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

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

**Proof.** ($\Rightarrow$) $d = ab \Rightarrow \deg d = \deg a + \deg b$

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

$\Rightarrow a, b \in D$ and $d = ab \Rightarrow$ either $a \in D^\times$ or $b \in D^\times$

$d$ is irr. in $D$ $\iff$ either $a \in D[x]^\times$ or $b \in D[x]^\times$.

($\Leftarrow$) $d = ab \Rightarrow$ either $a \in D[x]^\times$ or $b \in D[x]^\times$.

$a, b \in D$ $\Rightarrow$ either $a \in D^\times$ or $b \in D^\times$ as $D[x]^\times = D^\times$. $\blacksquare$

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

**Proof.** (existence) $\forall d \in D \setminus \{0\}$, $d = \prod_{i=1}^{m} p_i(x)$ and $p_i(x)$ are irreducible in $D[x]$.

$\deg d = \sum \deg p_i \Rightarrow \forall i$, $\deg p_i = 0 \Rightarrow \forall i, p_i \in D$.

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

Uniqueness. Suppose $p_i$'s and $q_j$'s are irreducible 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 irreducible in

$$D[x].$$ As $D[x]$ is a UFD, $m = n$ and $q_{o_1} = p_{o_1}$ for some permutation $o$.

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

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

Proposition 2. Suppose $D$ is an integral domain; and any irreducible element is prime. Then a decomposition to irreducible 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.
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 irreducible in $F[x]$.

Proof. ($\Rightarrow$) Suppose $f$ is not irreducible 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, $\exists c_1, c_2 \in F$, $f(x) = (c_1 f_1(x)) (c_2 f_2(x))$. So $f(x)$ is not irreducible in $D[x]$ as $\deg (c_1 f_1(x)) \neq 0$.

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

Since $f$ is primitive, we deduce that $f_1 \in D^*$. $\square$
Proof of \( D : \text{UFD} \implies \text{Dix} : \text{UFD} \):

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 \( \iff d \) is irred. in \( \text{Dix} \).

Suppose \( f(x) \in \text{Dix} \setminus D \). Then \( f(x) = c_{f} \cdot \overline{f}(x) \) where \( \overline{f}(x) \) 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 \( p(x) = c_{f} \cdot p_{1}(x) \cdots p_{m}(x) \). By a Lemma proved in the previous lecture \( \exists c_{i} \in F \) s.t. \( \overline{f}(x) = c_{1} \cdot (c_{1} \cdot p_{1}(x)) \cdots (c_{m} \cdot p_{m}(x)) = c_{f} \cdot \overline{p}_{1} \cdots \overline{p}_{m} \) in \( \text{Dix} \) in \( \text{Dix} \).

Let \( \overline{p}_{i}(x) = c_{i} \cdot p_{i}(x) \). So \( \overline{f} = \overline{p}_{1} \cdot \overline{p}_{2} \cdots \overline{p}_{m} \). Since \( \overline{f} \) is primitive, \( \forall i, \overline{p}_{i} \) is primitive. Since \( \overline{p}_{i} = c_{i} \cdot p_{i} \) and \( p_{i} \) is irre. in \( \text{Dix} \), \( \overline{p}_{i} \) is irre. in \( F[x] \).

As \( \overline{p}_{i} \) is primitive and irre. in \( F[x] \), \( \overline{p}_{i} \) is irre. in \( \text{Dix} \).

As \( D \) is a UFD, \( c_{f} \) can be written as a prod. of irredu.

And the claim follows.

Uniq. Suppose \( p(x) \in \text{Dix} \) is irre. If \( \deg p = 0 \), then \( p \) is irre. in \( D \) \( \Rightarrow p \) is prime in \( D \) \( \Rightarrow p D \in \text{Spec}(D) \)
Lecture 04: \( \implies \) uniqueness

Friday, January 12, 2018 1:20 AM

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

**Case 2.** \( \deg p \geq 1 \).

\[ p(x) = c(p) \bar{f}(x) \Rightarrow c(p) \in D^x \implies p : \text{primitive}. \]

\[ \bar{f}(x) \in D[x] \]

\[ p(x) \text{ irreducible} \]

\[ \cdot p : \text{primitive} \quad \Rightarrow \quad p : \text{irreducible in } D[x] \]

\[ p(x) | f(x) g(x) \quad \Rightarrow \quad p(x) | f(x) \text{ or } p(x) | g(x) \]

\[ f, g \in D[x] \]

\[ \text{in } F[x]. \]

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

\[ \Rightarrow \text{clearing the denom.} \quad \text{(This is an alternative route.)} \]

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

\[ \Rightarrow \text{By Gauss's lemma} \]

\[ c \cdot c(f) \sim c(p) \cdot c(q) \sim c(\bar{q}) \cdot \]

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

\[ \Rightarrow p(x) | f(x) \text{ in } D[x]. \]

So any irreducible is prime. Hence we deduce the

uniqueness. \( \blacksquare \)

In class we proved the following:
Lemma. Let $D$ be a UPD, and $F$ be its field of fractions. Suppose $f(x) \in D[x]$ is primitive. Then

$$\exists c \in F \mid c \cdot f(x) \in D[x]$$

Proof. It is clear that $Df(x) \subseteq D[x]$. Now suppose $\frac{a}{b} \cdot f(x) = g(x) \in D[x]$. Then $a \cdot f(x) = b \cdot g(x)$. Since $f$ is primitive, $a$ is a gcd of coeff. of $\frac{a}{b} \cdot f(x)$. Hence

$$a = u \cdot b \cdot c \cdot g$$

$u$ a unit, $c$ a gcd of coeff. of $g$.

$$\Rightarrow \frac{a}{b} = u \cdot c \cdot g \in D.$$

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