LECTURE 1: INTRODUCTION TO ALGEBRAIC GEOMETRY

1. What is algebraic geometry?

Algebraic geometry is the study of the geometric properties of solutions to systems of algebraic equations. This includes (among other things):

(1) How to describe or find solutions algebraically;
(2) The geometry and topology of the space of solutions;
(3) Counting the number of solutions when there are a finite number.

We will treat systems of algebraic equations as abstract geometric objects called **algebraic varieties**, or simply **varieties**. (Precise definitions of affine and projective algebraic varieties will come in later lectures.) The set of points on a variety X defined over a field K will be denoted $X(K)$.

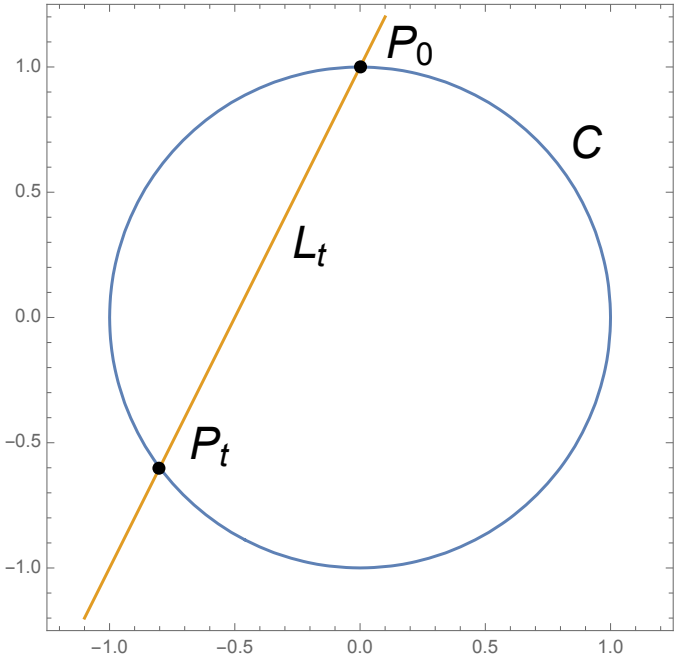
1.1. Example: the unit circle.

For a field K, let $C(K)$ be the set of points

$$C(K) = \{(x, y) \in K^2 : x^2 + y^2 = 1\}. \tag{1.1}$$

In particular, $C(\mathbb{R})$ is the unit circle in $\mathbb{R}^2$.

The unit circle C has a *rational parametrisation*—that is, a parametrisation by rational functions (ratios of polynomials). Consider the line L_t through the point $(0, 1)$ of slope t. The line L_t intersects the circle in exactly two points: $(0, 1)$ and another point P_t.



Finding P_t is a matter of solving the simultaneous equations

$$x^2 + y^2 = 1 \text{ and } y = tx + 1. \tag{1.2}$$

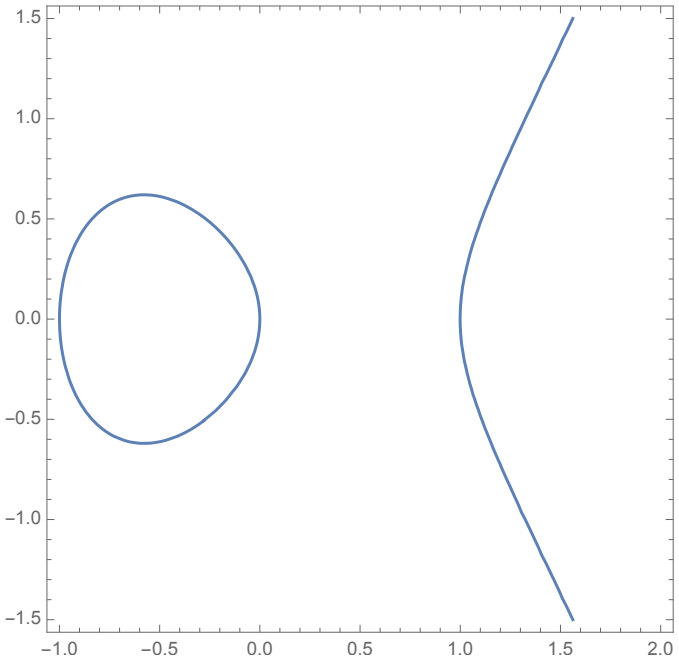
We find that $P_t = \left(\frac{-2t}{t^2+1}, \frac{-t^2+1}{t^2+1}\right)$. As t ranges over the set of real numbers, each point on the circle appears exactly once—including the original point $(0,1) = P_0$—with the exception of the point $(0,-1)$, which should correspond to the vertical line $y = 0$ of "infinite" slope.

The unit circle $C(\mathbb{R}) \subset \mathbb{R}^2$ is a *curve* in the traditional sense: a topological subspace of $\mathbb{R}^n$ that locally looks like $\mathbb{R}$. However, if we look at the *complex* points $C(\mathbb{C})$, we get a 2-dimension *surface* in $\mathbb{C}^2 \cong \mathbb{R}^4$. Indeed, in can be shown that $C(\mathbb{C})$ is topologically equivalent to a sphere with one point missing.

Nonetheless, we will refer to $C(\mathbb{C})$ as a **(complex) algebraic curve**, or an algebraic variety of dimension 1. We will justify this terminology—and define a general notion of the dimension of a variety—later in the unit.

1.2. **Example: a smooth cubic curve.** Let E be the curve defined by the equation

$$E : y^2 = x^3 - x. \tag{1.3}$$



There are some remarkable differences between E and the circle C discussed in the last section.

- Unlike the circle, E has no rational parametrisation.
- The set of complex points $E(\mathbb{C})$ forms a torus with a point missing (rather than a sphere with a point missing).

1.3. **Intersections of curves.** If two algebraic curves in $\mathbb{R}^2$ or $\mathbb{C}^2$ share no common component, then they will have finitely many points of intersection.

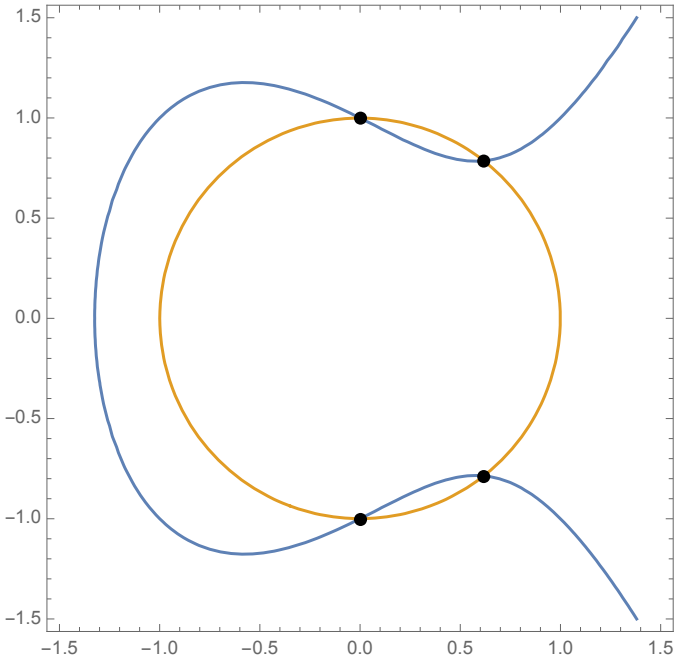
Near the end of the unit, we will prove Bézout's theorem, a result about the number of points of intersection of two complex algebraic curves. A rough, non-rigorous statement of Bézout's theorem is: Given algebraic curves C defined by an equation of degree m and D defined by an equation of degree n, with no common component, they will have mn points of intersection, provided that...

- we count complex points, not just real points;
- we count points "with multiplicity";
- we count points "at infinity".

The two curves

$$C : \{x^2 + y^2 = 1\} \text{ and } D : \{y^2 = x^3 - x + 1\} \tag{1.4}$$

have four real points of intersection, as we can see.



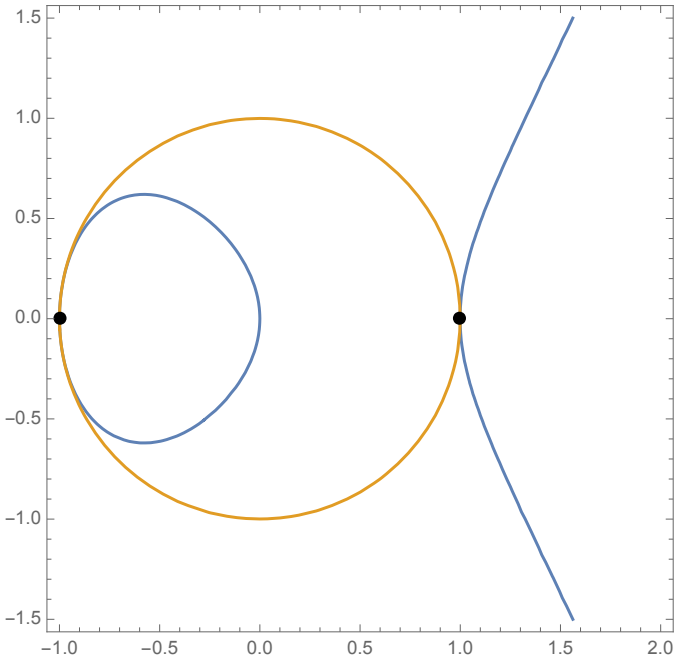
However, they actually have $6 = 2 \cdot 3$ points of intersection over $\mathbb{C}$. If $\phi = \frac{1+\sqrt{5}}{2}$, then

$$C(\mathbb{C}) \cap D(\mathbb{C}) = \{(0,1), (0,-1), (\phi^{-1}, \phi^{-1/2}), (\phi^{-1}, -\phi^{-1/2}), (-\phi, i\phi^{1/2}), (-\phi, -i\phi^{1/2})\}. \tag{1.5}$$

The two curves

$$C : \{x^2 + y^2 = 1\} \text{ and } E : \{y^2 = x^3 - x\} \tag{1.6}$$

have only 2 points of intersection, even over the complex numbers.



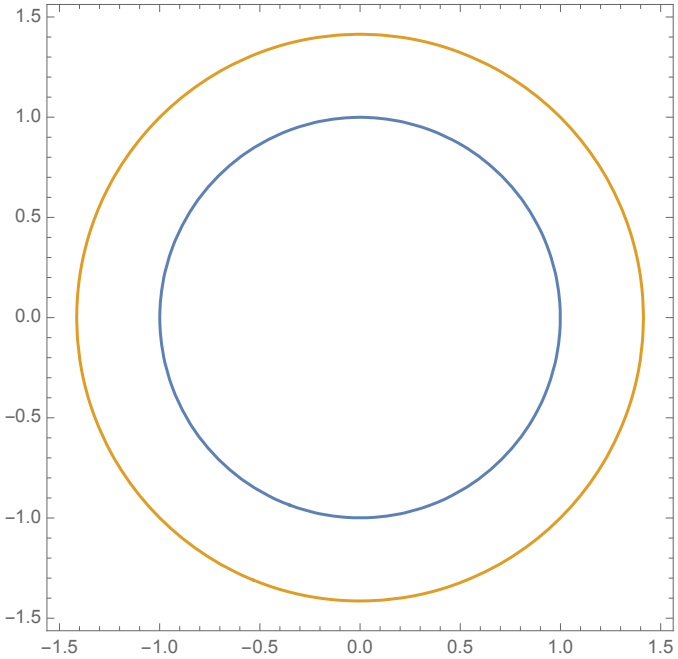
$$C(\mathbb{C}) \cap D(\mathbb{C}) = \{(1,0), (-1,0)\}. \tag{1.7}$$

However, notice how the curves are tangent at these two points. We will later define an *intersection multiplicity*, and we will be able to say that C and C intersect "with multiplicity 2" at $(1,0)$ and intersect "with multiplicity 4" at $(-1,0)$.

The two curves

$$C : \{x^2 + y^2 = 1\} \text{ and } F : \{x^2 + y^2 = 2\} \tag{1.8}$$

have no points of intersection (even over the complex numbers), because $1 \neq 2$.



However, after we develop the theory of projective geometry, we will define a precise sense in which C and F have 2 points of intersection "at infinity", each of multiplicity 2.

2. Revision of algebra topics

The mathematical foundations of algebraic geometry is *commutative algebra*. The basic objects of study in commutative algebra are *commutative rings with unity*. Unless otherwise specified, all rings R will be commutative rings with unity:

- R is a ring;
- $ab = ba$ for all $a, b \in R$;
- There is $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

In this unit, we will be dealing primarily with polynomial rings $R = \mathbb{C}[x_1, \ldots, x_n]$ and their quotients and localisations. (In all the major results we will prove, the field of complex numbers $\mathbb{C}$ could be replaced by any algebraically closed field of characteristic zero without changing the statements or proofs.)

2.1. **Ideals,** Spec**, and** mSpec**.**

Definition 2.1. *A subset $I \subseteq R$ is called an **ideal** if it satisfies the following properties:*

- *If $a, b \in I$, then $a + b \in I$.*
- *If $r \in \mathbb{R}$ and $a \in I$, then $ar \in I$.*

The ideal generated by $a_1, \ldots, a_n \in R$ will be written as

$$(a_1, \ldots, a_n) := \{a_1 r_1 + \cdots + a_n r_n : r_j \in R\}. \tag{2.1}$$

An ideal (a) with a single generator is called **principal**.

Definition 2.2. *An ideal I is **prime** if it satisfies the following properties:*

- $I \neq R$;
- *If $ab \in I$, then $a \in I$ or $b \in I$.*

*The set of all the prime ideals is called the **spectrum** of R and is denoted by $\mathrm{Spec}(R)$.*

The whole ring R is always an ideal

Definition 2.3. *An ideal I is **maximal** if it satisfies the following properties:*

- $I \neq R$;
- *If $I \leq J \leq R$, then $J = I$ or $J = R$.*

*The set of all maximal ideals of R is called the **maximal spectrum** of R and is denoted by $\mathrm{mSpec}(R)$.*

Proposition 2.4. *Every maximal ideal is prime.*

Proof. Let I be a maximal ideal of R, and suppose $ab \in I$. Then,

$$I \leq I + (a) \text{ and } I \leq I + (b), \tag{2.2}$$

so each of $I + (a)$ and $I + (b)$ are either I or R. If they are both R, then there exists $r, s \in I$ such that $r + a = s + b = 1$, so $1 = (r + a)(s + b) = rs + br + as + ab \in I$, so $R = I$, which is impossible by the definition of "maximal". Thus, at least one of $I + (a)$ and $I + (b)$ is equal to I, so $a \in I$ or $b \in I$. □

Example 2.5. *The prime ideals of $\mathbb{C}[x]$ are the*

$$\mathrm{Spec}(\mathbb{C}[x]) = \{(x - a) : a \in \mathbb{C}\} \cup \{(0)\}; \tag{2.3}$$

$$\mathrm{mSpec}(\mathbb{C}[x]) = \{(x - a) : a \in \mathbb{C}\}. \tag{2.4}$$

Example 2.6. *The prime ideals of $\mathbb{C}[x, y]$ are the*

$$\mathrm{Spec}(\mathbb{C}[x]) = \{(x - a, y - b) : a, b \in \mathbb{C}\} \cup \{(f(x, y)) : f(x, y) \textit{ is irreducible } \} \cup \{(0)\}; \tag{2.5}$$

$$\mathrm{mSpec}(\mathbb{C}[x]) = \{(x - a, y - b) : a, b \in \mathbb{C}\}. \tag{2.6}$$

2.2. **Quotient rings and localisation.** Let R be a (commutative) ring R (with unity).

Definition 2.7. *Let I be an ideal of R. The **quotient ring** R/I is defined to be the set of cosets*

$$R/I = \{r + I : r \in R\}. \tag{2.7}$$

Definition 2.8. *Let S be any subset of R. The localisation $S^{-1}R$ of R with respect to S is formally defined as a ring of "fractions" $\frac{r}{s}$, with the addition and multiplication laws*

- $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$;
- $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$;

and the equivalence relation

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \textit{ in } S^{-1}R \iff r_1 s_2 = r_2 s_1 \textit{ in } R. \tag{2.8}$$

If I is an ideal of R, then the localisation at I is defined to be

$$R_I := (R \setminus I)^{-1} R. \tag{2.9}$$

2.3. **Some ring properties.** Let R be a (commutative) ring R (with unity).

Definition 2.9. *The ring R is a **domain** (or "integral domain") if*

- $1 \neq 0$*;*
- *If $ab = 0$, then $a = 0$ or $b = 0$.*

Note that an ideal I of R is prime if and only if R/I is a domain, and I is maximal if and only if R/I is a field.

Definition 2.10. *The ring R is a **local ring** if R has a unique maximal ideal.*

If I is a prime ideal, then R_I is a local ring.

