Theorem. PID $\Rightarrow$ UFD.

Proof. Existence. We considered the following process:

1. If $d$ is irreducible, we are done
2. If not, $d = d_1 d_1'$ and $d_1, d_1'$ are non-zero, non-unit
3. Repeat for $d_1$ and $d_1'$.

If this process stops, we are done. If not, $\exists d_1, d_1' \in D$ st.
$d_1, d_1'$ are non-zero non-units and

$d = d_1 d_1', \ d_1 = d_2 d_2', \ d_2 = d_3 d_3', \ldots$. Hence

$\langle d \rangle \not\subseteq \langle d_1 \rangle \not\subseteq \langle d_2 \rangle \not\subseteq \ldots$. Let $I := \bigcup_{i=1}^{\infty} \langle d_i \rangle$.

Claim. $I \subset D$.

Proof of claim. We use ideal criterion; $x, y \in I, a \in D$,

$\Rightarrow x \in \langle d_i \rangle$ and $y \in \langle d_j \rangle$ for some $i, j \in \mathbb{Z}^+$. W.L.O.G. let's assume $i \leq j$. Hence $xy \in \langle d_j \rangle$, and so $x - y \in \langle d_j \rangle \subseteq I$.

Hence $x - y \in I$. We also have $ax \in \langle d_i \rangle \subseteq I$; and claim follows.
Lecture 23: PID implies UFD

Since \( D \) is a PID, \( \exists d' \in D, \ I = \langle d' \rangle \).

Hence \( \exists i \) s.t. \( d' \in \langle d_i \rangle \), which implies \( I = \langle d' \rangle \subseteq \langle d_i \rangle \).

And so for any \( i \leq j \), \( I \subseteq \langle d_j \rangle \subseteq I \); and this implies \( \langle d_j \rangle = I \) if \( i \leq j \); in particular \( \langle d_i \rangle = \langle d_{i+1} \rangle \) which is a contradiction. \( \square \)

**Uniqueness. What does it mean?**

Suppose \( p_i \)'s and \( q_j \)'s are irreducible, and

\[ p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m. \]

Then \( m = n \), and there is a reordering \( i_1, \ldots, i_n \) of \( 1, \ldots, n \) and units \( u_j \) s.t.

\[ p_j = u_j \cdot q_{i_j} \quad \text{for any } 1 \leq j \leq n. \]

We proceed by induction on \( n \).

\[ p_1 \cdots p_n \in \langle p_n \rangle \Rightarrow q_1 \cdots q_m \in \langle p_n \rangle \]

\( p_n \): irreducible \( \Rightarrow \langle p_n \rangle \): maximal \( \Rightarrow \langle p_n \rangle \): prime \( \quad \)

\( D \): PID \( \quad \)

for some \( i, \ q_i \in \langle p_n \rangle. \)
Hence \( \langle q_i \rangle \subseteq \langle p_n \rangle \) \( \iff \langle q_i \rangle = \langle p_n \rangle \) \( q_i \) : irreducible \( \iff \langle q_i \rangle \) is maximal \( \forall [i] \) which implies \( p_n = q_n q_i \) for some \( \nu_n \in \mathcal{D}^* \).

And so \( p_1 \cdots p_{n-1} p_n = q_1 \cdots q_m \) implies

\[
P_1 \cdots P_{n-1} \cdot \nu_n q_i = q_1 \cdots q_i q_i q_{i+1} \cdots q_m.
\]

Hence

\[
P_1 \cdots P_{n-1} \cdot \nu_n = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m
\]

\( p_1, p_2, \ldots, p_{n-1}, \nu np_n \) are irreducible in \( \mathcal{D} \); and so by the induction hypothesis \( m-1 = n-1 \) (which implies \( n=m \)); and \( p_1, \ldots, p_{n-2}, \nu np_n \) are the same as \( q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_m \) up to reordering and multiplying by units; and claim follows. 

Next we go back to the study of zeros of a polynomial. We will show any poly. \( p(x) \in \mathbb{F} \) has a zero in some field extension.
Theorem. Suppose $F$ is a field and $f(x) \in F[x]$ is an irreducible polynomial. Then

1. There exists a field $E$ and an injective ring homomorphism $i : F \rightarrow E$ such that:
   
   (1-a) for some $\alpha \in E$, $i(f)(\alpha) = 0$.
   
   (1-b) $E = \{ i(a_0) + i(a_1) \alpha + \ldots + i(a_{n-1}) \alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in F \}$

   where $n = \deg f$.

2. If $E'$ is a field and $i' : F \rightarrow E'$ is an injective ring homomorphism that satisfy (1-a) and (1-b), then there exists a homomorphism $\phi : E \rightarrow E'$ such that $\phi(i(a)) = i'(a)$ for any $a \in F$.

\[ \begin{array}{c}
F \xrightarrow{i} E \xrightarrow{\phi} E' \\
\phi \downarrow \\
F \xrightarrow{i'} E'
\end{array} \]

Idea of pf. Suppose $E$ is a field, and $\alpha \in E$ is a zero of $f(x)$. Then kernel of $\phi : E[x] \rightarrow E$, $\phi(p(x)) = p(\alpha)$ contains $f(x)$. Since $f(x)$ is irreducible, we have seen that $\text{ker} \phi = \langle f(x) \rangle$; and
Im φ₁ is a field; and \( \mathbb{F}[x]/\langle f(x) \rangle \sim \text{Im } \phi_α \). In particular,

\[
\phi_α + \langle f(x) \rangle \mapsto \phi_α
\]

\( x + \langle f(x) \rangle \mapsto x \).

So it seems we are forced to think about \( \mathbb{F}[x]/\langle f(x) \rangle \).