Hilbert's N'satz

$$\{\text{aav's in } \mathbb{A}^n\} \longleftrightarrow \left\{\begin{array}{c}\text{rad ideals}\\ k[x_1,\dots,x_n]\end{array}\right\}$$

$$V \longmapsto \mathbb{I}(V)$$

$$Z(V) \longleftarrow\!\shortmid\; I$$

Nontrivial part: Z inj on rad ideals

Weak N'satz Max ideals in $k[x_1,\dots,x_n]$ are of form

$$(x_1-a_1,\dots,x_n-a_n)$$

Lemma. Assume ~~k alg closed~~ and uncountably infinite.

If $L \supseteq k$ field ext and L fin. gen. as k-algebra

Then L is algebraic over k.

$\exists\, u_1,\dots,u_r \in L$ so that each elt of L is a polynomial in u_i with coeffs in k.

each $u \in L$ is a root of poly in k:

$$k_n u^n + \dots + k_1 u + k_0 = 0.$$

Example $\mathbb{C}(x)$ not alg over $\mathbb{C}$, not fg alg

Lemma. Assume ~~k alg closed~~ and uncountably infinite.

If $L \supseteq k$ field ext and L fin. gen. as k-algebra

Then L is algebraic over k.

Pf. Suppose $u \in L$ not algebraic.

① The set $\left\{\frac{1}{u-c} : c \in k\right\}$ uncountable & lin ind. over k.

Indeed, any lin. combo $\frac{b_1}{u-c_1} + \cdots + \frac{b_q}{u-c_q}$ $b_i, c_i \in k$

gives u as a root of a poly (clear fractions)

② Let $u_1, \ldots, u_r$ gens for L as k-alg.

$\rightsquigarrow \{u_1^{m_1} u_2^{m_2} \cdots u_r^{m_r}\}$ countable and is a k-basis for L.

This contradicts ①.

Lemma is true over arbitrary fields. Need

① Zariski's Lemma: L fin gen as k-alg $\Leftrightarrow$ L fin gen as k-module

② Noether normalization

~~Thm~~ Lemma. k = field, K extension
If K is fin gen as a k-alg
then K is algebraic over k.

Pf of WN. Say m = max ideal in
$R = k[x_1, \dots, x_n]$

$\Longrightarrow$ R/m is a field, fin gen as k-alg.
(since R is).

Have $k \cap m = \{0\}$. (else $m = R$)

$\longrightarrow$ image $\bar{k}$ of k in R/m is $\cong k$.

~~Thm~~ Lemma $\longrightarrow$ R/m alg. ext. of $\bar{k}$.

k alg closed $\Longrightarrow$ $R/m = \bar{k}$

Under $R \to R/m$
each $x_i \longmapsto \bar{a}_i \in \bar{k}$

Some $\bar{a}_i$ image of $a_i \in k$.

$\Longrightarrow m \supseteq (x_1 - a_1, \dots, x_n - a_n)$
$= m'$

But m' maximal

$\Longrightarrow m = m'$

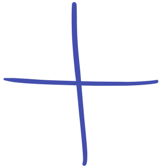
$\square$

Irreducibility

Basic example

① $Z(xy) \subseteq \mathbb{A}^2$

$$\begin{gathered} Z(xy) \\ \parallel \\ Z(x) \cup Z(y) \end{gathered}$$



Say $Z(xy)$ reducible.

An nonempty aav is <u>reducible</u> if it is the union of two distinct, nonempty aav's.

The maximal* irred ~~closed subsets~~ sub aav's are the irr<u>educible</u> comp<u>onents</u>.

* wrt inclusion

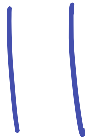
More examples

② $Z(x_1x_2, x_1x_3) \subseteq \mathbb{A}^3$

$$\begin{gathered} Z(x_1x_2, x_1x_3) \\ \parallel \\ Z(x_1) \cup Z(x_2, x_3) \end{gathered}$$

③ $Z(x^2-1) \subseteq \mathbb{A}^1$

$$\begin{gathered} Z(x^2-1) \\ \parallel \\ Z(x+1) \cup Z(x-1) \end{gathered}$$



not connected

④ A finite set in $\mathbb{A}^n$ is irred $\Longleftrightarrow$ ~~at most~~ one point

⑤ What about $\mathbb{A}^n$?

