Content:

Proposition	If I is an ideal in R, a ER, then $I = (a) \Leftrightarrow a$ is of minimal degree in I.
Proposition	If R is a euclidean ring, $a, b \in R - \{0\}$, $b \notin U(R)$, then $\partial(a) < \partial(ab)$.
Proposition	All ERs have unity.
Example	$\mathbb{Z}[\sqrt{-5}]$ is not a euclidean ring.
Example	3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$
Definition	prime ideal, maximal ideal
Examples	(6) is not prime or maximal, (3) is prime and maximal, (x) is prime but not maximal.

For Reference:

Theorem Every Euclidean Ring is a PID.

Proof:
Let I be an ideal in R where R is a Euclidean Ring.
If $I = \{0\} = (0)$, we're done. Suppose $I \neq \{0\}$.
Choose $a \in I$ such that $\partial(a) \leq \partial(b)$ $\forall$ $b \in I$.
Claim: $I = (a)$.
Clearly $(a) \subseteq I$.
Let $b \in I$. Then $b = aq + r$ where $r = 0$ or $\partial(r) < \partial(a)$ for some $q, r \in R$.
Since $aq \in I$ and $b \in I$, then $r \in I$. And since a is of minimal degree,
then $\partial(r) \not< \partial(a)$. $\therefore$ $r = 0$. Thus, $b = aq \in (a)$. So $I \subseteq (a)$, hence $I = (a)$.
$\therefore$ R is a PID.

Proposition If I is an ideal in a ER, R, then $I = (a) \Leftrightarrow a$ is of minimal degree in I.

Proof:
$\Leftarrow$: (See proof above.)
$\Rightarrow$: Assume $I = (a)$, Let $b \in I$. Then $b = aq$ for some $q \in R$.
Since R is a ER, then $\partial(a) \leq \partial(aq) = \partial(b)$.
So a is of minimal degree.

Proposition If R is a euclidean ring, $a, b \in R - \{0\}$, $b \notin U(R)$, then $\partial(a) < \partial(ab)$.

Proof:
We know $\partial(a) \leq \partial(ab)$ by property of ER. Suppose $\partial(a) = \partial(ab)$.
Let $I = (a)$. Then $ab \in I$. Since R is a ER, then $\exists$ $q, r \in R$ such that
$a = abq + r$ where $r = 0$ or $\partial(r) < \partial(ab)$.
Since $a - abq = r \in I$, then $\partial(r) \not< \partial(ab)$, as $\partial(a) = \partial(ab)$,
and a is of minimal degree. $\therefore$ $a - abq = 0$.
Since a is of minimal degree and $\partial(a) = \partial(ab)$, then
ab is of minimal degree. Thus, $I = (ab)$.
So then $a \in I = (ab)$. Thus $a = abq$ for some $q \in R$. So $1 = bq$.
Hence, $b \in U(R)$, a contradiction to our assumption.

Note In the proof that every ER is a PID, we can replace (a) with aR to get that all ideals in a ER are of the form $I = aR$ for some $a \in R$.

Theorem All ideals in a ER are of the form $I = aR$ for some $a \in R$.

Proof:
Let I be an ideal in R where R is a Euclidean Ring.
If $I = \{0\} = 0R$, we're done. Suppose $I \neq \{0\}$. Choose $a \in I$ such that $\partial(a) \leq \partial(b)\ \forall\ b \in I$. Claim: $I = aR$. Clearly $aR \subseteq I$.
Let $b \in I$. Then $b = aq + r$ where $r = 0$ or $\partial(r) < \partial(a)$ for some $q, r \in R$.
Since $aq \in I$ and $b \in I$, then $r \in I$. And since a is of minimal degree, then $\partial(r) \not< \partial(a)$. $\therefore\ r = 0$. Thus, $b = aq \in aR$. So $I \subseteq aR$, hence $I = aR$.

Note If we were to define an integral domain without unity, a ER must still have unity. Let's prove all ERs have unity.

Theorem All ERs have unity.

Proof:
R is an ideal in R, so as noted above, $R = aR$ for some $a \in R$.
And $a \in R$, so $a = ar$ for some $r \in R$. Claim: r is the unity.
Let $b \in R$. Then $ab = arb$. So $b = rb$. Thus r is the unity in R.

