Algebraic geometry is the study of varieties - zero locus of (finite) set of polynomials in, say, n complex variables.

Hilbert's "Nullstellensatz" provides link between algebra / geometry: Write $\underline{x} = (x_1, \dots, x_n)$ and $\mathbb{C}[\underline{x}]$ for polynomial ring in n variables.

$$\left\{ \begin{array}{c} \text{maximal ideals} \\ \text{in } \mathbb{C}[\underline{x}] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{pts in} \\ \mathbb{C}^n \end{array} \right\}$$

I: ideal in ring R means all linear combs $r_1 a_1 + \cdots + r_k a_k \in I$ (and $I \neq \phi$), maximal if not contained in larger ideal that is not whole ring.

Ex. Maximal ideals of $\mathbb{C}[x]$ are principal ideals generated by $(x-a)$ $a \in \mathbb{C}$.

$$\phi_a : \mathbb{C}[x] \longrightarrow \mathbb{C} \qquad \text{then } \ker(\phi_a) = \langle x-a \rangle$$
$$f(x) \longmapsto f(a)$$

pf: $\mathbb{C}[x]$ is a principal ideal domain, by Euclidean algorithm for polynomials.

But if our maximal ideal $M = \langle f \rangle$ then f has a root in $\mathbb{C}$, say a, $\Rightarrow$ $(x-a) \mid f \Rightarrow M \subseteq \langle x-a \rangle$

Since M maximal must have $M = \langle x-a \rangle$.

OR notice that since $\mathbb{C}[x] / \ker(\phi_a) \simeq \mathbb{C}$, a field

and $\ker(\phi_a) = \langle x-a \rangle$ by definition, then $\langle x-a \rangle$ maximal

(being in $\ker(\phi_a)$ means that a is a root $\Leftrightarrow$ f is divisible by $x-a$)

(general principal that R/M field $\Leftrightarrow$ M maximal)

Returning to nullstellensatz: claim that

$\phi_{\underline{a}} : \mathbb{C}[\underline{x}] \longrightarrow \mathbb{C}$ whose kernel $M_{\underline{a}}$ is generated by

$f(\underline{x}) \longmapsto f(\underline{a})$ $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ if $\underline{a} = (a_1, \ldots, a_n)$

By similar reasoning to the above,

$\ker(\phi_a) =: M_{\underline{a}}$ is maximal since $\phi_{\underline{a}}$ is surjective and $\mathbb{C}$ field.

Why is $M_{\underline{a}}$ generated by the above linear polynomials? Given arbitrary $f \in \mathbb{C}[\underline{x}]$,

Write $f(\underline{x}) = f(\underline{a}) + \sum_i c_i (x_i - a_i) + \sum_{i,j} c_{i,j} (x_i - a_i)(x_j - a_j) + \cdots$

(just multi-variate Taylor expansion)

e.g. $c_i = \partial f / \partial x_i (\underline{a})$, etc.

but could also justify this algebraically

All terms on RHS are divisible by $(x_i - a_i)$ for some i (except $f(\underline{a})$)

So if f vanishes at $\underline{a}$, then

$f(\underline{x})$ is in ideal gen'd by $(x_i - a_i)$ for $i = 1, \ldots, n$.

so $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal ideal. Why is any maximal ideal in $\mathbb{C}[\underline{x}]$ of the form $M_{\underline{a}}$ for some $\underline{a}$?

Need series of lemmas here:

Consider M = maximal ideal π : projection map $\mathbb{C}[\underline{x}] \longrightarrow \mathbb{C}[\underline{x}]/M$ (a field) K, say.

We can restrict the domain to $\mathbb{C}[x_1]$. Call result π_1.

