An ideal \( P \) in a commutative ring \( R \) is prime if \( P \neq R \) and if \( \forall a, b \in R \):

\[
ab \in P \implies a \in P \text{ or } b \in P
\]

- \( P \subseteq R \) is prime \iff \( R/P \) is an integral domain
- Hence maximal ideals are prime.

But \( \langle x \rangle \) \((\mathbb{Z}[x])\) is prime and not maximal.

So maximal \( \implies \) prime.

Def. An integral domain in a P.I.D. (principal ideal domain) if every ideal is principal.

Def. An integral domain \( R \) has a division algorithm ("in a Euclidean domain") if \( \exists f : R \times R \to \mathbb{N} \) so that \( \forall a, b \in R, b \neq 0 \), \( \exists q, r \in R \) with \( a = qb + r \) and \( (r = 0 \text{ or } s(r) < s(b)) \)

Examples: \( \mathbb{Z}, \mathbb{F}[x], \mathbb{Z}[i, \sqrt{-1}] = \text{Gaussian integers} \) have a division "algorithm."

Theorem 28.1. Every Euclidean domain is a P.I.D.

Proof. Let \( R \) be an integral domain with a division function \( s : R \times R \to \mathbb{N} \) and \( I \subseteq R \) an ideal.

If \( I = \{ 0 \} \) the zero ideal, there is nothing to prove. \( I = \langle 0 \rangle \).

Suppose \( I \neq 0 \). Consider

\[
S = \{ s(x) \mid x \in I \text{ and } x \neq 0 \}.
\]

By well-ordering \( \exists b \in I \) so that \( b \neq 0 \) and \( s(b) = \min(S) \)

Given \( a \in I \), \( \exists q, r \in R \) so that \( a = qb + r \) and

\[
r = 0 \text{ or } s(r) < s(b).
\]

Since \( c, b \in I \) and \( I \) is an ideal, \( r = a - qb \in I \).

Since \( s(r) < s(b) = \min S \), \( r \) has to be \( 0 \).

\[
\Rightarrow a = qb \in \langle b \rangle \implies I \subseteq \langle b \rangle (\subseteq I).
\]
Definition: Let \( R \) be a commutative ring.
\( x \in R \) is irreducible iff \( x \neq 0 \) and \( x \) is not a unit and
\[ x = ab \implies (a \text{ is a unit or } b \text{ is a unit}) \]
\( p \in R \) is prime iff \( (p) \subset R \) is a prime ideal.

Lemma 28.2: \( p \in R \) is prime \( \iff \) \((p) \neq \text{not a unit and } p | ab \implies p | a \text{ or } p | b)\)

Proof: Note: \( x \in (p) \implies x = qp \) for some \( q \in R \implies p | x \).

Therefore: \( (a, b \in (p) \implies [a \in (p) \lor b \in (p)]) \) if and only if
\[ (p | ab \implies [p | a \text{ or } p | b]) \]
Also \( (p) \neq R \implies p \text{ is not a unit} \]

Lemma 28.3: In \( R = \mathbb{Z}[(\sqrt{-5})] \) irreducibles need not be primes.

Proof: Consider \( N: \mathbb{Z}[(\sqrt{-5})] \to \mathbb{N} \)
\[ N(a + b\sqrt{-5}) = (a + b\sqrt{-5})^2 = a^2 + 5b^2 \]
1. \( N(a + b\sqrt{-5}) = 0 \iff a^2 + 5b^2 = 0 \iff (a = 0 \text{ and } b = 0) \)
2. \( N(a + b\sqrt{-5}) = 1 \iff a^2 + 5b^2 = 1 \iff b = 0, a = \pm 1 \)
3. \( \forall u, v \in \mathbb{Z}[(\sqrt{-5})] \quad N(uv) = N(u)N(v) \).

Therefore: \( \forall u, v \in \mathbb{Z}[(\sqrt{-5})] \quad N(u)N(v) = N(uv) \)
\[ \iff 1 = N(1) = N(u)N(v) \]
\[ \iff N(u) = N(v) = 1 \]
\[ \iff u = v = 1 \text{ or } u = v = -1 \]

4. The smallest values of \( N \) are
\( 0 = N(0), 1 = N(\pm 1), 4 = N(2), 5 = N(\pm \sqrt{-5}) \)
and \( 6 = N(\pm 1 \pm \sqrt{-5}) \)

Claim: \( 2 \in \mathbb{Z}[(\sqrt{-5})] \) is irreducible.

