1 Simple field extensions

Recall that a *field extension* an injective field homomorphism $K \to M$, often abbreviated as $M \mid K$.

Let $\iota : K \to M$ be a field extension and let $S \subseteq M$ be a subset.

The *field generated by S over K* is the subfield $K(S) \subseteq M$ defined as the intersection

$$K(S) := \bigcap_{\substack{\text{subfields } L \subseteq M \\ \text{with } L \supseteq S \text{ and } L \supseteq \iota(K)}} L$$

of all subfields of M containing both S and $\iota(K)$.

The elements of S are called *generators* of $K(S)$ over K.

The field extension $M \mid K$ is the composition of the natural field extensions $K(S) \mid K$ and $M \mid K(S)$.

Note that if $S = \{s_1, s_2, \dots, s_n\}$ is finite then $K(S)$ can be iteratively generated as

$$K(S) = K(s_1)(s_2)\cdots(s_n) \qquad \text{where we write } K(s) \text{ instead of } K(\{s\}).$$

In this setting we define $K(s_1, s_2, \dots, s_n) = K(S) = K(\{s_1, s_2, \dots, s_n\})$.

Definition. We say that $M \mid K$ is a *simple extension* if there is an element $m \in M$ such that $M = K(m)$.

Example. Let $K = \mathbb{Q}$ and let $M = \mathbb{Q}(i, \sqrt{2})$ be the field generated by i and $\sqrt{2}$ in $\mathbb{C}$.

We claim that M is a simple extension of $\mathbb{Q}$ generated by $i + \sqrt{2}$. Clearly

$$\mathbb{Q}(i + \sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2}),$$

Since $\mathbb{Q}(i + \sqrt{2})$ contains $(i + \sqrt{2})^{-1} = -\frac{1}{3}i + \frac{1}{3}\sqrt{2}$ we have

$$\sqrt{2} = \tfrac{1}{2}(i + \sqrt{2}) + \tfrac{3}{2}(i + \sqrt{2})^{-1} \in \mathbb{Q}(i + \sqrt{2}) \qquad \text{and} \qquad i = \tfrac{1}{2}(i + \sqrt{2}) - \tfrac{3}{2}(i + \sqrt{2})^{-1} \in \mathbb{Q}(i + \sqrt{2})$$

so we also have the reverse containment $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(i + \sqrt{2})$.

Recall that $M \mid K$ is *transcendental* if $\mathrm{Ann}(a) = \{P(x) \in K[x] : P(a) = 0\}$ is zero for some $a \in M$.

A field extension is *algebraic* if it is not transcendental.

Example. Let $M = \mathbb{Q}(x)$ and let $K = \mathbb{Q}$.

Then M is a simple transcendental extension of K generated by x.

Proposition. Let $M \mid K$ be a simple algebraic extension, so that $M = K(\alpha)$ for some $\alpha \in M$.

Let $P(x)$ be the minimal polynomial of α over K, that is, the unique monic irreducible element of $\mathrm{Ann}(a)$.

Then there is an isomorphism of K-extensions $K[x]/(P(x)) \cong M$ sending $x \mapsto \alpha$.

Proof. The existence of the map follows from the definitions.

Since $P(x) \neq 0$ as α is algebraic over K, the ideal $(P(x))$ is maximal in $K[x]$.

Thus the image of $K[x]/(P(x))$ in M is a field. By the definition of M, this field must be all of M. $\square$

Remark. Under the assumptions of the proposition, we have

$$[M : K] = \deg(P)$$

since in the K-vector space $K[x]/(P(x))$ the cosets

$$1 + (P(x)), \quad x + (P(x)), \quad x^2 + (P(x)), \quad \dots \quad x^{\deg(P)-1} + (P(x))$$

form a K-basis.

Corollary. Let $M = K(\alpha) \mid K$ be a simple algebraic extension.
Let $P(x)$ be the minimal polynomial of α over K, and let $L \mid K$ be a field extension.
Then the homomorphisms $M \mid K \to L \mid K$ are in bijection with the roots of $P(x)$ in L.

