

## Def<sup>n</sup> Extension field:

Suppose  $F$  is a field, then a field  $K$  is said to be an extension of  $F$  if  $F$  is a subfield of  $K$ .

Note: If  $F$  is a subfield of  $K$ , then  $K$  can be regarded as a vector space over  $F$  under ordinary field operations in  $K$ .

## Degree of field extension:

Let  $K$  be an extension of a field  $F$ . The dimension of  $K$  as a vector space over  $F$  (ie dimension of vector space  $K(F)$ ) is called degree of  $K$  over  $F$ .

Note: We will denote degree of  $K$  over  $F$  by  $[K:F]$ .

## Finite field Extension:

Let  $K$  be an extension of the field  $F$ . Then  $K$  is said to be a finite extension of  $F$  if the degree of  $K$  over  $F$  is finite.

ie  $K$  is a finite extension of  $F$  if the vector space  $K(F)$  is finite dimensional.

Ex: ①. If  $F$  is any field, then  $F$  can be treated as a subfield of  $F$ . Therefore  $F$  can be thought of an extension of  $F$ .

As the dimension of vector space  $F(F)$  is one [ $\because$  unity element  $1$  is a basis]. So degree of  $F$  over  $F$  is one ie  $[F:F] = 1$ .

Ex ②: The field  $C$  of complex numbers is a finite extension of the field  $R$  of real numbers.

The dimension of  $C(R)$  is two. [ $\because \{1, i\}$  is a basis] so degree of  $C$  over  $R$  is 2 ie  $[C:R] = 2$

Ex. 3. The field  $Q(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in Q\}$  <sup>(2)</sup>  
is a finite extension of field  $Q$ . The dimension of  
 $Q(\sqrt{2}, \sqrt{3})$  over  $Q$  is four [ $\because \{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$  is a basis].

So degree of  $Q(\sqrt{2}, \sqrt{3})$  over  $Q$  is 4 i.e.  $[Q(\sqrt{2}, \sqrt{3}), Q] = 4$

Transitivity of finite extension.

Thm: If  $L$  is finite extension of  $K$  and  $K$  is finite extension of  $F$ , then  $L$  is a finite extension of  $F$ .  
Moreover  $[L:F] = [L:K][K:F]$ .

Proof Let  $K$  is subfield of  $L$  and  $F$  is subfield of  $K$ , and let  $[L:K] = m$  &  $[K:F] = n$ .  
Suppose  $\alpha_1, \alpha_2, \dots, \alpha_m$  is a basis of  $L$  over  $K$  and  
 $\beta_1, \beta_2, \dots, \beta_n$  is a basis of  $K$  over  $F$ .  
Since  $K \subseteq L$ , therefore  $\beta_1, \beta_2, \dots, \beta_n \in L$  also.

$$\Rightarrow \alpha_i \beta_j \in L \quad \forall i=1, 2, \dots, m \text{ \& } j=1, 2, \dots, n$$

To prove this theorem it is sufficient to prove that  $\{\alpha_i \beta_j \mid i=1, 2, \dots, m, j=1, 2, \dots, n\}$  is a basis of  $L$  over  $F$ .

We will first prove that  $\{\alpha_i \beta_j\}$  generates  $L$  over  $F$ . Let  $\gamma$  be any element of  $L$ .  
Since  $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$  is a basis of  $L(K)$ , therefore  $\gamma$  can be expressed as linear combination of  $\alpha_1, \alpha_2, \dots, \alpha_m$  over the elements of  $K$ .  $\therefore$

So we have

$$\gamma = \sum_{i=1}^m k_i \alpha_i \quad \text{where } k_i \in K. \quad \forall i=1,2,\dots,m. \quad \text{--- (1)}$$

Now  $k_i \in K$  and  $\{\beta_1, \beta_2, \dots, \beta_n\}$  is a basis of  $K(F)$ .

Therefore we have

$$k_i = \sum_{j=1}^n f_{ij} \beta_j \quad \text{where } f_{ij} \in F \quad \forall i=1,\dots,m, \quad j=1,2,\dots,n \quad \text{--- (2)}$$

From (1) & (2)

$$\gamma = \sum_{i=1}^m \left( \sum_{j=1}^n f_{ij} \beta_j \right) \alpha_i$$

$$= \sum_{i=1}^m \sum_{j=1}^n f_{ij} (\alpha_i \beta_j) \quad \text{where } f_{ij} \in F.$$

Thus  $\gamma$  is a linear combination of elements  $\alpha_i \beta_j$  over  $F$ . Therefore the set  $\{\alpha_i \beta_j\}$  of  $mn$  elements generates the vector space  $L(F)$ .

Now we will prove that  $\{\alpha_i \beta_j\}$  is linearly independent over  $F$ .

$$\text{Let } \sum_{i=1}^m \sum_{j=1}^n f_{ij} (\alpha_i \beta_j) = 0$$

$$\Rightarrow \sum_{i=1}^m \left( \sum_{j=1}^n f_{ij} \beta_j \right) \alpha_i = 0$$

$$\Rightarrow \sum_{j=1}^n f_{ij} \beta_j = 0 \quad \text{for } i=1,2,\dots,m.$$

$$\therefore [\alpha_1, \alpha_2, \dots, \alpha_m \text{ are L.I.}]$$

$$\Rightarrow f_{ij} = 0 \quad \text{for } j=1,2,\dots,n, \quad i=1,2,\dots,m$$

$$\therefore [\beta_1, \beta_2, \dots, \beta_n \text{ are L.I.}]$$



$\Rightarrow$  Set  $\{\alpha_i \beta_j\}$  is L.I. over F.

Hence, the set  $\{\alpha_i \beta_j\}$  is a basis of L over F

So L is extension of F. and

$$[L:F] = mn \quad (\because \text{Basis contains } mn \text{ elements})$$

$$\text{i.e. } [L:F] = [L:K] \cdot [K:F]$$

Proved

Thm. If L is finite extension of F and K is a subfield of L which contains F, then  $[K:F] \mid [L:F]$  i.e.  $[K:F]$  is a divisor of  $[L:F]$ .

Proof: Let L, K, F be three fields and  $L \supseteq K \supseteq F$ .

Let  $[L:F]$  is finite and is equal to n.

Let  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  be a basis of L over F. Then  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  generates L over F.

Since  $K \supseteq F$ , therefore any linear combination of  $\alpha_1, \alpha_2, \dots, \alpha_n$  over F is also a linear combination over K. Therefore the set  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  also generates L over K. (It may not be L.I. over K) Since  $L(K)$  is generated by a finite set, so  $L(K)$  is finite dimensional vector space i.e.  $[L:K]$  is finite.

Further  $K(F)$  is subspace of  $L(F)$ . Since  $[L:F]$  is finite, therefore  $[K:F]$  is also finite.

$$[L:F] = [L:K] \cdot [K:F]$$

$$\Rightarrow [K:F] \text{ is divisor of } [L:F]$$

Proved