Lecture 32:

I ideal in $k[x_1, \ldots, x_n]$, gives an algebraic variety:

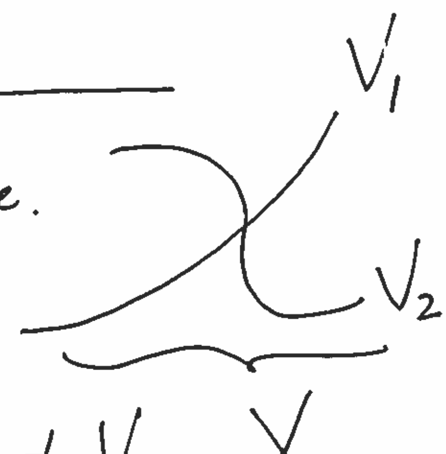
$\mathbb{V}(I) = \{a \in k^n \mid f(a) = 0 \text{ for all } f \in I\}$

$\mathbb{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in V\}$

$$\mathbb{V}(\mathbb{I}(V)) = V \quad \text{and} \quad \mathbb{I}(\mathbb{V}(I)) \supseteq \text{rad}(I)$$

equality when k is alg. closed

Def: A variety V is irreducible if whenever $V = V_1 \cup V_2$ for varieties V_i then $V = V_1$ or $V = V_2$.



Thm: V is irreducible $\iff$ $\mathbb{I}(V)$ is prime.

Pf: ($\Rightarrow$) Last time.

($\Leftarrow$) Suppose $V = V_1 \cup V_2$. Assume $V_1 \neq V$.

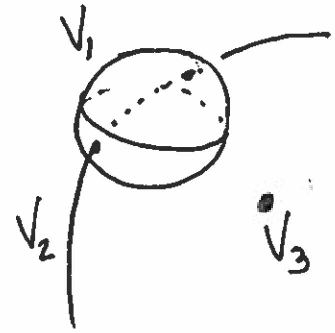
As $V_1 \subsetneq V$, have $\mathbb{I}(V_1) \supsetneq \mathbb{I}(V)$. [To see can't have equality, apply $\mathbb{V}$ and use $\mathbb{V}(\mathbb{I}(W)) = W$.]

Pick $f_1 \in \mathbb{I}(V_1) \setminus \mathbb{I}(V)$. Suppose $f_2 \in \mathbb{I}(V_2)$

Then $f_1 \cdot f_2 = 0$ on $V \Rightarrow f_1 \cdot f_2 \in \mathbb{I}(V)$.

As $\mathbb{I}(V)$ is prime, must have one $f_i \in \mathbb{I}(V)$, which must be f_2. Hence $\mathbb{I}(V_2) \subseteq \mathbb{I}(V)$ and so $V_2 \supseteq V \Rightarrow V = V_2$. So V is irreducible. $\blacksquare$

<u>Thm</u>: An algebraic variety $V \subseteq K^n$ is a finite union of irreducible varieties.



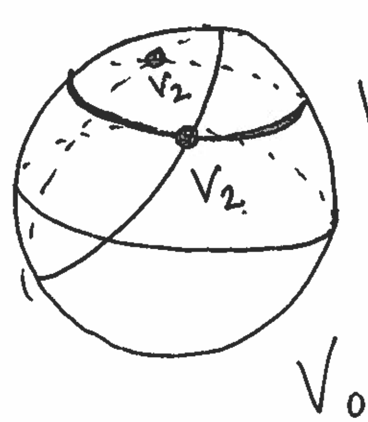
<u>Suppose not</u>: $V = V_1 \cup W_1$ with $V_1, W_1 \subsetneq V$. One of V_1, W_1 must be reducible, say $V_1 = V_2 \cup W_2$ with $V_2, W_2 \subsetneq V_1$.

Continuing, we construct infinitely many nested varieties:

$$V_0 \supsetneq V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \ldots\ldots$$

Doesn't mesh with our experience:

$\mathbb{R}^3$



$V_1 = V_0 \cap \{z = 1/2\}$

In $k[x_1, \ldots, x_n]$, consider $I_k = \mathbb{I}(V_k)$ and observe:

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

Could this actually happen? No!

<u>Def</u>: A ring R is <u>Noetherian</u> if every sequence of ideals

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq \cdots$$

eventually stabilizes, i.e. $\exists n$ with $I_k = I_n$ for all $k \geq n$.

<u>Hilbert's Basis Theorem</u>: If k is a field, then $k[x_1, x_2, \ldots, x_n]$ is Noetherian. [DF, §9.6]

[See one of the references for a proof.]

<u>Nullstellensatz</u>: If k is algebraically closed, then $\mathbb{I}(\mathbb{V}(I)) = \mathrm{rad}(I)$ for all ideals $I \subseteq k[x_1, \ldots, x_n]$. Thus

$$\left\{ \begin{array}{c} \text{Alg. var} \\ \text{in } k^n \end{array} \right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{ \begin{array}{c} \text{radical} \\ \text{ideals} \\ I \subseteq k[x_1, \ldots, x_n] \end{array} \right\}$$

are inverse bijections.

[Toward a proof of the Nullstellensatz...]

k field [not nec. alg. closed] $R = K[x_1, \dots, x_n]$

Given $a \in K^n$, consider $R \longrightarrow K$ sending $f \longmapsto f(a)$.

The kernel of this ring homom is

$$I(a) = (x_1 - a_1, \dots, x_n - a_n)$$

coor of a.

As $R/I(a) \cong k$, have each $I(a)$ is maximal. Note also that $I(a) = \mathbb{I}(\{a\})$

<u>Lemma</u>: If k is alg. closed, then the maximal ideals of $k[x_1, \dots, x_n]$ are exactly the $I(a)$.

<u>Note</u>: False for other fields, i.e. $(x^2+1) \subseteq \mathbb{R}[x]$ is maximal but not $(x-a)$ for some $a \in \mathbb{R}$.

Lemma is called the "Weak Nullstellensatz" since it gives a bijection

$$\left\{\begin{matrix}\text{points in}\\ k^n\end{matrix}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{matrix}\text{maximal ideals}\\ I \subseteq R\end{matrix}\right\}$$

Note a max. ideal is radical.

The full Nullstellensatz follows from the weak form and Hilbert's Basis Thm [DF, pg 700].

Proof of Lemma: Assume $K = \mathbb{C}$. Suppose $I \subseteq \mathbb{C}[x_1, \ldots, x_n] = R$ is maximal, and set $F = R/_I$. Note $F \supseteq \mathbb{C}$ as a subfield, and as $\mathbb{C}$ is algebraically closed, either

$F = \mathbb{C}$: Set a_i = image of x_i in F. Then $I = I(a)$.

$F/_\mathbb{C}$ is trancendental: In particular, $F \supseteq \mathbb{C}(t)$.

Note $\dim_\mathbb{C} \mathbb{C}(t)$ is uncountable since $\left\{ \frac{1}{t-a} \mid a \in \mathbb{C} \right\}$ is linearly independent over $\mathbb{C}$.

But R and hence $F = R/_I$ have countable bases over $\mathbb{C}$, a contradiction. Q.E.D.

If any finite subset is linearly dependent, have $a_i \in \mathbb{C}$, $c_i \neq 0$ in $\mathbb{C}$ with $\sum_{i=1}^{n} \frac{c_i}{t-a_i} = 0$. This is impossible as the RHS $\to \infty$ as $t \to a_1$