Lecture 1

Closed sets and the Zariski topology

Let k be an infinite field (e.g. $\mathbb{Q}, \mathbb{R}., \mathbb{C}$, or $\overline{\mathcal{F}}_q$), and let $k[x_1, \ldots x_n]$ be the polynomial ring in n indeterminants. We will often abbreviate $k[x_1, \ldots, x_n]$ by $k[x]$.

We call an n-tuple $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_+^n$ a multi-index. For any multi-index α, define the monomial x^α by

$$x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

We also define the degree of x^α to be $\deg(x^\alpha) = \sum \alpha_i$. The point of assming k is infinite is the next Proposition.

Proposition 1.1. *Let k be an infinite field. Then two elements $f, g \in k[x_1, \ldots, x_n]$ coincide if and only if $f(a) = g(a)$ for all $a \in k$.*

Exercise 1.1 (30 pushups). Prove Proposition 1.1.

Let $\mathbb{A}^n = \mathbb{A}_k^n$ denote affine n-space over k. Thus a point of $\mathbb{A}^n$ is an n-tuple $(a_1, a_2, \ldots, a_n)$ with each $a_i \in k$.

Definition 1.1. If $\mathcal{F} \subset k[x_1, \ldots x_n]$, let $V(\mathcal{F}) \subset \mathbb{A}^n$ denote the common zeros of the elements of $\mathcal{F}$. That is,

$$V(\mathcal{F}) = \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall \ f \in \mathcal{F}\}.$$

A subset X of $\mathbb{A}^n$ of the form $V(\mathcal{F})$ is said to be *Zariski closed* in $\mathbb{A}^n$. A Zariski closed subset is also called a *closed algebraic set.*

The Zariski closed sets in $\mathbb{A}^n$ are in fact the closed sets of a topology on $\mathbb{A}^n$ called the *Zariski topology.*

Definition 1.2. A *topology* on a set X is a family $\mathcal{U} = \{\mathcal{U}_\alpha\}_{\alpha \in A}$ of subsets $\mathcal{U}_\alpha \subset X$ (called *open* sets) such that

1. $X, \varnothing \in \mathcal{U}$
2. $\mathcal{U}$ is closed under arbitrary unions:
$$B \subset A \implies \bigcup_{\beta \in B} U_\beta \in \mathcal{U}$$
3. $\mathcal{U}$ is closed under finite intersections:
$$B \subset A \text{ finite } \implies \bigcap_{\beta \in B} U_\beta \in \mathcal{U}.$$

A subset of X is said to be *closed* if it is the complement of an open set.

Definition 1.3. Let $\mathcal{U}$ be a topology. Then $B \subset A$ is a base of $\mathcal{U}$ if for all $\alpha \in A$, there exists a $B_\alpha \subset B$ such that
$$U_\alpha = \bigcup_{\beta \in B_\alpha} U_\beta.$$

Example ($\mathbb{R}$): A basis for the standard topology of $\mathbb{R}$ is the set of open intervals.

Example ($\mathbb{R}^n$): A basis for the classical topology of $\mathbb{R}^n$ is the set of open balls. An important property of the classical topology of $\mathbb{R}^n$ is that distinct points $p, q \in \mathbb{R}^n$ can be separated by open balls, i.e. there exist open balls U and V such that $p \in U$ and $q \in V$ and $U \cap V = \varnothing$. In other words, $\mathbb{R}^n$ is *Hausdorff* (or T_2).

Now we define a topology on $\mathbb{A}_k f^n$, where k is a field. Recall that if $\mathcal{F} \subset k[x_1, \ldots, x_n]$, then $V(\mathcal{F}) = \{x \in \mathbb{A}^n \mid f(x) = 0 \text{ for all } f \in \mathcal{F}\}$ is said to be Zariski closed.

Definition 1.4. The *Zariski topology* on $\mathbb{A}^n$ is the topology whose closed sets are the Zariski closed .

To see that the Zariski topology is indeed a topology, we need the following

Proposition 1.2. *If $\mathcal{F}, \mathcal{G} \subset k[x_1, \ldots, x_n]$, then*

1. $V(\mathcal{F} \cup \mathcal{G}) = V(\mathcal{F}) \cap V(\mathcal{G})$;

2. *$V(\mathcal{F}\mathcal{G}) = V(\mathcal{F}) \cup V(\mathcal{G})$;*

3. *$V(\varnothing) = \mathbb{A}^n$; and*

4. *$V(k[x_1, \ldots, x_n]) = \varnothing$.*

Proof.Clearly $V(\mathcal{F}\cup\mathcal{G}) \subset V(\mathcal{F})\cap V(\mathcal{G})$. Let $a \in V(\mathcal{F})\cap V(\mathcal{G})$, and suppose $h \in \mathcal{F} \cup \mathcal{G}$. If $h \in \mathcal{F}$ then $h(a) = 0$ since $a \in V(\mathcal{F})$, and similarly if $h \in \mathcal{G}$. Hence $a \in V(\mathcal{F}\cup\mathcal{G})$, so we get 1. For 2., let $a \in V(\mathcal{F}\mathcal{G})$. If $a \notin V(\mathcal{F})\cup V(\mathcal{G})$, there are $f \in \mathcal{F}$ and $g \in \mathcal{G}$ such that $f(a) \neq 0$ and $g(a) \neq 0$. Thus $h(a) \neq 0$, where $h = fg$. But $h \in \mathcal{F}\mathcal{G}$, so this is impossible. On the other hand, let $a \in V(\mathcal{F}) \cup V(\mathcal{G})$. Then if $h = fg \in \mathcal{F}\mathcal{G}$, either $f(a) = 0$ and $g(a) = 0$, $h(a) = 0$. Hence $a \in V(\mathcal{F}\mathcal{G})$. The other assertions are clear. □

If $f \in k[x]$, put

$$U_f = \{p \in \mathbb{A}^n \mid f(p) \neq 0\} \qquad \text{or simply} \qquad \{f \neq 0\}.$$

Proposition 1.3. *The collection of principal open sets U_f is a basis for the open sets of the Zariski topology on $\mathbb{A}^n$.*

Example ($\mathbb{A}^1$): The closed sets in $\mathbb{A}^1$ are the finite subsets of k. Therefore, if k is infinite, the Zariski topology on k is not Hausdorff.

Definition 1.5. In a topological space X, the closure $\overline{F}$ of $F \subset X$ is the smallest closed set in X such that $F \subset \overline{F}$. Clearly $\overline{F} = \bigcap_{Y \text{ closed}} Y$.

Exercise 1.2. Show that the Zariski closure of an arbitrary subset $Y \subset \mathbb{A}^n$ is $\overline{Y} = V(\{ f \in k[x_1, \ldots, x_n] \mid f(Y) = 0 \})$.

Example: We saw that in $\mathbb{C}$, the Zariski closed sets are the finite sets. Thus, if Y is infinite, $\overline{Y} = \mathbb{C}$.

If $k = \mathbb{C}$, we can also consider the classical closure ${}^C\overline{Y}$.

Theorem 1.4. *Let X be an affine variety in $\mathbb{C}^n$. Let U be Zariski open in $\mathbb{C}^n$. Then the Zariski closure of $U \cap X$ in X coincides with the classical closure of $U \cap X$ in X.*

For the proof, see *Complex projective varieties* by D. Mumford. Note that the closure need not equal X.

Example: Let $X = V(xy) \subset \mathbb{C}^2$, let $U = \mathbb{C}^2 \backslash \{x = 0\}$. Then $X \cap U = V(y) \cap \{x \neq 0\}$. Then $\overline{X \cap U} = V(y) = {}^C\overline{X \cap U}$.

Exercise 1.3 (15 pushups). Let $k = \mathbb{Z}_p$. Is the Zariski topology on $\mathbb{A}^n$ Hausdorff?

The Hilbert Basis Theorem, which we will prove below, says that every ideal in $k[x]$ is finitely generated. It will follow that every Zariski closed subset of $\mathbb{A}^n$ has the form $V(\mathcal{F})$ where $\mathcal{F}$ is finite.

The Zariski topology is a coarse topology in the sense that it does not have many open sets. In fact, it turns out that $\mathbb{A}^n$ is what is called a Noetherian space.

Definition 1.6. A topological space X is called *Noetherian* if whenever $Y_1 \supset Y_2 \supset Y_2 \supset \cdots$ is a sequence of closed subsets of X, there exists an n such that $Y_n = Y_{n+j}$ for all $j \geq 1$.

EXAMPLE: $k = \mathbb{A}^1$is clearly Noetherian, since every closed subset is finite.

Definition 1.7. A closed subset Y of a topological space is said to be *irreducible* if whenever $Y = Y_1 \cup Y_2$, with Y_i closed, then $Y_1 \not\subset Y_2$ implies $Y_2 \subset Y_1$. Equivalently, Y is irreducible if and only if $Y = Y_1 \cup Y_2$ implies either $Y = Y_1$ or $Y = Y_2$.

Theorem 1.5. *Let X be a Noetherian topological space. Then every closed subset $Y \subset X$ may be uniquely expressed as a union of closed sets:*

$$Y = Y_1 \cup Y_2 \cup \cdots \cup Y_k,$$

where $Y_i \not\subset Y_j$ for all i, j, and each Y_i is irreducible.

PROOF. Suppose Z is a closed set in X which does not have an irreducible decomposition. Then whenever we write $Z = Z_1 \cup Z_2$ with Z_i closed and $Z_i \not\subset Z_j$ $(i \neq j)$, one of Z_1 or Z_2, say Z_1, does not have an irreducible decomposition either. Repeating this argument on Z_1 and so on, we obtain a strictly decreasing sequence of closed sets, none of which admits an irreducible decomposition. But this is impossible since X is Noetherian. To put this another way, consider the set $\mathcal{F}$ of all closed subsets Y of X that do not have such a decomposition. Since X is Noetherian, there exists a minimal closed set Z in $\mathcal{F}$. Thus $Z = Z_1 \cup Z_2$, with Z_i closed and $Z_i \not\subset Z_j$ $(i \neq j)$, as Z cannot be irreducible. But, by definition, Z_1, Z_2 both have irreducible decompositions, so Z does too, which is a contradiction. Hence $\mathcal{F} = \varnothing$.

Now suppose $Y = Z_1 \cup \cdots \cup Z_l = W_1 \cup \cdots \cup W_m$ give two irreducible decompositions of Y with $Z_i \not\subset Z_j$, and $W_i \not\subset W_j$ $(i \neq j)$. Now $Z_1 = (Z_1 \cap W_1) \cup \cdots \cup (Z_1 \cap W_m) = Y_1 \cup \cdots \cup Y_m$, where $Y_i = Z_1 \cap W_i$. We may assume $Y_i \not\subset Y_j$ (discard Y_i if $Y_i \subset Y_j$). Since Z_1 is irreducible, $Z_1 = Z_1 \cap W_i$, for some i. Thus $Z_1 \subset W_i$. Reversing this argument gives $W_i \subset Z_j$ for some j. Thus $Z_1 \subset Z_j$ so $j = 1$. Hence $Z_1 = W_i$ for some i. Since Z_1 was arbitrary, each $Z_m = W_{i_m}$ for some i_m. Interchanging the roles of W_i and

Z_i shows that $m \mapsto i_m$ is one-to-one. Hence the above decompositions agree up to indexing. $\square$

Definition 1.8. The $Y_1, \ldots, Y_k$, as above, are called the *irreducible components* of Y.

EXAMPLE (HYPERSURFACES): Let $f \in k[x_1, \ldots, x_n]$ be a nonconstant polynomial and $Y = V(f)$. Since $k[x]$ is a UFD, we can write $f = \prod_{1 \leq i \leq l} f_i$, where f_i is irreducible. Clearly,

$$Y = V(f_1) \cup \cdots \cup V(f_l).$$

I claim that $V(f_i)$ is irreducible. This is not obvious, and the proof will be postponed until Lecture 2. If two f_i and f_j differ by a unit, $V(f_i) = V(f_j)$. Thus the distinct $V(f_m)$ are the irreducible components of Y.

Lecture 2

The ideal of a variety

In this Lecture. we will introduce the ideal of a closed set and discuss the ideal-variety correspondence. We will also classify irreducible closed sets in $\mathbb{A}^n$.

We begin with the fundamental definition.

Definition 2.1. If $X = V(\mathcal{F})$, let $I(X) = \{ f \in k[x] \mid f(X) = 0 \}$. We call $I(X)$ the *ideal* of X.

The following result is obvious.

Proposition 2.1. *$I(X)$ is an ideal in $k[x]$.*

Exercise 2.1 (20 pushups). Show that if $f_1, \dots, f_r$ generate $I(X)$, then $X = V(f_1, \dots, f_r)$. Also, show $X = V\big(I(X)\big)$.

Proposition 2.2. *Let X_1, X_2 be closed. Then if $X_1 \subset X_2$, we have $I(X_2) \subset I(X_1)$ and conversely.*

Proof. One direction is clear. If $I(X_2) \subset I(X_1)$, then $V\big(I(X_1)\big) \subset V\big(I(X_2)\big)$. Since $V\big(I(X_1)\big) = X_1$, we get that $X_1 \subset X_2$. □

Theorem 2.3. *X is irreducible if and only if $I(X)$ is prime.*

Proof. Recall that $I(X)$ prime means that $fg \in I(X)$ implies that either $f \in I(X)$ or $g \in I(X)$. Suppose X is irreducible. Let $fg \in I(X)$. Now $X \subset V(f) \cup V(g)$, so $X = \big(X \cap V(f)\big) \cup \big(X \cap V(g)\big)$. By irreducibility, $X = X \cap V(f)$, say. Then $X \subset V(f)$ so $f \in I(X)$. Conversely, suppose that $I(X)$ is prime. Write $X = Y \cup Z$, with Y, Z closed, $Y \backslash Z$ and $Z \backslash Y$ nonempty. Then $I(Y) \not\subset I(Z) \not\subset I(Y)$. Let $f \in I(Y) \backslash I(Z)$, $g \in I(Z) \backslash I(Y)$. Then $fg \in I(Y) \cap I(Z)$, so $fg \in I(X)$. But $I(X)$ is prime, a contradiction. □

Exercise 2.2 (20 pushups). Show that if X has irreducible decomposition $X = X_1 \cup X_2 \cup \cdots \cup X_n$, then $I(X) = I(X_1) \cap I(X_2) \cap \cdots \cap I(X_n)$. Thus the ideal $I(X)$ of a Zariski closed set is an intersection of prime ideals.

Definition 2.2. A ring R is called *Noetherian* if either of the following two equivalent conditions hold.

1. Every ideal I in R is finitely generated as an R-module: $I = Rf_1 + Rf_2 + \cdots + Rf_k$ for some $f_1, \ldots, f_k \in I$
2. Every ascending chain of ideals $I_1 \subset I_2 \subset \cdots \subset I_n \subset \ldots$ eventually stabilizes.

Exercise 2.3 (10 pushups). Show that the two conditions are equivalent.

Exercise 2.4 (20 push ups). A k-algebra A is a k-vector space which is also a commutative ring with identity. An example of a k-algebra is $k[f_1, f_2, \ldots, f_s]$, where each $f_i \in k[x]$. A k-algebra A is said to be finitely generated if there exists a surjective ring homomorphism $\phi : k[x] \to A$. Show that a finitely generated k-algebra is Noetherian.

Theorem 2.4 (Hilbert Basissatz). *Let k be an arbitrary field (not necessarily infinite). Then the polynomial ring $k[x_1, \ldots, x_n]$ is Noetherian.*

A more general version of this is

Theorem 2.5. *If R is Noetherian, then so is the polynomial ring $R[x]$ (in one variable).*

We will prove theorem 2.4. For a proof of Theorem 2.5, consult, for example, *Commutative Algebra*, by D. Eisenbud. The we will give, which is taken from *Varieties, Ideals and Algorithms* by Cox. Little and O'Shea, is a nice illustration of techniques used in computational algebraic geometry, namely Gröbner bases. Of course, these ideas are very important in computer science as well. First, let us derive the main consequence.

Corollary 2.6. *$\mathbb{A}^n$ is a Noetherian space*

Proof. Let $Y_1 \supset Y_2 \supset \cdots \supset Y_m \supset \cdots$ be a descending sequence of Zariski closed sets. From this we get an ascending chain of ideals

$$I(Y_1) \subset I(Y_2) \subset \cdots \subset I(Y_m) \subset \cdots .$$

By the basis theorem, there exists a $r > 0$ such that $I(Y_r) = I(Y_{r+l})$ if $l \geq 1$. Thus $Y_r = V\big(I(Y_r)\big) = V\big(I(Y_{r+l})\big) = Y_{r+l}$. □

Remark: We have

$$\left\{\begin{matrix}\text{irreducible}\\ X \subset \mathbb{A}^n\end{matrix}\right\} \hookrightarrow \left\{\begin{matrix}\text{prime ideals}\\ \text{in } k[x]\end{matrix}\right\}$$

However, we don't know this correspondence is surjective. For example, in the case $k = \mathbb{R}$, the ideal $I = \langle x^2 + 1 \rangle$ is prime but is not the ideal of any variety.

Here is an application. Let us define the dimension of an irreducible Zariski closed set in $\mathbb{A}^n$.

Definition 2.3. Define $\dim X$ to be the maximum l such that there exists a sequence of irreducible Zariski closed sets Y_i $(0 \leq i \leq l)$ such that

$$X = Y_0 \supset Y_1 \supset Y_2 \supset \cdots \supset Y_l.$$

Exercise 2.5 (100 pushups). Show that $\dim \mathbb{A}^n = n$.

Lecture 3

Hilbert's Basis Theorem

Hilbert's Basis Theorem, or *Basissatz*, says that every ideal in $k[x_1, \dots, x_n]$ is finitely generated, that is $k[x_1, \dots, x_n]$ is a Noetherian ring. This is one of the first and most fundamental results in commutative algebra. As we have indicated above, one of the main consequences will be that $\mathbb{A}^n$ is a Noetherian space, hence every Zariski closed set in $\mathbb{A}^n$ has a (unique) irreducible decomposition. Before giving the proof, we need to introduce some elementary combinatorial ideas.

