Lecture 04: D[x] is UFD iff D is UFD

Wednesday, January 17, 2018 12:59 PM

The main goal of today's lecture is to prove

Theorem. D is a UFD $\iff$ $D[x]$ is a UFD.

This will be done in several steps.

Lemma 1. Let $d \in D \setminus \{0\}$. Then

$$d \text{ is irreducible in } D \iff d \text{ is irreducible in } D[x].$$

Pf. ($\Rightarrow$) $d = a(x)\, b(x) \Rightarrow \deg d = \deg a + \deg b$

$$\Rightarrow \deg a = \deg b = 0.$$

$$\left.\begin{array}{l} \Rightarrow a, b \in D \text{ and } d = ab \\ \quad d \text{ is irr. in } D \end{array}\right\} \Rightarrow \text{either } a \in D^\times \text{ or } b \in D^\times$$

$$\Rightarrow \text{either } a \in D[x]^\times \text{ or } b \in D[x]^\times.$$

($\Leftarrow$) $\left.\begin{array}{l} d = ab \\ a, b \in D \end{array}\right\} \Rightarrow$ either $a \in D[x]^\times$ or $b \in D[x]^\times$

$$\Rightarrow \text{either } a \in D^\times \text{ or } b \in D^\times \text{ as } D[x]^\times = D^\times. \quad \blacksquare$$

Lemma 2. $D[x]$ is a UFD $\Rightarrow$ D is a UFD.

Pf. (existence) $\forall\, d \in D \setminus \{0\}$, $d = \prod_{i=1}^{m} p_i(x)$ and $p_i(x)$ are irred. in $D[x]$. $\Rightarrow \deg d = \sum \deg p_i \Rightarrow \forall i, \deg p_i = 0 \Rightarrow \forall i, p_i \in D$.

By Lemma 1, $p_i \in D$ and p_i irred. in $D[x]$ imply p_i is irred. in D.

Lecture 04.

Wednesday, January 17, 2018 1:13 PM

<u>Uniqueness</u> Suppose p_i's and q_i's are irred. in D and $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$. Then, by Lemma 1, p_i's and q_j's are irred. in $D[x]$. As $D[x]$ is a UFD, $m=n$ and $q_{\sigma_i} = p_i$ for some permutation σ. ∎

Before we get to the proof of the converse, let's recall to statement that we have proved earlier:

<u>Proposition 1.</u> Suppose D is a Noetherian integral domain. Then any non-zero element can be written as a product of irreducible elements.

<u>Proposition 2.</u> Suppose D is an integral domain; and any irreducible element is prime. Then a decomposition to irred. is unique up to reordering its factors and multiplying them by units.

In our case, $D[x]$ is not necessarily Noeth. (in general) So we need some other method to show the existence.

Lecture 04: Irreducibility of primitive polynomials

Wednesday, January 17, 2018 1:27 PM

Proposition. Suppose D is a UFD, and F is its field of fractions. Let $f(x) \in D[x]$ be a primitive poly. of deg > 0. Then f is irreducible in $D[x]$ if and only if f is irred. in $F[x]$.

Pf. ($\Rightarrow$) Suppose f is NOT irred. in $F[x]$. Then

$f(x) = f_1(x) f_2(x)$ for some $f_i(x) \in F[x] \setminus F$. Hence by a lemma that we proved in the previous lecture, $\exists\, c_1, c_2 \in F$,

$$f(x) = \underbrace{(c_1 f_1(x))}_{\text{in } D[x]} \underbrace{(c_2 f_2(x))}_{\text{in } D[x]}.$$

So $f(x)$ is not irreducible in $D[x]$ as $\deg(c_i f_i(x)) \neq 0$.

($\Leftarrow$) Suppose $f(x) = f_1(x) f_2(x)$ for some $f_i(x) \in D[x]$. Since $f(x)$ is irred. in $F[x]$, either $\deg f_1 = 0$ or $\deg f_2 = 0$. If $\deg f_i = 0$, then f_i is a common divisor of all the coeff. of f. Since f is primitive, we deduce that $f_i \in D^\times$. ∎

Lecture 04: ==>

Friday, January 12, 2018 1:03 AM

Proof of D: UFD $\Rightarrow$ $D[x]$: UFD.

Existence.. If $f(x) \in D\setminus\{0\}$, then f can be written as a prod. of irred. in D. But $d \in D$ is irred $\Leftrightarrow$ d is irred. in $D[x]$.

