is finite over the degree 1 transcendental extension $\mathbb{C}(x)$, it is also finite over the intermediate extension $\varphi^*\mathbb{C}(W)$. □

The most important numerical invariant of a morphism of curves is its degree.

Definition 14.3. Let $\varphi : V \to W$ be a non-constant morphism of irreducible curves. The degree of the field extension $[\mathbb{C}(V) : \varphi^*\mathbb{C}(W)]$ is the <u>degree</u> $\deg(\varphi)$ of the morphism φ.

Remark 14.4. It is not immediate from our discussion, but we will soon see that the degree of a morphism can be calculated by choosing a sufficiently generic point on the target curve W and counting the elements in the preimage. This simple geometric idea motivates many of the statements and theorems, but the field extension provides a more flexible formalism.

Suppose $P \in V$ and $Q = \varphi(P) \in W$ are smooth points. We define the <u>ramification degree</u> of φ at P to be

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

for any local parameter π_Q on W at Q — note that this doesn't depend on the choice of local parameter. Let's see how this works in a simple example.

Example 14.5. *Consider the map $\varphi : \mathbb{A}^1 \to \mathbb{A}^1$ given on rings by the homomorphism*

$$\varphi^\star : \mathbb{C}[X] \to \mathbb{C}[X], \quad X \mapsto X^d.$$

The local parameter near 0 on the target is X, and therefore the ramification degree is just d.

The next theorem is key to the study of curves.

Theorem 14.6. *(i) Let $\varphi\colon V \to W$ be a morphism of* <u>*projective*</u> *possibly singular but irreducible curves. Then φ is surjective.*

(ii) If in addition V and W are smooth curves, then for any $Q \in W$,

$$\sum_{P \in V,\ \varphi(P)=Q} e_P = \deg(\varphi).$$

(iii) For all but finitely points P in V, we have $e_P = 1$.

The theorem is difficult, and we will not be able to prove it. We make several remarks on the proof though. First, we make the following definition.

Definition 14.7. A quasi-projective variety is a Zariski open subset U of a projective variety $V \subset \mathbb{P}^n$.

If $U \subset \mathbb{P}^n$ is an irreducible quasiprojective variety[11], rational functions and rational maps of quasi-projective varieties are defined in identical fashion to projective varieties. Indeed, if V is Zariski closure of U, then V is an irreducible projective variety. A rational map

$$U \dashrightarrow \mathbb{P}^m$$

is a rational map $V \dashrightarrow \mathbb{P}^m$ such that every point on U is in the domain. A good example of a quasi-projective variety are products $\mathbb{P}^n \times \mathbb{A}^m$, where the latter is given the topology as a subspace of $\mathbb{P}^n \times \mathbb{P}^m$, which in turn is give by the Segre embedding.

We return to the discussion of the theorem. Recall that a map of topological spaces is closed if the image of every closed set is closed. We will take the following fact on trust; its proof is not trivial but is also certainly not beyond your reach.

Proposition 14.8. *The projection map $\mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$ is a closed map.*

Once this is taken for granted the following result is straightforward.

Proposition 14.9. *Let $\varphi : X \to Y$ be a morphism of quasi-projective varieties and suppose X is proper. Then the image of φ is closed in Y.*

Proof. The first key idea is to factorize φ as follows:

$$X \to \Gamma_\varphi \subset X \times Y \to Y,$$

where Γ_φ is the graph:

$$\Gamma_\varphi := \{(x, \varphi(x))\} \subset X \times Y.$$

The second morphism is the projection. Now notice that the graph Γ_φ is closed: it is the preimage of the diagonal under the morphism:

$$\varphi \times 1 : X \times Y \to Y \times Y,$$

and the diagonal is Zariski closed (exercise!). Now, X sits inside $\mathbb{P}^n$ as a closed subset, so in fact, it would suffice to show that

$$\mathbb{P}^n \times Y \to Y$$

sends closed sets to closed sets. It would suffice to prove that for an open cover of Y by $\{U_i\}$, the projection

$$\mathbb{P}^n \times U_i \to U_i$$

[11] This is the most general instance of a variety that we will see; it is a very large class. In the modern world, a variety is still more general, and is defined as a scheme satisfying certain properties. It is hard to even prove that there exists a variety that is not quasi-projective, so we will not worry about this.

are closed maps for all i. Finally, each U_i actually sits inside an affine space, say $\mathbb{A}^m$ by definition. The way we have defined the topologies, it now reduces to showing that

$$\mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$$

is closed. We have asserted this already, and the result follows. $\square$

We now have as a corollary, the first claimed statement.

Corollary 14.10. *Let $\varphi\colon V \to W$ be a non-constant morphism of projective possibly singular but irreducible curves. Then φ is surjective.*

Proof. The image of φ is a closed and therefore either a point or W itself. Since the map is non-constant, we conclude. $\square$

Statement (ii) is sometimes called the finiteness theorem for curves. We will not include the proof in the lectures, and the material is non-examinable. I record a sketch of the proof for those who are interested.

Proof. (Non-examinable; sketch) We have $\mathbb{C}(W) \subset \mathbb{C}(V)$; rename the fields as $K \subset L$ for convenience. Now let A be the local ring $\mathcal{O}_{W,Q}$ and define B to be the intersection of $\mathcal{O}_{V,P}$ over all P in V mapping to Q. We have already seen that A is a local principal ideal domain, because Q is a smooth point on a curve. We have a homomorphism

$$A \to B$$

making B into a finitely generated A-module. Now observe that B is actually torsion-free as an A-module: if a is in A and b is in B such that ab is 0, then either a or b is 0. From the classification theorem for modules over a PID (i.e. the same theorem used to prove the classification of finitely generated abelian groups, and used to prove the existence of Jordan normal forms), we realize that B is $A^{\oplus r}$.

We now compute the rank r in two different ways; it is useful to know how to tensor modules over a ring for this, which is the real reason this proof is omitted, and why we only give a sketch. First we observe that it must be equal to $[L : K]$. On the other hand, if we reduce modulo the maximal ideal $\mathfrak{m}_Q$, it is straightforward to explicitly compute its dimension as a $\mathbb{C}$-vector space. These numbers are equal and give the formula. $\square$

Finally, we will prove statement (iii) a little later. The following is an important consequence:

Corollary 14.11. *Let V be a (smooth projective irreducible) curve and $f \in \mathbb{C}(V)^*$. Then:*

(i) If f regular for all $P \in V$ then $f \in \mathbb{C}$ is a constant function.

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

Proof. Given f, the trick is to consider

$$\varphi = (1 : f)\colon V \to \mathbb{P}^1$$

which is automatically a morphism. Now $\varphi(P)$ is the point $(0:1)$ if and only if f is not regular at P. But this immediately means that if f is regular everywhere, φ is not surjective, and therefore constant.