Throughout this lecture, k will denote an arbitrary infinite field. Recall $\mathbb{Z}_+$ denotes the nonnegative integers, and note that $\mathbb{Z}_+^n = \{\,(m_1, \dots, m_n) \mid m_i \geq 0\,\}$ is an additive semi-group, that is it is closed under addition. Recall also that for each multi-index $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_+^n$, we have defined a monomial $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \in k[x] = k[x_1, \dots, x_n]$. Clearly, $x^\alpha x^\beta = x^{\alpha+\beta}$, so

Proposition 3.1. *The assignment $\alpha \to x^\alpha$ defines an isomorphism of the additive semigroup $\mathbb{Z}_+^n$ onto the multiplicative semigroup consisting of all monomials $x^\alpha \in k[x]$.*

Proof. Easy. □

Lemma 3.2. *Let $A \subset \mathbb{Z}_+^n$ and let $I_A = \langle x^\alpha \mid \alpha \in A \rangle$. Then x^β is a monomial in I_A if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof.Suppose $x^\beta \in I_A$. Then

$$\begin{aligned} x^\beta &= \sum f_i x^{\alpha_i}, \qquad && \alpha_i \in A \\ &= \sum_{i,\gamma} c_\gamma x^{\alpha_i+\gamma}, \qquad && c_\gamma \in k. \end{aligned}$$

Since $x_1, \dots, x_n$ are indeterminates, the monomials are linearly independent, so all $c_\gamma = 0$ except for the c_γ where $x^{\alpha_i+\gamma} = x^\beta$, and for these $\sum c_\gamma = 1$. Hence there is some $\gamma \in \mathbb{Z}_+^n$ such that $\beta = \alpha + \gamma$, and the result follows. □

Exercise 3.1 (10 pushups). Consider $\mathbb{Z}_+^2$, and let

$$A = \{(1,2), (2,0), (3,1), (2,2)\}.$$

Draw a diagram of A and use the picture to find a minimal set of monomials which generate I_A.

Definition 3.1. An ideal in $k[x]$ which is generated by monomials is called a *monomial ideal.* If $A \subset \mathbb{Z}_+^n$, then we will call $A + \mathbb{Z}_+^n$ an ideal in $\mathbb{Z}_+^n$.

Clearly, the monomial ideals I_A in $k[x]$ correspond bijectively to the ideals $A + \mathbb{Z}_+^n$ in $\mathbb{Z}_+^n$. Let us call a set $a + \mathbb{Z}_+^n$ a *corner.*

Lemma 3.3. *Every ideal $A + \mathbb{Z}_+^n$ is the union of a finite number of corners.*

Exercise 3.2 (30 pushups). Prove Lemma 3.3.

Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{Z}^n$. Let us impose (somewhat arbitrarily) the ordering $e_1 > e_2 > \cdots > e_n$, and let us also say

$$\alpha = \sum_1^n \alpha_i e_i > \beta = \sum_1^n \beta_i e_i$$

if the first nonzero component of $\alpha - \beta$ is positive. We will call this partial order the *lexicographic order* of $\mathbb{Z}_+^n$, (lex for short). Lex satisfies:

1. If $\alpha > \beta$ then $\alpha + \gamma > \beta + \gamma$ for all $\gamma \in \mathbb{Z}_+^n$
2. $>$ is a total order (ie. either $\alpha > \beta$, $\alpha = \beta$, or $\alpha < \beta$ for all $\alpha, \beta \in \mathbb{Z}_+^n$)
3. Every subset of $\mathbb{Z}_+^n$ has a least element

Notice that in the lemma, the exposed corners are characterized as $a + \mathbb{Z}_+^n$, where a is *primitive* in the sense that $a \in A$, but there is no $\beta \in A$ and $\gamma \in \mathbb{Z}_+^n$ such that $\alpha = \beta + \gamma$. Thus Lemma 3.3 says that $A + \mathbb{Z}_+^n$ has only finitely many primitives. For example, $A + \mathbb{Z}_+^n$ has a least element α_0 which is among the elements with least e_n component. A consequence of the lemma, called Dickson's Lemma, is required.

Theorem 3.4 (Dickson's Lemma). *Every monomial ideal is finitely generated.*

Proof.Let I_A be the ideal. Let $\alpha_1, \dots, \alpha_m$ be the primitives in $A + \mathbb{Z}_+^n$. Then

$$A + \mathbb{Z}_+^n = \bigcup_{i=1}^{m} (\alpha_i + \mathbb{Z}_+^n).$$

Thus, every monomial in I_A has the form $x^{\alpha_i+\gamma} = x^{\alpha_i} x^{\gamma}$, for some $\gamma \in \mathbb{Z}_+^n$. Thus, $\langle x^{\alpha_1}, \dots, x^{\alpha_m} \rangle = I_A$, by Lemma 3.2. □

We can now obtain a Euclidean algorithm for $k[x_1, \dots, x_n]$. Recall that the Euclidean algorithm for a polynomial ring $k[x]$ in one variable says that if $f, g \in k[x]$ and $g \neq 0$, then there exist unique $q, r \in k[x]$ such that $f = qg + r$, where either $r = 0$ or the degree of r is less that the degree of g.

First, impose lex order on monomials on x^α. Thus, $x^\alpha > x^\beta$ if and only if $\alpha > \beta$ in lex order on $\mathbb{Z}_+^n$.

Definition 3.2. If $f \in k[x]$, let $\mathrm{LT}(f)$ be the highest monomial that occurs in f with nonzero coefficient.

Example: If $f(x, y, z) = 4x^3yz - 2x^2y^3z + x - 2y$ then x^3yz corresponds to $(3, 1, 1)$, x^2y^3z to $(2, 3, 1)$ etc. So $(3, 1, 1) > (2, 3, 1) > (1, 0, 0) > (0, 1, 0)$, and $LT(f) = x^3yz$.

Theorem 3.5 (Euclidean Algorithm). *Given $f_1, \dots, f_s$ in $k[x_1, \dots, x_n]$, then for any $F \in k[x]$, there exist polynomials $g_1, \dots, g_s$ such that*

$$F = g_1 f_1 + \cdots + g_s f_s + r$$

where either $r = 0$ or r is a linear combination of monomials, none of which are divisible by any of $LT(f_1)$, ..., $LT(f_s)$.

Example: Take $F = xy^2 + 1$, $f_1 = xy + 1$, and $f_2 = y + 1$. Then $F - yf_1 = 1 - y = 2 - (1 - y) = 2 - f_2$, hence $F = yf_1 - f_2 + 2$. Doing the computation again gives $F - xyf_2 = 1 - xy = 1 - x(y+1) + x$, so $F = (xy - x)f_2 + (x + 1)$. This demonstrates that $g_1, \dots, g_s$ and the remainder r are not unique.

The division algorithm is proved just as in the example, so we will skip the proof. You may consult, for example, VIA for a complete proof.

We can now prove the Basissatz.

Proof of Theorem 2.4. Let $I \subset k[x]$ be any ideal, and consider the monomial ideal

$$\mathrm{LT}(I) = \langle x^\alpha \mid x^\alpha = \mathrm{LT}(f) \text{ for some } f \in I \rangle.$$

By Dickson's Lemma, there exist $\alpha_1, \dots, \alpha_m \in \mathbb{Z}_+^n$ such that $LT(I) = \langle x^{\alpha_1}, \dots, x^{\alpha_m} \rangle$. Choose $f_1, \dots, f_m \in I$ such that $\mathrm{LT}(f_i) = x^{\alpha_i}$. Now let

$F \in I$ and apply the division algorithm:

$$F = \sum g_i f_i + r$$

where no monomial in r is divisible by any x^{α_i}. If $r \neq 0$, then $\mathrm{LT}(r) \in LT(I)$, so by Lemma 3.2, $\mathrm{LT}(r)$ is divisible by some α_i. But this contradicts the division algorithm, since no monomial in r is divisible by any $\mathrm{LT}(f_i)$. □

In the proof of the Basissatz, we showed that if $f_1, \dots, f_k \in I$ are such that $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_n)$ generate $\mathrm{LT}(I)$ (which is a monomial ideal and therefore finitely generated), then $f_1, \dots, f_k$ actually generate I. This kind of basis has a special name.

Definition 3.3 (Gröbner Basis). We say that $f_1, \dots, f_k$ is a *Gröbner basis* of an ideal $I \subset k[x]$ if and only if $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_k)$ generate $\mathrm{LT}(I)$.

Here is the nice property of Gröbner bases.

Theorem 3.6. *Let $f_1, \dots, f_s$ be a Gröbner basis of an ideal $I \subset k[x]$, and suppose $F \in k[x]$. Then all expressions*

$$F = g_1 f_1 + \cdots + g_s f_s + r$$

obtained by applying the Euclidean algorithm have the same remainder r.

Proof.Suppose $f'_1, \dots, f'_t$ is another Gröbner basis of I. Let $F \in k[x]$, and apply the Euclidean algorithm to F for both Gröbner bases getting

$$F = \sum g_i f_i + r = \sum h'_j f'_j + r'.$$

Subtracting gives

$$\sum g_i f_i - \sum h_j f'_j + (r - r') = 0$$

Now consider the larger Gröbner basis $f_1, \dots, f_s, f'_1, \dots, f'_t$. If $r \neq r'$ then $\mathrm{LT}(r - r') \neq 0$. But $\mathrm{LT}(r - r') \in \mathrm{LT}(I)$, which is impossible. □

Corollary 3.7. *If $f_1, \dots, f_s$ is a Gröbner basis for I, then any $F \in k[x]$ has a unique expression $F = f + r$, where $f \in I$ and no monomial in r is in $\mathrm{LT}(I)$.*

Example: Most ideal bases aren't Gröbner. Let $I = \langle x + y, xy + 1 \rangle$. Then

$$y(x + y) - (xy + 1) = y^2 - 1 \in I.$$

Thus $y^2 \in \mathrm{LT}(I)$, but $y^2 \notin \langle x, xy \rangle$.

Lecture 4

The Nullstellensatz

Now return to geometry. We have shown that for any closed $X \subset \mathbb{A}^n$, $I(X)$ is finitely generated. In particular, we have

Proposition 4.1. *Let $I(X) = \langle f_1, \ldots, f_s \rangle$. Then $X = V(f_1, \ldots, f_s)$.*

Let's return to a sticking point. Let $f \in k[x]$ be irreducible. Then is the hypersurface $X = V(\{f\})$ an irreducible variety? The answer doesn't seem to be clear. Since f is irreducible, the principal ideal (f) generated by f is prime, but is $I(X) = (f)$? Of course, if $k = \mathbb{R}$, $n = 1$, and $f(x) = x^2 + 1$, then $V(f) = \varnothing$, which is irreducible. However, $I(\varnothing) = k[x]$, and so $I\big(V(f)\big) \underset{\neq}{\supseteq} (f)$. The property we need is the nontrivial fact that if I is prime, $I = I\big(V(I)\big)$. NB: don't confuse this with the obvious property that $X = V(I(X))$. If indeed we have this property, we get a bijection

$$\left\{\begin{matrix}\text{irreducible}\\ \text{closed sets in } \mathbb{A}^n\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{prime ideals}\\ \text{in } k[x]\end{matrix}\right\}.$$

To obtain this, we have to assume k is algebraically closed. The result which gives us the key piece of information is Hilbert's *Nullstellensatz.*

Exercise 4.1 (20 push ups). Suppose k is finite. Show that the only irreducible closed sets in $X\mathbb{A}^n$ are points, and conclude that $I = I(V(I))$ does not hold in general.

Definition 4.1. The *radical* of an ideal I in a commutative ring R is the set

$$\operatorname{Rad}(I) = \sqrt{I} = \{\, f \in R \mid f^n \in I \text{ for some } n > 0 \,\}.$$

Example: Let $I = (y^2 - x + 1, 1 - x)$. Clearly $y^2 \in I$, so $y \in I\big(V(I)\big)$. However, $y \notin I$, so $I \neq \operatorname{Rad}(I)$. It is easy to see that $\operatorname{Rad}(I) = (y, x - 1)$.

An ideal I such that $I = \sqrt{I}$ is called a *radical ideal.*

Proposition 4.2. *For any ideal I in R, $\mathrm{Rad}(I)$ is an ideal. Moreover if I is prime, then $I = \mathrm{Rad}(I)$.*

PROOF. An exercise. □

Exercise 4.2 (10 push ups). Prove Proposition 4.2.

We have asked what $I\big(V(I)\big)$ is. We also asked when is

$$\left\{\begin{matrix}\text{irreducible}\\ \text{closed } X \subset \mathbb{A}^n\end{matrix}\right\} \hookrightarrow \left\{\begin{matrix}\text{prime ideals}\\ \text{in } k[x]\end{matrix}\right\}.$$

surjective?

We may now answer this question. The principal tool is Hilbert's Nullstellensatz. Recall, if $I \subset k[x]$ is an ideal, then $\mathrm{Rad}(I)$ is defined to be $\{\, f \in k[x] \mid f^m \in I \text{ for some } m \geq 0\,\}$.

Theorem 4.3 (Hilbert's Nullstellensatz). *Assume $k = \overline{k}$ (i.e. k is algebraically closed). If $I \subset k[x]$ is any ideal, then $I\big(V(I)\big) = \mathrm{Rad}(I)$.*

It is clear that $\mathrm{Rad}(I) \subset I\big(V(I)\big)$; for if $f^m\big(V(I)\big) = 0$, then $f\big(V(I)\big) = 0$.

Corollary 4.4. *If I is prime, then $I\big(V(I)\big) = I$.*

PROOF. Apply Proposition 4.2. □

Thus, if $k = \overline{k}$, we have two bijections:

$$\left\{\begin{matrix}\text{irreducible}\\ \text{closed } X \subset \mathbb{A}^n\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{prime ideals}\\ \text{in } k[x]\end{matrix}\right\},$$

and

$$\left\{\begin{matrix}\text{closed sets}\\ X \text{ in } \mathbb{A}^n\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{radical ideals}\\ \text{in } k[x]\end{matrix}\right\}.$$

The first step in the proof is to establish an apparently weaker form of the Nullstellensatz , the so-called Weak Nullstellensatz:

Theorem 4.5 (Weak Nullstellensatz). *Assume $k = \overline{k}$. If $I \subset k[x]$ is an ideal such that $V(I) = \varnothing$, then $I = k[x]$.*

PROOF.Assume $I \neq k[x]$. Then I is contained in a maximal ideal $\mathfrak{m}$. (By a maximal ideal, we mean a proper ideal $\mathfrak{m}$ such that, for all $f \in k[x] \setminus \mathfrak{m}$, $\langle \mathfrak{m}, f\rangle = k[x]$. Since any chain $I_1 \subset I_2 \subset \cdots$ of ideals has the property that $\bigcup I_j$ is an ideal, this follows from Zorn's Lemma. Hence $V(\mathfrak{m}) \subset V(I)$. Now we want to show $V(\mathfrak{m}) \neq \varnothing$. Let $F = k[x]/\mathfrak{m}$. Then F is a field extension of k since $k \hookrightarrow k[x] \to k[x]/\mathfrak{m}$ gives an imbedding of k onto a subfield of F. Since $k = \overline{k}$, it will follow that $k \cong F$ via this quotient map provided $\dim_k F < \infty$. Suppose we can show that this is the case. Then choose $a_i \in k$ such that $a_i \mapsto \overline{x}_i$. Then $x_i - a_i \in \mathfrak{m}$. Thus

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle \subset \mathfrak{m}. \tag{4.1}$$

By the Euclidean algorithm , we can express any $f \in k[x]$ as

$$f = \sum h_i(x_i - a_i) + r,$$

where no x_i divides any monomial in r. It follows that for any f, the remaider $r \in k$. Thus $\langle f, x_1 - a_1, \dots, x_n - a_n \rangle = k[x]$ if $r \neq 0$, so the left hand side of (4.1) is a maximal ideal. Consequently $\mathfrak{m} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Therefore $V(\mathfrak{m}) = (a_1, \dots, a_n)$, so $V(I) \neq \varnothing$. □

An important corollary of the proof is

Corollary 4.6. *Any maximal ideal in* $k[x_1, \dots, x_n]$ *is of the form*

$$\langle x_1 - a_1, \dots, x_n - a_n \rangle$$

for some $(a_1, \dots, a_n) \in \mathbb{A}^n$.

Definition 4.2. We call $\mathfrak{m}$ is the *maximal ideal* of $(a_1, \dots, a_n)$.

We now show how to conclude the Nullstellensatz from the Weak Nullstellensatz . After that, we will complete the proof of the Weak Nullstellensatz by showing $\dim_k F < \infty$. The proof uses a trick which goes back to a 1929 paper of Rabinowitsch.

Hilbert's Nullstellensatz. Let $I \subset k[x]$ be an ideal and suppose $f \in I\big(V(I)\big)$. I want to show $f^m \in I$ for some $m > 0$. Let J be the ideal in $k[x_1, \dots, x_n, x_{n+1}]$ generated by I and $x_{n+1}f - 1$. Clearly $V(J) = \varnothing$. Hence $J = k[x_1, \dots, x_{n+1}]$ (this would be trivial if $f \in I$, but we don't know this). Thus $1 \in J$, so

$$\begin{aligned} 1 &= \sum_{s=1}^{r} h_s g_s + h(x_{n+1}f - 1) \\ &= \sum_{t=0}^{m} \tilde{g}_t x_{n+1}^t + h(x_{n+1}f - 1), \end{aligned}$$

for some $h, h_s \in k[x_1, \dots, x_{n+1}]$ and $g_s, \tilde{g}_t \in I$. Now $R = k[x_1, \dots, x_{n+1}]$ is a domain, so we can consider its quotient field, $\overline{R}$. Setting $x_{n+1} = f^{-1}$, we get

$$1 = \sum_{0}^{m} \tilde{g}_t f^{-t}.$$

Clearing the denominators gives

$$f^m = \sum \tilde{g}_t f^{m-t},$$

so $f^m \in I$. □

Lecture 5

Affine varieties

The first important consequence of the Nullstellensatz is that if $I \subset k[x]$ is a radical ideal, then $I = I(V(I))$, provided k is algebrically closed. Hence another consequence is

Theorem 5.1. *Let k be algebraically closed. Then every radical ideal I is the intersection of a finite number of prime ideals. In fact, there exists a unique expression $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_m$ where $\mathfrak{p}_i \not\subset \mathfrak{p}_j$.*

PROOF.Let $X = V(I)$ have irreducible decomposition $X = X_1 \cup \cdots \cup X_m$ where $X_i \not\supset X_j$. Then $I(X) = I(X_1) \cap \ldots I(X_m)$. But $I = I(X)$ since $I(X) = \mathrm{Rad}(I) = I$, and each $I(X_i)$ is prime. □

The *coordinate ring* of a variety $X = V(I) \subset \mathbb{A}^n$ is

$$k[X] = k[x]/I(X) = \{\text{restrictions of polynomials to } X\}.$$

EXAMPLE: If $I = \langle xy - 1\rangle$, and $X = V(I)$ then $k[X] = k[x,y]/I \cong k[x, x^{-1}]$. Note that this is not a field; for example, $(1-x)^{-1} \notin k[x, x^{-1}]$, as

$$1/(1-x) = (1 + x + x^2 + \cdots).$$

Since any monomial $x^k y^j = x^{k-j}$, every element of $k[X]$ can be expressed as $p(x, x^{-1})$.

