Thm Suppose $f(x)$, $g(x)$ & $h(x)$ are polynomials over field F and if $f(x) \mid g(x).h(x)$ and g.c.d of $f(x)$ and $g(x)$ is 1, then $f(x) \mid h(x)$.

Proof: Since $f(x) \mid g(x).h(x)$

$\Rightarrow \exists$ a polynomial $q(x) \in F[x]$ such that

$$g(x).h(x) = f(x).q(x)$$

Since g.c.d of $f(x)$ and $g(x)$ is 1

$\Rightarrow \exists$ $m(x)$ and $n(x) \in F[x]$ such that

$$1 = m(x).f(x) + n(x).g(x) \quad \text{——— (1)}$$

$$\Rightarrow h(x) = h(x)\left[m(x).f(x) + n(x).g(x)\right]$$

$$= h(x).m(x).f(x) + h(x).n(x).g(x)$$

$$= h(x).m(x).f(x) + n(x).q(x).f(x)$$

(From (1))

$$= \{h(x).m(x) + n(x).q(x)\}f(x)$$

$$\Rightarrow f(x) \mid h(x).$$

Thm Suppose $f(x)$, $g(x)$, $h(x)$ are polynomials over a field F. If $f(x) \mid g(x).h(x)$ and $f(x)$ is irreducible then $f(x)$ divides at least one of $g(x)$ or $h(x)$

Proof Let us assume that $f(x) \nmid g(x)$

Since $f(x)$ is prime $\Rightarrow f(x)$ and $g(x)$ are relatively prime

ie g.c.d of $f(x)$ & $g(x)$ is 1

Hence by previous theorem

$$f(x) \mid h(x)$$

Similarly we can show that if $f(x) \nmid h(x)$ then

$f(x) \mid g(x)$ proved

Thm If R is an integral domain and $a \in R$ is prime element then a is irreducible.

Proof Let $a \in R$ be a prime element and let $a = bc$.
We want to show that either b or c is unit in R

We have $a | bc$. Since a is prime element
$\Rightarrow$ Either $a | b$ or $a | c$.
Let us assume that $a | b$ also $b | a$ ($\because a = bc$)
$\Rightarrow$ a is associate of b.
$\Rightarrow$ $\exists$ a unit $u \in R$ such that $a = bu$

Now $a = bc$ & $a = bu$
$\Rightarrow bc = bu$
$\Rightarrow c = u$ so c is unit
Proved

Thm If R is UFD and $a \in R$ then a is irreducible element iff a is prime

Proof If a is prime then a is irreducible (by previous thm)

<u>Conversely</u> Let a is irreducible.
Let $a = bc$.
We want to show that either $a | b$ or $a | c$.

If $b = 0$ then $b = a.0$ so $a | b$
If b is unit then $c = b^{-1}bc$ so $a | c$ ($\because a | bc$)
So we assume that b & c are non-zero non unit

Since $a|bc$, $\exists\ d \in R$ such that $bc = ad$ —— ①

Let us assume that d is not a unit

Since R is U.F.D, we have decompositions:

$b = b_1 b_2 \cdots b_m$, $c = c_1 c_2 \cdots c_n$, $d = d_1 d_2 \cdots d_p$

where b_i, c_j, d_k are irreducible.

$\Rightarrow b_1 b_2 \cdots b_m \cdot c_1 c_2 \cdots c_n = a\, d_1 d_2 \cdots d_p$ (From ①)

Now by uniqueness of decompositions in UFD,

$\Rightarrow$ Either $a \sim b_i$ for some i
or $a \sim c_j$ for some j

In first case $a|b$ & in second case $a|c$

Similar argument can be given if d is unit

Proved

Revision

Definition (Ideal): A non-empty subset of a ring R is called an ideal if

(i) S is subgroup of R under addition

(ii) $\forall\ r \in R$, $s \in S \Rightarrow rs, sr \in S$.

Principal Ideal: An ideal S of a ring R is called a principal ideal if $\exists\ a \in R$ s.t. $S = (a)$

i.e. if S is generated by a.

Principal Ideal Ring: A ring in which every ideal is principal ideal is called principal ideal ring.

Principal Ideal Domain: An integral domain in which every ideal is principal ideal is called principal ideal Domain.