Definition 2.11. *The ring R is a **principal ideal domain (PID)** if*

- *R is a domain;*
- *Every ideal $I \leq R$ is principal, that is, $I = (a)$ for some $a \in R$.*

Definition 2.12. *The ring R is a **unique factorisation domain (UFD)** if it is a domain and every element has a unique decomposition into prime elements (i.e., elements generating prime ideals), up to ordering and multiplication by units. Precisely,*

- *R is a domain;*
- *Every nonzero $r \in R$ has a decomposition $r = p_1 \cdots p_m$ into $p_j \in R$ such that (p_j) is a prime ideal;*
- *If $p_1 \cdots p_m = q_1 \cdots q_n$ such that the (p_j) and (q_j) are nonzero prime ideals, then $m = n$, and there is a permutation $\sigma \in S_n$ such that each $q_j = u_j p_{\sigma(j)}$ for some $u_j \in R^\times$.*

Some facts about PIDs and UFDs will be used throughout the unit:

- Every PID is a UFD.
- If K is a field, then the ring $K[x]$ is a PID.
- If K is a field and $n \geq 2$, then the ring $K[x_1, \ldots, x_n]$ is a UFD but is not a PID.

LECTURE 2: BASIC TOPOLOGY

1. DEFINITIONS

Recall the definition of a metric space.

Definition 1.1. *A **metric space** is a pair (X, d), where X is a set, and $d : X \times X \to \mathbb{R}_{\geq 0}$ is a distance function. The distance function must have the following properties:*

(1) $d(x, y) = 0 \iff x = y$.
(2) $d(x, y) = d(y, x)$.
(3) *(Triangle inequality)* $d(x, z) \leq d(x, y) + d(y, z)$.

In a metric space, the **open ball** of radius r about x is the set of all points of distance less than r from x.

$$B_r(x) := \{y \in X : d(x, y) < r\}. \tag{1.1}$$

An **open set** is any union of (possibly infinitely many) open balls.

A topological space is a way to generalise the notion of a metric space by *specifying which sets are open* instead of specifying a distance function. This is a useful notion even when talking about very pedestrian spaces, such as the Euclidean plane $\mathbb{R}^2$. The two metrics

$$d_1(x, y) = |x| + |y| \text{ and } d_2(x, y) = \sqrt{x^2 + y^2} \tag{1.2}$$

on $\mathbb{R}^2$ yield the same set of open sets, and topology gives us a way to say that they are "equivalent". Even more importantly, although all metric spaces will be topological spaces, not all topological spaces will be metric spaces. And (maybe surprisingly) non-metric topologies are central to the theory of algebraic geometry.

Definition 1.2. *A **topological space** is a pair $(X, \mathcal{T})$, where X is a set and $\mathcal{T}$ is a set of subsets of X called a **topology on** X. The topology $\mathcal{T}$ must satisfy the following properties:*

(1) $\emptyset, X \in \mathcal{T}$.
(2) *(Closure under unions) If $\mathcal{S} \subseteq \mathcal{T}$, then $\bigcup_{U \in \mathcal{S}} U \in \mathcal{T}$.*
(3) *(Closure under finite intersections) If $U_1, \ldots, U_n \in \mathcal{T}$, then $\bigcap_{j=1}^{n} U_j \in \mathcal{T}$.*

Any set X has two "trivial" topologies. The **indiscrete** topology on X is the smallest possible topology, $\mathcal{T} = \{\emptyset, X\}$. The **discrete** topology is the largest possible topology, that is, the full power set $\mathcal{T} = 2^X = \{S \subseteq X\}$.

If $(X, \mathcal{T})$ is a topological space, a subset $C \subseteq X$ is called **closed** if its complement of an open set, that is, if $X \setminus C \in \mathcal{T}$. It is straightforward to see that specifying which sets are closed is equivalent to specifying which sets are open.

In practice, it is often useful to define a topology not by specifying all the open sets (nor all the closed sets), but rather by specifying a subset of the open sets that "generates" the topology. Such a subset is called a *base*.

Definition 1.3. *A **base** for a topology on a set X is a set $\mathcal{B}$ of subsets of X, with the following properties:*

(1^*) $\bigcup_{B\in\mathcal{B}} B = X$.

(2^*) *If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \cap B_2$, then there exists $B_3 \in \mathcal{B}$ such that $x \in B_3 \subseteq B_1 \cap B_2$.*

*The **topology $\mathcal{T}$ generated by** $\mathcal{B}$ is the set of all unions of sets in $\mathcal{B}$.*

$$\mathcal{T} = \left\{ \bigcup_{A\in\mathcal{A}} A : \mathcal{A} \subseteq \mathcal{B} \right\}. \tag{1.3}$$

Proposition 1.4. *Let $\mathcal{B}$ be a base for a topology on X, and let $\mathcal{T}$ be the topology generated by $\mathcal{B}$. Then $(X, \mathcal{T})$ is, in fact, a topological space.*

Proof. We prove each of the properties listed in definition 1.2 in turn.

To prove (1), note that $\emptyset \in \mathcal{T}$ because it is the union over $\mathcal{S} = \emptyset$, whereas $X \in \mathcal{T}$ by (1^*).

To prove (2), simply note that a union of unions of sets in $\mathcal{B}$ is a union of sets in $\mathcal{B}$.

To prove (3), it suffices to show that the intersection $U_1 \cap U_2$ of two open sets

$$U_1 = \bigcup_{B\in\mathcal{S}_1} B \text{ and } U_2 = \bigcup_{B\in\mathcal{S}_2} B \tag{1.4}$$

is open. For each $x \in U_1 \cap U_2$, there exists $B_{1,x} \in \mathcal{S}_1$ such that $x \in B_{1,x}$ and $B_{2,x} \in \mathcal{S}_2$ such that $x \in B_{2,x}$. By (2^*), there exists $B_{3,x} \in \mathcal{B}$ such that $x \in B_{3,x} \subseteq B_{1,x} \cap B_{2,x}$. It follows that

$$U_1 \cap U_2 = \bigcup B_{3,x} \in \mathcal{T}. \tag{1.5}$$

We've now shown that $\mathcal{T}$ is a topology on X. □

Remark 1.5. *In fact, any set $\mathcal{S}$ of subsets of X may be used to define a topology, by first enlarging it to the base*

$$\mathcal{B} = \{X\} \cup \{\textit{finite intersection of sets in } \mathcal{S}\}. \tag{1.6}$$

Proposition 1.6. *Let (X, d) be a metric space, and let $\mathcal{B}$ be the set of all open balls in X. Then, $\mathcal{B}$ is a base for a topology on X.*

Proof. We have

$$\bigcup_{x\in X} B_1(x) = X, \tag{1.7}$$

so (1^*) is satisfied. To prove (2^*), consider $x \in B_{r_1}(x_1) \cap B_{r_2}(x_2)$. Let

$$\delta = \min\{r_1 - d(x, x_1), r_2 - d(x, x_2)\} > 0. \tag{1.8}$$

If $y \in B_\delta(x)$, then

$$d(y, x_1) \leq d(y, x) + d(x, x_1) < \delta + d(x, x_1) \leq r_1, \tag{1.9}$$

and by a similar argument, $d(y, x_2) \leq r_2$. We've now prove (2^*). □

We call the topology defined in proposition 1.6 the **metric topology**.

LECTURE 2: BASIC TOPOLOGY

1. The order topology

Here we give an important example of a non-metric topology.

Definition 1.1. *A **partially ordered set**, or **poset**, is a pair $(P, \leq)$, where P is a set and $\leq$ is a binary relation on P. The binary relation must satisfy the following properties:*

(1) *(reflexivity)* $x \leq x$.
(2) *(antisymmetry) If* $x \leq y$ *and* $y \leq x$, *then* $x = y$.
(3) *(transitivity) If* $x \leq y$ *and* $y \leq z$, *then* $x \leq z$.

Exercise 1.2. *Condition (2) in definition 1.1 is actually unneccessary, because it follows from (1) and (3).*

WARNING: There are several inequivalent topologies that can be defined in a natural way from a partial order. What we will call the *order topology* is this unit is not universally called the order topology everywhere in the mathematical literature. It is also not consistent with the most common definition of the order topology of a totally ordered set.

Definition 1.3. *Let $(P, \leq)$ be a poset. The **order topology** on P is defined to be the smallest topology on P where the sets $C_x = \{y \in P : x \leq y\}$ are closed. The topology generated by the basis of open sets*

$$\mathcal{B} = \{P \setminus (C_{x_1} \cup \cdots \cup C_{x_n}) : x \in X\}. \tag{1.1}$$

Example 1.4. *If $(\mathbb{R}, \leq)$ is given the order topology, the closed sets are the intervals $[a, \infty)$ for $a \in \mathbb{R}$, and the open sets are the intervals $(-\infty, a)$. This is NOT the same as the usual Euclidean topology on $\mathbb{R}$ (which is also often called "the order topology").*

Example 1.5. *The set 2^S of subsets of a set S form a poset under inclusion. We work out this example for the set $S = \{1, 2, 3\}$.*

2. The Zariski topology

Let R be a commutative ring with unity. We put a topology on $\mathrm{Spec}(R)$ as follows. For every ideal I, let

$$V_I := \{P \in \mathrm{Spec}(R) : I \leq P\}. \tag{2.1}$$

Proposition 2.1. *The V_I are the closed sets of a topology on $\mathrm{Spec}(R)$.*

Proof. (1) We have $V_R = \emptyset$ and $V_{(0)} = \mathrm{Spec}(R)$.

(2) If $\mathcal{I}$ is any collection of ideals, then we can take $J = \sum_{I \in iI} I$ to be the ideal generated by all the the ideals in $\mathcal{I}$. Hence,

$$\bigcap_{I \in \mathcal{I}} V_I = \{P \in \mathrm{Spec}(R) : I \leq P \text{ for all } I \in \mathcal{I}\} \tag{2.2}$$

$$= V_J. \tag{2.3}$$

(3) If $\{I_1, \ldots, I_n\}$ is a finite collection of ideals, then their intersection is also an ideal $L = \bigcap_{j=1}^{n} I_j$, and

$$\bigcup_{j=1}^{n} V_{I_j} = \{P \in \mathrm{Spec}(R) : I_j \leq P \text{ for some } 1 \leq j \leq n\} \tag{2.4}$$

$$= V_L. \tag{2.5}$$

We've now proven that $\mathrm{Spec}(R)$ satisfies the "closed set"-variants of the three axioms of a topological space. □

3. Continuous functions

Definition 3.1. *Let X and Y be topological spaces, and let $\phi : X \to Y$ be a function. The function ϕ is **continuous** if the inverse image of any open set is open. In other words, if $V \subseteq Y$ is open, then*

$$\phi^{-1}(V) = \{x \in X : f(x) \in V\} \text{ is open.} \tag{3.1}$$

Note that $\phi^{-1}(Y \setminus V) = X \setminus \phi^{-1}(V)$, so the condition that ϕ is continuous is also equivalent to, "the inverse image of any closed set is closed".

Now consider a ring homomorphism $f : R \to S$, where R and S are commutative rings with unity. Then, there is an induced map

$$f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R) \tag{3.2}$$

given by $f^*(Q) = f^{-1}(Q)$. We see that $f^*(Q)$ is prime, because for any $a, b \in R$,

$$ab \in f^*(Q) \implies f(ab) \in Q \tag{3.3}$$

$$\implies f(a)f(b) \in Q \tag{3.4}$$

$$\implies f(a) \in Q \text{ or } f(b) \in Q \tag{3.5}$$

$$\implies a \in f^*(Q) \text{ or } b \in f^*(Q). \tag{3.6}$$

Moreover, it turns out that f^* is continuous.

Proposition 3.2. *The induced map $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is continuous.*

Proof. For any ideal $I \leq R$, define $f_*(I)$ to be the ideal generated by all $f(r)$ such that $r \in R$. (Note that $f(I)$ itself may not be an ideal, unlike $f^{-1}(I)$).

$$(f^*)^{-1}(V_I) = \{Q \in \mathrm{Spec}(S) : f^*(Q) \in V_I\} \tag{3.7}$$

$$= \{Q \in \mathrm{Spec}(S) : I \leq f^*(Q)\}. \tag{3.8}$$

The statement that $I \leq f^*(Q)$ is saying, "if $r \in I$, then $f(r) \in Q$". This is equivalent to saying, "the ideal generated by $f(r)$ for $r \in I$ is contained in Q", that is, $f_*(I) \leq Q$. Hence,

$$(f^*)^{-1}(V_I) = \{Q \in \mathrm{Spec}(S) : f_*(I) \leq Q\} \tag{3.9}$$

$$= V_{f_*(I)}. \tag{3.10}$$

We've shown that the inverse image of any closed set is closed; thus, f^* is continuous. □

LECTURE 5: AFFINE SPACE

1. Affine space and the ideal-variety correspondence

Fix $n \in \mathbb{N}$, and let $R = \mathbb{C}[x_1, \ldots, x_n]$. We will fix this notation for the remainder or this lecture.

Definition 1.1 (Affine space as a set)**.** *Define* ***affine*** n***-space*** $\mathbb{A}^n := \mathbb{C}^n$ *as a set. Points of* $\mathbb{A}^n$ *will be denoted as* $a = (a_1, \ldots, a_n)$.

Definition 1.2. *If* $J \leq R$*, let*

$$\mathbb{V}(J) := \{a \in \mathbb{A}^n : (\forall f \in J) f(a) = 0\}. \tag{1.1}$$

A subset of $\mathbb{A}^n$ *of the form* $\mathbb{V}(J)$ *is called an* ***affine variety****.*

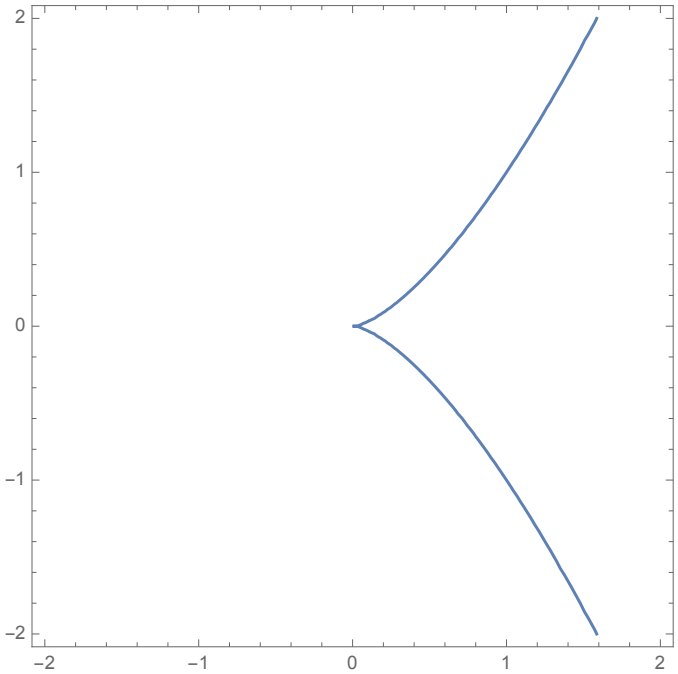
Definition 1.3. *If* $X \subseteq \mathbb{A}^n$ *is an affine variety, then define*

$$\mathbb{I}(X) := \{f \in R : (\forall a \in X) f(a) = 0\}. \tag{1.2}$$

Example 1.4. *If* $J = (x) \leq \mathbb{C}[x, y]$*, then the variety of* J *is a line,* $\mathbb{V}(J) = \{(x, y) \in \mathbb{A}^2 : x = 0\}$.

Example 1.5. *If* $J = (x, y - 1) \leq \mathbb{C}[x, y]$*, then the variety of* J *is a point,* $\mathbb{V}(J) = \{(0, 1)\}$.

Example 1.6. *If* $J = (y^2 - x^3) \leq \mathbb{C}[x, y]$*, then the variety of* J *is the* ***cuspidal cubic*** $\mathbb{V}(J) = \{(x, y) \in \mathbb{A}^2 : y^2 = x^3\}$.



The pair of maps $J \mapsto \mathbb{V}(J)$ and $X \mapsto \mathbb{I}(X)$ is known as the "ideal-variety correspondence". It follows from the definitions that both maps are order-reversing:

- If $J_1 \subseteq J_2$, then $\mathbb{V}(J_1) \supseteq \mathbb{V}(J_2)$.

- If $X_1 \subseteq X_2$, then $\mathbb{I}(X_1) \supseteq \mathbb{I}(X_2)$.

Proposition 1.7. *If X is any affine variety, then $\mathbb{V}(\mathbb{I}(X)) = X$.*

Proof. We have

$$\mathbb{V}(\mathbb{I}(X)) = \{a \in \mathbb{A}^n : (\forall f \in \mathbb{I}(X)) f(a) = 0\} \tag{1.3}$$

$$= \{a \in \mathbb{A}^n : \text{ If } f(b) = 0 \text{ for all } b \in X, \text{ then } f(a) = 0\}, \tag{1.4}$$

so if $a \in X$, then certainly $a \in \mathbb{V}(\mathbb{I}(X))$. Thus, $X \subseteq \mathbb{V}(\mathbb{I}(X))$.

