We have seen that \( \mathbb{Z} \) and \( \mathbb{F}[x] \) are both PIDs. And you know that in \( \mathbb{Z} \) any number can be written as a product of primes in a unique way (up to reordering). We will show the uniqueness for any PID.

**Definition.** An integral domain \( D \) is called a **Unique Factorization Domain** if any \( a \in D \), which is not either 0 or a unit, can be written as a product of irreducibles in \( D \) in a unique way (up to reordering and multiplying by a unit).

Before we get to the proofs, let's understand what “up to reordering and multiplying by a unit” means; consider \( x(x+1) \) in \( \mathbb{Q}[x] \). Notice that it can be written as \( (2x+2)(\frac{x}{2}) \), and any degree 1 polynomial is irreducible in \( \mathbb{Q}[x] \). This does not violate the uniqueness that we are looking for as after reordering we get \( (\frac{x}{2})(2x+2) \); and now the
factors differ only by a unit: $\frac{a}{2} = \frac{1}{2} \cdot a$ and $2x + 2 = 2(x + 1)$
and $2, \frac{1}{2} \in \mathcal{U}(\mathbb{Q}[x])$.

**Theorem** If $\mathcal{D}$ is a PID, then $\mathcal{D}$ is a UFD.

**Existence** First we prove that $\mathfrak{a}$ can be written as a product of irreducibles if $\mathfrak{a} \neq 0$ and $\mathfrak{a} \not\in \mathcal{U}(\mathcal{D})$.

*Why should it be true?* If $\mathfrak{a}$ is irreducible, then we are done.

If not, $\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2$ where $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are not units.

Continue this process for $\mathfrak{a}_1$ and $\mathfrak{a}_2$.

**Question** Why does this process stop?

(For $\mathbb{Z}$, we can use the absolute value; and for $\mathbb{F}[x]$, we can use the degree of polynomials to show this.)

**Proof of existence** (the general case: not part of the exam.)

$$\mathfrak{a} = \{a \in \mathcal{D} | a \neq 0, a \not\in \mathcal{U}(\mathcal{D}), a \text{ cannot be written as a product of irreducibles}\}$$

If $\mathfrak{a}$ is empty, we are done. So suppose to the contrary that $a_0 \in \mathfrak{a}$. Hence, in particular, $a_0$ is not irreducible. So $a_0 = a_1 b_1$
for some \( a_1, b_1 \in D \setminus U(D) \). Since \( D \) is an integral domain and \( a \neq 0 \), we have \( a_1 \) and \( b_1 \) are non-zero. If \( a_1, b_1 \notin A \), then that means \( a_1 \) and \( b_1 \) can be written as a product of irreducibles (as they are not either 0 or a unit). This implies \( a_1 = a_1 b_1 \) can be written as a product of irreducibles, which contradicts \( a_1 \in A \). So either \( a_1 \in A \) or \( b_1 \in A \). Without loss of generality, we can and will assume \( a_1 \in A \). By a similar argument inductively we can find a sequence \( a_1, a_2, \ldots \) of elements of \( D \) such that \( \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots \) and

\[
a_i = a_{i+1} b_{i+1} \quad \text{where} \quad b_{i+1} \notin U(D).
\]

Now let \( I = \bigcup_{i=0}^{\infty} \langle a_i \rangle \). Show that \( I \) is an ideal of \( D \).

Since \( D \) is a PID, \( \exists b \in D \) such that \( I = \langle b \rangle \).

So be \( \bigcup_{i=0}^{\infty} \langle a_i \rangle \), which means \( \exists i_0 \) such that \( b \in \langle a_{i_0} \rangle \).

Therefore \( \langle b \rangle \subseteq \langle a_{i_0} \rangle \Rightarrow \forall i \geq i_0, \langle a_i \rangle \subseteq \langle b \rangle \subseteq \langle a_{i_0} \rangle \)

and \( \langle a_{i_0} \rangle \subseteq \langle a_i \rangle \).

This implies \( \langle a_i \rangle = \langle a_{i_0} \rangle \). Show that \( \langle a_{i_0+1} \rangle = \langle a_{i_0} \rangle \) implies
b. \(x+1\) is a unit which is a contradiction. 

Here we present an alternative proof of the existence part when \(D = \mathbb{F}[x]\). (This proof was presented in class.)

Any non-constant polynomial \(f(x) \in \mathbb{F}[x]\) can be written as a product of irreducible polynomials in \(\mathbb{F}[x]\).

