# Algebraic Geometry

March 11, 2020

0 Introduction

What is algebraic geometry? Broadly speaking, it is the study of the geometry of solutions to systems of polynomial equations. For example, in $\mathbb{R}^2$, if we have the set X of solutions to $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, then we know that this set forms a circle, and we know lots of geometric facts about circles. If we take a more complicated function, such as $y^2 = x^3 - x$, we get something that looks like:
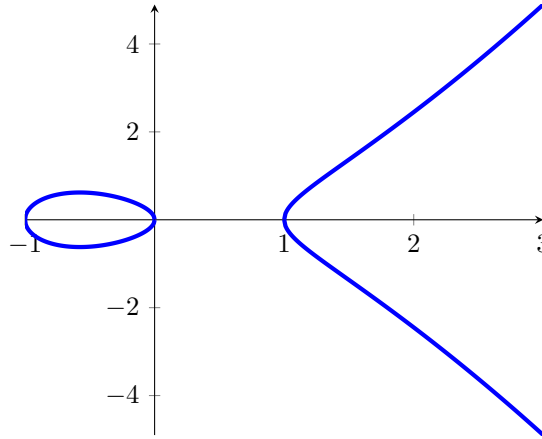
If we instead think about complex solutions, we get something of the form of a torus minus a single point, with another rich geometric structure.

In $\mathbb{C}^3$, if $X = \{(x, y, z) \in \mathbb{C}^3 : x^3 + y^3 + z^3 = 1\}$, then X contains 27 lines: $x = -\xi^m y, z = \xi^n$ for $i, j \in \{0, 1, 2\}$ gives 9 of them, and the other 18 come by rotating x, y, z in this linear system.

In $\mathbb{R}^3$, consider the equation $1 + x^3 + y^3 + z^3 = (1 + x + y + z)^3$.

1 Basic Setup

Fix a field K. We define an ***affine n-space over K*** to be $\mathbb{A}^n := K^n$. Let $A := K[x_1, x_2, \ldots, x_n]$ be the polynomial ring in n variables over K, and let $S \subseteq A$ be a subset of A. We then define $\mathbb{V}(S)$, the ***vanishing locus of S*** to be the set of all n-tuples $(a_1, \ldots, a_n) \in \mathbb{A}^n$ where $f(a_1, \ldots, a_n) = 0$ for all $f \in S$.

Proposition 1.1.

1. $\mathbb{V}(\{0\}) = \mathbb{A}^n$

2. $\mathbb{V}(A) = \emptyset$

3. $\mathbb{V}(S_1 \cdot S_2) = \mathbb{V}(S_1) \cup \mathbb{V}(S_2)$, where $S_1 \cdot S_2 = \{f_1 \cdot f_2 : f_1 \in S_1, f_2 \in S_2\}$.

4. Let I be an index set, $S_i \subseteq A$ for each $i \in I$. Then $\bigcap_{i \in I} \mathbb{V}(S_i) = \mathbb{V}(\bigcup_{i \in I} S_i)$

Proof. 1., 2. are obvious

1. If $p \in \mathbb{V}(S_1) \cup \mathbb{V}(S_2)$, then either $p \in \mathbb{V}(S_1)$ or $p \in \mathbb{V}(S_2)$. If $p \in \mathbb{V}(S_1)$, then $f_1(p) = 0$ for all $f_1 \in S_1$, and so $f_1(p) \cdot f_2(p) = 0$ for all $f_1 \in S_1, f_2 \in S_2$, so $p \in \mathbb{V}(S_1 \cdot S_2)$, and similarly for if $p \in \mathbb{V}(S_2)$.

   Conversely, suppose that $p \in \mathbb{V}(S_1 \cdot S_2)$, and $p \notin \mathbb{V}(S_1)$. Then there is some $f_1 \in S_1$ with $f_1(p) \neq 0$. But $f_1(p) \cdot f_2(p) = 0$ for all $f_2 \in S_2$, and so $f_2(p) = 0$ for all $f_2 \in S_2$), so $p \in \mathbb{V}(S_2)$.

2. If $p \in \mathbb{V}(S_i)$ for all $i \in I$, then $f_i(p) = 0$ for all $f_i \in S_i$, and so for all $f \in \bigcup_i S_i$, so $p \in \mathbb{V}(\bigcup_{i \in I} S_i)$.

   Conversely, if $p \in \mathbb{V}(\bigcup_i S_i)$, then $f(p) = 0$ for all the polynomials in $\bigcup_i S_i$, and so $p \in \bigcap_i S_i$.

   $\square$

These four properties should remind you of the four axioms for a topology.

A subset of $\mathbb{A}^n$ is ***algebraic*** if it of the form $\mathbb{V}(S)$ for some $S \subseteq A$. A ***Zariski open set*** in $\mathbb{A}^n$ is a set of the form $\mathbb{A}^n \setminus \mathbb{V}(S)$ for some $S \subseteq \mathbb{A}^n$. This proposition tells us that the Zariski open sets define a topology on $\mathbb{A}^n$, called the ***Zariski topology***.

Examples:

1. $K = \mathbb{C}$. The Zariski open (or closed) subsets of $\mathbb{C}^n = \mathbb{A}^n$ are in particular open (or closed) in the usual Euclidean sense, but not vice versa.

2. For any K, consider $\mathbb{A}^1, A = K[x], S \subseteq K[x]$. If S has a non-zero element, then $\mathbb{V}(S)$ is finite. Thus the closed sets are the finite subsets of $\mathbb{A}^1$, and all of $\mathbb{A}^1$. The open sets are $\emptyset$ and all the co-finite sets (i.e. sets with finite complement).

Recall that, if A is any commutative ring with $S \subseteq A$ a subset, then the ***ideal generated by S*** is the ideal $A \supseteq \langle S \rangle = \{\sum_{i=1}^q f_i g_i : q \geq 0, f_i \in S, g_i \in A\}$, or the smallest ideal of A containing S.

Lemma 1.2. *Let $S \subseteq A = K[x_1, \ldots, x_n]$. Then $\mathbb{V}(S) = \mathbb{V}(\langle S \rangle)$.*

Proof. If $p \in \mathbb{V}(S)$, then for $f_1, \ldots, f_q \in S; g_1, \ldots, g_q \in A$ we have:

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

So $p \in \mathbb{V}(\langle S \rangle)$, and so $\mathbb{V}(S) \subseteq \mathbb{V}(\langle S \rangle)$.

The other inclusion follows from the fact that $S \subseteq \langle S \rangle$, we must have $\mathbb{V}(\langle S \rangle) \subseteq \mathbb{V}(S)$. $\square$

Let $X \subseteq \mathbb{A}^n$ be a subset. Define $I(X) := \{f \in A : f(p) = 0 \ \forall p \in X\}$, the **ideal of X**. Note that $I(X)$ is indeed an ideal, since if $f, g \in I(X)$ then $f + g \in I(X)$, and if $f \in I(X), g \in A$, then $f \cdot g \in I(X)$. Note that if $S_1 \subseteq S_2 \subseteq A_1$, then $\mathbb{V}(S_2) \subseteq \mathbb{V}(S_1)$, and if $X_1 \subseteq X_2$, then $I(X_2) \subseteq I(X_1)$.

The **radical** of an ideal $I \subset A$ is the set $\sqrt{I} := \{x \in A : \exists \, n \in \mathbb{N} \text{ s.t. } x^n \in I\}$. This is defined in general for any commutative ring A, not just polynomial rings.

Lemma 1.3. $\sqrt{I}$ *is an ideal.*

Proof. If $f, g \in \sqrt{I}$, there is n, m such that $f^n, g^m \in I$. Then $(f+g)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} f^i g^{m+n-i}$. Now for each term in this sum, either we have $i \geq n$ or $m + m - i \geq m$, and so one of these terms is in I. Hence by the closure rules for ideals, $(f + g)^{m+n} \in I$, so $f + g \in \sqrt{I}$. Given $f \in \sqrt{I}, g \in A$, we have $(fg)^n = f^n g^n$, and $f^n \in I \implies f^n g^n \in I$, so $fg \in \sqrt{I}$. $\square$

Proposition 1.4.

1. *If $X \subseteq \mathbb{A}^n$ is algebraic, then $\mathbb{V}(I(X)) = X$.*

2. *If $I \subseteq A$ is an ideal, then $I(\mathbb{V}(I)) \supseteq \sqrt{I}$.*

Proof.

1. Since X is algebraic $X = \mathbb{V}(I)$ for some $I \subseteq A$. Certainly $I \subseteq I(X)$, and so $\mathbb{V}(I(X)) \subseteq \mathbb{V}(I) = X$. But $X \subseteq \mathbb{V}(I(X))$ trivially, and so $X = \mathbb{V}(I(X))$.

2. If $f \in \sqrt{I}$, then $f^n \in I$ for some n, and so f^n vanishes on $\mathbb{V}(I)$, thus f vanishes on $\mathbb{V}(I)$. Hence $f \in I(\mathbb{V}(I))$.

$\square$

Theorem 1.5 (Hilbert Nullstellensatz)**.** *Let K be algebraically closed. Then $I(\mathbb{V}(I)) = \sqrt{I}$.*

Proof. Deferred until later. $\square$

Example: If $K = \mathbb{R}$, $I = \langle x^2 + y^2 + 1 \rangle \subseteq \mathbb{R}[x, y]$, then $\mathbb{V}(I) = \emptyset$, so $I(\mathbb{V}(I)) = \mathbb{R}[x, y] \neq \sqrt{I}$.

We define an **affine (algebraic) variety** to be an algebraic subset of $\mathbb{A}^n$. Very often we can decompose affine varieties into smaller subsets. For instance, $\mathbb{V}(\langle xy \rangle) = + = - \cup | = \mathbb{V}(\langle x \rangle) \cup \mathbb{V}(\langle y \rangle)$. If $Y \subseteq X$ is a non-empty closed subset, then we say Y is **irreducible** if whenever $Y = Y_1 \cup Y_2$ with Y_1, Y_2 closed, then either $Y_1 = Y$ or $Y_2 = Y$. In the Euclidean topology on $\mathbb{C}^n$, the irreducible subsets are single points, but under the Zariski topology they are much more interesting. We will now turn to the question of identifying when an algebraic set is irreducible.

Proposition 1.6. *If $X_1, X_2 \subseteq \mathbb{A}^n$, then $I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.*

Proof. Since $X_1, X_2 \subseteq X_1 \cup X_2, I(X_1 \cup X_2) \subseteq I(X_1), I(X_2)$. Hence $I(X_1 \cup X_2) \subseteq I(X_1) \cap I(X_2)$.

Conversely, if $f \in I(X_1) \cap I(X_2)$, then f vanishes on both X_1 and X_2, and so on all of the union. So $I(X_1) \cap I(X_2) \subseteq I(X_1 \cup X_2)$. $\square$

Recall that an ideal $P \subseteq A$ of a commutative ring is said to be **prime** if it is not the whole ring, and whenever $fg \in P$, either $f \in P$ or $g \in P$.

Lemma 1.7. *Let $P \subseteq A$ be prime, and $I_1, \ldots, I_n \subseteq A$ be ideals. Suppose that $P \supseteq \bigcap_i I_i$. Then there is some i such that $P \supseteq I_i$, and if equality holds in either then it holds in both.*

Proof. Suppose $P \not\supseteq I_i$ for any i, so for all i there is some $x_i \in I_i \setminus P$. Then $x = \prod_i x_i \in I_i$ for all i, so $x \in \bigcap_i I_i$ and hence $x \in P$. But then some $x_i \in P$ because P is prime. ↯

If we have equality, then $P \subseteq I_i$ for all i, and by above there is some i for which $P \supseteq I_i$, so $P = I_i$. □

Proposition 1.8. *Let K be algebraically closed. Then an algebraic set $X \subseteq \mathbb{A}^n$ is irreducible if and only if $I(X)$ is prime.*

Proof.

$\implies$ If $f \cdot g \in I(X)$, then $X \subseteq \mathbb{V}(f \cdot g) = \mathbb{V}(f) \cup \mathbb{V}(g)$. So $X = (X \cap \mathbb{V}(f)) \cup (X \cap \mathbb{V}(g))$. Irreducibility implies that WLOG $X = X \cap \mathbb{V}(f)$, i.e. $X \subseteq \mathbb{V}(f)$ as $\mathbb{V}(f), \mathbb{V}(g), X$ are closed. Then $f \in I(X)$, and so $I(X)$ is prime.

$\impliedby$ If P is prime with $\mathbb{V}(P) = X_1 \cup X_2$, X_1, X_2 closed. Then $I(X_1) \cap I(X_2) = I(X_1 \cup X_2) = I(\mathbb{V}(P)) = \sqrt{P}$ by the Nullstellensatz. But if $f^n \in P$, then $f \in P$, and so $\sqrt{P} = P$. Hence $I(X_1) \cap I(X_2) = P$, and $P = I(X_1)$ or $I(X_2)$, so $\mathbb{V}(P) = X_1$ or X_2.

□

So if K is algebraically closed, then we have a one-to-one correspondence between algebraic subsets and radical ideals, and between irreducible algebraic subsets and prime ideals. This correspondence suggests that, just as prime ideals are the "building blocks" of ideals, so too are irreducible varieties the building blocks of algebraic sets.

Proposition 1.9. *Any algebraic set is a finite union of irreducible varieties.*

Proof. Let $\mathcal{S}$ be the set of non-empty closed subsets of $\mathbb{A}^n$ which cannot be written as a finite union of irreducible subsets. Suppose $\mathcal{S} \neq \emptyset$. Then we claim $\mathcal{S}$ has a minimal element with respect to inclusion.

If not, then there is an infinite descending chain of elements of $\mathcal{S}$, say, $X_1 \supsetneq X_2 \supsetneq \ldots$. If $I_j = I(X_j)$, then we get an *ascending* chain of ideals $I_1 \subsetneq I_2 \subsetneq \ldots$. But since $K[x_1, \ldots, x_n]$ is Noetherian (proven in IB GRM), every ascending chain of ideals is eventually stationary. ↯ .

Let $Y \in \mathcal{S}$ be a minimal element. Since $Y \in \mathcal{S}$, Y is not irreducible, and so $Y = Y_1 \cup Y_2$, with $Y_1, Y_2 \neq Y$. Since $Y_i \subsetneq Y$ and Y is minimal in $\mathcal{S}, Y_i \notin \mathcal{S}$, and so can be written as a finite union of irreducible closed subsets. But then Y can also be written as a finite union of irreducible closed subsets. □

If $Y = \bigcup_{i=1}^n Y_i$, with Y_i irreducible varieties, $Y_i \subseteq Y_j$ for $i \neq j$, then $Y_i, \ldots, Y_n$ are the **irreducible components** of Y.

Example: $\mathbb{V}(xy) = \mathbb{V}(x) \cup \mathbb{V}(y)$. Note that $\mathbb{V}(x)$ is irreducible because (x) is a prime ideal in $K[x, y]$ - to see this observe $K[x, y]/(x) \cong K[y]$ is an integral domain. So the irreducible component of $\mathbb{V}(xy)$ are $\mathbb{V}(x)$ and $\mathbb{V}(y)$, or the two coordinate axes.

