Lecture L111: Hilbert Basis Thm II; Polynomials over UFDs

§53.1 Hilbert Basis Theorem:

Theorem: Assume R is commutative and Noetherian. Then, so is $R[x]$.

Last time we defined leading ideals and proved a key technical result:

Definition: Given a commutative ring R and an ideal $\tilde{I} \subseteq R[x]$, we define:

$$L(\tilde{I}) := \{a \in R : a = L(f) \text{ for some } f \in \tilde{I}\} \subset R$$

(here, if $f = \sum_{n=0}^{D} a_n x^n$ $a_D \neq 0$, set $L(f) := a_D$. Set $LT(0) = 0$.)

Lemma: $L(\tilde{I}) \subset R$ is an ideal

Throughout, we assume R is a commutative ring.

Proposition: If R is a Noetherian ring and $D \in \mathbb{Z}_{\geq 1}$, then $R[x]/(x^D)$ is also Noetherian. Moreover, for any $J \subseteq R[x]/(x^D)$ ab subgroup with $RJ \subseteq J$, $\exists f_1, \dots, f_r \in J$ with $J = R \cdot f_1 + \dots + R f_r$.
(Example: J an ideal of $R[x]/(x^D)$)

Proof of Hilbert's Basis Theorem:

Let $\tilde{I} \subseteq R[x]$ be an ideal. We show that $\tilde{I}$ is finitely generated.

Step 1: Take the ideal $I = L(\tilde{I}) \subset R$. By Proposition §51.2, we know I is finitely generated because R is Noetherian. Write $I = (a_1, \dots, a_N)$ and therefore we get

$$g_1(x) = a_1 x^{d_1} + \boxed{\text{terms involving } x^{d_1-1}, \dots, x^0} \in \tilde{I}$$
$$\vdots \qquad \vdots$$
$$g_N(x) = a_N x^{d_N} + \boxed{\text{terms involving } x^{d_N-1}, \dots, x^0} \in \tilde{I}$$

Step 2: (Division Algorithm)

If $D = \max\{d_1, \dots, d_N\}$ ($d_i = \deg(g_i)$ $\forall i = 1, \dots, N$) then $\forall g(x) \in \tilde{I}$, $\exists \bar{g}(x) \in \tilde{I}$ st $\deg(\bar{g}) < D$

$$g = \bar{g} \mod (g_1, \dots, g_N)$$

Pf/ If $\deg(g) < D$ we have nothing to prove. Otherwise, we write

$$g(x) = \gamma x^M + \boxed{\text{terms involving } x^{M-1}, \dots, x^0} \in \tilde{I}$$

and $M \geq d_j$ $\forall j$.

As $\gamma \in I = (a_1, \dots, a_N)$ we have $r_1, r_2, \dots, r_N \in R$ st $\gamma = r_1 a_1 + \dots + r_N a_N$

$\Rightarrow$ $g(x) - \sum_{j=1}^{N} r_j g_j(x) x^{M-d_j} \in \tilde{I}$ has degree $< M$

We repeat this strategy until $\deg(\bar{g}) < D$ □

Step 3: Take care of polynomials in $\tilde{I}$ of degree $< D$ using Lemma §52.4

Let us denote by $\tilde{I}_{<D} = \{ f \in \tilde{I} : \deg(f) < D \}$

Then, $\tilde{I}_{<D} \subseteq R[x]/\langle x^D \rangle$ is an abelian subgroup and $R\tilde{I}_{<D} \subset \tilde{I}_{<D}$

By the argument from the proof of Lemma §52.4, $\exists\, f_1(x), \dots, f_p(x) \in \tilde{I}_{<D}$ such that $\tilde{I}_{<D} = R f_1(x) + R f_2(x) + \dots + R f_p(x)$.

Hence, combining this with the conclusion of Step 2:

$\tilde{I} = (g_1, \dots, g_N ; f_1, \dots, f_p)$ is finitely generated. □

§53.2 Polynomials over UFDs:

Recall: We have, so far, proved the following results for commutative rings.

Theorem 1:
- Euclidean domain $\Rightarrow$ PID $\Rightarrow$ UFD
- PID $\Rightarrow$ Noetherian domain

Theorem 2: On a UFD we have a well-defined notion of a greatest common divisor.

Key: On a UFD R: x is an irreducible element $\iff$ x is a prime element

(x irred: $x = ab \Rightarrow a \in R^\times$ or $b \in R^\times$ vs x prime $\equiv$ (x) is a prime ideal & $x \neq 0$)

($\Leftarrow$) is true for any domain R.

