Thm An ideal S of the Euclidean ring R is a maximal iff S is generated by some prime element of R.

Proof: We know that every ideal of Euclidean ring R is a principal ideal. Suppose S is an ideal of R generated by p so that $S=(p)$.

We have to prove

(i) if p is prime then S is maximal

(ii) if S is maximal the p is prime.

(i) Let us assume that p is prime

Let T is an ideal of R such that $S \subseteq T \subseteq R$.

Since T is also a principal ideal let $T=(q)$ where $q \in R$

$$\text{Since } S \subseteq T$$
$$\Rightarrow (p) \subseteq (q)$$
$$\Rightarrow p \in (q)$$
$$\Rightarrow \exists\ x \in R \text{ such that } p = xq$$
$$\Rightarrow q \mid p, \text{ Also } p \text{ is prime}$$

Therefore q shall be a unit in R or associate of p.

If q is unit in R then $T=(q)=R$

If q is associate of then $T=(q)=(p)=S$.

i.e either $T=R$ or $T=S$.

Hence S is maximal ideal.

(ii) Let S be a maximal ideal

We want to show that p is prime.

Let us suppose that p is not prime.

Let $p=mn$ where neither m nor n is unit in R.

Now $p = mn \Rightarrow m \mid p$

$\Rightarrow (p) \subseteq (m)$

ie $(p) \subseteq (m) \subseteq R \quad \because S = (p)$

Since S is maximal ideal

$\Rightarrow (p) = (m)$ or $R = (m)$

If $R = (m)$

$\therefore 1 \in R \Rightarrow 1 \in (m)$

$\Rightarrow \exists\ y \in R$ s.t $1 = my$.

$\Rightarrow m$ is invertible

$\Rightarrow m$ is unit in R, which is a contradiction.

If $(m) = (p)$

$\Rightarrow m \in (p)$

$\Rightarrow \exists\ z \in R$ s.t $m = zp$

$\therefore p = mn \Rightarrow p = zpn$

$\Rightarrow p - zpn = 0$

$\Rightarrow p(1 - zn) = 0$

$\Rightarrow 1 - zn = 0$ ($\because p \neq 0$ & R is without zero divisor.)

$\Rightarrow zn = 1$

$\Rightarrow n$ is invertible

$\Rightarrow n$ is unit in R, which is a contradiction

Hence p must be a prime element of R

Thm Unique Factorisation Theorem

A polynomial $f(x)$ of positive degree over a field F can be expressed as the product of an element of F and monic irreducible polynomials over F and that the decomposition is unique for the order in which the factors occur.

[Note. Monic polynomial is one in which coeff of highest degree term is 1]

Proof Let $f(x)$ be a polynomial of positive degree over a field F.

Case I : If $f(x)$ is irreducible then we are thru.

Case II : If $f(x)$ is reducible then we can write

$$f(x) = f_1(x) \cdot f_2(x) \quad \text{——} (1)$$

Where degree of $f_1(x)$ & $f_2(x)$ is less than that of $f(x)$.

Let us assume inductively that the theorem is true for all polynomials of degree less than that of $f(x)$.

Then $f_1(x) = a\, p_1(x) \cdot p_2(x) \cdots p_n(x)$ ——— (2)

& $f_2(x) = b\, q_1(x) \cdot q_2(x) \cdots q_m(x)$ ——— (3)

Where $p_i(x)$ & $q_i(x)$ are monic irreducible polynomials over F and $a, b \in F$.

$$\Rightarrow f(x) = ab\, p_1(x) \cdot p_2(x) \cdots p_n(x) \cdot q_1(x) q_2(x) \cdots q_m(x)$$

(From (2) & (3))

$\Rightarrow$ Theorem is true for $f(x)$ also

Hence by induction theorem is true for all polynomials of +ve degree over the field F.

Now it remains to prove that this decomposition is unique except for the order in which factors occur

Let us suppose that $f(x) = c\,p_1(x)\,p_2(x)\cdots p_n(x)$
& $f(x) = d\,q_1(x)q_2(x)\cdots q_m(x)$
where $c, d \in F$ and $p_i(x)$ & $q_j(x)$ are elements of $F[x]$ for all $i = 1,2,\ldots n$ & $j = 1,2,\ldots m$.

Obviously as each $p_i(x)$ & $q_i(x)$ are monic and c & d are leading coefficients so $c = d$

$$\Rightarrow p_1(x)p_2(x)\cdots p_n(x) = q_1(x)q_2(x)\cdots q_m(x) \quad \text{— (1)}$$

Since $p_1(x)$ is divisor of RHS expression

$\Rightarrow p_1(x)$ divides some factor $q_j(x)$ [$\because p_i(x)$ & $q_j(x)$ are (reducible]

Without loss of generality let us assume that $p_1(x) \mid q_1(x)$

Since $p_1(x)$ & $q_1(x)$ are both irreducible so $p_1(x) \sim q_1(x)$

ie $p_1(x)$ & $q_1(x)$ are associates.

Thus we have $p_1(x) = u \cdot q_1(x)$

where u is a unit in $F[x]$. Since $p_1(x)$ & $q_1(x)$ are monic, therefore u must be equal to 1, so we have

$$p_1(x) = q_1(x)$$

Cancelling out $p_1(x)$ & $q_1(x)$ from (1) we get-

$$p_2(x)p_3(x)\cdots p_n(x) = q_2(x)q_3(x)\cdots q_m(x) \quad \text{— (2)}$$

We repeat this argument for $p_2(x)$ and so on. If $m > n$, then after n steps left hand side becomes 1 while RHS reduces to product remaining $q_j(x)$ (after cancelling all $p_i(x)$) but $q_j(x)$ are irreducible polynomials so they can not be units

of $F[x]$ ie they cannot be polynomials of 0 zero degree So their product will be polynomial of degree greater than zero. So it cannot be 1.

Hence m cannot be greater than n

ie $m \leq n$.

Similarly interchanging the role of $p(x)$ & $q(x)$ we get $n \leq m$

Hence $m = n$.

Also we have proved that each $p_i(x)$ is equal to some $q_j(x)$ & each $q_j(x)$ is equal to some $p_i(x)$

Hence the theorem is established.

Value of polynomial at $x = c$

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $F[x]$ for an arbitrary field F and let $c \in F$ then $f(c) = a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n$ where indicated addition and multiplication are operations in F is called the value of $f(x)$ at $x = c$.

Obviously $f(c) \in F$.

Zero of a polynomial: Let $f(x)$ be a polynomial in $F[x]$ for any arbitrary field F and for $c \in F$ $f(c) = 0$, then c is called zero of $f(x)$

Polynomial Equation & its root:

Let $f(x)$ be polynomial in $F[x]$ for any arbitrary field F and $f(c) = 0$ for $c \in F$ then $x = c$ is the root of polynomial equation $f(x) = 0$