Proposition 1.10. *The irreducible components of Y are unique up to ordering.*

Proof. Exercise. □

Example: $A = K[x_1, \ldots, x_n]$ is a unique factorisation domain (UFD). If $f \in A \setminus \{0\}$, then f is irreducible if and only if (f) is prime. If instead, $f = f_1 \ldots f_n$ is a factorisation into irreducible components, then $\mathbb{V}(f) = \mathbb{V}(f_1) \cup \ldots \cup \mathbb{V}(f_n)$ is the irreducible decomposition of $\mathbb{V}(f)$.

For instance, $\mathbb{V}(y^2 - x^3 + x)$, the diagram on the first page of these notes, is irreducible.

2 Regular and Rational Functions

In algebraic geometry we are interested in polynomial functions, i.e. $f : \mathbb{A}^n \to K$ for some $f \in A = K[x_1, \ldots, x_n]$. Then, given $X \subseteq \mathbb{A}^n$ closed, we get $f|_X : X \to K$. Note that if there are $f, g \in A$ with $f|_X = g|_X$, then $(f - g)|_X = 0$, and so $f - g \in I(X)$.

Let $X \subseteq \mathbb{A}^n$ be an affine variety. We define the ***coordinate ring*** of X to be $A(X) \coloneqq A/I(X)$. The lecturer also uses the notation $K[X]$ to mean the same thing. I'm not sure why, but if you ever think we're doing some sort of polynomial ring in an affine variety, it's probably because of this.

If X is irreducible and $U \subseteq X$ is open, then a ***regular function*** on U is a function $f : U \to K$ such that, for every $p \in U$, there is an open neighbourhood $p \in V \subseteq U$, and functions $g, h \in A(X)$, with $h(q) \neq 0$ for all $q \in V$ and $f = g/h$ on V, i.e. everywhere in U it is *locally* a ratio of two polynomials.

Examples:

1. $f \in A(X)$ induces $f|_U : U \to K$, which is $f/1$ on U and so regular.

2. If $U \subseteq \mathbb{A}^1$, $U = \mathbb{A}^1 \setminus \{0\}$. Then $g(x)/x^n$ is a regular function on U for any polynomial g.

We write for $U \subseteq X$ open, $\mathcal{O}_X(U) \coloneqq \{f : U \to K : f \text{ a regular function}\}$. Note that $\mathcal{O}_X(U)$ is a ring, i.e. sums, products, and differences of regular functions are regular. $\mathcal{O}_X(U)$ is also a K-algebra, so we can multiply by scalars in K.

Lemma 2.1. $\mathcal{O}_X(X) = A(X)$ *if K is algebraically closed.*

Proof. Deferred until after Hilbert's Nullstellensatz. □

Recall that, if A is an integral domain, then we define the ***field of fractions*** of A to be $\left\{ \frac{f}{g} : f \in A, g \in A \setminus \{0\} \right\} / \sim$, with $\frac{f}{g} \sim \frac{f'}{g'}$ if $fg' = f'g$. This is, as the name would suggest, a field.

If $X \subseteq \mathbb{A}^n$ is an irreducible variety, then we define the ***function field*** of X to be the field of fractions of $A(X)$. We denote this $K(X)$. Note that $A(X)$ is an integral domain if and only if X is irreducible. Then $f \in K(X)$ can be written as $f = \frac{g}{h}$ for $g, h \in A(X)$, and this is a regular function on $X \setminus \mathbb{V}(h)$.

3 Morphisms

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

1. f is continuous in the Zariski topology (i.e. the induced topologies on X and Y)

2. For all open $V \subseteq Y$ and for any regular function $\varphi : V \to K$, the map $\varphi \circ f : f^{-1}(V) \to K$ is also regular.

The lecturer appreciates that this is a conceptually difficult definition, but has no idea how to make it clearer.

If $f : X \to Y$ is a morphism, then for any $\varphi \in A(Y), \varphi \circ f$ is a regular function on X, and hence $\varphi \circ f \in A(X)$ by **2.1**. This defines a map $f^{\#} : A(Y) \to A(X); \varphi \mapsto \varphi \circ f$.

Note that $f^{\#}$ is a K-algebra homomorphism:

- $f^{\#}(\varphi_1 + \varphi_2) = (\varphi_1 + \varphi_2) \circ f = \varphi_1 \circ f + \varphi_2 \circ f = f^{\#}(\varphi_1) + f^{\#}(\varphi_2)$.

- $f^{\#}(\varphi_1 \cdot \varphi_2) = f^{\#}(\varphi_1) f^{\#}(\varphi)$

- For $a \in K$, $f^{\#}(a \cdot \varphi) = f^{\#}(a) f^{\#}(\varphi) = a f^{\#}(\varphi)$

Theorem 3.1. *There is a one-to-one correspondence between morphisms $f : X \to Y$ of affine varieties and K-algebra homomorphisms $f^{\#} : A(Y) \to A(X)$.*

Proof. We've seen how to get $f^{\#}$ from f. So now suppose we have $f^{\#} : A(Y) \to A(X)$ a K-algebra homomorphism given. Suppose $X \subseteq \mathbb{A}^n, Y \subseteq \mathbb{A}^m$. Then:

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

Let $\bar{y}_i$ be the element of $A(Y)$ represented by y_i, and let $f_i = f^{\#}(\bar{y}_i) \in A(X)$.

Then let $f : X \to \mathbb{A}^m$ be given by $f(p) = (f_1(p), \ldots, f_m(p))$. We claim that the image of f lies in Y.

We have the maps $K[y_1, \ldots, y_m] \xrightarrow{\text{quotient map}} A(Y) \xrightarrow{f^{\#}} A(X)$ given by $y_i \mapsto \bar{y}_i \mapsto f_i$, and so $g \mapsto g(f_1, \ldots, f_m)$.

Then since $g \in I(Y)$, we have $g(f_1, \ldots, f_m) = 0$ in $A(X)$, and so in particular, evaluating at p, we get $g(f_1(p), \ldots, f_m(p)) = 0$ as desired. Note that if $\varphi \in A(Y)$ we can write $\varphi = \bar{g}$ for some $g \in K[y_1, \ldots, y_m]$, and then $f^{\#}(\varphi) = g(f_1, \ldots, f_m) \in A(X)$. Hence f is a map from X to Y.

Next, we must show that $f : X \to Y$ is a morphism.

For continuity, we show that if $Z \subseteq Y$ is closed, then $f^{-1}(Z) \subseteq X$ is closed. For this, note $I(Z) \supseteq I(Y)$, and write $\overline{I(Z)}$ for the image $I(Z)/I(Y)$ in $A(Y)$. This is the ideal of regular functions on Y vanishing on Z.

$$\begin{aligned}
\mathbb{V}(f^{\#}(\overline{I(Z)})) &= \{p \in X : g(p) = 0 \forall g \in f^{\#}(\overline{I(Z)})) \subseteq A(X)\} \\
&= \{p \in X : (h \circ f)(p) = 0 \forall h \in \overline{I(Z)}\} \\
&= \{p \in X : f(p) \in \mathbb{V}(\overline{I(Z)})\} \\
&= \{p \in X : f(p) \in Z\} \\
&= f^{-1}(Z)
\end{aligned}$$

If I denotes the inverse image of $f^{\#}(I(Z))$ under the quotient map $K[x_1, \ldots, x_n] \to A(X)$. Then $\mathbb{V}(I) = \mathbb{V}(f^{\#}(\overline{I(Z)}))$, and in particular $f^{-1}(z)$ is closed.

If $\varphi \in \mathcal{O}_Y(U)$, i.e. $\varphi : U \to K$ is regular, we need to show that $\varphi \circ f : f^{-1}(U) \to K$ is regular. Let $p \in f^{-1}(U)$. Then there exists a neighbourhood $V \subseteq U$ of $f(p)$ on which $\varphi|_V = \frac{g}{h}$ for $g, h \in A(Y)$ with h non-vanishing on V.

Then $(\varphi \circ f)|_{f^{-1}(V)} = \varphi|_V \circ f = \frac{g}{h} \circ f = \frac{g \circ f}{h \circ f} = \frac{f^{\#}(g)}{f^{\#}(h)}$. Here, $f^{\#}(g).f^{\#}(h) \in A(X)$, and $f^{\#}(h) = h \circ f$ does not vanish on $f^{-1}(V)$. Hence $\varphi \circ f$ is regular as desired, and hence a morphism. $\square$

The moral of this notationally heavy proof is that a morphism $f : X \to Y$ is given by a choice of polynomials $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ such that $f(p) = (f_1(p), \ldots, f_m(p)) \in Y$ for all $p \in X$.

Example: $f : \mathbb{A}^1 \to \mathbb{A}^2; t \mapsto (t, t^2)$, so that $f_1(t) = t, f_2(t) = t^2$. Then $f^{\#}$ is a homomorphism of rings from $K[y_1, y_2] \to K[t]$, with $f^{\#}(y_1) = t, f^{\#}(y_2) = t^2$. Note that $y_1^2 - y_2 \in \ker f^{\#}$, so in fact we have a K-algebra homomorphism, $f^{\#} : K[y_1, y_2]/(y_1^2 - y_2) \to K[t]$, inducing a morphism $f : \mathbb{A}^1 \to Y = \mathbb{V}(y_1^2 - y_2)$, a parabola.

We say X and Y as affine varieties are ***isomorphic*** if there is $f : X \to Y, g : Y \to X$ both morphisms with $f \circ g = \mathrm{id}_Y, g \circ f = \mathrm{id}_X$.

Corollary 3.2. *X and Y are isomorphic if and only if $A(X)$ and $A(Y)$ are isomorphic as K-algebras.*

4 Projective Space

Consider the two lines $\ell_1 = \mathbb{V}(x), \ell_2 = \mathbb{V}((1 + 1/t)x + 1)$, for t some parameter in K. Then the intersection $\ell_1 \cap \ell_2$ is is a single point for $t \neq \infty$. However, at $t = \infty$ the lines are parallel, and so we have lost this intersection. We think of this as being a failure of compactness, and introduce the idea of projective space to restore this compactness.

Let U be a vector space of dimension $n + 1$ over K. Then the ***projectivization*** of U, $\mathbb{P}(U)$ is the set of all 1-dimensional subspaces of U. We will write $\mathbb{P}^n := \mathbb{P}(K^{n+1})$.

For example, $\mathbb{P}^1 = \mathbb{P}(K^2) = \{\text{nonzero vectors in } K^2\}/\text{scaling action of } K^*$, where by this scaling action we identify $(1, 1) \sim (2, 2) \sim (-1, -1)$. More formally, this is the quotient space $\left(\mathbb{A}_K^2 \setminus \{0\}\right)/ \sim$ where $(z_0, z_1) \sim (\lambda z_0, \lambda z_1)$ for $\lambda \in K^*$, so that the equivalence classes of $\sim$ are straight lines through the origin.

Why does this "compactify" $\mathbb{A}^1$? Consider the subset of $\mathbb{P}^1$ given by $\{(z_0, z_1) \in \mathbb{P}^1 : z_0 \neq 0\} = \{(1, z_1/z_0) : z_0 \neq 0, z_1 \in K\}$, using the equivalence relation. But this is isomorphic to $\mathbb{A}^1$, by picking $z_1 = z_0 k$ for $k \in K$, so $\mathbb{P}^1$ contains all the information about $\mathbb{A}^1$ by encoding each element in $\mathbb{A}^1$ as the gradient of a line in $\mathbb{A}^2$, together with some missing information, where $z_0 = 0$. In the $\mathbb{A}^1$ "view" of $\mathbb{P}^1$, this point is the point at infinity, which seems special or distinguished in some way, but we view it as a line in $\mathbb{A}^2$, it is simply another straight line through the origin $\{(0, t) : t \in K\}$.

We can think of $\mathbb{P}^1$ in another way - if we draw in the unit circle centered on the origin in the $\mathbb{A}^2$ view of $\mathbb{P}^1$, we see we have a bijection between the straight lines through the origin (elements of $\mathbb{P}^1$ as defined) and pairs of antipodal points on the unit circle. So we can also view $\mathbb{P}^1$ as the unit circle in $\mathbb{A}^2$ with antipodal points identified.

7
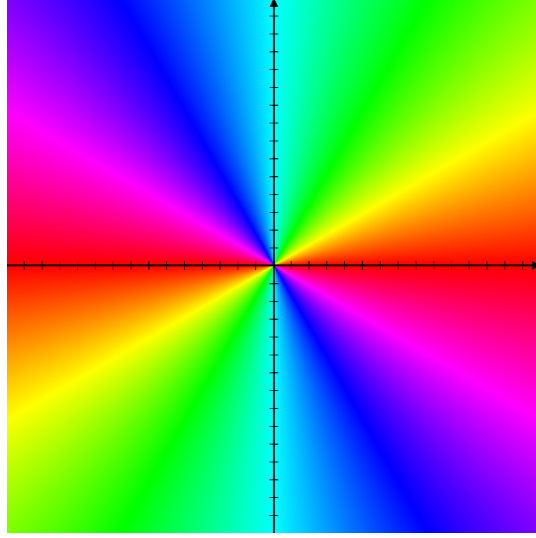
(a) $\mathbb{P}^1$ as the straight lines in $\mathbb{A}^2$, so that points of the same colour are identified
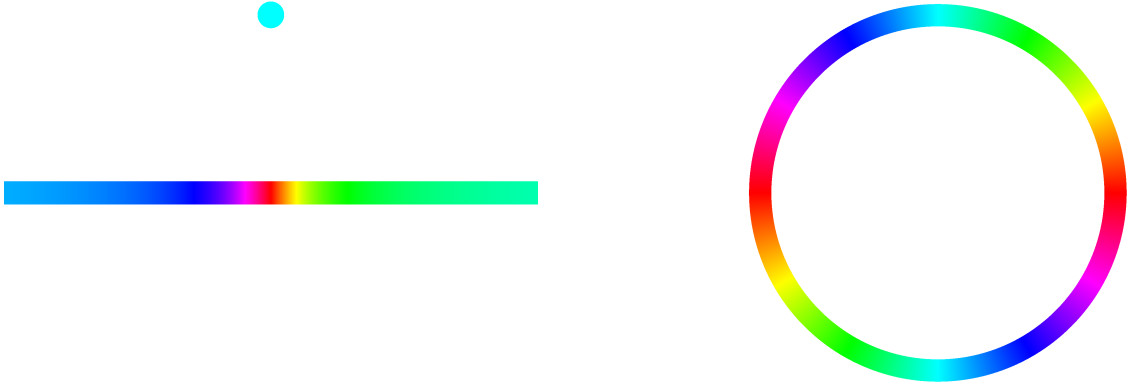
(b) $\mathbb{P}^1$ as the corresponding points in $\mathbb{A}^1$, i.e. the gradients of lines. Note the point at infinity

(c) $\mathbb{P}^1$ as the points on a circle, with antipodal points identified (points of the same colour)

For $\mathbb{P}^2_K$, consider $\mathbb{P}^2_K \supseteq \mathcal{U}_0 = \{(z_0, z_1, z_2) : z_0 \neq 0\} = \{(1, z_1/z_0, z_2/z_0) : z_0 \neq 0\} \cong \mathbb{A}^2_K$. The missing stuff at infinity is $\mathbb{P}^2 \setminus \mathcal{U}_0 = \{(0, z_1, z_2) : (z_1, z_2) \neq (0, 0)\}/\text{scaling} \cong \mathbb{P}^1$. Similarly as in the $\mathbb{P}^1$, we can think of $\mathbb{P}^2$ as being a sphere with antipodal points identified.

