Content:

Theorem	Correspondence Theorem for Rings. Let $I \subset R$, I an ideal. Then there is an inclusion preserving bijection φ from $S = \{J \mid J \text{ ideal in } R, I \subseteq J\}$ to $T = \{K \mid K \text{ ideal in } R/I\}$.
Proposition	J maximal $\Leftrightarrow$ J/I is maximal in R/I.
Proposition	J prime $\Leftrightarrow$ J/I is prime in R/I.
Definition	UFD
Example	$\mathbb{Z}, \mathbb{R}[x], \mathbb{R}, \mathbb{Z}[x]$ are UFDs.
Goal	Every PID is a UFD.
Lemma 1	In an integral domain in which criteria (1) for UFD is satisfied, then R is a UFD $\Leftrightarrow$ (p) is prime for all irreducible elements p.
Lemma 2	(1) If R is a commutative ring with unity and $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ is an ascending chain of ideals in R, then $\cup_{n\geq 1} I_n$ is an ideal in R. (2) If R is a PID, then it has no infinitely strictly increasing chain of ideals. (3) If R is a PID and $r \in R$, $r \neq 0$, $r \notin U(R)$, then r is a product of irreducibles.

Theorem **Correspondence Theorem for Rings.**
Let $I \subset R$, I an ideal. Then there is an inclusion preserving bijection φ from $S = \{J \mid J \text{ ideal in } R, I \subseteq J\}$ to $T = \{K \mid K \text{ ideal in } R/I\}$.

Proof:
Let $I \subset R$, I an ideal.
Define $\pi : R \to R/I$ by $\pi(x) = x + I$.
Define $\varphi: S \to T$ by $\varphi(J) = J/I$.
From the group correspondence theorem, φ is injective.

Recall-
Let $H, J \in S$ such that $\varphi(H) = \varphi(J)$. Then $H/I = J/I$.
Let $a \in H$. Then $\pi(a) = a + I \in H/I = J/I$.
Since π is surjective, $\exists\, b \in J$ such that $\pi(b) = b + I = a + I = \pi(a)$.
Thus, $b - a \in I$. Hence, $b - a \in J$ (since $I \subseteq J$).
And since $b \in J$, we have $-b + b - a = -a \in J$, hence $a \in J$. $\therefore$ $H \subseteq J$.
By symmetric proof, we have $J \subseteq H$, so $H = J$ as desired.
$\therefore$ φ is injective.

So we need only check that it is surjective.
Let $K \in T$. Then K is an ideal in R/I, hence $\pi^{-1}(K)$ is an ideal.

Since $\pi : R \to R/I$ is surjective, then $\exists\, J \in R$ such that $\pi(J) = K$.
Since $0 + I \in K$, and $\pi(0) = 0 + I \in K$, then $0 \in J \neq \emptyset$.
If $x, y \in J$, then $\pi(x - y) = \pi(x) - \pi(y) \in K$ as K is an ideal.
So $x - y \in J$. Thus, $J \subseteq_{\text{subring}} R$.
If $r \in R$, then $\pi(xr) = \pi(x)\pi(r) \in K$, so $xr \in J$. Thus, $J = \pi^{-1}(K)$ is an ideal.

And, finally we show $I \subseteq \pi^{-1}(K)$.
Let $a \in I$. Then $\pi(a) = a + I = 0 + I \in K$, as K is an ideal.
So $a \in \pi^{-1}(K)$. $\therefore$ $I \subseteq \pi^{-1}(K)$.
$\therefore$ φ is surjective.
$\therefore$ φ is a bijection from S to T.

Proposition J is a maximal ideal in $R \Leftrightarrow J/I$ is maximal in R/I.

Proof:
You do it.
Let I be a proper ideal in R.
Assume J is a maximal ideal in R. Then $I \subseteq J$.
Let K' be an ideal in R/I such that $J/I \subseteq K'$.
Then by the Correspondence Theorem for rings,
$\exists\ K \subseteq R$ such that $J \subseteq K$ and $K' = K/I$.
Since J is maximal, then $J = K$ or $K = R$.
Thus, $J/I = K'$ or $K' = R/I$.
$\therefore\ J/I$ is maximal in R/I.

Conversely, assume J/I is a maximal ideal in R/I where $I \subseteq J \subseteq R$.
Define $\pi : R \to R/I$ by $\pi(r) = r + I$.

