variety := a set of points in $\mathbb{A}^d$ that contains exactly all the solutions to some system of equations

= Z(some (possibly infinite) set of polynomials)

(possibly infinite) system of equations in finitely many (d) variables given by polynomials $\xmapsto{\ Z\ }$ solution set of our system $\subseteq \mathbb{A}^d$

the system of $\underline{\underline{\text{all}}}$ the polynomials that vanish at the given points $\xleftarrow{\ I\ }$ subsets of $\mathbb{A}^d$

$k[x_1, \dots, x_d]$ $\qquad\qquad$ $\mathbb{A}^d_k$

$$T \subseteq k[x_1, \dots, x_d] \xmapsto{\ Z\ } Z(T) = \{\underline{a} \in \mathbb{A}^d : f(\underline{a}) = 0 \ \forall f \in T\}$$

$$\{f \in k[x_1, \dots, x_d] : f(x) = 0 \quad \forall x \in X\} \xleftarrow{\ I\ } X \subseteq \mathbb{A}^d$$

$$T \subseteq k[x_1, \dots, x_d] \xmapsto{\ Z\ } Z(T) \subseteq \mathbb{A}^d \text{ variety}$$

$I(Z(T))$

possibly more polynomials

Properties 1) $Z(0) = \mathbb{A}_k^d$

2) $Z(1) = \emptyset$

3) $I(\emptyset) = (1) = k[x_1, \dots, x_d]$

4) $I \subseteq J \subseteq k[x_1, \dots, x_d] \Rightarrow Z(I) \supseteq Z(J)$

5) $S \subseteq T \subseteq \mathbb{A}_k^d \Rightarrow I(S) \supseteq I(T)$

6) $I = (T) \Rightarrow Z(T) = Z(I)$

Hilbert's Basis theorem $\Rightarrow$ any system of equations in $k[x_1, \dots, x_d]$ can be replaced by finitely many equations

Ex: $I(\{(a_1, \dots, a_d)\}) = (x_1 - a_1, \dots, x_d - a_d)$

Ex $X = \begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}$ generic matrix

$R = k[X] =: k\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}$ (k field)

$\Delta_1 = \det\begin{pmatrix} x_2 & x_3 \\ y_2 & y_3 \end{pmatrix}$ $\Delta_2 = \det\begin{pmatrix} x_1 & x_3 \\ y_1 & y_3 \end{pmatrix}$ $\Delta_3 = \det\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$

$I := (\Delta_1, \Delta_2, \Delta_3) \subseteq (x_1, x_2, x_3) =: J$

$\mathbb{A}_k^6 \equiv 2 \times 3$ matrices

$Z(I)$ = matrices of rank ≤ 1

$Z(J)$ = matrices with top row 0

$Z(J) \subseteq Z(I) \Rightarrow$ matrices with a 0 row have rank ≤ 1

Prime ideals $\quad P$ is prime if $\quad fg \in P \Rightarrow f \in P$ or $g \in P$

$$\Updownarrow$$

R/P is a domain

Ex: primes in $\mathbb{Z}$: (p), p prime
(0) ($\mathbb{Z}$ is a domain!)

Ex: primes in $k[x]$ = (f) $\quad f$ irreducible
(0) ($k[x]$ is a domain)

Ex: $P = (x^3 - y^2) \subseteq R = k[x, y]$ is prime, since

$$k[x, y] \xrightarrow{f} k[t^2, t^3] \subseteq k[t] \text{ (domain)}$$

$$\ker f = P \implies k[x, y]/P \text{ is a domain}$$

Will see: prime ideals $\Leftrightarrow$ irreducible varieties
X irreducible $\Leftrightarrow$ $I(X)$ prime

Maximal ideal $\quad m$ is maximal if

$$m \subseteq I \implies m = I \text{ or } I = R$$

$$\Updownarrow$$

R/m is a field

Residue field of $m := R/m$

Note A ring might have many residue fields.

