

Theorem: If K is an extension of a field F and $\textcircled{1}$
 let a_1, a_2, \dots, a_n be n elements of K algebraic ^{over} F
 then $F(a_1, a_2, \dots, a_n)$ is finite extension of F and
 consequently algebraic extension of F .

Proof We have $F \subseteq F(a_1) \subseteq F(a_1, a_2) \dots \subseteq F(a_1, a_2, \dots, a_n) \subseteq K$

Since a_k is algebraic over F

$\Rightarrow a_k$ is algebraic over $F(a_1, a_2, \dots, a_{k-1})$

$\Rightarrow (F(a_1, a_2, \dots, a_{k-1}))(a_k)$ is finite extension of $F(a_1, \dots, a_{k-1})$

$\Rightarrow F(a_1, a_2, \dots, a_k)$ is finite extension of $F(a_1, a_2, \dots, a_{k-1})$

$\Rightarrow [F(a_1, a_2, \dots, a_k) : F(a_1, a_2, \dots, a_{k-1})] = \lambda_k$ for $k=1, 2, \dots, n$

Now $[F(a_1, a_2, \dots, a_n) : F] = [F(a_1, a_2, \dots, a_n) : F(a_1, a_2, \dots, a_{n-1})]$
 $\times [F(a_1, a_2, \dots, a_{n-1}) : F(a_1, a_2, \dots, a_{n-2})]$
 $\times \dots \times [F(a_1) : F]$

$\Rightarrow [F(a_1, a_2, \dots, a_n) : F] = \lambda_n \lambda_{n-1} \dots \lambda_1$ (which is finite)

Hence $F(a_1, a_2, \dots, a_n)$ is a finite extension of F

Consequently $F(a_1, a_2, \dots, a_n)$ is algebraic extension of F (Proved)

Th^m: If K is an extension of field F , then elements
 in K which are algebraic over F form a subfield
 of K . In other words, if a, b in K are algebraic
 over F , then $a+b, a-b, a \cdot b$ and $\frac{a}{b}$ (if $b \neq 0$) are also
 algebraic over F .

Proof Suppose a, b in K are algebraic over F .

Since b is algebraic over F , it is also algebraic

over $F(a)$. ($\because F(a)$ is superfield of F)

Since b is algebraic over $F(a)$

$\Rightarrow (F(a))(b) = F(a, b)$ is a finite extension of $F(a)$

$\therefore [F(a, b), F(a)] = \text{finite}$

Now $[F(a, b), F] = [F(a, b), F(a)][F(a), F]$ is also finite

$\Rightarrow F(a, b)$ is finite extension of F

$\Rightarrow F(a, b)$ is algebraic extension of F

Since $a, b \in F(a, b)$

$\Rightarrow a+b, a-b, a \cdot b$ & $\frac{a}{b} (b \neq 0)$ are all algebraic over F (Prmo)

Thm If L is an algebraic extension of K and K is algebraic extension of F , then L is algebraic extension of F .

Proof Let $a \in L$,

Since L is algebraic extension of K

$\Rightarrow \exists$ some polynomial $x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \dots + \alpha_n$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in K$, such that 'a' satisfies the polynomial.

Since K is algebraic extension of F , therefore

$\alpha_1, \alpha_2, \dots, \alpha_n$ are algebraic over F .

So $M = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ is a finite extension over F . Now a satisfies the polynomial

$$x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \dots + \alpha_n$$

whose coefficients are elements of M .

Therefore a is algebraic over M . ③

$\Rightarrow M(a)$ is finite extension of M .

Now, Since $M(a)$ is finite extension of M & M is finite extension of F , therefore $M(a)$ is finite extension of F . So a is algebraic over F .

Since any arbitrary element a of L is algebraic over F , so L is algebraic extension of F .

Roots of Polynomial: Let F be any field and $p(x) \in F[x]$.

Then an element a lying in some extension field of F is called a root of $p(x)$ if $p(a) = 0$.

Thm: Remainder theorem

If $p(x) \in F[x]$ and K is an extension of F , then for any $c \in K$, $p(x) = (x-c)q(x) + p(c)$ where $q(x) \in K[x]$ and $\deg q(x) = \deg p(x) - 1$.

Proof

We have $F \subseteq K$

$$\Rightarrow F[x] \subseteq K[x]$$

$$\Rightarrow p(x) \in K[x]$$

$$\text{Also } x-c \in K[x]$$

So by division algorithm \exists polynomials $q(x)$ and $r(x)$ in $K[x]$ such that

$$p(x) = (x-c)q(x) + r(x).$$

where either $r(x)$ is constant polynomial or $\deg r(x) < \deg(x-c)$

Since $\deg(x-c) = 1$ so $r(x)$ must be a constant polynomial

We can write $\delta(x) = \delta$ where $\delta \in K$.

Thus we have $p(x) = (x-c)q(x) + \delta$ — (1)

$$\Rightarrow p(c) = (c-c)q(c) + \delta$$

$$\Rightarrow p(c) = 0 \cdot q(c) + \delta$$

$$\Rightarrow p(c) = \delta \quad \text{--- (2)}$$

Therefore $p(x) = (x-c)q(x) + p(c)$ — (3)

Now suppose degree of $p(x) = n$
and degree of $q(x) = m$.

The degree of polynomial on RHS of (3) is $m+1$
So by definition of equality of two polynomials
 $n = m+1$

$$\text{ie } m = n-1$$

$$\Rightarrow \deg q(x) = \deg p(x) - 1$$

Proved.

Factor theorem:

If $a \in K$ is a root of $p(x) \in F[x]$ where
 $F \subseteq K$ then in $K[x]$ $(x-a) \mid p(x)$.

Proof Let $p(x) \in F[x]$ and $a \in K$ where K is extension
field of F . By remainder theorem in $K[x]$ we have

$$p(x) = (x-a)q(x) + p(a)$$

$$\Rightarrow p(x) = (x-a)q(x) \quad (\because p(a) = 0 \text{ as } a \text{ is root of } p(x))$$

$$\Rightarrow (x-a) \mid p(x) \text{ in } K[x]$$

(Proved)