# A Zeroth Course in Modern Algebraic Geometry

Abhijnan Rej

Lectures at the Institute of Mathematics & Applications

Bhubaneswar 2012

# Preface

In the Spring of 2011 and 2012, I taught an introductory course on algebraic geometry for the third (and final) year BSc students at the Institute of Mathematics & Applications, Bhubaneswar. From the outset I wanted to teach a "modern" yet introductory course, emphasizing on the commutative algebra and, with out spelling it out as such, present the material as a zeroth level introduction to algebraic geometry in the language pioneered by Weil, Chevalley and ultimately the school of Alexander Grothendieck. My idea was to present a course that would add to the "mathematical culture" of our students rather than any specific mastery over the (difficult) subject matter.

The brevity of these notes makes a detailed table of contents uncalled for; the reader will quickly understand our "game plan" by browsing through this text. In preparing the lectures I have relied on many sources– some of them are listed in the beginning of this text and some are acknowledged in-line in the lectures themselves. The claim to any originality here is pointless and perhaps malicious, the only saving grace perhaps being a slightly unconventional arrangement of the material presented.

I thank Professors Sudarshan Padhy and Swadheen Pattanayak of IMA Bhubaneswar for their interest in the courses and encouragement towards writing the lectures up.

Bhubaneswar
July 26 2012

## Texts suggested for the whole course

---

1. D. Bump, *Algebraic Geometry*, Allied Publishers & World Scientific, 1998/2003.
2. W. Fulton, *Algebraic Curves*, freely available from the Web.
3. R.V. Gurjar and others, *Elliptic Curves*, TIFR and Narosa Publishing House, 2006.
4. I. Shafarevich, *Basic Algebraic Geometry I*, Springer.
5. Miles Reid, *Undergraduate Commutative Algebra*, CUP.
6. Miles Reid, *Undergraduate Algebraic Geometry*, CUP.

# Polynomials, valuations and local rings

# What is algebraic geometry?

(And for those of you are fans of *The Big Bang Theory*, no, I am not going to follow Sheldon Cooper and start with a warm summer evening in ancient Greece!)

The elementary answer is quite simple: it is the study of spaces that can be represented by a collection of polynomials.

A more sophisticated answer is it is a branch of mathematics where geometrical notions are studied using the methods of commutative (and homological) algebra.

Ponder this: Before Descartes in the 16th century, geometry was studied using synthetic notions introduced by Euclid thousands of years ago. Descartes introduced a tremendously powerful method using using coordinates to mark points (on a plane, 3-space, ...) which makes reproving Euclid's theorems more or less trivial.

Algebraic geometry, at its heart, is a far-reaching extension of Descartes' project through a deep study of polynomials and rings of polynomials. For all practical and rigorous purposes the right place to start would be with the work of André Weil in early 20th century and then will the generalizations of Grothendieck and his school since the middle of the 20th century.

## Some properties of polynomials

Main reasons for this are:

1. At the most elementary level, we consider rings of functions on an "algebraic space"– varieties or, more generally, schemes.

2. Whether the defining polynomials are, for example, irreducible or not determines the geometry of the varieties. In general properties of the polynomials and rings of polynomials determine the structure of these geometric objects.

So what we want to do is first study rings like $k[X]$ or $k[X_1, \ldots X_n]$ where all through

$$\boxed{k \text{ is a commutative ring or a field}}$$

I will follow Lang's *Algebra* (p.173 –).

NB: There is a (perhaps confusing!) terminological difference: what Lang calls factorial would be our unique factorization domain (UFD).

Aside: Those of you who really want to know what point of view we would adopt in this course, the answer is: both a mix of *valuation theoretic* and *ideal theoretic* notions. The first approach helps us understand the local properties better which the ideal theoretic notions provide a robust algebraic framework for what follows.

The main results to cover in these first lectures:

1. Gauss' lemma on the multiplicativity of content.

2. Eisenstein's test of irreducibility.

3. Hilbert's basis theorem: if $A$ is Noetherian then $A[X]$ is Noetherian.

4. and finally in a few different guises: **Hilbert's Nullstellensatz**!

Let $A$ be a commutative ring and let $f, g \in A[X]$, $\deg f, g \geq 0$. Assume that the leading coefficient of $g$ is a unit in $A$. Then we have the Euclidean algorithm: there exists $q, r \in A[X]$ such that

$$\begin{aligned} f &= gq + r, \\ \deg r &< \deg g. \end{aligned}$$

The proof of this fact follows from inducting on the degree and rewriting things (covered in previous semesters).

Recall:

1. If $A$ is a ring and $a \in A$, $Aa$ is a left ideal of $A$ called principal. If $A$ is also *commutative* and every ideal of $A$ is principal then we say that $A$ is a principal ring. (We also assume that $A$ does not have zero divisors.

2. If every element of $A$ admits a unique factorization into irreducibles then we call $A$ factorial or a unique factorization domain (UFD).

Note that there is an alternative useful characterization of a UFD:
**Remark 1.** Let $A$ be a ring. $A$ is a UFD (i.e. every element of $A$ can be factored uniquely into irreducibles) if and only if all sequences of principal ideals

$$Aa_1 \subset Aa_2 \subset \cdots$$

are stationary; that is, there exists some $m$ such that $Aa_m = Aa_{m+1}$.
**Example 2.**

$$\mathbb{Z}[i], \mathbb{Z}\Big[\exp\frac{2\pi i}{3}\Big], \ldots$$

**Theorem 3.** *Let $k$ be a field. Then the polynomial ring $k[X]$ is principal.*

*Proof.* Let $\mathfrak{a}$ be a nonzero ideal of $k[X]$ and $g \in \mathfrak{a}$ of minimal degree. Let $f \in \mathfrak{a}$ be nonzero. By the Euclidean algorithm we can always write

$$f = gq + r$$

for some $q, r \in k[X]$ with $\deg r < \deg g$. This gives the fact that $r \in \mathfrak{a}$ but then $r = 0$ since $g$ is of minimal degree which gives us $f = gq$. □

In fact $k[X]$ is a UFD (from the fact that PID $\implies$ UFD). NB: Lang needs an *entire* principal ring but we have already absorbed that in our definitions.

Recall that a root or zero of a polynomial $f(x) \in A[X]$ is an element $b \in B$ where $B \subset A$ is a subring and $f(b) = 0$. We have the following characterization of roots of polynomials.

**Theorem 4.** *Let $k$ be a field, $f$ a polynomial in one variable, $f(X) \in A[X]$, $n := \deg f(X) \geq 0$. Then*

1. *$f$ has atmost $n$ roots in $k$.*

2. *If $a$ is a root of $f$ in $k$, then $X - a$ divides $f(X)$.*

*Proof.* Note that in this case $r$ in the Euclidean Algorithm must be zero. Also note: let $a_i$ be a root and then induct on degree to get a factorization

$$(X - a_1)(X - a_2) \cdots (X - a_n) \text{ for } 1 \leq i \leq n$$

that divides $f(X)$. □

## Valuations and valuation rings

Let $A$ be a UFD and $F$ its quotient field (= field of fractions). Let $p$ be irreducible in $A$. Then each $x \in F$ can be represented as

$$x = p^r \frac{a}{b}.$$

**Definition 5.** Define a function $\mathrm{ord}_p$ from $F$ to $\mathbb{Z}$ at some irreducible $p$ by

$$\mathrm{ord}_p(x) = r.$$

They satisfy the obvious properties:

$$\begin{aligned} \mathrm{ord}_p(xy) &= \mathrm{ord}_p(x) + \mathrm{ord}_p(y), \\ \mathrm{ord}_p(x+y) &\geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}. \end{aligned}$$

**Definition 6.** A discrete valuation on a field $F$ is a function $v : F \to \mathbb{Z}$ such that

$$\begin{aligned} v(xy) &= v(x) + v(y), \\ v(x+y) &\geq \min\{v(x), v(y)\}. \end{aligned}$$

Set also (as a convention): $v(0) = +\infty$.

The value group of $v$ := image of $v$ in $\mathbb{Z}$. As as exercise, establish that

$$\begin{aligned} v\left(\frac{x}{y}\right) &= v(x) - v(y), \\ v(1) &= v(-1) = 0, \\ v(x^n) &= nv(x). \end{aligned}$$

**Remark 7.** $\mathrm{ord}_p$ on $F = \mathbb{Q}$ is an example of a valuation, called the $p$-adic valuation.

**Definition 8.** The ring

$$\boxed{R_v := \{x \in F : v(x) \geq 0\}}$$

is called the discrete valuation ring.

Some more definitions:

1. The group of units $R_v^* \subset R_v$ is defined as $R_v^* := \{x \in F : v(x) = 0\}$.

2. The residue class *field* is defined as $k(v) := R_v/M_v$ where $M_v = \{x \in F : v(x) > 0\}$.

**Remark 9.** $k(v)$ is indeed a field since $M_v$ is a maximal ideal. To see this directly, assume otherwise, i.e., let there be an ideal $\widetilde{M_v}$ containing $M_v$. Picking elements $\tilde{x} \in \widetilde{M_v}$ and $x \in M_v$ and using the fact that if $v(x) < v(\tilde{x})$ then $v(x) = v(x + \tilde{x})$ shows us that $M_v = \widetilde{M_v}$.

# Local rings

**Definition 10.** Let $A$ be a ring with a unique maximal ideal $\mathfrak{m}$. Such a ring is called a local ring. The field $A/\mathfrak{m}$ is called a residue field.

