Content:

Proposition	If R is an ID, $a, b \in R$, then $(a, b) = (d)$ for some $d \in R \Rightarrow d$ is a gcd of a and b.
Definition	Euclidean Ring
Examples	$k[x]$, $\mathbb{Z}$, fields, $\mathbb{Z}[i]$ are ERs
Theorem	Every ER is a PID. But not every PID is a ER.

Question In a PID, if p is irreducible, what can you say about a gcd of p and a, where $a \in R$? It could be p, 1, or an associate of p or 1.

Proof:
Suppose d is a gcd of p and a. Then $d \mid p$ and $d \mid a$.
So $dq = p$ for some $q \in R$.
Since p is irreducible, then d is a unit or q is a unit.
If d is a unit, then 1 is an associate of d, so 1 is a gcd of a and p.
If q is a unit, then p is an associate of d, so p is a gcd of a and p .

In your homework, you will prove:
If d is a gcd, then all associates of d are gcds.

Question If d is a gcd, are all gcds associates of d? Yes.

Proof:
Suppose d' is a gcd.
So $d \mid d'$ (since d' is a gcd and d is a common divisor.)
And $d' \mid d$ (since d is a gcd and d' is a common divisor.)
So d and d' are associates (proven in #5 of HW #1).

Proposition If R is an ID, $a, b \in R$, then $(a, b) = (d)$ for some $d \in R \Rightarrow d$ is a gcd of a and b.

Proof:
Assume $(d) = (a, b)$. Then $a \in (d)$ and $b \in (d)$. So $d \mid a$ and $d \mid b$.
Suppose $c \mid a$ and $c \mid b$.
We know $d \in (a, b) \Rightarrow d = ax + by$ for some $x, y \in R$ (#3 of HW #1).
So $d = (cm)x + (cn)y = c(mx + ny)$. So $c \mid d$. Hence d is a gcd of a and b.

Example $2, x \in \mathbb{Z}[x]$. $(2, x)$ is not a principal ideal. But 1 is a gcd of 2 and x.
Moral of story: (a, b) being principal is not a requirement for gcd.

3.6 Euclidean Rings

Definition A *Euclidean Ring* is and integral domain, R, equipped with a function $\partial: R - \{0\} \to \mathbb{N} \cup \{0\}$ called a degree function such that
(1) $\partial(a) \leq \partial(ab)$ $\forall$ $a, b \in R$, a, b not zero.
(2) $\exists$ $q, r \in R$ such that $a = bq + r$ where $r = 0$ or $\partial(r) < \partial(b)$.

Example $k[x]$ is a Euclidean Ring with $\partial(f) = \deg(f)$
$\mathbb{Z}$ is a Euclidean Ring with $\partial(n) = |n|$.

Note We lose uniqueness of q and r, as in $\mathbb{Z}$,
$5 = 3 \bullet 1 + 2 \quad (|2| < |3|)$
$5 = 3 \bullet 2 - 1 \quad (|-1| < |3|)$

Example Is a field a Euclidean Ring? Yes.
Let $a, b \in R$. Then $a = b(b^{-1}a) + 0$.
Define $\partial(x) = c \ \forall \ c \in \mathbb{N} \cup \{0\}$.

Example If R is a Euclidean Ring with $\partial(x) = 0$, what can we say about R?
It's a field.
Proof:
Let $a \in R$, $a \neq 0$. Then $1 = aq + r$ where $\partial(r) < \partial(a) = 0$ or $r = 0$.
Since $\partial(r) \not< 0$, then $r = 0$. So $1 = aq$, hence $a \in U(R)$.
$\therefore$ R is a field.

Example $\mathbb{Z}[i]$ is a Euclidean Ring.
Proof:
Define $\partial: \mathbb{Z}[i] \rightarrow \mathbb{N} \cup \{0\}$ by $\partial(a + bi) = a^2 + b^2$
Let $\alpha \in \mathbb{Z}[i]$. Then $\partial(\alpha) = \alpha\overline{\alpha}$. So $\partial(\alpha\beta) = \alpha\beta(\overline{\alpha\beta}) = a\overline{\alpha}\beta\overline{\beta} = \partial(\alpha)\partial(\beta)$.
Since $\partial(\beta) \geq 1$, then $\partial(\alpha) \leq \partial(\alpha)\partial(\beta) = \partial(\alpha\beta)$.
Note that this is also true in $\mathbb{Q}[i]$.
$\alpha/\beta = (\alpha\overline{\beta})/(\beta\overline{\beta}) = x + yi$ where $x, y \in \mathbb{Q}$.
So $x = a + u$ and $y = b + v$ where $a, b \in \mathbb{Z}$, $u, v \in \mathbb{Q}$, and $|u|, |v| \leq \frac{1}{2}$.
So $\alpha = \beta(x + yi) = \beta((a + u) + (b + v)i) = \beta(a + bi) + \beta(u + vi)$.
Since $\alpha \in \mathbb{Z}[i]$ and $\beta(a + bi) \in \mathbb{Z}[i]$, then $\beta(u + vi) \in \mathbb{Z}[i]$.
Suppose $r = \beta(u + vi) \neq 0$. Then $\partial(\beta(u + vi)) = \partial(\beta)\partial(u + vi)$.
Since $|u|, |v| \leq \frac{1}{2}$, then $u^2 + v^2 < 1$. So $\partial(\beta(u + vi)) < \partial(\beta)$.
$\therefore$ $\mathbb{Z}[i]$ is a Euclidean Ring.

Recall We showed $k[x]$ is a PID. This worked because of the division algorithm. So any time you have a division algorithm you have a Euclidean Ring.

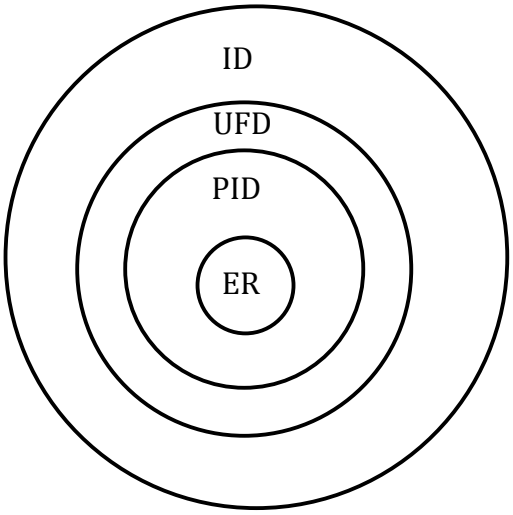
Theorem Every Euclidean Ring is a PID.

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 minimum 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.

Note Every Euclidean Ring is a PID, but not every PID is a Euclidean Ring.

Example Let $R = \{a + b\gamma |\ a, b \in \mathbb{Z}, \gamma = \frac{1}{2}(1 + \sqrt{-19})\}$.
It can be shown that R is a PID. However, in 1949 TS Motzkin showed R has no universal side divisors, and hence is not a Euclidean Ring.



On Monday We will show $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean Ring.