For (ii) we can assume that f is non-constant. Let t denote the rational function X_1/X_0. This is a local coordinate at the point $(1:0)$ in $\mathbb{P}^1$; for convenience we call this point 0. Now observe that $\varphi^\star t$ is precisely f. Therefore, if $f(P) = 0$ that implies that $e_P = \nu_P(\varphi^* t) = \nu_P(f)$. Similarly, $1/t$ is a local parameter near ∞, namely the point $(0:1)$, and a similar calculation shows that if $f(P) = \infty$ then

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

Finally, if $\varphi(P)$ is neither 0 nor ∞, then $\nu_P(f)$ is 0, and by the theorem above

$$\deg\varphi = \sum_{\varphi(P)=0} \nu_P(f) = \sum_{\varphi(P)=\infty} -\nu_P(f).$$

It follows immediately that $\sum_P \nu_P(f) = 0$. □

The statement is really saying that the number of zeroes and the number of poles of a rational function are the same, and that most points are neither.

15 Divisors theory on curves

For the rest of this course, curve will mean smooth, projective, irreducible curve, unless explicitly stated to the contrary.

We have seen have already seen that if V is a projective curve, then

$$\{\text{Everywhere regular functions on } V\} = \mathbb{C} \hookrightarrow \{\text{Rational functions on } V\} = \mathbb{C}(V).$$

The field $\mathbb{C}(V)$ is difficult to work with; as a $\mathbb{C}$-vector space it is infinite dimensional. We would like to cut it up into more manageable pieces. An element f determines a function on an open set

$$V \supset U \to \mathbb{C}$$

but we have no control over this U. It is better to remember more information. A simple minded fix is to fix a set of points $P_1, \dots, P_n$ on V and let U be the complement of $\{P_1, \dots, P_n\}$ and study functions that are regular on U. The notion of a divisor is a slightly better version of this idea.

Definition 15.1. A divisor on a curve V is a finite formal integer linear combination $\sum_{P\in V} n_P P$. The set of divisors can be identified with the group

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

If $D = \sum n_P P$ is a divisor, define the degree of the divos r as $\deg(D) = \sum n_P \in \mathbb{Z}$. The map $D \mapsto \deg(D)$ is homomorphism, whose kernel is denoted $\mathrm{Div}^0(V)$.

It is common to write $\nu_P(D)$ for the coefficient n_P of P in D.

The purpose of introducing divisors is that help to organize the vector space $\mathbb{C}(V)$.

Definition 15.2. Let D be a divisor. The space of rational functions with poles bounded by D is the set

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

If D is a divisor $\sum n_P P$ with all n_P non-negative, then $L(D)$ is the set of functions which have a pole of order no worse than n_P at the point P. If n_P is negative, then an element of $L(D)$ is forced to have a zero of order at least n_P at P.

A given rational function may lie in many different vector spaces $L(D)$. Nevertheless, given f in $\mathbb{C}(V)$, it lies in one natural space.

Definition 15.3. Let $f \in \mathbb{C}(V)^*$ be a nonzero rational function. Define the divisor of f to be

$$\operatorname{div}(f) = (f) := \sum_{P \in V} \nu_P(f) P.$$

Divisors of rational functions have degree 0, and are called principal divisors. They form a subgroup $\operatorname{Div}^0(V)$ whose quotient is the Picard group or Class group of V. If D and D' differ by a principal divisor, then they are said to be linearly equivalent.

Remark 15.4. Note that the Picard group and Class group grow into different incarnations in the study of general varieties and schemes, and only happen to coincide for smooth varieties. It's closely related to Poincaré duality. Note also that when V is higher dimensional, a divisor is a linear combination of codimension 1 subvarieties rather than points.

Proposition 15.5. *Every divisor of degree* 0 *on* $\mathbb{P}^1$ *is principal.*

Proof. Identify the points of $\mathbb{P}^1$ as $\mathbb{C}$ and the point ∞. Write the divisor as $D = \sum_{a \in \mathbb{C}} n_a(a) + n_\infty(\infty)$. As $\deg(D) = 0$, $n_\infty = -\sum n_a$. Let

$$f = \prod_{a \in k} (t-a)^{n_a}.$$

Then since $(t-a)$ is a local parameter at a and a unit at other points $b \neq a$, we see that $v_a(f) = n_a$. Since $1/(t-a)$ is a local parameter at ∞ for any a, $v_\infty(f) = -\sum n_a = n_\infty$. □

For a general curve V the degree homomorphism descends to a homomorphism $\operatorname{Cl}(V) \to \mathbb{Z}$. If V is isomorphic to $\mathbb{P}^1$ this homomorphism is an isomorphism. In fact, this characterizes $\mathbb{P}^1$ as we will see later.

The principal divisors are the simplest. We will see two other ways that divisors arise. The first is via hyperplane sections, and the second is via the theory of differentials.

Definition 15.6. Let $V \subset \mathbb{P}^n$ and consider a hyperplane $H = \mathbb{V}(L) \subset \mathbb{P}^n$ not containing V, defined by some linear form L. The hyperplane section of V by H is the divisor

$$\operatorname{div}(L) = \sum n_P P, \qquad \text{where if } X_i(P) \neq 0,\ n_P = \nu_P(L/X_i)$$

We take a moment to justify the well-definedness. If P is a point where both X_i and X_j are nonzero, we claim that the valuations of L/X_i and L/X_j coincide. Equivalently, our claim is that X_i/X_j is a rational function of valuation 0. However, since the rational function doesn't vanish at all, this is immediate.

Note also that this is a sum of points lying in $V \cap H$, because the n_P are necessarily positive.

Proposition 15.7. *Let* $V \subset \mathbb{P}^n$ *be a curve. Let* L *and* L' *be two linear forms, neither vanishing on* V*. Then there is an equality:*

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

In particular, the hyperplane sections of V *by* L *and* L' *have the same degree.*

Proof. Immediate from the definition. □

Definition 15.8. Let $V \subset \mathbb{P}^n$ be a curve. The degree of V is the degree of any hyperplane section of V.

Note that more generally, a hyperplane section can be defined for any non-constant morphism $\varphi : V \to \mathbb{P}^n$, without φ necessarily being an isomorphism onto its image. Let L be a linear form on $\mathbb{P}^n$. At a point P of V, choose i such that $X_i(P)$ is nonzero and take the divisor whose coefficient at such P is $\nu_P(\varphi^\star L/X_i)$.

If G is any homogeneous polynomial of degree m, then one can similarly define $\operatorname{div}(G)$ as a divisor on $V \subset \mathbb{P}^n$,

$$\operatorname{div}(G) = \sum n_P P, \qquad \text{where if } X_i(P) \neq 0,\, n_P = \nu_P(L/X_i^m)$$

If G is homogeneous of degree m, then $\operatorname{div}(G)$ is linearly equivalent to $m \times \operatorname{div}(L)$, where L is homogeneous of degree 1. Therefore, $\operatorname{div}(G)$ has degree md).

The following is a weak form of a beautiful theorem.

Theorem 15.9 (Bezout's Theorem, basic version)**.** *Two distinct irreducible plane curves of degrees m and n intersect in at most mn points.*

Proof. Suppose C and D are plane curves cut out as $\mathbb{V}(F)$ and $\mathbb{V}(G)$, with F and G irreducible homogeneous of degrees m and n. Then the the degree of $\operatorname{div}(G)$ on C is mn. In order to see this, notice that to calculate the degree, we can replace G by something linearly equivalent, such as the mth power of a linear homogeneous polynomial L. The number of intersection points with the vanishing locus of this linear L is at most n. The number of intersection points is at most the degree by the above discussion. ☐

Remark 15.10. There are two strengthenings of this. The first is that each intersection point can be given a positive multiplicity such that the sum of the intersection points with multiplicity is exactly mn. The proof is not so difficult, and can actually be extracted from what we've discussed already. The second is that if the curves are chosen generically then the number of intersection points is exactly mn.