**Example 11.** The discrete valuation ring (definition 8) is an example of a local ring with a fixed valuation $v$.

**Proposition 12** (Atiyah-McDonald, prop. 1.6)**.** *(i) Let $A$ be a ring and $\mathfrak{m} \neq (1)$ be an ideal of $A$ such that every $x \in A \setminus \mathfrak{m}$ is a unit in $A$. Then $A$ is a local ring and $\mathfrak{m}$ its maximal ideal. (ii) Let $A$ be a ring and $\mathfrak{m}$ a maximal ideal of $A$ such that every element in $1 + \mathfrak{m}$ is a unit in $A$. Then $A$ is a local ring.*

*Proof.* (i) Every ideal $\neq (1)$ consists of nonunits, hence it is contained in $\mathfrak{m}$. So $\mathfrak{m}$ is the only maximal ideal of $A$. (ii) Let $x \in A \setminus \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the ideal generated by $x$ and $\mathfrak{m} = (1)$, hence there exists $y \in A$ and $t \in \mathfrak{m}$ such that $xy + t = 1$ and so $xy = 1 - t$ belongs to $1 + \mathfrak{m}$ and is therefore a unit. Now from (i) the result follows. □

**Example 13.** $A = k[x_1, \ldots, x_n]$ with $k$ a field. Then let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal $(f)$ is prime.

**Example 14.** $A = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is of the form $(m)$ for some $m \geq 0$. The ideal $(m)$ prime iff $m$ is prime. All the ideals $(p)$ where $p$ is a prime is maximal. Then $\mathbb{Z}/(p)$ is the field with $p$ elements.

## Local rings and power series; relationship with complex analysis

I follow Reid.

Let $k$ be a field and define the ring of formal power series in variable $X$ over $k$ by $k[[X]]$ by

$$\begin{aligned} k[[X]] &:= \{ \text{ formal power series in } X \text{ with coefficients in } k, \\ &:= \{ \sum_{n=0}^{\infty} a_n X^n : a_n \in k \}. \end{aligned}$$

If $f = a_0 + a_1 X + a_2 X^2 + \ldots$ is a power series then $f$ has an inverse in $k[[X]]$ iff $a_0 \neq 0$. Why? Since here $f = a_0(1 + Xg)$ with some $g \in k[[X]]$ and

$$f^{-1} = a_0^{-1}(1 - Xg + X^2 g^2 - \ldots).$$

We can check that this is a well-defined power series since the coefficient of $X^n$ comes only from the first $(n+1)$ terms of the infinite series. Therefore

$$f \in k[[X]] \text{ is a nonunit } \iff a_0 = 0 \iff f \in (X)$$

so $k[[X]]$ is a local ring with maximal ideal $(X)$.

1. $k[[X]]$ is Noetherian (a few classes ago!)

2. $k[X] \subset k[[X]]$ and any polynomial $g(X)$ with $g(0) \neq 0$ is invertible in $K[[X]]$ so that the local ring

$$k[X]_{(X)} = \{h \in k(X) : h = f/g, f, g \in k[X], f \text{not dividing } g\}$$

is a subring of $k[[X]]$. This inclusion takes a rational function $h = f/g$ defined near 0 to its Taylor series at 0.

Recall that if $k = \mathbb{R}$ or $\mathbb{C}$ then we can talk about convergent power series. A definition from analysis:
**Definition 15.** A power series

$$f = \sum_{n=0}^{\infty} a_n X^n$$

in a variable $X$ has a radius of convergence $\rho$ if

$$|a_n| \leq \text{constant} \cdot \rho^{-n} \forall n$$

Positive radius of convergence = $\limsup \frac{\log |a_n|}{n} < \infty$. This implies $f$ is convergent on a small disc around 0 and can be viewed as an analytic function near 0.

Let $\mathbb{R}\{X\}$ or $\mathbb{C}\{X\}$ be power series with positive radius of convergence.
**Remark 16.** $f^{-1}$ is an analytic function represented by a convergent power series if and only if $a_0 \neq 0$. $\mathbb{R}\{X\}$ and $\mathbb{C}\{X\}$ are local rings with maximal ideal $(X)$.
**Remark 17.** The local ring $\mathbb{C}\{X\}$ is the ring of germs of analytic (= holomorphic) functions around 0. (Germ means that "every $f \in \mathbb{C}\{X\}$ is an analytic function on a neighborhood $U$ of 0".)

For most purposes $\mathbb{C}\{X\}$ is similar to $\mathbb{C}[[X]]$, something which is used quite extensively to study "local properties" of varieties both over $\mathbb{C}$ or over other algebraically closed fields. (By "local properties" I mean how the curve, surface, ... looks and behaves near a prescribed set of points.)

## Gauss' lemma– two equivalent proofs

Let $F$ be a field with a valuation $v$ and define $v^+$ on $F[x_1, \ldots, x_n]$ by

$$v^+(\sum a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}) = \min\{v(a_{i_1 \ldots i_n})\}.$$

**Proposition 18.** *For* $f, g \in F[x_1, \ldots x_n]$,

$$v^+(fg) = v^+(f) + v^+(g).$$

The first proof goes as follows: We do the case of $n = 1$ (the case of just $F[x]$) and then construct a map to the general case. First notice that in the $n = 1$ case, we can assume $f, g \in R_v[x]$. *This is true because:*

$$v^+(cf) = v(c) + v^+(f)$$

and since the definition involves taking a min (and this is just the $n = 1$ case!), can assume

$$v^+(f) = v^+(g) = 0.$$

Now let

$$\begin{aligned} f(x) &= a_m x^m + \cdots + a_0, \\ g(x) &= b_n x^n + \cdots + b_0. \end{aligned}$$

Claim: there exists $i$ and $j$ such that $a_i$ and $b_j$ are units and $a_p$ and $b_q$ nonunits for $p < i$ and $q < j$. (This is true because our $f$ and $g$ are elements of $R_v[x]$.) Now take the product $f(x)g(x)$ and we see that the coefficient of $x^{i+j}$ is a unit. Therefore $v^+(fg) = 0$ and we are done for $n = 1$.

In the general case, choose $d > \deg(fg)$ and map $x_i \mapsto x^{d^{i-1}}$. This transforms

$$f(x_1, \ldots, x_n) \mapsto f^*(x) := f(x, x^d, \ldots x^{d^{n-1}})$$

such that $v^+(f) = v^+(f^*)$. Therefore the general problem is reduced to the $n = 1$ case and we are done.

For the second proof (this one based on Lang), I remind you of something you might have seen in your previous courses:
**Definition 19.** Let $f(x) = a_0 + a_1 x + \ldots a_n x^n$. Define $\operatorname{ord}_p f = \min \operatorname{ord}_p a_i$ and write the content of $f$ to mean

$$\operatorname{cont}(f) := \prod_p p^{\operatorname{ord}_p f}.$$

With this definition we have another (*equivalent*) form for Gauss' lemma:
**Proposition 20.** *Let $A$ be a UFD and $K$ its field of fractions. Let $f, g \in K[x]$. Then*

$$cont(fg) = cont(f)cont(g).$$

This is proved in the following way: Let us write $f(x) = cf_1(x)$ where $c = \text{cont}(f)$ and $f_1(x)$ a primitive polynomial, i.e., with content 1. Write $g$ in the same way: $g = dg_1$, $d = \text{cont}(g)$. Then the statement boils down to showing that if $f, g$ have content 1, then $fg$ also has content 1 and this is the same as showing that for each prime $p$, $\text{ord}_p(fg) = 0$ (and hence through the fact that $(\text{something})^0 = 1$, we have the original statement!). Let

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_0, a_n \neq 0, \\ g(x) &= b_m x^m + \cdots + b_0, b_m \neq 0 \end{aligned}$$

be content 1 polynomials. Let $p \in A$ be prime. If we can show that $p$ does not divide all the coefficients of $fg$, we are done. ( Why?)

Let $r$ be the largest integer such that $0 \leq r \leq n, a_r \neq 0$ and $p$ doesn't divide $a_r$. Similarly let

$$\begin{aligned} b_s &\quad \text{be the coefficient of } g \text{ farthest to the left and} \\ b_s &\quad \neq 0 \text{ such that } p \text{ doesn't divide } b_s. \end{aligned}$$

The coefficient of $x^{r+s}$ in $f(x)g(x)$ is

$$\begin{aligned} c = a_r b_s &+ a_{r+1} b_{s-1} + \cdots \\ &+ a_{r-1} b_{s+1} + \cdots \end{aligned}$$

and $p$ doesn't divide $a_r b_s$. However $p$ divides every nonzero term since in each term there will be some coefficient $a_i$ to the left of $a_r$ or some coefficient $b_j$ to the left of $b_s$. Therefore $p$ does not divide $c$ and we are done.

Intuitively these two propositions and proofs are the same since

- valuation and content are “inverses" (metaphorically speaking!) since cont = 0 and val = 1 are the same.
- this becomes manifest when in the second proof we reduce the statement to proving $\mathrm{ord}_p(fg) = 0$.
- ultimately both proofs boil down to looking at the coefficient of the “cross term" $x^{i+j}$.

**Theorem 21.** *If $R$ is a UFD, then $R[x_1, \ldots x_n]$ is a UFD.*

The proof goes in the following way: Since $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$, we should just do the case of $n = 1$ and then proceed by induction. ($n = 1$ is the case $x = x_1$.) Since $F[x]$ is principal (last lecture) for $F$ a field of fractions of $R$, $F[x]$ is UFD (PID $\implies$ UFD.) Therefore every $f \in R[x] \subset F[x]$ can be written as

$$f = f_1 \cdots f_r,$$

where $f_i$ are irreducibles in $F[x]$. For all irreducible $p$ in $R$ we have

$$0 \leq \mathrm{ord}_p^+(f) = \mathrm{ord}_p^+(f_1) + \cdots \mathrm{ord}_p^+(f_r).$$

We can assume that each $\mathrm{ord}_p^+(f_i) \geq 0$ and $p$ is irreducible over $R$. Then each $f_i$ is irreducible in $R[x]$.

