## $\boxed{\text{Refresher: principal ideals \& factorization}}$

Let $R$ be a <u>commutative ring with $1_R$</u>, and $a \in R$.

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

- If $R$ is an integral domain, then

  $a$ & $b$ are associates iff $\underline{\langle a \rangle = \langle b \rangle}$.

  ◻ <u>Review</u>: why did I stipulate "integral domain?"

- $a$ is called <u>irreducible</u>

  if ~~$\forall b \in R$~~ 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 <u>prime</u> if

  whenever $a \mid bc$, either $a \mid b$ or $a \mid c$.

  ◻ <u>Review</u>: if $R$ is an integral domain, then prime $\Rightarrow$ irreducible.

- <u>$a$ divides $b$</u>, written $\underline{a \mid b}$,

  means $\exists q \in R$ st. $b = aq$.

  This is equivalent to saying $\underline{b \in \langle a \rangle}$.

• $R$ is a unique factorization domain (UFD) if

1) $R$ is an integral domain,

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

$\exists$ irreducibles $p_1, \cdots, p_\ell$ s.t. $a = p_1 p_2 \cdots p_\ell$,

3) If $p_1, \cdots, p_\ell$ & $q_1, \cdots, q_m$ are irreducibles with

$p_1 p_2 \cdots p_\ell = q_1 q_2 \cdots q_m$

then $\ell = m$ &, after possibly reordering the $q$'s,

$p_i$ & $q_i$ are associates for $i = 1, 2, \cdots, \ell$.

---

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 PID's.

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