A divisor $D = \sum n_P P$ is effective if $n_P \geq 0$ for all points P. We write this as $D \geq 0$. We introduced the vector spaces $L(D)$ earlier as functions with a certain property. We can also view it as a set of effective divisors.

$$\begin{aligned} L(D) &= \{f \in \mathbb{C}(V) \mid f = 0 \text{ or } \operatorname{div}(f) + D \geq 0\} \\ &= \{f \in \mathbb{C}(V) \mid \forall P \in V,\ \nu_P(f) + n_P \geq 0\} \quad \text{if } D = \sum_P n_P P. \end{aligned}$$

Proposition 15.11. *The set $L(D)$ is a complex vector space.*

Its dimension will be written $\ell(D)$.

Proof. if f and g are rational functions, observe that $\nu_P(f+g) \geq \nu_P(f) + \nu_P(g)$. It follows that sums of rational functions in $L(D)$ remain in $L(D)$. The remaining vector space axioms are obvious. ☐

Example 15.12. *Let ∞ denote the point $(0:1)$ on $V = \mathbb{P}^1$, and let $D = m(\infty)$. Writing $x = X_1/X_0$. Now observe that $L(D)$ is spanned by $1, x, \ldots, x^m$ so $\ell(D) = m + 1$.*

These numbers $\ell(D)$ for different divisors D are important invariants of a curve.

Proposition 15.13. *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, the vector space $L(D)$ is always finite dimensional.

Proof. (i) If $L(D) \neq 0$ then for $0 \neq f \in L(D)$, $\operatorname{div}(f) + D = E \geq 0$. But then $\deg(D) = \deg(E) \geq 0$ (as $\deg \operatorname{div}(f) = 0$).

(iii) Let $n = \nu_P(D)$. Define

$$e\nu_P\colon L(D) \to \mathbb{C}$$

by $e\nu_P(f) = (\pi_P^n f)(P)$. The kernel of this homomorphism is then $L(D-P)$ so $\ell(D-P) \geq \ell(D) - 1$.

(ii) now follows: if $d = \deg(D) \geq 0$ we see $\ell(D) \leq \ell(D-(d+1)P)+d+1 = d+1$ since $\deg(D-(d+1)P) = 0$. ☐

Proposition 15.14. *If D and E are linearly equivalent, i.e. they coincide in the group $Cl(V)$, then $L(D)$ and $L(E)$ are isomorphic and therefore $\ell(D)$ depends only on the class of D in the Class group.*

Proof. If $D - E$ is the principal, then there is some g such that $\operatorname{div}(g)$ is $D - E$. By sending f in $L(E)$ to fg in $L(D)$. ☐

More generally, there is a "multiplication":

$$L(D) \times L(E) \to L(D+E).$$

One instance of this occurs when we take a divisor D and consider $L(nD)$ for n in $\mathbb{Z}$. If D were effective then there is a natural object

$$A(D) := \bigoplus_{n\in\mathbb{N}} L(nD)$$

which is in fact a graded ring. It is often called the section ring.

16 Differentials on curves

The heart of the study of the geometry of algebraic curves is the following question. Given a divisor D on a curve V, what is the number $\ell(D)$ of meromorphic functions with poles bounded by D? More generally, one can ask for what integers ℓ and d does there exist a divisor of degree d on V such that $\ell(D) = \ell$. This is known as the Brill–Noether problem. It is a distilled down version of the following natural geometric questions.

(i) Let V be a curve. For what integers r and d does V admit a morphism

$$\varphi : V \to \mathbb{P}^r$$

of degree d, with $\operatorname{im}\varphi$ not contained in a hylperplane[12]?

(ii) Given curves V and W, for what integer d is there a non-constant morphism $V \to W$?

Note that if V is $\mathbb{P}^1$ the number $\ell(D)$ depends only on the degree of D.

The first landmark result that allows us to answer this question is the Riemann–Roch theorem and the related Riemann–Hurwitz theorem. An important lesson that was learned from computations – by Riemann and his student Roch – was that an important role is played by path integrals and a generalized residue theorem on the curve V in the Euclidean topology. Closely related: we need to know the genus of V. In essence we need to do calculus on V but purely with the tools of rings, fields, and modules.

Let $K/\mathbb{C}$ be a field extension. Informally, a differential is a finite $\mathbb{C}$-linear combination of formal symbols $x\ dy$ with x, y in K subject to the standard rules of calculus: (i) the $d(\cdot)$ expression should be linear for additive inputs in the argument, (ii) it should satisfy the Leibniz rule for multiplicative inputs in its argument, and (iii) it should output 0 for scalar inputs. Precisely:

[12]The hyperplane condition is only here to ensure that the problem is not stupidly solved by embedding smaller projective spaces linearly into larger ones

Definition 16.1. The space of differentials[13] $\Omega_{K/\mathbb{C}}$ is the quotient vector space M/N where

$$M = \big(K\text{-vector space generated by symbols } \delta x,\ x \in K\big)$$
$$N = \left(\begin{array}{l}\text{subspace generated by } \delta(x+y)-\delta x-\delta y,\ \delta(xy)-\\ x\,\delta y - y\,\delta x,\ \delta a \text{ for } x,\ y \in K,\ a \in \mathbb{C}.\end{array}\right)$$

and define dx to be the coset $\delta x + N$ in $\Omega_{K/\mathbb{C}}$.

The map $d\colon K \to \Omega_{K/\mathbb{C}}$ is the exterior derivative. It is linear over the scalar field $\mathbb{C}$.

We will write Ω_K for $\Omega_{K/\mathbb{C}}$ when the field $\mathbb{C}$ is clear from context, which is probably always will be.

Remark 16.2. It is sometimes useful to note that in fact the appropriate generality for the definition is the following. Let A and B be any commutative rings and let $\varphi : A \to B$ be a ring homomorphism. Then we can define the module of differentials of B over A (with φ implicit) in exactly the same way, by treating A as the "constants". The only reason we mention this is to convince the reader that the differentials are a piece of algebra always there to be considered, and therefore something useful may come from doing so.

A closely related notion is that of a derivation. We keep the notation above.

Definition 16.3. Let U be a K-vector space. A $\mathbb{C}$-linear transformation $D\colon K \to U$ is called a derivation if $D(xy) = xDy + yDx$.

Example 16.4. *The map $d\colon K \to \Omega_K$ is a derivation. The derivative map $d/dx\colon \mathbb{C}(x) \to \mathbb{C}(x)$ is also a derivation.*

The vector space Ω_K is the universal source of derivations, because we defined it to be. The following lemma is essentially a tautology but nevertheless can be fairly useful.