Proof. If $f : M \to L$ is a K-linear field homomorphism then $P(f(\alpha)) = f(P(\alpha)) = f(0) = 0$.
In this event we see that $f(\alpha) \in L$ is a root of $P(x)$.

Conversely, suppose $\beta \in L$ is a root of $P(x)$.
Then the proposition implies that there is a unique homomorphism $M \mid K \to L \mid K$ sending $\alpha \mapsto \beta$. □

Corollary. A finitely generated algebraic extension is a finite extension.

Example. Let $M = \mathbb{Q}(i) \subseteq \mathbb{C}$ and $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$.
Then $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$ and its roots $\pm i$ do not lie in L.
Hence there are no homomorphisms of field extensions $\mathbb{Q}(i) \mid \mathbb{Q} = M \mid K \to L \mid K = \mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$.

However, there are two homomorphisms $\mathbb{Q}(i) \mid \mathbb{Q} \to \mathbb{C} \mid \mathbb{Q}$.
These correspond to the two roots of $x^2 + 1$.

One homomorphism is the inclusion map, which sends $i \mapsto i$.
The other in the inclusion map composed with complex conjugation, which sends $i \mapsto -i$.

2 Splitting fields

Let K be a field and let $P(x) \in K[x]$ be a polynomial.

Definition. The polynomial $P(x)$ *splits* in K if for some elements $c, a_1, a_2, \dots, a_n \in K$ we have

$$P(x) = c \cdot (x - a_1) \cdot (x - a_2) \cdots (x - a_n).$$

Every constant polynomial splits: this corresponds to taking $n = 0$.

Example. The polynomial $x^2 + 1 = (x - i)(x + i)$ splits in $\mathbb{C}$ but not in $\mathbb{R}$.

Definition. A field L is *algebraically closed* if every polynomial $P(x) \in L[x]$ splits in L.

Remark. If $P(x) \in K[x]$ is irreducible and $\deg(P) > 1$ then one can show that $P(x)$ has no roots in K. In this case $P(x)$ does not split in K.

Definition. A field extension $M \mid K$ is a *splitting extension* (or *splitting field*) for $P(x) \in K[x]$ if

(1) $P(x)$ splits in M, and

(2) M is generated over K by the roots of $P(x)$ in M.

For the next three theorems we fix a polynomial $P(x) \in K[x]$.

Theorem. There exists a splitting field extension $M \mid K$ that is a splitting extension for $P(x)$.

Proof. We argue by induction on $\deg(P)$.
If $\deg(P) = 1$ then $K \mid K$ is a splitting extension for $P(x)$.

Suppose $\deg(P) > 1$ and that the theorem is verified for any polynomial of degree less than $\deg(P)$.
Let P_1 be an irreducible factor of $P(x)$.
Then $M_1 := K[x]/(P_1(x))$ is a field (see the HW).
Also, there is a natural map of rings $K \hookrightarrow M_1$, making it into a field extension.

By definition, $P(x)$ has a root a in M_1, corresponding to x in the presentation $M_1 = K[x]/(P_1(x))$.
Now let M be a splitting field for $P(x)/(x-a) \in M_1[x]$ over M_1, which exists by the inductive hypothesis.
By construction, $P(x)$ splits in M.

Let $a_2 \ldots, a_k$ be the roots of $P(x)/(x-a)$ in M.
Then $M = K(a)(a_2)\ldots(a_k) = K(a, a_2, \ldots, a_k)$ so M is generated over K by its roots in M.
Thus M is a splitting field of $P(x)$ over K. □

Theorem. If $L \mid K$ and $M \mid K$ are both splitting extensions for $P(x)$ then $L \mid K \cong M \mid K$.
(But there may be multiple, equally natural choices for the isomorphism: it is not canonical.)

Proof. We argue again by induction on $\deg(P)$.
If $\deg(P) = 1$ then there is nothing to prove.

