2.B Splitting fields and Algebraic Closure

In this section we develop the basic properties of splitting fields and algebraic closures.

2.B.1 Definition Let K/k be a field extension and let $f \in k[X]$ be a polynomial of positive degree. We say that f splits over K or split in $K[X]$ if f can be written as a product of linear factors in $K[X]$, i.e. $f = a(X-x_1)\cdots(X-x_n)$ for some $a, x_1, \dots, x_n \in K$.

For example, if $f \in k[X]$ and either $\deg f = 1$ or $\deg f = 2$ and f has a zero in k, then f splits over k. We shall prove below that every polynomial in $\mathbb{C}[X]$ splits over $\mathbb{C}$ (this is precisely the fundamental theorem of algebra).
In order to talk about zeros of a given polynomial $f \in k[X]$, we first need to show that there exists a finite field extension K/k that contains the zeros of f, i.e. f splits over K. We prove this in the following:

2.B.2 Theorem (Kronecker) Let $f \in k[X]$ be a polynomial of degree $n \geq 1$. Then there exists a field extension K_1 of k with $[K_1 : k] \leq n$ such that K_1 contains a zero of f. Furthermore, there exists a field extension K of k with $[K:k] \leq n!$ such that f splits over K, i.e. $f = a(X-x_1)\cdots(X-x_n)$, $x_1, \dots, x_n \in K$, $a \in k$.

Proof Let $p(X)$ be an irreducible factor of f in $k[X]$ and $K_1 := k[X]/(p(X))$. Then, since the ideal generated by $p(X)$ is a non-zero prime ideal in a PID $k[X]$, it is a

maximal ideal in $k[X]$ and hence K_1 is a field. Further, the map $k \longrightarrow k[X] \longrightarrow K_1$ is an injective homomorphism of fields and so k is isomorphic to a subfield of K_1. We shall identify k with image in K_1. Note that $[K_1 : k] = \deg p(X) \leq \deg f = n$ (see 2.A.6) and if x is the image of X in K_1, then $p(x) = p(X) = 0$ in K_1, i.e. x is a zero (of p and hence) of f in K_1.
This proves the first part. For the second part we use induction on n. By first part, there exists a field extension $K_1|k$ with $[K_1 : k] \leq n$ such that K_1 contains a zero x_1 of f. Then $f = (X - x_1)\, g$ with $g \in K_1[X]$, $\deg g = n-1$. By induction there exists a field extension $K|K_1$ with $[K : K_1] \leq (n-1)!$ such that g splits over K. But then f splits over K and $[K:k] = [K:K_1][K_1:k] \leq (n-1)! \cdot n = n!$.

2.B.3 Definition Let k be a field.
(1) Let $f \in k[X]$, $\deg f \geq 1$. A field extension $K|k$ is called a splitting field of f over k if f splits over K, i.e. $f = a(X - x_1) \cdots (X - x_n)$, $a \in k$, $x_1, \cdots, x_n \in K$ and $K = k(x_1, \cdots, x_n)$.
(2) Let S be a set of non-constant polynomials in $k[X]$. A field extension $K|k$ is called a splitting field of S over k if each $f \in S$ splits over K and $K = k(\underline{x})$, where $\underline{x} \subseteq K$ is the set of all zeros of all $f \in S$.

Theorem 2.B.2 yields immediately the existence of splitting fields for a finite set of polynomials.

2.B.4 Corollary Let k be a field and let $f_1, \cdots, f_m \in k[X]$

be non-constant polynomials. Then there exists a splitting field for $\{f_1, \cdots, f_m\}$ over k.

<u>Proof</u> Note that a splitting field for $\{f_1, \cdots, f_m\}$ is the same as a splitting field for the product $f = f_1 \cdots f_m$. By 2.B.2 there is a field extension K of k such that f splits over K. Let $x_1, \cdots, x_n \in K$ be all the zeros of f. Then $k(x_1, \cdots, x_n)$ is a splitting field of f over k.

2.B.5 Examples

The following lemma is used to prove that splitting fields are unique up to isomorphism and in a number of other places.

Let $\sigma : k \longrightarrow k'$ be a homomorphism of fields. Then there is an induced ring homomorphism, also denoted by $\sigma : k[X] \longrightarrow k'[X]$, $\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \sigma(a_i) X^i$.

Note that if $f(X) = (X - x_1) \cdots (X - x_n) \in k[X]$, then $\sigma(f(X)) = (X - \sigma(x_1)) \cdots (X - \sigma(x_n)) \in k'[X]$.

This relationship between σ and factorisation of polynomials will help us to study splitting fields.

