$$\boxed{\begin{aligned}&\text{Euclidean domain} \Rightarrow \text{Principal Ideal domain}\\ &\qquad \Rightarrow \text{uniquely factorization domain.}\end{aligned}}$$

Defn (UFD). $\forall a \in R$. if a is not irreducible

$a = a_1 b_1$. neither a_1. nor b_1 is unit

$a_1 = c_1 d_1$, $b_1 = c_2 d_2$ $\cdots$

Factoring terminates if after finite steps, all the factors are irreducible.

$a = p_1 p_2 p_3 \cdots p_m$. p_i are irreducible.

$= q_1 q_2 \cdots q_m$ q_m are irreducible.

The irreducible factorization is unique.

if $m = n$, and after rearranging $q_1 \cdots q_m$ suitably, q_i is an associate of p_i for each i.

Example:

In $\mathbb{Z}[i]$. $5 = (1+2i)(1-2i)$

$= (2+i)(2-i)$.

$1-2i$ and $2+i$ are associates.

$(2+i)\, i = 1-2i$.

$i(-i) = -1$ i is a unit in $\mathbb{Z}[i]$.

Lemma 1: In an integral domain R, any prime element is irreducible

Pf: p prime element, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

p irreducible if $p = ab$ one of a, b must be unit. (or one of a, b is an associate of p)

If p is prime and $p = ab$, then

$p \mid a$ or $p \mid b$.

Assume $a = p \cdot c$.

then $p = p \cdot cb \Rightarrow bc = 1$.

Lemma 2: If R is PID, then every irreducible element is a prime element.

Pf: Assume p is irreducible, then there is no principal ideal

$$(p) \subsetneq (c) \subsetneq (1).$$

so (p) is maximal ideal.

$R/(p)$ is a field.

So p is prime.

Prop: i) Suppose factoring process terminates in R. Then R is UFD iff every irreducible element is a prime element.

ii) PID is UFD.

i) Pf: $\Leftarrow$ $a = p_1 p_2 \cdots p_m$
$= q_1 q_2 \cdots q_n$.

$m \leq n$, induction on n.

$n = 1$, then $a = p_1 = q_1$.

$n \geq 2$, q_1 irreducible $\Rightarrow$ q_1 prime $\Rightarrow$ q_1 divides $p_1 \cdots p_m$, then q_1 divides p_j.

Assume $q_1 \mid p_1$. Since p_1 is irreducible.

q_1 is a unit or associates with p_1. Since q_1 is irreducible. q_1 is not a unit. So q_1, p_1 are associates.

We can assume $q_1 = p_1$ by multiplying a unit to p_1.

So $q_2 q_3 \cdots q_n = p_2 \cdots p_m$.

(ii) We only need to prove that factoring terminates.

Prop: ① and ② are equivalent:

① Factoring terminates

② R does not contain an infinite strictly increasing chain

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq \cdots$$

① $\Rightarrow$ ②. $(a_1) \subsetneq (a_2)$

$\Rightarrow$ $a_1 = a_2 b_1$ b_1 not unit.

$= a_3 b_2 b_1$

$= \cdots\cdots$

② $\Rightarrow$ ①. $a_1 = a_2 b_1$

$= a_3 b_2 b_1$

$= \cdots\cdots$

then $(a_1) \subsetneq (a_2) \subsetneq \cdots$

For PID, if $(a_1) \subseteq (a_2) \cdots$

Take the union $\bigcup (a_i) = I$.

I is an ideal, and $I = (a)$.

so $a \in \bigcup (a_i)$. assume

$a \in (a_j)$, then $(a_j) = \bigcup (a_i)$

so $(a_j) = (a_{j+1}) = \cdots$

Non UFD.

$\mathbb{Z}[\sqrt{-5}]$.

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

2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are all irreducible.