Note If R does not have unity, then $(a) \neq aR$, since $a \bullet 1 \notin R$.

Note Since all ERs are PIDs, and we showed $\mathbb{Z}[i]$ is a ER, then $\mathbb{Z}[i]$ is a PID.

Example $\mathbb{Z}[\sqrt{-5}]$ is not a euclidean ring.

Proof:
Define ∂: $\mathbb{Z}[\sqrt{-5}] \to \mathbb{N} \cup \{0\}$ by $\partial(a + b\sqrt{-5}) = a^2 + 5b^2$.
So $\partial(\alpha) = \alpha\overline{\alpha}$, hence $\partial(\alpha\beta) = \partial(\alpha)\partial(\beta)$, as before.
Let $I = (3, 2 + \sqrt{-5})$. Suppose $\mathbb{Z}[\sqrt{-5}]$ is a PID.
Then $\exists\ a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that $I = (a + b\sqrt{-5})$.
Since $3 \in I$, then $3 = (a + b\sqrt{-5})\alpha$ for some $\alpha = x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.
Since $2 + \sqrt{-5} \in I$, then $2 + \sqrt{-5} = (a + b\sqrt{-5})\beta$ for some $\beta \in \mathbb{Z}[\sqrt{-5}]$.
So $9 = \partial(3) = \partial((a + b\sqrt{-5})\alpha) = (a^2 + 5b^2)\partial(\alpha)$.
Since all this occurs in $\mathbb{Z}$, the only factors of 9 are 1, 3, and 9,
so we have 3 cases:
(1) $9 = a^2 + 5b^2$; (2) $3 = a^2 + 5b^2$; (3) $1 = a^2 + 5b^2$.
We know $3 \neq a^2 + 5b^2$ as there is no integer solution for this.
If $9 = a^2 + 5b^2$, then $\partial(\alpha) = x^2 + 5y^2 = 1$, hence $\alpha = \pm 1$.
Then $3 = \pm(a + b\sqrt{-5})$, which implies that
$2 + \sqrt{-5} = (a + b\sqrt{-5})\beta = \pm 3\beta$, a contradiction as $3 \nmid (2 + \sqrt{-5})$.
If $1 = a^2 + 5b^2$, then $a = \pm 1$ and $b = 0$. So $I = (a + b\sqrt{-5}) = (\pm 1) = \mathbb{Z}[\sqrt{-5}]$.
Claim: $1 \notin I$. Suppose $1 \in I$, then $1 = 3\gamma + (2 + \sqrt{-5})\tau$.
Then $2 - \sqrt{-5} = 3\gamma(2 - \sqrt{-5}) + 9\tau = 3(\gamma(2 + \sqrt{-5}) + 3\tau)$, a contradiction.
Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a PID, hence not a euclidean ring.

Example 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Proof:

Assume $3 = \alpha\beta$ for some $\alpha = a + b\sqrt{-5}$, $\beta = c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.

Define function ∂ as above.

Then $9 = \partial(3) = \partial(\alpha\beta) = \partial(\alpha)\partial(\beta)$.

$\partial(\alpha) \neq 3$, as before (there is no integer solution to $3 = a^2 + 5b^2$).

If $\partial(\alpha) = a^2 + 5b^2 = 1$, then $a = 1$, $b = 0$, hence $\alpha = \pm 1$.

Thus $\alpha \in U(\mathbb{Z}[\sqrt{-5}])$.

If $\partial(\alpha) = 9$, then $\partial(\beta) = c^2 + 5d^2 = 1$, hence $\beta = \pm 1$.

Thus $\beta \in U(\mathbb{Z}[\sqrt{-5}])$.

$\therefore$ 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

6.1 Prime 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 $(6) \subseteq \mathbb{Z}$.

(6) is not a prime ideal as $2 \cdot 3 \in (6)$ but $2 \notin (6)$ and $3 \notin (6)$.

(6) is not a maximal ideal as $(6) \subset (2) \subset \mathbb{Z}$.

(3) is a prime ideal and a maximal ideal.

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

(x) is prime as $f(x)g(x) \in (x) \Rightarrow x | f(x)$ or $x | g(x)$.

Next Time On Wednesday, we will have a better way to prove (x) is prime.