Content:

Theorem	R is a commutative ring with unity. I is a prime ideal in $R \Leftrightarrow R/I$ is an integral domain.
Theorem	R is a commutative ring with unity. I is a maximal ideal in $R \Leftrightarrow R/I$ is a field.
Example	$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ so (x) is prime but not maximal.
Corollary	In a commutative ring with unity, maximal $\Rightarrow$ prime.
Example	$(4) \subseteq \{\text{Even integers}\}$ is maximal, but not prime.
Theorem	If R is a PID and $I \neq \{0\}$ is a prime ideal, then I is maximal.
Corollary	R is a commutative ring with unity. If $R[x]$ is a PID then R is a field.
Theorem	R is a PID. $I = (a)$, $a \neq 0$, then I is maximal $\Leftrightarrow$ a is irreducible.
Examples	$(x) \subseteq \mathbb{Z}[x]$ is maximal and x is irreducible.

Announcements 3.6 #64 due Wednesday
Monday no class

Recap ID $\Leftarrow$ UFD $\Leftarrow$ PID $\Leftarrow$ ER
$\not\Rightarrow$ $\not\Rightarrow$ $\not\Rightarrow$

6.1 Prime Ideals and Maximal Ideals

Definition Let R be a commutative ring and I an ideal in R.
(1) I is a *prime ideal* if I is proper and whenever $ab \in I$, we have that $a \in I$ or $b \in I$.
(2) I is a *maximal ideal* if I is proper and whenever $I \subseteq J$, J an ideal we have that $I = J$ or $J = R$.

Example $(4) \subseteq \mathbb{Z}$ is not prime as $2 \bullet 2 \in (4)$ but $2 \notin (4)$ and is not maximal as $(4) \subset (2)$.

Example $(x) \subseteq \mathbb{Z}[x]$ is prime but is not maximal (as $(x) \subset (x, 2)$).

Note If $I = (a) \neq (0)$, then I is a prime ideal $\Leftrightarrow$ a is a prime element.

Example (0) is a maximal ideal in a field.
(0) is a prime ideal in an integral domain.

Theorem Let R be a commutative ring with unity.
Then I is a prime ideal in $R \Leftrightarrow R/I$ is an integral domain.
Proof:
Assume I is a prime ideal. Let $a, b \in R$ such that $(a + I)(b + I) = 0 + I$.
Then $ab + I = 0 + I$. Thus $ab \in I$. Since I is prime, then $a \in I$ or $b \in I$.
Thus, $a + I = 0 + I$ or $b + I = 0 + I$.
$\therefore$ R/I is an integral domain.
Conversely, Assume R/I is an integral domain.
Let $ab \in I$, $a, b \in R$. Then $ab + I = 0 + I$. So $(a + I)(b + I) = 0 + I$.
Since R/I is an integral domain, then $a + I = 0 + I$ or $b + I = 0 + I$.
Thus, $a \in I$ or $b \in I$. So I is a prime ideal.

Theorem Let R be a commutative ring with unity.
Then I is a maximal ideal in $R \Leftrightarrow R/I$ is a field.
Proof:
Assume I is maximal. Let $a + I \in R/I$ such that $a + I \neq 0 + I$.
Let $J = \{m + ar | m \in I, r \in R\}$. Note that $J \subseteq R$.
It's a quick check that J is an ideal in R.
Since I is maximal and $I \subseteq J$, then $I = J$ or $J = R$.
Since $a + I \neq 0 + I$, then $a \notin I$. So $I \neq J$. $\therefore$ $J = R$.
So $1 \in J$. So $1 = m_0 + ar_0$ for some $m_0 \in I$, $r_0 \in R$.
$(a + I)(r_0 + I) = ar_0 + I = ar_0 + m_0 + I = 1 + I$.
Thus $(a + I)^{-1} = r_0 + I$.
Conversely, assume R/I is a field.
Let J be an ideal such that $I \subseteq J$.
Suppose $I \neq J$. Let $a \in J$ such that $a \notin I$.
Then $a + I \neq 0 + I$. Since R/I is a field, $\exists$ $b \in R$ such that
$(a + I)(b + I) = 1 + I$.
So $ab - 1 \in I \subseteq J$. But $ab \in J$ since $a \in J$. Thus $1 \in J$. So $R = J$.

Example $(x) \subseteq \mathbb{Z}[x]$ and $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, an integral domain, but not a field.
So (x) is prime but not maximal.

Note I is maximal $\Rightarrow R/I$ is a field $\Rightarrow R/I$ is an integral domain $\Rightarrow I$ is prime.

Corollary In a commutative ring with unity, maximal $\Rightarrow$ prime.

Example $(4) \subseteq \mathbb{E}$ (Even integers). (4) is not prime, but (4) is maximal.
This is because $\mathbb{E}$ has no unity.

Note In $\mathbb{Z}[x]$ we don't have a division algorithm and is not a PID.
In $k[x]$, k a field, we do have a division algorithm.

Theorem If R is a PID and I is a non-zero prime ideal, then I is maximal.
Proof:
Assume $I \neq \{0\}$ and is a prime ideal in R.
Suppose $I \subseteq J$ where J is an ideal in R.
Since R is a PID, then $\exists\, b \in R$ such that $J = (b)$.
Similarly $\exists\, a \in R$ such that $I = (a)$.
And $(a) = I \subseteq J = (b) \Rightarrow b|a$. So $a = bq$ for some $q \in R$.
Thus $bq \in I$, hence $b \in I$ or $q \in I$.
If $b \in I$, then $J \subseteq I$ (as $a|b \Rightarrow (b) \subseteq (a)$). Hence $J = I$.
If $q \in I$, then $q = as$, for some $s \in R$. So $a = bq = bas$.
Thus $1 = bs \in J$. So $J = R$.

Corollary R is a commutative ring with unity. If $R[x]$ is a PID then R is a field.
Proof:
$R[x]$ is a PID $\Rightarrow R[x]$ has no zero divisors.
$\Rightarrow R$ has no zero divisors.
$\Rightarrow R$ is an integral domain.
$R[x]/(x) \cong R$, so (x) is a prime ideal, so (x) is maximal.
And since (x) is maximal, $R[x]/(x) \cong R$ is a field.

Theorem If R is a PID, $I = (a)$, and $a \neq 0$, then I is maximal $\Leftrightarrow$ a is irreducible.
Proof:
Assume I is maximal in R and $I = (a)$.
Suppose $a = bc$ for some $b, c \in R$. Then $b|a$, hence $a \in (b)$.
So $I \subseteq (b)$. Since I is maximal, then $I = (b)$ or $(b) = R$.
If $(b) = R$, then $1 = bx$, $x \in R$. So $b \in U(R)$.
If $I = (b)$, then a and b are associates.
$\therefore$ $a = bu$, $u \in U(R)$. So $bc = bu$, hence $c = u$. So $c \in U(R)$.
Thus, a is irreducible.
Conversely, assume a is irreducible.
Suppose $I \subseteq J$ where J is an ideal in R.
Since R is a PID, then $J = (b)$, $b \in R$.
$a \in J$, so $b|a$. Thus, $a = bq$, $q \in R$.
Since a is irreducible, $b \in U(R)$ or $q \in U(R)$.
If $b \in U(R)$, then $J = R$.
If $q \in U(R)$, then a and b are associates, hence $I = J$.

Example $(x) \subseteq \mathbb{Z}[x]$, (x) is not maximal, but x is irreducible.

Note In $k[x]$, maximal ideals are those generated by irreducible polynomials.