Let $f$ be irreducible in $R[x]$ with $f(x)$ dividing $a(x)b(x)$ in $R[x]$. If $\deg(f) = 0$ then $f$ is irreducible in $R$ and

$$0 < \mathrm{ord}_f^+(a(x)b(x)) = \mathrm{ord}_f^+(a(x)) + \mathrm{ord}_f^+(b(x)).$$

Therefore $f(x)$ divides $a(x)$ when $\mathrm{ord}_f^+(a(x)) > 0$ or $b(x)$ when $\mathrm{ord}_f^+(b(x)) > 0$. If $\deg(f) > 0$ then $\mathrm{ord}_p^+(f) = 0$ for every irreducible $p$ in $R$ and therefore $f$ is irreducible in $F[x]$ by the previous argument. Since $F[x]$ is UFD, $f(x)$ divides $a(x)$ or $b(x)$ so $a(x) = f(x)q(x)$ for example. Then

$$\begin{aligned} 0 \leq \mathrm{ord}_p^+(a(x)) &= \mathrm{ord}_p^+(f(x)) + \mathrm{ord}_p^+(q(x)) \\ &= \mathrm{ord}_p^+(q(x)) \end{aligned}$$

and $q(x)$ in $R[x]$. Hence $f(x)$ divides $a(x)$ in $R[x]$ with quotient $q(x)$ and we are done.

# Some commutative algebra, algebraic sets and the affine $n$-space

# Noetherian rings

A very good reference for the commutative algebra required for the course is chapter 1 of D. Eisenbud's *Commutative algebra with a view towards algebraic geometry*. I shall follow that chapter as well as Lang.

The basic goal would be a result in classical algebraic geometry which says that an algebraic variety (to be defined later!) has only finitely many irreducible components. There are two purely algebraic results that lead upto this, both due to David Hilbert: (1) The Basis Theorem and (2) The Nullstellensatz (German for "theorem of zeros").

At the heart is the notion of a Noetherian ring (named after Emmy Noether) which has a few equivalent definitions.
**Definition 22.** A ring $R$ is said to be Noetherian

1. if every ideal of $R$ is finitely generated.

2. if $R$ satisfies satisfies the ascending chain condition (ACC) which says that all chain of ideals in $R$ terminate. In other words, for every chain of ideals in $R$

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$$

there exists some $m \in \mathbb{Z}^+$ such that $\mathfrak{a}_m = \mathfrak{a}_{m+1}$.

**Proposition 23.** *The two definitions in definition 22 are indeed equivalent.*

*Proof.* If $\mathfrak{a}$ is an ideal of $R$ then by successively choosing elements $f_i$ of $\mathfrak{a}$ we get a chain of ideals

$$(f_1) \subset (f_1, f_2) \subset \dots$$

that can be made to ascend forever (unless one of them is $\mathfrak{a}$.) Thus if $R$ has ACC then $\mathfrak{a}$ must be finitely generated. Conversely, if

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$$

is a strictly ascending chain of ideals of $R$ and the ideal $\bigcup_i \mathfrak{a}_i$ has a finite set of generators then these generators must all be contained in one of the $\mathfrak{a}_j$ and thus $\mathfrak{a}_j = \mathfrak{a}$ and the chain terminates at $\mathfrak{a}_j$. □

This is the same as saying that every nonempty collection of ideals in $R$ has a maximal element.

## The Hilbert Basis Theorem

**Theorem 24.** *If $R$ is Noetherian, then the ring of polynomials $R[x]$ is Noetherian.*

*Proof.* Let $I \subset R[x]$ be an ideal. We need to show that $I$ is finitely generated. Choose a sequence of elements $f_1, f_2, \ldots \in I$ in the following way. Let $f_1$ be a nonzero element of the least degree in $I$. For $i \geq 1$, if $(f_1, \ldots f_i) \neq I$ then choose $f_{i+1}$ to be an element of least degree among those in $I$ but not in $(f_1, \ldots f_i)$, If $(f_1, \ldots, f_i) = I$ then stop choosing. Let $a_j$ be the initial coefficients of $f_j$. Since $R$ is Noetherian the ideal $J = (a_1, a_2, \ldots)$ of all the $a_i$ produced is finitely generated. We may choose a set of generators from among $a_i$ themselves. Let $m$ be the first integer such that $a_1, \ldots a_m$ generate $J$. We claim $I = (f_1, \ldots f_m)$.

Contrary to our process, chose an element $f_{m+1}$. Write $a_{m+1} = \sum_{j=1}^{m} u_j a_j$ for some $u_j \in R$. Since the degree of $f_{m+1}$ is atleast as great as the degree of any of the $f_1, \ldots, f_m$ we may define a polynomial $g \in R$ having the same degree and initial term as $f_{m+1}$ by the formula

$$g = \sum_{j=1}^{m} u_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \ldots f_m).$$

The difference $f_{m+1} - g$ is in $I$ but not in $(f_1, \ldots f_m)$ and has degree strictly less that the degree of $f_{m+1}$. This contradicts the choice of $f_{m+1}$ as having minimal degree. □

**Remark 25.** Even if $R$ itself is Noetherian there may exists a subring $S \subset R$ which may not be Noetherian (Bonus HW).

The basis theorem gets its name from the following related result:

**Proposition 26.** *Given any sequence of elements $f_1, f_2, \ldots \in R[x]$ there is a number $m$ such that for each $n > m$ there is an expression $f_n = \sum_{i=1}^{m} a_i f_i$ with $a_i \in R$. This is equivalent to saying that $R[x]$ is Noetherian.*

To study local analytic geometric properties, the following form of the Basis Theorem is very useful. Let $A[[x]]$ is ring of formal power series with coefficients in $A$.

**Theorem 27.** *If $A$ is Noetherian, then $A[[x]]$ is also Noetherian.*

*Proof.* (Griffiths–Harris, Lang) Let $\mathfrak{u}$ be an ideal of $A[[x]]$. We let $\mathfrak{a}_i$ be the set of elements of $A$ such that $a \in \mathfrak{a}_i$ is the coefficient of $x^i$ in a power series

$$ax^i + \text{ terms of higher degree}$$

lying in $\mathfrak{u}$. Then $\mathfrak{a}_i$ is an ideal of $A$ and $\mathfrak{a}_i \subset \mathfrak{a}_{i+1}$. Then the ascending chain of ideals stop:

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_r = \mathfrak{a}_{r+1} = \ldots$$

Let $a_{ij}$ ( $i = 0, \ldots, r$ and $j = 1, \ldots, n_i$) be the generators of the ideal $a_i$ and let $f_{ij}$ be the power series in $A$ having $a_{ij}$ as beginning coefficient. Given $f \in \mathfrak{u}$ starting with a term of degree $d$, say $d \leq r$, we can find elements $c_1, \ldots, c_{n_d} \in A$ such that

$$f - c_1 f_{d_1} - \ldots c_{n_d} f_{dn_d}$$

starts with a term of degree $\geq d+1$. Through induction, we can assume $d > r$. We then use a linear combination

$$f - c_1^{(d)} x^{d-r} f_{r1} - \ldots c_{n_r}^{(d)} x^{d-r} f_{rn_r}$$

to get a power series starting with a term of degree $d > r$. This power series can be expressed as a linear combination of $f_{r1}, \ldots, f_{rn_r}$ by means of the coefficients

$$g_1(x) = \sum_{\nu=d}^{\infty} c_1^{(\nu)} x^{\nu-r}, \ldots, g_{n_r}(x) = \sum_{\nu=d}^{\infty} c_{n_r}^{(\nu)} x^{\nu-r},$$

and we see that $f_{ij}$ generate our ideal $\mathfrak{u}$ as was to be shown. □

## Algebraic sets and rings of functions

We fix an algebraically closed field $k$ (= $\mathbb{C}$ to make things concrete). Everything would be with respect to this field. I will follow chapter 1 of R. Hartshorne's *Algebraic Geometry*.
**Definition 28.** An affine $n$-space over $k$, denoted as $\mathbb{A}^n_k$ or just $\mathbb{A}^n$, is the collection of all $n$-tuples of elements of $k$, to wit, $(a_1, \ldots, a_n)$ where $a_i \in k$ for all $1 \leq i \leq n$. $a_i$ is referred to as a coordinate of $\mathbb{A}^n$. A typical element $P \in \mathbb{A}^n$ is called a point.

Elements of the polynomial ring $A := k[x_1, \ldots, x_n]$ are interpreted to be functions

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

in the following way. Let $f(P) := f(a_1, \ldots, a_n)$. The zeros of a polynomial $f \in A$ are defined as $Z(f) := \{P \in \mathbb{A}^n : f(P) = 0\}$. For a subset $T \subset A$, the zero set is

$$Z(T) = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in T\}.$$

For $\mathfrak{a} \subset A$ an ideal generated by $T$, $Z(T) = Z(\mathfrak{a})$.

This definition shows that $Z(T)$ is a collection of common zeros of $f_1, \ldots, f_r$.
**Remark 29.** Since $A$ is Noetherian, $\mathfrak{a}$ has a finite set of generators. These furnish the polynomials $f_1, \ldots, f_r$.

**Definition 30.** A subset $Y$ of $\mathbb{A}^n$ is an algebraic set if there exists a subset $T \subseteq A$ such that $Y = Z(T)$.

Remark on notation: what Hartshorne (and we) call $Z$, Fulton in his *Algebraic Curves* book call $V$.

Examples (all for $k = \mathbb{C}$):

1. $Z(Y^2 - X(X^2 - 1)) \subset \mathbb{A}^2$
2. $Z(Y^2 - X^2(X + 1)) \subset \mathbb{A}^2$
3. $Z(W^2 - (X^2 + Y^2)) \subset \mathbb{A}^3$
4. $Z(Y^2 - XY - X^2Y + X^3) \subset \mathbb{A}^2$

## Properties of algebraic sets

We will follow Fulton's *Algebraic Curves*.