**Proof.** We proceed by the strong induction on \(\deg(f)\).

**Base of induction.** \(\deg(f) = 1\).

Since \(\mathbb{F}\) is a field, any degree 1 polynomial in \(\mathbb{F}[x]\) is irreducible. So \(f(x)\) is irreducible; this implies that \(f(x)\) is already written as a product of irreducible polynomials with only one factor.

**Strong induction step.** Suppose any non-constant polynomial \(g(x)\) of degree \(< k\) is a product of irreducible polynomials. We have to show any polynomial \(f(x)\) of degree \(k\) is a product of irreducible polynomials.
Case 1. \( f(x) \) is irreducible.

In this case, \( f(x) \) is already written as a product of irreducible polynomials, with only one factor.

Case 2. \( f(x) \) is NOT irreducible.

In this case, as \( f(x) \) is not a constant polynomial, we can write \( f(x) \) as a product of two non-constant polynomials \( g(x) \) and \( h(x) \).

Since \( f(x) = g(x)h(x) \) and \( g(x), h(x) \) are not constant, we have \( \deg g, \deg h < \deg f = k \).

So, by the strong induction hypothesis, \( g(x) \) and \( h(x) \) are products of irreducible polynomials; that means there are irreducible polynomials \( p_1(x), \ldots, p_n(x) \) and \( q_1(x), \ldots, q_m(x) \in F[x] \), such that \( g(x) = p_1(x) \cdots p_n(x) \) and \( h(x) = q_1(x) \cdots q_m(x) \). Thus \( f(x) = g(x)h(x) = p_1(x) \cdots p_n(x)q_1(x) \cdots q_m(x) \), which means \( f(x) \) can be written as a product of irreducible polynomials.
To prove uniqueness we prove the following lemma:

**Lemma.** Let $D$ be a PID. Suppose $p \in D$ is irreducible. If $a_1a_2\ldots a_n \in \langle p \rangle$, then, for some $i$, $a_i \in \langle p \rangle$.

**Proof.** We proceed by induction on $n$. If $n=1$, there is nothing to show.

**Inductive Step.** Suppose $a_1a_2\ldots a_{k+1} \in \langle p \rangle$.

Since $p$ is irreducible and $D$ is a PID, $\langle p \rangle$ is a maximal ideal. Hence $\langle p \rangle$ is a prime ideal. So $(a_1a_2\ldots a_k)a_{k+1} \in \langle p \rangle$

implies either $a_1a_2\ldots a_k \in \langle p \rangle$ or $a_{k+1} \in \langle p \rangle$.

If $a_{k+1} \in \langle p \rangle$, we are done;

If $a_1a_2\ldots a_k \in \langle p \rangle$, then by the induction hypothesis $a_i \in \langle p \rangle$ for some $1 \leq i \leq k$; and the claim follows.  

A bit less formal, but more clear argument:

Since $p$ is irreducible and $D$ is a PID, $\langle p \rangle$ is a maximal ideal of $D$. So $D/\langle p \rangle$ is a field. Since $a_1a_2\ldots a_n \in \langle p \rangle$, ...
we have \((a_1 + \langle p \rangle) \cdot (a_2 + \langle p \rangle) \cdots (a_n + \langle p \rangle) = a_1 a_2 \cdots a_n + \langle p \rangle = 0 + \langle p \rangle\)

is zero in \(D/\langle p \rangle\). In a field, if product of \(n\) elements is zero, then one of them is zero. Hence

\[\exists i, \ a_i + \langle p \rangle = 0 + \langle p \rangle,\] which implies \(a_i \in \langle p \rangle\). \(\blacksquare\)

**Lemma.** Suppose \(a, b \in D \setminus \{0\}\).

\(\langle a \rangle = \langle b \rangle\) in an integral domain \(D\) if and only if \(a = ub\) for some \(u \in U(D)\).

**Proof.** \((\Rightarrow)\) \(\langle a \rangle = \langle b \rangle \Rightarrow \exists u, v \in D\), \(a = ub\) and \(b = va\).

So \(a = uv\ a\). As \(a \neq 0\) and \(D\) has the cancellation laws, we have \(1 = uv\). Therefore \(u \in U(D)\) and \(a = ub\).

\((\Leftarrow)\) \(a = ub \Rightarrow \langle a \rangle \subseteq \langle b \rangle\)

\[a = ub \Rightarrow b = u^{-1}a \Rightarrow \langle b \rangle \subseteq \langle a \rangle\]

\(u \in U(D)\) \(\blacksquare\)
Lemma. Suppose \( D \) is a PID and \( p \) is irreducible in \( D \), and \( q \in \mathcal{D} \) is not a unit in \( D \). Then

\[ p \in \langle q \rangle \iff \exists u \in U(\mathcal{D}), \; p = qu \iff \langle p \rangle = \langle q \rangle ; \]

and in this case \( q \) is irreducible.

