This course is about algebraic geometry. At its heart, this is the study of solutions of systems of polynomial equations.

We'll need a heavy dose of algebra in this class!

Review the basics of rings!

Almost all our rings will be commutative with 1. A ring homomorphism is assumed to take 1 to 1.

Field of Fractions

Let $R$ be a ring. A field $F$ together with a homomorphism $R \rightarrow F$ is a field of fractions of $R$ if it has the following universal property:
every homomorphism $R \rightarrow K$ from $R$ to a field $K$ factors uniquely through $F$. 
i.e. there is a unique homomorphism
\[ F \xrightarrow{\alpha} K \] that makes
\[ R \xrightarrow{i} F \]
\[ f \xrightarrow{1} K \]
commute
(i.e. \( f = \alpha \circ i \)).

**Prop.** If \( R \) is a ring (commutative, with 1), then there is a field of fractions for \( R \).

**Proof.** Exercise. \( \square \)

Recall the def. of the polynomial ring \( R[X_1, \ldots, X_n] \) with coefficients in \( R \).
(formal expressions \( \sum a_I X^I \)).

**Prop.** If \( \phi : R \to S \) is a ring homomorphism and \( s_1, \ldots, s_n \in S \), there is a unique homomorphism \( \widetilde{\phi} : R[X_1, \ldots, X_n] \to S \).
such that $\tilde{\phi}(r) = \phi(r)$ for all $r \in R[x_1, \ldots, x_n]$, and

$\tilde{\phi}(x_i) = s_i$, $i = 1, \ldots, n$.

Proof. Uniqueness is clear. Existence amounts to checking that

$$(f + g)(s_1, \ldots, s_n) = f(s_1, \ldots, s_n) + g(s_1, \ldots, s_n)$$

and

$$(fg)(s_1, \ldots, s_n) = f(s_1, \ldots, s_n)g(s_1, \ldots, s_n)$$

for $f, g \in R[x_1, \ldots, x_n]$ which is easy. $\square$.

Cor. There is a canonical isomorphism

$$R[x_1, \ldots, x_n] \xrightarrow{\sim} R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n]$$

whenever $1 \leq k \leq n-1$.

For some other basic properties of rings that we will need, read Ch.I, Section 1 of Fulton, and, where necessary, re-read Herstein and your notes from last semester.
Recall the definition of an ideal of a ring \( R \) (as always, commutative with 1).

A collection of ideals

\[ I_1 \leq I_2 \leq I_3 \leq \ldots \leq R \]

is called an ascending chain of ideals.

It is stationary if there exists \( k \) such that \( I_l = I_k \) for all \( l \geq k \).

\( R \) is noetherian if every ascending chain of ideals in \( R \) is stationary.

**Hilbert Basis Theorem**: If \( R \) is noetherian, so is \( R[x] \).

**Cor**: If \( R \) is noetherian, so is \( R[x_1, \ldots, x_n] \).

**Cor**: If \( k \) is a field, then \( k[x_1, \ldots, x_n] \) is noetherian.

Proof. The only ideals in \( k \) are
and \( k \), so \( k \) is noetherian.

The conclusion follows from the previous corollary.

To prove Hilbert Basis Theorem, we first prove:

**Lemma** \( R \) is noetherian iff every ideal of \( R \) is finitely generated.

[Recall: the ideal generated by a subset \( S \subseteq R \) is]

\[
(S) = \bigcup_{S \subseteq I, I \text{ an ideal of } R} I
\]

An ideal \( I \subseteq R \) is finitely generated if there exists a finite subset \( S \subseteq I \) such that \( I = (S) \).

In this case, writing \( S = \{s_1, \ldots, s_n \} \), we have \( I = \{a_1s_1 + \cdots + a_ns_n | a_i \in \mathbb{R} \} \).
Proof of Lemma. Suppose first that every ideal of $R$ is finitely generated.

Let $\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \ldots$ be an ascending chain of ideals. Then

$$\mathcal{I} = \bigcup_{k} \mathcal{I}_k$$

is an ideal. Write $\mathcal{I} = (s_1, \ldots, s_n)$. Then each of $s_1, \ldots, s_n$ appears in one of the $\mathcal{I}_k$, say $s_1 \in \mathcal{I}_{k_1}, \ldots, s_n \in \mathcal{I}_{k_n}$. So $(s_1, \ldots, s_n) \subseteq \mathcal{I}_m$ where

$$m = \max \{ k_1, \ldots, k_n \}.$$ 

Thus $\mathcal{I} = (s_1, \ldots, s_n) \subseteq \mathcal{I}_m \subseteq \mathcal{I}_k \subseteq \mathcal{I}$ for all $k \geq m$, and the chain is stationary.