Write $X = \mathbb{V}(J)$ for some ideal $J \leq R$. By a similar argument to the above, $J \subseteq \mathbb{I}(\mathbb{V}(J))$. Applying $\mathbb{V}$ to both sides of the inclusion, $\mathbb{V}(J) \supseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(J)))$; in other words, $X \supseteq \mathbb{V}(\mathbb{I}(X))$. We've proved both inclusions; therefore, $\mathbb{V}(\mathbb{I}(X)) = X$. □

2. Hilbert's Nullstellensatz

Looking at proposition 1.7, one might guess that $\mathbb{V}$ and $\mathbb{I}$ are inverse functions; that is, not only does $\mathbb{V}(\mathbb{I}(X)) = X$, but also $\mathbb{I}(\mathbb{V}(J)) = J$. This is false (in general). For example, consider the ideal $J = (x^2) \leq \mathbb{C}[x, y]$. We compute

$$\mathbb{V}(J) = \{(x, y) \in \mathbb{A}^2 : x^2 = 0\} = \{(x, y) \in \mathbb{A}^2 : x = 0\}. \tag{2.1}$$

Thus,

$$\mathbb{I}(\mathbb{V}(J)) = \{f(x, y) \in \mathbb{C}[x, y] : (\forall y) f(0, y) = 0\}. \tag{2.2}$$

Writing $f(x, y) = \sum_{j=0}^{d} \sum_{k=0}^{e} c_{jk} x^j y^k$, we see that the condition that $f \in \mathbb{I}(\mathbb{V}(J))$ is equivalent to the condition that $\sum_{k=0}^{d} c_{0k} y^k = 0$ for all $y \in \mathbb{C}$, that is, each $c_{0k} = 0$. In turn, that is equivalent to the condition that $f(x, y)$ is divisible by x. Hence $\mathbb{I}(\mathbb{V}(J)) = (x) \neq J$.

This failure may be salvaged with the following theorem.

Theorem 2.1 (Hilbert's Nullstellensatz)**.** *Let $J \leq R = \mathbb{C}[x_1, \ldots, x_n]$. Then, $\mathbb{I}(\mathbb{V}(J)) = \operatorname{rad}(J)$, where*

$$\operatorname{rad}(J) = \{f \in R : f^n \in J \text{ for some } n\}. \tag{2.3}$$

If the ideal $J = \operatorname{rad}(J)$, then J is called **radical**. If P is a prime ideal, it's not difficult to see that P is radical (exercise).

Unlike the proof of proposition 1.7, the proof of theorem 2.1 is difficult. We skip the proof for now and will return to it in Lecture 9.

Corollary 2.2. $\operatorname{mSpec}(\mathbb{C}[x_1, \ldots, x_n]) = \{(x_1 - a_1, \ldots, x_n - a_n) : (a_1, \ldots, a_n) \in \mathbb{A}^n\}$.

Proof. Let $R = \mathbb{C}[x_1, \ldots, x_n]$. First, we show that the ideals $(x_1 - a_1, \ldots, x_n - a_n)$ are indeed maximal ideals of R. Let $J = (x_1 - a_1, \ldots, x_n - a_n)$. Then,

$$\mathbb{V}(J) = \{(b_1, \ldots, b_n) \in \mathbb{A}^n : f(\tag{2.4}$$

Let $\mathfrak{m}$ be a maximal ideal of R. By the Nullstellensatz, $\mathbb{I}(\mathbb{V}(\mathfrak{m})) = \operatorname{rad}(\mathfrak{m}) = \mathfrak{m}$. First consider the case when $\mathbb{V}(\mathfrak{m}) = \emptyset$. In this case, $\mathfrak{m} = \mathbb{I}(\emptyset) = R$, which is impossible because R is not a maximal ideal (by definition). Thus, $\mathbb{V}(\mathfrak{m}) \neq \emptyset$; choose any $a = (a_1, \ldots, a_n) \in \mathbb{V}(\mathfrak{m})$. Then,

$$\mathfrak{m} = \mathbb{I}(\mathbb{V}(\mathfrak{m})) \leq \mathbb{I}(\{a\}), \tag{2.5}$$

so by maximality, $\mathfrak{m} = \mathbb{I}(\{a\})$. But $\mathbb{I}(\{a\})$ is precisely the set of polynomials that vanish at a. By expanding a polynomial $f \in R$ about the point $x = a$,

$$f(x_1, \ldots, x_n) = \sum_{j_1,\ldots,j_n} c_{j_1,\ldots,j_n}(x_1 - a_1)^{j_1} \cdots (x_n - a_n)^{j_n}, \tag{2.6}$$

we see that $f \in \mathbb{I}(\{a\})$ if and only if the constant term $c_{0,\ldots,0} = 0$, which is equivalent to saying that $f \in (x_1 - a_1, \ldots, x_n - a_n)$. Thus, $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$.

It remains to show that $\mathbb{I}(\{a\}) = (x_1 - a_1, \ldots, x_n - a_n)$ is actually a maximal ideal. If J is any ideal containing $\mathbb{I}(\{a\})$, then $\mathbb{V}(J)$ is either $\emptyset$ or $\{a\}$. If $\mathbb{V}(J) = \emptyset$, then $\mathrm{rad}(J) = R$, so $J = R$. If $\mathbb{V}(J) = \{a\}$, then $\mathrm{rad}(J) = \mathbb{I}(\{a\})$, so $J \leq \mathbb{I}(\{a\})$; but we already know $J \geq \mathbb{I}(\{a\})$, so $J = \mathbb{I}(\{a\})$. Thus, $\mathbb{I}(\{a\})$ is a maximal ideal. □

Definition 2.3 (Zariski topology on $\mathbb{A}^n$)**.** *Affine space $\mathbb{A}^n$ may be identified with $\mathrm{mSpec}(\mathbb{C}[x_1, \ldots, x_n])$ via the bijection*

$$(a_1, \ldots, a_n) \mapsto (x_1 - a_1, \ldots, x_n - a_n). \tag{2.7}$$

The Zariski topology on $\mathbb{A}^n$ is the unique topology that makes this bijection a homeomorphism; that is, a set is defined to be closed if and only if it is the image of a closed set. Specifically, the closed sets are those of the form $\mathbb{V}(J)$ for $J \leq R$, that is, affine varieties.

LECTURE 6: COORDINATE RINGS AND FUNCTION FIELDS OF AFFINE VARIETIES

1. THE COORDINATE RING

Let $X \subseteq \mathbb{A}^n$ be an affine variety.

Definition 1.1. *A function $f : X \to \mathbb{C}$ is **regular** if there's a polynomial $F \in \mathbb{C}[x_1, \ldots, x_n]$ such that $f(x) = F(x)$ for all $x \in X$. The set of regular functions form a ring, which we call the **coordinate ring** $\mathbb{C}[X]$.*

There is a surjective homomorphism π from $\mathbb{C}[x_1, \ldots, x_n]$ to $\mathbb{C}[X]$, given by restriction of a polynomial $\pi(F) = F|_X$. This allows us to give a give an algebraic description of the coordinate ring.

Proposition 1.2. $\mathbb{C}[X] \cong \mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(X)$.

Proof. For any $F \in \mathbb{C}[x_1, \ldots, x_n]$,

$$\pi(F) = 0 \iff f(a) = 0 \text{ for all } a \in X \iff f \in \mathbb{I}(X). \tag{1.1}$$

Thus, $\mathbb{C}[X] \cong \mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(X)$. □

Here are some examples of coordinate rings.

- $\mathbb{C}[A^n] = \mathbb{C}[x_1, \ldots, x_n]$.
- $\mathbb{C}[\emptyset] = \{0\}$.
- $\mathbb{C}[\{a\}] = \mathbb{C}$.
- If $Y = \{y = 0\} \subseteq \mathbb{A}^2_{x,y}$, then $\mathbb{C}[X] \cong \mathbb{C}[x]$.
- If $H = \{xy = 1\} \subseteq \mathbb{A}^2_{x,y}$, then $\mathbb{C}[H] \cong \mathbb{C}[x, x^{-1}]$.

2. IRREDUCIBLE VARIETIES

Definition 2.1. *Let $X \subseteq \mathbb{A}^n$ be a nonempty affine variety. Then, X is **reducible** if it can be written in the form $X = X_1 \cup X_2$, where X_1 and X_2 are strict subvarieties of X (that is, $X_j \subseteq X$ is a variety and $X_j \neq X$, for $j = 1, 2$). The variety X is **irreducible** if it is not reducible.*

For example, consider the variety $X = \mathbb{V}((xy)) = \{(x, y) \in \mathbb{A}^2 : xy = 0\}$. This variety is reducible because it may be written as a union of the two coordinate axes:

$$X = \{(x, y) \in \mathbb{A}^2 : x = 0\} \cup \{(x, y) \in \mathbb{A}^2 : y = 0\}. \tag{2.1}$$

On the other hand, the varieties $\{(x, y) \in \mathbb{A}^2 : x = 0\}$ and $\{(x, y) \in \mathbb{A}^2 : y = 0\}$ cannot be decomposed further—that is, they are irreducible. Any affine variety X may be decomposed uniquely as a union of finitely many distinct irreducible varieties.

If you're thinking that irreducibility of varieties should be related to primality of ideals, you'd be correct. In fact, we have the following proposition.

Proposition 2.2. *Let $X \subseteq \mathbb{A}^n$ be an affine variety. Then, X is irreducible if and only if $\mathbb{I}(X)$ is prime.*

Proof. We proceed by proving the contrapositive.

Suppose that X is reducible. Write $X = X_1 \cup X_2$ for some strict subvarieties X_1 and X_2. Because X_1 and X_2 are the vanishing sets of some ideal in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, there must exist some $F_1, F_2 \in \mathbb{C}[x_1, \ldots, x_n]$ such that F_1 is identically zero on X_1 but not on X_2, and F_2 is identically zero on X_2 but not on X_1. Thus, the product F_1F_2 is identically zero on X—that is, zero in the coordinate ring $\mathbb{C}[X]$. Therefore, $F_1F_2 \in \mathbb{I}(X)$ but $F_1, F_2 \notin \mathbb{I}(X)$, so $\mathbb{I}(X)$ is not prime.

Conversely, suppose that $\mathbb{I}(X)$ is not prime. Then, there exists some $F_1, F_2 \in \mathbb{C}[x_1, \ldots, x_n]$ such that $F_1F_2 \in \mathbb{I}(X)$, but $F_1 \notin \mathbb{I}(X)$ and $F_2 \notin \mathbb{I}(X)$. Let $X_1 = \mathbb{V}((F_1)) \cap \mathbb{I}(X)$ and $X_2 = \mathbb{V}((F_2)) \cap \mathbb{I}(X)$. Then, $X = X_1 \cup X_2$. □

3. The function field

Let $X \subseteq \mathbb{A}^n$ be an irreducible affine variety. By proposition 2.2, the coordinate ring $\mathbb{C}[X] = \mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(X)$ is an integral domain.

Definition 3.1. *If X is an irreducible affine variety, then the* ***function field*** *(field of rational functions) $\mathbb{C}(X)$ is the field of fractions of $\mathbb{C}[X]$.*

Note that $Y = \{y = 0\} \subseteq \mathbb{A}^2_{x,y}$ and $H = \{xy = 1\} \subseteq \mathbb{A}^2_{x,y}$ have non-isomorphic coordinate rings (exercise), but their function fields are both $\mathbb{C}(x)$.

LECTURE 7: MORPHISMS OF AFFINE VARIETIES

1. MORPHISMS

Definition 1.1. *Let $X \subseteq \mathbb{A}^m$ and $Y \subseteq \mathbb{A}^n$ be affine varieites. A **morphism** from X to Y is a function $\varphi : X \to Y$ that is the restriction of a polynomial map from $\mathbb{A}^m$ to $\mathbb{A}^n$. An **isomorphism** is a morphism that is bijective and whose inverse is also a morphism.*

Remark 1.2. *Morphisms $\varphi : X \to Y$ are in one-to-one bijection with ring homomorphisms $f : \mathbb{C}[Y] \to \mathbb{C}[X]$.*

If $\varphi : X \to Y$ and φ is the restriction of $\Phi : \mathbb{A}^m \to A^n$, define the homomorphism $F : \mathbb{C}[y_1, \ldots, y_n] \to \mathbb{C}[x_1, \ldots, x_m]$ by

$$F(y_j) := \Phi_j(x_1, \ldots, x_n). \tag{1.1}$$

Define $f : \mathbb{C}[Y] \to \mathbb{C}[X]$ to be the restriction of F to $\mathbb{C}[Y]$ composed with the quotient map $\mathbb{C}[x_1, \ldots, x_m] \to \mathbb{C}[X]$.

If $f : \mathbb{C}[Y] \to \mathbb{C}[X]$ and f is the restriction of $F : \mathbb{C}[y_1, \ldots, y_n] \to \mathbb{C}[x_1, \ldots, x_m]$, define the homomorphism $\Phi : \mathbb{A}^m \to A^n$ by

$$\Phi_j(x_1, \ldots, x_n) = F(y_j). \tag{1.2}$$

Define $\varphi : X \to Y$ to be the restriction of Φ.

Exercise: Prove this is a well-defined bijection.

Proposition 1.3. *Two varieties X and Y are isomorphic if and only if $\mathbb{C}[X] \cong \mathbb{C}[Y]$.*

Proof. Exercise. □

Example 1.4. *Let $\varphi : \mathbb{A}^2_{x,y} \to \mathbb{A}^1_x$ be the projection map given by $\varphi(x, y) = x$.*

The corresponding ring homomorphism $f : \mathbb{C}[x] \to \mathbb{C}[x, y]$ is the unique homomorphism satisfying $f(x) = x$; that is, the inclusion map defined by $f(p(x)) = p(x)$ for any $p(x) \in \mathbb{C}[x]$.

Example 1.5. *A morphism from A^1_t to cuspidal cubic $Y = \{y^2 = x^3\} \subseteq \mathbb{A}^2_{x,y}$ is given by $t \mapsto (t^2, t^3)$.*

The corresponding ring homomorphism $f : \mathbb{C}[Y] \to \mathbb{C}[t]$ is defined on the generators of $\mathbb{C}[Y] = \mathbb{C}[x, y]/(y^2 - x^3)$ by $f(x) = t^2$ and $f(y) = t^3$.

Example 1.6. *Consider the points of $\mathbb{A}^{n^2}$ as $n \times n$ matrices with entries in $\mathbb{C}$. The special linear group may be regarded as a subvariety:*

$$\mathrm{SL}_2(\mathbb{C}) = \{M \in \mathbb{A}^{n^2} : \det(M) = 1\} \tag{1.3}$$

Then, the squaring map $\sigma(M) = M^2$ is a morphism of affine varieties from $\mathrm{SL}_2(\mathbb{C})$ to $\mathrm{SL}_2(\mathbb{C})$.

Two varieties X and Y are isomorphic if and only if $\mathbb{C}[X] \cong \mathbb{C}[Y]$.

2. RATIONAL MAPS

Definition 2.1. *A **rational map** from X to Y is a pair (f, U), where U is a nonempty Zariski open subset of X, and f is a function from U to Y defined by rational functions (ratios of polynomials).*

Definition 2.2. *A **birational map** from X to Y is a rational map f from X to Y which has a "rational inverse", that is, a rational map f^{-1} from Y to X such that $f^{-1}(f(x)) = x$ for all $x \in U$ and $f(f^{-1}(y)) = y$ for all $y \in V$, for some nonempty Zariski open subsets $U \subseteq X$ and $V \subseteq Y$.*

If there's a birational map from X to Y, we say that X and Y are **birationally equivalent**. In the particular case of a birational map from A^m to Y, we say that Y has a **rational parametrisation**.

Example 2.3. *Consider the "unit circle" $C = \{(x, y) \in \mathbb{A}^2 : x^2 + y^2 = 1\}$. As shown in lecture 1, the function*

$$p(t) = \left(\frac{-2t}{t^2+1}, \frac{-t^2+1}{t^2+1}\right) \tag{2.1}$$

defines a birational map from $\mathbb{A}^2$ to C. Note that $p(t)$ is defined on $\mathbb{A}^1 \setminus \{i, -i\}$.

Exercise: show that $p(t)$ is birational by constructing a rational inverse.

Proposition 2.4. *Two irreducible varieties X and Y are birationally equavalent if and only if $\mathbb{C}(X) \cong \mathbb{C}(Y)$.*

Proof. Exercise. □

Example 2.5. *Consider the cuspidal cubic $Y = \{y^2 = x^3\} \subseteq \mathbb{A}^2_{x,y}$. This curve has the rational parametrisation $\varphi(t) = (t^2, t^3)$. To show that $\varphi(t)$ is a rational parametrisation, consider the map $\psi(x, y) = \frac{y}{x}$ from $Y \setminus \{(0, 0)\}$ to $\mathbb{A}^1_t$. If $t \in \mathbb{A}^1_t \setminus \{0\}$, then $\psi(\varphi(t)) = \frac{t^3}{t^2} = t$; if $(x, y) \in Y \setminus \{(0, 0)\}$, then $\varphi(\psi(x, y)) = \left(\frac{y^2}{x^2}, \frac{y^3}{x^3}\right) = \left(\frac{x^3}{x^2}, \frac{y^3}{y^2}\right) = (x, y)$. Thus, ψ is a birational inverse to φ.*

LECTURE 9: PROOF OF HILBERT'S NULLSTELLENSATZ

1. Preliminary lemmas

I state without proof two lemmas from commutative algebra that we will need.
The first is the exercise (7) from **Homework 2**; see also exercise (5) from **Problems class 8**.

