5. The Hilbert Basis Theorem

Big idea: "Every ideal in $F[x_1, \dots, x_n]$ is finitely generated."
(We'll actually prove something more general):
R is Noetherian iff $R[x]$ is Noetherian.

Basic algebraic geometry (Motivation):

If F is an (algebraically closed) field and $S \subseteq F[x_1, \dots, x_n]$ a set of polynomials, then define the zero-set of S to be

$$Z(S) = \{ \vec{x} \in F^n : f(\vec{x}) = 0 \quad \forall f \in S \}.$$

A subset $V \subseteq F^n$ is an (affine) algebraic set if $V = Z(S)$ for some S, and is an (affine) algebraic variety if moreover, it is not the union of 2 proper affine algebraic sets.

* Consequence of the Hilbert Basis Theorem:

Let $I \subseteq F[x_1, \dots, x_n]$ be an ideal, and $V = V(I)$ the corresponding algebraic variety. Then I is finitely generated; so $V = Z(S)$ for some finite S,

i.e., "V is a set of common solutions to a finite set of polynomials."

Recall: A comm. ring is Noetherian if every ascending chain of ideals terminates.

Def: A ring R satisfies the <u>maximal condition</u> (for ideals) if every nonempty set $\mathcal{S}$ of ideals in R contains a maximal element I_0, i.e., if $I \in \mathcal{S}$ & $I_0 \subseteq I$, then $I_0 = I$.

Note: There might be several max'l elts, e.g., $\mathcal{S} = \{(2), (3)\}$ in $\mathbb{Z}$.

Prop 5.1: A comm. ring is Noetherian iff it satisfies the maximal condition.

Pf: Exercise.

Prop 5.2: A comm. ring R is Noetherian iff every ideal in R is finitely generated.

Pf: ($\Rightarrow$) If I is an ideal in R, let $\mathcal{S}$ be the set of all finitely generated ideals contained in I. Let I_0 be a max'l elt of $\mathcal{S}$, say $I_0 = (r_1, \dots, r_k)$. If $I_0 \subsetneq I$, choose $r \in I \setminus I_0$, and let $J = (r_1, \dots, r_k, r)$. Then $J \in \mathcal{S}$ but $I_0 \subsetneq J$ ↯.
Thus $I = I_0$ is fin. gen. ✓

($\Leftarrow$) Let $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Put $I = \bigcup_{i=1}^{\infty} I_i$. Say $I = (r_1, \dots, r_k)$ with $(r_1, \dots, r_i) = I_{j(i)}$ for $1 \le i \le j$. Then $I = I_{j(k)}$, so the chain terminates. ✓ $\square$

$\boxed{4}$

Let $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals in $R[x]$, and let

$$\mathcal{S} = \{ I_n(m) : 0 \leq n, m \in \mathbb{Z} \}.$$

By Prop 5.1, $\mathcal{S}$ has a max'l elt $I_r(s)$.

Consider the infinite 2D array of ideals of R:

$$\begin{array}{ccccccccccc}
I_0(0) & \subseteq & I_0(1) & \subseteq & \cdots & \subseteq & I_0(s-1) & \subseteq & I_0(s) & \subseteq & \cdots \\
\rotatebox{-90}{$\subseteq$} & & \rotatebox{-90}{$\subseteq$} & & & & \rotatebox{-90}{$\subseteq$} & & \rotatebox{-90}{$\subseteq$} & & \\
I_1(0) & \subseteq & I_1(1) & \subseteq & \cdots & \subseteq & I_1(s-1) & \subseteq & I_1(s) & \subseteq & \cdots \\
\rotatebox{-90}{$\subseteq$} & & \rotatebox{-90}{$\subseteq$} & & & & \rotatebox{-90}{$\subseteq$} & & \rotatebox{-90}{$\subseteq$} & & \\
I_2(0) & \subseteq & I_2(1) & \subseteq & \cdots & \subseteq & I_2(s-1) & \subseteq & I_2(s) & \subseteq & \cdots \\
\rotatebox{-90}{$\subseteq$} & & \rotatebox{-90}{$\subseteq$} & & & & \rotatebox{-90}{$\subseteq$} & & \rotatebox{-90}{$\subseteq$} & & \\
\vdots & & \vdots & & & & \vdots & & \vdots & & \\
 & & & & & & & & \boxed{I_r(s)} & = & I_r(s+1) = \cdots \\
 & & & & & & & & \parallel & & \\
 & & & & & & & & I_{r+1}(s) & = & \cdots \\
 & & & & & & & & \parallel & & \\
 & & & & & & & & \vdots & &
\end{array}$$

<u>Note</u>: "$\subseteq$" holds by the Exercise, part (2)

"$\rotatebox{-90}{$\subseteq$}$" holds by the Exercise, part (3).

The j^{th} column terminates, say at $I_{f(j)}(j)$.

Set $u = \max\{ f(0), f(1), \dots, f(s-1), r \}$.