In general, in $\mathbb{P}^n$ with ***homogeneous coordinates*** $[z_0, \ldots, z_n]$, (where the square brackets indicates that we are working with an equivalence class of coordinates)[1] we have subsets $\mathcal{U}_i = \{(z_0, \ldots, z_n) : z_i \neq 0\} \cong \mathbb{A}^n_k$ for $0 \leq i \leq n$, we have $\mathbb{P}^n_K \setminus \mathcal{U}_i = \mathbb{P}^{n-1}_K$.

---

[1]Also used in literature are the notations $(z_0 : z_1 : \ldots : z_n)$ or $[z_0 : z_1 : \ldots : z_n]$

4.1 Projective Varieties

We want to extend our idea of an affine variety to some sort of "projective variety" in projective space. The idea of polynomial function in $z_0, \ldots, z_n$ is not well defined on points in projective space, because of the scaling that we have quotiented out by. For instance, take the polynomial $f = z_0 + 1$ as a function on $\mathbb{P}^2_K$. We expect to obtain values in K for $f(p)$ where $p \in \mathbb{P}^2_K$. But $(1, 0, 0) \sim (-1, 0, 0)$ are equivalent in $\mathbb{P}^2_K$, and $f(1, 0, 0) = 2, f(-1, 0, 0) = 0$, so f is not well defined on $\mathbb{P}^2_K$.

It's not so much a problem that the value of the polynomial isn't well defined, and we never really used this property in the affine case. We only cared that the points where it was zero, $\mathbb{V}(f)$, was well defined. Similarly, in the projective case, we can see that the polynomial will have a well defined zero set when $f(Ap) = Bf(p)$ for fixed constants A, B independent of p. Plugging this into the definition of a polynomial, we obtain the following criterion:

A polynomial $f \in K[z_0, \ldots, z_n]$ is **_homogeneous of degree d_** if $f(\lambda p) = \lambda^d f(p)$ for all $\lambda \in K^*, p \in \mathbb{A}^n_K$. Equivalently, if the total degree of every term is d.

- $z_0^2 + 2z_1 z_2 + 8z_2^2$ is homogeneous, as the total degree of each term is 2.

- $z_0 + z_1^2 + 2z_2^3 + 1$ is not homogeneous, as the terms have total degree 1, 2, 3, 0 respectively.

A **_projective hypersurface_** in $\mathbb{P}^n_K$ is the vanishing set $\mathbb{V}(f) \subseteq \mathbb{P}^n_K$ for a f a homogeneous polynomial in $K[z_0, \ldots, z_n]$. This _is_ well defined, since f is homogeneous.

An ideal in $K[z_0, \ldots, z_n]$ is **_homogeneous_** if it is generated by homogeneous polynomials, not necessarily of the same degree.

Lemma 4.1. _The following two conditions are equivalent for an ideal $I \subseteq K[z_0, \ldots, z_n]$:_

1. I is homogeneous.

2. If $f \in I$, then every constituent in f of degree r, denoted $f_{[r]}$ also lies in I.

By this we mean that every polynomial $f \in K[z_0, \ldots, z_n]$ can be written as a sum $\sum_{r=0}^{d} f_{[r]}$ where $f_{[r]}$ is homogeneous of degree r. For example:

$$z_0 + 2z_1^2 + z_0 z_2 + z_2^3 + 3z_2 = \underbrace{0}_{f_{[0]}} + \underbrace{z_0 + 3z_2}_{f_{[1]}} + \underbrace{2z_1^2 + z_0 z_2}_{f_{[2]}} + \underbrace{z_2^3}_{f_{[3]}}$$

Proof. _2. $\implies$ 1._ is immediate, since I is generated by the constituent parts of all of its polynomials, which are all homogeneous.

For the other direction, let $I = \langle f_j \rangle$ where f_j is homogeneous of degree d_j. Then for $f \in I$, $f = \sum_j h_j f_j$ where h_j is arbitrary and f_j is homogeneous.

Now split h_j into its constituent homogeneous pieces, so that $h_j = \sum_r h_{j[r]}$, a sum of terms of degree r. Then $f_{[r]} = \sum h_{j[d_j - r]} f_{j[r]}$. Now $f_{j[r]} = f_j$ if $r = d_j$, and 0 otherwise since f_j is homogeneous, so $f_{j[r]} \in I$. Then $f_{[r]}$ is a sum of terms hg for $g \in I, h \in K[z_0, \ldots, z_n]$, and so $f_{[r]} \in I$ as required. $\square$

Let $I \subseteq K[z_0, \ldots, z_n]$ be a homogeneous ideal. Then the associated **_projective variety_** is $\mathbb{V}(I) = \{P \in \mathbb{P}^n_K : f(P) = 0 \forall f \in I\}$, which by the previous lemma is the same as saying $f(P)$ vanishes for every homogeneous $f \in I$. Projective space then inherits a Zariski topology in three ways:

1. Closed sets are given by $\mathbb{V}(I)$ for $I \subseteq K[z_0, \ldots, z_n]$ homogeneous.

2. $\mathbb{P}_K^n$ is covered by $n + 1$ open sets $\mathcal{U}_i = \mathbb{P}_K^n \setminus \{z_i = 0\}$, each in bijection with $\mathbb{A}_K^n$ which has a Zariski topology, so each $\mathcal{U}_i$ has a Zariski topology. Now declare a subset $C \subseteq \mathbb{P}_K^n$ closed if and only if $C \cap \mathcal{U}_i = 0$ for all i.

3. We describe $\mathbb{P}_K^n = \left(\mathbb{A}_K^{n+1} \setminus \{(0,0,0)\} \right) / \sim$, and then inherit the topology as a quotient topology of the Zariski topology on $\mathbb{A}_K^n$.

Lemma 4.2. *These three topologies are equivalent.*

Proof. Exercise for a topology course. $\square$

We call this topology the ***Zariski topology on*** $\mathbb{P}_K^n$.

Notice that, via description 3, $\mathbb{P}_\mathbb{C}^n$ is a compact topological space and even Hausdorff with respect to the second "Euclidean" topology, by observing it is a quotient of a unit hypersphere. We will often draw diagrams of projective space using this Euclidean topology, although this structure cannot be detected using the Zariski topology. The Zariski topology is weird, so we don't draw diagrams using it.

Let $\mathcal{U}_0 \subseteq \mathbb{P}_K^n$ be the locus where $Z_0 \neq 0$, and let $X = \mathbb{V}(f)$ for some $f \in K[\mathbf{z}]$. Then $X \cap \mathcal{U}_0$ can be described by $\mathbb{V}\left(f\left(1, \frac{z_1}{z_0}, \ldots, \frac{z_n}{z_0}\right) \right)$. As a consequence, every projective variety $X \subseteq \mathbb{P}_K^n$ is a union of $n + 1$ affine varieties, as $\bigcup_{i=0}^n X \cap \mathcal{U}_i$.

A projective variety $X \subseteq \mathbb{P}_K^n$ is irreducible if X cannot be written as a union $X = X_1 \cup X_2$ with the X_i nonempty proper subvarieties.

Let $X \subseteq \mathbb{P}_K^n$ be a projective variety. Then the ***homogeneous ideal of*** X $I^h(X)$ is the ideal generated by all homogeneous polynomials vanishing on X.

Lemma 4.3. *X is irreducible if and only if $I^h(X)$ is a prime ideal.*

Proof. This is the same as in the affine case, observing the following fact: If $J \subseteq K[\mathbf{z}]$ is homogeneous and non-prime then there exist $F, G \in K[\mathbf{z}]$ homogeneous with $FG \in J$ but neither F nor G in J. $\square$

Hence, via our discussion in the affine case, every projective variety has a unique irreducible component decomposition. Consider the ideal $I \subseteq K[\mathbf{z}]$ given by $I = \langle z_0, \ldots z_n \rangle$. Then $\mathbb{V}(I) = \emptyset$ in $\mathbb{P}_K^n$ as $(0, \ldots, 0) \notin \mathbb{P}_K^n$.

Theorem 4.4 (Projective Nullstellensatz)**.**

1. If $I \subseteq K[\mathbf{z}]$ is a homogeneous ideal such that $\mathbb{V}(I) = \emptyset \subseteq \mathbb{P}_K^n$, then $I \supseteq \langle z_0^m : \ldots : z_n^m \rangle$ for some $m > 0$.

2. If $X = \mathbb{V}(I)$ with I homogeneous, then $I^h(X) = \sqrt{I}$.

Proof. Essentially the same as the affine case, which will come later. $\square$

If $X \subseteq \mathbb{P}_K^n$ is a projective variety, then every algebraic function $X \to \mathbb{C}$ is constant, by Liouville's theorem. This is why we introduce the idea of rational functions.

4.2 Rational Functions

Let $X \subseteq \mathbb{P}_K^n$ be an irreducible projective variety. Then we define the ***function field*** $K(X) = \left\{ \frac{f}{g} : f, g \text{ homogeneous of same degree}, g \in I^h(X) \right\} / \sim$, where $\frac{f_1}{g_1} \sim \frac{f_2}{g_2} \iff f_1 g_2 - g_1 f_2 \in I^h(X)$.

Note that these ratios of polynomials of the same degree are well defined on projective space - when the scaling term of λ^d comes out in the numerator and the denominator it cancels, so that $\frac{f(\lambda z)}{g(\lambda z)} = \frac{f(z)}{g(z)}$.

We need to check that $K(X)$ is well defined, i.e. that the equivalence relation $\sim$ is indeed an equivalence relation, and also that $K(X)$ is a field. The first of these requires that $I^h(X)$ is prime.

The set of degree d homogeneous polynomials in variables is a K-vector space denoted $\mathcal{O}_{\mathbb{P}^n}(d)$, where $\dim_K \mathcal{O}_{\mathbb{P}^n}(d) = |\{\text{monomials of degree } d \text{ in } z_0, \ldots, z_n\}| = \binom{n+d}{d}$.

We can think of $(n+1) \times (n+1)$ matrices (i.e. elements of $GL(n+1, K)$) as changing coordinates in K^{n+1}, and inducing a change of homogeneous coordinates on $\mathbb{P}_K^n$. These changes of coordinates are unique up to scaling, so we have the group of matrices corresponding to changes of homogeneous coordinates given by $\mathbb{P}GL(n+1, K) \cong GL(n+1, K)/\text{scaling}$.

For example, $\mathbb{P}GL(2, \mathbb{C})$ is the group of Möbius transformations on $\mathbb{P}_\mathbb{C}^1$.

Let $p_1, \ldots, p_{n+2}$ be a set of points in $\mathbb{P}_K^n$ such that no $n+1$ of these lie in a hyperplane $\mathbb{V}(f)$ for $f \in \mathcal{O}_{\mathbb{P}^n}(1)$. Then there exists a change of coordinates $\phi : \mathbb{P}_K^n \to \mathbb{P}_K^n$ such that:

$$\phi(p_1) = [1 : 0 : \ldots : 0]$$
$$\phi(p_2) = [0 : 1 : \ldots : 0]$$
$$\vdots$$
$$\phi(p_{n+1}) = [0 : 0 : \ldots : 1]$$
$$\phi(p_{n+2}) = [1 : 1 : \ldots : 1]$$

This is a simple exercise in linear algebra. Hence we can see that $\mathbb{P}GL(n+1, K)$ acts transitively on the set of collections of $n+2$ points in general position. This follows by choosing an appropriate basis of K^{n+1}.

Proposition 4.5. *Let $F \in \mathcal{O}_{\mathbb{P}^2}(d)$ and assume that F is irreducible. Let $c = \mathbb{V}(F)$ and $\ell \subseteq \mathbb{P}^2$ be a line (i.e. $\ell = \mathbb{V}(G)$ for $G \in \mathcal{O}_{\mathbb{P}^2}(1)$). Then $\#\ell \cap c \leq d$, and in fact there exist positive integers $m_p(c, \ell)$ for $p \in c \cap \ell$ such that $\sum_{p \in c \cap \ell} m_p(c, \ell) = d$.*

Proof. Choose coordinates z_0, z_1, z_2 on $\mathbb{P}_K^2$ such that the following things hold:

- $\ell = \mathbb{V}(z_2)$
- $[0 : 1 : 0] \notin c$

This implies that $c \cap \ell \subseteq \mathbb{P}_K^2 \setminus \{z_0 = 0\}$. But this is $\mathbb{P}_K^2 \setminus \mathcal{U}_0 \cong \mathbb{A}_K^2$, and so we can work in the affine case.

If we choose $x = \frac{z_1}{z_0}, y = \frac{z_2}{z_0}$, then $c \cap \{z_0 \neq 0\} = \mathbb{V}(f(x_y)), f(x, y) = F(1, x, y)$. Now, since $[0 : 1 : 0] \notin c$, $f(x, y)$ has degree d in the x variable. Hence $c \cap \ell = \{f(x, y) = 0\}$, and the result

follows by the fundamental theorem of algebra, where the $m_p(c, \ell)$ are the multiplicities of the roots. $\qquad\square$

This implies that any two distinct lines in $\mathbb{P}^2_K$ intersect at a point.

in fact, if $C = \mathbb{V}(F_1), D = \mathbb{V}(F_2)$ for $F_i \in \mathcal{O}_{\mathbb{P}^2}(d_i)$ irreducible, then $C \cap D$ is $d_1 d_2$ points counted with multiplicity (Bezout's theorem).

Lemma 4.6. *Let F and G be homogeneous polynomials that are coprime, with $\deg(F), \deg(G) \leq 2$. Then*

$$\#\mathbb{V}(F) \cap \mathbb{V}(G) \leq \deg(F) \deg(G)$$

Proof. Omitted, similar to proposition above. $\qquad\square$

Proposition 4.7. *Let $p_1, \dots, p_5 \in \mathbb{P}^2_K$, where no three lie on a line. Then there exists a unique* **conic curve** *$C = \mathbb{V}(F), F \in \mathcal{O}_{\mathbb{P}^2}(2)$ passing through $p_1, \dots, p_5$. Moreover, C is irreducible.*

Proof. Suppose there existed two conics C_1, C_2 through the points. Then they intersect at > 4 points, so they contradict the lemma above. But why does such a conic exist?

Any conic is given by $\mathbb{V}(a_1 z_0^2 + a_2 z_1^2 + a_3 z_2^2 + a_4 z_1 z_2 + a_5 z_0 z_1 + a_6 z_0 z_2) = \mathbb{V}(F)$ where $(a_1, \dots, a_6) \in K^2 \setminus \{\mathbf{0}\}$. Now each condition that $\mathbb{V}(p_i) = 0$ is a linear condition in the coefficients $a_1, \dots, a_6$. Linear algebra guarantees a one dimensional solution, but they are all multiples of each other so we get a unique irreducible polynomial F, and so C exists and is irreducible. $\qquad\square$

If $F \in \mathcal{O}_{\mathbb{P}^2}(3)$, $\mathbb{V}(F)$ is usually called an elliptic curves.