Conversely, suppose $R$ is noetherian, and let $I \leq R$ be an ideal; we may assume $I \neq 0$. Choose
any nonzero $s_j \notin I$ and let $I_j = (s_j)$. Given $I_k = (s_1, \ldots, s_k) \subseteq I$, if

$I_k \neq I$ choose some $s_{k+1} \in I \setminus I_k$

and let $I_{k+1} = (s_1, \ldots, s_{k+1})$.

Continuing in this way we get an ascending chain

$I_1 \subset I_2 \subset \ldots$ which is not stationary, a contradiction. So it can't be the case that $I_k \neq I$ for every $k$, i.e. for some $k$ we eventually arrive at

$(s_1, \ldots, s_k) = I_k = I$.

Finally, Proof of Hilbert Basis Theorem:

let $I \subseteq R[x]$ be an ideal; we must prove $I$ is finitely generated.

Def: let $L$ be the set of leading
coefficients of elements of $I$.

Claim $L$ is an ideal of $R$.

Proof is an easy exercise, we'll discuss briefly in class.

By assumption there exist $c_1, \ldots, c_n \in R$ such that $L = (c_1, \ldots, c_n)$. By def. of $L$, there are $f_1, \ldots, f_n \in I$ s.t. $f_i$ has leading coeff. $c_i$. Let

$N = \max \{ \deg (f_i) \mid i = 1, \ldots, n \}$. 

For each $m$, $0 \leq m \leq N-1$, let

$L_m = \{ \text{leading coeff. of polynomials } g \in I \text{ with } \deg (g) \leq m \}$

Claim $L_m \subset R$ is an ideal.

Similarly to what we did for $L$, **And our previous lemma!**
we choose polynomials \( \{ f_m, k \} \) of degree \( \leq m \) whose leading coeff. generate \( L_m \).

Finally, we let

\[
I' = \bigcup_{\alpha M \leq N-1} \{ f_m, k \} \cup \{ f_1, \ldots, f_\alpha \}.
\]

Claim: \( I' = I \).

Certainly \( I' \subseteq I \) since \( I' \) is generated by a subset of \( I \), suppose \( I' \neq I \), and let \( G \in I \) be an element of smallest degree not in \( I' \). If \( \deg(G) \geq N \), write the leading coefficient \( c \in \mathbb{L} \) of \( G \) as \( c = \sum_{i=1}^{n} a_i \cdot c_i \) with \( a_i \in \mathbb{R} \).

Let \( e_i = \deg(G) - \deg(f_i) \). Then

\[
\deg \left( G - \sum a_i \cdot c_i f_i \right) < \deg(G) \quad \text{since}
\]
$G$ and $\Sigma a_i X^{e_i f_i}$ have the same leading term, namely $c_i$; so $G - \Sigma a_i X^{e_i f_i} \in I'$, so $G \in I'$. \*.

Similarly, if $\deg(G) = m < N$,
write $c \in L_m$ as
\[ c = \sum a_k c_m, \] where $a_k \in \mathbb{R}$ and $c_m, k$ is the leading coeff. of $f_m, k$. Then
\[ \deg(G - \sum a_k f_m, k) < m \] so $G - \sum a_k f_m, k \in I'$ and $G \in I'$. \*.

This completes the proof. \*.
A calculation: Let \( R = \mathbb{Z}[x] \),
\( I = (f_1 + px^2 \mid p \text{ prime}) \subseteq \mathbb{Z}[x] \).

With notation as in Hilbert Basis Theorem, \( L = (\text{leading coeff. of poly in } I \rangle) \supseteq (\mathbb{Q} \mid p \text{ prime}) \).

Now \( 3 - 2 = 1 \in (\mathbb{Q} \mid p \text{ prime}) \), so \( L = \mathbb{Z} \).

Set \( h = 2x^2 + 1 \), \( g = 3x^3 + 1 \). Then

\[-2xg + (3x^2 - 1)h = x^2 - 2x - 1 = : f \]

has leading coeff. 1. By proof of Hilbert Basis Theorem, we should then find \( L_0, L_1 \subseteq \mathbb{Z} \) and choose polynomials whose leading coeff. generate \( L_0, L_1 \).

This is harder [why?]. After some calculation, I found

\[5(3x^3 + 1) - 15x^2(2x^2 + 1) + 65x^5 + 1 = 11 \in I.\]

Now

\[-x^{11} + 11 + (11x^{11} + 1) = 1 \in I, \quad \text{so}\]

\[I = \mathbb{Z}[x]. \quad \text{So trying to carry out Hilbert we find } L_0 = \mathbb{Z}, \quad L_1 = \mathbb{Z} \quad \text{but also} \quad \text{just } \quad I = \mathbb{Z}[x].\]