For example, the residue fields of $\mathbb{Z}$ are $\mathbb{F}_p$ for all p prime

Exercise maximal $\Rightarrow$ prime

But prime $\not\Rightarrow$ maximal

Example (0) is prime but not maximal in $\mathbb{Z}$

Theorem Every ideal in R is contained in some maximal ideal

Proof Notes

Back to geometry:

Lemma k field

$R = k[x_1, \dots, x_d]$

$$\mathbb{A}^d_k \xleftrightarrow{\text{bijection}} \left\{ \begin{array}{c} \text{maximal ideals in } R \\ \text{with } R/m \cong k \end{array} \right\}$$

$$(a_1, \dots, a_d) \longmapsto (x_1 - a_1, \dots, x_d - a_d)$$

Proof Note that for each choice of $(a_1, \dots, a_d) \in \mathbb{A}^d_k$ $\dfrac{k[x_1, \dots, x_d]}{(x_1 - a_1, \dots, x_d - a_d)} \cong k$ ✓

Injective: these ideals are all distinct, since $x_i - a_i,\ x_i - b_i \in m$

$$\Rightarrow (x_i - a_i) - (x_i - b_i) = \underbrace{b_i - a_i}_{\in k, \neq 0} \in m \Rightarrow m = R$$

Surjective: $R/m \cong k \Rightarrow$ each class in R/m corresponds to a unique $a \in k$

so for each i, $x_i \equiv a_i \pmod{m}$ for some $a_i \in k$

$\Rightarrow x_i - a_i \in m$ for all $i \Rightarrow \underbrace{(x_1-a_1, \dots, x_d-a_d)}_{\text{maximal}} \subseteq m$

$$\Rightarrow (x_1-a_1, \dots, x_d-a_d) = m$$

<u>Example/Warning</u> Not all maximal ideals in $k[x_1, \dots, x_d]$ are of this form. Eg, when $k=\mathbb{R}$, $d=1$

In $\mathbb{R}[x]$, (x^2+1) is a maximal ideal

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C} \not\cong \mathbb{R}$$

But this bad behavior won't happen if $k = \overline{k}$

<u>Zariski's lemma</u> $k \subseteq L$ extension of fields

- If L is a fg k-algebra, then L is a finite dimensional k-vector space. (algebra finite $\Rightarrow$ module finite)

- As a consequence, if $k=\overline{k}$ and $k \subseteq L$ alg-fin, then $L = k$

(why? Alg-fin $\Rightarrow$ mod-fin $\Rightarrow$ integral $\Rightarrow$ algebraic)

So if $\mathfrak{m} \subseteq k[x_1, \dots, x_d]$ is a maximal ideal,

$k \subseteq k[x_1, \dots, x_d]/\mathfrak{m} \cong$ field is algebra finite

$\implies k[x_1, \dots, x_d]/\mathfrak{m} \cong k$

From now on: $k = \overline{k}$

<u>Nullstellensatz</u> $S = k[x_1, \dots, x_d]$, $k = \overline{k}$

① There is a bijection

$$\mathbb{A}^d_k \longleftrightarrow \{\text{maximal ideals of } S\}$$
$$(a_1, \dots, a_d) \longmapsto (x_1 - a_1, \dots, x_d - a_d)$$

② If R is a finitely generated R-algebra $\implies$ there is an induced bijection

$R = S/I$
$S = k[x_1, \dots, x_d]$

$$Z_k(I) \subseteq \mathbb{A}^d_k \longleftrightarrow \{\text{maximal ideals in } R\}$$

<u>Proof</u> ① $\{\text{maximal ideals with } R/\mathfrak{m} \cong k\} = \{\text{maximal ideals}\}$