Suppose that $\deg(P) > 1$.
Let $a \in M$ be a root of $P(x)$ in M and let $Q(x) \in K[x]$ be its minimal polynomial.
Then $Q(x)$ splits in M and also in L as $Q(x)$ divides $P(x)$.

Let a_1 be a root of $Q(x)$ in L.
Notice that $M \mid K(a)$ is a splitting extension of $P(x)/(x-a) \in K(a)$.
Similarly $L \mid K(a_1)$ is a splitting extension of $P(x)/(x-a_1) \in K(a_1)$.

Now let $J := K[x]/(Q(x))$. The ring J is a field since $Q(x)$ is irreducible.
Furthermore there are isomorphisms of K-extensions

$$J \cong K(a) \qquad \text{and} \qquad J \cong K(a_1).$$

Consider the J-extensions $M \mid J$ and $L \mid J$ arising from these isomorphisms.
By the inductive hypothesis, these J-extensions are isomorphic as

$$\deg(P(x)/(x-a)) = \deg(P(x)/(x-a_1)) < \deg(P).$$

But an isomorphism $M \cong L$ of J-extensions is also an isomorphism of K-extensions. □

Theorem. Suppose $L \mid K$ is a splitting extension for $P(x)$ and $J \mid K$ is any K-extension.
Then the images of all the homomorphisms of K-extensions $L \hookrightarrow J$ coincide.

Proof. If there are no homomorphisms of K-extensions from L to J then the statement is vacuous.

Suppose that there is a homomorphism $\phi : L \hookrightarrow J$ of K-extensions.
We know that L is generated over K by the roots of $P(x)$.
Hence image of ϕ is generated over K by the images of these roots in J under ϕ.
We claim that these images are the roots of $P(x)$ in J.

To see this, let $\alpha_1, \ldots, \alpha_d$ be the roots of $P(x)$ in L, repeated according to their multiplicities.
Then we have

$$P(x) = x^d - e_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + e_2(\alpha_1, \ldots, \alpha_d)x^{d-2} - \cdots + (-1)^d e_d(\alpha_1, \ldots, \alpha_d).$$

where

$$e_k(x_1, \ldots, x_d) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le d} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Thus the elements $\phi(\alpha_1), \ldots, \phi(\alpha_d)$ are the roots of

$$x^d - e_1(\phi(\alpha_1), \ldots, \phi(\alpha_d))x^{d-1} + e_2(\phi(\alpha_1), \ldots, \phi(\alpha_d))x^{a-2} + \cdots + (-1)^d e_d(\phi(\alpha_1), \ldots, \phi(\alpha_d))$$

which is equal to

$$x^d - \phi(e_1(\alpha_1, \ldots, \alpha_d))x^{d-1} + \phi(e_2(\alpha_1, \ldots, \alpha_d))x^{d-2} + \cdots + (-1)^d \phi(e_d(\alpha_1, \ldots, \alpha_d)) = P(x)$$

since the coefficients of $P(x)$ lie in K and ϕ is K-linear.
This shows that the set of roots of $P(x)$ in J does not depend on ϕ, so the theorem follows. □

Note the following useful fact.

Proposition. Let K be a field and let $P(x) \in K[x]$.
Suppose that there is a field extension $K \hookrightarrow L$ where L is algebraically closed.
Let $S \subseteq L$ be the roots of $P(x)$ in L. Then $K(S) \subseteq L$ is a splitting field for $P(x)$.

Proof. This is essentially true by definition since

- $P(x)$ splits in $K(S)$ as L is algebraically closed, and
- $K(S)$ is generated by S, which is exactly the set ot roots of $P(x)$ in $K(S)$.

□

This proposition is often applied when $K = \mathbb{Q}$ and $L = \mathbb{C}$.

For example, from this result we see that $\mathbb{Q}(i)$ is a splitting field for $x^2 + 1$.

It can be shown that for any field K, there is an algebraic extension $K \hookrightarrow \overline{K}$ with $\overline{K}$ algebraically closed. This extension is unique up to (non-canonical) isomorphism and is called the *algebraic closure* of K.

We shall not use this fact, however.