Introduction is done ✓

Today: Language of algebraic varieties.

Variety $\approx$ "Algebraic space"

Defined via polynomials.

Recall: Given ring R we have ring of formal polynomials:

$R[x]$ = expressions of form
$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$

where $n \geq 0$, $a_0, \ldots, a_1 \in R$.

Ring operations: Pretend that x is an element of R, even though it is not!

By induction, define

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$$

[Fancy: Polynomials are "free R-algebras."]

Formal polynomials vs. polynomial functions. Let $\mathbb{F}$ be an infinite field (usually $\mathbb{F} = \mathbb{C}$, maybe $\mathbb{R}$ or $\mathbb{Q}$)

Prop: Given $f, g \in \mathbb{F}[x_1, \dots, x_n]$ we have

$$\underbrace{f \equiv g}_{\substack{\text{as formal} \\ \text{expressions} \\ \text{i.e., same} \\ \text{coefficients}}} \iff \begin{array}{l} f(a_1, \dots, a_n) = g(a_1, \dots, a_n) \\ \text{for all points} \\ (a_1, \dots, a_n) \in \mathbb{F}^n \end{array}$$

Proof: We will show

$$f \equiv 0 \iff f(a_1, \dots, a_n) = 0 \ \forall a_1, \dots, a_n.$$

Then apply this to $f - g$.

Proof by induction.

$n = 1$: $f(x_1) \in \mathbb{F}[x_1]$. If $f \equiv 0$, done.

So assume $f \not\equiv 0$, say $\deg(f) = d \geq 0$.

Then f has $\leq d$ distinct roots in $\mathbb{F}$.

(Goes back to Descartes, 1637).

$n \geq 2$: Let $f(a_1, \dots, a_n) = 0 \ \forall\, a_1, \dots, a_n$.

Assume for contradiction $f \not\equiv 0$. Exand in terms of x_n:

$$f(\bar{x}) = \sum_k f_k(\bar{x}')\, x_n^k$$

where $\bar{x} = (x_1, \dots, x_n)$
$\bar{x}' = (x_1, \dots, x_{n-1})$.

Since $f \not\equiv 0$, have $f_k(\bar{x}') \not\equiv 0$ for some k. By induction, $\exists$ point $\bar{a}' = (a_1, \dots, a_{n-1})$ such that

$$f_k(\bar{a}') \neq 0.$$

But then

$$f(\bar{a}', x_n) = \sum_k f_k(\bar{a}')\, x_n^k \in \mathbb{F}[x_n]$$

has a nonzero coefficient, hence it must have a root $x_n = a_n$. We get the contradiction

$$f(\bar{a}) = f(\bar{a}', a_n) = 0. \qquad ///$$

$\mathbb{F}$ field $\Rightarrow$ $\mathbb{F}[x]$ has division with remainder.

$\Rightarrow$ $\mathbb{F}[x]$ is a PID.

$\Rightarrow$ $\mathbb{F}[x]$ is a UFD.

Gauss' Lemma: If R is a UFD then $R[x]$ is a UFD.

Corollary: $\mathbb{F}[x_1, \dots, x_n]$ is a UFD.

Proof: Last semester's notes. ///

Say ring R is "Noetherian" if every ideal is finitely generated:

Given ideal $I \leq R$, $\exists$ elements $f_1, \dots, f_m \in R$ such that

$$I = (f_1, \dots, f_m)$$
$$= R\text{-linear combinations}$$
$$= \{f_1 \tilde{f}_1 + \dots + f_m \tilde{f}_m : \tilde{f}_1, \dots, \tilde{f}_m \in R\}$$

Hilbert Basis Theorem:

R Noetherian $\Rightarrow$ $R[x]$ Noetherian

Corollary: $\mathbb{F}[x_1, \dots, x_n]$ Noetherian.

Proof: Last semester's notes. ///

On this foundation we try to build a theory of geometry.

