Math 361

February 22, 2023

Quiz

1. What does Gauss's lemma say about factorization of polynomials with integer coefficients?
2. Why is it the case that if $\alpha \in \mathfrak{O}_K$, then $N(\alpha)$, $T(\alpha) \in \mathbb{Z}$? (Appeal to known properties of the field polynomial f_α.)

Today

- Review some of last lecture.

Today

- Review some of last lecture.
- State and prove the Hilbert basis theorem.

Today

- Review some of last lecture.
- State and prove the Hilbert basis theorem.
- Finish the last lecture.

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules:

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules: every chain of submodules of M,
$$N_1 \subseteq N_2 \subseteq \cdots ,$$
eventually *stabilizes*.

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules: every chain of submodules of M,
$$N_1 \subseteq N_2 \subseteq \cdots ,$$
eventually *stabilizes*. In other words, there exists k such that $N_k = N_{k+1} = \cdots$.

Review+

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules: every chain of submodules of M,
$$N_1 \subseteq N_2 \subseteq \cdots,$$
eventually *stabilizes*. In other words, there exists k such that $N_k = N_{k+1} = \cdots$.
3. Every nonempty collection of submodules of M has a maximal element under inclusion.

Review+

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules.

Review+

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Review+

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. The image of a Noetherian module (under an R-linear mapping) is Noetherian.

Review+

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. The image of a Noetherian module (under an R-linear mapping) is Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Review+

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. The image of a Noetherian module (under an R-linear mapping) is Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Corollary. If R is Noetherian and M is an R-module, then M is Noetherian if and only if M is finitely generated.

Review+

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. The image of a Noetherian module (under an R-linear mapping) is Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Corollary. If R is Noetherian and M is an R-module, then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Hilbert basis theorem

Consider the parametrized curve in $\mathbb{R}^3$:

$$c(t) = (t, t^2, t^3).$$

Hilbert basis theorem

Consider the parametrized curve in $\mathbb{R}^3$:

$$c(t) = (t, t^2, t^3).$$

Which polynomials $f(x, y, z) \in \mathbb{R}[x, y, z]$ vanish on the image of c?

Hilbert basis theorem

Consider the parametrized curve in $\mathbb{R}^3$:

$$c(t) = (t, t^2, t^3).$$

Which polynomials $f(x, y, z) \in \mathbb{R}[x, y, z]$ vanish on the image of c?

$$x = t, \quad y = t^2, \quad z = t^3.$$

Hilbert basis theorem

Consider the parametrized curve in $\mathbb{R}^3$:

$$c(t) = (t, t^2, t^3).$$

Which polynomials $f(x, y, z) \in \mathbb{R}[x, y, z]$ vanish on the image of c?

$$x = t, \quad y = t^2, \quad z = t^3.$$

We need $f(t, t^2, t^3) = 0$ for all t.

Hilbert basis theorem

Consider the parametrized curve in $\mathbb{R}^3$:

$$c(t) = (t, t^2, t^3).$$

Which polynomials $f(x, y, z) \in \mathbb{R}[x, y, z]$ vanish on the image of c?

$$x = t, \quad y = t^2, \quad z = t^3.$$

We need $f(t, t^2, t^3) = 0$ for all t.

Let t be an indeterminate, and define the ideal

$$I = \{f \in \mathbb{R}[x, y, z] : f(t, t^2, t^3) = 0\}.$$

Hilbert basis theorem

Consider the parametrized curve in $\mathbb{R}^3$:

$$c(t) = (t, t^2, t^3).$$

Which polynomials $f(x, y, z) \in \mathbb{R}[x, y, z]$ vanish on the image of c?

$$x = t, \quad y = t^2, \quad z = t^3.$$

We need $f(t, t^2, t^3) = 0$ for all t.

Let t be an indeterminate, and define the ideal

$$I = \{f \in \mathbb{R}[x, y, z] : f(t, t^2, t^3) = 0\}.$$

Is I finitely generated?

