Let $R$ be a commutative ring with $1_R$, and $a \in R$.

- $\langle a \rangle = \{ ar : r \in R \}$ the principal ideal of $a$.
  - Review: why is "commutative" & "with $1_R$" important here?
  - An integral domain where every ideal is principal is a **PID** (principal ideal domain).
  - $a, b \in R$ are **associated** if $\exists u \in R^* \text{ st. } a = bu$.

- If $R$ is an integral domain, then
  - $a$ & $b$ are associates iff $\langle a \rangle = \langle b \rangle$.
  - Review: why did I stipulate "integral domain?"

- $a$ is called **irreducible**
  - if $\forall b, c \in R$ whenever $a = bc$, either $b$ is a unit or $c$ is a unit.
  - (so either $b$ or $c$ is an associate of $a$)

- $a$ is called **prime** if
  - whenever $a \mid bc$, either $a \mid b$ or $a \mid c$.
  - Review: if $R$ is an integral domain, then prime $\Rightarrow$ irreducible.

- $a$ divides $b$, written $a \mid b$,
  - means $\exists q \in R \text{ st. } b = aq$.
  - This is equivalent to saying $b \in \langle a \rangle$. 
\[ R \text{ is a unique factorization domain (UFD) if} \]

1) \( R \) is an integral domain,

2) For all nonzero & nonunit \( a \in R \),

\[ \exists \text{ irreducibles } p_1, \ldots, p_l \text{ st. } a = p_1p_2 \cdots p_l, \]

3) If \( p_1, \ldots, p_l \) & \( q_1, \ldots, q_m \) are irreducibles with

\[ p_1p_2 \cdots p_l = q_1q_2 \cdots q_m \]

then \( l = m \) & after possibly reordering the \( q \)'s,

\( p_i \) & \( q_i \) are associates for \( i = 1, 2, \ldots, \).

---

**Goal**: prove that \( \mathbb{Z} \), and \( \mathbb{Z}[\sqrt{-1}] \) are UFD's.

(we'll see a few more soon)

**Strategy**: We'll prove that every PID is a UFD, as follows:

1) Prove that all irreducibles are prime.

2) Prove that prime factorization is unique.

3) Prove that factorizations exist in PIDs.

Then we'll prove that \( \mathbb{Z} \) & \( \mathbb{Z}[\sqrt{-1}] \) (& others) are PIDs.