2.B.6 Lemma Let $\sigma : k \longrightarrow k'$ be an isomorphism of fields, K/k, K'/k' be field extensions and let $x \in K$, $x' \in K'$ be algebraic over k, respectively k'. Then the following statements are equivalent:

(i) There exists an isomorphism $\tau : k(x) \longrightarrow k'(x')$ with $\tau(x) = x'$ and $\tau|k = \sigma$, that is, the diagram

$$\begin{tikzcd} k(x) \arrow[r, "\tau"] & k'(x') \\ k \arrow[u, hook] \arrow[r, "\sigma"] & k' \arrow[u, hook] \end{tikzcd}$$

is commutative

(we also say τ over σ)

(ii) There exists a homomorphism $\tau : k(x) \longrightarrow k'(x')$ over σ with $\tau(x) = x'$

(iii) $\mu_{x', k'} = \sigma(\mu_{x,k})$

Proof (i) $\Rightarrow$ (ii): Trivial.

(ii) $\Rightarrow$ (iii): σ induces an isomorphism of rings, also denoted by $\sigma : k[X] \longrightarrow k'[X]$, $\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=1}^{n} \sigma(a_i) X^i$.

Since $\mu_{x,k}$ is irreducible and monic in $k[X]$, $\sigma(\mu_{x,k})$ is an irreducible and monic in $k'[X]$. Further, (since $\tau|k = \sigma$,) we have

$$\sigma(\mu_{x,k})(x') = \tau(\mu_{x,k})(\tau(x)) = \tau(\mu_{x,k}(x)) = \tau(0) = 0 .$$

Therefore $\mu_{x',k'} = \sigma(\mu_{x,k})$.

<u>(iii) $\Rightarrow$ (i)</u>: Since $\mu_{x',k'} = \sigma(\mu_{x,k})$, the isomorphism $\sigma : k[X] \longrightarrow k'[X]$ of rings induces a commutative diagram

$$\begin{tikzcd}
k[X] \arrow[r, "\approx", "\sigma"'] \arrow[d, two heads, "\pi"'] & k'[X] \arrow[d, two heads, "\pi'"] \\
k[X]/(\mu_{x,k}) \arrow[r, "\approx"] \arrow[d, equal] & k'[X]/(\mu_{x',k'}) \arrow[d, equal] \\
k[x] = k(x) \arrow[r, "\approx", "\tau"'] & k'[x'] = k'(x')
\end{tikzcd}$$

Furthermore, $\tau(x) = \tau(\pi(X)) = \pi'(\sigma(X)) = \pi'(X) = x'$ and $\tau|k = \sigma$.

<u>**2.B.7 Corollary**</u> Let $K|k$ be a field extension and let $x, x' \in K$ be algebraic over k. Then the following statements are equivalent:

(i) There exists a k-isomorphism $\tau : k(x) \longrightarrow k(x')$ such that $\tau(x) = x'$.

(ii) There exists a k-homomorphism $\tau : k(x) \longrightarrow k(x')$ such that $\tau(x) = x'$.

(iii) x and x' have the same monic minimal polynomial over k, i.e. $\mu_{x,k} = \mu_{x',k}$.

Now we prove one of the most important result in Galois theory. It proves the uniqueness of splitting fields, although its main use is to construct automorphisms of a field and hence to calculate the Galois group of a field extension.
First we prove the special case of splitting fields of a single polynomial. The proof of this special case is easy and the argument is useful, many applications of this theorem require this special case only. The proof in the general case use Zorn's lemma and is not very intutive

2.B.8 Theorem Let $\sigma : k \longrightarrow k'$ be an isomorphism of fields and let $f \in k[X]$ be a non-constant polynomial and $f' := \sigma(f) \in k'[X]$ be the corresponding polynomial Let K/k (resp. K'/k') be a splitting field of f (resp. of f') over k (resp. over k'). Then there exists an isomorphism $\tau : K \longrightarrow K'$ over σ. Furthermore, if $x \in K$ and if x' is a zero of $\sigma(\mu_{x,k})$ in K', then τ can be chosen so that $\tau(x) = x'$.
In particular, any two splitting fields for (a polynomial) $f \in k[X]$ over k are k-isomorphic

Proof We prove the assertion by induction on $n := \deg f$. If $n = 1$, then f splits over k, i.e. $K = k$ and the result is trivial in this case. Now, assume $n > 1$ and that the result is true for splitting fields (of polynomials) of degree less than n. Since f (resp. f') splits over K (resp. K'), we have

$$f = a(X - x_1)\cdots(X - x_n),\ a \in k,\ x_1, \dots, x_n \in K \text{ and}$$
$$f' = a'(X - x_1')\cdots(X - x_n'),\ a' \in k',\ x_1', \dots, x_n' \in K'.$$

Let $g = \mu_{x_1,k}$ and $g' = \sigma(g)$. Then g divides f in $k[X]$ and g' divides f' in $k'[X]$. Therefore $g'(x'_i) = 0$ for some i, $1 \leq i \leq n$, i.e. $g' = \mu_{x'_i,k'}$. We may assume that $i=1$, i.e. $g' = \mu_{x'_1,k'}$. Therefore by 2.B.6 there exists an isomorphism $\sigma_1 : k(x_1) \longrightarrow k'(x'_1)$ over σ with $\sigma_1(x_1) = x'_1$.