<u>Note</u> If $i > r$ and $j \geq s$, then $I_i(j) = I_r(s)$ by maximality.

Let R be a comm. ring with 1. If I is an ideal in $R[x]$ and $m \in \mathbb{Z}_{\geq 0}$, let $I(m)$ be the set of leading coeffs of degree-m polynomials in I (i.e, the "a_m" term), with 0.

Exercise: (Easy)!

(1) $I(m)$ is an ideal of R.
(2) $I(m) \subseteq I(m+1)$ for all m.
(3) If J is an ideal with $I \subseteq J$, then $I(m) \subseteq J(m)$ for all m.

Prop 5.3: Let R be a comm. ring with 1, and let I, J be ideals in $R[x]$ with $I \subseteq J$ and $I(m) = J(m)$ for all $m \in \mathbb{Z}_{\geq 0}$. Then $I = J$.

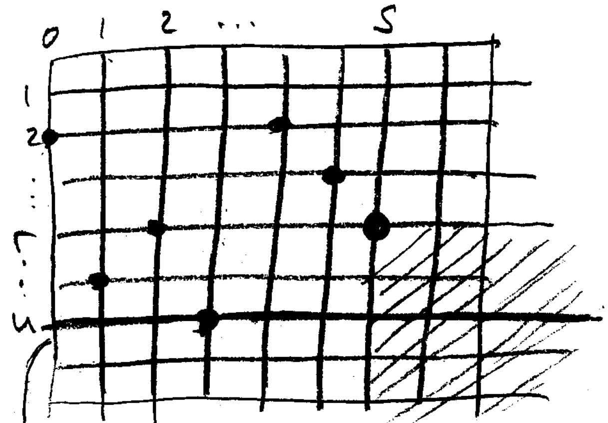
Pf: If not, choose $f(x) \in J \setminus I$ of min'l degree $m > 0$. Since $I(m) = J(m)$, there is some $g(x) \in I$ of degree m with the same leading coefficient as $f(x)$.
Then, $f(x) - g(x) \in J \setminus I$ and $0 < \deg(f(x) - g(x)) < m$. $\lightning$
$\square$

Thm 5.4 (The Hilbert Basis Theorem): Let R be a comm ring with 1. If R is Noetherian, then the polynomial ring $R[x_1, \ldots, x_n]$ is also Noetherian.

Pf: Since $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$, we may assume $n = 1$, and write $x_1 = x$.

Pf (cont.)

Schematically:



$I_u(m) = I_{u+k}(m) \;\; \forall k \geq 0$

$\Rightarrow I_u = I_{u+k} \;\; \forall k \geq 0$.

Let $i \geq u$.

Clearly, $I_i(m) \supseteq I_u(m)$

Claim: $I_i(m) = I_u(m)$.

True for $m < s$ by choice of u. ✓

If $m \geq s$, then $I_i(m) \supseteq$

$I_i(m) \supseteq I_r(m)$
$I_u(m) \supseteq I_r(m)$ by maximality of ascending chains.

$\Rightarrow I_i(m) = I_r(m) = I_u(m)$. ✓

Now apply Prop 5.3: Since $I_u \subseteq I_i$ and $I_u(m) = I_i(m)$ for all m, $I_u = I_i$ for all $i \geq u$, thus the chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ terminates, so $R[x]$ is Noetherian. $\square$

Remark: The Hilbert Basis Theorem also holds for the ring $R[[x]]$ of formal power series over R.

Non-example: $R[x_1, x_2, x_3, \ldots]$ is not Noetherian.

Cor: Suppose S is a ring with 1, R a comm. Noetherian subring with $1_S \in R$, and $s_1, \ldots, s_n$ in the center of S. Then $R[s_1, \ldots, s_n]$ is Noetherian.

Pf: By Thm 2.3 (substitution),

$\exists$ homom $R[x_1,..,x_n] \longrightarrow R[s_1,..,s_n]$

$$f(x_1,..,x_n) \longmapsto f(s_1,..,s_n)$$

$$\begin{tikzcd}
R \arrow[rr, hook, "\Phi"] \arrow[dr, "\theta"'] & & R[x_1,\dots,x_n] \arrow[dl, dashed, "E_{s_1\cdots s_n}"] \\
& R[s_1,..,s_n] \subseteq S &
\end{tikzcd}$$

Clearly, homomorphic images of Noetherian rings are Noetherian. $\square$

Summary: The Hilbert Basis Theorem says that every ideal I in $F[x_1,..,x_n]$ is finitely generated.

Question: How do we find a "basis" for I (actually, just a generating set, we don't need uniqueness).

Say we have $f(x_1,..,x_n) \in R[x_1,..,x_n]$. We want to determine if $f(x_1,..,x_n) \in I$.

Answer: This can be done with a Gröbner basis. There is an algorithm (Buchberger) for constructing one.

But it has some drawbacks (inefficient, not minimal size).