Lemma 16.5 (Universal property)**.** *A map $D\colon K \to U$ is a derivation if and only if there is a K-linear map $\lambda\colon \Omega_K \to U$ such that $\lambda(dx) = D(x)$ for all $x \in K$.*

In other words, every derivation on K factors (uniquely) through the external differentiation $d : K \to \Omega_K$.

Proof. If λ is such a K-linear map then certainly $D = \lambda \circ d$ is linear over $\mathbb{C}$ and $D(xy) = \lambda(d(xy)) = x\lambda(dy) + y\lambda(dx)$, by definition. Conversely, given a derivation $D\colon K \to U$, write $\Omega_{K/\mathbb{C}} = M/N$ as in the definition: i.e. M is the K-vector space of symbols δx and N is the relation set of linearity, Leibniz rule. Define a K-linear map $\hat{\lambda}\colon M \to U$ by $\delta y \mapsto D(y)$ for all $y \in K$. Then as D is a derivation it follows that $\hat{\lambda}(N) = 0$ so we get a K-linear map λ as required. □

For any derivation, and therefore for d in particular, if $y \neq 0$ then $Dx = D(y(x/y)) = yD(x/y) + (x/y)Dy$ so the the quotient rule from calculus holds $D(x/y) = y^{-2}(yDx - xDy)$. We use this in the following lemma, which is a generation result for Ω_K.

Lemma 16.6. *(i) Let $f = g/h$ in $\mathbb{C}(X_1, \dots, X_n)$ be a rational function in n variables and write and $y = f(x_1, \dots, x_n) \in K$ as a rational expression in elements x_i in K. Then $dy = \sum_i (\partial f/\partial X_i)(x_1, \dots, x_n)\, dx_i$.*

(ii) If $K = \mathbb{C}(x_1, \dots, x_n)$ for $x_i \in K$ then $\{dx_i\}$ spans Ω_K.

Proof. (i) follows from the calculus rules for $d(xy)$, $d(x/y)$ and complex linearity linearity. (ii) is an immediate consequence. □

[13] In the literature you will often find these under the name Kähler differentials. It is well-recorded that Kähler was an unapologetic Nazi, and since there's no mathematical benefit to keeping his name in front of the term differentials, the instructor has decided to excise it.

When K is the function field of an algebraic curve, in fact Ω_K is a 1-dimensional vector space over K. We will prove this below, but please keep in mind that we should not conflate this one dimensional vector space with K – there is no field structure on Ω_K.

Theorem 16.7. *Let $K/\mathbb{C}(t)$ a finite extension with t transcendental over $\mathbb{C}$. Then $\Omega_{K/\mathbb{C}}$ is one-dimensional, spanned by dt.*

Proof. First suppose $K = \mathbb{C}(t)$. Then the lemma above, the vector space $\Omega_{K/\mathbb{C}}$ is generated by dt so has dimension ≤ 1. It is now enough to show it is nonzero. By the universal property of Ω_K discussed above, it enough to show there is a non-zero derivation $K \to K$, and d/dt is one.

For the general case, write $K_0 = \mathbb{C}(t)$ so that $K = K(\alpha) = \mathbb{C}(t, \alpha)$ by the primitive element theorem. Let $h \in K_0[X]$ be the minimal polynomial of α. Then $h'(\alpha) \neq 0$ by minimality. Again by the lemma above, Ω_K is spanned by dt and $d\alpha$. If for $f \in K_0[X]$ we write $D_t f = \partial f/\partial t$ (i.e. apply d/dt to the coefficients of f), then the first part of the lemma gives

$$0 = d(h(\alpha)) = (D_t h)(\alpha)dt + h'(\alpha)d\alpha$$

so Ω_K is spanned by dt. It therefore is enough to show $\Omega_K \neq 0$, or equivalently to write down a none-zero derivation $K \to K$.

The point is now that we already know what this derivation does to K_0, and we just need to extend to the elements that involve α. Since the field K is presented as a quotient, we first define a "ring derviation" $D\colon K_0[X] \to K$ by

$$D(f) = D_t(f) \text{ if } f \in K_0, \quad D(X) = -\frac{(D_t h)(\alpha)}{h'(\alpha)}, \quad D(X^n) = n\alpha^{n-1}D(X).$$

Then $D(h) = D_t(h)(\alpha) + h'(\alpha)D(X) = 0$, so for any $f \in K_0[X]$, $D(fh) = f(\alpha)D(h) + h(\alpha)D(f) = 0$. So D vanishes on the ideal $hK_0[X] \subset K_0[X]$, hence descends to a derivation $\bar{D}\colon K = K_0[X]/(h) \to K$, whose restriction to K_0 is D_t, hence is non-zero. □

In our situation V is a curve, and K above will be the field of rational functions $\mathbb{C}(V)$. A rational differential on V is an element of $\Omega_{\mathbb{C}(V)}$, and the latter will be denoted Ω_V for convenience. A differential is regular at P for a point P on V if it can be expressed as

$$\omega = \sum_i f_i dg_i$$

where f_i and g_i are regular as rational functions at P. The module of differentials that are regular at P is the subset

$$\Omega_{V,P} = \{\omega \in \Omega_V : \omega \text{ is regular at } P\}.$$

The subset is not a vector space over $\mathbb{C}(V)$, but the condition of regularity is preserved by multiplication by $\mathcal{O}_{V,P}$.

We recall that the key to producing divisors out of rational functions was that we could measure the order of vanishing of a rational function at a point. In turn, the key structure was the fact that in $\mathcal{O}_{V,P}$ was that the maximal ideal was principal.

Theorem 16.8. *$\Omega_{V,P}$ is the free $\mathcal{O}_{V,P}$ module generated by $d\pi_P$ for any local parameter π_P at P, i.e.*

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

We come to the proof in a moment, but let us look at the structure that this reveals. If π'_P is another local parameter, then we have $d\pi'_P = ud\pi_P$ where $u \in \mathcal{O}^*_{V,P}$. More generally, if ω is a rational differential form, we know that $\pi^k_P\omega$ is regular for some k. Given this, we can always write ω as $fd\pi_P$ where f is a rational function. We have our new source of divisors.

Definition 16.9. If ω is a rational differential on V and P is a point on V, define $\nu_P(\omega) = \nu_P(f)$ where $\omega = fd\pi_P$.

By the last remark this doesn't depend on the choice of local parameter, and $\nu_P(\omega) \geq 0$ if and only if ω is regular at P.

Lemma 16.10. *Let $\omega \in \Omega_V$ be a nonzero differential on a curve V. Then $\nu_P(\omega) = 0$ for all but finitely many P.*

Proof. As $\nu_P(f\,dg) = \nu_P(f) + \nu_P(dg)$ and $\nu_P(f) = 0$ for all but finitely many P, it's enough to consider $\omega = dg$. Moreover, since g must be transcendental in order to have any contribution to the divosor, we see that $\mathbb{C}(V)/\mathbb{C}(g)$ is finite.. Now consider $\varphi = (1 : g)\colon V \to \mathbb{P}^1$. By the finiteness theorem, there are only finitely many $P \in V$ with $g(P) = \infty$ or $e_P > 1$. If P is a point without ramification (i.e. ramification index 1) then $\varphi^\star(t - g(P))$ is a local parameter, but this is just $g - g(P)$. We now see that $\nu_P(dg) = 0$. $\square$

Definition 16.11. If ω is a rational differential on V, define $\operatorname{div}(\omega)$ as

$$\operatorname{div}(\omega) = \sum_{P \in V} \nu_P(\omega).$$

The differentials are well-behaved from our point of view.