Proposition 5.2. *Let X be closed in $\mathbb{A}^n$. Then any maximal ideal in $k[X]$ is of the form $\mathfrak{m}_a = \{ f \in k[X] \mid f(a) = 0 \}$ for some $a \in X$.*

PROOF.Let $\mathfrak{m}$ be maximal. Then if $\phi : k[x] \to k[X]$ is the quotient map, $\phi^{-1}(\mathfrak{m})$ is a maximal ideal. Indeed, $\phi^{-1}(\mathfrak{m}) \cong k$. Thus $\phi^{-1}(\mathfrak{m}) = \mathfrak{m}_a$, for some $a \in \mathbb{A}^n$. It follows that if $\overline{f} = \phi(f) \in \mathfrak{m} \subset k[X]$, then $f(a) = 0$. But by definition, $\mathfrak{m}_a \supset I(X)$, so $a \in X$. Therefore, $\mathfrak{m} = \phi(\mathfrak{m}_a) = \{ f \in k[X] \mid f(a) = 0 \}$ for some $a \in X$. □

Corollary 5.3. *Every ring homomorphism $\phi : k[x] \to k$ sending 1 to 1 has the form $\phi(f) = f(a)$ for some $a \in X$.*

Proof. Let ϕ be such a morphism. Then I claim $\ker(\phi)$ is a maximal ideal. For since $\phi(1) = 1$, it follows that $k[x]/\ker(\phi) \cong k$. But as k is a field, $\ker(\phi)$ must be maximal. Thus there exists $a \in X$ for which $\ker(\phi) = \{f \in k[X] \mid f(a) = 0\}$. Writing

$$f = f(a) + F,$$

where $F \in \ker(\phi)$, we get that $\phi(f) = \phi(f(a)) = f(a)$, since ϕ is k-linear. □

Let $X \subset \mathbb{A}^n$ be closed. Then we may write $k[X]$ as $k[\overline{x}_1, \ldots, \overline{x}_n]$, where $\overline{x} = x + I(X)$. Thus $k[X]$ is a finitely generated k-algebra. In general, we say that a ring A with identity is a k-algebra if A is a k-vector space such that $r(ab) = (ra)b = a(rb)$ for all $a, b \in A$ and $r \in k$. Put another way, multiplication defines a k-linear map

$$A \otimes_k A \to A.$$

Hence $k[X]$ is a finitely generated, commutative k-algebra without nilpotents. Conversely,

Proposition 5.4. *Suppose k is algebraically closed. Then any finitely generated commutative k-algebra A without nilpotents is $k[X]$ for some variety X.*

Proof.Let $A = k[z_1, \ldots, z_m]$ be such a k-algebra. Let $k[x_1, \ldots, x_m]$ be a polynomial ring. Then there exists a ring homomorphism $\phi : k[x_1, \ldots, x_m] \to A$ by $a \mapsto a \in k$, and $x_i \mapsto z_i$. This is due to the fact that $k[x_1, \ldots, x_m]$ is a polynomial ring, so there are no relations between $x_1, \ldots, x_n$. Clearly ϕ is surjective. Let $I = \ker \phi$. Then I is a ideal (see the next Lemma), so if $X = V(I)$, then $k[X] = k[x]/\operatorname{Rad}(I) \cong A$. □

Lemma 5.5. *An ideal I in $k[x_1, \ldots, x_m]$ is radical if and only if $k[x]/I$ has no nilpotents.*

Proof of Lemma. Let $\overline{f}^m = 0$ (i.e. $f^m \in I$). Then $\overline{f} = 0$ so $f \in I$; therefore I is radical. The proof of the converse is identical. □

Example: Let s and t be indeterminates over k. Consider $A = k[s^2t^3, s^2t, st]$. Then I claim A has no nilpotents. Indeed, $A \subset k[s, t]$. Now let u, v, w be new indeterminates and define a map $k[u, v, w] \to A$ by

$$u \to s^2t^3, \ v \to s^2t, \ w \to st.$$

This extends to a surjective homomorphism with kernel $(w^4 - uv)$. Therefore $A = k[X]$ where $X = V(w^4 - uv)$. (Outline of the proof: the dimension of

A is two, and moreover, A is a domain. Hence the closed set X guaranteed by the previous Proposition is an irreducible closed set in $\mathbb{A}^3$ of dimension 2. Clearly $(w^4 - uv) \subset I(X)$. Thus $X \subset V(w^4 - uv)$. But $w^4 - uv$ is irreducible. Since both varieties have dimension 2, they are equal. Thus $I(X) = (w^4 - uv)$.)

Now to complete this picture, we would like to know the following: "If two finitely generated k-algebras without nilpotents are isomorphic, then the closed sets defined in Proposition 5.4 are isomorphic, and conversely." In order to have this equivalence, we have to define morphisms. Morphisms are also called regular maps.

Definition 5.1. Let X, and Y be closed in $\mathbb{A}^n$, and $\mathbb{A}^m$ respectively, and let $f : Y \to X$ be a map. Then we say that f is a *regular map* from Y to X if there exists a polynomial map $F : \mathbb{A}^m \to \mathbb{A}^n$ such that $F|Y = f$.

Clearly, $k[X]$ is the set of regular maps from X to k.

Proposition 5.6. *Let $f : Y \to X$ be regular. Then f induces a homomorphism f^* of k-algebras $k[X] \to k[Y]$ by putting $f^*(g) = g \circ f$. Conversely, any k-algebra homomorphism $\varphi : k[X] \to k[Y]$ comes from a regular map $\Phi : Y \to X$.*

Example: $X = V(x^2 - y^3) \subset \mathbb{A}^2$. The map $x \mapsto (x^3, x^2)$ is regular. $k[X] = k[x, y]/(x^2 - y^3)$ so

$$\begin{aligned} f^*(\overline{x})(t) &= \overline{x}(t^3, t^2) = t^3 \\ f^*(\overline{y})(t) &= t^2 \end{aligned}$$

In particular, f^* is not surjective: $f^*(z) = x$ has no solutions. Thus f, which is a bijective map, is not an isomorphism in the following sense.

Definition 5.2. Let $f : Y \to X$ be regular. Then f is said to be an *isomorphism* if and only if there exists a regular map $g : X \to Y$ such that $f \circ g = 1_X$ and $g \circ f = 1_Y$.

Proof of Proposition. The first assertion is easy to prove. If $g \in k[x]$, then $g \circ f \in k[y]$. If $h \in I(X)$, then $h \circ f \in I(Y)$. For $h \circ f(y) = h\big(f(y)\big) = 0$, as $f(y) \in X$. Thus $f^* : k[x] \to k[y]$ induces $f^* : k[x]/I(X) \to k[y]/I(Y)$ via $\overline{g} \to \overline{f^* g}$.

Now let $\phi : k[X] \to k[Y]$ be given. Note that $\overline{x}_1, \ldots, \overline{x}_n$ generate $k[X]$. Let $f_i \in k[y]$ be such that $\overline{f}_i = \phi(\overline{x_i})$ in $k[Y]$. I claim that $\Phi : \mathbb{A}^m \to \mathbb{A}^n$ such that $\Phi(u_1, \ldots, u_m) = \big(f_1(u), \ldots, f_n(u)\big)$ has the property that $\Phi(Y) \subset X$.

Let $y \in Y$, and $G \in I(X)$. Then

$$\begin{aligned} G\big(\Phi(y)\big) &= G\big(f_1(y), \ldots, f_n(y)\big) \\ &= G\big(\overline{f}_1(y), \ldots, \overline{f}_n(y)\big) \qquad \text{(Since } y \in Y,\ f(y) = \overline{f}(y)\text{)} \\ &= G\big(\phi(\overline{x}_1)(y), \ldots, \phi(\overline{x}_n)(y)\big) \\ &= \phi\big(G(\overline{x}_1, \ldots, \overline{x}_n)\big)(y) \\ &= \phi(0)(y) = 0. \end{aligned}$$

Consequently, $\Phi(y) \in X$. □

Note that the map F is not necessarily unique, but Φ is.

Corollary 5.7. *Two Zariski closed sets $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are isomorphic if and only if there is a k-algebra isomorphism $k[X] \cong k[Y]$.*

Let us now define an *affine variety* to be an irreducible closed subset of some $\mathbb{A}^n$. We can also define a category whose objects are affine varieties and whose morphisms are regular maps. Define a k-algebra homomorphism $\phi : A \to B$ to be a ring homomorphism which takes the identity to the identity, hence is linear over k. We then have

Proposition 5.8. *The assignment $\phi \to \phi^*$ is a contravariant functor from the category of affine varieties and regular maps to the category of finitely generated k-algebras which are domains and k-algebra homomorphisms which gives an equivalence of categories.*

Exercise 5.1. Prove this proposition.

The fact that the points of an affine variety X are in a bijective correspondence with the maximal ideals in $k[X]$ also leads to an abstract formulation of the notion of an affine variety. We can say that an *abstract affine variety* consists of a pair (R, X), where R is a finitely generated k-algebra without zero divisors, and X is defined to be $X = \text{specm}(R)$, the set of maximal ideals in R. We can view R as a set of functions on X as follows: if $f \in R$ and $x \in X$, then $f(x)$ is the element of $k \cong R/x$ defined by the unique decomposition $f = f(x) + f^*$, where $f^* \in x$.

Lemma 5.9. *If $f, g \in S$ have the property that $f(y) = g(y)$ for all $y \in$ specm(S), then $f = g$.*

PROOF. Let $h = f - g$. Then $h(y) = 0$ for all $y \in \text{specm}(S)$. If we appeal to Proposition 5.4, then we can realize S as $k[Z]$ for a closed irreducible $Z \subset \mathbb{A}^m$ for some m. It follows that $h(z) = 0$ for all $z \in Z$. But this implies there exists an $H \in k[x_1, \ldots, x_m]$ such that $H = h = 0$ on Z. This means $h = 0$ in S. □

If $\phi^* : R \to S$ is a homomorphism of k-algebras, where S is another finitely generated k-algebra without zero divisors and (S, Y) is the associated abstract affine variety, then a map $\phi : Y \to X$ is defined by pulling back maximal ideals: $\phi(y) = (\phi^*)^{-1}(y)$. This map induces a k-algebra homomorphism $\Phi : R \to S$ by $\Phi(f)(y) = f((\phi^*)^{-1}(y))$. The fact that $\Phi(f)$ is well defined follows from Lemma 5.9.

Conversely, suppose we are given a map $\phi : Y = \text{specm}(S) \to X = \text{specm}(R)$. We want to define a homomorphism of k-algebras $\phi^* : R \to S$. If $f \in R$, let $\phi^*(f)(y) = f(\phi(y))$. It follows from Thus ϕ^* is well defined. It is easy to see ϕ^* is a homomorphism (check this). This argument gives us the additional fact that the intersection of all the maximal ideals in S is $\{0\}$.

Lecture 6

Some commutative algebra

The final step in the proof of the Nullstellensatz is to show that $\dim_k F < \infty$. This requires we introduce the notion of integrality.

Lemma 6.1. *Suppose K is a field and $L = K[a_1, \ldots, a_n]$ is a finitely generated K-algebra. Then if L is a field, each a_i is algebraic over K.*

That is, each a_i satisfies an algebraic equation over K. In particular there exist $r_0, \ldots, r_{m(-i)-1} \in K$ such that

$$a_i^{m(i)} + r_{m-1} a_i^{m(-i)-1} + \cdots + r_0 = 0$$

It follows that the monomials $a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n}$ where $0 \leq p_i \leq m(i)$ span L over K. Thus $\dim_K L < \infty$. If K is alg closed, it follows that $L = K$.

We can now prove the Lemma. Let $R \subset S$ be rings.

Definition 6.1. We say $s \in S$ is *integral over R* if and only if s satisfies a monic equation

$$s^m + a_{m-1} s^{m-1} + \cdots + a_0 = 0$$

where the $a_i \in R$.

Lemma 6.2. *The set of elements of S which are integral over R forms a subring of S containing R (called the* integral closure *of R in S.)*

Exercise 6.1. Prove Lemma 6.2.

The following lemma clarifies why the notion of integral independence is so important.

Lemma 6.3. *Suppose $\mathbb{F}$ is a field and every element of $\mathbb{F}$ is integral over a subring R of $\mathbb{F}$ containing 1. Then R is a field.*

Proof. Let $a \in R$. Then a has an inverse a^{-1} in $\mathbb{F}$. Since a^{-1} is integral over R, we have an expression

$$a^{-m} + r_{m-1}a^{-m+1} + \cdots + r_0 = 0.$$

Thus

$$1 + r_{m-1}a + \cdots + r_0 a^m = 0,$$

so

$$a(-r_{m-1} - \cdots - r_0 a^{m-1}) = 1$$

It follows from this that $a^{-1} \in R$. □

To prove Lemma 6.1, we induct on n starting with $n = 1$. Thus assume $K[u]$ is a field, and suppose u transcendental over K. Then $(1+u)^{-1}$ exists, say $(1+u)^{-1} = c_0 + c_1 u + \cdots + c_r u^r$. Then

$$(1+u)(c_0 + c_1 u + \cdots + c_r u^r) = 1,$$

so

$$c_0 + (c_0 + c_1)u + (c_1 + c_2)u^2 + \cdots + (c_{r-1} + c_r)u^r + c_r u^{r+1} = 1.$$

By the linear independence of the powers of u over k, $c_0 = 1$ and $c_r = 0$. Thus $c_0 = \pm c_1 = \pm c_2 = \pm \cdots = \pm c_r = 0$, which shows the result holds if $n = 1$.

Now suppose $L = K[a_1, \ldots, a_n]$ is a field and the result is true for $n-1$. Denote a_n by u. Note $K \subset K(u) \subset L$. Applying the induction hypothesis to $L = K(u)[a_1, \ldots, a_{n-1}]$, we deduce that each $a_1, \ldots, a_{n-1}$ is algebraic over $K(u)$. Thus we get expressions

$$g_{i1}(u)a_i^m + g_{i2}(u)a_i^{m-1} + \cdots + g_{im}(u) = 0$$

where $1 \leq i \leq n-1$ and all $g_{ij} \in K[u]$. Putting

$$g = \prod g_{1i},$$

it follows that each a_i is integral over the subring $K[u, g^{-1}] = \mathbb{F}$. Therefore, by Lemma 6.2, every element of $\mathbb{F}[a_1, \ldots, a_{n-1}]$ is integral over $\mathbb{F}$. Clearly $L = \mathbb{F}[a_1, \ldots, a_{n-1}]$, so Lemma 6.3 implies $\mathbb{F}$ is a field. We can suppose that

u doesn't divide g, for otherwise we can replace g by an h not divisible by u so that $K[u, h^{-1}] = \mathbb{F}$. Hence we get an equation

$$uP(u, g^{-1}) = 1$$

in $\mathbb{F}$ for some $P \in K[x, y]$. clearing the denominators gives

$$uQ(u, g) = g^M$$

for some $Q \in K[x, y]$. But this is impossible, since $g^M \notin \langle u \rangle$. Hence u cannot be transcendental, so the proof of the Lemma is finished. □

Lecture 7

Rational Functions on Affine Varieties

In this Lecture, we will assume the basic facts about localization ala Eisenbud. Let $X \subset \mathbb{A}^n$ be an affine variety.

Definition 7.1. The *rational function field* of X is defined to be the field $k(X)$ of quotients of $k[X]$. The elements of $k(X)$ are called *rational functions* on X. A rational function f on X is said to be *regular* at $a \in X$ iff $f = g/h$ where $g, h \in k[X]$ and $h(a) \neq 0$.

We can also localize the concept to an open subset of X.

Definition 7.2. Let $X \subset \mathbb{A}^n$ be as above, and let U be open in X. A function $f : U \to k$ is said to be *regular at* $p \in U$ if there exists a neighborhood V of p such that $f = g/h$ on V, where $g, h \in k[x]$ and $h \neq 0$ everywhere on V (equivalently $h(p) \neq 0$). We say f is *regular on* U if it is regular at each point of U. We will denote the set of $f : U \to k$ which are regular at $p \in U$ by $\mathcal{O}_{U,p}$. The set of $f : U \to k$ which are regular at every $p \in U$ will be denoted by $\mathcal{O}(U)$.

Recall that the Zariski topology has a basis consisting of the principal open sets $U_\phi = \{\phi \neq 0\} \subset \mathbb{A}^n$, where $\phi \in k[x]$. Let $k[X, 1/\phi]$ denote the localization of $k[X]$ at the multiplicative set $S = \{\phi^m \mid m \geq 0\}$. We will call $k[X, 1/\phi]$ the *localization of* $k[X]$ at ϕ.

To obtain the basic result about regular functions, we need a simple extension of the Nullstellensatz which goes as follows.

Proposition 7.1. *Let X be a closed set in $\mathbb{A}^n$, and let I be an ideal in $k[X]$. Suppose $Y \subset X$ is the variety of I, i.e. $Y = \{x \in X \mid g(y) = 0 \ \forall \ y \in X\}$. Then if $f \in k[X]$ satisfies $f = 0$ on Y, there is an $m > 0$ such that $f^m \in I$.*

Proof. Let $f = g + I(X)$, where $g \in k[x]$. Clearly Y is closed in $\mathbb{A}^n$, and g vanishes on Y, so for some $m > 0$, $g^m \in \pi^{-1}(I)$, where $\pi : k[x] \to k[X]$ is the natural quotient map. This follows from the fact that $Y = V(\pi^{-1}(I))$. Therefore, $f^m = \pi(g^m) \in I$. □

Proposition 7.2. *Let X be an affine variety in $\mathbb{A}^n$ and $U = X \cap U_\phi$ ($\phi \in k[x]$). Suppose $f : U \to k$ is regular at each $p \in U$. Then $f \in k[X, 1/\bar{\phi}]$, where $\bar{\phi} = \phi + I(X)$. Hence $\mathcal{O}(U) = k[X, 1/\phi]$.*

Proof. Throughout the proof, we will denote the restriction of an element $g \in k[x]$ to $k[X]$ by $\bar{g}$, that is, $\bar{g} = g + I(X)$. By assumption, for each $a \in U$, there exists a principal open set $U_\alpha = \{h_\alpha \neq 0\}$ in X on which $f = g_\alpha/h_\alpha$. Now as

$$\bigcup_{\alpha \in A} U_\alpha \supset U,$$

where A is an appropriate index set, it follows that

$$X \cap V(\phi) \supset X \cap \bigcap_{\alpha \in A} V(h_\alpha). \tag{7.1}$$

But the Zariski topology is Noetherian, so in (7.1), we may replace A by a finite subset $B \subset A$. Hence the Nullstellensatz for X tells us that for some $m > 0$, $\bar{\phi}^m = \sum_\alpha r_\alpha \bar{h}_\alpha$ for some $r_\alpha \in k[X]$. I also claim that by continuity, $\bar{h}_\alpha f = \bar{g}_\alpha$ on U. Consequently

$$f\bar{\phi}^m = \sum_{\alpha \in B} r^\alpha \bar{h}_\alpha f = \sum_{\alpha \in B} r_\alpha \bar{g}_\alpha$$

on U. But this implies $f \in k[X, 1/\bar{\phi}]$. Conversely, every element of $k[X, 1/\phi]$ defines a function f as in the Proposition , so the proof is complete. □

By letting $\phi = 1$, we get the following corollary.

Corollary 7.3. *Let X be affine. Then the set of functions that are regular at every point of X are the elements of $k[X]$ (which is also known as the set of regular funtions on X). Moreover, the set of globally defined rational functions is $k[X]$.*

Exercise 7.1. Prove Corollary 7.3.

