2. Field extensions

Recall the concept of a field:

Definition. A *field* is a commutative ring F such that for every $a \in F \setminus \{0\}$ there exists $b \in F$ satisfying $ab = 1$. In this situation, we write $b = a^{-1}$.

Examples. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ (the finite field with p elements, where p is a prime).

Definition. Let L be a field and K be a subfield of L. Then we say that L is an *extension* of K and that L/K is a *field extension*.

Examples. $\mathbb{C}/\mathbb{R}$; $\mathbb{C}/\mathbb{Q}$; $\mathbb{F}/\mathbb{Q}$, where $F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Let us prove that F is a subfield of $\mathbb{R}$. If $u = a + b\sqrt{2} \in F$ and $v = c + d\sqrt{2} \in F$ (with $a, b, c, d \in \mathbb{Q}$), then

$$u - v = (a - c) + (b - d)\sqrt{2} \in F$$

and

$$uv = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2} \in F.$$

If $w = a + b\sqrt{2} \in F$ $(a,b \in \mathbb{Q})$ and $w \neq 0$, then

$$w^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in F.$$

Adding elements to a field

Lemma 2.1. *Let L be a field, and let $\{F_\lambda\}_{\lambda \in \Lambda}$ be a family of subfields of L. Then $\cap_{\lambda \in \Lambda} F_\lambda$ is also a subfield of L.*

Proof. Let $F = \cap_{\lambda \in \Lambda} F_\lambda$. Since $0, 1 \in F_\lambda$ for all $\lambda \in \Lambda$, we have $0, 1 \in F$. Let $a, b \in F$. Then $a, b \in F_\lambda$ for all $\lambda \in \Lambda$, so $a - b \in F_\lambda$, and $ab \in F_\lambda$ for all $\lambda \in \Lambda$. Thus, $a - b \in F$ and $ab \in F$. Let $c \in F \setminus \{0\}$. Then $c^{-1} \in F_\lambda$ for all $\lambda \in \Lambda$, whence $c^{-1} \in F$. Hence, F is a subfield of L. □

Definition. Let L/K be a field extension, and let $A \subseteq L$ be a subset. We denote by $K(A)$ the intersection of all subfields of L that contain both K and A. We say that $K(A)$ is the *subfield of L generated by A over K* (alternatively, *generated by $K \cup A$*).

Note that $K(A)$ is indeed a subfield by Lemma 2.1.

If $A = \{a_1, \ldots, a_n\}$, we write $K(a_1, \ldots, a_n)$ for $K(A)$.

Proposition 2.2. *Let L/K be a field extension. Let $A \subseteq L$ be a subset. If $M \subseteq L$ is a subfield containing $K \cup A$, then $K(A) \subseteq M$.*

Proof. Obvious from the definition. $\square$

Remark. This means that $K(A)$ is the smallest subfield of L containing $K \cup A$, thus giving an alternative description of $K(A)$. (When we say that M is the smallest subfield containing $K \cup A$, we mean that M contains $K \cup A$ and that any other subfield M' that contains $K \cup A$ contains M.)

Example. We claim that

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Indeed, let F be the RHS. We have previously proved that F is a field. Certainly, F contains $\mathbb{Q}$ and $\sqrt{2}$. So, by Proposition 2.2, $F \supseteq \mathbb{Q}(\sqrt{2})$. On the other hand, since $\mathbb{Q}(\sqrt{2})$ is closed under addition and multiplication, we have $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ for all $a, b \in \mathbb{Q}$. So $F \subseteq \mathbb{Q}(\sqrt{2})$. Thus, $F = \mathbb{Q}(\sqrt{2})$ as claimed.

Proposition 2.3. *Let $K \subseteq L$ be fields and $A, B \subseteq L$. Then*

(i) $K(A \cup B) = K(A)(B)$;
(ii) Suppose that L' is a subfield of L containing both K and A. Then $K(A)$ is the same, whether defined as a subfield of L or as a subfield of L'.