Proposition 16.12. *If ω and ω' are nonzero rational differentials on V, then*

$$\operatorname{div}(\omega) - \operatorname{div}(\omega')$$

is principal.

Proof. Since Ω_V is a 1-dimensional vector space, we can write $\omega = f\omega'$. It is essentially immediate from the definitions that $\operatorname{div}(\omega) - \operatorname{div}(\omega')$ is the divisor of f. $\square$

As a consequence, the divisor of a rational differential is well-defined as a class in the Picard group of V. Any divisor of the form $\operatorname{div}(\omega)$ is called a canonical divisor[14]. The class is called the canonical class and is typically denoted K_V.

We come to the proof of the proposition.

Proof of Theorem 16.8. We want to check that $d\pi_P$ generates a module over a ring, and therefore we are going to use Nakayama's lemma. Obviously $\mathcal{O}_P d\pi_P \subset \Omega_P$. Given any 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 applying the Leibniz rule we have $df = gd\pi_P + \pi_P dg \in \mathcal{O}_P d\pi_P + \pi_P\Omega_P$. Therefore

$$\mathcal{O}_P d\pi_P \subset \Omega_P \subset \mathcal{O}_P d\pi_P + \pi_P\Omega_P$$

and then applying Nakayama's Lemma with $R = \mathcal{O}_P$, $J = \mathfrak{m}_P$, $M = \Omega_P \supset N = \mathcal{O}_P d\pi_P$, we get $\Omega_P = \mathcal{O}_P d\pi_P$. The only tricky thing to check is that Ω_P is finitely generated as a module over $\mathcal{O}_P$.

[14]Notice the absurdly non-canonical use of the word canonical. The canonical object is really the class in the Picard group.

Choose an affine piece $V_0 \subset \mathbb{A}^n$ of V containing P, so that $\mathbb{C}[V_0] = \mathbb{C}[x_1, \ldots, x_n]$, where these x_i generate $\mathbb{C}[V_0]$ as an algebra over $\mathbb{C}$. If $f \in \mathcal{O}_P$ then $f = g(\underline{x})/h(\underline{x})$ for polynomials g, h with $g(P) \neq 0$, and then

$$df = \sum \frac{h\partial g/\partial X_i - g\partial h/\partial X_i}{h^2}(\underline{x})dx_i$$

by the quotient rule. Since h does not vanish at P, the expression preceding dx_i is in $\mathcal{O}_P$. Therefore $\{dx_i\}$ generate Ω_P. as a module over $\mathcal{O}_P$. □

It may seem superficially that the construction above is identical to getting divisors from rational functions. Indeed, at each point, a differential $fd\pi$ contributes $\nu_P(f)$ to the divisor. But the key is that although at every point the constructions look the same, differentials transform in a different way when we move between points on a curve. This is especially visible in the following.

Example 16.13. *Let V be $\mathbb{P}^1$ and let t be the coordinate on the standard affine $\mathbb{A}^1 \subset \mathbb{P}^1$. Consider the differential dt. At any point a, with $a \in \mathbb{C}$, the function $t - a$ is a local parameter. Since dt and $d(t - a)$ coincide, the divisor has no support any such point. At ∞, the function $\frac{1}{t}$ is a local parameter. By calculus, $dt = -t^2 d(1/t)$, so $v_\infty(dt) = v_\infty(t^2) = -2$. Therefore $\mathrm{div}(dt) = -2(\infty)$ is a canonical divisor.*

The canonical divisor is the route to the genus in algebraic geometry.

Definition 16.14. Let V be a curve. The genus of V is the quantity $\ell(K_V)$ where K_V a canonical divisor on V. It is denoted $g(V)$.

We notice immediately, and as a sanity check, that $g(\mathbb{P}^1) = 0$. Crucially, we notice that K_V cannot be principal! In particular, the divisor of a rational differential genuinely gives a new source of divisors.

17 Differentials on plane curves

The purpose of this section is to convince you that although calculations with differentials are slightly esoteric, and involve a lot of bookkeeping, they really are very concrete – as long as the curve is concrete. The most concrete curves are plane curves.

We first show that there exists a curve of genus 1, and thereby for the first time in this course, show that there exist non-isomorphic algebraic curves! We phrase it as an example.

Example 17.1. *Smooth plane cubics have genus 1. Consider $V = \mathbb{V}(F)$ plane cubic, with*

$$F = X_0 X_2^2 - \prod_{i=1}^{3}(X_1 - \lambda_i X_0),$$

with $\lambda_i \neq \lambda_j$ if $i \neq j$. The curve is nonsingular. Suppose the affine equation is given by

$$f(x, y) = y^2 - \prod(x - \lambda_i) = y^2 - g(x).$$

By differentiating this equation, we observe the following basic relation on V:

$$2y\, dy = g'(x)\, dx \text{ in } \Omega_V.$$

By using this relation, and by using the fact that we understand local parameters on smooth plane curves we will compute the genus. We begin with a well-chosen differential.

Consider the differential ω given by dx/y. We will compute its divisor and use the above relation to show that it is 0. In order to do this, we will need a supply of local parameters. If P is a point with non-zero

y-coordinate in $\mathbb{A}^2$, then $\partial f/\partial y(P)$ is nonzero so $x - x(P)$ is a local parameter by what we have discussed previously. In this case ω contributes 0 to the divisor.

Similarly, one sees that if $y(P)$ is 0, then $x(P)$ is λ_i. But now $\partial f/\partial x$ is equal to $-g'(\lambda_i)$, which is nonzero. It follows that y is a local parameter. The differential dx/y can be expressed as $2dy/g'(x)$ so $\nu_P(\omega)$ is once again 0.

There is one final point, which is the point $(0:0:1)$. Now use the affine patch X_2 is nonzero. If we use coordinates z and t, then the equation becomes

$$z = \prod_i (t - \lambda_i z).$$

At the point $(0,0)$ on the curve, the rational function t is a local coordinate, since the z-derivative of the equation does not vanish. On the other hand, the t-derivative of f does vanish at $(0,0)$. Therefore z vanishes to order at least 2. Therefore $(t - \lambda_i z)$ vanishes to order 1, and therefore $\nu_P(z)$ is 3. Finally by using basic calculus, observe that $dx/y = d(1/t)/(z/t) = -(t^3/z)dt$ and $\nu_P(\omega) = 0$.

The example has the following consequence.

Theorem 17.2. *Let V be a smooth cubic plane curve. Then V has genus 1, and in particular, it is not isomorphic to $\mathbb{P}^1$.*

We will now generalize this to general plane curves, and try to understand their canonical divisors.

Theorem 17.3. *Let $V = \mathbb{V}(F) \subset \mathbb{P}^2$ 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. The strategy is the same as the example calculation we have done previously: we choose an appropriate differential ω, and then use the equation F to obtain different expressions of ω. We use what we know about local parameters of plane curves to calculate the divisor of ω.