4.3 The Rational Normal Curve, or the Twisted Cubic, and Other Short Stories

Suppose we have a map from $\mathbb{P}^1 \to \mathbb{P}^3$, where $[x_0 : x_1] \mapsto [x_0^3 : x_0^2 x_1 : x_0 x_1^2 : x_1^3]$. We call this map the ***twisted cubic***. In the affine patch $\{x_0 \neq 0\}$, this is given by $\mathbb{A}^1 \to \mathbb{A}^3; t \mapsto (t, t^2, t^3)$, the ***rational normal curve***. The image of this map is an algebraic variety with equations

$$z_0 z_2 - z_1^2 = 0 \tag{1}$$
$$z_0 z_3 - z_1 z_2 = 0 \tag{2}$$
$$z_1 z_3 - z_2^2 = 0 \tag{3}$$

Take another map from $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3; ([x_0 : x_1], [y_0 : y_1]) \mapsto [x_0 y_0 : x_0 y_1 : x_1 y_0 : x_1 y_1]$ - it is easy to check this is well defined. This map in injective onto $\mathbb{P}^3$, and its image is precisely the vanishing locus of equation (2) - this can be checked by considering the affine patches where the map becomes a morphism $\mathbb{A}^1 \to \mathbb{A}^3$. The vanishing locus of $(z_0 z_3 - z_1 z_2)$ endows $\mathbb{P}^1 \times \mathbb{P}^1$ with the structure of a projective algebraic variety.

We call $\Sigma_{1,1} \subseteq \mathbb{P}^3$ the image of $\mathbb{P}^1 \times \mathbb{P}^1$ under this map.

1. $\Sigma_{1,1}$ contains a family of lines $\{L_t\}_{t \in \mathbb{P}^1}$ such that $L_t \cap L_{t'} = \emptyset$ if $t \neq t'$.

2. There is in fact another family $\{M_t\}_{t \in \mathbb{P}^1}$ of disjoint lines such that $M_t \cap L_{t'} = *$, some single point, for all $t, t' \in \mathbb{P}^1$.

We get these lines by fixing one coordinate of $\mathbb{P}^1$ and letting the other vary - in this way injectivity gives the families of lines.

If X is an irreducible projective variety, then its **field of rational functions** is given by

$$K(X) = \left\{ \frac{F}{G} : F, G \in K[\mathbf{z}] \text{ homogeneous of same degree}, G \notin I^h(X) \right\} / \sim$$

$$\frac{F_1}{G_1} \sim \frac{F_2}{G_2} \iff F_1 G_2 - F_2 G_2 \in I^h(X)$$

However, computing $K(X)$ is a pain - checking if things are members of ideals is a pain to do. Instead, we can compute $K(X)$ via the affine case.

4.4 Projective Closures

If $f \in K[z_1, \ldots, z_n]$, then $\mathbb{V}(f) \subseteq \mathbb{A}_k^n$. If we consider $\mathbb{A}_K^n = \mathbb{P}_K^n \setminus \{z_0 = 0\}$, we can consider the Zariski closure of $\mathbb{V}(f)$ in $\mathbb{P}_K^n$. To do this, we need to **homogenize** our polynomials. Say d is the maximum degree of a variable z_i appearing in f. Then $f^h := z_0^d f(z_1/z_0, \ldots, z_n/z_0)$. For example, if $f(z_1, z_2) = z_1^3 + z_1 z_2, f^h(z_0, z_1, z_2) = z_1^3 + z_0 z_1 z_2$.

Similarly for an ideal $I \subseteq K[z_1, \ldots, z_n]$, we define I^h to be $\langle f^h | f \in I \rangle \subseteq K[Z_0, \ldots, Z_n]$

Lemma 4.8 (Computing Projective Closures). *If $X^0 \subseteq \mathbb{A}_K^n$, is an affine variety given by $\mathbb{V}(I)$, then $\bar{X}^0 \subseteq \mathbb{P}_K^n$, $(\mathbb{A}_K^n = \mathbb{P}_K^n \setminus \{z_0 = 0\})$, in the Zariski topology, is given by $\mathbb{V}(I^h)$.*

Proposition 4.9. *Let $X \subseteq \mathbb{P}_K^n$ be an irreducible projective variety given by $\bar{X}^0$ for $X^0 \subseteq \mathbb{A}_K^n$ an affine variety. Then $K(X) = \{$Field of fractions of $K[X^0]\} = K(X^0)$.*

For example:

1. $K(\mathbb{P}_K^n) \cong K(z_1, \ldots, z_n)$

2. If $C \subseteq \mathbb{P}_K^3$ is the twisted cubic, then $K(C) \cong K(z)$. Then C is the projective closure of $\{(t, t^2, t^3) \subseteq \mathbb{A}^3 : t \in K\}$, which has coordinate ring $K[z]$.

3. Let $\mathbb{G}_m = \mathbb{V}(xy - 1) \subseteq \mathbb{A}_K^2$. The coordinate ring of $\mathbb{G}_m$ is the fraction field of $K[z, z^{-1}]$, i.e. $K(z)$. Notice that the fraction field of $K[z] = K(\mathbb{A}_K^1) = K(\mathbb{P}_K^1) = K(z)$, so $\mathbb{G}_m \subseteq \mathbb{A}_K^1 \subseteq \mathbb{P}_K^1$.

Proof of Lemma. The goal is to show that $X = \mathbb{V}(I^h)$ is the smallest closed set containing $X^0 = \mathbb{V}(I)$. Assume there exists $Y \supseteq X^0$ closed in $\mathbb{P}_K^n$. Observe that $Y = \mathbb{V}(J)$ for some homogeneous ideal $J \subseteq K[\mathbf{Z}]$. Given any $F \in J$ homogeneous then there exists $f \in K[z_1, \ldots, z_n]$ such that $F = Z_0^d f^h$ for some $d \geq 0$.

Observe now that $Z_0^d f^h$ vanishes on X^0, so f vanishes on X^0. This implies that $f \in \sqrt{I}$, or $f^m \in I$ for some $m \geq 1$, and then $(f^m)^h = (f^h)^m \in I^h \implies Z_0^d (f^h)^m \in I^h$. This implies that $J \subseteq \sqrt{I^h}$, so $Y \supseteq X$. $\qquad\square$

Proof Sketch. There is a natural bijection between $K(X)$ and $K(X^0)$, obtained as follows:

Given $\frac{f}{g} \in K(X^0)$, then we can produce an element of $K(X)$ by homogenization and topping up the degree: let $m = \max \deg\{f, g\}$. Then $\frac{Z_0^m f(z_1/z_0, \ldots, z_n/z_0)}{Z_0^m g(z_1/z_0, \ldots, z_n/z_0)} \in K(X)$.

Conversely, given $\frac{F(Z_0, \ldots, Z_n)}{G(Z_0, \ldots, Z_n)}$, we produce a rational function on X^0, by $\frac{F(1, z_1, \ldots, z_n)}{G(1, z_1, \ldots, z_n)} \in K(X^0)$. It easy but painful to check that these are mutual inverses. $\qquad\square$

Given $\varphi \in K(X)$, write $\varphi = \frac{F}{G}$ for $F, G \in \mathcal{O}_{\mathbb{P}^n}(d)$, and then we obtain a function $\varphi : X \backslash \mathbb{V}(G) \to K$.

Given $F_0, \ldots, F_m \in \mathcal{O}_{\mathbb{P}^n}(d)$, we obtain a map

$$\underline{F} : \mathbb{P}^n_K \backslash \bigcap_i \mathbb{V}(F_i) \to \mathbb{P}^m_K$$

$$[Z_0 : \ldots : Z_n] \mapsto [F_0(Z_0, \ldots, Z_n) : \ldots : F_n(Z_0, \ldots, Zn)]$$

We write $\underline{F} : \mathbb{P}^n_K \dashrightarrow \mathbb{P}^m_K$, where the dashed arrow means the function is partially defined. Given this $\underline{F}$, the set $\bigcap_i \mathbb{V}(F_i)$ is called the **base locus**.

We say two rational maps $\underline{F}, \underline{G}$ are equivalent on a projective variety $X \subseteq \mathbb{P}^n_K$ if $F_i G_j - F_j G_i \in I(X)$ for all i, j. note that they can possibly have different base loci.

Given $\varphi : X \dashrightarrow \mathbb{P}^n_K$, an (equivalence class of) rational map $P \in X$ is a **regular point** for φ if there exists a representative $\varphi = \underline{F}$ such that $P \notin$ the base locus of $\underline{F} = \bigcap_i \mathbb{V}(F_i)$. We can then define a **morphism** of projective varieties to be a rational map $\varphi : X \dashrightarrow \mathbb{P}^n_K$ with the property that P is a regular for φ for all $P \in X$. We write $\varphi : X \to \mathbb{P}^m_K$.

Let $P \in \mathbb{P}^n_K$ be any point and $\mathbb{P}^{n-1}_K \cong H \subseteq \mathbb{P}^n_K$ be a hyperplane such that $P \notin H$. Then define the **projection away from P** as follows: given $Q \in \mathbb{P}^n_K$, let $\overline{PQ}$ be the unique line passing through these points. Then define φ:

$$\varphi : \mathbb{P}^n_K \dashrightarrow \mathbb{P}^{n-1}_K \cong H$$
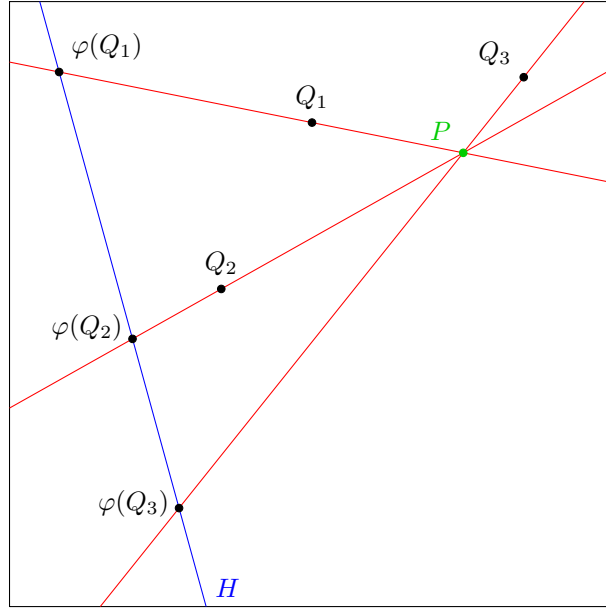
$$Q \mapsto \overline{PQ} \cap H$$

Figure 2: The projection φ away from P in $\mathbb{P}^2$ onto $H \cong \mathbb{P}^1$

To honestly check this is a rational map, change coordinates such that $H = \{Z_n = 0\}$ and

$P = [0 : \ldots : 0 : 1]$. Then the rational map is given by:

$$\mathbb{P}^n \dashrightarrow \mathbb{P}^n$$
$$[Z_0 \ldots : Z_n] \mapsto [Z_0 : \ldots : Z_{n-1}]$$

The **degree d Veronese morphism** is given as follows. Choose a basis for $\mathcal{O}_{\mathbb{P}^n}(d)$, say $F_1, \ldots, F_{\binom{n+d}{d}}$. Then:

$$\mathcal{V}_d : \mathbb{P}^n \to \mathbb{P}^{\binom{n+d}{d}-1}$$
$$P \mapsto [\ldots : F_j(P) : \ldots]$$

Then the twisted cubic is simply the degree 3 Veronese map of $\mathbb{P}^1$.

Given a rational map $\varphi : X \dashrightarrow Y$ defined by restriction from a rational map $\mathbb{P}^n_K \dashrightarrow \mathbb{P}^m_K$, we define $\operatorname{dom}\varphi$ to be the set of all regular points for φ on X. Then φ is said to be **dominant** if $\varphi(\operatorname{dom}\varphi)$ is Zariski dense.

Let X and Y be irreducible. A rational map $\varphi : X \dashrightarrow Y$ is called **birational** if there exists a rational map $\varphi : Y \dashrightarrow X$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity whenever they are defined. We say a projective variety A is birational to another projective variety B whenever there exists some birational map between them, or we might say that A and B are birational.

For example:

- A^n and $\mathbb{P}^n$ are birational
- $\mathbb{V}(y^2 - x^3)$ is birational to $\mathbb{A}^1$
- $\mathbb{V}(y^2 - x^3 + x) \subseteq \mathbb{A}^2_K$ is *not* birational to $\mathbb{A}^1_K$ for char $K \neq 2$.

Theorem 4.10. *Let X and Y be projective varieties. Then X is birational to Y if and only if $K(X) \cong K(Y)$.*

A **quasi-projective variety** is a Zariski open subset of a projective variety, i.e. $\mathbb{V}(I) \setminus \mathbb{V}(J)$ for two ideals I, J. Note that, since $\emptyset$ is a projective variety, every projective variety is also a quasi-projective variety.

5 Products

If X and Y are quasi-projective varieties, then $X \times Y$ is also a quasi-projective variety. If X and Y are projective (or irreducible), then $X \times Y$ is also projective (or irreducible), respectively.

This fact relies on the fact that, given $\mathbb{P}^n_K$ and $\mathbb{P}^m_K$, the set $\mathbb{P}^n_K \times \mathbb{P}^m_K$ is naturally a projective variety, and the rest follows from basic topological arguments.

We can approach this from the point of view of creating a Zariski topology on $\mathbb{P}^n_K \times \mathbb{P}^m_K$ using what we already know - a point $P \in \mathbb{P}^n_K \times \mathbb{P}^m_K$ is given by $([a_0 : \ldots : a_n], [b_0 : \ldots : b_m])$ where we can scale the first and second parts *independently*. We then can consider some appropriate notion of a **bihomogeneous** polynomial in $(n+1) + (m+1)$ variables, obtaining an algebraic structure by using their vanishing loci.

Here however, we will use a slightly different approach:

5.1 Segre Embedding

The **Segre embedding** is the map:

$$\sigma_{n,m} : \mathbb{P}^n_K \times \mathbb{P}^m_K \to \mathbb{P}^{(n+1)(m+1)-1}_K$$
$$([x_0 : \ldots : x_n], [y_0 : \ldots : y_m]) \mapsto [\ldots : x_i y_j : \ldots]$$

Claim 5.1. $\sigma_{n,m}$ *is injective.*

Proof. Let $c = [\ldots : C_{ij} : \ldots] \in \mathrm{im}(\sigma_{n,m})$ and $(a,b) \in \sigma_{n,m}^{-1}(\{c\})$, say $a = [A_0 : \ldots : A_n], b = [B_0 : \ldots : B_m]$.

We may assume, up to a change of coordinates, that $C_{0,0} = 1$, so $A_0 = B_0 = 1$. This then forces that $B_i = C_{0,i}$ and $A_j = C_{j,0}$, so a, b are unique, so $\sigma_{n,m}$ is injective. $\square$

Claim 5.2. *The image of $\sigma_{n,m}$ is closed.*

Proof. The equations are $\{Z_{ij}Z_{k\ell} - Z_{i\ell}Z_{kj} = 0\}$ for all i, j, k, ℓ. Checking that $\mathrm{im}(\sigma_{m,n})$ is equal to the vanishing locus of these equation is a locally affine calculation which is left as an exercise. $\square$

$$\mathbb{P}^n_K \times \mathbb{P}^m_K$$

Note that the projection maps $\pi_1 \swarrow \quad \searrow \pi_2$, $\mathbb{P}^n_K \qquad \mathbb{P}^m_K$ are both morphisms.

