Thm: Let $a \in K$ is algebraic over F and $p(x)$ be a minimal polynomial for a over F. Then $p(x)$ is irreducible over F.

Proof: Suppose $f(x) \in F[x]$ be a minimal polynomial for 'a' over F. We want to show that $f(x)$ is irreducible over F.

Let us assume to the contradiction that $f(x)$ is not irreducible over F. Then we can resolve $f(x)$ into non-trivial factors.

Let $f(x) = p(x).q(x)$ ——— ①

where $p(x)$ & $q(x)$ are polynomials of +ve degree over F and degree of each of them is less than the degree of $f(x)$.

Now $f(a) = 0$

$\Rightarrow p(a).q(a) = 0$

$\Rightarrow p(a) = 0$ or $q(a) = 0$

$\Rightarrow$ a satisfies $p(x)$ or $q(x)$

$\Rightarrow f(x)$ is not a minimal polynomial for a over F ($\because$ degree of $p(x) <$ degree of $f(x)$ & degree of $q(x) <$ degree of $f(x)$)

Which is a contradiction, Hence $f(x)$ is irreducible over F.

Proved

Degree of algebraic element: Let K be an extension of the field F. The element $a \in K$ is said to be algebraic of degree n over F, if it satisfies a non-zero polynomial of degree n over F, but no non-zero polynomial of degree less than n over F.

In other words an element $a \in K$ is said to be algebraic of degree n over F if the degree of minimal polynomial for a over F is n.

Algebraic Extension An extension K of a field F is said to be algebraic extension of F if every element of K is algebraic over F.

If there exists an element $a \in K$ which is not algebraic over F, then K is called transcendental extension of F.

Ex: ① The field $\mathbb{C}$ of complex number is an algebraic extension of $\mathbb{R}$, the field of real numbers.

② The field $\mathbb{R}$ of real numbers is not an algebraic extension of $\mathbb{Q}$, the field of rational numbers. ($\because \pi \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$.)

Theorem: Let K be an extension of F. If $a \in K$ be an algebraic element of degree n over F, then

$$F(a) = \left\{ \beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_{n-1} a^{n-1} \,\middle|\, \beta_0, \beta_1, \cdots \beta_{n-1} \in F \right\}$$

Also expression for each element of F(a) in the form $\beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_{n-1} a^{n-1}$ is unique.

Proof: If $n = 1$ then $a \in F$

$\Rightarrow F(a) = F$.

The statement of theorem is true for $n = 1$

Let $a \in K$ is algebraic over F of degree n where $n>1$.

$\Rightarrow$ There exists a minimal polynomial of degree n for 'a' over F

Let $p(x) = x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + \alpha_n$ be minimal polynomial for 'a' over F.

$$\Rightarrow p(a) = 0$$

$$\Rightarrow a^n + \alpha_1 a^{n-1} + \alpha_2 a^{n-2} + \cdots + \alpha_n = 0$$

$$\Rightarrow a^n = -(\alpha_1 a^{n-1} + \alpha_2 a^{n-2} + \cdots + \alpha_n) \quad \text{---(1)}$$

Multiplying a on both sides

$$\Rightarrow a^{n+1} = -(\alpha_1 a^n + \alpha_2 a^{n-1} + \cdots + \alpha_n)$$

$$\Rightarrow a^{n+1} = -\{-\alpha_1(\alpha_1 a^{n-1} + \alpha_2 a^{n-2} + \cdots + \alpha_n) + \alpha_2 a^{n-2} + \cdots + \alpha_n\}$$

$\Rightarrow a^{n+1}$ is linear combination of elements $1, a, a^2, \cdots a^{n-1}$ over F.

We can continue above process to show that a^{k+1} is a linear combination of elements $1, a, \cdots a^{n-1}$ over F.

Now let $T = \{\beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_{n-1} a^{n-1} \mid \beta_0, \beta_1 \cdots \beta_{n-1} \in F\}$

We want to show that $T = F(a)$.

So at first we will show that T is a subfield of K.

Let $u = \beta_0 + \beta_1 a + \beta_2 a^2 + \cdots + \beta_{n-1} a^{n-1}$

& $v = \gamma_0 + \gamma_1 a + \gamma_2 a^2 + \cdots + \gamma_{n-1} a^{n-1}$

be two elements of T.