- Suppose $f(x) \in D[x]\setminus D$. Then $f(x) = c_f \bar{f}(x)$ where $\bar{f}(x)$ is primitive. Let F be the field of fractions of D. Then $F[x]$ is a PID; and so it is a UFD. So $\exists\, p_i(x) \in F[x]$ that irred. and $f(x) = c_f \cdot p_1(x) \cdots\cdots p_m(x)$. By a Lemma proved in the previous lecture $\exists\, c_i \in F$ s.t. $f(x) = c_f \cdot \underbrace{(c_1 p_1(x))}_{\text{in } D[x]} \cdots\cdots \underbrace{(c_m p_m(x))}_{\text{in } D[x]}$

Let $\bar{p}_i(x) = c_i\, p_i(x)$. So $\bar{f} = \bar{p}_1 \cdot \bar{p}_2 \cdots\cdots \bar{p}_m$. Since $\bar{f}$ is primitive, $\forall i$, $\bar{p}_i$ is primitive. Since $\bar{p}_i = c_i\, p_i$ and p_i is irre. in $F[x]$, $\bar{p}_i$ is irred. in $F[x]$.

As $\bar{p}_i$ is primitive and irr. in $F[x]$, $\bar{p}_i$ is irr. in $D[x]$.

As D is a UFD, c_f can be written as a prod. of irredu.

And the claim follows.

Uniq. Suppose $p(x) \in D[x]$ is irred. If $\deg p = 0$, then p is irred. in D. $\Rightarrow$ p is prime in D $\Rightarrow$ $pD \in \operatorname{Spec}(D)$

Lecture 04: ==> uniqueness

Friday, January 12, 2018 1:20 AM

$\Rightarrow p D[x] \in \mathrm{Spec}(D[x]) \Rightarrow p$ is prime in $D[x]$.

<u>Case 2.</u> $\deg p \geq 1$.

$$\left.\begin{array}{l} \cdot\, p(x) = c(p)\, \bar{p}(x) \\ \bar{p}(x) \notin D[x]^\times \\ p(x) \text{ irred} \end{array}\right\} \Rightarrow c(p) \in D^\times \Rightarrow p: \text{primitive}.$$

$$\left.\begin{array}{l} \cdot\, p: \text{primitive} \\ p: \text{irred. in } D[x] \end{array}\right\} \Rightarrow p: \text{irr. in } F[x]$$

$$\Rightarrow p: \text{prime in } F[x]$$

$$\left.\begin{array}{l} p(x) \mid f(x)\, g(x) \\ f, g \in D[x] \end{array}\right\} \Rightarrow p(x) \mid f(x) \text{ or } p(x) \mid g(x) \text{ in } F[x].$$

w.l.o.g. $f(x) = p(x)\, q(x)$ for some $q(x) \in F[x]$.

$\Rightarrow$ clearing the denom. (This is an alternative route)

$$c\, f(x) = p(x)\, \bar{q}(x) \quad \text{where } \bar{q}(x) \in D[x]$$

$\Rightarrow$ By Gauss's lemma

$$c\, c(f) \sim c(p)\, c(\bar{q}) \sim c(\bar{q}).$$

$\Rightarrow \quad f(x) = p(x)\, \tilde{q}(x)$ for some $\tilde{q}(x) \in D[x]$

$\Rightarrow \quad p(x) \mid f(x)$ in $D[x]$.

So any irred. is prime. Hence we deduce the uniqueness. ∎

In class we proved the following:

Lecture 04: extra property of primitive polynomials

Wednesday, January 17, 2018 2:15 PM

<u>Lemma.</u> Let D be a UFD, and F be its field of fractions. Suppose $f(x) \in D[x]$ is primitive. Then

$$\{c \in F \mid c\, f(x) \in D[x]\} = D.$$

<u>Pf.</u> It is clear that $D f(x) \subseteq D[x]$.

- Now suppose $\frac{a}{b} f(x) = g(x) \in D[x]$. Then $a\, f(x) = b\, g(x)$. Since f is primitive, a is a gcd of coeff. of $\underline{a\, f(x)}$. Hence

$$\left.a = \underbrace{u}_{\text{a unit}}\ b\ \underbrace{c_g}_{\text{a gcd of coeff. of } g}\right\} \Rightarrow \frac{a}{b} = u\, c_g \in D.$$

(if $a=0$, there is nothing to prove.) ∎