Now, $f = (X - x_1)\, g$ in $k(x_1)[X]$ and $f' = (X - x'_1) g'$ in $k'[X]$. Further, $K | k(x)$ (resp. $K' | k'(x'_1)$) is a splitting field of g (resp. g') over $k(x_1)$ (resp. over $k'(x'_1)$) and $\deg g = \deg g' = n-1$. Therefore by induction hypothesis there exists an isomorphism $\tau : K \longrightarrow K'$ over σ_1, i.e. $\tau | k(x) = \sigma_1$. Therefore $\tau : K \longrightarrow K'$ is an isomorphism over σ. The last assertion now follows from 2.B.6.

In 2.B.4 we have proved the existence of splitting fields for a finite subset of polynomials. Suppose that K is a splitting field over k of the set of all non-constant polynomials over k. We shall prove that such a field K exists. Assuming that such a field K exists, we make the following observations:

(1) $K|k$ is algebraic.

(2) If $L|K$ is an algebraic extension, then $L=K$. In particular, K has no algebraic extension. For, if $x \in L$, then x is algebraic over K and hence over k and the monic minimal polynomial $\mu_{x,k} \in k[X]$ splits over K, in particular, $x \in K$.

(3) The existence of K will imply existence of a splitting fields of an arbitrary set of polynomials in $k[X]$.

(4) We shall see later that every algebraic extension $E|k$ is k-isomorphic to a subfield of K. This will allow us to view all algebraic extensions of k as subfields of K.

The above observations lead us to the following:

2.B.9 Definition and Lemma. A field k is called algebraically closed if it satisfies the following equivalent conditions:

(i) There are no algebraic extensions of k other than k itself.

(ii) There are no finite extensions of k other than k itself.

(iii) If $L|k$ is a field extension, then $k = \{x \in L \mid x \text{ is algebraic over } k\}$.

(iv) Every $f(X) \in k[X]$ splits over k.

(v) Every $f(X) \in k[X]$ has a zero in k.

(vi) Every irreducible polynomial in $k[X]$ is linear, i.e. degree 1.

Proof (i) $\Rightarrow$ (ii): Immediate from the fact that any finite extension is algebraic.

(ii) $\Rightarrow$ (iii): Let $x \in L$ be algebraic over k. Then $k(x)$ is a finite extension of k and hence $k(x) = k$, i.e. $x \in k$.

(iii) $\Rightarrow$ (iv): Let $f(X) \in k[X]$ and $L|k$ be a splitting field of f over k. Then $L|k$ is algebraic over k and hence $L = k$ by (iii), i.e. f splits over k.

(iv) $\Rightarrow$ (v): Trivial

(v) $\Rightarrow$ (vi): Let $f \in k[X]$ be an irreducible polynomial. By (v) f has a zero in k and so f has a linear factor. Therefore, since f is irreducible, f must be linear.

(vi) $\Rightarrow$ (i): Let $L|k$ be an algebraic extension and let $x \in L$. Then $[k(x) : k] = \deg \mu_{x,k} = 1$ by (vi), since $\mu_{x,k}$ is irreducible over k. Therefore $x \in k$ and so $L = k$.

2.B.10 Example The fields $\mathbb{Q}$ of rational numbers and $\mathbb{R}$ of real numbers are not algebraically closed, since the polynomial X^2+1 has no zero in $\mathbb{Q}$ or in $\mathbb{R}$. Any finite field k is not algebraically closed, since the polynomial $\prod_{a \in k}(X-a) + 1$ has no zero in k.

The field $\mathbb{C}$ of complex numbers is algebraically closed. This fact is usually referred as the fundamental theorem of algebra and will be proved in

Let $A := \{ x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q} \}$. Then A is a field and the field extension $A/\mathbb{Q}$ is algebraic. Moreover, A is an algebraically closed field. This can be proved easily by using the fact that $\mathbb{C}$ is algebraically closed.

2.B.11 Definition Let k be a field. An <u>algebraic closure of</u> k is an algebraic extension K/k such that K is algebraically closed.

For example, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$ and A is an algebraic closure of $\mathbb{Q}$. However, $\mathbb{C}$ is <u>not</u> an algebraic closure of $\mathbb{Q}$, since $\mathbb{C}$ is not algebraic over $\mathbb{Q}$.

We would like to prove the existence of an algebraic closure of an arbitrary field k. The main difficulty in proving this is set-theoretic rather than algebraic. The basic idea is to apply <u>Zorn's lemma</u> to a suitably chosen set of algebraic field extensions of k.