Let R be an integral domain.

Eg. Let $R = \mathbb{Z}\{\sqrt{-5}\} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

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

Let $d \in R$, invertible or non-invertible.

Let $R^* = \{$all invertible elts of $R\}$.

In integral domain R,

Def. Let $a = bc$. b is a factor of a ($b \mid a$) and a is a multiple of b.

If c is invertible, then $b = ac^{-1}$, say $a \sim b$. associate. (Eg. In $\mathbb{Z}$, $2 = (-2)\cdot(-1)$. $2\cdot(-1) = -2$. $2 \sim -2$).

Def. ① An elt $d \in R$ is called irreducible if $d = ab$ then a or b is invertible

② An elt $d \in R$ is called a prime if $d \mid ab$, then $d \mid a$ or $d \mid b$.

Rmk. irreducible $\not\Leftrightarrow$ prime. (in general.)

Lemma. In an ID, a prime is irreducible

Proof: Let R be an ID and let $d \in R$ be a prime.

Suppose $d = ab$. Then $d \mid ab$ and so $d \mid a$ or $d \mid b$ because d is a prime.

If $d \mid a$, then $a = d \cdot c$ for some $c \in R$. $a = dc = abc$.

Then, $a - abc = 0 = a(1 - bc) \Rightarrow 1 - bc = 0$, $bc = 1$. $\Rightarrow b$ is invertible

Thus, by def. d is irreducible $\square$.

- An irreducible elt is not neccessarily a prime.

Eg. Let $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

Claim: (i) 2 is irreducible.

(ii) 2 is not a prime.

Proof: (i): Suppose $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ for some $a, b, c, d \in \mathbb{Z}$.

Then, taking complex conjugation, $2 = (a - b\sqrt{-5})(c - d\sqrt{-5})$

Then, $4 = (a^2 + 5b^2)(c^2 + 5d^2)$ in $\mathbb{Z}$. Thus $b = d = 0$. and $4 = a^2 \cdot c^2$

So either $a^2 = 4$ and $c^2 = 1$ i.e. either $a = \pm 2$ and $c = \pm 1$

or $a^2 = 1$ and $c^2 = 4$. or $a = \pm 1$ and $c = \pm 2$.

Then $2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) = ac = (\pm 2)(\pm 1)$ or $(\pm 1)(\pm 2)$.

So 2 is irreducible.

(ii): $2 \mid 6$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$

If 2 is a prime. then $2 \mid 1+\sqrt{-5}$ or $2 \mid 1-\sqrt{-5}$.

Suppose $2 \mid (1+\sqrt{-5})$. Then $1+\sqrt{-5} = 2(a+b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$.

Then $1 = 2 \cdot a$ and $\sqrt{-5} = 2b\sqrt{-5}$. not possible. So $2 \nmid 1+\sqrt{-5}$. Similarly, $2 \nmid 1-\sqrt{-5}$.

So 2 is not a prime.

<u>eg</u>. $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. The factorization is not unique.

However, in $\mathbb{Z}$, $\mathbb{C}$, $\mathbb{Z}[x]$, $\mathbb{R}(x)$, factorization is unique.

<u>Def</u>. (UFD). Let D be an ID. Then D is called a <u>unique factorization domain (UFD)</u>

if (1) each non-zero non-invertible elt of D can be written as a product of finitely many irreducibles of D. (factor chain condition)

(2) for any $a \in D$, $a \neq 0$,

$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ with p_i, q_i irreducible

$\Rightarrow s = t$, $p_i \sim q_i$ after renumbering the indices.

<u>Thm</u>. Let D be an ID. Then D is a UFD iff

(i) condition (1) in def:

each non-zero non-invertible elt of D can be written as a product of finitely many irreducibles of D.

(ii) each irreducible is a prime.

<u>Proof</u>: First, assume (i) (ii).

Let $a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ where p_i, q_j irreducible. (by (ii), p_i, q_j prime).

Then, $p_1 \mid q_1(q_2 \cdots q_t)$ So $p_1 \mid q_1$ or $p_1 \mid q_2 \cdots q_t$.

If $p_1 \mid q_i$, then $p_1 \overset{a}{\sim} q_1$. (both irr.)

If $p_1 \mid q_2(q_3 \cdots q_t)$, then $p_1 \mid q_2$ or $p_1 \mid q_3 \cdots q_t$. ......

Repeating the process to an end, we have $p_1 \overset{a}{\sim} q_i$ for some i. Similarly, $p_2 \overset{a}{\sim} q_j$ $(i \neq j)$, ...

So D is a UFD.

Conversely, let D be a UFD. Then we need to prove each irreducible is a prime.

Let irreducible $d \in D$ be s.t. $d \mid ab$. where a, b not invertible (otherwise $d \mid a$ or $d \mid b$).

Then $ab = d \cdot c$ for some $c \in D$.

If c is invertible, then $d = abc^{-1} = a(bc^{-1})$ not possible.

So c is not invertible. Since D is a UFD, we have

$a = p_1 \cdots p_r$, $b = q_1 \cdots q_s$, $c = u_1 \cdots u_t$.

Then $p_1 \cdots p_r \cdot q_1 \cdots q_s = d \cdot u_1 \cdots u_t$ and $d \sim p_i$ or $d \sim q_j$ as d is irr. and D is UFD.

So $d \mid a$ or $d \mid b$. i.e. d is a prime $\square$.

<u>Rmk</u>: $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ is not a UFD.

UFD $\equiv$ "irreducible" and "prime" are the same.

<u>Def</u>: An ID is called a <u>principle ideal domain (PID)</u> if each of its ideals is a principle ideal, i.e. generated by a single elt.

<u>Thm</u>: A PID is a UFD. but a UFD is not neccessarily a PID.

<u>Eg</u>. $\mathbb{Z}[x]$ is a UFD, but $(2, x)$ is a principle ideal. So $\mathbb{Z}[x]$ is not a PID.

<u>Prop</u>. Let D be a PID, and $p \in D \setminus \{0\}$.

Then (1) p is a prime $\Leftrightarrow$ p is irreducible.

$\Updownarrow$

(2) (p) is a prime ideal $\Leftrightarrow$ (p) is a maximal ideal.

<u>Proof</u>: Let p be irreducible. Then (p) is maximal. (Otherwise $(p) < \underset{(q)}{\overset{\shortparallel}{I}} < D$).

So $D/(p)$ is a field, so is ID, and (p) is a prime ideal, and p is a prime.

Conversely, ... $\square$.

<u>Proof of "PID is UFD"</u>:

Since irr. $\equiv$ prime by the prop. we only need to prove that

"each non-invertible elt. is a prod. of finitely many irr.".