I Selecting a Differential: First choose coordinates so $(0:1:0)$ is not in V. Let $x = X_1/X_0$, $y = X_2/X_0$. We view them as rational functions on V. Setting $f(X,Y)$ to be $F(1,X,Y)$, we see that $f(x,y)$ is 0. Differentiating this expression moves it from a relation between elements in $\mathbb{C}(V)$ to a relation in Ω_V. Explicitly, the exterior derivative gives

$$(\partial f/\partial X)(x,y)\,dx + (\partial f/\partial Y)(x,y)\,dy = 0$$

in Ω_V. We now choose our differential to be:

$$\omega = \frac{dx}{(\partial f/\partial Y)(x,y)} = -\frac{dy}{(\partial f/\partial X)(x,y)}$$

e will now calculate to show that $\operatorname{div}(\omega)$ is $(d-3)\operatorname{div}(X_0)$, where $\mathbb{V}(X_0)$ is the line H at infinity, which would give the theorem.

II Calculation in a Patch: We first do the calculation in $\mathbb{A}^2 \subset \mathbb{P}^2$. Let P be a point in $V \cap \mathbb{A}^2$. If $(\partial f)/\partial Y)(P) \neq 0$, then $x - x(P)$ is a local parameter at P. We therefore find

$$\nu_P(\omega) = \nu_P(1/(\partial f)/\partial Y)(P)) = 0.$$

Otherwise, we have $(\partial f)/\partial X)(P) \neq 0$. In this case $y - y(P)$ is a local parameter and we similarly have $\nu_P(\omega) = 0$.

III Calculation at Infinity: We now know that the divisor is supported on the line at infinity. Since $(0:1:0)$ is not contained in V, any point at infinity is contained in the $\{X_2 \neq 0\}$. On this open set, we can rewrite the equation of the curve as follows. The equation is given by $g(z,w) = 0$, with

$$z = X_0/X_2 = 1/y, \quad w = X_1/X_2 = x/y$$

and $g(Z,W) = F(Z,W,1) \in \mathbb{C}[Z,W]$.

Now consider a new differential $\eta = dz/(\partial g/\partial W)(z,w) = -dw/(\partial g/\partial Z)(z,w)$. This is not meant to be the same differential as ω!

The preceding argument shows that $\nu_P(\eta) = 0$ for any P in this the affine piece $\{X_2 \neq 0\}$. But $f(X,Y) = Y^d g(1/Y, X/Y)$ so $\partial f/\partial X = Y^{d-1}(\partial g/\partial V)(1/Y, X/Y)$ and we have

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

If $X_2(P) \neq 0$, then we can calculate $\nu_P(\omega) = (d-3)\nu_P(z) + \nu_P(\eta) = (d-3)\nu_P(z)$. Since $z = X_0/X_2$, this means $(\omega) = (d-3)\mathrm{div}(X_0)$ as claimed. □

We can go a step further and write a basis for the space of differentials on a plane curve of degree d.

Proposition 17.4. *If $f(x,y) = 0$ is an affine equation for for a smooth projective plane curve $V \subset \mathbb{P}^2$, and assume the degree is at least 3. Then*

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

is a basis for the vector space $L(K_V)$, where K_V is the canonical divisor given by $(d-3)H$.

Proof. Omitted; the result follows from the preceding proof and a linear independence argument for the terms $x^r y^s$. If these were not independent, then a linear combination of them would be zero on the curve, which contradicts the fact that V is irreducible of degree d. □

Corollary 17.5. *If d, d' are distinct integers larger than 2, then no two smooth plane curves of degrees d and d' are isomorphic. In particular, there exist infinitely many non-isomorphic algebraic curves.*

18 The Riemann–Roch theorem and consequences

Let V be a smooth projective algebraic curve. We have define the genus of V to be the dimension $\ell(K_V)$ of the space of regular differential forms. We have seen that $\mathbb{P}^1$ has genus 0 and that smooth plane cubics have genus 1. We have also seen that the degree of the canonical divisor of a plane curves grows linearly with the degree of the curve.

Theorem 18.1 (Riemann-Roch)**.** *Let g be the genus of V, and $K = K_V$ a canonical divisor. For any divisor D,*

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

The proof is beyond the scope of the course. I will say a word about the proof, after recording the following elementary consequence.

Corollary 18.2. *Let K be a canonical divisor on a curve V. Then* $\deg(K) = 2g-2$.

Proof. Take $D = K$ so that $\ell(D) = \ell(K) = g$ and $\ell(K-D) = \ell(0) = 1$. □

Remark 18.3. Many readers will have seen this number $2g-2$ before. It is the negative of the number of poles of a vector field on an orientable topological surface of genus g. You may also have seen it as the topological Euler characteristic of such a surface. The amazing fact about the Riemann–Roch theorem is that the left hand side and the right hand side have different natures. The left hand side involves functions, differentials, and the algebraic structure of a curve. The right hand side is "topological": the degree is just the number of points and g is the genus. In this sense, Riemann–Roch has a geometric left hand side and a topological right hand side. In this guise, it is part of a much larger family of results. The theorem can be viewed as a version of the Gauss–Bonet theorem, and both of them are a special case of the Atiyah–Singer index theorem. Another result that you should have nearby in your mind is the residue theorem.

Remark 18.4. In order to get a flavour for the result[15], we record a proof of Riemann–Roch in a special case, which the instructor learned from notes of Joe Harris. Suppose that D is an effective divisor, given by $p_1 + \cdots + p_n$ and K_V is a representative of the canonical divisor such that $K_V - D$ is also effective. Let us also assume the points are distinct, so $L(D)$ are functions with a pole of order at most 1. Suppose we know that $\deg(K)$ is $2g-2$ already; this can be deduced independently.

Given a rational function f, there is a residue of f at p_i. Let z_i be a local coordinate near p_i. For a regular function regular at p_i, we can extract a power series expressing the function in terms of z_i. For the constant term we look at the image of f under the evaluation map at p_i. For the next term, subtract off a constant term to make the function 0 at p_i. We now divide out by z_i and evaluate at p_i to extract the linear coefficient. Proceeding inductively, and working formally with ratios of power series, we extract a Laurent series. Since the coefficients of p_i in D is 1, the power series only goes to z_i^{-1} and no lower. Call the coefficient of z_i^{-1} in this power series the residue.

We have a linear map $L(D) \to \mathbb{C}^n$ given by taking the residue at p_i in each factor. The kernel is precisely $\mathbb{C}$, i.e. the constant functions: if there are no poles at any p_i the function must be constant.

There is also a linear map $L(K) \to \mathbb{C}^n$. First, we have differentials dz_i for each p_i. Given ω, the ratio ω/dz_i is a rational function. The rational function can be evaluated at p_i. Now notice that the kernel is $L(K-D)$.

The next step is to show that the images of these two maps under the map to $\mathbb{C}^n$ are orthogonal. The simplest way to see this is to use the Stokes theorem and Cauchy's theorem. Replacing the divisor D with $K-D$ and repeating the argument, the standard inequalities for dimensions from linear algebra and the degree of K being $2g-2$ gives us the Riemann–Roch theorem.