We also get that $k[x_1, \dots, x_n, 1/\phi]$ is the set of regular functions on U_ϕ. In fact, let

$$X_\phi \leftrightarrow \{\, (x_1, \dots, x_{n+1}) \in \mathbb{A}^n \mid x_{n+1}\phi(x_1, \dots, x_n) - 1 = 0\}.$$

Thus $X_\phi = V(h$, where $h = x_{n+1}\phi - 1 \in k[x_1, \ldots, x_{n+1}]$. Now projection onto the first n coordinates gives us a regular map $\Phi : X_\phi \to \mathbb{A}^n$ with image U_ϕ.

Exercise 7.2. Describe the ring of functions that are regular on $U = k^2 \setminus 0$. Conclude that U cannot support an affine variety. (Hint: use the abstract formulation.)

Exercise 7.3. Repeat the previous Exercise for the functions regular on $k \setminus \{\text{finite number of points}\}$.

Definition 7.3. Two affine varieties X and Y that have isomorphic function fields $k(X)$ and $k(Y)$ are said to be *birational.* A *rational* variety is one whose function field is isomorphic to the function field $k(x_1, \ldots, x_n)$ of $\mathbb{A}^n$.

Exercise 7.4. The purpose of this exercise is to show that two birational affine varieties X and Y need not themselves be isomorphic. Let $X = V(x^2 - y^3) \subset \mathbb{A}^2$ and let $Y = \mathbb{A}^1$. Show that $k(X) = k(t)$, where

$$t = \frac{\overline{x}}{\overline{y}}.$$

Clearly $k(\mathbb{A}^1) = k(x)$, where x is an indeterminate. Conclude that $k(x) \cong k(t)$. On the other hand, show that the coordinate rings $k[X]$ and $k[\mathbb{A}^1]$ of X and $\mathbb{A}^1$ are not isomorphic, and hence conclude X and Y are not isomorphic.

Lecture 8

Projective Varieties

If V is a finite dimensional k-vector space, the *projective space* $\mathbb{P}(V)$ of V is defined to be the set of lines through the origin in in V. When $V = \mathbb{A}^{n+1}$, we will denote $\mathbb{P}(V)$ by $\mathbb{P}^n$. Let k^* be the multiplicative group of non zero elements of k. Then $\mathbb{P}^n$ may also be viewed as the set of orbits of the natural action of k^* on $(\mathbb{A}^{n+1} \setminus 0)$. (Recall, if a group G acts on a set S, the *orbit* of $s \in S$ is $Gs = \{gs \mid g \in G\}$.) Thus,

$$\mathbb{P}^n = \{\text{lines through } 0 \text{ in } \mathbb{A}^{n+1}\} = (\mathbb{A}^{n+1} \setminus 0)/k^*.$$

We will denote the k^*-orbit of $(a_0, a_1, \ldots, a_n)$ by $[a_0, a_1, \ldots, a_n]$. Thus

$$[a_0, a_1, \ldots, a_n] = [ta_0, ta_1, \ldots, ta_n]$$

for any $t \neq 0$. Note that $[a_0, a_1, \ldots, a_n]$ is undefined when all $a_i = 0$. If $v \in \mathbb{A}^{n+1} \setminus 0$, then $[v] \in \mathbb{P}^n$ denotes the line kv spanned by v. If $W \subset V$ is a subspace of dimension $k+1$, then

$$\mathbb{P}(W) = \{[w] \mid w \in W \setminus 0\} \subset \mathbb{P}(V)$$

will be called a *k-plane in* $\mathbb{P}(V)$.

Example: A line in $\mathbb{P}^n$ therefore corresponds to a 2-plane in $\mathbb{A}^{n+1}$. A hyperplane in $\mathbb{P}^n$ corresponds to an n-plane in $\mathbb{A}^{n+1}$.

It is well known that $\mathbb{P}^2$ gives an example of a projective plane geometry: two points lie on a unique line, and every pair of distinct lines in $\mathbb{P}^2$ meet in a point.

Exercise 8.1. Verify this claim, i.e. show that $\mathbb{P}^2$ satisfies the axioms of a projective plane geometry.

If V and W are subspaces of $\mathbb{A}^{n+1}$, linear algebra tells us that

$$\dim(V+W) = \dim V + \dim W - \dim(V \cap W),$$

so

$$\dim(V \cap W) \geq \dim V + \dim W - (n+1).$$

If $\dim(V+W) = n+1$ then equality holds above; however, unless $\dim V + \dim W \geq n+1$, the above inequality is vacuous. We therefore infer

Lemma 8.1. *If $V + W = \mathbb{A}^{n+1}$, then*

- $\dim \mathbb{P}(V \cap W) = \dim \mathbb{P}(V) + \dim \mathbb{P}(W) - n$
- $\operatorname{codim} \mathbb{P}(V \cap W) = \operatorname{codim} \mathbb{P}(V) + \operatorname{codim} \mathbb{P}(W)$.

In other words, codimensions add.

The Zariski topology on $\mathbb{P}^n$ is the natural topology induced from the (relative) Zariski topology on $\mathbb{A}^{n+1} \setminus 0$. Thus, the closed sets in $\mathbb{P}^n$ are the subsets X such that $\pi^{-1}(X)$ are closed in $\mathbb{A}^{n+1} \setminus 0$. By definition, a closed set in $\mathbb{A}^{n+1} \setminus 0$ has the form $Z \cap \mathbb{A}^{n+1} \setminus 0$ for some closed set in $\mathbb{A}^{n+1}$. I claim that $0 \in Z$. For if Z is closed and $Z \cap \mathbb{A}^{n+1} \setminus 0 = \pi^{-1}(X)$, then for any $v \in Z \cap \mathbb{A}^{n+1} \setminus 0$, we have $tv \in Z \cap \mathbb{A}^{n+1} \setminus 0$ for all $t \in k^*$. But then $kv \subset Z$ since kv and Z are closed. Thus $0 \in Z$.

More generally, we have the

Exercise 8.2. Let X, Y be closed in $\mathbb{A}^n$ and suppose X is irreducible. Show that if $F \in k[x]$ has the property that $F = 0$ on $X \setminus Y$, then $F = 0$ on X. Conclude that every nonempty open set in X is dense.

A subset Z of $\mathbb{A}^m$ which is closed under k is called a *cone*. If Z is a cone, we will denote $(Z \setminus 0)/k^*$ by $\mathbb{P}(Z)$. Thus the closed sets in $\mathbb{P}^n$ have the form $X = \mathbb{P}(Z)$, where Z is a closed cone in $\mathbb{A}^{n+1}$. We call Z the *cone over* X.

We will see that the Zariski toplology on $\mathbb{P}^n$ is Noetherian. Hence every closed set in $\mathbb{P}^n$ has a unique irreducible decomposition. We thus have the following

Definition 8.1. A closed irreducible subset of $\mathbb{P}^n$ is called a *projective variety.*

Let us make some further comments on the topology of $\mathbb{P}^n$. If $k = \mathbb{C}$, we can use the fact that $\mathbb{P}^n$ has a covering $U_0, U_1, \ldots, U_n$ with

$$U_i = \{[a_0, \ldots, a_n] \mid a_i \in \mathbb{C}^*\}$$

to transfer the classical topology of $\mathbb{C}^n$ to U_i via the identification

$$[a_0, \dots, a_n] \to (a_0/a_i, a_1/a_i, \dots, a_n/a_i) \in \mathbb{A}^n.$$

Note a_i/a_i does not appear on the right hand side. In fact, we may define a set $V \subset \mathbb{P}^n$ to be open if $V \cap U_i$ is open for each i.

Exercise 8.3. Show that this is a topology. Moreover, show that it coincides with the quotient topology on $\mathbb{P}^n$ induced by the quotient map $\pi : \mathbb{C}^{n+1}\backslash 0 \to \mathbb{P}^n$.

The complement of U_i is the hyperplane $a_i = 0$. Thus $\mathbb{P}^n$ is the union of $\mathbb{A}^n$ and the hyperplane $a_i = 0$. In particular, $\mathbb{P}^1$ is the union of $\mathbb{A}^1$ and a point at infinity, $\mathbb{P}^2$ is the union of $\mathbb{A}^2$ and a line at infinity and so on.

Remark: If X is Zariski closed (in $\mathbb{A}^n$ or $\mathbb{P}^n$), we define a topology on X by saying $W \subset X$ is open if and only if $W = X \cap U$, where U is open in $\mathbb{A}^n$ (or $\mathbb{P}^n$). This is the so-called relative topology on X.

Recall that a topological space X is called compact if every open cover has a finite subcover (ie. if $\{U_\alpha\}_{\alpha\in B}$ is a collection of open sets satisfying $\cup_{\alpha\in B} U_\alpha = X$, then there exists a finite finite $F \subset B$ such that $X = \bigcup_{\alpha\in F} U_\alpha$).

Proposition 8.2. *$\mathbb{P}^n$ is a compact Hausdorff space in the classical topology. In particular, $\mathbb{P}^1$ is the one point compactification of $\mathbb{C}$.*

Now we can now extend a previously stated result about affine varieties over $\mathbb{C}$.

Theorem 8.3. *Let X be an affine or projective variety over $\mathbb{C}$ and suppose X_0 is a Zariski open subset of X. This means $X_0 = X\backslash Y$ where Y is Zariski closed. Then the closures of X_0 in the classical and Zariski topologies coincide.*

Exercise 8.4. Prove Theorem 8.3.

In particular, every projective variety in $\mathbb{P}^n$ is compact in the classical topology.

Lecture 9

The homogeneous coordinate ring

There are various aspects of projective varieties we need to consider in more detail. such as what the Nullstellensatz says in the projective setting. Let us begin by considering the ideal of a closed set in $\mathbb{P}^n$. Note first that $k[x_0, x_1, \ldots, x_n]$ is a graded k-algebra. That is,

$$k[x_0, \ldots, x_n] = \bigoplus_{m \geq 0} A_m,$$

where A_m denotes the k-vector space of homogeneous polynomials of degree m, and this decomposition has the property that $A_j A_m \subset A_{j+m}$. Clearly, a polynomial $f \in k[x_0, \ldots, x_n]$ is homogeneous of degree d if $f(\lambda x) = \lambda^d f(x)$ for all $x \in \mathbb{A}^{n+1}$ and all $\lambda \in k^*$.

Suppose $Z \subset \mathbb{A}^{n+1}$ is a closed cone and let $X = \mathbb{P}(Z)$. Define the ideal of X to be $I(X) = I(Z)$.

Lemma 9.1. *If $Z \subset \mathbb{A}^{n+1}$ is a closed cone, then*

$$I(Z) = \bigoplus_{m \geq 0} \big(I(Z) \cap A_m\big).$$

In other words, if $g = \sum_i g_i$, with $g_i \in A_i$, and $g = 0$ on Z, then each $g_i = 0$ on Z. In particular, if X is projective, then $I(X)$ is homogeneous.

Proof. Let $g(x) = 0$. Then $g(\lambda x) = 0$ for all $\lambda \in k$. But

$$g(\lambda x) = \lambda^m g_m(x) + \lambda^{m-1} g_{m-1}(x) + \cdots + \lambda^0 g_0(x).$$

This polynomial is identically zero, hence all the coefficients must be zero since k an algebraically closed field is infinite. □

The following proposition characterizes the closed cones in $\mathbb{A}^2$.

Proposition 9.2. *Let $f(x,y)$ be homogeneous of degree d. Then f may be factored*

$$f = \prod_{1\le i\le d} (a_i x + b_i y), \qquad a_i, b_i \in k.$$

Note that this Proposition needs the assumption $k = \overline{k}$; for example, $x^2 + y^2 = (x+iy)(x-iy)$ cannot be factored over $\mathbb{R}$.

Exercise 9.1. Prove Proposition 9.2 and conclude that the only closed cones in $\mathbb{A}^2$ are finite unions of lines. Thus describes the closed subsets of $\mathbb{P}^1$.

In general, an ideal in a graded ring $R = \bigoplus_{m\ge 0} R_m$ which satisfies the condition

$$I = \bigoplus_{m\ge 0} (I \cap R_m)$$

is called *homogeneous*. If I is homogeneous, the quotient R/I is also a graded ring with

$$R/I = \bigoplus_{m} (R/I)_m,$$

with $(R/I)_m = R_m/I_m$. This is due to the fact that $R_m I_n \subset I_{m+n}$.

Definition 9.1. If X is a projective variety, we will define its *homogeneous coordinate ring* to be $S(X) = k[x]/I(X)$.

In particular, $S(X)$ is a graded ring, in fact a graded k-algebra:

$$S(X) = \bigoplus_{m\ge 0} S_m(X) = \bigoplus_{m\ge 0} A_m/I(X)_m.$$

Some of the results already proven in the affine setting extend easily to the projective situation.

Proposition 9.3. *Let $X = \mathbb{P}(Z)$ as above. Then:*

(i) $I(X) = I(Z)$ is generated by finitely many homogeneous polynomials.

(ii) The Zariski topology on $\mathbb{P}^n$ is Noetherian.

(iii) X is irreducible iff $I(X)$ is prime.

Exercise 9.2. Prove this Proposition.

Let us now establish the projective version of the Nullstellensatz. Suppose $I \subset k[x_0, x_1, \dots, x_n]$ is a homogenous ideal.

Theorem 9.4 (Projective Weak Nullstellensatz). *Suppose $\mathbb{P}\big(V(I)\big) = \varnothing$. Then $I \supset \mathfrak{m}_0^r$ for some $r > 0$.*

Proof. Since I is homogeneous, $I \neq k[x_0, x_1, \dots, x_n]$. Thus, $V(I) = \{0\}$. Therefore, by the usual Nullstellensatz, $x_i^m \in I$ for some $m > 0$. The result now follows. □

Theorem 9.5 (Projective Nullstellensatz). *If I is a homogeneous ideal in $k[x_0, x_1, \dots, x_n]$ and $X = \mathbb{P}\big(V(I)\big)$ is a nonempty projective variety, then $I\big(X\big) = \mathrm{Rad}(I)$.*

Proof. Let $Z = V(I)$. Then $I(Z) = I(X)$. Now $I(Z) = \mathrm{Rad}(I)$ by the usual Nullstellensatz. Thus $I(X) = \mathrm{Rad}(I)$ too. □

Now let X be a projective variety. The elements of $S(X)$ are not functions on X. They are the functions on the cone C_X over X. To get functions on X, we can consider the elements of degree zero in the quotient field of $S(X)$. We will return to this later. Another option is to work locally.

Definition 9.2. Let $U \subset \mathbb{P}^n$ be open in X. A function $f : U \to k$ is said to be *regular* at $p \in U$ if and only if there is an open neighborhood V of p on which $f = g/h$, where g and h are homogeneous of the same degree and $h \neq 0$ on V.

This definition is very similar to one we gave in the affine case. The requirement that g and h are homogeneous of the same degree means that $g(\lambda x)/h(\lambda x) = g(x)/h(x)$, so $f(x)$ is independent of the homogeneous coordinates of x. Just as in the affine case, it is customary to denote the ring of functions $f : U \to k$ such that f is regular at p by $\mathcal{O}_{U,p}$. We will denote the functions that are regular at every point of U by $\mathcal{O}(U)$.

By copying the proof of the corresponding result in the affine case, we get

Proposition 9.6. *Let $s \in A_1 = k[a_0, \dots, a_n]_1$ be a homogeneous linear polynomial. Let $U = \mathbb{P}^n \setminus V(s)$. Then $O(U)$ consists of the degree 0 terms in the localization of $k[a_0, \dots, a_n]$ at the multiplicative set determined by s.*

Thus every element of $O(U)$ is of the form $f(a_0, \dots, a_n)/s^d$, where $f \in A_d$.

One of the properties of projective varieties that distinguishes them from affine varieties is given in the next

Theorem 9.7. *If X is projective, then every function $f : X \to k$ regular at every $p \in X$ is constant. That is, $\mathcal{O}(X) \cong k$.*

Proof. We will prove this in the case $X = \mathbb{P}^n$. The general case isn't much different. Let $f = r/s$ near p where r, s are homogeneous polynomials of the same degree and $s(p) \neq 0$. If there is a point $q \in \mathbb{P}^n$ with $s(q) = 0$, then we can write $f = u/v$ near q, where u and v are homogeneous polynomials of the same degree and $v(q) \neq 0$. Now any two open sets in $\mathbb{P}^n$ meet. (This is where the irreducibility is used.) Thus there exists an non empty open set where $rv = us$. Since such open sets are dense, $rv = us$ in $k[x]$. Now we can assume that r and s have no common factors. Thus s divides v. This contradicts $s(q) = 0$ and $v(q) \neq 0$. It follows that s cannot vanish on $\mathbb{P}^n$, hence $\mathbb{P}(V(s)) = \emptyset$. Hence, if s has positive degree, then a power of the maximal ideal is contained in (s). But there is no non constant function with this property, so s is constant, hence so is f. □

Let's next look at what projective varieties are like locally. Recall $\mathbb{P}^n$ has a covering by open sets $U_0, U_1, \dots U_n$, where

$$U_i = \{[z] \mid z_i \neq 0\}.$$

I claim each U_i carries the structure of an affine variety. Let us demonstrate this for U_0. Consider the map the map $\phi : U_0 \to \mathbb{A}^n$ given by

$$\phi([a_0, a_1, \dots, a_n]) = (a_1/a_0, a_2/a_0, \dots, a_n/a_0).$$

The inverse is the map $\phi^{-1} : \mathbb{A}^n \to U_0$ defined by

$$\phi^{-1}(x_1, \dots, x_n) = [1, x_1, \dots, x_n].$$

Now ϕ induces a comorphism from $k[x_1, \dots, x_n]$ to a set of functions on U_0. We have to decide what kind of functions. Let $f \in k[x]$ have degree d. Put

$$f^h(z_0, \dots, z_n) = z_0^d \, f(z_1/z_0, z_2/z_0, \dots, z_n/z_0).$$

Then

$$f^h(\lambda z_0, \dots, \lambda z_n) = \lambda^d z_0^d \, f(z_1/z_0, z_2/z_0, \dots, z_n/z_0) = \lambda^d f^h(z_0, \dots, z_n).$$

Hence f^h is homogeneous of degree d.

Definition 9.3. We say that f^h is the *standard homogenization* of $f \in k[x]$.

Now

$$\phi^*(f)([a_0, a_1, \dots, a_n]) = f\phi([a_0, a_1, \dots, a_n]) = f(a_1/a_0, a_2/a_0, \dots, a_n/a_0).$$

But

$$\begin{aligned} f(a_1/a_0, a_2/a_0, \dots, a_n/a_0) &= a_0^d \, \frac{f(a_1/a_0, a_2/a_0, \dots, a_n/a_0)}{a_0^d} \\ &= \frac{f^h(a_0, \dots, a_n)}{a_0^d}, \end{aligned}$$

This is clearly a regular function on U_0. In fact, it's clear that ϕ^* determines an isomorphism from $k[x_1, \dots, x_n]$ to $\mathcal{O}(U_0)$. Therefore U_0 carries the structure of the affine variety $\mathbb{A}^n$. That is, $U_0 = \text{Specm } \mathcal{O}(U_0)$. Any closed set Y in $\mathbb{A}^n$ maps under ϕ^{-1} to $U_o \cap X$, where X is the set of zeros of a homogeneous ideal in $k[a_0, \dots, a_n]$.