Given $f \in \mathbb{F}[x_1, \dots, x_n]$ we define a "hypersurface" in affine n-space:

$$V(f) = \{(a_1, \dots, a_n) : f(a_1, \dots, a_n) = 0\}$$
$$\subseteq \mathbb{F}^n$$

Example $(n=1)$: $f(x) = x - a$.

$$V(x-a) = \{b \in \mathbb{F} : f(b) = 0\}$$
$$= \{a\} \in \mathbb{F}.$$

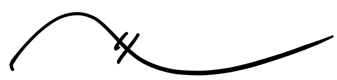
If $\mathbb{F}$ algebraically closed, then for any $f \in \mathbb{F}[x]$,

$$V(f) = \{\text{roots of } f\} \subseteq \mathbb{F}.$$

[Hypersurface $\subseteq \mathbb{F}$ is just a finite set of points!]

Example $(n=2)$: $f(x,y) = x^2 + y^2 - 1$.

$$V(f) = \text{unit circle} \subseteq \mathbb{F}^2.$$



More generally, for any set of polynomials $S \subseteq \mathbb{F}[\bar{x}]$ we define a set of points:

$$V(S) = \{\bar{a} \in \mathbb{F}^n : f(\bar{a}) = 0 \ \forall f \in S\}.$$

And for any set of points $T \subseteq \mathbb{F}^n$ we define a set of polynomials:

$$I(T) = \{f \in \mathbb{F}[\bar{x}] : f(\bar{a}) = 0 \ \forall \bar{a} \in T\}.$$

Descartes' Theorem: Let $f(x) = x - a$.

$$IV(x-a) = (x-a)$$

$= \text{principal ideal}$

$\{(x-a)\,g(x) : g(x) \in \mathbb{F}[x]\}.$

In other words: for all $g(x) \in \mathbb{F}[x]$, $a \in \mathbb{F}$, we have

$$g(a) = 0 \iff x-a \mid g(x).$$

Study's lemma: If $\mathbb{F}$ is algebraically closed and if $f \in \mathbb{F}[x_1, \dots, x_n]$ is irreducible, then

$$IV(f) = (f).$$

In other words, if g vanishes on the hypersurface $V(f)$ ($f(\bar{a}) = 0$ implies $g(\bar{a}) = 0 \ \forall \bar{a} \in \mathbb{F}^n$) then g is divisible by f.

Meaning: Every hypersurface has a unique "minimal polynomial"

Proof: Later... ///

The maps V, I provide a correspondence between sets of polynomials & certain kinds of geometric shapes:

$$V: \begin{array}{c}\text{subsets}\\ \text{of } \mathbb{F}[\bar{x}]\end{array} \begin{array}{c}\longrightarrow \\ \longleftarrow\end{array} \begin{array}{c}\text{subsets}\\ \text{of } \mathbb{F}^n\end{array} : I$$

[Note: $I(T)$ is always an ideal.]

Purely formal properties (concept of a "Galois connection"):

- $S \subseteq IV(S)$ "closure
  $T \subseteq VI(T)$ operators"

- $S_1 \subseteq S_2 \Rightarrow V(S_1) \supseteq V(S_2)$
  $T_1 \subseteq T_2 \Rightarrow I(T_1) \supseteq V(T_2)$

- $IVI = I$ & $VIV = V$

[Consequence: $V(S) = V(IV(S))$,

so we can restrict our attention to ideals of $\mathbb{F}[\bar{x}]$.]

- Def: Say $S \subseteq \mathbb{F}[\bar{x}]$, $T \subseteq \mathbb{F}^n$ are <u>closed</u> when

$$S = IV(S)$$
$$T = VI(T).$$

Turns out that

$T \subseteq \mathbb{F}^n$ is closed $\iff$

$T = V(I)$ for some ideal $I \subseteq \mathbb{F}[\bar{x}]$

Such closed sets are called "Zariski closed" (or "varieties").