Hilbert basis theorem

Theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Hilbert basis theorem

Theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.

Hilbert basis theorem

Theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.
- Recall that a ring R is Noetherian, if and only if all of its ideals are finitely generated.

Hilbert basis theorem

Theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.
- Recall that a ring R is Noetherian, if and only if all of its ideals are finitely generated.
- Letting $R = K$ be a field and $S = K[x_1, \ldots, x_n]$, the Hilbert basis theorem says

Hilbert basis theorem

Theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.
- Recall that a ring R is Noetherian, if and only if all of its ideals are finitely generated.
- Letting $R = K$ be a field and $S = K[x_1, \ldots, x_n]$, the Hilbert basis theorem says that every ideal in S finitely generated.

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

We need to show that S is Noetherian.

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

We need to show that S is Noetherian. Then there exists an R-module surjection

$$\begin{aligned} R[x_1, \ldots, x_n] &\to S \\ f(x_1, \ldots, x_n) &\mapsto f(s_1, \ldots, s_n). \end{aligned}$$

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

We need to show that S is Noetherian. Then there exists an R-module surjection

$$\begin{aligned} R[x_1, \ldots, x_n] &\to S \\ f(x_1, \ldots, x_n) &\mapsto f(s_1, \ldots, s_n). \end{aligned}$$

Since the image of a Noetherian ring is Noetherian, it suffices to prove that the polynomial ring $R[x_1, \ldots, x_n]$ is Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

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

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. For instance,

$$\mathbb{Z}[x, y] \ni xy^3 + 5xy^2 + 7x^5y^3 + 9x^6y^2 + 15 =$$

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. For instance,

$$\mathbb{Z}[x, y] \ni xy^3 + 5xy^2 + 7x^5y^3 + 9x^6y^2 + 15 = (x + 7x^5)y^3 + (5x + 9x^6)y^2 + 15 \in \mathbb{Z}[x][y].$$

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \dots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$. For instance,

$$\mathbb{Z}[x, y] \ni xy^3 + 5xy^2 + 7x^5y^3 + 9x^6y^2 + 15 = (x + 7x^5)y^3 + (5x + 9x^6)y^2 + 15 \in \mathbb{Z}[x][y].$$

By induction, it suffices to show that R Noetherian $\Rightarrow R[x]$ Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

What is wrong with the following argument?

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

What is wrong with the following argument? In fact, $I = (f)$ for some f since $R[x]$ is a PID (from the division algorithm).

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

What is wrong with the following argument? In fact, $I = (f)$ for some f since $R[x]$ is a PID (from the division algorithm).

Answer: The division algorithm assumes R is a field.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$,

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$,

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$,

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$, we have $rf \in I$

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$, we have $rf \in I$ so its leading term, ra, is in A.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$, we have $rf \in I$ so its leading term, ra, is in A. Hence, A is closed under "outside-in" multiplication. $\square$

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \dots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \dots, x^{d-1}\}$.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module,

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian. Hence, $I_{<d}$ is a finitely generated R-module.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian. Hence, $I_{<d}$ is a finitely generated R-module. Say

$$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}.$$

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I.$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian. Hence, $I_{<d}$ is a finitely generated R-module. Say

$$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}.$$

Claim: $I = (g_1, \ldots, g_s, h_1, \ldots, h_t)$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

Proof of the Hilbert basis theorem

$A = (a_1, \dots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \dots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \dots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \dots, h_t\}$ = all elements of I of degree $< d$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$,

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be a

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Proof of the Hilbert basis theorem

$A = (a_1, \dots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \dots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \dots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \dots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \dots, g_s, \dots, h_1, \dots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$,

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$, and has degree $< e$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$, and has degree $< e$.

We are done by induction on the degree of f. (Why?)

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$, and has degree $< e$.

We are done by induction on the degree of f. (Why?) $\square$

Previous lecture

If time, finish the last lecture.