② $\{\text{max ideals of } R\}$

$\updownarrow$

$\{\text{max ideals of } S, \supseteq I\} \longleftrightarrow \{a \in \mathbb{A}^d,\ a \in Z_k(I)\}$

$$I \subseteq (x_1 - a_1, \dots, x_d - a_d) \longmapsto Z(I) \supseteq \{a\}$$

Thm (Weak Nullstellensatz) $k = \overline{k}$

$I \subseteq k[x_1, \dots, x_d]$ proper ideal $\Rightarrow$ $Z(I) \neq \emptyset$

Proof $I \subseteq m$ maximal $\Rightarrow$ $\underbrace{Z(m)}_{\text{point!}} \subseteq Z(I)$

I ideal $\xmapsto{Z}$ $Z(I)$ variety $\xmapsto{I}$ $\mathcal{I}(Z(I))$

how does this relate to I?

Ex: $R = k[x]$, $I_n = (x^n)$ $n \geq 1$

$Z(I_n) = \{0\}$ for all n

What do all these different ideals have in common?

Remark $f \in k[x_1, \dots, x_d]$, $\underline{a} \in \mathbb{A}^d$

$f(\underline{a}) \neq 0 \Leftrightarrow f(\underline{a})$ invertible

$\Leftrightarrow$ $b f(\underline{a}) - 1 = 0$ for some b

$\Leftrightarrow$ $y f(\underline{a}) - 1 = 0$ has a solution

So:

$$\left\{\begin{array}{l} f_1 = 0 \\ \vdots \\ f_m = 0 \end{array}\right. \text{ and } \left\{\begin{array}{l} g_1 \neq 0 \\ \vdots \\ g_n \neq 0 \end{array}\right. \text{ has a solution}$$

$$\Leftrightarrow \left\{\begin{array}{l} f_1 = 0 \\ \vdots \\ f_m = 0 \end{array}\right. \text{ and } \left\{\begin{array}{l} y g_1 - 1 = 0 \\ \vdots \\ y g_n - 1 = 0 \end{array}\right. \text{ has a solution}$$

$$\Longleftrightarrow \quad \left\{\begin{array}{l} f_1 = 0 \\ \vdots \\ f_m = 0 \\ y g_1 \cdots g_n - 1 = 0 \end{array}\right. \quad \text{has a solution}$$

thm (Strong Nullstellensatz) $k = \overline{k}$

$R = k[x_1, \dots, x_d]$

$$f \in I(Z(I)) \iff f^n \in I \text{ for some } n$$

Proof

$(\Leftarrow)$ $f^n \in I \Rightarrow f^n(a) = 0$ for all $a \in Z(I)$

$\Downarrow$ k field

$f(a) = 0$ for all $a \in Z(I)$

$\Downarrow$

$f \in I(Z(I))$

$(\Rightarrow)$ $f \in I(Z(I))$

so polynomials in $I = 0 \Longrightarrow f = 0$

thus $\left\{\begin{array}{l} \text{polynomials in } I = 0 \\ f \neq 0 \end{array}\right.$ has no solutions

$$\Rightarrow \quad \mathcal{Z}\left(I + (yf-1)\right) = \emptyset \quad \text{in} \quad R[y]$$

$$\xrightarrow[\text{Nullstellensatz}]{\text{weak}} \quad I + (yf-1) = R[y]$$

$$\Leftrightarrow \quad 1 \in I + (yf-1)$$

If $I = (g_1, \dots, g_m)$,

$$1 = r_0 \cdot (1 - yf) + r_1 g_1 + \dots + r_m g_m$$

$$\Big\downarrow \; y \mapsto \frac{1}{f} \quad \text{in } \operatorname{frac}(R[y])$$

$$1 = r_1\left(\underline{x}, \frac{1}{f}\right) \cdot g_1(x) + \dots + r_m\left(\underline{x}, \frac{1}{f}\right) g_m(x)$$

take the largest negative power of f appearing $\Rightarrow$ clear denominators

$$f^n = \underbrace{s_1}_{\text{only on } \underline{x}} g_1 + \dots + s_m g_m$$

$\searrow$ equation in R

$$\Rightarrow f^m \in I$$