Prop. $X \subseteq \mathbb{A}^n$ aav.

X irred $\iff \mathbb{I}(X)$ prime.

Pf. $(\Leftarrow)$ Say $\mathbb{I}(X)$ prime.

and $X = X_1 \cup X_2$

Then $\mathbb{I}(X) = \mathbb{I}(X_1) \cap \mathbb{I}(X_2)$

$\mathbb{I}(X)$ prime $\Rightarrow \mathbb{I}(X) = \mathbb{I}(X_1)$ WLOG ~~or $\mathbb{I}(X_2)$~~

(If $P = I \cap J$ then
$IJ \subseteq I \cap J = P \Rightarrow P = I$ or J).

(Prime $\Rightarrow$ radical) so SN $\Rightarrow$

$X = X_1$

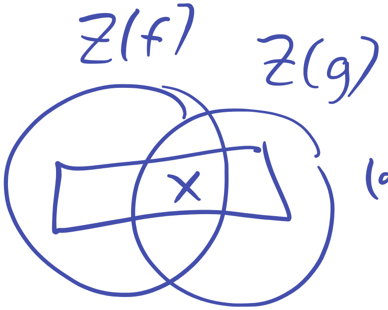
$(\Rightarrow)$ Say X irred & $fg \in \mathbb{I}(X)$

Then $X \subseteq Z(fg) = Z(f) \cup Z(g)$

$\Rightarrow X = (Z(f) \cap X) \cup (Z(g) \cap X)$

$\xRightarrow{\text{irred.}} X = Z(f) \cap X$

$\Rightarrow X \subseteq Z(f) \Rightarrow f \in \mathbb{I}(X)$. $\square$



(a priori)

Consequences

① $\mathbb{A}^n$ irred since (0) prime

② $f \in k[x_1,\dots,x_n]$ irred

$\iff Z(f)$ irred.

[If $f = f_1 f_2$

$Z(f) = Z(f_1) \cup Z(f_2)$]

Dictionary

aav's	$\longleftrightarrow$	rad ideals
irred aav's	$\longleftrightarrow$	prime ideals
pts (in $\mathbb{A}^n$)	$\longleftrightarrow$	max ideals (in $k[x_1,\dots,x_n]$)

Decomposing into irreducibles

$k[x_1,\dots,x_n]$ Noetherian (Hilb. basis thm)

$\Rightarrow$ any desc. chain of aav's is... eventually stationary.

(Noetherian property for aav's)

Prop ① An aav can be written as a finite union of irred aav's

$X_1 \cup \dots \cup X_r$

② If $X_i \not\subset X_j$ $\forall i \neq j$ the X_i unique.

In this case, X_i called the irred components of X.

Prop ① An aav can be written as a finite union of irred aav's

$$X_1 \cup \cdots \cup X_r$$

② If $X_i \not\subset X_j$ $\forall\, i \neq j$ the X_i unique.

In this case, X_i called the <u>irred</u> components of X.

Pf of ① Let X be a minimal counterexample. under inclusion If there is a counterex, a minimal one exists by Noetherian property.

Since it's a counterex, it's reducible:

$$X = X_1 \cup X_2$$

But X minimal $\Longrightarrow$ X_1, X_2 finite unions of irred's.

② Say

$$X = X_1 \cup \cdots \cup X_r$$
$$= X_1' \cup \cdots \cup X_s'$$

$X_1 \subset \bigcup X_i'$

In fact $X_1 \subset X_i'$ some i (otherwise X_1 reduces).

Next week: end of Chap 1

- Morphisms = polynomial maps

- Coordinate ring $k[V]$

  $= \{\text{poly fns on } V\}$

  $= k[x_1, \dots, x_n] / \mathbb{I}(V)$