**Thm:** Let K be an extension of a field F and let K be algebraic over F. Suppose 'a' satisfies an irreducible polynomial $p(x)$ in $F[x]$ then $p(x)$ must be a minimal polynomial for a over F.

**Proof:** Let $M = \{f(x) \in F[x] : f(a) = 0\}$.

We claim that M is an ideal of $F[x]$.

Let $f(x)$ & $g(x) \in M$

$\Rightarrow f(a) = 0$ & $g(a) = 0$

$\Rightarrow f(a) - g(a) = 0$

$\Rightarrow f(x) - g(x) \in M$

Let $f(x) \in M$ and $h(x) \in F[x]$.

$\Rightarrow f(a) = 0$

$\Rightarrow f(a) \cdot h(a) = 0$ & $h(a) \cdot f(a) = 0$

$\Rightarrow f(x) \cdot h(a) \in M$ & $h(x) \cdot f(x) \in M$

Hence M is an ideal of $F[x]$.

Also $M \neq F[x]$

$\because f(x) = 1 \in F[x]$

but $f(x) \notin M$ as $f(a) = 1 \neq 0$

Now, $p(x)$ is irreducible polynomial in $F[x]$

Let $N = (p(x))$ be ideal of $F[x]$ generated by $p(x)$

$\Rightarrow$ N is maximal ideal of $F[x]$ as $F[x]$ is Euclidean ring

Also $p(x) \in M$ as $p(a) = 0$

Let $n(x) \in N$

$\Rightarrow n(x) = m(x) \cdot p(x) \quad (\because N = (p(x)))$

Also $n(a) = m(a) \cdot p(a) = m(a) \cdot 0 = 0$

$\Rightarrow n(x) \in M$

Thus $N \subseteq M$.

Now Since $N$ is maximal ideal and $M \neq F[x]$

Also $N \subseteq M \subseteq F[x]$

$\Rightarrow N = M.$

$\Rightarrow M = (p(x))$.

Now, Suppose $p(x)$ is not a minimal polynomial for a over $F$. Let $q(x)$ be polynomial in $F[x]$ of degree lower than that $p(x)$ and satisfied by $a$.

Since $q(a) = 0 \Rightarrow q(x) \in M$

~~Also~~ $\Rightarrow q(x) = p(x) \cdot r(x)$ for some $r(x) \in F[x]$

$\Rightarrow$ degree of $q(x) \geq$ degree of $p(x)$

Which is a contradiction

Hence $p(x)$ must be a minimal polynomial.

**Thm:** Let $K$ be an extension of a field $F$. Then the element $a \in K$ is algebraic over $F$ if & only if $F(a)$ is finite extension of $F$.

**Proof:** Let $F(a)$ is a finite extension of $F$. We want to prove that $a$ is algebraic over $F$.

Let $[F(a) : F] = m$

Since $F(a)$ is a field and $a \in F(a)$, therefore $m+1$ elements $1, a, a^2, \ldots a^m$ are all in $F(a)$

Also dimension of vectorspace $F(a)$ over $F$ is $m$ so any $m+1$ vectors are linearly dependent over $F$.

So $\exists$ elements $\alpha_0, \alpha_1, \cdots \alpha_m \in F$ not all zeros such that

$$\alpha_0 \cdot 1 + \alpha_1 \cdot a + \alpha_2 a^2 + \cdots + \alpha_m a^m = 0$$

$\Rightarrow$ $a$ satisfies the polynomial (non-zero)

$$f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_m x^m \in F[x]$$

$\Rightarrow$ $a$ is algebraic over $F$.

Conversely let $a \in K$ be algebraic over $F$. We want to show that $F(a)$ is finite extension of $F$

Let $p(x)$ be a polynomial over $F$ of lowest positive degree satisfied by $a$. Let degree of $p(x) = n$ then $a$ is algebraic of degree $n$ over $F$.

Therefore $F(a) = \{\beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1} \mid \beta_0, \beta_1 \cdots \beta_{n-1} \in F\}$

$\Rightarrow$ $F(a)$ is a vectorspace over $F$ spanned by the elements $1, a, a^2, \cdots a^{n-1}$

We want to show that $1, a, a^2, \cdots a^{n-1}$ is Linearly independent over $F$.

Let $\gamma_0 + \gamma_1 a + \gamma_2 a^2 + \cdots \gamma_{n-1} a^{n-1} = 0$

$\Rightarrow$ $a$ satisfies the polynomial

$$q(x) = \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots + \gamma_{n-1} x^{n-1} \in F[x]$$

$\Rightarrow$ $q(x)$ must be a zero polynomial because $p(x)$ is minimal polynomial of $a$ whose degree is $n$.

$$\Rightarrow \gamma_0 = 0, \gamma_1 = 0, \cdots \gamma_{n-1} = 0$$

$\Rightarrow 1, a, a^2, \ldots a^{n-1} \in F(a)$ are linearly independent over F. Also $1, a, a^2, \ldots a^{n-1}$ spans $F(a)$

Thus $1, a, a^2, \ldots a^{n-1}$ is a basis for $F(a)$ over F

Hence $[F(a) : F] = n$

ie $F(a)$ is finite extension of F.

**Thm:** Every finite extension K of a field F is algebraic.

**Proof:** Suppose K is finite extension of F.

We want to show that K is algebraic extension of F. ie to show that every element a in K is algebraic over F. Let $[K:F] = m$

Since K is a field and $a \in K$

$\Rightarrow 1, a, a^2, \ldots a^m$ are all in K.

Since dimension of K over F is m

$\Rightarrow$ m+1 elements $1, a, \ldots a^m$ of K are linearly dependent over F.

So $\exists\ \alpha_0, \alpha_1, \alpha_2, \ldots \alpha_m \in F$ not all zeros such that

$$\alpha_0 \cdot 1 + \alpha_1 a + \alpha_2 a^2 + \ldots \alpha_m a^m = 0$$

$\Rightarrow$ a satisfies a polynomial

$$q(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_m a^m \in F[x]$$

of degree at most m.

$\Rightarrow$ a is algebraic over F

Hence the theorem

(Proved)