Corollary 18.5. *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 $(d-3)$ multiplied by the degree of V. The rest is numerics. □

Another corollary of Riemann–Roch is that the calculation of $\ell(D)$ is straightforward for "most D".

Corollary 18.6. *If the degree of D is larger than $2g-2$ then $\ell(D)$ is $\deg(D) - g + 1$.*

Divisors of small degree, relative to the genus, are "special". In fact, we define a divisor D to be special if $\ell(K-D)$ is nonzero. The first two examples of special divisors are (i) the trivial divisor $D = 0$, and (ii) the canonical divisor $D = K_V$.

We know everything there is to know about $\mathbb{P}^1$. The next case up is curves of genus 1.

Corollary 18.7. *If $g(V) = 1$ then if $\deg(D) > 0$ then $\ell(D) = \deg(D)$.*

[15] Perhaps more accurately, after three years of teaching this course without being able to prove Riemann–Roch for students who attend it, the instructor's frustration boiled over into the following multi-paragraph rant.

Proof. $\ell(K - D) = \ell(-D) = 0$. □

We certainly do not know everything there is to know about genus 1 curves! Let us say a word or two about their basic structure. Fix $P_0 \in V$. The pair (V, P_0) or, for brevity, just V itself, is called an elliptic curve. Traditionally we write E instead of V.

Let P, Q be points on E. Then by the Riemann–Roch theorem, we have $\ell(P + Q - P_0) = 1$. Therefore, there is a unique effective divisor of degree 1, i.e. a point which we'll call R, such that $P + Q - P_0 \sim R$. In other words, once we've chosen a basepoint,

We define:

$$\boxed{P +_E Q = R}$$

(It would perhaps be more correct, but over-pedantic, to write $P +_{(E,P_0)} Q$.)

The result is variety that is simultaneously an abelian group.

Theorem 18.8. *The operation $+_E$ makes E into an abelian group, with identity element P_0. Moreover the map $P \mapsto [P - P_0] \in \mathrm{Cl}(E)$ is an isomorphism of groups between E and $\mathrm{Cl}^0(E)$, the groups of divisor classes of degree 0 on E.*

Proof. Let $\beta(P) = [P - P_0] \in \mathrm{Cl}^0(E)$. We first show that β is a injection. If we have $\beta(P) = \beta(Q)$ that implies that $P - P_0 \sim Q - P_0$ in the class group, and therefore that $P \sim Q$. However, since $\ell(P) = 1$, the only functions that are allowed a potential pole at P are the constants. It follows that P and Q must coincide, so β is injective.

Now consider surjectivity. Let D be a divisor of degree 0, that we want to show has the class of $P - P_0$, for some P. If D is a divisor of degree 0 then as $\ell(D + P_0) = 1$ there exists P with $D + P_0 \sim P$, so $[D] = \beta(P)$. Therefore β is a bijection (of sets). Finally, if $P +_E Q = R$ then $\beta(P +_E Q) = [R - P_0] = [P + Q - P_0 - P_0] = [P - P_0] + [Q - P_0] = \beta(P) + \beta(Q)$. So β transforms $+_E$ into addition in $\mathrm{Cl}^0(E)$, and therefore $(E, +_E)$ is a group and β is an isomorphism. □

Theorem 18.9. *Let (E, P_0) be the plane curve given by the vanishing of*

$$F = X_0 X_2^2 - \prod_{i=1}^{3} (X_1 - \lambda_i X_0).$$

with λ_i distinct complex numbers. Choose P_0 to be the point $(0:0:1)$. Then the equation $P +_E Q +_E R = 0_E$ if and only if P, Q, R are collinear.

Proof. Observe that $P +_E Q +_E R = 0_E$ if and only if $P + Q + R \sim 3P_0$. In turn, this holds if and only if there exists a rational function f such that the divisor of f is $P + Q + R - 3P_0$. Now, by a similarly calculation to the previous cubic plane curve calculation, if x and y are the functions X_1/X_0 and X_2/X_0 have a pole of order at most 3 at P_0. By a similarly calculation to the example in the previous section, they have different orders of vanishing. By Riemann–Roch $\ell(3P_0)$ is 3 and $L(3P_0) = \langle 1, x, y \rangle = \langle 1, X_1/X_0, X_2/X_0 \rangle$. Therefore, the function f must be of the form $f = G/X_0$ for a linear form G with the divisor $\mathrm{div}(G)$ being $P + Q + R$. □

The group law is really very concrete and geometric. Although the statement of Riemann–Roch may seem rather abstract, its consequences are really concrete and beautiful statements. Another instance is the Riemann–Hurwitz formula.

Let $\varphi \colon V \to W$ be a finite morphism of curves. What is the relation between the genus of V and the genus of W?

Let $\omega = f\,dt$ be an element in Ω_W, where $\mathbb{C}(W)/\mathbb{C}(t)$ exhibits $\mathbb{C}(W)$ as a finite extension. Then $\mathbb{C}(V)/\varphi^\star(\mathbb{C}(t))$ is also finite. In particular, Ω_V is generated by $d\varphi^\star(t)$. Define

$$\varphi^\star(\omega) = \varphi^\star(f)\,d\varphi^\star(t).$$

Let P be a point on V and let $Q = \varphi(P)$. We will compare $\nu_P(\varphi^\star(\omega)$ and $v_Q(\omega)$. Let e_P be the ramification degree of φ at P, and π_P, π_Q local parameters.

Lemma 18.10. *We have $\nu_P(\varphi^\star(d\pi_Q)) = e-1$, where e is the ramification of φ at P. More generally, $\nu_P(\varphi^\star\omega) = e\nu_Q(\omega) + e - 1$.*

Proof. Write ω as $u \cdot \pi_Q^n\,d\pi_Q$. The pullback is a ring homomorphism so it suffices to understand how the individual pieces pull back. The units pull back to units so can be ignored. The term π_Q pulls back to a unit multiple of π_P^e. The result now applies from the formal rules of calculus that we have established. □

The Riemann–Hurwitz formula is a beautiful consequence, obtained by taking degree for the divisor obtained by pulling back a differential.

Theorem 18.11 (Riemann-Hurwitz formula)**.** *Let $\varphi\colon V \to W$ be a finite morphism of curves in characteristic zero. Let $n = \deg(\varphi)$. Then*

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

Proof. Let $0 \neq \omega \in \Omega_W$. Then

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

□

A beautiful consequence is the following.

Corollary 18.12. *Let V and W be curves with $g(W)$ larger than $g(V)$. Then any morphism $V \to W$ is constant.*

Another one is the following.

Corollary 18.13. *Let V be a product of two curves of genus at least 1. Then V is smooth and projective, and contains no subvariety isomorphic to $\mathbb{P}^1$.*

As an aside, products of curves are excellent examples of higher dimensional algebraic varieties. The current course will only discuss curves. Algebraic surfaces are much more complicated, but between products of curves and hypersurfaces in $\mathbb{P}^3$, one sees a large sweep of the phenomena that the general theory of surfaces exhibits.

Notice that if V is a curve that admits a degree 1 morphism to $\mathbb{P}^1$, then V must in fact be $\mathbb{P}^1$. Essentially the same fact tells us that if D is the divisor P for a point P on V, then $\ell(D)$ is necessarily 1. The simplest divisors on curves of positive genus have degree 2. They have a special name.