Proposition 9.8. *If X is closed in $\mathbb{P}^n$, then $\phi(X \cap U_i)$ is closed in $\mathbb{A}^n$ for each i and conversely. In particular, every closed set in $\mathbb{P}^n$ is covered by open sets, which are isomorphic to closed sets in $\mathbb{A}^n$. Finally, every projective variety X has an open cover by affine varieties..*

Proof. We showed above that $\phi(X \cap U_i)$ is closed in $\mathbb{A}^{n+1}$ iff $X \cap U_i$ is closed in U_i. Thus we only need to see that it is irreducible iff X is. But if $X \cap U_i$ is irreducible, then so is X. □

To summarize the discussion above, since $\phi^* : k[x_1, \dots, x_n] \to \mathcal{O}(U_0)$ is an isomorphism of finitely generated k-algebras, $\phi : U_0 \to \mathbb{A}^n$ is an isomorphism of affine varieties. Thus any affine variety $Y \subset \mathbb{A}^n$ has a *projective completion* $\overline{Y}$ in $\mathbb{P}^n$ obtained by embedding Y in U_0 (or any other U_i), and taking the closure. This is a standard way to construct a projective completion of a given affine variety Y.

This discussion brings us to an important class of varieties. Namely, we have the

Definition 9.4. A subset $X \subset \mathbb{P}^n$ is called a *quasi-projective variety* if $X = Y \setminus Z$, where $Y \subset \mathbb{P}^n$ is projective and Z is closed in $\mathbb{P}^n$.

In other words, a quasi-projective variety is by definition an open subset of a projective variety. Note that we are requiring quasi-projective varieties to be irreducible, although Shafarevich doesn't require this condition.

Exercise 9.3. Show that every affine variety is quasi-projective.

We can extend Proposition 9.8 to the quasi-projective case. In fact, we have

Proposition 9.9. *Let $X \subset \mathbb{P}^n$ be a quasi-projective variety and let $x \in X$. Then x has a neighborhod which is an affine variety.*

Proof. (Also see Shafarevich, p. 49.) Suppose $X \subset \mathbb{P}^n$ is quasi-projective, say $X = W \setminus Y$, where W is projective and Y is closed. Let $x \in X$ and say for example that $x \in U_0$. We need the following Lemma.

Lemma 9.10. *Let Y_1 and Y_2 be disjoint closed subsets of $\mathbb{A}^n$. Then there exists a $g \in k[x_1, \ldots, x_n]$ such that $g(Y_1) = 0$ and $g(Y_1) = 1$.*

Exercise 9.4. Prove Lemma 9.10.

Now apply Lemma 9.10 to $Y_1 = \phi(x)$ and $Y_0 = \phi(U_0 \cap Y)$. We know $Z = \mathbb{A}^n \setminus V(g)$ is affine and open in $\mathbb{A}^n$, and, by choice of g, $\phi(x) \in Z$. Therefore, $(W \cap U_0) \cap \phi^{-1}(Z)$ is a open neighborhood of x isomorphic to a closed subset of $\mathbb{A}^n$. Now choose an irreducible component containing x and we are through. □

Lecture 10

Rational and regular functions and maps

We now take up the question of what are rational and regular functions on quasi-projective varieties and what are rational and regular maps between quasi-projective varieties. We have already defined these concepts in the affine case, and in fact we saw that a regular function on an affine variety X is the same thing as an element of the coordinate ring $k[X]$. Moreover, we defined the notion of a regular function on a projective variety X and observed that the only (globally) regular functions are the constants.

Let us begin with the function field of a projective variety X. The homogeneous coordinate ring $S(X)$ is a graded k-algebra and also a domain. Thus a candidate for the function field, or field of rational functions on X is

$$k(X) = \{f(x)/g(x) \mid f, g \in A_m \ \exists \ m, \ g \neq 0\}.$$

Since f and g are homogeneous of the same degree, it follows that an element of f/g of $k(X)$ is a regular function on some open set $U \subset X$, namely where $g \neq 0$.

Example: Let $X = \mathbb{P}^1$. Then if f and g in $k[x_0, x_1]$ are homogeneous of the same degree d, we have

$$f(x_0, x_1)/g(x_0, x_1) = x_0^d f(1, z)/x_0^d g(1, z) = r(z)/s(z),$$

where $z = x_1/x_0$. It follows easily that $k(\mathbb{P}^1) \cong k(z)$. Similarly, $k(\mathbb{P}^n) \cong k(z_1, \dots z_n)$, the quotient field of $k[z_1, \dots, z_n]$. In particular, $k(\mathbb{P}^n) = k(\mathbb{A}^n)$.

It isn't as clear how to proceed in the case X is quasi-projective, so we will take a slightly round about approach. First of all, we make the following definition.

Definition 10.1. If Y is an open subset of a closed set $W \subset \mathbb{P}^n$, let $k[Y]$ denote the ring of all k-valued functions on Y which are regular at every point. We call $k[Y]$ the *ring of regular functions on* Y.

There are two limiting cases. If Y is affine of the form $X \setminus H$, where X is projective and H is a hyperplane, then we know $k[Y]$ is the coordinate ring of Y. On the other hand, if Y is projective, then $k[Y] \cong k$.

Remark: When Y is quasi-projective, it isn't always true that $k[Y]$ is finitely generated. This definitely distinguishes the quasi-projective and affine cases.

We now define the function field of a quasi-projective variety. Let $X \subset \mathbb{P}^n$ be quasi-projective. Let $\mathcal{O}_X$ denote the set of rational functions

$$f(a_0, \ldots, a_n)/g(a_0, \ldots, a_n),$$

where $f, g \in A_d$ for some d and $g \notin I(X) := I(\overline{X})$. Thus, $\mathcal{O}_X$ is the terms of degree 0 in the localization of $k[a_0, \ldots, a_n]$ at the prime ideal $I(X)$. Let M_X denote the ideal of all $f/g \in \mathcal{O}_X$ where $f \in I(X)$. Since any element of the complement of M_X is invertible, $\mathcal{O}_X/M_X$ is a field.

Definition 10.2. The field $k(X) = \mathcal{O}_X/M_X$ is by definition the *function field of* X.

Exercise 10.1. We now have two definitions of $k(X)$ if X is projective. Do they coincide? Also, verify that if X is quasi-projective, then $k(X) = k(\overline{X})$.

We now take up morphisms of projective varieties. The naive way to define a "morphism" $f : X \to Y$, where $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ are projective varieties is the following: f is just the restriction of some $F : \mathbb{P}^m \to \mathbb{P}^n$, where $F = (g_0, \ldots, g_n)$ and $g_i \in A_d$ for all d. The problem is what to do if the g_i have a common zero at a point of X?

Example: Let $X = \{x^2 - y^2 + z^2 = 0\}$ and $Y = \mathbb{P}^1$. Then $F : \mathbb{P}^2 \to \mathbb{P}^1$ given by $F([x, y, z]) = [x, y - z]$ is undefined at $[0, 1, 1]$. However, we define $f([0, 1, 1]) = [1, 0]$. Note that $\mathbb{P}^1 = U_0 \cup U_1$ so $f^{-1}(U_0) = X \setminus [0, 1, -1]$ and $f^{-1}(U_1) = X \setminus [0, 1, 1]$. Also $f : F^{-1}(U_0) \to U_0$ is $[x, y, z] \mapsto (y - z)/x$ and $f : f^{-1}(U_1) \to U_1$ is $[x, y, z] \mapsto x/(y - z)$. Finally, $p = [0, 1, 1] \in f^{-1}(U_0)$. Now we ask whether f regular at p. We have

$$\frac{y - z}{x} = \frac{y^2 - z^2}{x(y + z)} = \frac{x^2}{x(y + z)} = \frac{x}{y + z}.$$

So f is given on $f^{-1}(U_0)$ by $x/(y + z)$ which is regular.

This example suggests that this preliminary definition of regular maps needs to be modified.

Definition 10.3. Let X and Y be two quasi-projective varieties. A map $\phi : X \to Y$ is called *regular* if ϕ is continuous and for every open $V \subset Y$ and regular function f on V, the function $\phi^*(f) = f\phi$ is regular on $\phi^{-1}(V)$.

Proposition 10.1. *Let X be a projective variety, and suppose a map $F : X \to ¶^m$ given by an $(m+1)$-tuple of elements of A_d has no* base points, *that is the components have no common zero in X. Then F is a regular map.*

Of course, if F doesn't have any base points, then, by the weak Nullstellensatz , the ideal generated by (IX) and the components of F contains a power of the maximal ideal at 0.

Exercise 10.2. Do regular maps of projective varieties induce homomorphisms of the homogeneous coordinate rings?

Let's now look at a basic example. Consider all the monomials z^α, where $\alpha \in \mathbb{Z}_+^{n+1}$ and $\sum \alpha_i = d$. It's a basic fact that the number of such monomials is $\binom{n+d}{d}$. For a given n, the *Veronese variety of degree d* is defined to be the image of the map $\nu_d : \mathbb{P}^n \to \mathbb{P}^N$, $N = \binom{n+d}{d} - 1$, sending $[z_0, z_1, \dots, z_n] \mapsto [z^{\alpha_0}, z^{\alpha_1}, \dots, z^{\alpha_N}]$, where the α_i run through these monomials in some order. Clearly, the map v_d is regular.

Example: Let's show explicitly that the image of $v_2 : \mathbb{P}^1 \to \mathbb{P}^2$ is a projective variety. Let monomials of degreee two be given the order $(2,0)$, $(1,1)$, and $(0,2)$. Then

$$\nu_2([z_0, z_1]) = [z_0^2, z_0z_1, z_1^2].$$

Since $2(1,1) = (2,0) + (0,2)$, the image of ν_2 is contained in the curve $x_1^2 = x_0x_2$, where x_0, x_1, x_2 are the homogeneous coordinates on $\mathbb{P}^2$. Also, since $x_0 = z_0^2$ and $x_2 = z_1^2$, all possible first an d third components are hit by ν_2. Thus $\nu_2(\mathbb{P}^1) = \{x_1^2 = x_0x_1\}$. Clearly, $\nu_2(\mathbb{P}^1)$ is irreducible. In fact, it has to be, since otherwise, pulling back the irreducible components would imply that $\mathbb{P}^1$ could not be irreducible.

We will presently show that the image of a projective variety under a regular map is also a projective variety. this will be our first major result on projective varieties. Before we can show this however, we need to consider products of projective varieties. This is the next topic.

Lecture 11

Product varieties and the graph of a regular map

The construction of products in the category of affine algebraic varieties is basically straightforward, since the product of two affine spaces is also an affine space: $\mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}$. Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be Zariski closed. The problem is whether $X \times Y \subset \mathbb{A}^{m+n}$ Zariski closed? We know that if $V, W \subset \mathbb{A}^{m+n}$ are Zariski closed, then $V \cap W$ is also Zariski closed. In fact, $I(V \cap W) = \mathrm{Rad}(I(V) + I(W))$. To see $X \times Y$ is affine notice that

$$X \times Y = (X \times \mathbb{A}^n) \cap (\mathbb{A}^m \times Y).$$

But $X \times \mathbb{A}^n$ and $\mathbb{A}^m \times Y$ are clearly closed. Indeed, $X \times \mathbb{A}^n = V(\pi_1^* I(X))$ where $\pi_1 : \mathbb{A}^{m+n} \to \mathbb{A}^m$ is the first projection, with a similar expression for $\mathbb{A}^m \times Y$ in terms of the second projection π_2. (Note: we are not claiming $\pi_1^* I(X)$ is an ideal.) The

Proposition 11.1. *Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be Zariski closed. Then $X \times Y$ is Zariski closed in $\mathbb{A}^{m+n}$. Moreover,*

(1) *if $X = V(f_1, \dots, f_r)$ and $Y = V(g_1, \dots, g_s)$, then*

$$X \times Y = V(\pi_1^* f_1, \dots, \pi_1^* f_r, \pi_2^* g_1, \dots, \pi_2^* g_s),$$

and

$$I(X \times Y) = \mathrm{Rad}(I(X \times \mathbb{A}^n) + I(\mathbb{A}^m \times Y);$$

(2) *$X \times Y$ is specm$\big(A(X) \otimes_k A(Y)\big)$.*

Exercise 11.1. Give the proof.

The proof of (2) consists in showing that $A(X) \otimes_k A(Y) \cong A(X \times Y)$. By the universal property of the tensor product, there exists a map such that $f \otimes g \to f \times g \in A(X \times Y)$, where $f \times g(x, y) = f(x)g(y)$, and it can be shown that this map induces the desired isomorphism.

A slightly subtle point is the fact that the product of two irreducible closed sets is also irreducible. In other words, the product of two affiine varieties is also an affine variety. One proof of this is to shown that $A(X) \otimes_k A(Y)$ is a domain if $A(X)$ and $A(Y)$ are. Another proof is to use the result that if $F : W \to Z$ is a regular map whose fibres are equidimensional and irreducible, then W is irreducible iff Z is. The projection maps $X \times Y \to X$ and $X \times Y \to Y$ are in fact clearly regular and satisfy the hypotheses of this result.

One of the major differences between affine and projective varieties is that projection maps are not closed. (Recall that a closed map is one which sends closed sets to closed sets.) Thus the product topology on $\mathbb{A}^m \times \mathbb{A}^n$ is not the Zariski topology. This stifles any attempt to show that the product of two irreducible closed sets is irreducible from topological considerations alone. Here is an example.

Example: Let $X = Y = \mathbb{A}^1$. Then the projection of the variety $\{xy = 1\}$ in $X \times Y$ is not a closed subset of X. Hence the projection is not a closed map. However, if we adjoin the point at infinity to the second factor, then $\pi_1(X)$ is closed. The Fundamental Theorem of Elimination Theory says the the projection $\mathbb{A}^m \times \mathbb{P}^n \to \mathbb{A}^m$ is closed. We will discuss this in more detail later.

Exercise 11.2. Show that the product of two Noetherian spaces is Noetherian.

We now consider the product of closed sets X, Y in the projective setting. Suppse $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ are Zariski closed. Now $X \times Y \subset \mathbb{P}^m \times \mathbb{P}^n$,which is not a projective space. The way we proceed is to introduce the *Segre map* $\varphi : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{(m+1)(n+1)-1}$. The Segre map is given by

$$\varphi([x_0, \dots, x_m], [y_0, \dots, y_n]) = [x_i y_j].$$

It's convenient to view this point as an $(m+1) \times (n+1)$ matrix $[Z_{ij}]$ in homogeneous coordinates , where $Z_{ij} = w_i z_j$. For example,

$$\varphi([x_0, x_1], [y_0, y_1]) = \begin{pmatrix} x_0 y_0 & x_0 y_1 \\ x_1 y_0 & x_1 y_1 \end{pmatrix}.$$

Let $\varphi(\mathbb{P}^m \times \mathbb{P}^n)$ be denoted by $S(m,n)$. Then $S(m,n)$ is the variety of zeros of the 2×2 minors of $[z_{ij}]$. That is,

$$S(m,n) = V\left\{\det\begin{pmatrix} Z_{i_1j_1} & Z_{i_1j_2} \\ Z_{i_2j_1} & Z_{i_2j_2}\end{pmatrix} \mid \text{all } 0 \leq i_i \leq i_2 \leq m, 0 \leq j_1 \leq j_2 \leq n\right\}.$$

In other words, $s(\mathbb{P}^m \times \mathbb{P}^n)$ is projective.

Proposition 11.2. *The Segre map $\varphi : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{(m+1)(n+1)-1}$ is a bijection of $\mathbb{P}^m \times \mathbb{P}^n$ onto a Zariski closed set in $\mathbb{P}^{(m+1)(n+1)-1}$.*

Proof. See Sharfarevich, pp 55-56.

Exercise 11.3. Give the explicit proof the $S(1,1)$ is closed in $\mathbb{P}^3$.

Example: The image of $\varphi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ is the locus of points $[Z_{ij}]$ with $Z_{00}Z_{11} - Z_{01}Z_{10}$. $S(1,1)$ is called a *quadric surface.* Note that $\varphi(\mathbb{P}^1 \times p)$ and $\varphi(q \times \mathbb{P}^1)$ are lines in $\mathbb{P}^3$. Thus the quadric is a doubly ruled surface.

We now show that $\varphi(X \times Y)$ is Zariski closed. If $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ are closed, $X \times Y$ is the subset of $\mathbb{P}^m \times \mathbb{P}^n$ consisting of all points such that $f(x)r(x,y) + g(y)s(x,y) = 0$, where $f \in I(X)$ and $g \in I(Y)$, and g, g, r, s are all homogeneous. It follows that $X \times Y$ is the locus of zeros of polynomials of the type

$$h(x,y) = \sum_{|I|=d, |J|=e} a_{IJ}x^I y^J.$$

Such polynomials are called *bihomogeneous* of bidegree (d,e). If $d \neq e$, say $d < e$, we may replace h by the functions $y_i^k h(x,y)$, $|k| = e - d$. Thus we can suppose that all h are of bidegree (d,d). Now notice that the comorphism φ^* defines an isomorphism $k[Z_{ij}]_e \to k[x,y]_{(e,e)}$, where $k[x,y]_{(e,e)}$ denotes the bihomogeneous polynomials of bidegree (e,e). Thus we may make the following

Definition 11.1. We say that $X \times Y \subset \mathbb{P}^m \times \mathbb{P}^n$ is *Zariski closed* if it is the locus of a family of bihomogeneous polynomials. The corresponding topology on $\mathbb{P}^m \times \mathbb{P}^n$ is called the *box topology.*

We now prove

Proposition 11.3. *Let $X \subset \mathbb{P}^m$, $Y \subset \mathbb{P}^n$ be closed. Then $X \times Y$ is closed in $\mathbb{P}^m \times \mathbb{P}^n$. Moreover, $\varphi(X \times Y)$ is closed in $\mathbb{P}^{(m+1)(n+1)-1}$. Hence, φ is a closed map. Consequently, $\varphi(X \times Y)$ is projective.*

Proof. The first claim is already proven. For the second, suppose h is bihomogeneous of bidegree (e,e) and $h(x,y) = 0$. Then $h = \varphi^*(f)$ for some

$f \in k[Z_{ij}]_e$, so $f(\varphi(x, y)) = 0$, and conversely. Hence $\varphi(X \times Y)$ is closed in $\mathbb{P}^{(m+1)(n+1)-1}$. □

Therefore $X \times Y$ itself can be viewed as a projective variety.

Exercise 11.4. Prove that if $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ are quasi-projective , then $\varphi(X \times Y)$ is also quasi-projective .

