

# Extension Fields

## Definition

Let  $F$  and  $K$  be fields such that  $F$  is a subring of  $K$ .  $F$  is called a *subfield* of  $K$  and  $K$  is called an *extension field* of  $F$ .

Note that  $K$  (vectors) is a vector space over  $F$  (scalars), called an *F-vector space*, and denoted  $K/F$ . A basis for  $K/F$  is called an *F-basis* for  $K$ . The dimension of  $K/F$  is denoted by  $[K : F] = \dim_F(K)$  and represents the cardinality of an *F*-basis for  $K$ .

If  $[K : F]$  is finite then  $K$  is called a finite extension of  $F$ .

## Example

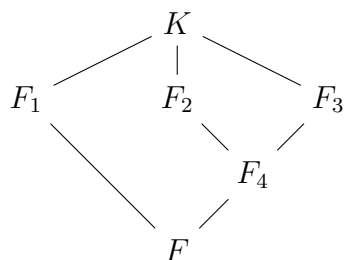
$F$	$K$	$[F : K]$	BASIS
$\mathbb{Q}$	$\mathbb{C}$	$\infty$	
$\mathbb{R}$	$\mathbb{C}$	2	$\{1, i\}$
$\mathbb{Q}$	$\mathbb{Q}(\sqrt{d})$	2	$\{1, \sqrt{d}\}$
$\mathbb{Q}$	$\mathbb{Q}(\sqrt[n]{d})$	$n$	$\{1, \sqrt[n]{d}, \sqrt[n]{d^2}, \dots, \sqrt[n]{d^{n-1}}\}$

## Notation

$K/F$  is sometimes denoted as follows:

$$\begin{array}{c} K \\ | \\ F \end{array}$$

The reason for this is that there may be a tree of subfields of interest:



## Definition: Generated Extension

Let  $K/F$  and  $S \subseteq K$ . The smallest subfield of  $K$  containing both  $F$  and  $S$ , denoted  $F(S)$ , is called the extension of  $F$  *generated* by  $S$  and is the intersection of all extended fields  $L$  of  $F$  such that  $S \subseteq L \subseteq K$ .

## Definition: Simple Extension

Let  $K/F$  and  $\alpha \in K$ . The field extension generated by  $\{\alpha\}$ , denoted  $F(\alpha)$ , is called the *simple* field extension of  $F$  generated by  $\alpha$ , and  $\alpha$  is called a primitive element for  $F(\alpha)/F$ .

Note that  $F(\alpha)$  is the field of fractions for the ring  $F[x]$  with polynomials evaluated at  $\alpha$ :

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in F[x] \text{ and } g(\alpha) \neq 0 \right\}$$

When the  $\alpha$  is algebraic then  $g(\alpha)$  can be eliminated by a technique such as rationalization. Thus,  $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$ ; however  $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$  because  $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$ .

### **Theorem**

Let  $K/L$  and  $L/F$  be field extensions:

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

Furthermore, if  $A$  is an  $F$ -basis for  $L$  and  $B$  is an  $L$ -basis for  $K$  then:

$$AB = \{ab \mid a \in A \text{ and } b \in B\}$$

is an  $F$ -basis for  $K$ .

### **Proof**

Let  $n = [K : L]$  and  $m = [L : F]$

Assume  $c \in K$

$c = \sum_{i=1}^n \ell_i b_i$ , where  $\ell_i \in L$  and  $b_i \in B$

But each  $\ell_i$  can be written as  $\ell_i = \sum_{j=1}^m f_j a_j$ , where  $f_j \in F$  and  $a_j \in A$

So  $c = \sum_{i=1}^n \left( \sum_{j=1}^m f_j a_j \right) b_i = \sum_{i,j} f_{ji} (a_j b_i)$

Therefore  $AB$  spans  $K$ .

Now assume  $\sum_{i,j} f_{ji} (a_j b_i) = 0$  for some finite  $\{a_i b_i\} \subseteq AB$

For a given  $i$ , let  $\ell_i = \sum_j f_{ji} a_j$

$$\sum_i \ell_i b_i = 0$$

But the  $b_i$  are linearly independent and so each  $\ell_i = 0$

So for each  $i$ ,  $\sum_j f_{ji} a_j = 0$

But the  $a_i$  are linearly independent and so each  $f_{ji} = 0$

Therefore the  $a_j b_i$  are linearly independent.

Therefore  $AB$  is an  $F$ -basis for  $K$  and  $[K : L][L : F] = [K : F]$ .