Proof. Exercise. $\square$

Proposition 2.4. *Let $K \subseteq L$ be fields and A be a subset of L. Then $K(A)$ is the set of all elements of L that can be obtained from elements of $K \cup A$ by repeatedly applying the operations of addition, subtraction, multiplication and division.*

Proof. Omitted (exercise): this proposition will not be used directly. $\square$

Degree of an extension

If L/K is a field extension, then L may be viewed as a vector space over K.

Definition. A field extenstion L/K is said to be *finite* if L is a finite-dimensional vector space over K. In this case, the dimension of L as a K-vector space is called the *degree* of the extension L/K and is denoted by $[L : K]$.

Examples.

Extension	Degree	Basis
$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$	2	$\{1, \sqrt{2}\}$
$\mathbb{R}/\mathbb{Q}$	∞	
$\mathbb{C}/\mathbb{R}$	2	$\{1, i\}$
$\mathbb{Q}(i)/\mathbb{Q}$, $i = \sqrt{-1}$	2	$\{1, i\}$

Theorem 2.5 (Tower Law)**.** *Suppose that $K \subseteq M \subseteq L$ are fields.*

(i) The extension L/K is finite if and only if both L/M and M/K are finite.

(ii) If L/K is finite, then

$$[L : K] = [L : M][M : K].$$

Proof. First, suppose that L/K is finite. Then M/K is finite because a subspace of a finite-dimensional vector space is finite. Further, let $\{v_1, \dots, v_s\}$ be a finite set spanning L as a vector space over K. It is clear that $\{v_1, \dots, v_s\}$ also spans L as a vector space over M, which implies that L/M is finite.

It remains to prove the following: if M/K and L/M are finite, then L/K is finite and $[L : K] = [L : M][M : K]$. Let $\{e_1, \dots, e_n\}$ be a basis of L over M and $\{f_1, \dots, f_m\}$ be a basis of M over K. Then $[L : M] = n$ and $[M : K] = m$. Let

$$T = \{e_i f_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}.$$

It suffices to prove that T is a basis of L over K, for then L/K is finite and

$$[M : K] = mn = [M : L][L : K].$$

First, we will prove that T spans L over K. Let $u \in L$. Then

$$u = \sum_{i=1}^{n} a_i e_i \quad \text{for some } a_1, \dots, a_n \in M$$

since $\{e_1, \dots, e_n\}$ is a basis of L over M. Each a_i can be expressed in the form

$$a_i = \sum_{j=1}^{m} b_{ij} f_j \quad \text{where } b_{ij} \in K$$

because $\{f_1, \dots, f_m\}$ is a basis of M over K. Thus,

$$u = \sum_i a_i e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} b_{ij} f_j \right) e_i = \sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij}(f_j e_i).$$

So T spans L over K.

Secondly, let us prove that T is linearly independent over K. Suppose that

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}e_if_j = 0 \quad \text{where } c_{ij} \in K \text{ for all } i, j.$$

For each i, consider

$$w_i = \sum_{j=1}^{m} c_{ij}f_j \in L.$$

Then

$$\sum_{i=1}^{n} w_ie_i = \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}e_if_j = 0.$$

Since $e_1, \dots, e_n$ are linearly independent over M, we deduce that $w_1 = \cdots = w_n = 0$. That is,

$$\sum_{j=1}^{m} c_{ij}f_j = 0 \quad \text{for each } i.$$

But since $f_1, \dots, f_m$ are linearly independent over K, we have $c_{ij} = 0$ for all i, j, as required. □

Example. Consider $L = \mathbb{Q}(\sqrt{2}, i)$. Let $F = \mathbb{Q}(\sqrt{2})$, so $L = F(i)$. First, one can prove that

$$L = \{c + di \mid c, d \in F\}$$

in the same way as in the previous example; that is, $1, i$ span L over F. Thus, $[L : F] = 2$ (as $1, i$ are linearly independent over F and even over $\mathbb{R}$). By Tower Law,

$$[L : \mathbb{Q}] = [L : F][F : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Moreover, by the proof of Tower Law, $\{1, \sqrt{2}, i, i\sqrt{2}\}$ is a basis of L over $\mathbb{Q}$.