19 Equations for curves via Riemann–Roch

Let $V \subset \mathbb{P}^m$ be a curve, not contained in any hyperplane, and let $D = \mathrm{div}(X_0)$. Let $G \in \mathbb{C}[\underline{X}]$ be a nonzero linear form, and consider $f = G/X_0 \in \mathbb{C}(V)^*$. Then $\mathrm{div}(f) + D = \mathrm{div}(G) \geq 0$, hence $f \in L(D)$. Thus we get an injective linear map

$$\boxed{\beta\colon \{\text{Linear Homogeneous Polynomials}\} \hookrightarrow L(D), \qquad G \mapsto G/X_0}$$

Let us make two observations about this to motivate what is to come. Suppose P and Q are points fo V. Then

(i) There exist linear forms F and G such that $F(P) \neq 0$ and $G(P) = 0$, but with $G(Q) \neq 0$. In other words, $\beta(F)$ is a an element of $L(D)$ not vanishing at P, and $\beta(G)$ is an element of $L(D-P)$ not vanishing at Q.

(ii) Since P is a smooth point, we can find its tangent line L, which is a line inside $\mathbb{P}^m$. We can find a linear form F such that $F(P)$ is 0, but F does not vanish on all of L.

($\star$) We deduce that D satisfies the following condition. For every P, Q on V, we have $\ell(D-P-Q) = \ell(D) - 2$.

Definition 19.1. Let V be a curve and D a divisor with $\ell(D) = n + 1 \geq 2$. Let $B = \{f_0, \ldots, f_n\}$ be a basis for $L(D)$. The morphism associated to D with respect to B is given by

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

We say that φ_D is an embedding if it is an isomorphism from V to its image. The morphism φ_D with respect to a different basis B' is related by a linear transformation of $\mathbb{P}^n$.

If the precise choice of basis is not important, we will just refer to φ_D without basis as the morphism associated to D.

The reason for our two key observations is that they precisely characterize an embedding. The following theorem is very useful, but the proof will be omitted.

Theorem 19.2. *The morphism φ_D associated to D is an embedding if and only condition ($\star$) holds.*

For example, the following corollary tells us that every genus g curve can be embedded into the same projective space.

Corollary 19.3. *Suppose D has degree larger than $2g$, then φ_D is an embedding.*

Proof. The proof follows immediately from Riemann–Roch. Indeed, D and $D - P - Q$ both have large degree, so Riemann–Roch controls the spaces $L(-)$ as having dimension $d - g + 1$ exactly. The condition ($\star$) is a consequence. □

The equations for curves that come out of Riemann–Roch are typically not explicit. If E is an elliptic curve however, this can be made very concrete.

Theorem 19.4. *Let E be an elliptic curve with basepoint P_0. Then the divisor $3P_0$ gives an embedding of E as a cubic in $\mathbb{P}^2$.*

We have already seen that every plane cubic is a genus 1 curve. The above result gives the converse.

Proof. We already know from Riemann–Roch that $L(3P_0)$ is 3. Let x and y be non-constant functions. Since $L(2P_0)$ contains a non-constant function, but $L(P_0)$ does not, we can assume that x lies in $L(2P_0)$ but y does not. In other words, at P_0 the valuation of x is -2 while the valuation of y is -3. This gives a morphism

$$(1 : x : y) : E \to \mathbb{P}^2.$$

It is an embedding by the discussion above. In order to get equations for the image, we need to consider powers of x. The function x^2 lies in $L(4P_0)$ and in fact

$$L(4P_0) = L(3P_0) \oplus \mathbb{C}x^2.$$

Similarly, xy is in $L(5P_0)$. But now y^2 and x^3 are both in $L(6P_0)$ but not in $L(5P_0)$. Therefore there is a linear dependence in $L(6P_0)$ between $1, x, x^2, x^3, xy, y^2$. The linear equation gives rise to a cubic equation for E after homogenizing. Let F be the resulting equation. We obtain a morphism

$$\varphi : V \to \mathbb{V}(F) \subset \mathbb{P}^2.$$

Since φ is an embedding and V is a curve of genus 1, this can only happen if $\mathbb{V}(F)$ is smooth and is equal to the image of V. □

In particular, the divisor $2K_V$ for V a curve of genus g at least 3 gives an embedding of V into projective space of dimension $3g-4$. In genus 2, we can take $3K_V$ instead. This "gives equations" for curves in the same projective space.

Corollary 19.5. *Every curve of genus g can be embedded in $\mathbb{P}^m$ for some number m depending only on g.*

Proof. Take m to be $\ell(2K_V)$ for g at least 3 and $\ell(3K_V)$ for g equal to 2. □

In fact, the following theorem seems stronger but is actually less useful.

Theorem 19.6 (Non-examinable)**.** *Every curve can be embedded in $\mathbb{P}^3$.*

Let V be a curve of genus at least 1. Then it cannot admit a degree 1 morphism to $\mathbb{P}^1$, or equivalently, it cannot have a divisor D of degree 1 and $\ell(D) \geq 2$. A simple claim, which is left as an exercise shows that it would have to be isomorphic to $\mathbb{P}^1$.

Definition 19.7. A curve V of genus $g > 1$ is hyperelliptic is there exists $\pi \colon V \to \mathbb{P}^1$ of degree 2.

If V is hyperelliptic as above, then we can consider the divisor $D = \pi^*(\infty)$. The space $L(D)$ has dimension at least 2, since it contains the constant functions, as well as the pullback of X_1/X_0. We claim that it is exactly 2. Indeed, if D is $P+Q$ then $\ell(P)$ is 1 because V is not isomorphic to $\mathbb{P}^1$. Therefore $\ell(D)$ is at most 2.

Theorem 19.8. *(i) Let $g(V) > 1$. If there exists an effective divisor D of degree 2 on V with $\ell(D) = 2$ then $\pi = \varphi_D \colon V \to \mathbb{P}^1$ has degree 2, $\pi^\star(\infty) = D$ and V is hyperelliptic.*

(ii) Every curve of genus 2 is hyperelliptic.

(iii) There exist hyperelliptic curves of every genus at least 2.

Proof. (i) The statement will be assigned as an exercise.

(ii) If $g = 2$ then $\ell(K) = 2 = \deg(K)$, which gives thr result.

(iii) By using the degree-genus formula for $\mathbb{P}^1 \times \mathbb{P}^1$, a bidegree $(d, 2)$ curve on $\mathbb{P}^1 \times \mathbb{P}^1$ has genus $d-1$. The projection onto the second factor gives a morphism to $\mathbb{P}^1$ of degree 2. □

Hyperelipticity of a curve is very closely controlled by the properties of K_V.

Theorem 19.9. *Suppose V is not hyperelliptic. Then $\varphi_K : V \to \mathbb{P}^{g-1}$ is an embedding.*

Proof. Suppose φ_K were not an embedding. Then K must violate condition $(\star)$ above. As a consequence, there must exist points P and Q such that $\ell(K - P - Q)$ is at least $g - 1$. But by Riemann–Roch that means $D = P + Q$ has $\ell(D)$ at least 2. $\square$