Then $u - v = (\beta_0 - \gamma_0) + (\beta_1 - \gamma_1)a + (\beta_2 - \gamma_2)a^2 + \cdots + (\beta_{n-1} - \gamma_{n-1})a^{n-1}$ is also an element of T.

Let $u = \beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1} (\neq 0)$ be an element of T.

Let $q(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1} \in F[x]$.

then obviously $q(a) \neq 0$

We claim that $q(x)$ is not a divisor of $p(x)$ because if $q(x)$ is a divisor of $p(x)$, then we must have $p(x) = (a_0x + a_1)q(x)$ —— (1)

where $a_0x + a_1$ is non-zero polynomial in $F[x]$.

Putting $x = a$ in (1) we get

$$p(a) = (a_0a + a_1)q(a)$$

$$\Rightarrow 0 = (a_0a + a_1)q(a)$$

$$\Rightarrow a_0a + a_1 = 0 \quad (\because q(a) \neq 0)$$

$\Rightarrow a$ satisfies a polynomial $a_0x + a_1$ whose degree is 1 which is a contradiction

Hence $q(x)$ does not divide $p(x)$

Since $p(x)$ is irreducible, and $q(x)$ does not divide $p(x)$. so $p(x)$ and $q(x)$ are relatively prime so $\exists$ polynomial $r(x)$ & $s(x)$ such that

$$p(x).r(x) + q(x).s(x) = 1$$

Putting $x = a$ we get

$$p(a).r(a) + q(a).s(a) = 1$$

$$\Rightarrow q(a).s(a) = 1 \quad [\because p(a) = 0]$$

$$\Rightarrow u.s(a) = 1.$$

$\Rightarrow s(a)$ is multiplicative inverse of u.

Now in $f(a)$ all powers of a higher than $n-1$ can be replaced by linear combinations of $1, a, a^2, \dots a^{n-1}$ over F

$$\Rightarrow f(a) \in T.$$

$$\text{ie } u^{-1} \in T$$

Now in the product $u^{-1}v$ all powers of a higher than $n-1$ can be replaced by linear combination of $1, a, a^2, \dots a^{n-1}$ over F, Therefore $u \neq 0$, & $v \in T$

$$\Rightarrow u^{-1}v \in T$$

Thus T is a subfield of K.

Also from the definition T, it is clear that a & F both are in T.

Also any subfield of K containing F & a also contains T. Thus

$$T = F(a)$$

Now let $u \in T$ & $u = \beta_0 + \beta_1 a + \dots + \beta_{n-1} a^{n-1}$ & also $u = \gamma_0 + \gamma_1 a + \dots + \gamma_{n-1} a^{n-1}$, then

$$\beta_0 + \beta_1 a + \dots + \beta_{n-1} a^{n-1} = \gamma_0 + \gamma_1 a + \dots + \gamma_{n-1} a^{n-1}$$

$$\Rightarrow (\beta_0 - \gamma_0) + (\beta_1 - \gamma_1) a + \dots + (\beta_{n-1} - \gamma_{n-1}) a^{n-1} = 0$$

Thus $h(x) = (\beta_0 - \gamma_0) + (\beta_1 - \gamma_1) x + \dots + (\beta_{n-1} - \gamma_{n-1}) x^{n-1} \in F[x]$

$h(x)$ must be zero polynomial otherwise a will not be algebraic of degree n over F. ($\because$ degree of $h(x) < n$)

$$\Rightarrow h(x) = 0$$

$$\Rightarrow \beta_0 - \gamma_0 = 0, \ \beta_1 - \gamma_1 = 0, \ \dots \ (\beta_{n-1} - \gamma_{n-1}) = 0$$

$$\Rightarrow \beta_0 = \gamma_0, \ \beta_1 = \gamma_1, \ \dots \ \beta_{n-1} = \gamma_{n-1}$$

$\Rightarrow$ The expression $u = \beta_0 + \beta_1 a + \beta_2 a^2 + \dots + \beta_{n-1} a^{n-1}$ is unique. Hence the theorem.