Lemma 1.1. *Let R be any commutative ring with unity, and let $I \leq R$. Then,*

$$\operatorname{rad}(I) = \bigcap_{\substack{P \geq I \\ P \in \operatorname{Spec}(R)}} P. \tag{1.1}$$

The second is a result about field extensions due to Oscar Zariski. The proof can be found in Atiyah and MacDonald's *Introduction to Commutative Algebra* or (presented rather tersely) on Wikipedia. I may update these notes to include a proof (although you will not need to know it for the exam).

Lemma 1.2 (Zariski's lemma)**.** *Let L be a field extension of a field K. Suppose that L is finitely generated as a K-algebra (that is, there is a surjective map $K[x_1, \ldots, x_n] \twoheadrightarrow L$ for some L). Then, L is a finite extension of K (that is, finitely generated as a K-module).*

For example, the field $K = \mathbb{C}$ is algebraically closed (by the Fundamental Theorem of Algebra), so it has no finite extensions. Zariski's lemma implies a stronger-looking condition—that any field extension of $\mathbb{C}$ that is finitely generated as a $\mathbb{C}$-algebra is equal to $\mathbb{C}$ itself. It's worth noting that $\mathbb{C}(t)$ is *not* finitely generated as a $\mathbb{C}$-algebra.

2. Proof of the Nullstellensatz

Let $R = \mathbb{C}[x_1, \ldots, x_n]$, J an ideal of R, and $X = \mathbb{V}(J) \subseteq \mathbb{A}^n$. We have

$$\operatorname{rad}(J) = \{f \in R : f^k \in R \text{ for some } k\} \leq \mathbb{I}(X) = \{f \in R : f(a) = 0 \text{ for all } a \in \mathbb{V}(J) \tag{2.1}$$

because $f^k(a) = 0 \implies f(a) = 0$.
Now consider $f \in R$ such that $f \notin \operatorname{rad}(J)$. By lemma 1.1,

$$\operatorname{rad}(J) = \bigcap_{\substack{P \geq J \\ P \in \operatorname{Spec}(R)}} P. \tag{2.2}$$

Choose some particular prime ideal $P \geq J$ such that $f \notin P$. Then, R/P is a domain.

Consider the image $\overline{f}$ of f in R/P; since $f \notin P$, $\overline{f} \neq 0$. Taking $S = (R/P)[\overline{f}^{-1}]$, the inclusion map $R/P \to S$ is injective. Let $\mathfrak{m}$ be any maximal ideal of S, so $S/\mathfrak{m}$ is a field. Let ψ be the composition of the maps

$$R \twoheadrightarrow R/P \hookrightarrow S \twoheadrightarrow S/\mathfrak{m}; \tag{2.3}$$

then, the $n+1$ elements $\psi(x_1), \ldots, \psi(x_n), \psi(f)^{-1}$ generate $s/\mathfrak{m}$ as a $\mathbb{C}$-algebra. By Zariski's lemma, $S/\mathfrak{m}$ is a finite extension of $\mathbb{C}$; but $\mathbb{C}$ is algebraically closed, so in fact $S/\mathfrak{m} \cong \mathbb{C}$ in such a

way that the composition of the maps

$$\mathbb{C} \hookrightarrow \mathbb{C}[x_1, \ldots, x_n] = R \xrightarrow{\psi} S/\mathfrak{m} \cong \mathbb{C} \tag{2.4}$$

is the identity map. Let φ be the composition of the isomorphism $S/\mathfrak{m} \cong \mathbb{C}$ with φ.

Let $a_j = \varphi(x_j)$. Then, $\varphi(f) = f(a_1, \ldots, a_n) \in \mathbb{C}$. But $\overline{f}$ is invertible in S, so $\overline{f} \notin \mathfrak{m}$, and thus $\varphi(f) \neq 0$. So $f(a_1, \ldots, a_n) \neq 0$.

On the other hand, if $g \in P$, then $g(a_1, \ldots, a_n) = \varphi(g) = 0$. Thus, the point $(a_1, \ldots, a_n) \in \mathbb{V}(P) \subseteq \mathbb{V}(J)$, even though $f(a_1, \ldots, a_n) \neq 0$. Hence $f \notin \mathbb{I}(J)$.

We've shown that $f \notin \operatorname{rad}(J) \implies f \notin \mathbb{I}(J)$, that is, $\mathbb{I}(J) \leq \operatorname{rad}(J)$. We already proved the reverse inclusion, so $\mathbb{I}(J) = \operatorname{rad}(J)$.

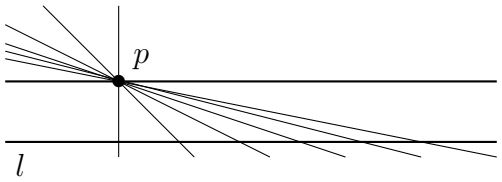
Lecture 10: Projective varieties

Why projective geometry?

Almost all pairs of lines drawn in the plane meet at precisely one point. Unfortunately this isn't always true due to the existence of *parallel lines*. However parallel lines are the exception rather than the rule. Indeed, one version Euclid's fifth axiom (due to the Scottish mathematician John Playfair) states that:

> In a plane, given a line l and a point p not on l, at most one line parallel to l can be drawn through p.

As the lines drawn through p approach the parallel line it is clear that the point of intersection moves further and further away, in either direction.



We would like to solve our problem by saying that parallel lines actually *do* intersect, and their intersection is a point at ∞. Projective space provides a way to make this rigourous.

1 Projective space

Definition 1. *The n-dimensional projective space* $\mathbb{P}^n$ is

$$\mathbb{P}^n = \{l \subset \mathbb{A}^{n+1} : 0 \in l\},$$

the set of all lines in $\mathbb{A}^{n+1}$ that pass through the origin $0 \in \mathbb{A}^{n+1}$.

1.1 Projective space as a quotient of $\mathbb{A}^{n+1} \setminus 0$.

Given a line l and any *nonzero* point $p \in l$ with coordinates $(p_0, \ldots, p_n) \in \mathbb{A}^{n+1}$, then all other points on l are given by $(\lambda p_0, \ldots, \lambda p_n)$ as $\lambda \in \mathbb{C}$ varies. Therefore we can identify $\mathbb{P}^n$ with the set of equivalence classes

$$\mathbb{P}^n = (\mathbb{A}^{n+1} \setminus 0)/\sim$$

where $\sim$ is the equivalence relation

$$(p_0, \ldots, p_n) \sim (p'_0, \ldots, p'_n) \iff \exists \lambda \in \mathbb{C}^\times \text{ such that } p_i = \lambda p'_i \quad \forall i$$

(i.e. two points of $\mathbb{A}^{n+1}$ are considered to give the same point in $\mathbb{P}^n$ if they lie on the same line).

We write points in $\mathbb{P}^n$ in coordinates as $(p_0 : \ldots : p_n)$, subject to the rescaling rule $\sim$. The coordinates p_i can take any value in $\mathbb{C}$, except $(0 : \cdots : 0)$ which is *not* a point of $\mathbb{P}^n$.

1.2 The standard affine charts.

We can parameterise almost all of the lines in $\mathbb{A}^{n+1}$ if we assume one of our coordinates is nonzero.

Definition 2. The *ith standard affine chart* for $\mathbb{P}^n$ is the subset

$$U_i = \{(p_0 : \ldots : p_n) \in \mathbb{P}^n : p_i \neq 0\}$$

where the ith coordinate is nonzero for $i = 0, \ldots, n$.

To see why it is called an affine chart we define maps

$$\phi_i \colon U_i \to \mathbb{A}^n \qquad \phi_i(p_0 : \cdots : p_n) = (\tfrac{p_0}{p_i}, \cdots, \tfrac{p_{i-1}}{p_i}, \tfrac{p_{i+1}}{p_i}, \cdots, \tfrac{p_n}{p_i}),$$

$$\psi_i \colon \mathbb{A}^n \to U_i \qquad \psi_i(a_1, \cdots, a_n) = (a_1 : \cdots : a_i : 1 : a_{i+1} : \cdots : a_n).$$

These maps are well-defined on their image and domain, and are inverses. (Why? See Problem sheet 3, qu. 1.) Therefore these maps provide isomorphisms $U_i \cong \mathbb{A}^n$ and, since at least one coordinate is nonzero $\forall p \in \mathbb{P}^n$, we have

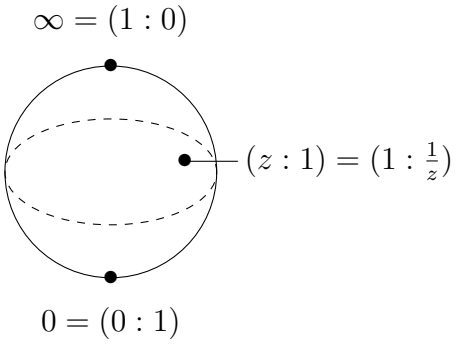
$$\mathbb{P}^n = U_0 \cup U_1 \cup \ldots \cup U_n.$$

1.3 The projective line as the Riemann sphere.

In the case of the projective line $\mathbb{P}^1$ we have a covering by two affine charts $\mathbb{P}^1 = U_0 \cup U_1$, with $U_0, U_1 \cong \mathbb{A}^1$, $U_0 \cap U_1 = \mathbb{A}^1 \setminus 0$ and which are related by the map

$$\phi_1 \circ \psi_0 \colon (\mathbb{A}^1 \setminus 0) \to (\mathbb{A}^1 \setminus 0), \qquad (\phi_1 \circ \psi_0)(z) = \phi_1(1 : z) = \tfrac{1}{z}.$$

This is the glueing description of $\mathbb{P}^1$ as *the Riemann sphere*:



1.4 Decomposition of $\mathbb{P}^n$ into affine pieces.

What does the complement $\mathbb{P}^n \setminus U_i$ look like? It is the subset of lines in $\mathbb{A}^{n+1}$ contained in the linear subspace $\{a_i = 0\} \simeq \mathbb{A}^n$. Therefore $\mathbb{P}^n \setminus U_i \simeq \mathbb{P}^{n-1}$. Continuing inductively we can write $\mathbb{P}^n$ as a disjoint union of sets

$$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1} = \cdots = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^0$$

where $\mathbb{A}^0$ is an affine space of dimension 0 (i.e. a point).

2 Homogeneous polynomials

Definition 3. A polynomial $f \in \mathbb{C}[x_0, \ldots, x_n]$ is *homogeneous of degree* d if every monomial appearing in f has the same degree d.

Note that any $f \in \mathbb{C}[x_0, \ldots, x_n]$ of degree d has a unique expression $f = \sum_{i=0}^{d} f_i$ where f_i is homogeneous of degree i for all $i = 0, \ldots, d$.

Lemma 4. *If f is homogeneous of degree d then*

$$f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$$

for any $\lambda \in \mathbb{C}$.

Proof. Exercise. □

Definition 5. An ideal $I \subset \mathbb{C}[x_0, \ldots, x_n]$ is *homogeneous* if every $f \in I$ can be written as a sum of homogeneous parts $f = \sum_{i=1}^{d} f_i$ with $f_i \in I$ for all i.

An ideal I is homogeneous, if and only if there is a finite generating set $I = \langle f_1, \ldots, f_n \rangle$ such that each f_i is homogeneous (see Problem sheet 3, qu. 4).

2.1 Graded rings.

The ring $R = \mathbb{C}[x_0, \ldots, x_n]$ is a *graded ring*. This means that it has an additive decomposition $R = \bigoplus_{d \geq 0} R_d$, as a $\mathbb{C}$-vector space, where multiplication obeys the rule: if $f \in R_d$ and $g \in R_e$ then $fg \in R_{d+e}$. In this case, R_d is the set of all homogeneous polynomials of degree d.

3 Projective varieties

By Lemma 4, if $f \in \mathbb{C}[x_0, \ldots, x_n]$ is a homogeneous polynomial then the condition $f(p) = 0$ is well-defined for points $p \in \mathbb{P}^n$. (But not for general f!)

Definition 6.

1. A *projective algebraic set* is a subset
$$\mathbb{V}(I) = \{p \in \mathbb{P}^n : f(p) = 0,\ \forall f \in I\}$$
defined by the vanishing of a homogeneous ideal $I \subset \mathbb{C}[x_0, \ldots, x_n]$.
2. Given any subset $X \subset \mathbb{P}^n$, the *ideal of functions vanishing on X* is:
$$\mathbb{I}(X) = \langle f \in \mathbb{C}[x_0, \ldots, x_n] : f(p) = 0,\ \ \forall p \in X \rangle\,.$$
3. The *Zariski topology* on $\mathbb{P}^n$ is the topology for which the closed sets are given by the projective algebraic sets.[1]
4. A *projective variety* X is a projective algebraic set which is irreducible in the Zariski topology, i.e. X cannot be written as $X = X_1 \cup X_2$—a union of two non-trivial projective algebraic sets.

We make the same definitions for projective varieties as we did for affine varieties (*Zariski closure*, *irreducibility* etc.). All the usual statements for $\mathbb{V}$ and $\mathbb{I}$ carry over from the affine case, e.g. $X \subseteq \mathbb{V}(\mathbb{I}(X))$. Note that the standard affine patch $U_i \subset \mathbb{P}^n$ is an open subset in the Zariski topology, since it is the complement to a Zariski closed set $U_i = \mathbb{P}^n \setminus \mathbb{V}(x_i)$.

[1] *Note*: $\mathbb{P}^n$ also has the usual topology as a complex (or real) manifold coming from the standard open affine charts $U_i \cong \mathbb{A}^n \subset \mathbb{P}^n$. However the Zariski topology still makes sense if we replace $\mathbb{C}$ by a general field k.

Lecture 11: Examples & the projective Nullstellensatz

Recap.

- In the last lecture we defined projective space

$$\mathbb{P}^n = \left\{(p_0 : \ldots : p_n) : (p_0 : \ldots : p_n) = (\lambda p_0 : \ldots : \lambda p_n),\ \forall \lambda \in \mathbb{C}^\times\right\}$$

  and introduced the standard affine charts $U_i = \{p \in \mathbb{P}^n : p_i \neq 0\} \cong \mathbb{A}^n$.

- An projective algebraic set $X = \mathbb{V}(I) \subset \mathbb{P}^n$ is the subset of $\mathbb{P}^n$ defined by the vanishing of a homogeneous ideal $I \subset \mathbb{C}[x_0, \ldots, x_n]$.

1 Affine charts on a projective variety

We can use the charts $U_i \subset \mathbb{P}^n$ to obtain affine charts for any projective algebraic set $X \subset \mathbb{P}^n$.

Definition 7. If $X \subset \mathbb{P}^n$ is a projective algebraic set then the ith affine chart on X is:

$$X_{(i)} := X \cap U_i = \{p \in X : p_i \neq 0\}.$$

Note that $X_{(i)}$ is an affine algebraic set in $\mathbb{A}^n$. We have an isomorphism $\phi_i \colon U_i \to \mathbb{A}^n$, where the coordinates on $\mathbb{A}^n$ are $y_j = \frac{x_j}{x_i}$ for $j = 0, \ldots, \widehat{i}, \ldots, n$,[1]. Therefore if $X = \mathbb{V}(I) \subset \mathbb{P}^n$ for a homogeneous ideal $I \subset \mathbb{C}[x_0, \ldots, x_n]$, then $X_{(i)} = \mathbb{V}(I_{(i)}) \subset \mathbb{A}^n$ is given by the vanishing of the (inhomogeneous) ideal

$$I_{(i)} = \langle f(y_0, \ldots, y_{i-1}, 1, y_{i+1}, \ldots, y_n) : f \in I\rangle \subset \mathbb{C}[y_0, \ldots, \widehat{y_i}, \ldots, y_n].$$

The ideal $I_{(i)}$ is called the *dehomogenisation of I with respect to x_i*.[2]

2 Projective closure of an affine variety

Homogenisation. We can reverse this process and turn inhomogeneous polynomials/ideals into homogeneous polynomials/ideals by adding a new variable.

Definition 8.

1. If $f \in \mathbb{C}[x_1, \ldots, x_n]$ is a polynomial of degree d, then the polynomial

$$\widetilde{f} = x_0^d f\left(\tfrac{x_1}{x_0}, \ldots, \tfrac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \ldots, x_n]$$

   is the *homogenisation of f with respect to x_0*.

[1] *Note:* the hat notation $\widehat{\cdot}$ in a sequence means that we omit that term.

[2] In practice, we often don't bother changing notation from x_j to y_j and simply just set $x_i = 1$. This is usually harmless, but you have to be careful when comparing coordinates on two different charts $X_{(i)}$ and $X_{(j)}$.

2. If $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is an ideal, then the ideal

$$\widetilde{I} = \left\langle \widetilde{f} \in \mathbb{C}[x_0, x_1, \ldots, x_n] : \forall f \in I \right\rangle$$

is the *homogenisation of I with respect to x_0*.