Lecture 12

Regular and Rational Maps on Projective Varieties (Revised)

We now turn to some properties of regular and rational maps of varieties. An important consideration when we consider rational maps will be the graph construction. The graph of a map $F : X \to Y$ is defined to be

$$\mathcal{G}_F = \{(x, F(x)) \mid x \in X\} \subset X \times Y.$$

Note that it is possible that F is continuous, but its graph is not be closed (in the product topology on $X \times Y$).

Exercise 12.1. Show that if $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ are Zariski closed, then the graph $\mathcal{G}_F$ of a regular map $F : X \to Y$ is Zariski closed in $\mathbb{A}^m \times \mathbb{A}^n$.

Here is an exercise on the product topology.

Exercise 12.2. Show that if Y is any Hausdorff topological space, then the graph of any continuous map $F : X \to Y$ is closed. Find an example where the graph isn't closed.

Exercise 12.3. Taking the Zariski topology on $\mathbb{P}^1$, is the graph of the identity map $i : \mathbb{P}^1 \to \mathbb{P}^1$ closed in the product topology?

Proposition 12.1. *Let $X \subset \mathbb{P}^m$ be Zariski closed. Then if $F : X \to \mathbb{P}^n$ is regular, the graph $\mathcal{G}_F \subset \mathbb{P}^m \times \mathbb{P}^n$ is also Zariski closed.*

PROOF. Write $F(x) = [f_0(x), \dots, f_n(x)]$ where the f_i are some functions, and let $[y_0, \dots, y_n]$ be homogeneous coordinates on $\mathbb{P}^n$. Suppose $f_j(x) \neq 0$. By the definition of a regular map, the function $F^*(y_i/y_j)$ is regular on an open set in X so since $F^*(y_i/y_j) = y_iF/y_jF = f_i/f_j$, we may assume all the f_i are homogeneous polynomials and $F(x) = [f_0(x), \dots, f_n(x)]$ on an open set in X. Hence, every $x \in X$ has a neighbourhood $U_x \subset X$ so that

$$F(x) = [f_0(x), \dots, f_n(x)]$$

on U_x, where the f_i are homogeneous polynomials of the same degree with no common zeros on U_x. Hence, in $\pi_1^{-1}(U_x) \subset X \times Y$, we have

$$\mathcal{G}_F = \big\{ \big([x_0, \dots, x_m], [y_0, \dots, y_n]\big) \mid y_i f_j(x) = y_j f_i(x) \big\}.$$

If we therefore cover X with finitely many U_x's. we therefore obtain a finite number of bihomogeneous polynomials which cut out the graph $\mathcal{G}_F$ in $X \times Y$. This means the graph $\mathcal{G}_F$ is Zariski closed. □

The above proof also shows

Proposition 12.2. *Let $X \subset \mathbb{P}^m$ be Zariski closed, and assume $F : X \to \mathbb{P}^n$ is regular. Then for each $a \in X$, there exists an open neighborhood U_a of a on which $F(x) = [f_0(x), \dots, f_n(x)]$, where the f_i are homogeneous polynomials of the same degree with no common zeros on U_a.*

We will consider the quasi-projective case below, when we study rational maps.

As was mentioned previously, one of the basic results in beginning algebraic geometry is

Theorem 12.3. *The projection maps $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^m$ and $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$ are closed.*

This implies

Corollary 12.4. *The image of a closed set in $\mathbb{P}^m$ under a regular map to $\mathbb{P}^n$ is closed.*

We now consider rational maps. Intuitively, we think of a rational map $F : \mathbb{P}^m \dashrightarrow \mathbb{P}^n$ is being defined by a sequence of elements $(a_0, \dots, a_m)$ of the function field $k(\mathbb{P}^m)$. More generally, if X is a projective variety, then we can take a sequence in $k(X)$. By clearing away the denominators, we can therefore take an arbitrary sequence of homogeneous polynomials $(f_0, \dots, f_n)$ all of the same degree. Of course, as we've seen already, a different sequence of homogeneous polynomials $(g_0, \dots, g_n)$ can define the same map locally. Thus we have to think of a rational map $F : X \dashrightarrow \mathbb{P}^n$ as being an equivalence class of $(n+1)$-tuples. The points of X where all the $f_i = 0$ for every possible way of representing the map locally will comprise the indeterminacy locus of F. This represents the set of points where F cannot be defined. Now let us make the formal definition.

Definition 12.1. Let X be quasi-projective (in particular, irreducible). Then a *rational map* $F : X \dashrightarrow Y$ is an equivalence class of pairs (U, γ), where U is Zariski open and dense, and $\gamma : U \to Y$ is regular (under the obvious equivalence relation). If $p \in U$ for some pair (U, γ), we say F is defined at p. The complement of the U's is the *indeterminancy locus* of F.

Clearly the indeterminancy locus is always Zariski closed.

Example: Let X be quasi-projective and irreducible. Then every rational function $f/g \in k(X)$ defines a rational map $F : X \dashrightarrow \mathbb{P}^1$ by $F(x) = [f(x), g(x)]$. Since we may suppose that f and g don't have any common factors, it follows that the indeterminacy locus, that is the set of points where $f = g = 0$ has "codimension 2" in X. We will treat dimension later, but for now, we can use the definition $\dim X = \text{tr.deg.} k(X)$. In particular, if X is a curve, i.e. $\dim X = 1$, then every rational function F defines a regular map. If X is a surface ($\dim X = 2$), then F is undefined on a finite set.

Example: Let $[x, y, z]$ denote homogeneous coordinates on $\mathbb{P}^2$. Let $p = [0, 1, 1]$ and let $\mathbb{P}^1$ be the line $\{z = 0\}$. The projection $\pi_p : \mathbb{P}^2 \setminus p \to \mathbb{P}^1$ is the map sending $[x, y, z]$ to the intersection of the line through $[x, y, z]$ and p with $\mathbb{P}^1$. I claim $\pi_p([x, y, z]) = [x, y - z]$. The reason is that the two plane in $\mathbb{A}^3$ spanned by (x, y, z) and $(0, 1, 1)$ has basis $(x, y - z, 0)$ and $(0, 1, 1)$. This two plane meets $\mathbb{P}^1 = \{z = 0\}$ in $[x, y - z]$.

In general, suppose $p \in \mathbb{P}^n$ and let H be a hyperplane in $\mathbb{P}^n$ such that $p \notin H$. Then the map $\pi_{p,H} : \mathbb{P}^n \setminus p \to H$ defined by putting $\pi_{p,H}(a)$ equal to the intersection of the line through a and p with H (which by linear algebra is a unique point of H) is called the *projection onto H centred at p*. It is a projection since $\pi_{p,H}(a) = a$ if $a \in H$. Suppose $X \subset \mathbb{P}^n$ is Zariski closed and $p \notin X$. Then restricting the projection $\pi_{p,H} : X \to H$ is a regular map. Such maps give an explicit way to produce study properties of projective varieties, since $\pi_{p,H}(X)$ will be a projective subvariety of a $\mathbb{P}^{n-1}$. We will see that X and $\pi_{p,H}(X)$ have the same dimension. (This is part of the Noether Normalization Theorem.)

The case where $p \in X$ gives another situation entirely. This leads to a famous map called blowing up which we will soon define.

Example: Let's take another look at to Example 10 Let $X = V(x^2 - y^2 + z^2) \subset \mathbb{P}^2$, and $F = [x, y - z]$. Recall $F : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$ is projection from $[0, 1, 1]$. But

$$[x, y-z] = \left[1, \frac{y-z}{x}\right] = \left[1, \frac{y^2 - z^2}{x(y+z)}\right] = \left[1, \frac{x}{y+z}\right] = [y+z, x].$$

The upshot is that the indeterminancy locus of F is empty. This gives an example where $p \in X$, and $\pi_p : X \dashrightarrow \mathbb{P}^1$ is regular.

Remark: Suppose X is a projective (i.e. irrreducible) and $F : X \dashrightarrow \mathbb{P}^n$ is a rational map. Let $Z \subset X \times \mathbb{P}^n$ denote the closure of the graph of F (restricted to its regular set). Somewhat surprisingly, Z is not necessarily irreducible. In fact we will see an explicit example where this happens when we blow up a point of a nodal curve in $\mathbb{P}^2$. The point is that by definition, Z is $Y \setminus W$ for a pair of Zariski closed sets $Y, W \subset \mathbb{P}^n$.

Exercise 12.4. Show that the closure of Z is Y if Y is irreducible. In particular, $\overline{Z}$ is irreducible if and only if $Z = Y \setminus W$ (as above), where Y is projective.

Hence, let

$$Z = Z_1 \cup Z_2 \cup \cdots \cup Z_r$$

be the irreducible decomposition of Z. The first projection $\pi_1 : Z \to X$ maps each Z_i to a closed subset of X. Hence, for at least one i, $\pi_1(Z_i) = X$. Now F is regular on an open subset of X, so I claim that only one component of Z projects onto X, for two components that project to X coincide over a dense open set in X. But two irreducible varieties which meet in an open set coincide. Let Z_1 be that component. Then if $i > 1$, $Z_i \subset Y \times \mathbb{P}^n$ where Y is a closed subset of X. We will call these Z_i the *irrelevant components*. We give an example below to show the Z_i $(i > 1)$ can be non trivial. We will now call Z_1 the graph of F and denote Z_1 by $\mathcal{G}_F$.

The image of a rational map is defined to be $\pi_2(\mathcal{G}_F)$. We will see later that $\pi_2(\mathcal{G}_F)$ is a closed subset of $\mathbb{P}^n$. If $Y := \pi_2(\mathcal{G}_F)$, we will write $F : X \dashrightarrow Y$.

The composition $G \circ F$ of two rational maps $F : X \dashrightarrow Y$ and $G : Y \dashrightarrow Z$ is defined when there exists a $p \in X$ such that F is defined at p and G is defined at $F(p)$.

Definition 12.2. A projective variety $X \subset \mathbb{P}^m$ is called *rational* if there exists a rational map $F : X \dashrightarrow \mathbb{P}^n$ for some n and a rational map $G : \mathbb{P}^n \dashrightarrow X$ such that:

(1) $G \circ F$ and $F \circ G$ are both defined; and

(2) both $G \circ F$ and $F \circ G$ are the identity (wherever defined).

A rational map $F : X \dashrightarrow Y$ is said to be *birational* if there exists a rational map $G : Y \dashrightarrow X$ such that (1) and (2) are satisfied.

Proposition 12.5. *A rational map $F : X \dashrightarrow Y$ of quasi-projective varieties is birational if and only if F^* defines an isomorphism $k(Y) \cong k(X)$.*

Exercise 12.5. Show that if $F : X \to \mathbb{P}^1$ is the map π_p of Example 12, then F is a regular bijection. Is the inverse map regular? Is F birational?

One of the main problems in algebraic geometry is to determine when two varieties are birational. We will mention an important special case of this question in the next section.

Exercise 12.6. Prove that $\mathbb{P}^1 \times \mathbb{P}^1$ is a rational variety, where we think of $\mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3$ via the Segre embedding.

Proposition 12.6. *A projective variety $X \subset \mathbb{P}^n$ is rational if and only if $k(X) \cong k(x_1, \dots, x_n)$, where $x_1, \dots, x_n$ are algebraically independent over k.*

Example: Let $C = \{ZY^2 = X^3 + X^2Z\} \subset \mathbb{P}^2$. Note $p = [0, 0, 1] \in C$, $q = [1, 0, 0] \notin C$. Then $\pi_q : C \to \mathbb{P}^1_{YZ}$ is generically three-to-one, hence cannot be birational. On the other hand, $\pi_p : C \dashrightarrow \mathbb{P}^1_{XY}$ does define a birational map.

Exercise 12.7. Consider the rational map $F" X \to \mathbb{P}^1$ defined in Example12.6. Show that F induces an isomorphism $F^* : k(\mathbb{P}^1) \cong k(X)$, so that X is rational. Find a formula for F^{-1} and determine whether or not F^{-1} regular?

We saw above that if X is irreducible, a rational map $F : X \dashrightarrow Y$ gives an irreducible closed subset $\mathcal{G}_F \subset X \times Y$ such that π_1 is generically one-to-one. Conversely, given an irreducible subvariety $Z \subset X \times Y$ such that π_1 is generically one-to-one on Z, then we can show that Z arises from a rational map. How? Well, $\pi_1^* : k(X) \to k(Z)$ is an imbedding; in fact, it is an isomorphism so $[k(Z) : \pi^* k(X)] = 1$. This is like the case of affine varieties with $A(X)$ instead of $k(X)$. Thus we get $\pi_2^* : k(Y) \to k^*(Z) = k^*(X)$. Hence, using homogeneous coordinates $[y_0, \dots, y_m]$ on Y we have

$$\pi_2^*(y_i/y_j) = f_i(x_0, \dots, x_n)/f_j(x_0, \dots, x_n).$$

Thus, $y_i f_j(x) = y_j f_i(x)$. I claim that $F = [f_0, \dots, f_m]$!

We can now say that F is birational if $\mathcal{G}_F^{-1} = \{(y,x) \mid (x,y) \in \mathcal{G}_F\} \subset Y \times X$ is rational! A birational map is generically one-to-one. In the above example, F is a regular birational map. If $p = [0,0,1]$, then π_p gives a birational map $\{ZY^2 = X^3 + ZX^2\} \to \mathbb{P}^1$. However, if $q = [1,0,0]$, then $\pi_1 : X \to \mathbb{P}^1$ is generically three-to-one, and hence is not birational. But π_q is regular.

In the next lecture, we will describe a very important example of a birational map, namely the canonical blowing up map $\pi : B_p(\mathbb{P}^n) \to \mathbb{P}^n$.

Lecture 13

Blowing up $\mathbb{P}^n$ at a Point

As mentioned in the last lecture, one of the main problems in algebraic geometry is to determine when two projective varieties are birational. One of the most important cases of this problem is to determine whether every projective variety X is birational to a smooth variety. A variety is *smooth* if it has no singular points. We will take up the notion of a singularity later. This problem was solved for k of characteristic zero by Hironaka for which he won the Fields Medal in 1962. Hironaka showed that given X, there is a smooth projective variety Y and a regular birational map $F : Y \to X$ which has some other neat properties which I won't go into. He also proved this result for analytic varieties over $\mathbb{C}$. The question still remains open, however, for varieties over a field k of positive characteristic.

Hironaka's proof uses a rational map called *blowing up.* We will now study a special case of blowing up. we will describe blowing up $\mathbb{P}^n$ at a point. For simplicity, we can restrict ourselves to the case $n = 2$, which shows the essential features of the general construction. The blowing up construction doesn't seem to have any analogues outside of algebraic geometry. In topology, there is a construction called surgery, which gives a topological way of describing blowing up, but which lacks the fine aspects of the algebraic-geometric construction.

Throughout this section, we will assume $p = [0, 0, \ldots, 0, 1] \in \mathbb{P}^n$. Assuming $q \neq p$, let $l(q, p)$ be the line in $\mathbb{P}^n$ through p and q. Notice that the set of lines $\{l(p, q)\}$ is the same as $\mathbb{P}^{n-1}$, the set of lines through the origin in $\mathbb{A}^n$. In fact an explicit identification is $l(p, q) \mapsto l(p, q) \cap \mathbb{P}^{n-1}$, where we are viewing $\mathbb{P}^{n-1}$ as the locus $\{z_n = 0\}$. It is clear that if $[x_0, x_1, \ldots, x_n] \in l(p, q)$, then $l(p, q) \cap \mathbb{P}^{n-1} = [x_0, x_1, \ldots, x_{n-1}]$. Thus, our identification is induced by the projection map $\pi_p : \mathbb{P}^n \setminus p \to \mathbb{P}^{n-1}$ sending

$[x_0, x_1, \ldots, x_n] \mapsto [x_0, x_1, \ldots, x_{n-1}]$.

Definition 13.1. The blow up of $\mathbb{P}^n$ at $p = [0, 0, \ldots, 0, 1]$ is defined to be Zariski closure of the graph of $\pi_p \subset \mathbb{P}^n \times \mathbb{P}^{n-1}$. We denote the blow up of $\mathbb{P}^n$ at p by $B_p(\mathbb{P}^n)$.

More generally, if $p \in \mathbb{P}^n$ is arbitrary, define H_p to be the hyperplane $\{p \cdot x = 0\}$. Then define $B_p(\mathbb{P}^n)$ to be the closure of the graph of the projection of $\pi_p : \mathbb{P}^n \to H_p$.

There are several alternative descriptions of $B_p(\mathbb{P}^n)$:

1. $B_p(\mathbb{P}^n)$ is the closure of the graph in $\mathbb{P}^n \times \mathbb{P}^{n-1}$ of the projection map $\pi_p : \mathbb{P}^n \setminus p \to \mathbb{P}^{n-1}$ sending $[z_0, z_1, \ldots, z_n] \mapsto [z_0, z_1, \ldots, z_{n-1}]$,

2. $B_p(\mathbb{P}^n) = \big\{ \big(q, \pi_p(q)\big) \mid q \neq p \big\} \cup \big\{ \big(p, l(q,p)\big) \mid q \in \mathbb{P}^n \setminus p \big\}$,

3. $B_p(\mathbb{P}^n) = \mathbb{P}^n \setminus p \cup \{l(p,q) \mid p \neq q\}$ (sewing the lines through p into $\mathbb{P}^n$),

4. $B_p(\mathbb{P}^n)$ is the variety in $\mathbb{P}^n \times \mathbb{P}^{n-1}$ defined by the equations $z_i y_j = z_j y_i$, where $0 \leq i, j \leq n-1$

Here we use the fact that the correspondence $l(q,p) \leftrightarrow \pi_p(q)$ shows that lines in $\mathbb{P}^n$ through p are in one-to-one correspondence with points of $\mathbb{P}^{n-1}$. The map $\pi_2 : B_p(\mathbb{P}^n) \to \mathbb{P}^{n-1}$ can be thought of as sending $\big(q, l(q,p)\big)$ to $l(q,p)$. Moreover, π_1 sends $\big(q, l(q,p)\big)$ to q if $q \neq p$, and sends $l(q,p)$ to p.

Take $n = 2$ for example. One can picture $B_p(\mathbb{P}^2)$ as a spiral staircase, where the central axis is $\pi_1^{-1}(p) = \mathbb{P}^1$ and each tread is a set of the form $\{r \in \mathbb{P}^2 \mid r \in l(p,q) \exists q\}$.

Now let $X \subset \mathbb{P}^n$ be closed. If $p \notin X$, then define $B_p(X)$ to be the graph of $\pi_{p,X} = \pi_p | X$. It is clear that $B_p(X)$ is closed and irreducible if X is. Moreover, $\pi_1 : B_p(X) \to X$ is regular and the inverse map $x \mapsto \big(x, \pi_p(x)\big)$ shows that X and $B_p(X)$ are isomorphic projective varieties.

The following remark is needed.