**Proposition 31.** *The union of two algebraic sets is algebraic. The intersection of any family of algebraic sets is algebraic set. The empty set and the whole affine space is algebraic.*

*Proof.* If $Y_1 = Z(T_1)$ and $Y_2 = Z(T_2)$ then $Y_1 \cup Y_2 = Z(T_1 T_2)$ (the product of elements of $T_1$ by elements of $T_2$). If $P \in Y_1 \cup Y_2$ then either $P \in Y_1$ or $P \in Y_2$ so $P$ is a zero of every polynomial in $T_1 T_2$. Conversely if $P \in Z(T_1 T_2)$ and let $P \notin Y_1$ then there is an $f \in T_1$ such that $f(P) \neq 0$. Now for any $g \in T_2$, $(fg)(P) = 0$ implies $g(P) = 0$ so that $P \in Y_2$.

If $Y_\alpha = Z(T_\alpha)$ is any family of algebraic sets, then $\bigcap Y_\alpha = Z(\bigcup T_\alpha)$ so $\bigcap Y_\alpha$ is also an algebraic set. Finally $\emptyset = Z(1)$ and the whole space $\mathbb{A}^n = Z(0)$. □

Let $k$ be a field.

**Definition 32.** For any subset $X \subset \mathbb{A}^n$,

$$I(X) := \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots a_n) \in X\}.$$

**Definition 33.** An algebraic set $Z \subset \mathbb{A}^n$ is reducible if

$$Z = Z_1 \cup Z_2$$

where $Z_1, Z_2 \subset \mathbb{A}^n$ and $Z_i \neq \mathbb{A}^n$ where $i = 1, 2$. An algebraic set is irreducible if this is not the case.

**Proposition 34.** *An algebraic set $Z$ is irreducible if and only if $I(Z)$ is prime.*

*Proof.* (Forward) If $I(Z)$ is not prime the suppose $F_1F_2 \in I(Z), \quad F_i \notin I(Z)$. Then

$$Z = (Z \cap Z(F_1)) \cup (Z \cap Z(F_2))$$

and $Z \cap Z(F_i) \subset Z$ so $Z$ is reducible.

(Reverse) Conversely if $Z = Z_1 \cup Z_2$, $Z_i \subset Z$, the $I(Z) \subset I(Z_i)$. Let $F_i \in I(Z_i)$ but $F_i \notin I(Z)$. Then $F_1F_2 \in I(Z)$ so $I(Z)$ not prime. □

**Proposition 35.** *Let $Z$ be an algebraic set of $\mathbb{A}^n$. Then there are unique irreducible algebraic sets $Z_1, \ldots Z_m$ such that*

$$Z = Z_1 \cup \cdots \cup Z_m$$

*and $Z_i \neq Z_j$ for $i \neq j$.*

*Proof.* Let

$$\mathcal{I} := \{\text{algebraic sets } V \subset \mathbb{A}^n : V \text{ is not a union of a finite no. of irreducible algebraic sets}\}.$$

We have to show $\mathcal{I} = \emptyset$. Assume otherwise– let $Z$ be a minimal member of $\mathcal{I}$. Since $Z \in \mathcal{I}$ it is not irreducible so $Z = Z_1 \cup Z_2$ and $Z_i \in \mathcal{I}$. So $Z_i = V_{i_1} \cup \cdots V_{i_{m_i}}$ with $V_{ij}$ irreducible. But $V = \bigcup_{i,j} V_{ij}$ so we obtain a contradiction. Therefore any algebraic set $Z = Z_1 \cup \cdots \cup Z_m$ where $Z_i$ is irreducible for all $1 \leq i \leq m$. To prove the uniqueness of this decomposition– let $Z = W_1 \cup \cdots W_m$ be another decomposition. Then $Z_i = \bigcup_i (W_j \cap Z_i)$ so $Z_i \subset W_{j(i)}$ for some $j(i)$. Similarly $W_{j(i)} \subset Z_k$ for some $k$. But $Z_i \subset Z_j \implies i = j$ so $Z_i = W_{j(i)}$. Similarly each $W_j$ equals some $V_{i(j)}$. □

## Closed algebraic subsets of $\mathbb{A}^n$

**Definition 36.** A closed subset of $\mathbb{A}^n$ is a subset $X$ consisting of all common zeros of a finite number of of polynomials with coefficients in $k$.

**Example 37.** All closed subsets $X$ of $\mathbb{A}^1$. Such a set of given by a system of equations $f_1(x) = \ldots = f_m(x) = 0$ for $x = (x_1, \ldots, x_n)$. If all the $f_i$ are identical to zero then $X = \mathbb{A}^1$. If the $f_i$s don't have any common factor, then they don't have any common root and $X$ does not have any points. If the highest common factors of all the $f_i$'s is $D(x)$ then $D(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ and $X$ consists of finitely many points $x = \alpha_1, \ldots, x = \alpha_n$.

**Example 38.** Let $\alpha \in \mathbb{A}^r$ be a point with coordinates $(\alpha_1, \ldots, \alpha_r)$ and $\beta \in \mathbb{A}^s$ be another point with coordinates $(\beta_1, \ldots, \beta_n)$. Then take $\alpha$ and $\beta$ to a point in $\mathbb{A}^{r+s}$ with coordinates $(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$. Thus we can identify $\mathbb{A}^{r+s}$ with the pairs $(\alpha, \beta)$. The maps

$$\begin{aligned} \mathbb{A}^{r+s} &\longrightarrow \mathbb{A}^r, \\ \mathbb{A}^{r+s} &\longrightarrow \mathbb{A}^s \end{aligned}$$

are called projection maps. Let $X \subset \mathbb{A}^r$ and $Y \subset \mathbb{A}^s$ be closed. Then the set of pairs $(x, y) \in \mathbb{A}^{r+s}$ with $x \in X$ and $y \in Y$ is called the product of $X$ and $Y$ and denoted as $X \times Y$ . This is also a closed set.

## Regular functions

I follow Shafarevich.
**Definition 39.** Let $X \subset \mathbb{A}^n$. A function $f$ defined on $X$ with values in $k$ is called regular if there exists a polynomial $F(x)$ with coefficients in $k$ such that $f(x) = F(x)$ for all $x \in X$.

This definition is generalized in the following way: let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$.
**Definition 40.** A map $f : X \to Y$ is regular if there exists $m$ regular functions $f_1, \ldots, f_m$ on $X$ such that

$$f(x) = (f_1(x), \ldots f_m(x))$$

for all $x \in X$.

Note that for assuming a function regular is a very strong condition– we are essentially only allowing polynomial functions on $\mathbb{A}^n$. Also note: a regular function then is just a regular map $X \to \mathbb{A}^1 = k$.
**Example 41.** The projection map $(x, y) \mapsto x$ is a regular map.
**Example 42.** The map $f(t) = (t^2, t^3)$ is a regular map of the line $\mathbb{A}^1$ to the curve $y^2 = x^3$.

## Intermezzo example: zeta function of a variety

Let $X \subset \mathbb{A}^n_{\mathbb{F}_p}$. The points of $X$ correspond to the solutions of the system of congruences $F_i(T) = 0 \mod p$. Consider $\phi : \mathbb{A}^n \to \mathbb{A}^n$ defined by

$$\phi(\alpha_1, \ldots, \alpha_n) = (\alpha_1^p, \ldots, \alpha_n^p).$$

This is a regular map taking $X \subset \mathbb{A}^n$ to itself. To see this, if $\alpha \in X$, that is $F_i(\alpha) = 0$ and since $F_i(T) \in \mathbb{F}_p[T]$ it follows from the fact that we are dealing with finite fields:

$$\boxed{F_i(\alpha_1^p, \ldots, \alpha_n^p) = (F_i(\alpha_1, \ldots, \alpha_n))^p = 0}$$

The map $\phi : X \to X$ is called the Frobenius map. Why is this map so important?

Answer: points of $X$ with coordinates in $\mathbb{F}_p$ are characterized among all points of $X$ as the fixed points of $\phi$– the solutions to the equation

$$\alpha_i^p = \alpha_i$$

are all the elements of $\mathbb{F}_p$.

We can iterate this map– $\alpha \in \mathbb{F}_{p^r}$ are characterized by

$$\alpha^{p^r} = \alpha$$

and so points $x \in X$ with coordinates in $\mathbb{F}_{p^r}$ are fixed points of $\phi^r$.

Let

$$\boxed{\nu_r := \#\{\text{points } x \in X \text{ with coordinates in } \mathbb{F}_{p^r}\}}$$

These numbers are understood as coefficients of a generating function

$$P_X(t) = \sum_{r=1}^{\infty} \nu_r t^r.$$

**Theorem 43** (without proof!, I believe due to Dwork)**.** $P_X(t)$ *is a rational function of* $t$

The main point is that this function $P_X(t)$ associated to a closed set $X$ is very similar to the Riemann zeta function

$$\zeta(s) = \sum \frac{1}{n^s}.$$

We want to demonstrate this fact!

Note

1. If $x \in X$ is a point with coordinates in $\mathbb{F}_{p^r}$ then $X$ contains all points which are in the image of the i-th iterate of the Frobenius $\eta = \{\phi^i(x)\}$. This is called a cycle and the number $r$ of points of $\eta$ the degree of $\eta$.

2. Group together all the $\nu_r$ points into cycles– the coordinates of any of these points generate $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^r}$ and it is a fact that $d|r$.