Warning. We really have to homogenise *all* elements of the ideal. Only homogenising a generating set for I may not give a generating set for $\widetilde{I}$ (see Problem Sheet 3, qu. 7).

We can use homogenisation to obtain projective varieties from affine ones.

Definition 9. If $X = \mathbb{V}(I) \subset \mathbb{A}^n$ is an affine algebraic set for some ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$, then the *projective closure of X* is the projective algebraic set $\widetilde{X} = \mathbb{V}(\widetilde{I}) \subset \mathbb{P}^n$ defined by the homogenisation $\widetilde{I} \subset \mathbb{C}[x_0, x_1, \ldots, x_n]$.

Taking the projective closure of an affine variety gives the same result as embedding the variety in one of the standard affine charts of projective space and then taking the Zariski closure (see Problem Sheet 3, qu. 5).

3 Examples

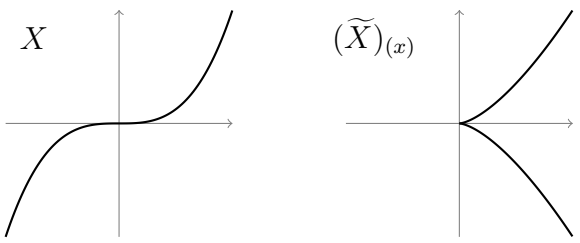
Example 10.

1. As we discussed in the warm-up to the last lecture, we can now check that two parallel lines in the plane meet at one point at ∞. Suppose $L_1, L_2 \subset \mathbb{A}^2_{x,y}$ are two parallel lines given by $L_1 = \mathbb{V}(ax + by + c)$ and $L_2 = \mathbb{V}(ax + by + c')$ for some $a, b, c, c' \in \mathbb{C}$ with $c \neq c'$ and not both of $a, b = 0$. Then the projective closures are $\widetilde{L_1} = \mathbb{V}(ax + by + cz)$ and $\widetilde{L_2} = \mathbb{V}(ax + by + c'z)$ and their intersection $\widetilde{L_1} \cap \widetilde{L_2} \subset \mathbb{P}^2_{(x:y:z)}$ is given by

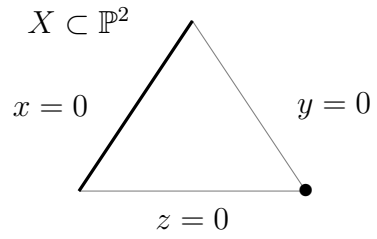
$$\widetilde{L_1} \cap \widetilde{L_2} = \mathbb{V}(ax + by + cz, ax + by + c'z) = \mathbb{V}(ax + by, z) = \{(b : -a : 0)\}.$$

(In fact, given that the point $(b : -a : 0)$ is independent of c and c', we have just shown that all lines parallel to L_1 and L_2 meet in the same point at ∞.)

2. Suppose we take the affine variety $X = \mathbb{V}(x - y^3) \subset \mathbb{A}^2_{x,y}$. What does X look like "at ∞"? The projective closure is $\widetilde{X} = \mathbb{V}(xz^2 - y^3) \subset \mathbb{P}^2_{(x:y:z)}$, and the intersection of $\widetilde{X}$ with the hyperplane at ∞ is given by $\widetilde{X} \cap \mathbb{V}(z) = \{(1 : 0 : 0)\}$. To see what $\widetilde{X}$ looks like near the point $(1 : 0 : 0) \in \mathbb{P}^2$ we can consider the affine chart $U_x = \{x \neq 0\}$ to find that $(\widetilde{X})_{(x)} = \mathbb{V}(z^2 - y^3)$ has a cusp!



3. Suppose $X = \mathbb{V}(xy, xz) \subset \mathbb{P}^2_{(x:y:z)}$ so that $X = \mathbb{V}(x) \cup \mathbb{V}(y, z)$ is the union of the line $\mathbb{V}(x) = \{(0 : y : z)\}$ and the point $\mathbb{V}(y, z) = \{(1 : 0 : 0)\}$.



Restricting to the affine patch $X_{(x)} = \mathbb{V}(y, z) \subset \mathbb{A}^2_{y,z}$, and taking the projective closure $\widetilde{X_{(x)}}$ doesn't give back X—we are missing the line $\mathbb{V}(x) \subset (\mathbb{P}^2 \setminus U_x)$! Similarly, for either $\widetilde{X_{(y)}}$ or $\widetilde{X_{(z)}}$ we lose the point $\mathbb{V}(y, z)$.

4 The projective Nullstellensatz

There is a projective version of the Nullstellensatz. As in the affine case, it is easy to prove that $\mathbb{I}(\mathbb{V}(I)) \subseteq \sqrt{I}$ for a homogeneous ideal I and that $X = \mathbb{V}(\mathbb{I}(X))$ for a projective algebraic set X. However it is no longer true that $\mathbb{V}(I) = \emptyset \iff I = \langle 1 \rangle$, due to the ideal $\langle x_0, \ldots, x_n \rangle$ which defines the point $(0, \ldots, 0) \in \mathbb{A}^{n+1}$. We call $\langle x_0, \ldots, x_n \rangle$ the *irrelevant ideal* of $\mathbb{C}[x_0, \ldots, x_n]$.

Theorem 11 (Projective Nullstellensatz)**.** *Suppose that $I \subset \mathbb{C}[x_0, \ldots, x_n]$ is a homogeneous ideal and that $\mathbb{V}(I) \subset \mathbb{P}^n$ is the corresponding projective algebraic set.*

1. *$\mathbb{V}(I) = \emptyset$ if and only if $\langle x_0, \ldots, x_n \rangle \subseteq \sqrt{I}$.*
2. *If $\mathbb{V}(I) \neq \emptyset$ then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.*

Proof. For $I \subset \mathbb{C}[x_0, \ldots, x_n]$ we consider the affine algebraic set $\mathbb{V}_{\mathbb{A}^{n+1}}(I) \subset \mathbb{A}^{n+1}$, which has the property that

$$(p_0, \ldots, p_n) \in \mathbb{V}_{\mathbb{A}^{n+1}}(I) \iff (\lambda p_0, \ldots, \lambda p_n) \in \mathbb{V}_{\mathbb{A}^{n+1}}(I) \quad \forall p \in \mathbb{A}^{n+1}, \forall \lambda \in \mathbb{C}^\times.$$

Since $\mathbb{V}_{\mathbb{P}^n}(I) = (\mathbb{V}_{\mathbb{A}^{n+1}}(I) \setminus 0)/\sim$, we have

$$\mathbb{V}_{\mathbb{P}^n}(I) = \emptyset \iff \mathbb{V}_{\mathbb{A}^{n+1}}(I) \subseteq \{0\} \iff \langle x_0, \ldots, x_n \rangle \subseteq \sqrt{I}$$

where the second $\iff$ comes from using the affine Nullstellensatz for $\mathbb{V}_{\mathbb{A}^{n+1}}(I)$. If $\mathbb{V}_{\mathbb{P}^n}(I) \neq \emptyset$, then we have

$$f \in \mathbb{I}(\mathbb{V}_{\mathbb{P}^n}(I)) \iff f \in \mathbb{I}(\mathbb{V}_{\mathbb{A}^{n+1}}(I)) \iff f \in \sqrt{I}.$$

where, again, the second $\iff$ comes from using the affine Nullstellensatz for $\mathbb{V}_{\mathbb{A}^{n+1}}(I)$. □

Corollary 12. *The correspondences $\mathbb{I}$ and $\mathbb{V}$ give the following inverse bijections between graded rings and projective geometry:*

Graded rings		*Projective geometry*
$\mathbb{C}[x_0, \ldots, x_n]$	$\longleftrightarrow$	*projective space* $\mathbb{P}^n$
{ *hgs radical ideals* }	$\longleftrightarrow$	{ *proj algebraic sets* }
$\cup$		$\cup$
{ *hgs prime ideals* }	$\longleftrightarrow$	{ *proj varieties* }
$\cup$		$\cup$
{ *hgs maximal ideals* }	$\longleftrightarrow$	{ *points in* $\mathbb{P}^n$ }

Lecture 12: Rational functions and morphisms

Recall. We can write a projective algebraic subset $X = \mathbb{V}(I)$ as the locus where some ideal of homogeneous polynomials $I \subset \mathbb{C}[x_0, \ldots, x_n]$ vanishes:

$$\mathbb{V}(I) = \{p \in \mathbb{P}^n : f(p) = 0, \ \forall f \in I\}.$$

However, it is important to note that homogeneous polynomials do *not*, in general, give well-defined functions on X. Indeed, if f is well-defined on $\mathbb{P}^n$ of degree d, then we must have

$$f(p_0, \ldots, p_n) = f(\lambda p_0, \ldots, \lambda p_n) = \lambda^d f(p_0, \ldots, p_n) \quad \forall \lambda \in \mathbb{C}^\times.$$

If $f(p_0, \ldots, p_n) \neq 0$ then this implies that $d = 0$ and that f is a constant function! Therefore, in order to work with functions on X we have to work with *rational functions*.

1 Rational functions

Let $X \subset \mathbb{P}^n$ be a projective algebraic variety (i.e. irreducible in the Zariski topology).

Definition 13. A *rational function* on X is a partially defined function $f \colon X \dashrightarrow \mathbb{C}$ given by $f = \frac{g}{h}$, where $g, h \in \mathbb{C}[x_0, \ldots, x_n]$ are homogeneous polynomials *of the same degree* d.

As long as $h(p_0, \ldots, p_n) \neq 0$, this *does* give a well-defined function on X since

$$f(\lambda p_0, \ldots, \lambda p_n) = \frac{\lambda^d g(p_0, \ldots, p_n)}{\lambda^d h(p_0, \ldots, p_n)} = \frac{g(p_0, \ldots, p_n)}{h(p_0, \ldots, p_n)} = f(p_0, \ldots, p_n) \quad \forall \lambda \in \mathbb{C}^\times.$$

Lemma 14. *If $h, h' \notin \mathbb{I}(X)$, then two rationals functions $f = \frac{g}{h}$ and $f' = \frac{g'}{h'}$ define the same rational function on X if and only if $gh' - g'h \in \mathbb{I}(X)$.*

Proof. Since $h, h' \notin \mathbb{I}(X)$ it follows that $U = X \setminus \mathbb{V}(h, h')$ is a non-empty Zariski open subset of X, and therefore that $\mathbb{I}(X) = \mathbb{I}(U)$. The two functions f and f' are the same if and only if $(f - f')(p) = 0$ for all $p \in U$. But since $f - f' = \frac{g}{h} - \frac{g'}{h'} = \frac{gh' - g'h}{hh'}$ and $hh' \neq 0$ on U, we have that $(f - f')(p) = 0$ for all $p \in U$ if and only if $(gh' - g'h) \in \mathbb{I}(U)$. □

Example 15. If $X = \mathbb{V}(y^2z - x(x^2 + z^2) \subset \mathbb{P}^2$ then it looks like the rational function $f = \frac{z}{x}$ is not defined at the two points where $x = 0$, $X \cap \mathbb{V}(x) = \{(0 : 1 : 0), (0 : 0 : 1)\}$. However, it follows from Lemma 14 that $\frac{z}{x}$ and $\frac{x^2+z^2}{y^2}$ determine the same rational function on X because $y^2z - x(x^2 + z^2) \in \mathbb{I}(X)$. Now $y^2 \neq 0$ at $(0 : 1 : 0)$, so we can evaluate f at this point using the new expression to get

$$f = \frac{z}{x} = \frac{x^2 + z^2}{y^2} \implies f(0 : 1 : 0) = \frac{0^2 + 0^2}{1^2} = 0.$$

We find that f actually *is* well-defined at the first point $(0 : 1 : 0)$, although still not at the second point $(0 : 0 : 1)$.

Note that Lemma 14 gives an equivalence relation for rational functions on X:

$$\frac{g}{h} \sim \frac{g'}{h'} \iff gh' - g'h \in \mathbb{I}(X).$$

We can define rational functions on X using this equivalence relation $\sim$.

Definition 16.

1. The *rational function field* of X is

$$\mathbb{C}(X) = \left\{ \frac{g}{h} : \begin{matrix} g, h \in \mathbb{C}[x_0, \ldots, x_n] \text{ are hgs of the} \\ \text{same degree, and } h \notin I(X) \end{matrix} \right\} \Big/ \sim$$

2. We say that $p \in X$ is a *regular point* of $f \in \mathbb{C}(X)$ if we can write f as $f = \frac{g}{h}$, for some g, h such that $h(p) \neq 0$ (and an *indeterminate point* of f if not).

3. The *domain of definition of* $f \in \mathbb{C}(X)$ is

$$\operatorname{dom}(f) = \{p \in X : f \text{ is regular at } p\}$$

and the *ideal of denominators of* f is

$$\operatorname{denom}(f) = \left\langle h \in \mathbb{C}[x_0, \ldots, x_n] : f = \frac{g}{h} \text{ for some choice of } g, h \right\rangle.$$

Note that $\operatorname{dom}(f) = X \setminus \mathbb{V}(\operatorname{denom}(f))$ is a non-empty Zariski open subset of X for any $f = \frac{g}{h} \in \mathbb{C}(X)$. (It is non-empty since $h \notin \mathbb{I}(X)$ implies that there is at least one point $p \in X$ such that $h(p) \neq 0$, and hence p is a regular point of f).

2 Rational maps and morphisms

We can use rational functions to define rational maps.

Definition 17. Suppose $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ are two projective algebraic varieties.

1. A *rational map* $f \colon X \dashrightarrow Y$ is a partially defined map given by

$$f(p) = (f_0(p) : \ldots : f_n(p)) \qquad \text{for some } f_0, \ldots, f_n \in \mathbb{C}(X)$$

where $f(p) \in Y \subset \mathbb{P}^n$ when $f(p)$ is defined. We call f *birational* if there exists a rational map $g \colon Y \dashrightarrow X$ such that $f \circ g = \mathrm{id}_X$ and $g \circ f = \mathrm{id}_Y$.

2. A rational map f is *regular* at $p \in X$, if there exists an expression $f = (f_0 : \ldots : f_m)$ such that each f_i is regular at p and at least one $f_i(p) \neq 0$.

3. A *morphism* $f \colon X \to Y$ is a rational map which is regular at all points $p \in X$. We call f an *isomorphism* if there exists a morphism $g \colon Y \to X$ such that $f \circ g = \mathrm{id}_X$ and $g \circ f = \mathrm{id}_Y$.

Note that (as in the affine case) two projective varieties X and Y are birational if and only if $\mathbb{C}(X) = \mathbb{C}(Y)$. We call a variety X *rational* if it is birational to a projective space $\mathbb{P}^n$ (or equivalently if $\mathbb{C}(X) \cong \mathbb{C}(x_0, \ldots, x_n) = \mathbb{C}(\mathbb{P}^n)$).

Example 18.

1. Suppose that $X = \mathbb{V}(x_0x_1 - x_2x_3) \subset \mathbb{P}^3$ is a quadric hypersurface and consider the birational map $\pi\colon X \dashrightarrow \mathbb{P}^2$ with $\pi(p_0 : p_1 : p_2 : p_3) = (p_1 : p_2 : p_3)$, given by forgetting the x_0 coordinate. The map $\phi(p_1 : p_2 : p_3) = \left(\frac{p_2p_3}{p_1} : p_1 : p_2 : p_3\right)$ is a birational inverse to π, so that X is birational to $\mathbb{P}^2$ and hence rational. Is π an isomorphism? What is $\mathrm{dom}(\pi) \subset X$ and $\mathrm{dom}(\phi) \subset \mathbb{P}^2$?

2. **Product of projective varieties.** Since the product of affine spaces is an affine space $\mathbb{A}^m \times \mathbb{A}^n \cong \mathbb{A}^{n+m}$ it is easy to see that the product of two affine algebraic sets $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ is an affine algebraic set:

$$X \times Y = \left\{ p \in \mathbb{A}^{m+n} \ : \ \begin{array}{c} f(z_1, \ldots, z_m) = 0, \ \forall f \in \mathbb{I}(X) \text{ and} \\ g(z_{m+1}, \ldots, z_{m+n}) = 0, \ \forall g \in \mathbb{I}(Y) \end{array} \right\}.$$

However for projective varieties it is no longer clear, since $\mathbb{P}^m \times \mathbb{P}^n \ncong \mathbb{P}^{n+m}$ (unless either $m = 0$ or $n = 0$). First we must show that $\mathbb{P}^m \times \mathbb{P}^n$ is a projective variety by finding an embedding[1] $\phi\colon \mathbb{P}^m \times \mathbb{P}^n \hookrightarrow \mathbb{P}^N$ for some N. In fact, we can take $N = mn + n + m = (m+1)(n+1) - 1$, where we think of coordinates z_{ij} on $\mathbb{P}^N$ as being the entries of a $(m+1) \times (n+1)$ matrix. Now take $\phi\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N$ to be the map:

$$\phi\Big((x_0 : \ldots : x_m) \times (y_0 : \ldots : y_m)\Big) = \begin{pmatrix} x_0y_0 & x_0y_1 & \cdots & x_0y_n \\ x_1y_0 & x_1y_1 & \cdots & x_1y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_my_0 & x_my_1 & \cdots & x_my_n \end{pmatrix}$$

and show that ϕ maps $\mathbb{P}^m \times \mathbb{P}^n$ onto the subvariety $Z \subset \mathbb{P}^N$ defined by

$$Z = \mathbb{V}\left(\det \begin{pmatrix} z_{ik} & z_{il} \\ z_{jk} & z_{jl} \end{pmatrix} = z_{ik}z_{jl} - z_{il}z_{jm} : 1 \leq i, j \leq m, 1 \leq k, l \leq n\right).$$

If you have done qu. 6 on Homework sheet 3 you can try generalising your solution to show that $\mathbb{P}^m \times \mathbb{P}^n \cong Z$ in the case of arbitrary n and m. Now we can take the product of two arbitrary projective varieties $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ by considering the image $\phi(X \times Y) \subset \mathbb{P}^N$.