Proposition 13.1. *The blow up $B_p(\mathbb{P}^n)$ is irreducible.*

Proof.The ideal $I = \langle z_i y_j - z_j y_i \mid 0 \leq i, j \leq n-1 \rangle$ is prime. This follows from the fact that the quotient of the algebra of bihomogeneous polynomials of equal bidegrees by I is a domain. I omit the details. □

We can also argue slightly differently. For simplicity, let $n = 2$. Let U_p be an affine an open set about p. Then $\pi_1^{-1}(U_p)$, we can view $B_p(\mathbb{P}^2)$ as being the union of two dense open sets, one isomorphic to the points of the form (a,b,t), where $at=b$ and the other to isomorphic to the points of the form (a,b,s), where $bs=a$. But both opens are therefore irreducible, so their union is irreducible. □

If $p\in X$, the situation is different. First of all, how do we define $B_p(X)$? If we put $B_p(X)=\pi_1^{-1}(X)$, this means $\pi_1^{-1}(p)\subset B_p(X)$, which we may not want.

Example: Suppose that $X=V(x^2-y^2)\subset\mathbb{P}^2_{xyz}$. Then $X=X_1\cup X_2$, where $X_1=V(x-y)$ and $X_2=V(x+y)$. Thus X is the union of two lines through p. Clearly, $\pi_1^{-1}(X)\subset B_p(\mathbb{P}^2)$ has three irreducible components, even though X has two. But suppose we define $B_p(X)$ to be the Zariski closure of $\pi_1^{-1}(X\setminus p)$ in $B_p(\mathbb{P}^2)$. Then $B_p(X)$ is the union of two disjoint lines in $\mathbb{P}^2\times\mathbb{P}^1$. Hence, $B_p(X)$ is now smooth, although no longer connected. Thus, with this provisional definition, $B_p(X)$ is nicer than X because the singular point has been removed, i.e. resolved.

Suppose $k=\mathbb{C}$. If $p,q\in X$, then $l(q,p)$ is a secant line to X at p, and $\lim_{q\to p} l(q,p)$ is thus a tangent line. More precisely, it is a point of the projectivation of the tangent space to X at p, which is the set of tangent lines to X at p. Thus, in general, the Zariski closure of $\pi_1^{-1}(X\setminus p)$ is a proper subset of $\pi_1^{-1}(X)$. Let us therefore make the following definition:

Definition 13.2. If X is a subvariety of $\mathbb{P}^2$ and $p\in X$, define $B_p(X)$ to be the unique irreducible component in Zariski closure of $\pi_1^{-1}(X\setminus p)$ in $B_p(\mathbb{P}^2)$ which projects to X.

Here is another example where when blowing up a variety makes things may get better.

Example: Consider the nodal curve $X=V(zy^2-x^3)\subset\mathbb{P}^2_{xyz}$. Near p, ie. in $X_2=U_2\cap X$, we see that X is the curve $y^2=x^3$ with a cusp at $(0,0)$. Of course, the cusp is a singular point which we would like to resolve. We will investigate what $B_p(X)$ looks like near $q=\big([0,0,1],[1,0]\big)$. (Note that $q\in B_p(X)$.) Thus we need to find some local coordinates for $B_p(\mathbb{P}^2)$ about $\big([0,0,1],[1,0]\big)$. Consider the set of points $\big([x,y,1],[x,y]\big)$, where $x\neq 0$. Then the line $[x,y]\subset\mathbb{A}^2$ is parameterized by its slope $w=y/x$. Thus suppose we choose affine coordinates to be x and w. When the equation $y^2=x^3$ is expressed in the coordinates (x,w), it becomes $w^2x^2=x^3$ since $y=wx$. The Zariski closure of the locus $w^2x^2=x^3$ is the union of the parabola $x=w^2$ and its tangent line $x=0$ at $(0,0)$, this illustrates the problem encountered in Remark 12. There is an irrelevant component in the closure of $\pi_1^{-1}(X\setminus p)$ in $B_p(\mathbb{P}^2)$. Hence the variety $B_p(X)$ looks like $w^2=x$ near $z=1$, and so we can say that we have resolved the singularity of X at p since the parabola $x = w^2$ is smooth at $(0, 0)$. The mapping $B_p(X) \to X$ sends $(x, w) \to (x, xw)$ where $x = w^2$.

If we think of the $k = \mathbb{C}$ situation again, and think of taking limits, we can illuminate somewhat why the closure of the graph of a rational map can be reducible. Suppose $p \in X$. Now $B_p(X)$ is the union of $X \setminus p$ and the set of limits of sequences (r_n, l_n), where $r_n \in X \setminus p$, $r_n \to p$ and $l_n = \ell(r_n, p)$. Then $r_n = (x_n, y_n) = (x_n, w_n x_n)$ and $l_n = [x_n, x_n w_n] = [1, w_n]$. Perhaps the point is that l_n does not explicitly involve x_n.

Lecture 14

Elimination Theory

The Fundamental Theorem of Elimination Theory is the result mentioned several times above that the projection maps $\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\pi_1} \mathbb{P}^m$ and $\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\pi_2} \mathbb{P}^n$ are closed. That is, if $Y \subset \mathbb{P}^m \times \mathbb{P}^n$ is closed, so is $\pi_i(Y)$ for $i = 1, 2$. A corollary is:

Corollary 14.1. *If X is a projective variety and $F : X \to \mathbb{P}^n$ a regular map, then $F(X)$ is projective.*

Proof.Apply the fact that the graph of F is closed in $X \times \mathbb{P}^n$ and use the fundamental theorem. □

A detailed discussion of elimination theory is given in Cox, Little and O'Shea. We will treat the matter somewhat briefly. The basic concept is the resultant of two polynomials in one variable. Let $f(z), g(z) \in k[z]$ have degrees degrees m and n respectively. We want to test whether they have a common root. The condition for this is that there exists a polynomial h of degree $\leq m + n - 1$ which f, g both divide. The polynomial h can be expressed as $h = pf = qg$, where $\deg p \leq n - 1$ and $\deg q \leq m - 1$. Hence h exists if and only if the spans of $f, zf, \ldots, z^{n-1}f$ and of $g, zg, \ldots, z^{m-1}g$ have a non-zero vector in common. This happens if and only if the $(m+n)$th order determinant

$$\det\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_m & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{m-1} & a_m & 0 & \dots & 0 \\ 0 & 0 & a_0 & \dots & a_{m-2} & a_{m-1} & a_m & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & a_0 & a_1 & \dots & a_m \\ b_0 & b_1 & b_2 & \dots & b_n & 0 & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_{n-1} & b_n & 0 & \dots & 0 \\ 0 & 0 & b_0 & \dots & b_{n-2} & b_{n-1} & b_n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & b_0 & b_1 & \dots & b_n \end{pmatrix} = 0$$

This determinant is called the *resultant* of f and g, and is denoted $R(f, g)$. Since k is algebraically closed, we have

Lemma 14.2. *Two polynomials $f(z), g(z) \in k[z]$ have a common root if and only if $R(f, g) = 0$.*

More generally, suppose f, and g are polynomials in z with coefficients in $k[x_1, \dots, x_n]$. We can still form $R(f, g) \in k[x_1, \dots, x_n]$. Then

$$R(f, g)(y_1, \dots, y_n) = 0$$

if and only if $f(y, z) = g(y, z)$ for some z.

Lemma 14.3. *If f, g are homogeneous, so is $R(f, g)$.*

Proof. This is somewhat messy so we will skip it. □

Let us apply this to projections. Let $p = [0, \dots, 0, 1] \in \mathbb{P}^n$, and let $\pi_p : \mathbb{P}^n \setminus p \to \mathbb{P}^{n-1}$ p=[0,. . . ,0,1] be the projection. Now let $X \subset \mathbb{P}^n \setminus p$ be closed. We first show

Theorem 14.4. *$\pi_p(X)$ is closed in $\mathbb{P}^{n-1}$.*

Proof. Let $I(X) \subset k[z_0, \dots, z_n] = k[z]$ be the ideal of X. For $f, g \in k[z]$, let $R(f, g) \in k[z_0, \dots, z_{n-1}]$ be the resultant with respect to z_n.

Claim. $\pi_p(X) = V\big(\{R(f, g) \mid f, g \in I(X)\}\big)$

Proof of Claim. Let $q = [a_0, \dots, a_{n-1}]$. Then $\pi_p^{-1}(q) = p \cup \{ [a_0, \dots, a_{n-1}, s] \mid s \in k$. Now $q \in \pi(X)$ if and only if $s \in k$ such that $[a_0, \dots, a_{n-1}, s] \in X$. This holds if and only if for all $f, g \in I(X)$, $f(\cdot) = g(\cdot) = 0$, which holds if and only if $R(f, g)(q) = 0$ for all $f, g \in I(X)$. The result of the theorem follows. □

What does elimination theory have to do with

$$\pi_2 : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$$

being a closed map?

It suffices (by an argument which will be omitted) to assume $m = 1$. Let $S \subset \mathbb{P}^1 \times \mathbb{P}^n$ be closed, say $S = V(f_1, \ldots, f_r)$, where $f_i \in k[z_0, z_1, x_0, \ldots, x_n]$ are homogeneous. Introduce new indeterminants $s_1, \ldots, s_r$ and $t_1, \ldots, t_r$, and consider the resultant

$$R\big(\sum s_i f_i(z, 1, x_0, \ldots, x_n), \sum t_i f_i(z, 1, x_0, \ldots, x_n)\big)$$

with respect to z. Rewrite this equation as $\sum R_{\alpha,\beta}(X) t^\alpha s^\beta$. Then the claim is that $\pi_2(S) = V(R_{\alpha,\beta})$. □

Lecture 15

The Noether Normalization Lemma

We now consider projections as a way of studying projective varieties. Let's begin with an example. Let $X = \{xy = z^2\} \subset \mathbb{P}^2$. The projection $\pi_p : \mathbb{P}^2 \to \mathbb{P}^1$ from $p = [0,0,1]$ sending $[x,y,z] \mapsto [x,y]$ is 2 to 1 at almost all points of X; the points $[-x,-y,z]$ and $[x,y,z]$ project to $[x,y]$. However, $\pi_p^{-1}[1,0]$ and $\pi_p^{-1}[0,1]$ contain only one point, so $[1,0]$ and $[0,1]$ are exceptional. They are so called *double points*. Near these points, π_p behaves like $t \mapsto t^2$. Indeed, $\pi_p^{-1}[1,0] = [1,0,0]$ and near this point, X looks like $y = z^2$ and $\pi_p(z^2, z) = z^2$. This map is two to one except at $(0,0)$. We (tentatively) say that $\pi_p : X \to \mathbb{P}^1$ has *degree* 2. Note that the image $\pi_p(X) = \mathbb{P}^1$.

Proposition 15.1. *Let $X \subset \mathbb{P}^n$ be closed and assume $p \notin X$. Then all fibres of $\pi_p : X \to \mathbb{P}^{n-1}$ are finite.*

Proof.We will show that there exists a d such that every fibre has less than or equal to d elements. Suppose $X = V(f_1, \ldots, f_r)$. Let d be the maximum degree of $f_1, \ldots, f_r$. Then if $x \in X$, $f_i \mid l(p, \pi_p(x))$ has degree less than or equal to d, and hence at most d zeros. Thus $|\pi_p^{-1}(x)| \leq d$. □

A basic result, which we will soon prove, is that if X is irreducible and $\operatorname{char} k = 0$, then there exists a $d \geq 1$ such that $|\pi^{-1}(x)| = d$ for all x in a Zariski open (hence dense) subset of $\pi_p(X)$. The following two lemma will be used below.

Lemma 15.2. *Assume $Y \subset \mathbb{P}^n$ is closed, $p \notin Y$ and $\overline{Y} = \pi_p(Y)$ is irreducible. Then there exists an irreducible component W of Y such that $\pi(W) = \overline{Y}$. Moreover, if Y is irreducible, so is $\overline{Y}$.*

Exercise 15.1. Prove the Lemma.

We now want to prove the Noether Normalization Lemma. Suppose first that $X \subset \mathbb{P}^n$ is closed and irreducible, $p = [0, \dots, 0, 1] \notin X$, and $\overline{X} = \pi_p(X)$. Now π_p induces a k-algebra homomorphism $\pi_p^* : S(\overline{X}) \to S(X)$. Indeed, if $f \in k[z_0, \dots, z_{n-1}]$, then $\pi_p^* f(z_0, \dots, z_n) = f(z_0, \dots, z_{n-1})$. Clearly if f is homogeneous, so is $\pi_p^* f$ (of the same degree). We must show that $\pi_p^* I(\overline{X}) \subset I(X)$. Let $f \in I(\overline{X})$, and let $y \in X$. Then $\pi_p^* f(y) = f\big(\pi_p(y)\big) = 0$. Thus π_p^* induces a homomorphism of graded rings

$$\pi^* : S(\overline{X}) \to S(X).$$

Claim. *π_p^* is injective.*

Proof. If $\pi_p^*(\overline{f}) = 0$, then $\pi_p^* f \in I(X)$ so $\pi_p^* f(y) = 0 = f\big(\pi(y)\big)$. But $\pi_p(X) = \overline{X}$, so $f \in I(\overline{X})$. □

Thus we can assume $S(\overline{X}) \subset S(X)$.

Proposition 15.3. *Let $X \subset \mathbb{P}^n$ be closed and irreducible, and suppose $p \notin X$. Then $S(X)$ is a module of finite type over $S(\overline{X})$.*

Proof.Since $p \notin X$, there exists an element of $I(X)$ of the form

$$f = Z_n^d + a_1(Z_0, \dots, Z_{n-1}) Z_n^{d-1} + \cdots + a_d(Z_0, \dots, Z_{n-1}). \tag{15.1}$$

We may assume f is homogeneous, so Eq. (15.1) says that $1, z_n, z_n^2, \dots, z_n^{d-1}$ generate $S(X)$ as an $S(\overline{X})$ module. Thus $S(X)$ is a module of finite type over $S(\overline{X})$ with generators $1, z_n, z_n^2, \dots, z_n^{d-1}$, where $z_i = \overline{Z_i}$. □

We can dispense with the requirement that $p = [0, \dots, 0, 1]$ as follows. Let $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ be an isomorphism such that $T(p) = [0, \dots, 0, 1]$. Clearly, T induces an isomorphism $T : \mathbb{P}^n \to \mathbb{P}^n$. Thus, if $p \notin X$, we replace X by $Y = T(X)$ and p by $T(p)$ and hence deduce results about $S(X)$ from results about $S(Y)$ since $T^* : S(Y) \to S(X)$ is an isomorphism too.

The following result is called the Noether Normalization Lemma.

Theorem 15.4. *Let $X \subset \mathbb{P}^n$ be a projective variety such that $X \neq \mathbb{P}^n$. Then there is a sequence of projective varieties and regular maps*

$$X = X_0 \to X_1 \to \cdots \to X_{r-1} \to X_r \cong \mathbb{P}^{n-r}$$

such that

(1) *for all i, if $\pi_i : X_i \to X_{i+1}$ is the associated regular map, then π_i is surjective and has finite fibres,*

(2) *every $S(X_i)$ is finite over $S(X_{i+1})$.*

In particular, $S(X)$ is a module of finite type over $k[x_0, \ldots, x_{n-r}]$.

Proof. In Proposition 15.3, we were able to construct $\pi_p : X \to \mathbb{P}^{n-1}$ provided $X \neq \mathbb{P}^n$. Thus we can apply Proposition 15.3 until eventually $X_r = \mathbb{P}^{n-r}$. The rest of the Theorem is an immediate application of Proposition 15.3. □

The sequence of projections

$$X = X_0 \to X_1 \to \cdots \to X_{r-1} \to X_r \cong \mathbb{P}^{n-r}$$

in Theorem 15.4 is in fact a projection in a more general sense. Let $\sigma_0, \ldots, \sigma_j$ be linearly independent elements of the dual space $(\mathbb{A}^{n+1})^* = \mathrm{Hom}(\mathbb{A}^{n+1}, k)$, and put $W = V(\sigma_0, \ldots, \sigma_j)$. Then W is a linear subspace of $\mathbb{P}^n$ of dimension $n - j - 1$, and the projection $\pi_W : \mathbb{P}^n \setminus W \to \mathbb{P}^j$ is defined by

$$\pi_W([Z_0, \ldots, Z_n]) = ([\sigma_0(Z_0, \ldots, Z_n), \ldots, \sigma_j(Z_0, \ldots, Z_n)]).$$

Note that $\pi_p : \mathbb{P}^n \setminus p \to \mathbb{P}^{n-1}$ is defined by letting $\sigma_i = dZ_i$ if $0 \leq i \leq n-1$, so that $p = V(\sigma_0, \ldots, \sigma_{n-1})$. By examing the construction of the map $\pi = \pi_1 \pi_2 \cdots \pi_r$ in Theorem 15.4, we see that $\pi = \pi_W$, where W is spanned by $p_1, \ldots, p_r$. Hence, we

Theorem 15.5. *Given a projective variety $X \subset \mathbb{P}^n$, there exists a subspace $W \subset \mathbb{P}^n$ of dimension $n - j - 1$ such that $W \cap X = \emptyset$ and $\pi_W : X \to \mathbb{P}^j$ is a surjective regular map. Moreover, $S(X)$ is a module of finite type over $\pi_W^*(k[x_0, \ldots, x_j]) \cong k[x_0, \ldots, x_j]$.*

In the next chapter, we will show that if the field k has characteristic 0, then we may assume d has been chosen so that over a Zariski open set U in $\mathbb{P}^j$, every fibre has exactly d points.

We can use the observation that the map in Theorem 15.4 is a projection to derive an affine version of the Noether Normalization Lemma.

Theorem 15.6. *Let $Y \subset \mathbb{A}^{n+1}$ be an affine variety. Then there exists a regular surjective map $F : Y \to \mathbb{A}^m$ with finite fibres such that $k[Y]$ is a module of finite type over $F^*(k[\mathbb{A}^m]) \cong k[w_1, \ldots, w_m]$.*

Exercise 15.2. Prove Theorem 15.6.

In the next chapter, we will show that if the field k has characteristic 0, then we may assume d has been chosen so that over a Zariski open set U in $\mathbb{P}^j$, every fibre has exactly d points.

Let $\pi_p : X \to \overline{X}$ be the usual projection. We've shown that $S(\overline{X}) \subset S(X)$ via π_p^* and that $S(X)$ is a module of finite type over $S(\overline{X})$. To clarify the significance of this, let us state some algebraic results about integrality. Complete proofs can be found in Dummit and Foote (pp. 665 ff) or in Eisenbud. Let S be a commutative ring with identity 1, and let R be a subring of S such that $1 \in R$. Recall the definition

Definition 15.1. An element $s \in S$ is *integral over* R is there is a monic polynomial in $f \in R[x]$ such that $f(s) = 0$. The set of elements in S that are integral over R is called the *integral closure of* R in S. We say that R is integrally closed in S if every every element of S integral over R is in R, i.e. R is its own integral closure in S. Finally, a domain is called *integrally closed* or *normal* if R is integrally closed in its field of quotients.