5.2 The Blow-up

The **blowup** of $\mathbb{A}^2_K$ at the origin is given as follows:

$$\mathrm{Bl}_{(0,0)} \mathbb{A}^2 = \left\{ ((x,y), [z:w]) \in \mathbb{A}^2_K \times \mathbb{P}^1_K \mid xz - yw = 0 \right\}$$

Since $\mathbb{A}^2 \times \mathbb{P}^1 \to \mathbb{A}^2$ is a morphism, there is an induced morphism:

$$\mathrm{Bl}_{(0,0)} \mathbb{A}^2_K \xrightarrow{\pi} \mathbb{A}^2_K$$

If $P \in \mathbb{A}^2_K, P \neq (0,0)$ then $\pi^{-1}(P)$ is exactly one point. In fact, $\mathrm{Bl}_{(0,0)} \mathbb{A}^2 \setminus \pi^{-1}(0,0) \to \mathbb{A}^2_K \setminus \{(0,0)\}$ is then invertible, and so π is birational map. If instead $P = (0,0)$ then $\pi^{-1}(P) = \mathbb{P}^1_K$.

We can think of $\mathbb{P}^1$ as separating lines through the origin based on incoming slope. The notion of blowups can be generalised to $\mathrm{Bl}_Z X$ for $Z \subseteq X$ some closed subvariety.
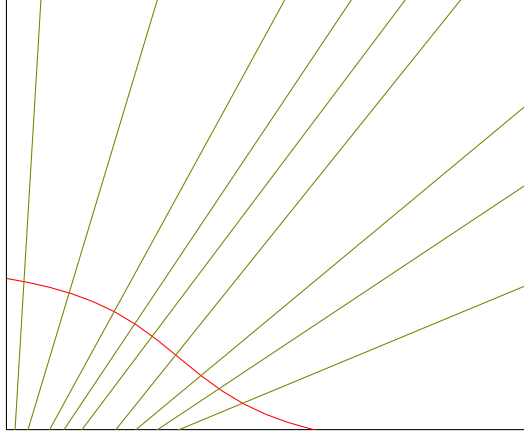
6 Smoothness, Tangent Spaces, and Dimension

Given $X \subseteq \mathbb{P}^n_{\mathbb{C}}$ a variety, we want to know when X viewed in Euclidean space is a manifold.
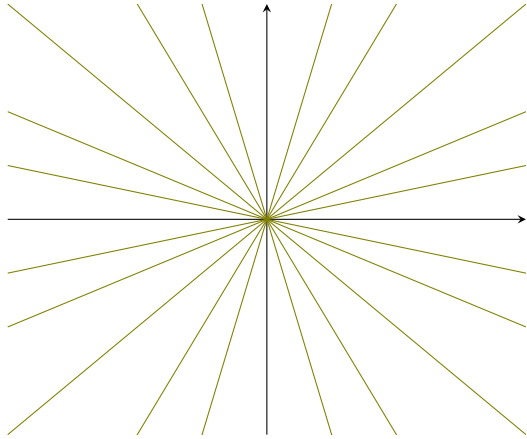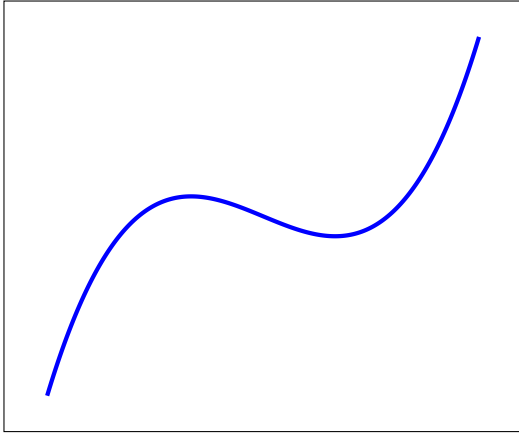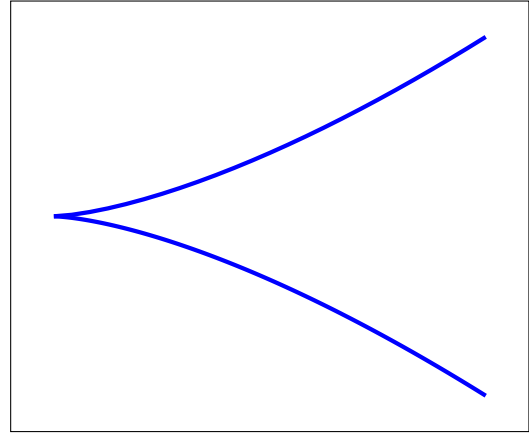
(a) $\mathbb{A}^2$

(b) $\text{Bl}_{(0,0)} \mathbb{A}^2$

(a) $\mathbb{V}(f)$ for $f = y - x^3 + 3x$

(b) $\mathbb{V}(f)$ for $f = y^2 - x^3$

The curve on the left is smooth, and forms a manifold, whilst the curve on the right has a cusp, so does not form a manifold. We will end up calling it singular.

6.1 Hypersurfaces

Let $X = \mathbb{V}(f) \subseteq \mathbb{A}^n_K$. A line in $\mathbb{A}^n_K$ through a point $P = (a_1, \ldots, a_n) \in X$ is given by

$$L = \{(a_1 + b_1 t, \ldots, a_n + b_n t) | t \in K\}$$

where $(b_1, \ldots, b_n) \in K^n \setminus \{\mathbf{0}\}$.

We say L is **_tangent to X at P_** if $g(t) = f(a_1 + b_1 t, \ldots, a_n + b_n t)$ vanishes to order 2 at $t = 0$. More precisely, let

$$f^{lin} := \sum_i \frac{\partial f}{\partial z_i}(P)(z_i - a_i)$$

be the **linearisation** of f near P. Then we can define the **affine tangent space to X at P** by:

$$T_{X,P}^{aff} := \mathbb{V}(f^{lin}) \subseteq \mathbb{A}_K^n$$

As a sanity check, make sure that this gives the usual tangent line for $y = f(x)$. Note that $T_{X,P}^{aff}$ is centered at the P, not at the origin. By shifting it to the origin by translation by P, we get the **tangent space to X at P**, given by:

$$T_{X,P} = \left\{ v \in K^n \mid \sum v_i \frac{\partial f}{\partial z_i}(P) = 0 \; \forall f \in I \right\}$$

where $X = \mathbb{V}(I)$. Then $T_{X,P} + P = T_{X,P}^{aff}$.

For example, in the case $X = \mathbb{V}(y^2 - x^3)$, we calculate f^{lin} at $(0,0)$ to be 0, and so $T_{X,(0,0)}^{aff}$ is $\mathbb{A}_K^2$.

6.2 Digression On Cubics

Let $f_2 \in \mathcal{O}_{\mathbb{P}^2}(3)$ such that $\mathbb{V}(f_2)$ is smooth. Then $\mathbb{V}(f^2)$ is an **elliptic curve**. In particular, $K(E)$ is not isomorphic to $K(z)$. We say that X is **rational** if X is birational to $\mathbb{P}^r$ for some r.

Let $f_3 \in \mathcal{O}_{\mathbb{P}^3}(3)$. We call $\mathbb{V}(f_3)$ a **cubic surface**. We'll take $f_3 = z_0^2 z_1 + z_1^2 z_2 + z_2^2 z_3 + z_3^2 z_0$, and let $S = \mathbb{V}(f_3)$. Consider the rational map $\varphi : S \dashrightarrow \mathbb{P}^2$, taking $[z_0 : \ldots : z_3] \mapsto [z_0 z_3 : z_1 z_2 : z_2 z_3]$. We can also take some map $\psi : \mathbb{P}^2 \dashrightarrow S$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity map, and so $K(S) = K(z_1, z_2)$, and S is smooth. This holds for any smooth cubic surface in $\mathbb{P}_K^3$, and they are all rational.

If $f_4 \in \mathcal{O}_{\mathbb{P}^4}(3)$, then $\mathbb{V}(f_4) = X$ is sometimes called a **cubic threefold** - it was a landmark result of the late 20th century to prove that X is not rational.

If $f_5 \in \mathcal{O}_{\mathbb{P}^5}(3)$. and $Y = \mathbb{V}(f_5)$ is a smooth **cubic fourfold**, then the rationality of Y is an open question.

6.3 Dimension and Smoothness

Let X be an irreducible variety. Then we define the **dimension** of X as:

$$\dim X = \min_{p \in X} \{ \dim T_{X,p} \}$$

If X is reducible, the we can write it uniquely as a union of irreducible varieties $X_1 \cup \ldots \cup X_n$, and let $\dim X = \max_i \dim X_i$. If all X_i have the same dimension, then X is **pure**.

A point $p \in X$ is said to be **smooth** if $\dim_K X = \dim_K T_{X,p}$, and a non-smooth point is said to be **singular**.

Proposition 6.1. *Let X be a variety. Then the set of singular points is a closed proper subvariety.*

Proof. It suffices to treat the case where X is affine so $X = \mathbb{V}(I)$ for $I = \langle f_1, f_2, \ldots, f_n \rangle \subseteq K[\mathbf{x_i}]$.

Treating $\left(\frac{\partial f_j}{\partial z_i}(p)\right)$ as a matrix, we then have from the definition $\dim_K T_{X,p} = n - \text{rank}\left(\frac{\partial f_j}{\partial z_i}(p)\right)$. The locus where this rank is $\leq n - r$ for any $r \in \mathbb{N}$ is the closed subvariety given by the vanishing of the $(n - r) \times (n - r)$ minors. $\qquad\square$

Morally what this tells us, since open subsets of varieties are dense, is that most points on an algebraic variety are smooth points.

Proposition 6.2. *If X and Y are irreducible and birational then $\dim X = \dim Y$.*

Let $\phi : X \dashrightarrow Y$ be a rational map regular at $p \in X$, where $X \subseteq \mathbb{A}_K^n, Y \subseteq \mathbb{A}_K^m$. Then we can write $\phi = (f_1, \ldots, f_m)$, where $f_j \in K(z_1, \ldots, z_n)$ is regular at p. We can then define $d\phi_p : T_{X,p} \to T_{Y,\phi(p)}$, the ***differential of ϕ at p***, defined by:

$$d\phi_p(\mathbf{v}) = \left(\sum_{i=1}^n v_i \frac{\partial f_j}{\partial z_i}(p)\right)_j$$

It follows from the chain rule that $d\phi_p(\mathbf{v})$ does indeed lie in $T_{Y,\phi(p)}$ - checking this is left as an exercise.

If $X \dashrightarrow_\phi Y \dashrightarrow_\psi Z$, and $p \in \text{dom}(\phi)$, $\phi(p) \in \text{dom}(\psi)$, then $d\psi_{\phi(p)} \circ d\phi_p = d(\psi \circ \phi)_p$.

Proposition **6.2** follows immediately from this.

We might ask the following question: if X is a variety, is X isomorphic to a ***hypersurface***? The answer to this question is no - consider $X = \mathbb{V}(xy, yz, zx)$, a union of the coordinate axes in $\mathbb{A}^3$. We might think this is isomorphic (it is certainly *homeomorphic*) to a ***planar triple point***, e.g. $\mathbb{A}^2 \supseteq Y = \mathbb{V}(xy(x - y))$. Then $X \not\cong Y$ because the dimension $T_{X,(0,0,0)}$ is 3, and Y can have no such point.

Theorem 6.3. *Given any irreducible variety X there exists a hypersurface Y such that X is birational to Y, i.e. $K(X) = K(Y)$.*

The proof of this will come later, but first we'll have a short digression on field theory.

Let L be a finitely generated field extension of K. The field L is called a ***purely transcendental extension*** of K if there exist elements $x_1, \ldots, x_n$ algebraically independent[2] over K such that $L = K(x_1, \ldots, x_n)$.

Proposition 6.4. *Let L/K be a finitely generated field extension. Then there exists a subfield $K \subseteq M \subseteq L$ purely transcendental over K such that L/M is algebraic and separable. Moreover, $L = M(y)$ for some $y \in L$.*

Proof (Characteristic 0). Since L is finitely generated, we know that $L = K(x_1, \ldots, x_m)$. There is a maximal algebraically independent subset of $\{x_i\}$. Re-order this set such that $\{x_1, \ldots, x_n\}$ form this subset. Then take $M = K(x_1, \ldots, x_n)$, which is purely transcendental. Then by finite generation L/M is finite and algebraic, and in characteristic 0 separability is automatic. For the final statement, apply the theorem of the primitive element. $\qquad\square$

The integer n will turn out to be unique and equal to $\dim X$ where X is a variety with $K(X) = L$.

---

[2]i.e. with no polynomial equation in $x_i, i \neq j$ with x_j a root.

Proposition 6.5. *Let $L = K(x_1, \ldots, x_n)$ be pure transcendental, and x_{n+1} is algebraic. Then the ideal $I = \{g \in K[z_1, \ldots, z_{n+1}] : g(\mathbf{x}) = 0\}$ is principal, i.e. $I = (f)$. Moreover, if f contains the variable z_i, then the set $\{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1}\}$ is algebraically independent.*

Proof. Since $\{x_i\}$ are algebraically independent, the subring $L \supseteq R = K[x_1, \ldots, x_n]$ is isomorphic to the polynomial ring in n variables, and in particular is a UFD.

Then let $h \in L[t]$ be the minimal irreducible polynomial for x_{n+1}. Let b be the LCM of the denominators of its coefficients. So then if we take $f = b \cdot h$, where $f \in K[x_1, \ldots, x_n, t]$. Since h is irreducible, the Gauss lemma implies that f is irreducible in R.

Let $g \in K[z_1, \ldots, z_{n+1}]$ be an element of I. In $K[t]$, g is a multiple of h. Again by the Gauss lemma, if h divides g then f divides g, and so I is principal and generated by f.

For the last part, assume $\{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1}\}$ was algebraically dependent. Then there exists $g \in I$ not containing z_i such that $g(x_1, \ldots, x_{n+1}) = 0$. But f divides g, which is a contradiction. $\square$

Corollary 6.6. *If X is an irreducible variety and $K(X)$ is its function field, then:*

$$\dim X = \operatorname{tr} \deg_K K(X)$$

Proof. Exercise - reduce the the case where $X = \mathbb{V}(f)$ and apply the second part of the previous proposition. $\square$

Proof of 6.3. Given X irreducible, apply the **6.5** to $K(X)$. So $K(X) \equiv \operatorname{FractionField}(K[z_1, \ldots, z_n]/(f))$ $\square$

Theorem 6.7 (Affine Nullstellensatz I). *Every maximal ideal in $K[z_1, \ldots, z_n]$ is of the form $m = (z_1 a_1, \ldots, z_n a_n)$ for $a_i \in K$. If $I \subsetneq K[\mathbf{z}_i]$ is a non-unit ideal, then $\mathbb{V}(I) \neq \emptyset$.*

Proof in uncountable case. For the first part, clearly every ideal of that form is maximal. Conversely, let $m \subseteq K[\mathbf{z}_i]$. Consider $L = K[\mathbf{z}_i]/m$, which is a field, and let $a_i = z_i + m$. If $L = K$, then $a_i \in K$ as required. Otherwise, L/K must be transcendental.

Take $t \in L \setminus K$. Then $K \subseteq K(t) \subseteq L$, and t is transcendental. now, let $U_m = \langle a_1^{m_1} \ldots a_n^{m_n} \rangle$ where $\sum m_i = m$. These are all finite dimensional over K, but $\bigcup_m U_m = K$. Observe for each $c \in K$, the elements $\frac{1}{t-c}$ are linearly independent. But there are uncountably many of them. Only finitely many lie in each U_m, so we get a contradiction. $\square$

7 Curves

An ***algebraic curve*** is an algebraic variety of dimension 1.