Proof: If \( 2 = uv \) for some \( u, v \in \mathbb{Z}[(\sqrt{-5})] \) then
\[ 4 = N(u)N(v) \]
\[ a^2 + 5b^2 = 2 \] has no solutions if \( a, b \in \mathbb{Z} \).
\[N(u) = 1 \text{ and } N(v) = 4 \text{ or } (N(u) = 4 \text{ and } N(v) = 1)\]

\[N(u) = 1 \Rightarrow u \in a \text{ unit.}\]

Similarly \(N(v) = 1 \Rightarrow v \in a \text{ unit.}\)

\[\therefore \ 2 \in \mathbb{Z} \left[ \sqrt{5} \right] \text{ is irreducible.}\]

**Claim 2.** \(2 \text{ is not prime in } \mathbb{Z} \left[ \sqrt{5} \right] \)

**Proof.** \(2 \cdot 3 = 6 = 1 + 5 = (1 + \sqrt{5})(1 - \sqrt{5})\)

If \(2 | (1 + \sqrt{5}) \) \(\Rightarrow 3 | (1 + \sqrt{5}) \) \(\Rightarrow 3 \in \mathbb{Z} \left[ \sqrt{5} \right] \text{ with } \)

\[1 + \sqrt{5} = 3q\]

\[\Rightarrow 6 = N(1 + \sqrt{5}) = N(2) N(q) = 4 N(q)\]

Since \(N(q) \in \mathbb{N}, \text{ this is impossible.}\)

**Conclusion:** \(2 \in \mathbb{Z} \left[ \sqrt{5} \right] \text{ is irreducible and not prime.}\)

(\text{nonzero!})

**Lemma 28.4** In an integral domain, primes are irreducibles.

**Proof.** We want to show: \(p \in \text{ a prime, } p \neq 0, \text{ and } p = ab\)

\(\Rightarrow a \text{ or } b \text{ are units.}\)

Suppose \(p = ab. \) Then \(p \mid (ab). \) Since \(p \) is prime \(p \mid a \) or \(p \mid b. \) Say \(p \mid a. \) Then \(a = qp \) for some \(q. \)

\[\Rightarrow p = ab = p q b\]

\[\Rightarrow p (1 - qb) = 0. \]

Since \(p \neq 0 \) and we're in an integral domain \(1 - qb = 0\)

\[\Rightarrow 1 = qb \Rightarrow b \in a \text{ unit.}\]

Similarly, \(p \mid b \Rightarrow a \in a \text{ unit.}\)

**Lemma 28.5** Let \(R \) be a P.I.D. Then \(x \in R \) is irreducible

\[\Leftrightarrow x \in a \text{ (nonzero) prime.}\]

**Proof.** Suppose \(x \in \text{ a nonzero prime.} \) Then \(x \) is irreducible by 28.4.
Suppose $x$ is irreducible.

We argue first that the ideal $\langle x \rangle$ is maximal.

Suppose $\langle x \rangle \subseteq I \subseteq R$ for some ideal $I$. Since $R$ is a PID $I = \langle c \rangle$ for some $c \in R$. Since $x \in \langle x \rangle \subseteq \langle c \rangle$, $x = qc$ for some $q \in R$.

Since $x$ is irreducible, either $q$ is a unit (and then $c = q^{-1}x$, so $c \in \langle x \rangle$ so $I = \langle c \rangle \subseteq \langle x \rangle$ so $I = \langle x \rangle$) or $c$ is a unit (and then $I = \langle c \rangle = R$).

$\Rightarrow \langle x \rangle$ is maximal.

Since $\langle x \rangle$ is maximal, $\langle x \rangle$ is prime (recall: $\langle x \rangle$ maximal $\Rightarrow R/\langle x \rangle$ is a field $\Rightarrow R/\langle x \rangle$ is integrally closed $\Rightarrow \langle x \rangle$ is prime).

$\Rightarrow x$ is prime.

In $\mathbb{Z}$, $\mathbb{F}(x)$, $\mathbb{Z}[F]$ irreducibles are nonzero primes.

Since $\mathbb{Z}$, $\mathbb{F}(x)$, $\mathbb{Z}[F]$ are Euclidean rings, hence PIDs.

In $\mathbb{Z}[\sqrt{-3}]$ not all irreducibles are primes.

Hence $\mathbb{Z}[\sqrt{-3}]$ is not a PID.

Corollary (of proof of 28.5) In a PID irreducibles define maximal ideals. Hence if $R$ is a PID and $x \in R$ is irreducible, $R/\langle x \rangle$ is a field.