These gives us a formula

$$\nu_r = \sum_{d|r} d\mu_d$$

where $\mu_d$ is the number of cycle of degree $d$. Then we perform the following manipulations:

$$\begin{aligned} P_X(t) &= \sum_{r=1}^{\infty} \sum_{d|r} d\mu_d t^r, \\ &= \sum_{d=1}^{\infty} d\mu_d \sum_{m=1}^{\infty} t^{md}, \\ &= \sum_{d=1}^{\infty} \mu_d \frac{dt^d}{1-t^d}. \end{aligned}$$

Introduce the function

$$Z_X(t) = \prod_\eta \frac{1}{1 - t^{\deg \eta}}.$$

Then $P_X(t)$ can be written as

$$P_X(t) = \frac{Z_X'(t)}{Z_X(t)} t.$$

This is *exactly* like the Riemann zeta function:

$$\begin{aligned} p^{\deg \eta} &:= N(\eta), \\ t &= p^{-s}. \end{aligned}$$

Then

$$Z_X(t) = \zeta_X(s) = \prod_\eta \frac{1}{1 - N(\eta)^{-s}}.$$

This is exactly analogous to the formula for the Riemann zeta:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

for $p$ a prime number.

The amazing thing is that the equivalent of the Riemann Hypothesis (RH) (all nontrivial zeros of $\zeta(s)$ have real part $\frac{1}{2}$) was shown to be true for $Z_X(t)$ in 1972 by Deligne (which got him the Fields Medal!) The proof uses extremely hard techniques of algebraic geometry and number theory.

Big open and extremely hard question: can we adapt Deligne's proof to give a proof for the RH for the actual Riemann $\zeta(s)$?

## Isomorphism of closed subsets of the affine space

---

I follow Shafarevich.

**Definition 44.** A regular map $f : X \to Y$ of closed sets is an isomorphism if it has an inverse, that is, if there exists a regular map $g : Y \to X$ such that $f \circ g = 1$ and $g \circ f = 1$.
**Remark 45.** We have

$$X \simeq Y \iff k[Y] \simeq k[X].$$

This is another way of saying that the category of closed subsets of the affine space is isomorphic to a subcategory of the category of commutative $k$-algebras. To determine which subcategory, I remind you that a $k$-algebra $A$ is isomorphic to a coordinate ring $k[X]$ of some closed subset $X$ iff $A$ has no nilpotent elements other than 0 and is finitely generated as an algebra over $k$.

**Example 46.** The generalized parabola $y = x^k$ is isomorphic to the line $\mathbb{A}^1$ and the isomorphism is given by the maps $f(x,y) = x$ and $g(t) = (t, t^k)$.

**Example 47.** This is a nonexample. The projection $f(x,y) = x$ of the hyperbola $xy = 1$ to the $x$-axis is not an isomorphism/one-to-one correspondence: the hyperbola does not contain any point $(x,y)$ for which $f(x,y) = 0$.

**Example 48.** The map $f(t) = (t^2, t^3)$ of the line to the curve $y^2 = x^3$ is seen to be a one-to-one correspondence. It is, though, not as isomorphism since the inverse is of the form $g(x,y) = y/x$ and the function $y/x$ is not regular at 0.

**Example 49.** . This is an important example that introduces the diagonal. Let $X, Y \subset \mathbb{A}^n$ closed subsets. Consider

$$X \times Y \subset \mathbb{A}^{2n}$$

and the linear subspace $\Delta \subset \mathbb{A}^{2n}$ defined by

$$t_1 = u_1, \ldots, t_n = u_n,$$

called the diagonal.

Consider the map

$$\begin{array}{rcl} X \cap Y & \xrightarrow{\phi} & \mathbb{A}^{2n}, \\ z & \mapsto & \phi(z) = (z, z). \end{array}$$

$\phi(z)$ is a point in $X \times Y \cap \Delta$. The map

$$\phi : X \cap Y \to X \times Y \cap \Delta$$

is an isomorphism between $X \cap Y$ and $X \times Y \cap \Delta$.

We can, in this way, study the intersection of two closed sets by studying a different closed set with a linear subspace.

## Bonus material: theorems of Abhyankar–Moh and C.P. Ramanujam

---

Closed subsets of the affine space have completely nontrivial properties. As an example:
**Theorem 50** (Abhyankar–Moh)**.** *A curve $X \subset \mathbb{A}^2$ is isomorphic to $\mathbb{A}^1$ iff there exists an automorphism of $\mathbb{A}^2$ that takes $X$ to a line.*

Note that an automorphism of $\mathbb{A}^2$ is an isomorphism to itself!

The group $\mathrm{Aut}\ \mathbb{A}^2$ is generated by the maps

$$\begin{aligned} x' &= \alpha x, \\ y' &= \beta y + f(x). \end{aligned}$$

Here $\alpha, \beta \neq 0$ and $f$ is a polynomial.

A very important open problem in this area is:
**Conjecture 51** (Jacobian conjecture)**.** *Let $k$ be of characteristic 0. A map given by*

$$x' = f(x,y),\ y' = g(x,y)$$

*is an automorphism of $\mathbb{A}^2$ iff the Jacobian determinant*

$$\frac{\partial(f,g)}{\partial(x,y)}$$

*is a nonzero constant.*

There is an amazing theorem characterizing the affine plane as an algebraic variety, due to the brilliant Indian algebraic geometer C.P. Ramanujam:

**Theorem 52** (Ramanujam, Ann. Math. 1971)**.** *Let $X$ be a nonsingular surface over $\mathbb{C}$. Let $X$ be contractible and simply connected at infinity. Then $X \simeq \mathbb{A}^2$.*

Note what Ramanujam's theorem does is to show

$$\boxed{\text{When is it that if } X \times \mathbb{A}^1 \simeq \mathbb{A}^3, X \simeq \mathbb{A}^2?}$$

The answer is no in general even for $k = \mathbb{C}$ and depends on the topology of $X$ in a very important way.

# The Nullstellensatz

Nice summary of the main idea (Eisenbud):

> Gauss' fundamental theorem of algebra establishes the basic link between algebra and geometry. It says that a polynomial in one variable over $\mathbb{C}$, an algebra object, is determined upto a scalar factor by the set of its roots (with multiplicities). Hilbert's Nullstellensatz extends this link to certain ideals of polynomials in many variables.

Recall that for any subset $X \subset \mathbb{A}^n$, we defined

$$I(X) := \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots a_n) \in X\}.$$

Let $A(X)$ denote the $k$-algebra of functions on $X$ defined by the coordinate functions $x_i$. We have

$$\boxed{A(X) = k[x_1, \ldots, x_n]/I(X)}$$

(This is clear from the definition of $A(X)$ and $I(X)$!)

Caution: Not every homomorphic image of $A(x) \to X$ is a coordinate ring of some set. For example let $f^d = 0$ for some $f \in A(X)$ and a fixed $d$. Now by evaluation at a point $p \in X$, we have $f^d(p) = f(p)^d = 0$ so $f(p)$ is nilpotent for all $p \in X$. But since $X$ is a subset of $k^n$, they are all identical to zero and $A(X)$ is then said to be reduced. (In general if all nilpotent elements of a given ring are zero we call that ring reduced).

Let $R$ be a commutative ring.
**Definition 53.** The radical of an ideal $I \subset R$ then

$$\text{rad } I := \{f \in R : f^m \in I \text{ for some integer } m\}.$$

**Lemma 54.** *$rad\ I$ is an ideal of $R$.*

*Proof.* If $f^m$ and $g^n = 0$ then $(af + bg)^{n+m} = 0$ since it is sum of polynomials each divisible by either $f^n$ or $g^m$. □

A radical ideal is an ideal $I$ such that $I = \text{rad } I$.

Combining the definitions that $R$ is reduced iff the only nilpotent elements are zero and that of a radical ideal, we see that

$$\boxed{R/I \text{ is a reduced ring iff } I \text{ is a radical ideal}}$$

Finally (!) we have a statement of the Nullstellensatz.

**Theorem 55.** *Let $k$ be an algebraically closed field. If $I \subset k[x_1, \ldots, x_n]$ is an ideal then*

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

*Thus, the correspondences $I \mapsto Z(I)$ and $X \mapsto I(X)$ induce a bijection between the collection of algebraic subsets of $\mathbb{A}^n_k = k^n$ and radical ideals of $k[x_1, \ldots, x_n]$.*

An interesting corollary of the Nullstellensatz (justifying the quote from Eisenbud in the beginning of the lecture):

**Corollary 56.** *A system of polynomial equations*

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0, \\ &\ldots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

*over an algebraically closed field $k$ has no solutions in $k^n$ if and only if 1 can be expressed as a linear combination*

$$1 = \sum p_i f_i$$

*with polynomial coefficients $p_i$.*

*Proof.* Granted the Nullstellensatz (to be proved after we have seen its use in the following lectures), if $Z(f_1, \ldots, f_m) = \emptyset$ then 1 is in the radical of $(f_1, \ldots, f_m)$. The other direction follows directly from the definition of a radical ideal. □

# Abstract algebraic varieties and affine algebraic varieties

## The Nullstellensatz (contd.)

Another corollary:
**Corollary 57.** *If $k$ is an algebraically closed field and $A$ a $k$-algebra then $A = A(X)$ for some algebraic set $X$ iff $A$ is reduced and finitely generated as a $k$-algebra.*

*Proof.* (Eisenbud, p.35) If $A = A(X)$ for some $X \subset k^n$, then $A = k[x_1, \ldots, x_n]/I(X)$ is generated as a $k$-algebra by $x_1, \ldots, x_n$. Since $I(X)$ is a radical ideal, $A$ is reduced. Conversely, if $A$ is finitely generated $k$-algebra, then after choosing generators, write $A = k[x_1, \ldots, x_n]/I$ for some ideal $I$. Since $A$ is reduced, $I$ is a radical ideal. This $I = I(Z(I))$ by the Nullstellensatz and we can take $X = Z(I)$. □

Another very important consequence of the Nullstellensatz is:
**Corollary 58.** *Let $X \subset \mathbb{A}^n$ be an algebraic set. Every maximal ideal of $A(X)$ is of the form $\mathfrak{m}_p = (x - a_1, \ldots, x_n - a_n)/I(X)$ for some $p = (a_1, \ldots, a_n) \in X$. More specifically we have a bijection*

$$\{\textit{points of } X\} \leftrightarrow \{\textit{maximal ideals of } A(X)\}.$$

Before we prove this corollary, let me remark on a result in analysis that is exactly in the spirit of this corollary.