3 Lack of regular functions on a projective variety

The following result may at first sight might appear surprising, but cf. Liouville's theorem in complex analysis (which says that any bounded holomorphic function on $\mathbb{C}$ must be constant).

Theorem 19. *If X is a projective variety and $f \in \mathbb{C}(X)$ is regular at all points of X, then f is a constant function.*

It easily follows that a projective variety has no non-trivial morphisms to an affine variety.

Corollary 20. *If $f\colon X \to Y$ is a morphism from a projective variety $X \subset \mathbb{P}^n$ to an affine variety $Y \subset \mathbb{A}^m$ then f is a constant map (i.e. f maps X to a point).*

Proof. If $f\colon X \to Y$ is a morphism then in coordinates $f = (f_1, \ldots, f_m)$ where $f_i \in \mathbb{C}(X)$ is a regular at p for each i and for all $p \in X$. By the Theorem, f_i is constant for all i and hence f is constant. □

[1] i.e. a morphism $\phi\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N$ which is an isomorphism onto the image $\phi(\mathbb{P}^m \times \mathbb{P}^n)$.

Lecture 14: Tangent space, singularities and dimension

Let us start by supposing that $X = \mathbb{V}(f) \subset \mathbb{A}^n$ is an *affine hypersurface*—i.e. an affine variety defined by a single irreducible nonconstant equation $f \in \mathbb{C}[x_1, \ldots, x_n]$.

1 The tangent space T_pX

Definition 21. A *tangent line* to $p \in X$ is a line $L \subset \mathbb{A}^n$ which intersects X at p with multiplicity ≥ 2.

What does this condition for L to be tangent to $p \in X$ mean? We can parameterise the line as $L = \{(p_1 + m_1 t, \ldots, p_n + m_n t) : t \in \mathbb{C}\}$, where m_i is the slope of L in the x_i-direction. Now substitute $x_i = p_i + m_i t$ into f and expand out as a polynomial in terms of t to get:

$$f(p_1 + m_1 t, \ldots, p_n + m_n t) = f(p) + \sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_p m_i t + O(t^2)$$

where $\left.\frac{\partial f}{\partial x_i}\right|_p \in \mathbb{C}$ is the constant obtained by evaluating $\frac{\partial f}{\partial x_i}$ at p.[1] The condition for L to be a tangent line at $p \in X$ means that $t = 0$ is a double root of this expression (i.e. that the coefficients of the t^0 and t^1 terms vanish). Therefore, for L to be tangent we require

$$\sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_p m_i t = 0 \implies \sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_p (x_i - p_i) = 0$$

where the condition on the right is independent of the choice of m_i, and hence independent of the choice of L.

Definition 22. The *tangent space to $p \in X$* is the subspace $T_pX \subset \mathbb{A}^n$ defined by this linear equation, i.e.

$$T_pX = \left\{ q \in \mathbb{A}^n : \sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_p (q_i - p_i) = 0 \right\}$$

Example 23.

1. Suppose $X = \mathbb{V}(x^2 - 3xy + y^2 + 2x - y + 1) \subset \mathbb{A}^2_{x,y}$. Then at the point $p = (3, 2)$ we have

$$\left.\frac{\partial f}{\partial x}\right|_p = (2x - 3y + 2)|_p = 2, \qquad \left.\frac{\partial f}{\partial y}\right|_p = (-3x + 2y - 1)|_p = -6,$$

   so the tangent space $T_pX \subset \mathbb{A}^2$ is the line defined by the equation:

$$2(x - 3) - 6(y - 2) = 0 \implies x - 3y + 3 = 0.$$

[1] In this setting differentiation is understood purely formally—i.e. $\frac{\partial}{\partial x_i}$ is an operation on polynomials which satisfies the Leibnitz rule $\frac{\partial(fg)}{\partial x_i} = \frac{\partial f}{\partial x_i} g + f \frac{\partial g}{\partial x_i}$ and sends $x_i^n \mapsto n x_i^{n-1}$, $x_j \mapsto 0$ if $j \neq i$, and $\lambda \mapsto 0$ if $\lambda \in \mathbb{C}$. It is defined for arbitrary polynomials by extending $\mathbb{C}$-linearly.

2. **Projective hypersurfaces.** For projective hypersurface $X = \mathbb{V}(f) \subset \mathbb{P}^n$ we can define the (projective) tangent space as a linear subspace of $\mathbb{P}^n$, by the formula:

$$T_p^{\text{proj}} X = \left\{ q \in \mathbb{P}^n : \sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_p q_i = 0 \right\}$$

To check that we actually have $p \in T_p^{\text{proj}} X$ we need to use *Euler's formula*, which says that $\sum_{i=0}^{n} \frac{\partial f}{\partial x_i} x_i = \deg(f) f$ for a homogeneous polynomial $f \in \mathbb{C}[x_0, \ldots, x_n]$.

Exercises: (1) Prove Euler's formula. (2) Suppose $U_i \subset \mathbb{P}^n$ is a standard affine chart containing $p \in X$, and $T_p X_{(i)}$ is the affine tangent space of $p \in X_{(i)}$ in $U_i \cong \mathbb{A}^n$. Show that $T_p X_{(i)} = (T_p^{\text{proj}} X)_{(i)}$.

2 Singularities

Note that the equation defining the tangent space $T_p X$ is nonzero as long as at least one of the partial derivatives $\frac{\partial f}{\partial x_i}$ does not vanish at p.

Definition 24. The point $p \in X$ is *singular* if $\left.\frac{\partial f}{\partial x_i}\right|_p = 0$ for all $i = 1, \ldots, n$, and *nonsingular* (or *smooth*) otherwise. The *singular locus of* X is the set of all singular points of X

$$\text{sing}(X) = \left\{ p \in X : \left.\frac{\partial f}{\partial x_i}\right|_p = 0, \quad \forall i = 1, \ldots, n \right\}$$

A hypersurface X is *nonsingular* if $\text{sing}(X) = \emptyset$.

Remark. The reason that we call nonsingular points 'smooth' is that, by the inverse function theorem, the nonsingular points of X are precisely the points where X is a *manifold*.

In the case we are considering of a hypersurface $X \subset \mathbb{A}^n$, the tangent space is either $T_p X \cong \mathbb{A}^{n-1}$ if p is nonsingular or $T_p X \cong \mathbb{A}^n$ (i.e. the whole space) if p is singular.

Proposition 25. *The nonsingular locus* $X \setminus \text{sing}(X)$ *is a dense Zariski open subset of* X*.*

Proof. The singular locus $\text{sing}(X) \subset X$ is a Zariski closed subset since it is defined by the vanishing of the following polynomials

$$\text{sing}(X) = \mathbb{V}\left(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n} \right) \subset \mathbb{A}^n.$$

Therefore we only need to show that there is at least one nonsingular point $p \in X$. If there is no nonsingular point then $\frac{\partial f}{\partial x_i} \in \mathbb{I}(X) = \langle f \rangle$ for all $i = 1, \ldots, n$. But, thinking of $\frac{\partial f}{\partial x_i}$ as a polynomial in x_i, we have $\deg_{x_i} \frac{\partial f}{\partial x_i} = \deg_{x_i} f - 1 < \deg_{x_i} f$. Since f is irreducible, if $0 \neq g \in \langle f \rangle$ then $\deg_{x_i} g \geq \deg_{x_i} f$. Therefore we must have $\frac{\partial f}{\partial x_i} = 0$ for all i. Over $\mathbb{C}$ only possibility is that f is a constant function, which contradicts our assumptions on X. □

Example 26. The affine variety $X = \mathbb{V}(x^3 + 3x^2 - y^2) \subset \mathbb{A}^3$ is singular at the point $(0, 0)$ and nonsingular elsewhere, since

$$\text{sing}(X) = \mathbb{V}\left(x^3 + 3x^2 - y^2, 3x^2 + 6x, -2y \right) = \mathbb{V}(x, y) = \{(0, 0)\} \subset \mathbb{A}^2.$$

(*Note*: if we had just considered the ideal $\mathbb{V}\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$, and forgotten to include the equation $f(x, y) = x^3 + 3x^2 - y^2$ defining X, then we may end up thinking that $(-2, 0)$ is also a singular point of X. However $(-2, 0) \notin X$ since $f(-2, 0) = 4 \neq 0$.)

3 The general case

Now suppose that $X \subset \mathbb{A}^n$ is any affine algebraic variety. The general definition of the tangent space is similar to the hypersurface case.

Definition 27. The *tangent space to* $p \in X$ is the subspace $T_pX \subset \mathbb{A}^n$ defined by the linear equations

$$T_pX = \left\{ q \in \mathbb{A}^n : \sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_p (q_i - p_i) = 0, \quad \forall f \in \mathbb{I}(X) \right\}.$$

4 Dimension

Definition 28. The *Jacobian matrix* $\mathrm{Jac}(I)$ of an ideal $I = \langle f_1, \ldots, f_r \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ is the $r \times n$ matrix of partial derivatives

$$\mathrm{Jac}(I) = \left(\frac{\partial f_i}{\partial x_j} \right)_{i=1,\ldots,r,\ j=1,\ldots,n}$$

The following proposition lets us define the *dimension* of X.

Proposition 29. *The function* $\dim T_\bullet X \colon X \mapsto \mathbb{Z}$*, where* $(\dim T_\bullet X)(p) = \dim T_pX$*, is an upper-semicontinuous function on* X *with respect to the Zariski topology (which is just a fancy way of saying that the sets* $X_d = \{p \in X : \dim T_pX \geq d\}$ *are all Zariski closed).*

Proof. The dimension of tangent space at a point $p \in X$ is given by

$$\begin{aligned}
\dim T_pX &= \dim \left\{ q \in \mathbb{A}^n : \sum_{j=1}^{n} \left.\frac{\partial f_i}{\partial x_j}\right|_p (q_j - p_j) = 0, \quad \forall i = 1, \ldots, r \right\} \\
&= \dim \left\{ q \in \mathbb{A}^n : \left.\mathrm{Jac}(\mathbb{I}(X))\right|_p \cdot \begin{pmatrix} q_1 - p_1 \\ \vdots \\ q_n - p_n \end{pmatrix} = 0 \right\} \\
&= \dim \ker \left.\mathrm{Jac}(\mathbb{I}(X))\right|_p .
\end{aligned}$$

Now we have $p \in X_d \iff \dim T_pX \geq d \iff \operatorname{rank} \left.\mathrm{Jac}(\mathbb{I}(X))\right|_p \leq n - d$, and this happens if and only if every $(n-d+1) \times (n-d+1)$ minor of $\left.\mathrm{Jac}(\mathbb{I}(X))\right|_p$ vanishes. Each of these minors is a determinant of a matrix with polynomial entries, and hence a polynomial. Therefore $X_d \subseteq X$ is Zariski closed, since X_d is defined by the vanishing of some polynomials. □

This means that there is a well-defined lowest value $d_{\min}$ of $\dim T_\bullet X$ on a dense open subset of X, i.e. $d_{\min}$ is the value of d such that $X_d = X$ and $X_{d+1} \subsetneq X$.

Definition 30.

1. This lower bound $d_{\min}$ for $\dim T_\bullet X$ is called the *dimension* of X, and denoted $\dim(X)$.
2. We call a point $p \in X$ *nonsingular* if $\dim T_pX = \dim(X)$ and *singular* otherwise. The *singular locus of* X is the (Zariski closed) subset $\mathrm{sing}(X) \subset X$ of all singular points of X. A variety X is *nonsingular* if $\mathrm{sing}(X) = \emptyset$.

Other ways of defining dimension. It is important to know that there are other ways of defining the dimension of an algebraic variety which are more algebraic. For example, the *transcendence degree* $\mathrm{trdeg}_{\mathbb{C}} F$ of a field extension $F/\mathbb{C}$ is defined to be the size of a maximal set of algebraically independent elements $\{t_1, \ldots, t_k\} \subset F$ (i.e. $t_1, \ldots, t_k$ do not satisfy any polynomial equation with coefficients in $\mathbb{C}$). For an algebraic variety X it turns out that $\dim(X) = \mathrm{trdeg}_{\mathbb{C}} \mathbb{C}(X)$. See Reid's *Undergraduate Algebraic Geometry* §6 for a discussion.

Lecture 15: Curves

For the rest of the course we will focus on curves—i.e. algebraic varieties of dimension 1. (*Note*: although these are 1-dimensional over $\mathbb{C}$, they are 2-dimensional over $\mathbb{R}$.) Much of the theory discussed in this lecture is true for any curve, but for simplicity we will restrict to the case of plane curves.

Recall. The *field of rational functions* on an affine algebraic variety $X \subset \mathbb{A}^n$ is given by

$$\mathbb{C}(X) = \left\{ \tfrac{g}{h} : g, h \in \mathbb{C}[x_1, \ldots, x_n] \right\} / \left(\tfrac{g}{h} = \tfrac{g'}{h'} \iff gh' - g'h \in \mathbb{I}(X) \right)$$

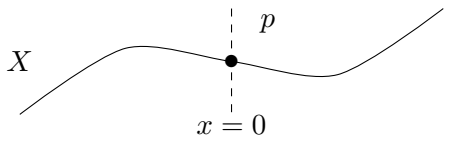
and that $\phi \in \mathbb{C}(X)$ is *regular at* p if there exists a representation $\phi = \frac{g}{h}$ where $h(p) \neq 0$.

1 Local geometry

Suppose $X = \mathbb{V}(f) \subset \mathbb{A}^2$ is an irreducible plane affine curve which is nonsingular at $p \in X$. Wlog we can translate p to the origin $(0,0)$ and assume that the line $\mathbb{V}(x)$ is *not* tangent to $p \in X$ (else reflect X in the diagonal of $\mathbb{A}^2$ to switch $x \leftrightarrow y$). Now f must be of the form

$$f(x,y) = ax + by + \cdots \quad \text{(terms of degree} \geq 2\text{)} \tag{$*$}$$

where $a, b \in \mathbb{C}$. At least one of $a, b \neq 0$, since $p \in X$ is nonsingular, and in fact $b \neq 0$, since $\mathbb{V}(x)$ is not the tangent line to $p \in X$. We have the following picture:



1.1 Order of vanishing of a regular function

Definition 31. The *order of vanishing* $v_p(\phi)$ of a regular function ϕ at p is

$$v_p(\phi) = \max \left\{ n \geq 0 : \tfrac{\phi}{x^n} \text{ is regular at } p \right\}.$$

By definition we also set $v_p(0) = \infty$.

Lemma 32.

1. *If ϕ is regular at p and $\phi(p) = 0$ then $v_p(\phi) > 0$.*
2. *If $v_p(\phi) = n$ then $\frac{\phi}{x^n}$ is regular and nonzero at p. This property determines $v_p(\phi)$ uniquely.*
3. $v_p(\phi\psi) = v_p(\phi) + v_p(\psi)$
4. $v_p(\phi + \psi) \geq \min\{v_p(\phi), v_p(\psi)\}$ *and equality holds if* $v_p(\phi) \neq v_p(\psi)$.

Proof.

1. We need to show that if ϕ is regular at p and $\phi(p) = 0$, then $\frac{\phi}{x}$ is also regular at p. But if $\phi(p) = 0$ then $\phi = \frac{g}{h}$ where $g(p) = 0$, so we can write $g(x, y) = xg_1 + yg_2$ for some $g_1, g_2 \in \mathbb{C}[x, y]$. Now $\frac{\phi}{x} = \frac{g_1}{h} + \frac{y}{x}\frac{g_2}{h}$ where $\frac{g_1}{h}$, $\frac{g_2}{h}$ are regular at p, so the result will follow if we can show $\frac{y}{x}$ is regular at p. From $(*)$ we can write $f(x, y) = xf_1 + yf_2$ with $f_1, f_2 \in \mathbb{C}[x, y]$ where $f_1(p) = a$ and $f_2(p) = b \neq 0$. As a rational function on X, we have $\frac{y}{x} = -\frac{f_1}{f_2}$, since $f = xf_1 + yf_2 \in \mathbb{I}(X)$. Since $f_2(p) \neq 0$ this shows that $\frac{y}{x}$ is regular at p.

