

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 ,

ie. there is a unique homomorphism

$F \xrightarrow{a} K$ that makes

$$\begin{array}{ccc} R & \xrightarrow{i} & F \\ & \searrow f & \downarrow \text{Ga} \\ & & K \end{array} \quad \text{commute}$$

(ie. $f = a \circ i$).

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 $R[X_1, \dots, X_n]$ with coefficients in R . (formal expressions $\sum a_I X^I$).

Prop If $\varphi: R \rightarrow S$ is a ring homomorphism and $s_1, \dots, s_n \in S$, there is a unique homomorphism $\tilde{\varphi}: R[X_1, \dots, X_n] \rightarrow S$

such that $\tilde{\varphi}(r) = \varphi(r)$ for all

$r \in R \subseteq R[X_1, \dots, X_n]$, and

$$\tilde{\varphi}(X_i) = s_i, \quad i=1, \dots, n.$$

Proof. Uniqueness is clear. Existence

amounts to checking that

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

and

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

$\forall f, g \in R[X_1, \dots, X_n]$ which is easy. \square .

Cor There is a canonical isomorphism

$$R[X_1, \dots, X_n] \xrightarrow{\sim} R[X_1, \dots, X_k][X_{k+1}, \dots, X_n]$$

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, reread 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

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq R \text{ is}$$

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 $R[x_1, \dots, x_n]$.

Cor If k is a field, then $k[x_1, \dots, x_n]$ is noetherian.

Proof. The only ideals in k are

$\{0\}$ and k , so k is noetherian.
The conclusion follows from the previous
Corollary. \square

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

$$(S) = \bigcap_{\substack{S \subseteq I \\ I \text{ an ideal} \\ \text{of } R}} I.$$

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 $S = \{s_1, \dots, s_n\}$,
we have $I = \{a_1 s_1 + \dots + a_n s_n \mid a_1, \dots, a_n \in R\}$.

Proof of lemma. Suppose first that every ideal of R is finitely generated.

Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals. Then

$$I = \bigcup_k I_k$$

is an ideal. Write $I = (s_1, \dots, s_n)$.

Then each of s_1, \dots, s_n appears in one of the I_k , say $s_1 \in I_{k_1}, \dots, s_n \in I_{k_n}$.

So $\{s_1, \dots, s_n\} \subseteq I_m$ where

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

Thus $I = (s_1, \dots, s_n) \subseteq I_m \subseteq I_l \subseteq I$

for all $l \geq m$, and the chain is stationary.

Conversely, suppose R is noetherian, and let $I \subseteq R$ be an ideal; we may assume $I \neq \{0\}$. Choose

any nonzero $s_1 \in I$ and let $I_1 = (s_1)$.

Given $I_k = (s_1, \dots, s_k) \subseteq I$, if

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

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

Continuing in this way we get an ascending chain

$I_1 \subsetneq I_2 \subsetneq \dots$ 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

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

□

Finally:

Proof of Hilbert Basis Theorem:

let $I \subseteq \mathbb{R}[x]$ 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 $c_1, \dots, c_n \in L$ such that $L = (c_1, \dots, c_n)$. By def. of L , there are $f_1, \dots, f_n \in I$ s.t. f_i has leading coeff. c_i . Let $N = \max \{ \deg(f_i) \mid i=1, \dots, n \}$.

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

$$L_m = \left\{ \begin{array}{l} \text{leading coeff. of polynomials } g \in I \\ \text{with } \deg(g) \leq m \end{array} \right\}$$

Claim $L_m \subseteq R$ is an ideal.

Similarly to what we did for L ,

* And our previous lemma!

we choose polynomials $\{f_{m,k}\}_k$ of degree $\leq m$ whose leading coeff. generate L_m .

Finally, we let

$$\mathcal{I}' = \left(\bigcup_{0 \leq m \leq N-1} \{f_{m,k}\} \cup \{f_1, \dots, f_n\} \right).$$

Claim $\mathcal{I}' = \mathcal{I}$.

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

Let $e_i = \deg(G) - \deg(f_i)$. Then $\deg(G - \sum a_i X^{e_i} f_i) < \deg(G)$ since

G and $\sum a_i x^{e_i} f_i$ have the same leading term, namely c ; so

$$G - \sum a_i x^{e_i} f_i \in I', \text{ so } G \in I'. \quad *$$

Similarly, if $\deg(G) = m < N$,

write $c \in L_m$ as

$$c = \sum a_k c_{m,k} \text{ where } a_k \in R$$

and $c_{m,k}$ is the leading coeff. of

$f_{m,k}$. Then

$$\deg(G - \sum a_k f_{m,k}) < m \text{ so}$$

$$G - \sum a_k f_{m,k} \in I' \text{ and } G \in I'. \quad *$$

This completes the proof. \square .

A Calculation let $R = \mathbb{Z}[x]$,

$$I = (\{1 + px^p \mid p \text{ prime}\}) \subseteq \mathbb{Z}[x].$$

With notation as in Hilbert Basis Thm,

$$L = (\{\text{leading coeff of poly in } I\}) \supseteq (\{p \mid p \text{ prime}\})$$

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

Set $h = 2x^2 + 1$, $g = 3x^3 + 1$. Then

$$-2xg + (3x^2 - 1)h = x^2 - 2x - 1 =: f, \text{ has}$$

leading coeff. 1. By proof of Hilbert, we should then find $L_0, L_1 \in \mathbb{Z}$ and choose polys. whose leading coeff. generate L_0, L_1 .

This is harder [why?]. After some calculation

I found

$$5(3x^3 + 1) - 15x^3(2x^2 + 1) + 6(5x^5 + 1) = 11 \in I.$$

Now $-x^{11} \cdot 11 + (11x^{11} + 1) = 1 \in I$, so

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