**Proposition 59** (Gelfand–Naimark)**.** *Let $S$ be a compact Hausdorff space (Hausdorff = "given two points $P$ and $Q$ there exists disjoint open sets $U_P$ and $U_Q$ containing $P$ and $Q$ respectively.") Let $R$ be the ring of complex-valued $C^0$ functions on $S$. Then the maximal ideals of $R$ are in bijection with the points of $S$.*

Look at any book on functional analysis, e.g. Rudin's *Functional analysis*.
**Lemma 60.** *Any maximal ideal is radical. Also every prime ideal is radical. (NB: Maximal implies prime.)*

The proof of the lemma is left as an exercise.

*Proof.* (of corollary 58, Eisenbud p.35) The maximal ideals of $A(X)$ correspond to the maximal ideals of $k[x_1, \ldots, x_n]$ containing $I(X)$ so just consider the case $X = \mathbb{A}^n$, $A(X) = k[x_1, \ldots, x_n]$. By lemma 60, a maximal ideal $\mathfrak{m}$ is radical so $I(Z(\mathfrak{m})) = \mathfrak{m}$ by the Nullstellensatz. But if $p \in Z(\mathfrak{m})$ then $\mathfrak{m} \subset \mathfrak{m}_p$ and since $\mathfrak{m}$ is assumed to be maximal $\mathfrak{m} = \mathfrak{m}_p$. Therefore the maximal ideals of $A(X)$ are in 1-1 correspondence to $p = (a_1, \ldots, a_n) \in X$. $\square$

For the proof of the Nullstellensatz we need a few more definitions (!)
**Definition 61.** A ring $R$ is called Jacobson if every prime ideal of $R$ is the intersection of maximal ideals.

Our strategy to prove the Nullstellensatz would be the following

1. Claim that a stronger condition holds, involving Jacobson rings

2. Deduce the previous corollary 58 from this claim.

3. Conclude the proof of the Nullstellensatz from these two facts.

**Theorem 62** (strong Nullstellensatz)**.** *Let $R$ be Jacobson. If $S$ is finitely generated as an $R$-algebra then $S$ is Jacobson. If $\mathfrak{n}$ is a maximal ideal then $\mathfrak{m} := \mathfrak{n} \cap R$ is maximal ideal of $R$ and $S/\mathfrak{n}$ is a finite field extension of $R/\mathfrak{m}$.*

*Proof.* (of corollary 58 , Eisenbud p. 134) We note that $k[x_1, \ldots, x_r]/\mathfrak{m}_p = k$ so $\mathfrak{m}_p$ is maximal. Let the map

$$k[x_1, \ldots, x_r] \longrightarrow k[x_1, \ldots, x_r]/\mathfrak{m}_p = k$$

be evaluation at $p$.Thus $I(X) \subset \mathfrak{m}_p$ iff $p \in X$. We know that the maximal ideals of $A(X)$ are the maximal ideals of $S := k[x_1, \ldots, x_r]$ containing $I(X)$, taken modulo $I(X)$ it only remains to show that every maximal ideal of $S$ has the form $\mathfrak{m}_p$ for some $p$.

Let $\mathfrak{n}$ be a maximal ideal of $S$. Then by previous (unproved) theorem 62 with $R = k$, $S/\mathfrak{n}$ is algebraic over $k/(\mathfrak{n} \cap k) = k$. Since $k$ is algebraically closed $S/\mathfrak{n} = k$. Let $a_i$ be the image of $x_i$ under the map $S \to S/\mathfrak{n} = k$ and let $p = (a_1, \ldots, a_r)$. This implies $\mathfrak{m}_p$ is contained in $\mathfrak{n}$. Since $\mathfrak{m}_p$ is maximal, $\mathfrak{m} - p = \mathfrak{n}$. □

*Proof.* Theorem 55. From the corollary 58 we know that the points of $Z(I)$ correspond to the maximal ideals of $k[x_1, \ldots, x_n]$ containing I. Thus $I(Z(I))$ is the intersection of all maximal ideals containing $I$. From theorem 62 the ring $S = k[x_1, \ldots, x_n]$ is Jacobson so every prime ideal that contains $I$ is an intersection of maximal ideals (from the definition of Jacobson). Thus $I(Z(I))$ is equal to the intersection of all prime ideals containing $I$. This is just $\mathrm{rad}\ (I)$ (HW: why?). □

## The space of maximal ideals: a topological version

---

Let $A$ be a (commutative, unital) ring. By $\mathrm{Specmax}(A)$ we mean the set of all maximal ideals of $A$. (But, later on we would be interested in $\mathrm{Spec}\ (A)$, the set of all prime ideals of $A$.)

Let $X$ be a compact Hausdorff space and let $C(X)$ denote the ring of all real-valued continuous functions on $X$. For each $x \in X$, let $\mathfrak{m}_x$ be the set of all $f \in C(X)$ such that $f(x) = 0$.

**Proposition 63.** *The ideal $\mathfrak{m}_x$ is maximal.*

*Proof.* $\mathfrak{m}_x$ is maximal since it is the kernel of a surjective homomorphism $C(X) \to \mathbb{R}$ which maps $f$ to $f(x)$. □

If $\widetilde{X}$ denotes $\mathrm{Specmax}(C(X))$ we have defined a map

$$\begin{array}{rcl} \mu : X & \longrightarrow & \widetilde{X}, \\ x & \mapsto & \mathfrak{m}_x. \end{array}$$

**Theorem 64.** *$\mu$ is a bijection (in fact, a homeomorphism of $X$ onto $\widetilde{X}$.)*

The proof of this theorem goes as follows: Let $\mathfrak{m}$ be a maximal ideal of $C(X)$ and let $Z(\mathfrak{m})$ be the set of common zeros of the functions in $\mathfrak{m}$; that is

$$Z(\mathfrak{m}) = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose that $Z = \emptyset$. Then for each $x \in X$, there exists $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since $f_x$ is continuous, there exists an open neighborhood $U_x$ of $x \in X$ on which $f_x$ doesn't vanish.

Since $X$ is assumed to be compact, there is a finite number of neighborhoods $U_{x_1}, \ldots U_{x_n}$ which cover $X$. Let

$$f = f_{x_1}^2 + \cdots + f_{x_n}^2.$$

Then $f$ doesn't vanish at any point of $X$ and so is a unit in $C(X)$. But this contradicts $f \in \mathfrak{m}$ hence $Z \neq \emptyset$. Let $x \in Z$. Then $\mathfrak{m} \subseteq \mathfrak{m}_x$ because $\mathfrak{m}$ is maximal. Hence $\mu$ is surjective. By Urysohn's lemma, the continuous functions separate the points in $X$, Hence $x \neq y \implies \mathfrak{m} \neq \mathfrak{m}_x$. Therefore, $\mu$ is injective. QED.

Let $f \in C(X)$ and let

$$\begin{aligned} U_f &= \{x \in X : f(x) \neq 0\}, \\ \widetilde{U}_f &= \{\mathfrak{m} \in \widetilde{X} : f \notin \mathfrak{m}\}. \end{aligned}$$

One sees from the definitions that

$$\mu(U_f) = \widetilde{U}_f.$$

The open sets $U_f$ (resp. $\widetilde{U}_f$) forms a basis for a topology of $X$ (resp. $\widetilde{X}$) and $\mu$ is a homeomorphism.

Upshot: The space $X$ can be reconstructed from the ring of functions on $C(X)$. An extremely deep generalization of this idea lies in the description of a space only in terms of sheaves associated to that space, an idea that generalizes algebraic geometry to very abstract levels (due to Grothendieck and his school.)

## The prime spectrum and Zariski topology

Let $A$ be a commutative ring and let $X$ denote the set of all prime ideals of $A$. For each subset $E$ of $A$, let $V(E)$ denote the set of all prime ideals which contain E.

**Proposition 65.** *The following holds:*

1. *If $\mathfrak{a}$ is an ideal generated by $E$, then $V(E) = V(\mathfrak{a}) = V(rad(A))$.*
2. *$V(0) = X$, $V(1) = \emptyset$.*
3. *If $E_i$, $i \in I$, a family of subsets of $A$ then*
$$V(\bigcup_{i \in I} E_i) = \bigcap_{i \in I} V(E_i).$$
4. *$V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.*

From this proposition we see that $V(E)$ satisfies the axioms for closed sets in a topological space. This is called the Zariski topology. The space $X$ is written as $\mathrm{Spec}(A)$. This space is also the base topological space for an abstract algebraic object called an affine prescheme.

## Affine algebraic varieties

**Definition 66.** Let $k$ be an algebraically closed field and let

$$f_\alpha(x_1, \ldots, x_n) = 0$$

be a set of polynomial equations in $n$-variables with coefficients in $k$. The set $X$ of points $p = (p_1, \ldots, p_n) \in k^n$ which satisfy these equations is an affine algebraic variety.

Consider the set of all polynomials $g \in k[x_1, \ldots, x_n]$ with the property that $g(p) = 0$ for all $p \in X$. This set is an ideal $I(X)$ in the polynomial ring and is called the ideal of the variety $X$. The quotient ring

$$A(X) = k[x_1, \ldots, x_n]/I(X)$$

is the ring of polynomial functions on $X$ because two polynomials $g, h$ define the same polynomial function on $X$ if and only if $g - h$ vanishes at every point of $X$, that is, if and only if $g - h \in I(X)$.

Let $\eta_i$ be the image of $x_i$ in $A(X)$. The $\eta_i$, $1 \leq i \leq n$, are the coordinate functions on $X$. If $p \in X$ then $\eta_i(p)$ is the $i$-th coordinate of $x$. $A(X)$ is generated as a $k$-algebra by the coordinate functions, and is called the coordinate ring (or affine algebra) of $X$.