Lemma 1: $\ker(\pi_1) = 0$ or maximal ideal.

pf: if $\neq 0$, then consider $f \in \ker(\pi_1)$. K field so $\ker(\pi_1) \neq \mathbb{C}[x_1]$

so f non-const. $\Rightarrow$ $f = (x_1 - a_1) g$ with $\pi_1(f) = \pi_1(x_1 - a_1)\pi_1(g)$

~~[illegible]~~ K field, so an integral domain $\Rightarrow$ either $x_1 - a_1 \in \ker(\pi_1)$

which would imply $\langle x_1 - a_1 \rangle = \ker(\pi_1)$, or else g (with degree $< \deg(f)$) in $\ker(\pi_1)$. If latter occurs, ...

... Then keep going until arrive at linear polynomial in $\ker(\pi_1)$ //

Almost there. Nothing special about x_1 in above lemma, so have $x_i - a_i \in \ker(\pi_i)$ for some $a_i \in \mathbb{C}$ for each $i = 1, \dots, n$. (i.e. $x_i - a_i \in M$) and hence $M = \langle x_1 - a_1, \dots, x_n - a_n \rangle$

AS LONG AS $\ker(\pi_1) \neq 0$,

so we need to rule this case out.

If $\ker(\pi_1) = 0$ then $\mathbb{C}[x_1] \hookrightarrow K$: field

Any such injection can be extended to map on fraction field of integral domain into field $\mathbb{C}(x_1) : \{ f/g \mid g \neq 0 \}$

or really equivalence class, since f, g could have common factors

Just map $f/g \longmapsto \pi_1(f)\,\pi_1(g)^{-1}$.

thus $\mathbb{C}(x_1)$ is a subfield of K.

show this gives contradiction as follows:

$\mathbb{C}[\underline{x}]$ has countable basis (monomials in $x_1, \dots, x_n$) as vector space $/ \mathbb{C}$.

$\Rightarrow$ K has countable basis over $\mathbb{C}$ (take images of monomials mod M)

Show $\mathbb{C}(x)$ has uncountably many linearly independent elements.

Lemma: $\left\{ \frac{1}{x-a} \;\middle|\; a \in \mathbb{C} \right\}$ are linearly independent.

pf: Suppose ~~[illegible]~~ we take a non-trivial ~~[illegible]~~ linear combination $\sum_{i=1}^{n} \frac{c_i}{x - a_i}$. Suppose w.l.o.g. $c_1 \neq 0$

This is not zero function since it has pole at a_1 not canceled by others.

Final lemma: if V: vector space with countable basis $\{e_1, e_2, \ldots\}$

then every linearly independent set of vectors is at most countably

infinite.

pf: If L: linearly indep. subset of V, $V_n = \langle e_1, \ldots, e_n \rangle$

Let $L_n = L \cap V_n$. This is linearly indep., $\subseteq V_n$, hence finite.

But $L = \bigcup_n L_n$ so at most countably infinite. //

Explore consequences of nullstellensatz:

V: variety defined as zero locus of $f_1(\underline{x}), \ldots, f_r(\underline{x})$

I: ideal generated by $\langle f_1, \ldots, f_r \rangle$. Then there exists a bijection

$$\left\{ \begin{matrix} \text{max. ideals} \\ \text{of } \mathbb{C}[\underline{x}]/I \end{matrix} \right\} \xleftrightarrow[\text{bij.}]{} \left\{ \begin{matrix} \text{pts of} \\ V \end{matrix} \right\}$$

pf: maximal ideals of $\mathbb{C}[\underline{x}]/I \longleftrightarrow$ maximal ideals of $\mathbb{C}[\underline{x}]$ containing I (image under projection to I)

An ideal contains $I \iff$ it contains $f_1, \ldots, f_r$.

and maximal ideals (by Nullstellensatz) are $\ker(\phi_{\underline{a}})$ for $\underline{a} \in \mathbb{C}^n$.

So just need to determine condition for $f_i \in M_{\underline{a}}$. ($\iff f_i(\underline{a}) = 0$ i.e. $\iff \underline{a} \in V$)

Classical form of Nullstellensatz: V = variety of zeros of $f_1, \ldots, f_r$

I: ideal $\langle f_1, \ldots, f_r \rangle$. If $g \equiv 0$ on V then

$g^r \in I$ for some r.