2. By definition $\phi' = \frac{\phi}{x^n}$ is regular at p and, if $\phi'(p) = 0$, then $\frac{\phi'}{x} = \frac{\phi}{x^{n+1}}$ is regular at p by (1), contradicting the definition of $\nu_p(\phi)$. Clearly there can be at most one n such that $\frac{\phi}{x^n}$ is regular and nonzero at p.

3. If $v_p(\phi) = m$ and $v_p(\psi) = n$ then $\frac{\phi\psi}{x^{m+n}} = \frac{\phi}{x^m}\frac{\psi}{x^n}$ is regular and nonzero at p, hence $v_p(\phi\psi) = m + n$ by (2).

4. Let $v_p(\phi) = m$, $v_p(\psi) = n$ and (wlog) assume $m \leq n$. Then $\frac{\phi+\psi}{x^m}$ is regular at p, so $v_p(\phi + \psi) \geq \min\{m, n\}$. If $m < n$ then $\frac{\phi}{x^m}$ is nonzero at p whereas $\frac{\psi}{x^m}$ is zero at p, so $\frac{\phi+\psi}{x^m}$ must be nonzero at p. Hence $v_p(\phi + \psi) = \min\{m, n\}$ by (2). □

For an irreducible projective curve $X \subset \mathbb{P}^2$ we can define v_p at any nonsingular point $p \in X$ by restricting to an affine patch containing p and following this construction. It can be shown that v_p is independent of any choices made.

1.2 Order of vanishing of a rational function

Definition 33.

1. A rational function $\phi = \frac{g}{h} \in \mathbb{C}(X)$ has *order of vanishing* $v_p(\phi) = v_p(g) - v_p(h)$ at p. If $v_p(\phi) = -n < 0$ we say that ϕ has a *pole of order* n at $p \in X$.

2. A rational function $t \in \mathbb{C}(X)$ with $v_p(t) = 1$ is called a *uniformiser* at $p \in X$.

It can be shown that $v_p(\phi)$ is independent of the choice of g and h. Note that in the previous discussion, $x \in \mathbb{C}(X)$ was a uniformiser at p. Given any uniformiser t and any $0 \neq \phi \in \mathbb{C}(X)$, we have $v_p(\phi) = n \iff \frac{\phi}{t^n}$ is regular and nonzero at p.

Lemma 34. *A rational function $\phi \in \mathbb{C}(X)$ is regular at p if and only if $v_p(\phi) \geq 0$.*

Proof. Clearly if ϕ is regular at p then $v_p(\phi) \geq 0$. Conversely, write $\phi = \frac{g}{h}$ where $v_p(g) = m$ and $v_p(h) = n$. Pick a uniformiser t and write $g = g't^m$ and $h = h't^n$ where g', h' are regular and nonzero at p. Then $\phi = \frac{g'}{h'}t^{m-n}$. If $v_p(\phi) = m - n \geq 0$ then ϕ is regular at p. □

Example 35. Suppose $X = \mathbb{A}^1_x$. At the point $\lambda \in \mathbb{A}^1$ the function $x - \lambda$ is a uniformiser. For a regular function $f \in \mathbb{C}[x]$ we have $v_\lambda(f) = \max\{m \geq 0 : (x - \lambda)^m \text{ divides } f(x)\}$, or in other words the multiplicity of λ as a root of f. In particular, summing over all $\lambda \in \mathbb{A}^1$ we get $\deg(f) = \sum_{\lambda\in\mathbb{A}^1} v_\lambda(f)$. Similarly, for a rational function $\phi = \frac{g}{h}$, we have $\sum_{\lambda\in\mathbb{A}^1} v_\lambda(\phi) = \deg g - \deg h$.

Now suppose that[1] $m := \deg g - \deg h \geq 0$, and consider $\phi(x)$ as a rational function on $\mathbb{P}^1$ by taking the homogenisation $\widetilde{\phi}(x, y) = \frac{\widetilde{g}}{y^m\widetilde{h}}$ with respect to y. Note that at $\infty = (1 : 0)$, the rational function $\frac{y}{x} \in \mathbb{C}(\mathbb{P}^1)$ is a uniformiser, and we have $\widetilde{g}(1, 0), \widetilde{h}(1, 0) \neq 0$. Therefore $v_\infty(\widetilde{\phi}) = -m$ and $\sum_{\lambda\in\mathbb{P}^1} v_\lambda(\widetilde{\phi}) = \sum_{\lambda\in\mathbb{A}^1} v_\lambda(\widetilde{\phi}) + v_\infty(\widetilde{\phi}) = 0$. So a rational function $\phi \in \mathbb{C}(\mathbb{P}^1)$ always has the *same number of zeroes as poles* (counted with multiplicity).

[1] Or come up with a similar argument if $\deg g - \deg h < 0$.

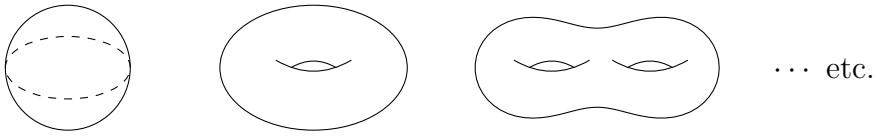
1.3 Extending rational maps from plane curves

Proposition 36. *Given an irreducible plane curve X, a rational map $f\colon X \dashrightarrow \mathbb{P}^n$ and a nonsingular point $p \in X$, then f can always be defined at p. In particular, if X is nonsingular then f can always be extended to a morphism $f\colon X \to \mathbb{P}^n$.*

Proof. We want to show that f is defined at $p \in X$. Pick a uniformiser $t \in \mathbb{C}(X)$ at p. Then we can write $f = (f_1 t^{a_1} : \ldots : f_m t^{a_m})$, where $a_i \in \mathbb{Z}$ and the f_i are all regular and nonzero at p. Now suppose that $a = \min_{i=0,\ldots,m} a_i$ and let $b_i = a_i - a$. Multiplying all coordinates of f by t^{-a} gives $f = (f_1 t^{b_1} : \ldots : f_m t^{b_m})$ where $b_i \geq 0$ for all i and at least one $b_i = 0$. This expression for f is a well-defined at p since the ith coordinate of $f(p)$ is either 0 if $b_i > 0$ or $f_i(p) \neq 0$ if $b_i = 0$, and there is at least one nonzero coordinate. □

2 Global geometry—the genus

The main global invariant that distinguishes a nonsingular curve is called the *genus*. From the topological point of view, the genus $g \in \mathbb{Z}_{\geq 0}$ is the number of 'holes' that the curve has:



$g = 0$ $g = 1$ $g = 2$

Giving a rigorous algebraic definition of the genus would take too long, so we will just consider some examples.

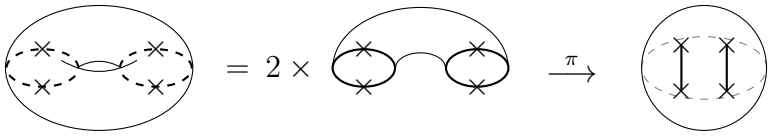
Fact 37. A nonsingular plane curve $C \subset \mathbb{P}^2$ of degree d has genus $g(C) = \frac{(d-1)(d-2)}{2}$.

Lines and conics. We already know that a line or a plane conic is isomorphic to $\mathbb{P}^1$, which we have already seen is the *Riemann sphere* (cf. Lecture 10). Therefore, these curves have genus 0. (In fact, *any* curve of genus 0 must *always* be isomorphic to $\mathbb{P}^1$!)

Cubic curves. *Sketch that a nonsingular cubic curve C has $g(C) = 1$.*

Fact 38. An irreducible plane cubic $C \subset \mathbb{P}^2$ is isomorphic to a plane cubic in *Weierstrass normal form* $\mathbb{V}(y^2z - x^3 - axz^2 - bz^3)$ for some $a, b \in \mathbb{C}$.

A cubic C in Weierstrass form has a projection $\pi\colon C \to \mathbb{P}^1$ with $\pi(x : y : z) = (x : z) \in \mathbb{P}^1$ and $\pi(0 : 1 : 0) = (1 : 0)$. The morphism π is generally 2-to-1, given by considering $y = \pm\sqrt{\frac{x^3+axz^2+bz^3}{z}}$ as a two-valued function on $\mathbb{P}^1$. However there are four *ramification points* where y is single valued, given by $(1 : 0)$ and $(\alpha_i : 1)$ for $\alpha_1, \alpha_2, \alpha_3$ the roots of $x^3 + ax + b = 0$. If we cut $\mathbb{P}^1$ along two branch curves each joining two of the four points, we get two 'sheets' isomorphic to a twice-punctured copy of $\mathbb{P}^1$, where y is single-valued. We can join the sheets up together to get a torus.



Remark. Note, not every value of $g(C) \in \mathbb{Z}_{\geq 0}$ can occur for a nonsingular plane curve $C \subset \mathbb{P}^2$! In particular, there are no plane curves with $g(C) = 2$. Curves of genus 2 do exist, but they can't be embedded in $\mathbb{P}^2$. (In fact 'most' curves can't be embedded in $\mathbb{P}^2$.)

Lecture 16: Bézout's theorem

In this lecture we will see how to define the *intersection multiplicity* $m_p(C, D)$ of two plane curves C and D at a point $p \in \mathbb{P}^2$. We will then prove *Bézout's theorem*:

Theorem 39 (Bézout's theorem)**.** *Suppose that $C, D \subset \mathbb{P}^2$ are two projective plane curves of degrees $\deg C = d$, $\deg D = e$, which have no common components. Then C and D intersect in precisely de points when counted with multiplicity, i.e.*

$$\sum_{p \in C \cap D} m_p(C, D) = de.$$

Note that C and D are not necessarily nonsingular or irreducible and may intersect in a horribly complicated way (e.g. see Figure 1). The trick to proving the theorem is to come up with the right definition for $m_p(C, D)$.

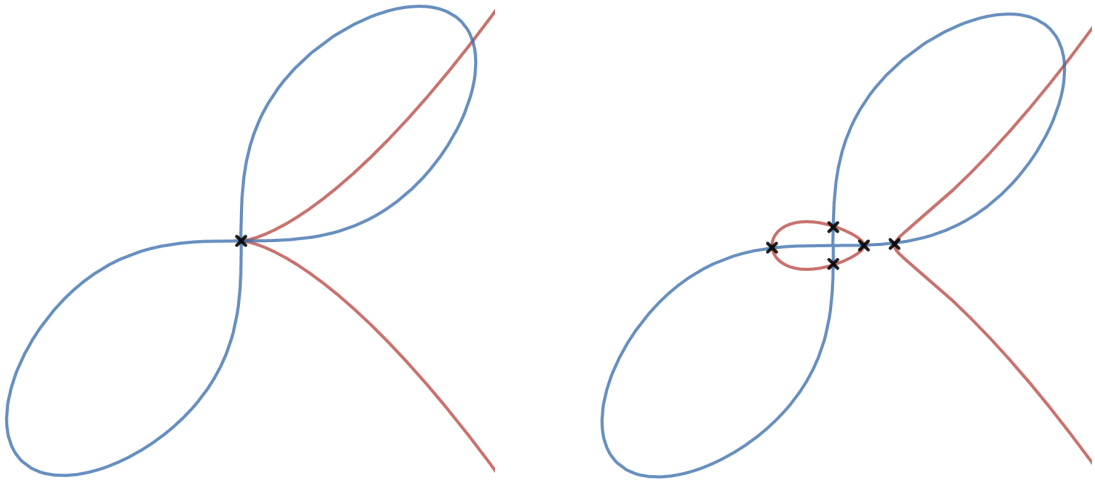


Figure 1: How many times do the curves $C = \mathbb{V}(x^3 - y^2)$ and $D = \mathbb{V}(x^4 + y^4 - xy)$ intersect at the origin $0 \in \mathbb{A}^2$? By considering $C_\epsilon = \mathbb{V}(x^3 - \epsilon x + \epsilon^2 - y^2)$ as $\epsilon \to 0$, we suspect that $m_0(C, D) \geq 5$. (In fact $m_0(C, D) = 5$, as you should soon be able to show using the resultant.)

Remark. For the purpose of counting intersection multiplicities correctly, it is convenient to allow a plane curve C to have multiple components (i.e. if $C = \mathbb{V}(f) \subset \mathbb{P}^2$ and f factors into irreducibles as $f = f_1^{a_1} \cdots f_n^{a_n}$, then the irreducible component $C_i = \mathbb{V}(f_i)$ is counted a_i times).

1 Some easy cases

1.1 A line and a curve

Suppose that $C = \mathbb{V}(f) \subset \mathbb{P}^2$ is a (not necessarily irreducible) curve of degree d and that L is the line $L = \mathbb{V}(ax + by + cz) \subset \mathbb{P}^2$ with $a, b, c \in \mathbb{C}$, not all zero. Without loss of generality we can assume that $a \neq 0$. If L is an irreducible component of C then we set $m_p(C, L) = \infty$.

Suppose L is not an irreducible component of C. Then $f_L(y,z) := f\left(-\frac{by+cz}{a}, y, z\right) \in \mathbb{C}[y,z]$ is a nonzero polynomial of degree d. A root $f_L(y_0,z_0)=0$ corresponds to an intersection point $p=(x_0:y_0:z_0)\in C\cap L$, where $x_0=-\frac{by_0+cz_0}{a}$. We define the intersection multiplicity to be $m_p(C,L)=m$, where m is the multiplicity of the root (yz_0-y_0z) of f_L. Clearly in this case $\sum_{p\in C\cap L} m_p(C,L)=\deg f$, so Bézout's theorem holds.

1.2 Two conics

We can write a conic $f(x,y,z)=ax^2+2bxy+2cxz+dy^2+2eyz+fz^2$ as a matrix product

$$f(x,y,z)=\begin{pmatrix}x & y & z\end{pmatrix}\begin{pmatrix}a & b & c\\ b & d & e\\ c & e & f\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix}=\boldsymbol{x}^T M_f \boldsymbol{x}$$

This gives a bijection $M_f \leftrightarrow f$, between 3×3 symmetric matrices over $\mathbb{C}$ and homogeneous quadratic polynomials in $\mathbb{C}[x,y,z]$.

Definition 40. Suppose that $f,g\in\mathbb{C}[x,y,z]$ are two linearly independent homogeneous quadratic polynomials, and let $C_1=\mathbb{V}(f)$ and $C_2=\mathbb{V}(g)$ be the corresponding conics. The *pencil* $|C_1,C_2|$ is the set of conics

$$|C_1,C_2|=\left\{\mathbb{V}\left(\lambda f+\mu g\right)\subset\mathbb{P}^2 : (\lambda:\mu)\in\mathbb{P}^1\right\}.$$

Proposition 41.

1. *The conic $C=\mathbb{V}(f)\subset\mathbb{P}^2$ is singular, if and only if* $\det(M_f)=0$.
2. *The pencil of conics $|C_1,C_2|$ contains either* 1, 2 *or* 3 *singular conics.*

Proof.

1. Check for yourself that $C=\mathbb{V}(f)$ is singular at $(x_0:y_0:z_0)\in\mathbb{P}^2$ if and only if the vector $(x_0\ y_0\ z_0)\in\ker M_f$.
2. A conic $C\in|C_1,C_2|$ is given by $C=\mathbb{V}\left(\lambda f_1+\mu f_2\right)$. Therefore the singular conics are given by the roots of the (nonzero) cubic polynomial $\det(\lambda M_{f_1}+\mu M_{f_2})=0$. □

Intersection of two conics. We can use a singular conic $C_0\in|C_1,C_2|$ to find the four intersection points $C_1\cap C_2$. Note that if $f(p)=g(p)=0$ then $\lambda f(p)+\mu g(p)=0$ for all $(\lambda:\mu)\in\mathbb{P}^1$. Therefore $p\in C_1\cap C_2$ if and only if $p\in C$ for all $C\in|C_1,C_2|$. Since C_0 is singular we have $C_0=L_1\cup L_2$ (allowing for the case $L_1=L_2$) and we combine multiplicities by adding them, i.e. $m_p(C_0,D)=m_p(L_1,D)+m_p(L_2,D)$. Therefore Bézout's theorem holds:

$$\sum_{p\in C_1\cap C_2} m_p(C_1,C_2)=\sum_{p\in L_1\cap C_2} m_p(L_1,C_2)+\sum_{p\in L_2\cap C_2} m_p(L_2,C_2)=2+2=4.$$

2 The resultant

In order to correctly define the intersection multiplicity of two plane curves at a point, we first need to introduce the resultant. Suppose $f,g\in R[x]$ are two polynomials with coefficients in a commutative ring R. Write them as

$$f=\sum_{i=0}^{d} f_i x^i,\quad g=\sum_{i=0}^{e} g_i x^i$$

where $f_i,g_i\in R$ and $f_d,g_e\neq 0$.