Similar to the topological version of the previous lecture, for each $p \in X$ define $\mathfrak{m}_p$ be the ideal of all $f \in A(X)$ such that $f(p) = 0$. The following proposition is left as homework:

**Proposition 67.** *This ideal $\mathfrak{m}_p$ is a maximal ideal of $A(X)$.*

**Theorem 68.** *Let $\widetilde{X} = Specmax(A(X))$ and define a map map $X \xrightarrow{\mu} \widetilde{X}$ given by $p \mapsto \mathfrak{m}_p$. This map is an isomorphism.*

*Proof.* The map $\mu$ is injective: if $p \neq q$ we must have $p_i \neq q_i$ for some $i$ and $\eta_i - x_i$ is in $\mathfrak{m}_p$ but not in $\mathfrak{m}_q$ so that $\mathfrak{m}_p \neq \mathfrak{m}_q$. So show that $\mu$ is surjective, appeal to a version of the Nullstellensatz proved a couple of classes ago which said that every maximal ideal in the ring $k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for points $(a_1, \ldots, a_n)$. □

## The prime spectrum and irreducible varieties

---

Recall

**Definition 69.** Let $A$ be a (commutative) ring (with 1). Then

$$\mathrm{Spec}(A) := \{\text{prime ideals of} A\}.$$

I claimed in the previous lectures that $\mathrm{Spec}(A)$ is a topological space with a very specific topology, the Zariski topology. Today we are going to spell out the relationship between $\mathrm{Spec}(A)$ and affine varieties (following Reid's undergraduate commutative algebra book).

**Proposition 70.** *Let $A = k[x_1, \ldots, x_n]$. Then*

$$Spec(A) = \{irreducible\ varieties\ X \subset k^n\}.$$

This proposition follows from the fact that a variety $X$ is irreducible if and only if $I(X)$ is prime.

**Proposition 71.** *Let $A = k[x_1, \ldots, x_n]$ be a finitely generated $k$-algebra ($k$ algebraically closed). Let $J$ be the ideal of relations between $x_1, \ldots, x_n$ such that $A = k[x_1, \ldots, x_n]/J$. There is a bijection*

$$Spec(A) \leftrightarrow \{irreducible\ subvarieties\ X = Z(J)\}.$$

*Proof.* Note (from previous lectures) that maximal ideals are in bijection with points of $Z(J)$. Prime ideals of $K[x_1, \ldots, x_n]$ containing $J$ so by the previous proposition every prime ideal $P$ of $A$ is of the form $P = I(X) \mod J$ for an irreducible variety $X \subset k^n$ with $J \subset P = I(X)$. This, by the properties of $Z$, is same as saying

$$Z(P) \subset Z(J)$$

and now $Z(P) = Z(I(X)) = X$. □

So to put everything together again (sec. 5.4 of Reid UCA):
**Definition 72.** A geometric ring $A$ is a finitely generated $k$-algebra which is reduced. This is the same as saying that

$$A = k[x_1, \ldots, x_n]/I$$

where $I = \operatorname{rad} I$. (This is an important definition since it shows you how reduced can be reinterpreted in terms of radical ideals.)

So the *geometric case* is the datum $(Z, A)$ where $\operatorname{Specmax}(A) = Z$ (with Zariski topology) and $A$ is a ring of functions on $\operatorname{Specmax}(A)$

Now for the case that the ring $A$ is arbitrary (i.e. not necessarily geometric). Then:

1. $\mathrm{Spec}(A)$ is a set.

2. (this is extremely important!) for any $P \in \mathrm{Spec}(A)$ define $f(P)$ to be the residue of $f$ modulo $P$:

$$\begin{aligned} f : P \mapsto f(P) &= f \mod P \in A/P \\ &\subset \mathrm{Frac}(A/P) = k(P). \end{aligned}$$

   This is interesting because as we change $P$ around we get different $k(P)$. This is bit like vector fields taking values in different tangent spaces as we change the points around.

3. The Zariski topology on $Z$ (as before) is exactly analogous to the Zariski topology on $\mathrm{Spec}(A)$.

## Regular functions and function fields

I follow Hartshorne. Also recall definition 10 and the subsequent discussion.

**Definition 73.** Let $Y$ be a variety and denote by $\mathcal{O}(Y)$ the ring of all regular functions on $Y$. If $P \in Y$ is a point define the local ring of $P$ on $Y$ denoted as $\mathcal{O}_{P,Y}$ or simply $\mathcal{O}_P$ to be the germ of regular functions on $Y$ near $P$. Put differently, an element of $\mathcal{O}_P$ is a pair $(U, f)$ where $U$ is an open subset of $Y$ containing $P$ and $f$ is a regular function on $U$ with the identification

$$(U, f) \sim (V, g)$$

if $f = g$ on $U \cap V$.

One has to check that $\mathcal{O}_P$ is indeed a local ring– that is, it has a unique maximal ideal. This ideal is $\mathfrak{m}$, the set of germs of regular functions that vanish at $P$. (If $f(P) \neq 0$ then $1/f$ is regular in some neighborhood of $P$.) Note

$$\mathcal{O}_P/\mathfrak{m} \simeq k.$$

**Definition 74.** If $Y$ is a variety, define the function field $K(Y)$ of $Y$ as: every element of $K(Y)$ is an equivalence class of pairs $(U, f)$ where $U$ is a nonempty open subset of $Y$, $f$ is a regular function on $U$ and where $(U, f) \sim (V, g)$ if $f = g$ on $U \cap V$. These elements of $K(Y)$ are called rational functions on $Y$.

**Proposition 75.** *$K(Y)$ is a field.*

*Proof.* $Y$ is irreducible since any two nonempty sets have a nonempty intersection. $K(Y)$ is a ring since we can define addition and multiplication the usual way. Let $(U, f) \in K(Y)$ with $f \neq 0$. Then we can restrict $f$ to the open set $V = U \setminus U \cap Z(f)$ where it never vanishes so $1/f$ is regular and therefore $(V, 1/f)$ is the inverse of $(U, f)$. □

So we have three basic objects associated to a variety $Y$:

1. The ring of regular or global functions $\mathcal{O}(Y)$.

2. The local ring $\mathcal{O}_P$ at a point $P \in Y$.

3. The function field $K(Y)$.

By restricting functions, we have

$$\boxed{\mathcal{O}(Y) \longrightarrow \mathcal{O}_P \longrightarrow K(Y)}$$

These maps are injective.

# Introduction to dimension

I follow Hartshorne.

One final general notion that needs to be discussed and developed before we move on to the specific cases of curves and surfaces is that of *dimension* of an affine variety.

Slogan: Dimension is a Local Notion!

We will develop the local properties first which allows us to give a definition of dimension. The key notion here is going to be local rings and *transcendence degree*.

**Definition 76.** Let $L$ be a field extension of $K$. The transcendence degree of $L$ is the largest cardinality of an algebraically independent subset of $L$ over $K$. $L/K$ is called purely transcendental if there exists a subset $S$ of $L$ which is algebraically independent over $K$ and with $L = K(S)$.

**Example 77.** The field of rational functions in $n$ variable with coefficients in $k$ is purely transcendental over $k$ with transcendence degree $n$. The transcendence basis can be $\{x_1, \ldots, x_n\}$.

**Definition 78.** Let $A$ be a ring. The height of a prime ideal $\mathfrak{p} \subset A$ is the supremum of all integers $n$ such that there exists a chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

of distinct prime ideals.

**Definition 79.** The Krull dimension of a ring $A$ is the supremum of heights of all prime ideals of $A$.

**Proposition 80.** *If $Y$ is an affine algebraic subset then the dimension of $Y$ is equal to the Krull dimension of its affine coordinate ring $A(Y)$.*

*Proof.* If $Y$ affine algebraic in $\mathbb{A}^n$ then the closed irreducible subsets of $Y$ correspond to elements in $\operatorname{Spec}(A)$ for $A = k[x_1, \ldots, x_n]$ containing $I(Y)$. They also correspond to the prime ideals of $A(Y)$. Therefore $\dim Y$ is the length of the longest chain of prime ideals in $A(Y)$, giving us the dimension. □

**Remark 81.** The notion of dimension of an affine algebraic variety $X$ makes sense only when $X$ is irreducible. If $X$ is not irreducible, then write

$$X := X_1 \cup \cdots \cup X_k.$$

Then

$$\dim X = \max \dim X_i$$

for $1 \leq i \leq k$.

Assume the following statements to be true or look up their proofs in any commutative algebra book.

**Theorem 82.** *Let $B$ be an integral domain which is a finitely generated $k$-algebra (for $k$ some field not necessarily algebraically closed). Then*

1. *The dimension of $B$ is equal to the transcendence degree of the quotient field $K(B)$ of $B$ over $k$.*

2. *For any prime ideal $\mathfrak{p}$ in $B$ we have*

$$\textit{height}\ \mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

**Theorem 83** (Krull's Hauptidealsatz)**.** *Let $A$ be a Noetherian ring and let $f \in A$ be an element neither a unit nor a zero divisor. Then every minimal prime ideal $\mathfrak{p}$ containing $f$ has height 1*

Finally also:

**Proposition 84.** *A Noetherian integral domain $A$ is a unique factorization domain iff every prime ideal of height 1 is principal.*

With these (unproven) facts at hand we demonstrate some first properties of dimension of affine varieties.