Example: The integers are integrally closed in the rationals: every rational root of an integral polynomial is integral. You probably learned this in high school under the name *rational root test.*

Proposition 15.7. *Let S, R be as above and let $s \in S$. Then the following are equivalent:*

(1) *s is integral over R;*

(2) *$R[s]$ is a finitely generated R-module;*

(3) *there exists a subring $T \subset S$ containing $R[s]$ such that T is a finitely generated R-module.*

The implications (1) implies (2) implies (3) are obvious. To prove (3) implies (1), let $T \subset S$ be a subring which contains s, and suppose $t_1, \dots, t_r$ generate T over R. Since $st_i \in T$, there are $a_{ij} \in R$ such that

$$st_i = \sum_j a_{ij} t_j.$$

Now let $A = (a_{ij})$ and I_r be the $r \times r$ identity matrix. By Cramer's Rule, these equations imply that

$$\det(A - sI_r)t_i = 0$$

for each i. But as $1 \in T$ is a linear combination of the t_i, it follows that $\det(A - sI_r) = 0$ as well. Thus there exists a monic polynomial over R having s as a root.

Corollary 15.8. *Let S and R be as above. Then:*

(1) *$s, t \in S$ are integral over R, then so are $s \pm t$ and st;*

(2) *the integral closure of R in S is a subring of S;*

(3) *if S is a finitely generated R-module, then S is integral over R; and*

(4) *integrality is transitive, that is, if T is a subring of S which is integral over R and if S is integral over T, then S is integral over R.*

Let's again consider the usual setup where $\pi_p : X \to \overline{X}$ is the projection centred at p. We have seen that $S(X)$ is a finitely generated $S(\overline{X})$-module, so every element of $S(X)$ is integral over $S(\overline{X})$. It follows without much difficulty that $[k(X) : k(\overline{X})] < \infty$ (why?). More precisely, $[k(X) : k(\overline{X})] = d$. Therefore,

$$\operatorname{tr\,deg} k(X) = \operatorname{tr\,deg} k(\overline{X}), \tag{15.2}$$

which is a fact that will be useful in the next section where we define the dimension of a variety.

Lecture 16

The dimension of a variety

Let $X \subset \mathbb{P}^n$ be an arbitrary quasi-projective variety such that $\overline{X}$ is irreducible. We now make an important definition:

Definition 16.1. The dimension $\dim(X)$ of X is defined to be $\dim(X) = \operatorname{tr\,deg} k(X)$.

By definition, the transcendence degree $\operatorname{tr\,deg}_k k(X)$ of $k(X)$ over k is the largest n such that there exists a subring of $k(X)$ isomorphic to a polynomial ring $k[x_1, \ldots, x_n]$.

By the Noether Normalization Lemma, when X is projective, we can find a subspace $\mathbb{P}(W) \subset \mathbb{P}^n$ such that $X(c)ap\mathbb{P}(W)$ is empty and the projection $\pi_W : X \to \mathbb{P}^r$, $r = \operatorname{codim} W - 1$, is a surjective regular maps with finite fibres. By (15.2), it follows that $\dim X = r$. Stating this a little more generally, we have

Proposition 16.1. *The dimension of an irreducible projective variety is r if and only if there exists a surjective regular map $F : X \to \mathbb{P}^r$ so that each fibre is finite.*

Exercise 16.1. Prove Proposition 16.1. (Note that you have to first show that $k(\mathbb{P}^r) \subset k(X)$.)

Example: The dimension of $\mathbb{P}^n = n$.

Example: Let X be an irreducible curve in $\mathbb{P}^2$, that is $X = V(f)$, where $f \in k[x, y, z]$ is homogeneous and irreducible. Then for any $p \in \mathbb{P}^2 \setminus X$, $\pi_p(X)$ is a closed subset of $\mathbb{P}^1$ Since $\pi_p(X)$ is irreducible, either $\pi_p(X) = \mathbb{P}^1$ or $\pi_p(X)$ is a point q. But in this case, $X \subset \pi^{-1}(q)$. Since $p \notin X$, it follows that X is a point, which is contrary to the assumption that X is a curve. Indeed, if X is a point, then the cone in $\mathbb{A}^3$ over X is a line. But a line cannot be cut out by a single equation $f = 0$ (why?). Thus $\pi_p(X) = \mathbb{P}^1$, so $\dim X = 1$. It follows that $\dim(X) = n - 1$

Example: Now let X be a hypersurface in $\mathbb{P}^n$, say $X = V(f)$ where f is homogeneous and irreducible. The if $p \notin X$, the projection map $\pi_p : X \to \mathbb{P}^{n-1}$ is surjective. Indeed, if $q \in \mathbb{P}^{n-1}$, then the polynomial f has a zero on the line $\ell(p, q)$, hence $\pi_p(X) = \mathbb{P}^{n-1}$.

Similarly, Theorem 15.6 says that an irreducible affine variety X admits a regular surjective map onto $\mathbb{A}^m$ so that $k[X]$ is finite. Hence $\dim(X) = m$. Another way to proceed is to compute the dimension of the projective completion X of Y. In other words, $\dim Y = \operatorname{tr}\deg_k k(Y) = \operatorname{tr}\deg_k k(X)$.

There is an alternate definition of $\dim(Y)$ which was proposed when we defined Noetherian spaces. This was the

Definition 16.2. The *dimension* of an irreducible affine variety Y is the largest k such that there exists a sequence of irreducible closed subsets $Y_0, \dots, Y_k$ of Y such that

$$Y = Y_0 \supsetneq Y_1 \supsetneq \cdots \supsetneq Y_k.$$

Turning the definition into a statement about ideals using the variety ideal correspondence, we obtain

Proposition 16.2. *If Y is irreducible and affine, then* $\dim(Y)$ *is the largest k such that there exists an ascending chain of prime ideals*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_k = k[Y].$$

One can easily formulate a corresponding definition for the quasi-projective case. Both definitions give the same result, but we will skip the proof.

We begin by proving an important property of dimension.

Theorem 16.3. *If X and Y are irreducible and both are projective or affine, and if*

1. *$X \subset Y$, and*
2. $\dim(X) = \dim(Y)$,

then

$$X = Y.$$

Proof. It suffices to do the case where X and Y are both affine. Then the restriction morphism $k[Y] \to k[X]$ is surjective. Let $\dim X = r$. Then there are $u_1, \dots, u_r \in k[X]$ such that $k[u_1, \dots, u_r] \subset k[X]$ is a polynomial ring. Let $k[v_1, \dots, v_r] \subset k[Y]$ be a subring which surjects to $k[u_1, \dots, u_r]$. Then $v_1, \dots, v_r$ are algebraically independent. Hence every element $t \in k(Y)$ satisfies an equation

$$a_0(v)t^m + a_1(v)t^{m-1} + \cdots + a_{m-1}(v)t + a_m(v) = 0,$$

where can also assume that all $a_i \in k[v]$, m is minimal and $a_0 \neq 0$. If $X \neq Y$, we can choose a $t \in k[Y]$ such that $t = 0$ on X, i.e. $t = 0$ in $k[X]$. This implies $a_m(u_1, \dots, u_r) = 0$. But then $a_m = 0$ because $u_1, \dots, u_r$ are algebraically independent. As we have contradicted the minimality of m, the proof is finished. □

As an application of Theorem 16.3, we will now show that if $\mathrm{char}(k) = 0$, then a general fibre of the projection $\pi_p : X \to \mathbb{P}^{n-1}$ has d distinct elements, where d is the integer defined in (15.1). In other words, a projection is generically d to 1. The integer d is called the *degree of* the map $\pi_p : X \to \mathbb{P}^{n-1}$. We will denote this degree by $\deg(\pi_p)$.

Theorem 16.4. *Assume* $\mathrm{char}\, k = 0$*, and let* $X \subset \mathbb{P}^n$ *be closed and irreducible, and assume* $p \notin X$*. Let* $d = \deg(\pi_p)$*, where* $\pi_p : X \to \mathbb{P}^{n-1}$ *is the projection centred at* p*. Then there exists a Zariski open subset* $U \subset \overline{X} = \pi_p(X)$ *such that if* $q \in U$*, then* $|\pi_p^{-1}(q)| = d$*.*

Proof. Without loss of generality, we may suppose $p = [0, \dots, 0, 1]$, so $\pi_p([Z_0, \dots, Z_{n-1}, Z_n]) = [Z_0, \dots, Z_{n-1}]$. Let $f \in I(X)$ denote the homogeneous polynomial in (15.1). Note that by the choice of f and the fact that $\mathrm{char}(k) = 0$, the polynomial

$$\frac{\partial f}{\partial Z_n} = dZ_n^{d-1} + (d-1)a_1(Z_0, \dots, Z_{n-1})Z_n^{d-2} + \dots,$$

does not vanish on X. Thus $Y = V(\frac{\partial f}{\partial Z_n}) \cap X$ is a proper subvariety of X. Since X is irreducible, every irreducible component Y_i of Y has dimension less than $\dim(X)$. By the above discussion,

$$\dim(\overline{X}) = \dim(X) > \dim(Y_i) = \dim\big(\pi_p(Y_i)\big).$$

Since $\overline{X}$ is irreducible, each $\pi_p(Y_i)$ is a proper subvariety of $\overline{X}$. Now let U be the complement of $\pi_p(Y)$ in $\overline{X}$. Then if $q \in U$, the polynomial f restricted to $\pi_p^{-1}(q)$ only has simple roots.

Now let $C_{\overline{X}} \subset \mathbb{P}^n$ denote the cone in $\mathbb{P}^n$ over $\overline{X}$. That is,

$$C_{\overline{X}} = \bigcup_{q \in \overline{X}} \ell(p, q).$$

Then $C_{\overline{X}}$ is closed, and I claim that

$$V = C_{\overline{X}} \cap V(f)$$

is X. Suppose $V \neq X$, and let Z denote any component of V containing X. Then $\dim(Z) = \dim(\overline{X}) = \dim(X)$, so $X = Z$. Thus it suffices to show V is irreducible. So assume V is not irreducible. Suppose $S(V)$ has zero divisors a and b. Thus $ab = 0$ but neither a nor b are zero. By a previous argument, $S(V)$ is an $S(\overline{X})$ module generated by $1, Z_n, \ldots, Z_n^{d-1}$, so we may write $a = \sum \alpha_i Z_n^i$ and $b = \sum \beta_j Z_n^j$, where $0 \leq i, j \leq d-1$. The relation $ab = 0$ gives the same relation in $S(X)$ via $S(V) \xrightarrow{\iota^*} S(X)$, where $\iota : X \to V$ is the inclusion. Hence in $S(X)$, $\iota^*(ab) = 0$. But $\iota^*(ab) = \iota^*(a)\iota^*(b)$, so the fact that $S(X)$ is a domain says either $\iota^*(a) = 0$ or $\iota^*(b) = 0$, say $\iota^*(a) = 0$. Assuming $\alpha_m \neq 0$ is the highest non vanishing coefficient of a, we thus get a relation

$$Z_n^m + (\alpha_{m-1}/\alpha_m)Z_n^{m-1} + \cdots + \alpha_0/\alpha_m = 0,$$

where $m \leq d-1$. Since $k(X)$ is obtained from $k(\overline{X})$ by adjoining a single element (say for example Z_n/Z_0, it follows from this that $[k(X) : k(\overline{X})] \leq d-1$. On the other hand, by the definition of d, $k(X)$ is a vector space over $k(\overline{X})$ of dimension d(Math 422!), i.e. $[k(X); k(\overline{X})] = d$. This is a contradiction, so it follows that V is irreducible, and so $X = V$. Consequently, $|\pi_p^{-1}(q)| = |\ell(p,q) \cap X|$ for $q \in U$, and the theorem is proved. □

Since the regular maps are closed, the the composition of two or more projections

$$F = \pi_1\pi_2 \cdots \pi_r : X \to \overline{X} \subset \mathbb{P}^m$$

also has the property that over a Zariski open $U \subset \overline{X}$, every fibre has the same dimension. Thus, using the notation of Theorem 15.5, if we define

$$\deg(\pi_W) = \deg(\pi_1)\deg(\pi_2)\cdots\deg(\pi_r), \tag{16.1}$$

where $\pi_i = \pi_{p_i}$ and W is the $r-1$ plane spanned by $p_1, \ldots, p_r$, then over a Zariski open subset of $\overline{X}$, we have that every fibre of π_W has $\deg \pi_W$ points.

Exercise 16.2. Verify the claim in this sentence.

It turns out that the integer $\deg(\pi_W)$ depends only on X and not on the choice of a subspace W of dimension $n - \dim(X)$.

Definition 16.3. The *degree* of the projective variety $X \subset \mathbb{P}^n$ is this integer $\deg(\pi_W)$.

We also obtain from (16.1) and the definition of degree the formula

$$\deg(X) = \deg(\pi_p)\deg(\overline{X}). \tag{16.2}$$

For example, it isn't hard to see that the degree of a linear subspace of $\mathbb{P}^n$ is one.

Example: Let $X = \{xy^2 = z^3\}$ and $p = [0,0,1]$. Now $\pi_p^{-1}([1,0]) = [1,0,0]$. But $\pi_p^{-1}([1,u]) = [1,u,u^{2/3}]$, which consists of three points if $u \neq 0$. Thus the degree of X is 3.

The Riemann-Hurwitz Formula Let's bring in a well known formula from Riemann surface theory, which relates the local behavior of a non constant regular map between compact Riemann surfaces to global topological invariants. Here we need to suppose the field $k = \mathbb{C}$. We will restrict ourselves to Riemann surfaces which are smooth algeraic curves in $\mathbb{P}^2$. Let $X \subset \mathbb{P}^2$ be Zariski closed, irreducible, and of dimension one. Then $X = V(f)$, where $f(Z_0, Z_1, Z_2)$ is an irreducible homogeneous polynomial. If we also suppose $df_q \neq 0$ at each $q \in X$, then X is called a smooth projective algebraic curve. In analytic terms, X is a compact Riemann surface. Thus, X has a topological genus $g(X)$, that is X is topologically equivalent to a sphere with $g(X)$ handles attached. For example, $g(\mathbb{P}^1) = g(S^2) = 0$.

Example: Consider the elliptic curve

$$\overline{E} = \{[x,y,t] \mid ty^2 = ax^3 + bxt^2 + ct^3\} \subset \mathbb{P}^2,$$

where a, b, and c are chosen such that the roots of $ax^3 + bx + c = 0$ are distinct. This assumption implies $\overline{E}$ is smooth. Note $\overline{E} = E \cup [0,1,0]$, where $E = \overline{E} \cap \{t \neq 0\}$. Let $p = [1,0,0]$ and note also that $p \notin \overline{E}$. Then $\pi_p : \overline{E} \to \mathbb{P}^1_{y,t}$ is regular. Note that $\pi^{-1}[0,1] = \{[\zeta_1,0,1],[\zeta_2,0,1],[\zeta_3,0,1]\}$, a triple point, and $\pi^{-1}[1,0] = [0,1,0]$. The elliptic curve $\overline{E}$ of this example has $g(\overline{E}) = 1$: topologically it is a torus.

Let X and Y be irreducible projective algebraic curves as above, and let $\phi : X \to Y$ be a non constant regular map, eg a projection. Then it can be shown that ϕ is surjective and finite to one. Moreover, there exists a positive integer n such that $|\phi^{-1}(x)| = n$ on a dense Zariski open set in Y. In fact we just proved this for $\pi_p : X \to \mathbb{P}^1$. The integer n is called the *degree of* ϕ and denoted $\deg(\phi)$. Consequently, there are only finitely many points $p_1, \ldots, p_r \in X$ where $|\phi^{-1}(\phi(p_i))| \neq n$, and for these points, we have $|\phi^{-1}(\phi(p_i))| < n$.

Exercise 16.3. Let X and Y be irreducible projective curves, and suppose $f : X \to Y$ is a regular map.

(i) Show that if f is non-constant, then it is surjective.

(ii) Show that in fact, f is finite to one. That is, for each $y \in Y$, $f^{-1}(y)$ is finite.

(iii) Show that $[k(X); f^*(k(Y))] < \infty$.

(iv) If f is one to one, is it necessarily an isomorphism?

Exercise 16.4. Show that $\deg(\phi) = [k(X) : \phi^*\big(k(Y)\big)]$.

The *ramification index* ρ_i of ϕ at p_i is defined as follows: in a deleted neighbourhood of p_i, it turns out that ϕ is a μ_i to 1 covering for some $\mu_i > 1$. Thus put $\rho_i = \mu_i - 1$. Then the positive integer $\rho(\phi) = \sum \rho_i$ is called the *ramification index* of ϕ

The Euler characteristic of a smooth projective curve X satisfies $\chi(X) = 2-2g(X)$. The Euler characteristic of a topological space Y with only finitely many non trivial singular homology groups $H^j(Y, \mathbb{Q})$ over the rationals $\mathbb{Q}$ is defined to be

$$\chi(Y) = \sum_i (-1)^i b_i(Y),$$

where $b_j(Y) = \dim H^j(Y, \mathbb{Q})$ is the jth Betti number of Y. If Y is a compact connected Riemann surface, then $b_0(Y) = b_2(Y) = 1$ and $b_1(Y) = 2g(Y)$, hence $\chi(Y) = 2 - 2g(Y)$. In particular, this gives the formula for the Euler characteristic of a smooth projective curve.

Theorem 16.5 (Riemann-Hurwitz Formula). *Let X and Y be smooth, irreducible projective curves and $\phi : X \to Y$ a regular map of degree n. Then*

$$\chi(X) + \rho(\phi) = n\chi(Y).$$

In particular, if $Y = \mathbb{P}^1$, then

$$\rho(\phi) = 2\big(n + g(X) - 1\big)$$

In the case where $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is the identity map, we have $n = 1$, $g = 0$, and $\sum \rho_i = 0$. In fact, the Riemann-Hurwitz Formula implies that if $g(X) > 0$, there aren't any regular maps $\phi : X \to \mathbb{P}^1$ with $\phi^{-1}(x) = n > 0$ for all $x \in \mathbb{P}^1$. Indeed, then $\rho(\phi) = 0$, so the left hand side of the formula is 0. But $n > 0$, so the only way the right hand side can be zero is if $n = 1$ and $g(X) = 0$. This also follows from algebraic topology using the fact that S^2 is simply connected and such a ϕ has to be a covering map.

Exercise 16.5. Let $\overline{E}$ denote the elliptic curve of the previous example. Use the Riemann-Hurwitz formula to show $g(\overline{E}) = 1$.

Exercise 16.6. Let X and Y be smooth irreducible projective curves. Show that if $g(X) > ng(Y)$, then there are no non constant unramified regular maps $\phi : X \to Y$ of degree n.

Exercise 16.7. Let X be the Fermat curve $\{x^n + y^n + z^n = 0\}$. Use the Riemann-Hurwitz Formula to calculate $g(X)$.

Using the Riemann-Hurwitz Formula to calculate $g(X)$ is usually not necessary due to the fact that there is a simple genus formula. Namely, if X is a smooth projective curve, then

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