We will show $I \subseteq J \Rightarrow \pi^{-1}(J/I) = J$ (i.e. $I \subseteq J \Rightarrow \pi: R \to R/I$ is injective).
Note that $\pi(J) = J/I$.
We know $J \subseteq \pi^{-1}(\pi(J))$ by basic set theory.
To show the reverse inclusion, let $a \in \pi^{-1}(\pi(J))$.
Then $\pi(a) = \pi(j)$ for some $j \in J$.
So $a + I = j + I$, hence $a - j + I = 0 + I$, which gives us $a - j \in I$.
Since $I \subseteq J$, then $a - j \in J$. And since $j \in J$, then $a = a - j + j \in J$.
Thus $\pi^{-1}(\pi(J)) \subseteq J$, hence $J = \pi^{-1}(\pi(J))$.

We now will show J is an ideal in R.
By homomorphism properties we have the following:
$0 \in J = \pi^{-1}(J/I)$ as $0 + I \in J/I$. So $J \neq \varnothing$.
If $x, y \in J$, then $\pi(x - y) = \pi(x) - \pi(y) \in J/I$, hence $x - y \in J$.
If $x \in J$ and $a \in R$, then $\pi(xa) = \pi(x)\pi(a) \in J/I$, hence $xa \in J$.
$\therefore\ J$ is an ideal in R.

And lastly we will show J is maximal.
Let K be an ideal in R that contains J.
Then by the Correspondence Theorem for rings,
$\exists\ K'$, an ideal in R/I such that $J/I \subseteq K'$ and $K' = K/I$.
Since J/I is maximal, then $J/I = K'$ or $K' = R/I$. So $J = K$ or $K = R$.
$\therefore\ J$ is a maximal ideal in R.

Proposition Suppose I is a proper ideal in R and $I \subseteq J \subset R$.
Then J is a prime ideal in $R \Leftrightarrow J/I$ is a prime ideal in R/I.

Proof:
Let I be a proper ideal in R.
Suppose $(a + I)(b + I) = ab + I \in J/I$.
We know $ab \in J$, so $a \in J$ or $b \in J$.
Hence $a + I \in J/I$ or $b + I \in J/I$.
$\therefore$ J/I is a prime ideal in R/I.

Conversely, assume J/I is a prime ideal in R/I where $I \subseteq J \subseteq R$.
Done in HW #3, Exercise 6.5.
Define $\pi : R \to R/I$ by $\pi(r) = r + I$.
We will show $I \subseteq J \Rightarrow \pi^{-1}(J/I) = J$ (i.e. $I \subseteq J \Rightarrow \pi: R \to R/I$ is injective).
Note that $\pi(J) = J/I$.
We know $J \subseteq \pi^{-1}(\pi(J))$ by basic set theory.
To show the reverse inclusion, let $a \in \pi^{-1}(\pi(J))$.
Then $\pi(a) = \pi(j)$ for some $j \in J$.
So $a + I = j + I$, hence $a - j + I = 0 + I$, which gives us $a - j \in I$.
Since $I \subseteq J$, then $a - j \in J$. And since $j \in J$, then $a = a - j + j \in J$.
Thus $\pi^{-1}(\pi(J)) \subseteq J$, hence $J = \pi^{-1}(\pi(J))$.
We now will show J is an ideal in R.
By homomorphism properties we have the following:
$0 \in J = \pi^{-1}(J/I)$ as $0 + I \in J/I$. So $J \neq \varnothing$.
If $x, y \in J$, then $\pi(x - y) = \pi(x) - \pi(y) \in J/I$, hence $x - y \in J$.
If $x \in J$ and $a \in R$, then $\pi(xa) = \pi(x)\pi(a) \in J/I$, hence $xa \in J$.
$\therefore$ J is an ideal in R.
We now show J is prime.
Suppose $\exists$ $a, b \in R$ such that $ab \in J$. Then $\pi(ab) = \pi(a)\pi(b) \in J/I$.
Thus, $\pi(a) \in J/I$ or $\pi(b) \in J/I$ as J/I is prime.
$\therefore$ $a \in J$ or $b \in J$, hence J is prime.

Definition *Unique Factorization Domain*
Let R be an integral domain. R is a UFD if
(1) Every non-unit, non-zero $r \in R$ is a product of irreducibles.
(2) If $up_1p_2\cdots p_m = vq_1q_2\cdots q_n$ where $u, v \in U(R)$
and p_i and q_i are irreducibles, then
$m = n$ and after re-ordering, p_i and q_i are associates for each i.

Example $\mathbb{Z}, \mathbb{R}[x], \mathbb{R}$, are UFDs.
$\mathbb{Z}[\sqrt{-5}\,]$ is not a UFD.

Goal Every PID is a UFD.

Lemma 1 In an integral domain in which criteria (1) for UFD is satisfied, then R is a UFD $\Leftrightarrow$ (p) is prime for all irreducible elements p.