Proof. \( p \in \langle q \rangle \Rightarrow \exists a \in \mathcal{D} \) such that \( p = qa \).

Since \( p \) is irreducible, either \( q \) is a unit or \( a \) is a unit.

By the assumption \( q \) is not a unit, so \( a \in U(\mathcal{D}) \).

- If \( p = qu \), then \( p \in \langle q \rangle \).

- By the previous lemma, \( \exists u \in U(\mathcal{D}), \; p = qu \iff \langle p \rangle = \langle q \rangle \).

Suppose \( p \) and \( q \) are above. Then

Since \( p \) is irreducible in \( D \) and \( D \) is a PID, \( \langle p \rangle \) is a maximal ideal. Therefore \( \langle q \rangle \) is a maximal ideal of \( D \).

Since \( D \) is a PID and \( \langle q \rangle \) is a maximal ideal, \( q \) is irreducible in \( D \). \[ \square \]

Exercise. Show that the above lemma is still true when \( D \) is only an integral domain.
Lemma. Let $q_1, p_1, ..., p_n$ be irreducibles in a PID. Then $p_1 ... p_n \in \langle q \rangle$ implies $q = u p_i$ for some $1 \leq i \leq n$ and $u \in U(D)$.

Proof. By one of Lemmas, $\exists i$ such that $p_i \in \langle q \rangle$. So $\langle p_i \rangle \subseteq \langle q \rangle$. Since $p_i$ is irreducible and $D$ is a PID and $q$ is not a unit of $D$, by the previous lemma $q = u p_i$ for some $u \in U(D)$. ■

Lemma. Suppose $D$ is a PID, $q_1, ..., q_m$, $p_1, ..., p_n$ are irreducible in $D$, and $q_1 ... q_m = p_1 ... p_n$. Then

1. $m = n$
2. $q_1 = u_1 p_{i_1}$, $q_2 = u_2 p_{i_2}$, ..., $q_m = u_m p_{i_m}$ where $i_1, ..., i_m$ is a permutation of $1, ..., m$; and $u_i \in U(D)$.

Proof. We prove it by induction on $m$.

Base of induction. $m = 1$. Then

$q_1 = p_{i_1}$, $\Rightarrow$

$p_1 ... p_n \in \langle q_1 \rangle \Rightarrow \exists i_1$ and $u_1 \in U(D)$ s.t. $q_1 = p_{i_1} u_1$.

$\Rightarrow$ by the cancellation law, $p_1 ... p_{i_1-1} u_1 p_{i_1+1} ... p_n = 1$

which implies $p_j$'s are units for $j \neq i_1$. This is not possible, unless $n = 1$. When $n = 1$, we get $q_1 = p_{i_1}$. 
The induction step.

\[ q_1 q_2 \ldots q_{m+1} = p_1 p_2 \ldots p_n \Rightarrow p_1 p_2 \ldots p_n \in \langle q_{m+1} \rangle \]

There exists \( q_{m+1} \) and \( u_{m+1} \in U(D) \) such that

\[ q_{m+1} = u_{m+1} p_{i_{m+1}}. \]

Therefore

\[ q_1 q_2 \ldots q_m u_{m+1} p_{i_{m+1}} = p_1 p_2 \ldots p_n. \]

By the cancellation law we get

\[ q_1 q_2 \ldots q_m = (u_{m+1}^{-1} p_1) p_2 \ldots p_{i_{m+1}-1} p_{i_{m+1}} \ldots p_n. \]

Since \( p_1 \) is irreducible in \( D \) and \( u_{m+1}^{-1} \in U(D) \), by one of the lemmas \( u_{m+1}^{-1} p_1 \) is irreducible in \( D \).

Now by the induction hypothesis, \( m = n-1 \); and there are \( i_1, \ldots, i_m \) (a reordering of \( i_1, \ldots, n \) \( \setminus \{ i_{m+1} \} \)) and \( u_1', u_2', \ldots, u_m \in U(D) \) such that

\[ q_1 = u_1' u_{m+1}^{-1} p_1, \quad q_2 = u_2 p_{i_2}, \ldots, q_m = u_m p_{i_m}. \]

Notice that, since \( U(D) \) is a group and \( u_1', u_{m+1} \in U(D) \), \( u_1' u_{m+1}^{-1} \in U(D) \). Let \( u_1 = u_1' u_{m+1}^{-1} \). So \( q_j = u_1' p_{j_1} \) for \( 1 \leq j \leq m+1 \); and the claim follows.