Definition 42. The *resultant of f and g (with respect to x)* is $R_{f,g} = \det M_{f,g}$, where $M_{f,g}$ is the following $(d+e) \times (d+e)$ matrix:

$$M_{f,g} = \begin{pmatrix} f_0 & f_1 & \cdots & f_{d-1} & f_d & & & \\ & f_0 & f_1 & \cdots & f_{d-1} & f_d & & \\ & & \ddots & & & & \ddots & \\ & & & f_0 & f_1 & \cdots & f_{d-1} & f_d \\ g_0 & g_1 & \cdots & g_{e-1} & g_e & & & \\ & g_0 & g_1 & \cdots & g_{e-1} & g_e & & \\ & & \ddots & & & & \ddots & \\ & & & g_0 & g_1 & \cdots & g_{e-1} & g_e \end{pmatrix}$$

where the coefficients of f are written in the first e rows, the coefficients of g are written in the next d rows and all of the remaining entries are 0.

The point of the resultant is that it gives us a criteron to check if f and g share a common root, without having to find the root explicitly.

Proposition 43. *If $R = \mathbb{C}$, then $f, g \in \mathbb{C}[x]$ share a common root if and only if $R_{f,g} = 0$.*

Proof. If f and g have some common root α, then we can write $f(x) = b(x)(x-\alpha)$ and $g(x) = a(x)(x-\alpha)$ for some polynomials $a, b \in \mathbb{C}[x]$ with $\deg a = e-1$ and $\deg b = d-1$. This happens if and only if we have two such polynomials $a, b \in \mathbb{C}[x]$, with

$$a(x)f(x) = b(x)g(x) \implies \sum_{i=0}^{d+e-1} \sum_{j=0}^{i} a_i f_j x^{i+j} = \sum_{i=0}^{d+e-1} \sum_{j=0}^{i} b_i g_j x^{i+j}.$$

Writing this expression out as a matrix product gives $\boldsymbol{x}^t M_{f,g} \boldsymbol{v}$, where $\boldsymbol{x} = (1, x, \cdots, x^{d+e-1})$ and $\boldsymbol{v}$ is the (nonzero) vector

$$\boldsymbol{v} = (a_0, a_1, \cdots, a_{e-1}, -b_0, -b_1, \cdots, -b_{d-1}) \in \mathbb{C}^{d+e}.$$

Since this holds for all $x \in \mathbb{C}$, we must have $\boldsymbol{v} \in \ker M_{f,g} \implies R_{f,g} = 0$. □

We are interested in the case that $R = \mathbb{C}[y, z]$ and $f, g \in \mathbb{C}[y, z][x] = \mathbb{C}[x, y, z]$ are homogeneous polynomials, in which case $R_{f,g}(y, z) \in \mathbb{C}[y, z]$ is a polynomial in y and z.

Proposition 44 (Properties of the resultant)**.**

1. *Suppose $f, g \in \mathbb{C}[x, y, z]$ have $f(1, 0, 0) \neq 0$ and $g(1, 0, 0) \neq 0$. Then f and g have a nontrivial common factor if and only if $R_{f,g}(y, z) = 0$.*

2. *$R_{f,g}(y_0, z_0) = 0$ for some $y_0, z_0 \in \mathbb{C}$ if and only if there exists some $x_0 \in \mathbb{C}$ such that $f(x_0, y_0, z_0) = g(x_0, y_0, z_0) = 0$.*

3. *If $f, g \in \mathbb{C}[x, y, z]$ are homogeneous polynomials of degrees d, e, then $R_{f,g}(y, z) \in \mathbb{C}[y, z]$ is a homogeneous polynomial of degree de.*

Remark. In (1) we suppose that $f(1, 0, 0) \neq 0$ so that f has a x^d term, i.e. the degree of $f(x, y, z)$ is the same as the degree of f regarded as a polynomial in terms of x. Similarly for g.

3 Sketch proof of Bézout's Theorem 39

Theorem 45 (Weak version of Bézout's theorem)**.** *Suppose that $C, D \subset \mathbb{P}^2$ are plane curves of degrees $\deg C = d$, $\deg D = e$ with no common components. Then $\#(C \cap D) \leq de$.*

Proof. If $\#(C \cap D) > de$, let $\{p_1, \ldots, p_{de+1}\} \subset C \cap D$ be a set of distinct points. Choose a point $q \in \mathbb{P}^2$ such that q does not lie on C, D or any of the lines $\overline{p_i p_j} \subset \mathbb{P}^2$. By translating, we can assume $q = (1 : 0 : 0)$ and therefore that $C = \mathbb{V}(f)$ and $D = \mathbb{V}(g)$ where f, g are homogeneous polynomials of degrees d, e with $f(1, 0, 0), g(1, 0, 0) \neq 0$.

Now $R_{f,g}(y, z)$ is a homogeneous polynomial of degree de by Proposition 44(3), and if $p_i = (x_i : y_i : z_i)$ then $R_{f,g}(y_i, z_i) = 0$ by Proposition 44(2). Moreover $(y_i : z_i) \neq (y_j : z_j)$ for any i, j since otherwise the points p_i, p_j, q would be collinear in $\mathbb{P}^2$. But now $R_{f,g}(y, z)$ has at least $de + 1$ distinct roots, so we must have $R_{f,g}(y, z) = 0$ is identically zero. By Proposition 44(1), C and D share a common component. □

Definition 46. Suppose we have two plane curves C, D satisfying the following conditions

1. $(1 : 0 : 0) \notin C \cap D$,
2. $(1 : 0 : 0) \notin \overline{p_i, p_j}$ for any $p_i, p_j \in C \cap D$,
3. $(1 : 0 : 0) \notin T_p C$ and $(1 : 0 : 0) \notin T_p D$ for any $p \in C \cap D$.

We define the *intersection multiplicity* $m_p(C, D)$ to be the multiplicity of the root $(y_0 : z_0)$ of $R_{f,g}(y, z)$ for any $p = (x_0 : y_0 : z_0) \in C \cap D$ (and $m_p(C, D) = 0$ for any $p \notin C \cap D$).

Using this definition of $m_p(C, D)$ a careful adjustment of the proof of Theorem 45 can be used to prove Bézout's Theorem 39.

Lecture 18: Some consequences of Bézout's theorem

1 Elementary consequences

We start with some very elementary consequences of Bézout's theorem:

Corollary 47.

1. *A plane curve has finitely many singular points.*
2. *A nonsingular plane curve is irreducible.*
3. *The intersection multiplicity $m_p(C, D) = 1$ if and only if p is a nonsingular point of both C and D, and the tangent lines T_pC and T_pD are distinct.*

Proof.

1. Given $C = \mathbb{V}(f)$ of degree d, we know that $\operatorname{sing}(C) \subseteq \mathbb{V}(f) \cap \mathbb{V}(\frac{\partial f}{\partial x})$. By Bézout's theorem, this is a set of $\leq d(d-1)$ points.
2. Suppose C has a decomposition $C = C_1 \cup C_2$ with $\deg C_1, \deg C_2 \geq 1$. Then by Bézout's theorem there is at least one point $p \in C_1 \cap C_2 \subset C$, and C must be singular at p.
3. Omitted. See Kirwan's textbook *Complex algebraic curves.* □

2 The Cayley–Bacharach theorem

Definition 48. The *linear system* $L_d(p_1, \ldots, p_m) \subset \mathbb{C}[x, y, z]$ is the $\mathbb{C}$-vector space of homogeneous polynomials of degree d that vanish at $p_1, \ldots, p_m \in \mathbb{P}^2$.

If $f \in L_d(p_1, \ldots, p_m)$ then each point p_i imposes at most one extra condition on the coefficients of f, so

$$\dim L_d(p_1, \ldots, p_m) \geq \binom{d+2}{2} - m$$

where $\binom{d+2}{2}$ is the dimension of the space of all homogeneous polynomials of degree d in $\mathbb{C}[x, y, z]$. The dimension may be larger than expected if the points don't impose independent conditions—for example $\dim L_1(p, q, r) = 0$ if p, q, r are non-collinear, but if p, q, r lie on a line $L = \mathbb{V}(f)$ then $\dim L_1(p, q, r) = 1$ (where $L_1(p, q, r)$ is spanned by f).

Theorem 49. *Suppose we have eight points $p_1, \ldots, p_8 \in \mathbb{P}^2$, no four of which are collinear and no seven of which lie on any conic. Then*

$$\dim L_3(p_1, \ldots, p_8) = 2$$

(i.e. the eight points all impose independent conditions on $f \in L_3(p_1, \ldots, p_8)$).

Proof. We have $\dim L_3(p_1, \ldots, p_8) \geq \binom{5}{2} - 8 = 2$, so we only have to prove that the dimension cannot be bigger. Suppose that $\dim L_3(p_1, \ldots, p_8) \geq 3$. We will find a contradiction.

Case 1. *Suppose no three points lie on a line and no six points lie on a conic.* Let p_9, p_{10} be two more points on the line $L = \overline{p_1 p_2}$. Then

$$\dim L_3(p_1, \ldots, p_8, p_9, p_{10}) \geq \dim L_3(p_1, \ldots, p_8) - 2 \geq 1$$

and therefore there is a (possibly degenerate) cubic curve X passing through $p_1, \ldots, p_{10}$. Since $\#X \cap L \geq 4$, by Bézout's theorem we must have $L \subset X$, so that $X = C \cup L$ where C is a conic. But now the six points $p_3, \ldots, p_8 \in X \setminus L$ must live on the conic C—a contradiction!

Case 2. *Suppose that p_1, p_2, p_3 lie on a line L.* Let p_9 be a fourth point on L. By a similar argument to before, any cubic curve through $p_1, \ldots, p_9$ breaks up as $C \cup L$ for some conic curve C passing through $p_4, \ldots, p_8$. Since

$$L_3(p_1, \ldots, p_8, p_9) \geq \dim L_3(p_1, \ldots, p_8) - 1 \geq 2,$$

there are two distinct conics C_1, C_2 through the five points $p_4, \ldots, p_8$. But now $\#C_1 \cap C_2 \geq 5$ and $C_1 \neq C_2$, so Bézout's theorem implies that C_1 and C_2 share a common line L'. Therefore $C_1 = L_1 \cup L'$ and $C_2 = L_2 \cup L'$. Since no four of the points lie on L', at least two of the points (p_7 and p_8 say) must lie on L_1, and also on L_2. But now $\#L_1 \cap L_2 \geq 2$ and $L_1 \neq L_2$—another contradiction!

Case 3. *Suppose that $p_1, \ldots, p_6$ lie on a conic C.* Choose a seventh point $p_9 \in C$. Then any cubic X that passes through $p_1, \ldots, p_8, p_9$ has $\#X \cap C \geq 7$, so by Bézout's theorem $X = C \cup L$ for some line L which must pass through p_7 and p_8. Since

$$L_3(p_1, \ldots, p_8, p_9) \geq \dim L_3(p_1, \ldots, p_8) - 1 \geq 2,$$

there are at two such cubics $X_1 = C \cup L_1$ and $X_2 = C \cup L_2$. But then $\#L_1 \cap L_2 \geq 2$ and $L_1 \neq L_2$—contradiction! □

Corollary 50 (Cayley–Bacharach theorem)**.** *Let C_1, C_2 be two cubic curves that intersect at nine distinct points $p_1, \ldots, p_9$. Any cubic curve C that passes through the first eight $p_1, \ldots, p_8$ must also pass through the ninth point p_9.*

Proof. If four of the points lie on a line L then C_1 and C_2 must both contain L and cannot intersect in nine distinct points. If seven of the points lie on a conic C then C_1 and C_2 must both contain C and cannot intersect in nine distinct points. Now the eight points $p_1, \ldots, p_8$ satisfy the conditions of Theorem 49 and hence

$$\dim L_3(p_1, \ldots, p_8) = 2.$$

This means that the equations f_1, f_2 defining C_1, C_2 form a basis for $L_3(p_1, \ldots, p_8)$, and therefore the equation for C is of the form $f = \lambda f_1 + \mu f_2$ for some $\lambda, \mu \in \mathbb{C}$. Since $f(p_9) = \lambda f_1(p_9) + \mu f_2(p_9) = 0$ we have that $p_9 \in C$. □

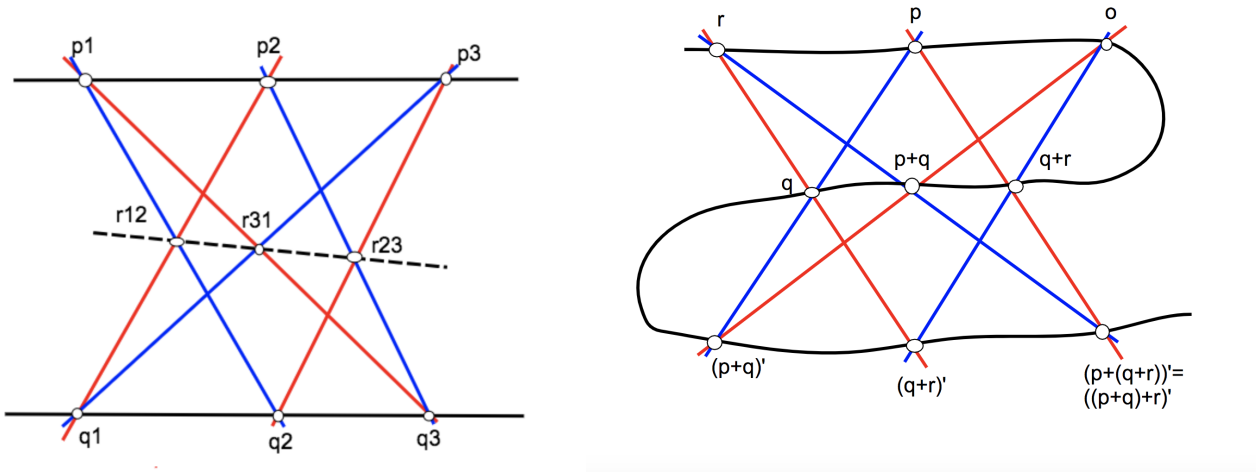
3 Pappus' theorem

Pappus' theorem is a classical theorem in plane Euclidean geometry.

Theorem 51. *Suppose that $\{p_1, p_2, p_3\}$ is one set of three collinear points and $\{q_1, q_2, q_3\}$ is another. Then the points $\{r_{12}, r_{23}, r_{31}\}$, where $r_{ij} = \overline{p_i q_j} \cap \overline{p_j q_i}$, are also collinear.*

Proof. The degenerate cubic curves $C_1 = \overline{p_1 q_2} \cup \overline{p_2 q_3} \cup \overline{p_3 q_1}$ and $C_2 = \overline{p_1 q_3} \cup \overline{p_2 q_1} \cup \overline{p_3 q_2}$ both pass through all nine points $p_1, p_2, p_3, q_1, q_2, q_3, r_{12}, r_{23}, r_{31}$. Now apply Corollary 50 with the degenerate cubic curve $C = \overline{p_1 p_2} \cup \overline{q_1 q_2} \cup \overline{r_{12} r_{23}}$. □

Proof by picture. Picture proof of Pappus' Theorem 51 (on the left) and the associativity of the group law on an elliptic curve (on the right, cf. Theorem 53). In each case the cubic C_1 is drawn in red, C_2 is drawn in blue and C (or E) is drawn in black.



4 The group law on an elliptic curve

Definition 52. An *elliptic curve* is an irreducible nonsingular plane cubic curve $E \subset \mathbb{P}^2$ with a chosen point $o \in E$.

Given an elliptic curve E, we can define an *additive group law* on the points of E with the following properties:

1. For any $p \in E$, the line $\overline{op}$ intersects E at three points o, p, q (counted with multiplicity). Define $p' := q$, and note that $p'' = p$ for all $p \in E$.

2. For any $p, q \in E$, the line $\overline{pq}$ intersects E at three points p, q, r (again, counted with multiplicity). We define $(p+q)' := r$, and hence $p + q = (p+q)'' = r'$ as above.

Theorem 53. *This construction defines an Abelian group law on E with identity element O.*

Proof. First, to show addition is well-defined we need to show that the line $L = \overline{pq}$ is well-defined. This is clearly true if $p \neq q$. If $p = q$ then we let L be the tangent line T_pE, which is well-defined since E is nonsingular and $\dim E = 1$.

Showing that o is the identity and $p + q = q + p$ are easy. To find the inverse of p we let o' be the third intersection point of $T_oE \cap E$. Then $\overline{po'}$ intersects E at three points p, o', q and, by the addition rule applied to $\overline{pq}$, we have $p + q = o'' = o$. Therefore q is the inverse of p.

The hardest part of the theorem is to prove associativity, i.e. that $(p+q)+r = p+(q+r)$. We consider the reducible cubic

$$C_1 = \overline{pq} \cup \overline{o, q+r} \cup \overline{p+q, r}$$

which meets E at the nine points

$$p,\ q,\ (p+q)' \quad o,\ q+r,\ (q+r)', \quad p+q,\ r,\ ((p+q)+r)'$$

and similarly the reducible cubic

$$C_2 = \overline{qr} \cup \overline{o, p+q} \cup \overline{p, q+r}$$

which meets E at the nine points

$$q,\ r,\ (q+r)' \quad o,\ p+q,\ (p+q)', \quad p,\ q+r,\ (p+(q+r))'.$$

Since C_1, C_2 and E have the eight points $o, p, q, r, p+q, q+r, (p+q)', (q+r)'$ in common, the last intersection point is also equal by Corollary 50. Therefore $p+(q+r) = (p+q)+r$. $\square$