Recall: Given a domain R, $\gcd(a,b) = d \in R$ is an element satisfying:

(1) $d \mid a$ & $d \mid b$ in R

(2) If $c \in R$, $c \mid a$ & $c \mid b$ in R, then $c \mid d$ in R.

Lemma 1: On a UFD R, for each $a, b \in R$ not both 0, $\gcd(a,b) \in R$ exists. Furthermore, it is unique up to multiplication by a unit in R.

Lemma 2: In a Euclidean domain R we have $\gcd(a,b) \in (a,b)$ $\forall a, b \in R$

Proof: Same strategy used to prove the statement when $R = \mathbb{Z}$ works for any R Eucl. dom.

NEXT GOALS: ① Show R UFD $\Rightarrow R[x]$ UFD.

② Show UFDs $\not\subseteq$ Noetherian Domains & Noetherian Domains $\not\subseteq$ UFDs

§53.3 Gauss' Lemma:

Fix R a UFD & let $F = F(R)$ be its field of fractions.

Recall: $F(R) = S^{-1}R$ where $S = R \setminus \{0\}$ is the multiplicatively closed set of all non-zero elements of R.

We are going to view $R \subseteq F$ and $R[x] \subseteq F[x]$ (as subrings)

Definition: A polynomial $p \in R[x] \setminus \{0\}$ is said to be primitive if

$$\gcd(\text{coefficients of } p(x)) = 1 \text{ in } R.$$

That is, if $p = \sum_{j=0}^{n} c_j x^j$ with $c_n \neq 0$ Then, $d \mid c_j \ \forall j = 0, \cdots n \Rightarrow d \in R^\times$

$c_j \in R$

Example: $R = \mathbb{Z}$, $f(x) = 2x + 4$ is not primitive $f(x) = 2(x+2)$ is a non-trivial factorization in $\mathbb{Z}[x]$, but a trivial one in $\mathbb{Q}(x)$. ← primitive

Lemma (Gauss): If R is a UFD and $p(x) \in R[x]$ is a primitive polynomial, then: $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$.

Proof: ($\Leftarrow$) is easy: if $p(x) = f(x)g(x)$ with $f, g \in R[x] \subseteq F[x]$, then the irreducibility of $p(x)$ over $F[x]$ implies $f(x) \in F[x]^\times$ or $g(x) \in F[x]^\times$.

By using degree( ), we know $F[x]^\times = F^\times$, so $F^\times \cap R[x] = R \cap F^\times = R \setminus \{0\}$

Thus, we have $f(x) \in R \setminus \{0\}$ or $g(x) \in R \setminus \{0\}$.

By symmetry, assume $f \in R \setminus \{0\}$. Then, by construction f divides each coefficient of $p(x)$ over R, hence $f \in R^\times$ because p is a primitive element. Then, $f \in R^\times = R[x]^\times$

Thus, $p(x)$ is irreducible over $R[x]$.

($\Rightarrow$) is the hard direction. Assume $p(x)$ is irreducible over $R[x]$.

Claim 1: $\deg(p(x)) = n \geq 1$

Pf/ If $\deg(p(x)) = 0$, then $p = r \in R$ primitive implies $p \in R^\times = (R[x])^\times$, which cannot occur because irreducible elements are not units. □

- We argue by contradiction and assume $p(x) = A(x)B(x)$ for some $A(x), B(x) \in F[x]$ that are not units, ie $\deg(A(x)) = k \geq 1$ & $\deg(B(x)) = n-k \geq 1$.

Clearing denominators, we can find some $d \in R \setminus \{0\}$ such that:

(*) $\boxed{d \cdot p(x) = a(x)\, b(x) \quad \text{with } a(x), b(x) \in R}$

Here, $a(x) = rA(x)$, $b(x) = sB(x)$ with $r, s \in R$, so $d = r \cdot s$.

Claim 2: $\exists\ \alpha, \beta \in R$ s.t. $d = \alpha\beta$ & $\frac{a(x)}{\alpha} \in R[x]$, $\frac{b(x)}{\beta} \in R[x]$

Proof: Next Time.

The irreducibility of $p(x)$ over $R[x]$ will say $\frac{a(x)}{\alpha} \in (R[x])^\times = R^\times$ or $\frac{b(x)}{\beta} \in R^\times$, contradicting the fact that $\deg A(x) = \deg\left(\frac{a(x)}{\alpha}\right) > 0$ & $\deg B(x) = \deg\left(\frac{b(x)}{\beta}\right) > 0$ □