- Follows from Hilbert basis theorem that any variety is an intersection of finitely many hypersurfaces:

$$\begin{aligned} V &= V(I) \\ &= V(f_1, \dots, f_m) \\ &= V(f_1) \cap \dots \cap V(f_m). \end{aligned}$$

• So far everything was "easy."
The next result is not easy.

Hilbert's Nullstellensatz:
Let $\mathbb{F}$ be algebraically closed, let $J \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be an ideal. Then the "Galois closure" of J is given by the "radical closure":

$$IV(J) = \sqrt{J}$$
$$= \{ g \in \mathbb{F}[\bar{x}] : g^k \in J \text{ for some } k \geq 1 \}$$

Proof: Last semester's notes. We won't need it this semester. ///

The NSS is a generalization of Study's Lemma: Given prime factorization of a polynomial

$$f = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} \in \mathbb{F}[x_1, \ldots, x_n],$$

then we have

$I(\text{hypersurface})$

$= IV(f)$

$= \sqrt{(f)} \overset{*}{=} (p_1 p_2 \cdots p_m)$ forget the exponents.

Proof of $*$: If $f \mid g^k$ for some $k \geq 1$ then each prime factor of f divides g^k, hence divides g, hence

$$p_1 p_2 \cdots p_m \mid g.$$

Conversely, if $p_1 p_2 \cdots p_m \mid g$ then

$$f \mid g^k \text{ where } k \geq \max(e_1, \ldots, e_m).$$

///

In particular, if f is itself prime,

$$IV(f) = \sqrt{(f)} = (f).$$

["Prime ideals are radical."]

Minimal & Maximal Ideals:

If R is a UFD then

minimal nonzero ideals of R = principal (nonzero, nonunit) ideals of R.

On the other hand, consider a point $\bar{a} = (a_1, \dots, a_n) \in \mathbb{F}^n$. What is the ideal?

$$I(\{\bar{a}\}) = ?$$

Claim: $I(\{\bar{a}\}) = M_{\bar{a}}$

$$:= (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$$

$$= \{(x_1 - a_1) f_1 + \dots + (x_n - a_n) f_n : f_1, \dots, f_n \in \mathbb{F}[x_1, \dots, x_n]\}$$

Proof: Given any $g \in I(\{\bar{a}\})$, i.e., with $g(\bar{a}) = 0$, we first divide by $x_1 - a_1$ to get quotient & remainder:

$$g = (x_1 - a_1) q_1 + r_1,$$

where $r_1(x_2, \dots, x_n)$ does not involve x_1.
Then divide r_1 by $x_2 - a_2$ to get

$$\begin{aligned} g &= (x_1 - a_1) q_1 + r_1 \\ &= (x_1 - a_1) q_1 + (x_2 - a_2) q_2 + r_2, \end{aligned}$$

where $r_2(x_3, \dots, x_n)$ does not involve x_1, x_2.
Repeat to obtain:

$$g = (x_1 - a_1) q_1 + \dots + (x_n - a_n) q_n + \alpha$$

for some constant $\alpha \in \mathbb{F}$ and plug in $\bar{x} = \bar{a}$ to see that $\alpha = 0$. We conclude that $g \in M_{\bar{a}}$, hence

$$I(\{\bar{a}\}) \subseteq M_{\bar{a}}.$$

Now consider the "evaluate at $\bar{a}$" ring homomorphism:

$$\begin{aligned} \mathbb{F}[\bar{x}] &\longrightarrow \mathbb{F} \\ f &\longmapsto f(\bar{a}). \end{aligned}$$

This is a surjective ring hom. with kernel $I(\{\bar{a}\})$, so that

$$\frac{\mathbb{F}[\bar{x}]}{I(\{\bar{a}\})} \approx \mathbb{F}.$$

Since $\mathbb{F}$ is a field this implies that $I(\{\bar{a}\})$ is a maximal ideal. Hence

$$I(\{\bar{a}\}) \subseteq M_{\bar{a}} \implies I(\{\bar{a}\}) = M_{\bar{a}}$$

///