**Proposition 85.** *The dimension of $\mathbb{A}^n$ is $n$.*

*Proof.* Remember we do need a proof here since we can't always think of $\mathbb{A}^n$ as $\mathbb{C}^n$. From a previous proposition we know that the dimension of the polynomial ring $k[x_1, \ldots, k_n]$ is $n$ ($\mathbb{A}^n$ has coordinate ring $k[x_1, \ldots, x_n]$!) and this can be concluded from (1) of a previous theorem showing that the dimension = transcendence degree □

**Proposition 86.** *A variety $Y$ in $\mathbb{A}^n$ has dimension $n-1$ if and only if it is a zero set $Z(f)$ of a single nonconstant irreducible polynomial in $A = k[x_1, \ldots, x_n]$.*

*Proof.* Let $f$ be irreducible– we know $Z(f)$ is a variety. The ideal associated to this variety is the prime ideal $\mathfrak{p} = (f)$. By the Krull Hauptidealsatz, $\mathfrak{p}$ has height 1 so by the formula ($B$ integral domain finitely generated as a $k$-algebra)

$$\text{height } \mathfrak{p} + \dim B/\mathfrak{p} = \dim B,$$

$Z(f)$ has dimension $n-1$. In the other direction, a variety of dimension $n-1$ correspond to a prime ideal of height 1. Now $A$ is a UFD so $\mathfrak{p}$ is principal necessarily generated by the irreducible polynomial $f$. Hence $Y = Z(f)$. □

# Introduction to projective varieties

## Projective varieties: general facts

---

I follow Hartshorne Chapter 1, section 2. Let $k$ algebraically closed all through.
**Definition 87.** The projective $n$-space, denoted as $\mathbb{P}^n_k$ or simply $\mathbb{P}^n$, is the set of equivalence classes of $n+1$ tuples $(a_0, \ldots, a_n)$ of elements of $k$ not all zero, under the equivalence relation

$$(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$$

for all $\lambda \in k$ nonzero.

This is same as saying that $\mathbb{P}^n$ is the quotient of $\mathbb{A}^{n+1} \setminus (0, \ldots, 0)$ with the equivalence relation that identifies all points on a given line through the origin.

We now want a more "algebraic" definition of a projective space in terms of zeros of a homogeneous polynomial.

## Graded rings and homogeneous polynomials

Write $A = k[x_1, \ldots, x_n]$ be the polynomial ring in $n$ variables.
**Definition 88.** A graded ring is a ring $A$ with a decomposition

$$A = \bigoplus_{d \geq 0} A_d$$

of $A$ into a direct sum of abelian groups ($\mathbb{Z}$-modules!) $A_d$ such that for any $A_d \cdot A_e \subseteq A_{d+e}$.

An element of $A_d$ is called a homogeneous element of degree $d$. Every element of $A_d$ can be written as a finite sum of homogeneous elements.
**Definition 89.** An ideal $\mathfrak{a} \subset S$ is homogeneous if

$$\mathfrak{a} = \bigoplus_{d \geq 0} (\mathfrak{a} \bigcap S_d).$$

**Remark 90.** The ring $A = K[x_1, \ldots, x_n]$ can be made graded in the following way: take $A_d$ to be the set of all linear combinations of monomials of total weight $d$ in $x_0, \ldots, x_n$.

Let $f$ be homogeneous of degree $d$. Then by definition

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n)$$

so whether $f$ is zero or not depends only on the equiv class of $(a_0, \ldots, a_n)$.

**Definition 91.** The zeros of homogeneous polynomials $f$ can be defined as

$$Z(f) = \{P \in \mathbb{P}^n : f(P) = 0\}$$

for $T$ a set of homogeneous elements of $A$. The zero set of $T$ is defined as

$$Z(T) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in T\}.$$

For $\mathfrak{a}$ a homogeneous ideal of $T$,

$$Z(\mathfrak{a}) = Z(T)$$

where $T$ is the set of all homogeneous elements of $\mathfrak{a}$.

All the usual notions as in the case of affine subsets hold true for projective spaces– irreducibility etc. Also note: since $A$ is Noetherian any set of homogeneous elements $T$ has a finite subset $f_1, \ldots, f_r$ such that $Z(T) = Z(f_1, \ldots, f_r)$.

A subset $Y$ of $\mathbb{P}^n$ is an algebraic set if there exists a set $T$ of homogeneous elements of $A$ such that $Y = Z(T)$. With this we have a fundamental definition:
**Definition 92.** A projective (algebraic) variety is an irreducible algebraic subset in $\mathbb{P}^n$. A quasiprojective variety is an open subset of a projective variety.
**Example 93.** The Segre Embedding is defined in the following way– let

$$\begin{array}{rcl} \psi : \mathbb{P}^r \times \mathbb{P}^s & \longrightarrow & \mathbb{P}^N, \\ (a_0, \ldots, a_s) \times (b_0, \ldots, b_s) & \mapsto & (\ldots, a_i b_j, \ldots) \end{array}$$

with $N = rs + r + s$. This map is injective and well defined (HW:check!) Then $\text{image of} \psi$ is a subvariety of $\mathbb{P}^N$.

Why? Because let $\mathfrak{a}$ be the kernel of the homomorphism

$$\begin{array}{rcl} k[\{z_{ij}\}] & \to & k[x_0, \ldots, x_r, y_0, \ldots, y_s], \\ z_{ij} & \mapsto & x_i y_j \end{array}$$

where $z_{ij}$ are the homogeneous coordinates of $\mathbb{P}^N$. Then $\text{image of } \psi = Z(\mathfrak{a})$.

So we have defined $\mathbb{P}_k^n$ to be a set of $(n+1)$-tuples $(x_0, \ldots, x_n) \in k^{n+1}$ modulo the equivalence

$$(x_0, \ldots, x_n) \sim (\alpha x_0, \ldots, \alpha x_n), \alpha \in k^*.$$

The tuple $(x_0, \ldots, x_n)$ is called the set of homogeneous coordinates.

$\mathbb{P}_k^n$ can be covered with $n+1$ subsets $U_0, \ldots, U_n$ where

$$U_i = \{\text{points represented by homogeneous coordinates } (x_0, \ldots, x_n), x_i \neq 0\}$$

Each $U_i$ is naturally isomorphic to $k^n$:

$$\begin{array}{rcl} U_i & \longrightarrow & k^n, \\ (x_0, x_1, \ldots, x_n) & \mapsto & (\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}) \end{array}$$

## The projective Nullstellensatz

**Definition 94.** A closed algebraic set in $\mathbb{P}_k^n$ is a set consisting of all roots of a finite collection of homogeneous polynomials $f_i \in k[x_0, \ldots, x_n] =: A$, $1 \leq i \leq n$.

This is OK since if we have two sets of homogeneous coordinates $(x_0, \ldots, x_n), (\alpha x_0, \ldots, \alpha x_n)$ then

$$f(x_0, \ldots, x_n) = 0 \iff f(\alpha x_0, \ldots, \alpha x_n) = 0.$$

As we have seen a homogeneous ideal is an ideal generated by a finite set of homogeneous polynomials. If $\mathfrak{a}$ is such an ideal then define

$$\boxed{Z(\mathfrak{a}) := \{P \in \mathbb{P}_k^n : \text{ if } x = (x_0, \ldots, x_n) \text{ homogeneous coordinates of } P, f(x) = 0 \text{ for all } f \in A\}}$$

If $\Sigma \subset \mathbb{P}_k^n$ is a closed algebraic set then define

$$\boxed{I(\Sigma) = \{\text{ideal generated by all homogeneous polynomials that vanish identically on } \Sigma\}}$$

**Theorem 95** (The projective Nullstellensatz)**.** *The sets $Z$ and $I$ set up a bijection between the set of closed algebraic subsets of $\mathbb{P}_k^n$ and the set of all homogeneous ideals $\mathfrak{a} \subset k[x_0, \ldots, x_n]$ such that*

$$\mathfrak{a} = rad\ \mathfrak{a}$$

*except for one ideal $\mathfrak{a} = (x_0, \ldots, x_n)$.*

The proof goes as follows: If $\Sigma$ is a closed algebraic subset then $Z(I(\Sigma)) = \Sigma$. Therefore $Z$ and $I$ give a bijection between closed algebraic subsets of $\mathbb{P}_k^n$ and those homogeneous ideals such that $\mathfrak{a} = I(Z(\mathfrak{a}))$.

Claim: these ideals are their own radical. Moreover $\emptyset = Z((x_0, \ldots, x_n))$ and hence $1 \in I(Z((x_0, \ldots, x_n)))$ so $(x_0, \ldots, x_n)$ does not satisfy the above equation. Let $\mathfrak{a}$ be an ideal which is its own radical. Let $Z^*(\mathfrak{a})$ be a closed algebraic set corresponding to $\mathfrak{a}$ in the affine space $\mathbb{A}_k^{n+1}$ with coordinates $x_0, \ldots, x_n$. Then $Z^*(\mathfrak{a})$ is invariant under the substitutions

$$(x_0, \ldots, x_n) \mapsto (\alpha x_0, \ldots, \alpha x_n)$$

for all $\alpha \in k^*$. Therefore either (1) $Z^*(\mathfrak{a})$ is empty or (2) $Z^*(\mathfrak{a})$ equals the origin only, or (3) $Z^*(\mathfrak{a})$ is a union of lines through the origin. Through the affine Nullstellensatz theorem 55 we know $\mathfrak{a} = I(Z^*(\mathfrak{a}))$. For the 1st case, this implies $\mathfrak{a} = k[x_0, \ldots, x_n]$ hence $I(Z(\mathfrak{a}))$– always containing $\mathfrak{a}$– must equal $\mathfrak{a}$ since there is no bigger ideal. For the 2nd case, this implies $\mathfrak{a} = (x_0, \ldots, x_n)$ which has already been excluded. For the 3rd case, if $f$ is a homogeneous polynomial then $f$ vanishes on $Z(\mathfrak{a})$ iff $f$ vanishes on $Z^*(\mathfrak{a})$. Therefore by the affine Nullstellensatz, if $f$ vanishes on $Z(\mathfrak{a})$ then $f \in \mathfrak{a}$, that is

$$I(Z(\mathfrak{a})) \subset \mathfrak{a}.$$

The other inclusion follows straight from the definition. QED.