Proposition 7.1. *If X is an irreducible curve and $W \subseteq X$ is a proper closed subvariety, then w is finite.*

Proof. We've already proven this for plane curves. We can assume X is affine and let $I(X)$ be the associated ideal, and that W is irreducible. By the Nullstellensatz, we know that $I(X) \subsetneq I(W)$, and let $\varphi : W \hookrightarrow X$ be the inclusion map - this induces a homomorphism of coordinate rings given by restriction $\varphi^* : K[X] \to K[W]$.

If W is not a point, then $K[W] \neq K$, so take $t \in K[W] \setminus K$. The element t is transcendental over K. Then take $0 \neq x \in K[x]$ with $\varphi^*(x) = 0$ and $y \in K[X]$ with $\varphi^*(y) = t$. Note that x and y are algebraically independent, but $\dim X = 1 \implies \operatorname{tr} \deg K(X) = 1$ so we get a contradiction. $\qquad\square$

7.1 Basic Structure on Curves

Let X be an irreducible curve. Given $p \in X$, the **local ring of X at p** is defined to be $\mathcal{O}_{X,p} = \mathcal{O}_p = \{\frac{f}{g} : f, g \in K[X], g(p) \neq 0\}$ - the functions defined on some open set containing p.

Then $\mathcal{O}_{X,p} \supseteq m_p = \{F \in \mathcal{O}_{X,p} : F(p) = 0\}$. It is an easy exercise to show that m_p is an ideal, and almost as easy to show that it is maximal. Moreover, $\mathcal{O}_{X,p} \setminus \mathcal{O}_{X,p}^*$, the set of non-units in $\mathcal{O}_{X,p}$, is precisely m_p, so m_p is the unique maximal ideal in $\mathcal{O}_{X,p}$.

This definition of a local ring is similar to one from commutative algebra: a **local ring** is a commutative ring that is not a field with a unique maximal ideal.

For example, if X is an irreducible curve, $\mathcal{O}_{X,p}$ is a local ring. Other examples of local rings include $\mathbb{C}[\![t]\!]$, the formal power series in t, with unique maximal ideal generated by t.

Theorem 7.2. *If X is an irreducible curve and $p \in X$ is a smooth point, then the ideal $m_p \trianglelefteq \mathcal{O}_{X,p}$ is principal.*

We will refer to a generator of m_p as a **local parameter/coordinate** at p.

Proof. Assume $p \in X_0 \subseteq \mathbb{A}_K^n$ is an affine patch of X at p. After a change of coordinates, we can assume that p is the origin. We can write $K[X_0] = \frac{K[z_1,\ldots,z_n]}{I(X_0)} = K[x_1,\ldots,x_n]$ as an algebra <u>NOT</u> as a polynomial ring - the x_is can have relations. They are just the images of the z_is under the quotient map.

Then $\mathcal{O}_{X,p} = \mathcal{O}_{X_0,p} = \{\frac{f}{g} : f, g \in K[X_0], g \notin (x_1,\ldots,x_n)\}$. So then $m_p = \{\frac{f}{g} : f, g \in K[X_0], f \in (x_1,\ldots,x_n), g \notin (x_1,\ldots,x_n)\} = x_1 \mathcal{O}_{X,p} + \ldots + x_n \mathcal{O}_{X,p}$.

We change coordinates, so that $T_{X,p}^{aff} = T_{X,p} = \{z_2 = z_3 = \ldots = z_n = 0\}$. Since the z_i linearise equations for X_0, there exist functions $f_2, \ldots, f_n \in I(X_0)$ such that $f_i = z_i - h_i$ where h_i has no terms of degree ≤ 1. In $\mathcal{O}_{X,p}$ we have $x_i = h_i(x_1,\ldots,x_n) \in (x_1^2, x_1 x_2, \ldots, x_n^2) = m_p^2$.

Note that this implies that the image of x_1 inside m_p/m_p^2 is a generator as a K-vector space, $K[X_0]/m = \mathcal{O}_{X,p}/m_p$.

In turn, by applying Nakayama's Lemma, we can conclude that x_1 generates m_p. $\qquad\square$

Lemma 7.3 (Nakayama's Lemma). *Let R be a local ring with maximal ideal m, and let M be a finitely generated R-module. If $mM = M$ then $M = 0$.*

Proof. Google $\qquad\square$

Corollary 7.4. *If (R, m) are as above, and if $t_1, \ldots, t_r \in m$ generate m/m^2, as an R/m-vector space, then they generate m.*

This is the corollary we need to finish off the proof.

Proof. Let $n = \langle t_1, \ldots, t_n \rangle \subseteq m$. If the images of $\{t_i\}$ generate m/m^2, then $n + m^2 = m + m^2 \implies n + m^2/n = m + m^2/n \implies m(m/n) = (m/n)$. So by Nakayama, $m/n = 0$, and $m = n$. $\qquad \square$

Corollary 7.5. *If X is an irreducible curve and $p \in X$ be a smooth point, then the maximal ideal $m_p \subseteq \mathcal{O}_{X,p}$ of functions vanishing at p is principal, and $\mathcal{O}_{X,p}$ is a discrete valuation ring, i.e. there exists $\mathrm{ord}_p : K(X)^* \to \mathbb{Z}$ such that:*

$$\mathcal{O}_{X,p} = \{f \in K(X)^* \,|\, \mathrm{ord}_p(f) \geq 0\} \cup \{0\}$$
$$m_p = \{f \in \mathcal{O}_{x,p} : \mathrm{ord}_p(f) > 0\} \cup \{0\}$$

Proof. We know $m_p = (\pi_p)$ as m_p is principal by **7.2**, and so $m_p^n = (\pi_p^n)$. We will examine $J = \bigcap_n m_p^n$. Observe that $m_p J = J$, so $J = 0$ by Nakayama's lemma.

Then for $f \in \mathcal{O}_{X,p}$, define $\mathrm{ord}_p(f)$ to be the largest $n \in \mathbb{Z}_{\geq 0}$ such that $f \in m_p^n$. If $f \in K(X)^* \setminus \mathcal{O}_{X,p}$, then $f^{-1} \in \mathcal{O}_{X,p}$. In this case, we define $\mathrm{ord}_p(f) = -\mathrm{ord}_p(f^{-1}) \in \mathbb{Z}_{\leq 0}$. $\qquad \square$

We will also use $v_p(x) = \mathrm{ord}_p(x)$ as an alternative notation. By convention, we wil say that $v_p(0) = +\infty$, so that $v_p : K(X)^* \to \mathbb{Z} \cup \{\infty\}$.

Corollary 7.6. *If X is a smooth projective curve and $X \dashrightarrow_\varphi \mathbb{P}^m$ is a rational map then φ is a morphism.*

Proof. Let $\varphi = (\varphi_0, \ldots, \varphi_m)$ and $p \in X$ as above. Pick a local parameter π_p at p, and calculate $\min_i \{v_p(\varphi_i)\} = n$, say. Then replace $(\varphi_0, \ldots, \varphi_m)$ with $(\pi_p^{-n} \varphi_0, \ldots, \pi_p^{-n} \varphi_m)$ to get an equivalent rational map, but this time regular at p. $\qquad \square$

Corollary 7.7. *Any birational map of smooth projective curves*

$$\varphi : X_1 \dashrightarrow X_2$$

is an isomorphism. A smooth projective curve is uniquely determined by the field of functions.

Theorem 7.8. *The image of a projective variety under a morphism is closed.*

Proof. Google $\qquad \square$

Corollary 7.9. *Any morphism of projective irreducible curves is either surjective or constant.*

Proof. Given $\varphi : X_1 \to X_2$, since $\varphi(X_1)$ is closed and connected, then $\varphi(X_1) = X_2$ or $\varphi(X_1) = \bullet$. $\qquad \square$

Proposition 7.10. *Let $\varphi : X_1 \to X_2$ be a non-constant morphism of algebraic curves. Then:*

- *φ is a finite map, i.e. $|\varphi^{-1}(p)| < \infty$ for all $p \in X_2$*

- *We have a pullback $\varphi^* : K(X_2) \hookrightarrow K(X_1)$ exhibiting $K(X_1)$ as a finite algebraic extension of $K(X_2)$.*

Proof. The first statement is clear since $\varphi^{-1}(p)$ is closed for all $p \in X_2$. For the second part, observe that $\varphi(X_1)$ is infinite since $k = \bar{k}$ so $\varphi(X_1)$ is dense, so φ^* makes sense. Now $K(X_2)$ lives inside $K(X_1)$ which is transcendental over K but algebraic over $K(t)$, so the extension $[K(X_1) : K(X_2)]$ is finite. $\qquad \square$

The number of preimages of $p \in X_2$ is finite, but can depend on the choice of p. For example, if we take $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ by squaring. Then $\varphi^{-1}(0) = 0, \varphi^{-1}(\infty), \varphi^{-1}(a) = \pm\sqrt{a}$.

Given $\varphi : X_1 \, to X_2$ a morphism of irreducible curves, the ***degree of*** φ, $\deg \varphi = \deg[K(X_1) : K(X_2)]$. When φ^* is separable, it is a fact that $\deg \varphi$ is equal to the maximum number of preimages of points in X_2. Store this fact as true without asking for proof, or just Googleit.

What about the non-generic points in X_2 and their preimages?

Given $\varphi : X_1 \to X_2$ as before and $p \in X_1$, define the ***ramification index*** of φ at p to be $\operatorname{ord}_p(\varphi^* \pi_q)$ where π_q is a local parameter for X_2 near $\varphi(p) = q$.

Theorem 7.11. *Let $\varphi : X_1 \to X_2$ be a morphism of projective irreducible curves.*

1. *If φ is non-constant, then φ is surjective.*

2. *If X_1 and X_2 are smooth, then for any $q \in X_2$, $\deg \varphi = \sum_{p \in \varphi^{-1}(q)} e_p$ where e_p is the ramification index at p.*

3. *If $\operatorname{char}(K) = 0$ or if φ^* is separable, then $e_p = 1$ generically, i.e. outside a finite set.*

Proposition 7.12. *Let X be a smooth projective curve and $f \in K(X)$ is regular for all points $p \in X$. Then $f \in K$.*

Proof. Examine $\varphi = 1 \cdot f : X \to \mathbb{P}^1$. The image must include ∞ if φ is non-constant, but this contradicts regularity of f. $\qquad\square$

7.2 Brill-Noether Problem

Let X be a smooth projective irreducible curve. For what integers $r, d \geq 0$ does X admit a morphism (embedding):

$$X \xrightarrow{\varphi} \mathbb{P}^r_K$$

where φ has degree d? ($\varphi(x)$ should not be contained in a hyperplane). (We say the ***degree*** of φ is the number of preimages of a generically chosen hyperplane in $\mathbb{P}^r$).

We won't answer this question because it is too hard, but we will try to make some progress in this direction. We will need the Riemann-Roch theorem, Riemann-Hurwitz theorem, and the ideas of genus and canonical divisor.

Let X be a curve and $\varphi : X \to \mathbb{P}^r_K$ be a morphism. The map φ is given by rational functions $(\varphi_0, \ldots, \varphi_r)$. If we consider the open set $\mathbb{P}^r_K \setminus \{z_r = 0\}$, we can divide by φ_r to get $\left\{ \frac{\varphi_i}{\varphi_r} \right\}_{i=0}^{r-1}$ rational function on an open set of X.

In other words, given $\varphi : X \to \mathbb{P}^r_K$ we get r rational functions, say $f_1, \ldots, f_r \in K(X)$ which are undefined on precisely the same points: where $\varphi_r = 0$. In fact we can say more - they are also undefined in the same way in the sense of orders of poles from complex analysis: given $f \in K(X)$ and $p \in X$, we say that f has a ***pole*** at p if $\operatorname{ord}_p(f) < 0$, and that the order of this pole is $- \operatorname{ord}_p(f)$.

A ***divisor*** D on a curve X is an element of the group $\operatorname{Div}(X) = \bigoplus_{p \in X} \mathbb{Z}p$ - all finite $\mathbb{Z}$-linear combinations of points. The ***degree*** of a divisor $D = \sum a_i p_i$ is given by $\deg D = \sum a_i$. As a point of notation, $\operatorname{Div}^d(X) = \{D \in \operatorname{Div}(X) : \deg D = d\}$.

A rational function $f \in K(X)^*$ gives rise to a divisor as follows:

$$\mathrm{div}(f) = \sum_{p \in X} \mathrm{ord}_p(f) \cdot p$$

Lemma 7.13. *For $f \in K(X)^*$, $\mathrm{div}(f) \in \mathrm{Div}(X)$, i.e. $\mathrm{ord}_p(f) = 0$ for all but finitely many $p \in X$. In fact, $\deg(\mathrm{div}(f)) = 0$.*

Proof. Given f, take $\varphi : X \to \mathbb{P}^1; x \mapsto [1 : f(x)]$. We need to calculate the zeroes and poles of f, which correspond to the points of X mapping to 0 and ∞ respectively. Take a local parameter t around 0 and $\frac{1}{t}$ around ∞. Then applying the results from the basic structure on curvs:

$$\deg(\varphi) = \sum_{p \in X, p \mapsto 0} e_p = \sum_{p \in X, p \mapsto \infty} e_p$$

where in each case the e_ps give the orders of zeros and poles. In particular, the weighted numbers of zeroes and poles are equal. $\square$

The image of the homomorphism div is contained in $\mathrm{Div}^0(X)$, and is called the ***set of principal divisors***.

Proposition 7.14. *Every degree 0 divisor on $\mathbb{P}^1$ is principal.*

Proof. Exercise. $\square$

The ***Jacobian group*** of X is $\mathrm{Div}^0(X)/\{\mathrm{div}(f) : f \in K(X)^*\}$, and the ***Picard group*** of X is $\mathrm{Div}(X)/\{\mathrm{div}(f) : f \in K(X)^*\}$.

As a fun fact, over $\mathbb{C}$, $\mathrm{Jac}(X)$ is a projective variety, and is homeomorphic to $(S^1)^g$ for some $g \in \mathbb{N}$.

7.3 Hyperplane Sections

Given $X \subseteq \mathbb{P}^r_K$, the coordinate functions on $\mathbb{P}^r_K \setminus \{z_r = 0\} \cong \mathbb{A}^r_K$ give rational function on X which are morphisms away from $X \cap \{Z_r = 0\}$. Let $L \in \mathcal{O}_{\mathbb{P}^r}(1)$ and $H = \mathbb{V}(L)$ and $X \nsubseteq H$. Then define $\mathrm{div}(L) = \sum_{p \in X} n_p p$, where $n_p = v_p(L/z_i)$ for any coordinate $z_i(p) \neq 0$ - this doesn't depend on i. Then n_p is nonzero only for $p \in Z \cap H$. Note that these are not principal because $\deg L$ is $\geq$ than the number of intersection points of X and H.

Keep in mind that $\overline{\mathbb{V}(y - x^2)}$ in $\mathbb{P}^2$, then $\mathrm{div}(X)$ is $2 \cdot (0,0)$.

Given $D, E \in \mathrm{Div}^d(X)$, we say that $D \sim E$ (linear equivalence) if $D - E = \mathrm{div} f$.

Proposition 7.15. *Given $X \subseteq \mathbb{P}^r_K$ and $L_1, L_2 \in \mathcal{O}_{\mathbb{P}^r}(1)$ such that $\mathbb{V}(L_i) \nsupseteq X$, then $\mathrm{div}(L_1) \sim \mathrm{div}(L_2)$.*

Proof. $\mathrm{div}(L_1) - \mathrm{div}(L_2) = \mathrm{div}(L_1/L_2)$. $\square$

If X is a projective curve it can be exhibited as $\mathbb{V}(I) \subseteq \mathbb{P}^N$ for different choices of I, N. Is there a canonical way of doing so?