Proof:
Assume R is a UFD and p is irreducible in R.
Let $ab \in (p)$, then $ab = px$ for some $x \in R$.
Suppose $a = up_1p_2\cdots p_m$ and $b = vq_1q_2\cdots q_n$ where $u, v \in U(R)$ and p_i and q_i are irreducibles.
Since R is a UFD, p is an associate of p_i or q_i.
Thus $p|a$ or $p|b$. So $a \in (p)$ or $b \in (p)$. Thus (p) is a prime ideal.

Conversely, suppose $up_1p_2\cdots p_m = vq_1q_2\cdots q_n$ where $u, v \in U(R)$, p_i and q_i are irreducibles, and (p_i) and (q_i) are prime ideals for each i.
Induct on $\max\{m, n\}$.

If $\max\{m, n\} = 1$, then $up_1 = vq_1$ or $up_1 = v$ or $u = vq_1$.
We know $up_1 \neq v$ and $u \neq vq_1$ as this would imply p_1 is a unit or q_1 is a unit.
So $up_1 = vq_1$ and clearly p_1 is an associate of q_1 (i.e. $m = n$ and p_i and q_i are associates for each i.)

Let $k > 1$ and assume unique factorization criterion (2) holds for all $\max\{m, n\} \leq k$. Note that (p_1) is prime by hypothesis.
So $up_1p_2\cdots p_m = vq_1q_2\cdots q_n \Rightarrow p_1 | vq_1q_2\cdots q_n \Rightarrow vq_1q_2\cdots q_n \in (p_1)$.
So $q_i \in (p_1)$ for some i since (p_1) is a prime ideal.
We know $q_i = p_1x$. Since q_i is irreducible, p_1 or x is a unit.
$p_1 \notin U(R)$ since p_1 is irreducible thus x is a unit.
So q_i and p_1 are associates. Hence $wp_1p_2\cdots p_m = q_1q_2\cdots q_n$.
After cancellation, we have $wp_2\cdots p_m = q_1\cdots \hat{q}_i \cdots q_n$ where
By our induction hypothesis we have $m - 1 = n - 1$. And since we have that q_i and p_1 are associates, we have $m = n$ and after reindexing, p_i and q_i are associates for each i. $\therefore$ R is a UFD.

Lemma 2 (1) If R is a commutative ring with unity and $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$ is an ascending chain of ideals in R, then $J = \cup_{n\geq 1} I_n$ is an ideal in R.

Proof:
p. 329 Read it.
We claim that J is an ideal. If $a \in J$, then $a \in I_n$ for some n.
If $r \in R$, then $ra \in I_n$ as I_n is an ideal. Hence, $ra \in J$.
If $a, b \in J$, then there are ideals I_n and I_m with $a \in I_n$ and $b \in I_m$.
Since the chain is ascending, we may assume that $I_n \subseteq I_m$, and so $a, b \in I_m$.
As I_m is an ideal, $a + b \in I_m$ and, hence, $a + b \in J$. $\therefore$ J is an ideal.

(2) If R is a PID, then it has no infinitely strictly increasing chain of ideals.

Proof:
Assume R is a PID. Suppose we have $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \cdots$
an ascending chain of ideals in R.
Let $J = \cup_{n\geq 1} I_n$. Then by (1) J is an ideal.
Since R is a PID, $\exists\, d \in R$ such that $(d) = J$.
Thus, $d \in J$, hence $d \in I_n$ for some n.
So $J = (d) \subseteq I_n \subsetneq I_{n+1} \subseteq J$, clearly a contradiction.
Hence R has no infinitely strictly increasing chain of ideals.

(3) If R is a PID and $r \in R$, $r \neq 0$, $r \notin U(R)$, then r is a product of irreducibles.

Proof:
Assume R is a PID and $r \in R$, $r \neq 0$, and $r \notin U(R)$.
Suppose r cannot be factored into a product of irreducibles.
Then $r = a_0 b_0$ where $a_0, b_0 \notin U(R)$ and either a_0 cannot be factored into a product of irreducibles or b_0 cannot.
Without loss of generality, suppose it's a_0.
Then $\exists\, a_1, b_1 \notin U(R)$ such that $a_0 = a_1 b_1$ and either a_1 cannot be factored into a product of irreducibles or b_1 cannot. We can continue this process...
Since a_i is not an associate of a_{i+1} for each i, then we have
$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$,
a strictly increasing chain of ideals in R, a contradiction to part (2).
$\therefore$ r is a product of irreducibles.

Summary Our goal was to show every PID is a UFD. By the previous 2 lemmas, we have the result. By Corollary 6.16 (If R is a PID and $p \in R$ is irreducible, then (p) is a prime ideal.), we only need that UFD condition (1) is satisfied and R is a PID to satisfy the consequent "(p) is prime for all irreducible elements p." of Lemma 1.
Lemma 2 gives us condition (1) for any PID, hence we can use Lemma 1 to finish the proof that every PID is a UFD.