4. Hilbert's basis theorem

Throughout, R is a commutative ring and F is a field.

Big idea: Every ideal in $F[x_1, \ldots, x_n]$ is finitely generated.

We'll actually prove something more general:

"R is Noetherian iff $R[x]$ is Noetherian."

Def: R is Noetherian if every ascending chain of ideals stabilizes, i.e., if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, then for some N, $I_N = I_{N+1} = \cdots$.

Ex: $R = \mathbb{Z}$ is Noetherian. Consider $(720) \subseteq (72) \subseteq (12) \subseteq (3) \subseteq \cdots$

Non-ex: $R = \mathbb{Z}[x_1, x_2, x_3, \ldots]$. Consider $(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$

Prop 4.1: If R is a PID, then R is Noetherian.

Pf: Consider $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, and define $I = \bigcup_{j=1}^{\infty} I_j = (a)$, $a \in R$.

Pick I_N containing a.

Then $(a) \subseteq I_N = I = (a) \Rightarrow I_N = I$.

Thus, $I_N = I_{N+1} = \cdots = I \Rightarrow R$ is Noetherian. $\square$

Def: A ring R satisfies the maximal condition (for ideals) if every nonempty set S of ideals in R contains a maximal element J, i.e., $J \in S$ and $J \subseteq I \Rightarrow J = I$.

Note: There might be multiple maximal elements in S.

Prop 4.2 (Exercise): R is Noetherian iff it satisfies the maximal condition.

<u>Prop 4.3</u>: R is Noetherian iff every ideal is finitely generated.

<u>Pf</u>: $(\Rightarrow)$ Take an ideal I of R.

Let $S = \{$ all f.g. ideals contained in $R \}$.

We need to show that $I \in S$.

Let $J = (r_1, \dots, r_n)$ be a maximal element of S.

If $a \in J \setminus I$, then $J \subsetneq (r_1, \dots, r_n) \subseteq I$, which contradicts maximality, hence $J = I \in S$. ✓

$(\Leftarrow)$ Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ be an ascending chain of ideals.

Put $I = \bigcup_{j=1}^{\infty} I_j = (r_1, \dots, r_k)$.

Then $r_j \in I_{N_j}$ for some N_j.

Let $N = \max(N_j)$. Then $(r_1, \dots, r_n) \subseteq I_N \subseteq I = (r_1, \dots, r_n)$, and so $I_N = I_{N+1} = \dots = I$, hence R is Noetherian. $\square$

<u>Def</u>: For an ideal I of $R[x]$, let $I(m)$ be the set of all coefficients of degree-m polynomials, along with zero.

<u>Exercise</u> (easy):

(1) $I(m)$ is an ideal of R

(2) $I(m) \subseteq I(m+1)$ for all m

(3) If $I \subseteq J$ are ideals, then $I(m) \subseteq J(m)$.

<u>Prop 4.4:</u> Let $I \subseteq J$ be ideals of $R[x]$. If $I(m) = J(m)$ for all m, then $I = J$.

<u>Pf:</u> If not, then pick $f(x) \in J \setminus I$ 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.

Then $f(x) - g(x) \in J \setminus I$ and $0 < \deg(f(x) - g(x)) < m$. $\lightning$ $\square$

<u>Thm 4.5:</u> (Hilbert's basis theorem). If R is Noetherian, then the polynomial ring $R[x_1, \dots, x_n]$ is Noetherian.

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

Let $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in R, and let $S = \{ I_n(m) : 0 \le n, m \in \mathbb{Z} \}$.

By Prop 4.2, S has a max'l element, $I_r(s)$.

Consider the 2D array of ideals of R:

$$
\begin{array}{ccccccccccccc}
I_0(0) & \subseteq & I_0(1) & \subseteq & \cdots & \subseteq & I_0(s-1) & \subseteq & I_0(s) & \subseteq \cdots & & & \\
\cap\!| & & \cap\!| & & & & \cap\!| & & \cap\!| & & & & \\
I_1(0) & \subseteq & I_1(1) & \subseteq & \cdots & \subseteq & I_1(s-1) & \subseteq & I_1(s) & \subseteq \cdots & & & \\
\cap\!| & & & & & & \cap\!| & & \cap\!| & & & & \\
I_2(0) & \subseteq & I_2(1) & \subseteq & \cdots & \subseteq & I_2(s-1) & \subseteq & I_2(s) & \subseteq \cdots & & & \\
 & & & & & & & & \cap\!| & & & & \\
 & & & & & & & & \vdots & & & & \\
 & & & & & & \cdots & \subseteq & I_r(s) & = & I_r(s+1) & = & \cdots \\
 & & & & & & & & \| & & \| & & \\
 & & & & & & & & \vdots & & & &
\end{array}
$$

$\boxed{4}$

Note: "$\subseteq$" holds by the Exercise, part (2)

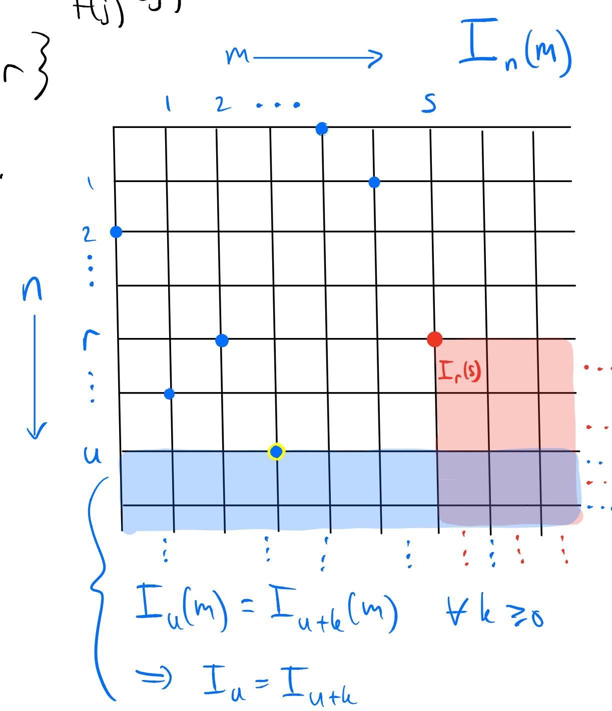
"$\supseteq$" holds by the Exercise, part (3).

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

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

By construction: $I_{u+k}(m) = I_u(m) \quad \forall k \geq 0.$

By Prop 4.4, since $I_u \subseteq I_{u+k}$ and $I_u(m) = I_{u+k}(m) \quad \forall m$, $I_u = I_{u+k} \quad \forall k \geq 0$, thus the chain $I_0 \subseteq I_1 \subseteq \dots$ stabilizes, so $R[x]$ is Noetherian. $\square$



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

Cor: Suppose S is a (not necessarily commutative) ring with unity, and R a comm. Noetherian subring with $1_S \in R$, and $s_1, \dots, s_n$ in the center of S. Then $R[s_1, \dots, s_n]$ is Noetherian.

Pf: By Thm 2.3 (substitution),

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

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

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[dr, "\theta"'] & R[x_1, \dots, x_n] \arrow[d, dashed, "E_{s_1, \dots, s_n}"] \\ & R[s_1, \dots, s_n] \end{tikzcd}$$

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

<u>Remark</u>: The Hilbert Basis theorem doesn't tell us how to find a basis for I, or what a particular "nice" basis might look like.

This is a question in <u>computational algebra</u>.

One nice type of basis is called a <u>Gröbner basis</u>, and the <u>Buchberger algorithm</u> constructs one.