Last time, we saw that, given $X \subseteq \mathbb{P}^r$ a curve and $L \in \mathcal{O}_{\mathbb{P}^r}(1)$ and $H = \mathbb{V}(L)$, we obtained a divisor on X whose support lies on $H \cap X$, defined by $\operatorname{div}(L) = \sum n_p p$ where $n_p = \operatorname{ord}_p(L/z_i)$ for some $z_i(p) \neq 0$.

If H is chosen generically then $\operatorname{div}(L) = \sum_{p \in X}[p]$. For divisors D_1, D_2 given by $D_i = \operatorname{div}(L_i)$, where $L_1, L_2 \in \mathcal{O}_{\mathbb{P}^r}(1)$, the principal divisor. $\operatorname{div}(L_1/L_2) = D_1 - D2 \implies D_1 \sim D_2$.

There's no reason to restrict H to be a hyperplane - any hypersurface will do. Analogously, given $F \in \mathcal{O}_{\mathbb{P}^r}(d)$ with $\mathbb{V}(F) \not\supseteq X$, we can define $\operatorname{div}(F)$ on X by taking $n_p = \operatorname{ord}_p(F/z_i^d)$ for $z_i(p) \neq 0$.

Theorem 7.16 (Bezout's Theorem). *Given $X \subseteq \mathbb{P}^2$ and $Y = \mathbb{V}(F)$, $F \in \mathcal{O}_{\mathbb{P}^2}(d)$. If $\deg(X) = c$, then $\#(X \cap Y) \leq cd$, and we have equality if we count with multiplicity.*

Proof. Take $F = \prod_{i=1}^d L_i$, of generically chosen linear forms, and then reduce to the case already proved. $\qquad\square$

A divisor $D \in \operatorname{Div}(X)$ is ***effective*** if $D = \sum n_p[p]$ with $n_p \geq 0$.

Let D be a divisor. We want to consider rational functions on X with poles bounded by D. We define:

$$L(D) = \{0\} \cup \{f \in K(X)^* : \operatorname{div}(f) + D \text{ is effective}\}$$

It is easy to see that this is a vector space over K. It is harder to see that if $D \sim E$ then there is an isomorphism $L(D) \xrightarrow{\cong} L(E)$, and it is a non-examinable fact that $L(D)$ is always finite dimensional.

If $D \sim E$ then $D - E = \operatorname{div}(g)$ for $g \in K(X)^*$. Now observe that multiplication by g gives $L(D) \xrightarrow{\times g} L(E)$.

Given $L(D)$, if we choose a basis $F_1, \ldots, F_s$, we obtain a morphism:

$$X \to \mathbb{P}^s$$
$$p \mapsto [1 : F_1(p) : \ldots : F_s(p)]$$

Proposition 7.17. *Given a divisor D, let $\ell(D) = \dim_K L(D)$.*

1. *If $\deg D < 0$, then $\ell(D) = 0$.*

2. *For any $p \in X$, $\ell(D) \leq \ell(D - p) + 1$.*

3. *If $\deg D \geq 0$, $\ell(D) \leq d + 1$.*

Proof.

1. Suppose $f \in L(D)$ is nonzero. Then $E = \operatorname{div}(f) + D \geq 0$, so is effective. But E has the same degree as D since $\deg(\operatorname{div}(f)) = 0 \nleq$.

2. Consider the following map. If $p \in X$ and $n = n_p$, writing $\sum n_p[p] = D$, pick a local parameter at p and consider:

$$L(D) \to K$$
$$f \mapsto \pi_p^n f(p)$$

$L(D - p)$ is the kernel of this map.

3. Apply 2. repeatedly.

$\square$

The residue theorem from complex analysis says that, given a meromorphic function on $\mathbb{P}^1$, $\sum_{p \in \mathbb{P}^1} Res(f, p) = 0$. There is a similar statement for Riemann surfaces.

7.4   Differentials

Let L/K be an extension. The space of **Kahler differentials** is the quotient M/N where $M = $ vector space over K generated by symbols $\delta x, x \in L$, and N is the vector space of relations given by $\delta(x + y) = \delta x + \delta y$, $\delta(xy) = x\delta y + y\delta x$, $\delta a = 0$ for $a \in K$.

The image of δx in M/N is denoted dx. We define $\Omega_{L/K} = M/N$. There is a canonical map $K \to \Omega_{L/K}$, $f \mapsto df$.

We will now develop a meaningful way to take $\omega \in \Omega_{L/K}$ for $L = K(X)$, and produce a canonical divisor class $\operatorname{div}(\omega) \in \operatorname{Pic}(X)$.

A **K-linear derivation** is an L-vector space U and a map $D : L \to U$ satisfying the product rule $D(xy) = xD(y) + yD(x)$. For any K-derivation D there exists a unique factorization making

$$
\begin{array}{ccc}
\Omega_L & \xrightarrow{\quad \lambda \quad} & U \\
& \nwarrow \qquad \nearrow & \\
& L &
\end{array}
$$

commute. Moreover, every derivation to a vector space U is given by such a λ.

Lemma 7.18. *If $f = g/h$ for $g, h \in K[z_1, \dots, z_n]$ such that $y = f(x_1, \dots, x_n) \in L$ (and so $x_i \in L$), then:*

$$
dy = \sum_{i=1}^{w} \frac{\partial f}{\partial z_i}(z_1, \dots, x_n) dx_i
$$

If $L = K(x, \dots, x_n)$, then Ω_L is spanned by $dx_1, \dots, dx_n$

Proof. The first part follows by calculus - this is precisely how we constructed Ω_L, and the second follows from the first. $\square$

Lemma 7.19. *Let $K(x)$ be purely transcendental and $L/K(x)$ be a finite and separable extension. Then Ω_L is spanned by dx.*

Proof. If $L = K(x)$ then $\dim_L \Omega_L \leq 1$. To show that Ω_L is nonzero, it suffices to exhibit a nonzero derivation. Take $\frac{d}{dx} : K(x) \to K(x)$. If $L \neq K(x)$ then take $L = K(x, \alpha)$ where α is algebraic over $K(x)$ by the primitive element theorem. Let $L_0 = K(x)$, and $h(y) \in L_0[y]$ be the minimal polynomial of d. Then:

$$
0 = d(h(\alpha)) = D_x h(\alpha) dx + h'(\alpha) d\alpha
$$

26

So $d\alpha$ lies in the span of dx, and so dx spans Ω_L. To show that Ω_L is nonzero, we'll exhibit a derivation on $L = L_0(\alpha) = L_0[y]/h(y)$.

We then define $D : L_0[y] \to L$ by, if $f \in L_0$, then $D(f) = D_x(f)$, and otherwise $D(y) = \frac{-D_x(h(\alpha))}{h'(\alpha)}, D(y^n) = n\alpha^{n-1}D(y)$. We can check this vanishes on (h), and so gives a derivation on K, and its restriction to L_0 is the derivation $\frac{d}{dx}$, so is nonzero. $\qquad\square$

Given a point $p \in X$, we define the **_meromorphic differentials on X that are regular at p_**, $\Omega_{X,p} = \{\omega \in \Omega_L : \exists\, f_i, g_i \in \mathcal{O}_{X,p} : \omega = \sum f_i dg_i\}$.

Proposition 7.20. *The $\mathcal{O}_{X,p}$-module $\Omega_{X,p}$ is freely generated by $d\pi_p$, where π_p is any local parameter at p.*

Sketch proof. Firstly we show that $\Omega_{X,p}$ is finitely generated, which is done by choosing an affine chart, and then we apply Nakayama's lemma. $\qquad\square$

Given this, let $\omega \in \Omega_L$, then we can define a divisor:

$$\mathrm{div}(\omega) = \sum_{p \in X} n_p[p], n_p := \mathrm{ord}_p(f), \omega = f \cdot d\pi_p$$

Example: Let $X = \mathbb{P}^1_K$, with coordinate t, and take $\omega = dt$. A local parameter at any point $p \neq \infty$ is given by t. Thus $v_p(\omega) = 0$ for all $p \neq \infty$, as 1 vanishes to order 0 everywhere. Near ∞, the local parameter is $1/t$, so $dt = t^{-2}d(1/t)$, so $\mathrm{div}(\omega) = -2[\infty]$.

Let $\omega \in \Omega_K$. Then the class of $[\mathrm{div}(\omega)] \in \mathrm{Pic}(X)$ is called the **_canonical divisor class_**, and is denoted K_X. The **_genus_** of an algebraic curve X is defined to be:

$$g(X) = \dim_K L(K_X)$$

If X is a curve over $\mathbb{C}$, we can consider the associated Euclidean topological space over $\mathbb{R}$. If $g(X) = g$, then X is determined up to homeomorphism to be a genus g surface in the topological sense. It is useful to think of $g(X)$ as begin related to the curvature of X, where $g = 0$ means positive curvature, $g = 1$ means no curvature, and $g \geq 2$ means negatively curved.

So now our goal is to compute $\ell(D)$ for some divisor D based on $d = \deg D$ and $g = g(X)$.

Theorem 7.21 (Riemann). *$\ell(D) \geq d - g + 1$, where $\ell(D) = \dim_K L(D)$.*

Note that if $X = \mathbb{P}^1$, then $\ell(D) = d + 1$, as $D \equiv d[\infty]$ by example sheet 3, so $L(D) = \langle 1, x, x^2, \ldots, x^d \rangle$. If $g \geq 1$, then each element in a basis for $L(K_X)$ produces a constraint on the form of elements of $L(D)$ for any D.

Theorem 7.22 (Riemann-Roch). *For X a curve and $D \in \mathrm{Div}(X)$, $d = \deg(D)$, we have $\ell(D) - \ell(K_X - D) = d - g + 1$.*

This theorem has some consequences: if $K_X = D$, we get that $\deg(K_X) = 2g - 2$, and if $\deg(D) > 2g - 2$ then $\ell(D) = d - g + 1$. We say this is "above the Riemann-Roch range". Our goal is thus hard to do when the degree is small, but easy when it's large. If $g(X) \geq 1$ then there are no degree 1 divisors on X, i.e. points in X with $\ell(p) = 1$. This is because there are no non-constant meromorphic functions with exactly 1 order 1 pole. A harder thing to show is that for every $g \geq 1$ there is a curve X with $g(X) = g$ such that X admits a non-constant degree 2 morphism to $\mathbb{P}^1$.

Proposition 7.23. *If X is a curve in $\mathbb{P}^2$ then the canonical divisor on X is given by $(d-3)H$ where d is the degree of X and H is the divisor of a hyperplane (line) section.*

Proof. Choose coordinates on $\mathbb{P}^2$ such that $[0:1:0] \notin X$. Write $X = \mathbb{V}(F), F \in \mathcal{O}_{\mathbb{P}^2}(3)$, and dehomogenize away from $\{Z_0 = 0\}$. Let $x = \frac{Z_1}{Z_0}$, $y = \frac{Z_2}{Z_0}$ - view this as elements in $K(X)$. Then $f(x,y) = 0, f(T_1, T_2) = F(1, T_1, T_2)$.

In Ω_X, $\frac{\partial f}{\partial T_1}(x,y)dx + \frac{\partial f}{\partial T_2}(x,y)dy = 0$.

Choose $\omega = \frac{dx}{(\partial f/\partial T_2)(x,y)} = \frac{-dy}{(\partial f/\partial T_1)(x,y)}$. Claim: $\mathrm{div}(\omega) = (d-3)H_\infty$, where H_∞ is the divisor associated to Z_0.

We find local parameters to calculate $v_p(\omega)$ for $p \in X$. If $\frac{\partial f}{\partial T_2}(p)$ is nonzero, then $x - x(p)$ is a local parameter. Otherwise $y - y(p)$ is a local parameter. Thus calculation shows that there are no zeros or poles for ω on the patch $\mathbb{P}^2_K \setminus \{Z_0 = 0\}$. Now we do the calculation at infinity. Note that any point at infinity is contained in $\{Z_2 \neq 0\}$. On this patch, the equation for X is given by

$$g(S_1, S_2) = F(S_1, S_2, 1) \text{ and } z = \frac{Z_0}{Z_2} = \frac{1}{y}, w = \frac{Z_2}{Z_2} = \frac{x}{y}$$

Take $\eta = \frac{dz}{(\partial g/\partial S_2)(z,w)} = \frac{-dw}{(\partial g/\partial S_1)(z,w)}$ to be another form. Note η has no zeroes or poles on $X \cap \{Z_2 \neq 0\}$. Using the formal calculus and a change of coordinates, $\omega = z^{d-3}\eta$. Then $\mathrm{div}(\omega) = (d-3)\,\mathrm{div}\, z = (d-3)H_\infty$. $\square$

Corollary 7.24. *The degree-genus formula for $\mathbb{P}^2$: for $d \geq 3$,*

$$g(X) = \binom{d-1}{2}$$

Proposition 7.25. *If $X \subseteq \mathbb{P}^2$ is a smooth degree d curve then if K_X denotes the canonical divisor, then $K_X = (d-3)H$, where H is the divisor associated to any line in $\mathbb{P}^2$.*

Corollary 7.26. *Given $X \subseteq \mathbb{P}^2$ as above, with $X = \overline{\mathbb{V}(f(x,y) = 0)}$, then $L(K_X)$ has at basis given by $\{\frac{x^r y^s}{\partial f/\partial y}dx : 0 \leq r+s \leq d-3\}$.*

Example sheet 4 gives a version of this proposition and the degree-genus formula for $\mathbb{P}^1 \times \mathbb{P}^1$.

8 Elliptic Curves

An ***elliptic curve*** is a smooth projective irreducible curve E of genus 1, together with a choice of point $p_0 \in E$. An elliptic curve is group, i.e. it has a multiplication map $m : E \times E \to E$, constructed as follows:

Given points $p, q \in E$, then $\ell(p+1-p_0) = 1$ by Riemann-Roch, since the canonical divisor on a genus 1 curve is trivial. I.e., there is a unique rational function $f \in K(E)$ with $\mathrm{div}(f)+p+q-r \geq 0$, and so there is unique point $r \in E$ with $p + q - p_0 \sim r$. Then we set $p +_{E,p_0} q = r$.

Theorem 8.1. *The addition operation above turns (E, p_0) into an abelian group. Moreover, the map $AJ : E \to \mathrm{Jac}(E)(\mathrm{Div}^0(E)/ \sim) =; p \mapsto [p - p_0]$ is an isomorphism of groups. AJ is for Abel-Jacobi.*

Proof. Homomorphism property is clear. We'll check that AJ is injective and surjective.

For injectivity, if $AJ(p) = AJ(q)$, then $p - p_0 \sim q - p_0$, so in fact $p \sim q$. Then $p - q = \mathrm{div}(f)$. But there is a unique function up to a scalar with a pole at p, since $L(p) = K$. Since any such f is constant, $p = q$.

For surjectivity, let $D \in \mathrm{Div}^0(E)$. Then $D + p_0$ has degree 1, and so by Riemann-Roch, $\ell(D + p_0) = 1$. Therefore, $D + p_0$ is equivalent to an effective divisor or degree 1. So $D = p - p_0$ for some $p \in E$. But then $AJ(p) = [D]$. $\qquad \square$

For a concrete version, it is a fact that we'll prove eventually that every genus 1 curve is isomorphic to a cubic in $\mathbb{P}^2$ given by $\mathbb{V}(F)$ for $F = Z_0 Z_2^2 = \prod_{i=1}^3 (Z_1 - \lambda_i Z_0)$ with $\lambda_1, \lambda_2, \lambda_3 \in K$ distinct.

Theorem 8.2. *Take $E \subseteq \mathbb{P}^2$ a cubic curve with $p_0 = [0 : 0 : 1]$. Then the group law on (E, p_0) is given as follows: $p +_E q +_E r = p_0$ (i.e. the identity in (E, p_0)) if and only if p, q, r are collinear.*

Proof. $p +_E q +_E r = \mathrm{id}_E = p_0 \iff p + q r - 3p_0 \sim 0$. This latter condition holds iff $\mathrm{div}(f) = p + q + r - 3p_0$ for some $f \in K(E)$. Now observe that $\ell(3p_0) = 3$ by Riemann-Roch, and in fact:

$$L(3p_0) = \langle 1, \frac{Z_1}{Z_0}, \frac{Z_2}{Z_0} \rangle = \langle 1, x, y \rangle$$

Geometrically, this is because $E \cap \{Z_0 = 0\}$ is p_0 with multiplicity 3. Then f must be given as $\frac{G}{Z_0}$ where G is a linear form, i.e. $G = \mathcal{O}_{\mathbb{P}^2}(1)$. Then $\mathrm{div}(G) = p + q + 1$, but $\mathbb{V}(G)$ is a line so p, q, r lie on a line. $\qquad \square$

How about $g > 1$? If $g(X) \neq 1$, then X is never a group. However, $\mathrm{Jac}(X)$ is always both a group and projective variety, and AJ is always injective $X \to \mathrm{Jac}(X)$.

9 Morphisms of Smooth Curves

Here, curves are smooth and projective. What we want to understand is: given a morphism $\varphi : X \to Y$ between two curves, how does the genus of X relate to the genus of Y. Recall, the genus $g(X) = \ell(K_X)$ for K_X a canonical divisor, and $2g - 2 = \deg K_X$, by Riemann-Roch. If φ is non-constant then φ is surjective. Associated to φ is the ramification data $\varphi : X \to Y, p \in X, q = \varphi(p)$. Then $e_p = v_p(\varphi^* \pi_q)$.

In $\mathbb{C}$-analysis we're taking a local parameter t near q, expanding $\varphi^* t$ in a power series near p and taking the leading term's exponent. Based on this we study the function $\mathbb{C} \to \mathbb{C}, z \mapsto z^e$. 0 has a unique preimage, but any nonzero $z_0 \in \mathbb{C}$ has e preimages.

Theorem 9.1 (Riemann-Hurwitz)**.** *If $\mathrm{char}\, K \neq 0$, given $\varphi : X \to Y$ non-constant, then $2g(X) - 2 = d(2g(Y) - d) + \sum_{p \in X}(e_p - 2)$, where $\deg \varphi = d$.*

Recall $2g - 2$ is the Euler characteristic of a Riemann surface of genus g. So, thinking about triangulations, we're basically saying that we get d times as many triangles in X as in Y, but we've overcounted because of the points where this map locally looks like $z \mapsto z^e$, and we have $e_p - 1$ too many vertices, so we need the correction factor.

Proof. Given $\varphi : X \to Y$, let $\omega = f dt \in \Omega_Y$, where $f \in K(Y)$, and $K \subseteq K(t) \subseteq K(Y)$ is such that $K(t)$ is pure transcendental and $[K(Y) : K(t)]$ is finite. Then $K(X)/K(t)$ is also finite, and Ω_X is generated by $\varphi^* dt$. Given $f \in K(Y)$, define $\varphi^* f \in K(X)$ by composition, i.e. $\varphi^*(f dt) = \varphi^* f d(\varphi^* t)$, getting $\varphi^* : \Omega_Y \to \Omega_X$. The goal is to calculate $\deg K_X$ and $\deg K_Y$ and relate using φ^*.

Lemma 9.2. *Let $\varphi : X \to Y$ and $p \in X$ with $q = \varphi(p)$. Then for $\omega \in \Omega_Y$, we have $v_p(\varphi^*\omega) = e_p v_q(\omega) + e - 1$, where e_p is the ramification index.*

Proof. Observe that if π_p and π_q are local parameters, then $\varphi^*\pi_q = \pi_p^{e_p} \implies d(\varphi^*\pi_q) = d(\pi_p^{e_p}) = e_p \pi_p^{e_p - 1} d\pi_p$. Now apply this to a local expression for ω as $f d\pi_q$ $\qquad\square$

Then:

$$
\begin{aligned}
2g(X) - 2 &= \deg \operatorname{div}(\varphi^*\omega) \\
&= \sum_{p \in X} v_p(\varphi^*\omega) \\
&= \sum_{q \in Y} \sum_{p \mapsto q} v_p(\varphi^*\omega) \\
&= \sum_{q \in Y} \sum_{p \mapsto q} (e_p v_p(\omega) + e_p - 1) \\
&= \sum_{q \in Y} d v_q (\omega + \sum_{p \mapsto q} e_p - 1) \\
&= d(2g(Y) - 2) + \sum_{p \in X} (e_p - 1)
\end{aligned}
$$

$\qquad\square$

Theorem 9.3 (Luroth)**.** *Let $K = \bar{K}$ be a field and consider a tower $K \subseteq L \subseteq K(t)$. Then L is purely transcendental over K.*

Theorem 9.4 (Fermat's Last Theorem for Polynomials)**.** *Let $K = \bar{K}$ and $\operatorname{char} K = 0$. Then if $f, g, h \in K[x, y]$ are homogeneous non-constant such that $f^n + g^n = h^n$, then $n \leq 2$.*

Both of these are really just corollaries of:

Corollary 9.5. *If $\varphi : X \to Y$ is as above, i.e. a non-constant morphism, then $g(X) \geq g(Y)$.*

Proof of FLT for Polynomials. Consider $X = \mathbb{V}(Z_0^n + Z_1^n - Z_2^n) \subseteq \mathbb{P}_K^2$. Then we can check that if X is a nonsingular curve of genus $g(x) = \frac{(n-1)(n-2)}{2}$. If such f, g, h existed, then we would have a morphism $\mathbb{P}^1 \to \mathbb{P}^2$ splitting via X given by $[x : y] \mapsto [f(x, y) : g(x, y) : h(x, y)]$. So we get $\mathbb{P}^1 \to X$ non-constant by hypothesis. Since $g(\mathbb{P}^1) = 0$, $\frac{(n-1)(n-2)}{2} = 0$ and so $n \leq 2$. $\qquad\square$

Our next goal is to attach to each curve X a canonical collection of morphisms $X \to \mathbb{P}^r$.

Let X be a curve and $D \in \operatorname{Div}(X)$. Choose a basis for the vector space $L(D)$, say $\{\varphi_0, \varphi_1\}$. Then there is a well defined morphism $\varphi_0 : X \to \mathbb{P}^r$ given by $p \mapsto [\varphi_0(p) : \ldots : \varphi_r(p)]$, defined everywhere since X is a smooth projective curve. If $D \sim D'$, then φ_D and $\varphi_{D'}$ give the same morphism upto an $PGL(r+1)$ action on $\mathbb{P}^r$, i.e. there is a rational function $f \in K(X)$ such that

$\text{div}(f) = D - D'$, and so $L(D) \mapsto L(D')$ by multiplication by f, and so after choosing bases we get the same map.

We say $\varphi : X \to \mathbb{P}^r$ is an ***embedding*** if X is isomorphic to $\text{im}(\varphi)$. Some examples of non-embeddings are things like $\mathbb{A}^1 \coprod \mathbb{A}^1 \to \mathbb{A}^2$ via $\mathbb{V}(xy)$ - two disjoint lines going to two lines crossing over. This is non-injective, so not an embedding. The other classic example is $\mathbb{A}^1 \to \mathbb{A}^2$, $t \mapsto (t^2, t^3)$. This is injective but the image has a cusp and so it is not an embedding.

Let $X \hookrightarrow \mathbb{P}^r$ be an embedding of a curve. If, given $p, q \in X$, there exist $F, G \text{in} \mathcal{O}_{\mathbb{P}^r}(1)$ such that $F(p) \neq 0$ and $G(p) = 0 \neq G(q)$. Then if we let D be the divisor associated with the hyperplane H in $\mathbb{P}^r$, i.e. $D = H \cap X$ with multiplicity, if $i^* : \mathcal{O}_{\mathbb{P}^r}(1) \to L(D)$, then $i^*F \in L(D) \setminus L(D - p)$, and $i^*G \in L(D - p) \setminus L(D - p - q)$. Since X is smooth it has a tangent line at $T_pX \subseteq \mathbb{P}^r$. So there exists $F \in \mathcal{O}_{\mathbb{P}^r}(1)$ that vanishes at p and not identically on T_pX. This implies that $i*F \in L(D - p) \setminus L(D - 2p)$.

These conditions are equivalent to the following: for any $p, q \in X, \ell(D - p - q) = \ell(D) - 2$. This is because given $D \in \text{Div}\, X, \ell(D_p) \geq \ell(D) - 1$.

Theorem 9.6 (Embedding Criterion)**.** *Let X be a smooth curve and $D \in \text{Div}\, X$, then φ_D is an embedding if and only if D satisfies for any $p, q \in X, \ell(D - p - q) = \ell(D) - 2$.*

Proof sketch. Smooth projective birational curves are isomorphic. This condition certainly guarantees that φ_D is an injection, and taking $p = q$ lets us say that φ_D is injective over tangent spaces as well, so $\text{im}(\varphi_D)$ is smooth. $\qquad\square$

Corollary 9.7. *Let $D \in \text{Div}\, X$ of degree at least $2g + 1$. Then $\varphi_D : X \to \mathbb{P}^{\ell(D)-1}$ is an embedding.*

Proof. Degrees of $D, D - p, D - q - p$ are all at least $2g - 1$, so $K - d, K - (D - p), D_(D - p - q)$ all have negative degree where K is the canonical divisor of X. So $\ell(K - D) = 0$. We conclude that for all $p, q \in X, \ell(D - p - q) = \ell(D) - 2$. $\qquad\square$

If $g = 2$, then $2g - 2 = 2, 2g + 1 = 5$, so $3K_X$ has degree ≥ 5. If $g \geq 3$ then $2g - 2 \geq 4, 2g + 1 < 4 - 2 = 2(2g - 2)$.

Corollary 9.8. *Let X be any curve. Then the morphism $\varphi_{3K} : X \to \mathbb{P}^{\ell(3K)-1}$ is an embedding.*

$\ell(3K) = (6g - 6) - g + 1 = 5g - 5$, so every genus g curve embeds in $\mathbb{P}^{5g+6}$.

In a low genus, such as $g = 1$ for elliptic curves, we have (E, p_0) say. Then we get $\varphi_{3p_0} : E \to \mathbb{P}^2$ of degree 3, so every elliptic curve is a cubic.

Let E be a curve of genus 1 and $p_0 \in E$ so that (E, p_0) is an elliptic curve.

If $g(X) = 0, 1$ then K_X is either negative of zero, so K_X never embeds the curve X. If $g(X) = 0$, then $K_X = K_{\mathbb{P}_1} = -2[\infty]$, so $-K_X$ gives an embedding of $\mathbb{P}^1$ into $\mathbb{P}^2$ as a conic. But if $g(X) = 1$, it is not clear how to construct a canonical embedding.

Theorem 9.9. *Any such elliptic curve (E, p_0) can be realized as the vanishing $\mathbb{V}(F) \subseteq \mathbb{P}^2$ where $F \in \mathcal{O}_{\mathbb{P}^2}(3)$, and $F(1, x, y) = y^2 + a_1 xy + a_3 y - (x^3 + a_2 x^2 + a_4 x + a_5)$ which we call Weierstrass Normal Form. If $\text{char}\, K \neq 2$, we can take $F(1, x, y) = y^2 - x(x - 1)(x - \lambda)$, which is Legendre normal form.*

Proof. Take $D = 3p_0$. Since $g(E) = 1$, if $p \in E$ then $\ell(np) = n$ for all $n \geq 1$ by Riemann-Roch. Then:

- $L(p_0) = K$
- $L(2p_0) = k^2 = \langle 1, x \rangle, v_{p_0}(x) = -2$
- $L(3p_0) = \langle 1, x, y \rangle, v_{p_0}(y) = -3$
- $L(4p_0) = L(3p_0) \oplus K \cdot x^2$
- $L(5p_0) = L(4p_0) \oplus K \cdot xy$
- $L(6p_0)$ contains both x^3 and y^2, and $\dim_K(L(6p_0)) = 6$

So $\{1, x, x^2, x^3, xy, y, y^2\}$ has a linear dependence. So extract $F(1, x, y)$ from this linear dependence to get the Weierstrass form, and call the homogenization $F(z_0, z_1, z_2)$. Then take $E \dashrightarrow \mathbb{P}^2, p \mapsto [1, x(p), y(p)]$ and observe that it satisfies the equation $F(z_0, z_1, z_2) = 0$.

Now since E and $\mathbb{V}(F)$ are both smooth and projective, this rational map extends to an isomorphism.

In char $K = 2$, complete the square to get the Legendre form. $\square$

A **hyperelliptic curve** is a smooth projective curve X of genus ≥ 2 such that there exists a non-constant morphism of degree 2 from $X \to \mathbb{P}^1$, or equivalently if there exists a divisor D with $\deg D = 2, \ell(D) = 2$.

Lemma 9.10. *If $g(X) = 2$, then X is hyperelliptic.*

Proof. Take $D = K_X$, this has degree 2 and $\ell(K_X) = 2$ by Riemann-Roch. $\square$

For every $g \geq 2$ there is a hyperelliptic curve X with $g(X) = g$. By Riemann-Hurwitz, given a 2-to-1 morphism $X \xrightarrow{f} \mathbb{P}^2$, there are exactly $2g + 2$ branch points, i.e. points $p \in \mathbb{P}^1$ such that $f^{-1}(p)$ is a single point.

As a sanity check, if $g = 0$ check that $\mathbb{P}^1 \to \mathbb{P}^1$ via $z \mapsto z^2$ has precisely 2 branching points - 0 and ∞.

Theorem 9.11. *Let X be a curve of $g \geq 3$, then the morphism $\varphi_{K_Y} : X \to \mathbb{P}^{g-1}$ is an embedding if and only if X is non-hyperelliptic.*

Proof. If $\varphi_K : X \to \mathbb{P}^{g-1}$ is not an embedding, then there exists $p, q \in X$ with $\ell(K_X - p - q) \geq g - 1$. Then if $D = p + q$, Riemann-Roch gives $\ell(D) - \ell(K - D) = d - g + 1$, and so $\ell(D) \geq 2$, X is hyperelliptic. $\square$

We say X has a g_d^r if X admits a map $X \to \mathbb{P}^r$ of degree d with image not contained in a hyperplane.

Theorem 9.12 (Enriques-Babbage)**.** *If X is a curve of genus ≥ 3 then if X has no g_2^1, g_3^1 or g_5^2 then the image of $\varphi_{K_X} : X \hookrightarrow \mathbb{P}^{g-1}$ is equal to the vanishing of quadrics.*

Not having a g_2^1, g_3^1 or g_5^2 is a generic behaviour.