3.A Normal extensions

In this section we continue to study splitting fields and consider the following two questions:

(1) Let $K|k$ be a splitting field of a subset $S \subseteq k[X]$. Can we determine all the polynomials in $k[X]$ those split over K?

(2) Can we give intrinsic characterisation of K? for example, a one that does not refer to the set S

The answer to both these questions is yes and is given in the following:

3.A.1 Theorem and Definition Let $K|k$ be a field extension. Then the following statements are equivalent:

(i) If an irreducible polynomial $f \in k[X]$ has a zero in K, then all the zeros of f are contained in K i.e. f splits into linear factors over K.

(ii) All k-conjugates of $x \in K$ are contained in K

(iii) $\sigma(K) \subseteq K$ for every $\sigma \in \mathrm{Gal}(\overline{K}/k)$.

(iv) $\sigma(K) \subseteq K$ for every k-embedding $K \xrightarrow{\sigma} \overline{k}$

(v) $\sigma(K) = K$ for every k-embedding $K \xrightarrow{\sigma} \overline{k}$

(vi) $K|k$ is a splitting field over k for some subset $S \subseteq k[X]$

An algebraic field extension $K|k$ is called <u>normal</u> if any one of the above equivalent condition holds.

<u>Proof</u> <u>(i) $\Rightarrow$ (ii)</u> Let $x \in K$ and $y \in \overline{k}$ be a k-conjugate of x, i.e. $\mu_x = \mu_y$ or equivalently y is a zero of the irreducible polynomial $\mu_x \in k[X]$. Therefor since one zero x of μ_x is in K, $y \in K$ by (i).

<u>(ii) $\Rightarrow$ (iii)</u> Let $x \in K$ and let $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Then $\sigma(x)$ is a k-conjugate of x and hence $\sigma(x) \in K$ by (ii). Therefore $\sigma(K) \subseteq K$.

<u>(iii) $\Rightarrow$ (iv)</u> Let $\sigma : K \longrightarrow \overline{k}$ be a k-embedding. Then there exists $\overline{\sigma} : \overline{k} \longrightarrow \overline{k}$ a k-automorphism which extends $\sigma : K \longrightarrow \overline{k}$, i.e. $\overline{\sigma} \in \mathrm{Gal}(\overline{k}/k)$ and $\overline{\sigma}|K = \sigma$. Therefore $\sigma(K) = \overline{\sigma}(K) \subseteq K$ by (iii).

<u>(iv) $\Rightarrow$ (v)</u>. Let $\sigma : K \longrightarrow \overline{k}$ be a k-embedding of K into $\overline{k}$. Then $\sigma(K) \subseteq K$ by (iv) and there-exists an k-automorphism $\overline{\sigma} : \overline{k} \longrightarrow \overline{k}$ with $\overline{\sigma}|K = \sigma$. Therefore $\overline{\sigma}^{-1}|K : K \longrightarrow \overline{k}$ is a k-embedding and hence by (iv) $\overline{\sigma}^{-1}(K) \subseteq K$. Therefore $K = \overline{\sigma}.\overline{\sigma}^{-1}(K) \subseteq \overline{\sigma}(K) = \sigma(K)$ and hence $\sigma(K) = K$.

<u>(v) $\Rightarrow$ (vi)</u> Let $S = \{\mu_x \mid x \in K\} \subseteq k[X]$. Then $K = k\left(\bigcup_{x \in K} V_K(\mu_x)\right)$. To show that K is a splitting field of S over k, it is enough to show that $V_K(\mu_x) = V_{\overline{k}}(\mu_x)$ for every $x \in K$. Let $x \in K$ and let $y \in V_{\overline{k}}(\mu_x)$. Then x and y are k-conjugates. Therefore there exists $\sigma \in \mathrm{Gal}(\overline{k}/k)$ such that $y = \sigma(x)$ and hence $y = \sigma(x) \in \sigma(K) = K$ by (v).

(vi) $\Rightarrow$ (iv) Suppose that K is a splitting field of $S \subseteq k[X]$ over k and that $\sigma: K \longrightarrow \overline{k}$ be a k-embedding. To show that $\sigma(K) \subseteq K$, it is enough to show that for every $x \in K$ which is a zero of some $f \in S$, $\sigma(x) \in K$. Now, since $f(x) = 0$ for some $f \in S$, $0 = \sigma(f(x)) = f(\sigma(x))$, i.e. $\sigma(x)$ is a zero of $f \in S$. Therefore $\sigma(x) \in K$, since every $f \in S$ splits into linear factors over K.

(iv) $\Rightarrow$ (i): Let $f \in k[X]$ be irreducible over k and let $x \in K$ be a zero of f. If $y \in \overline{k}$ is an another zero of f. Then x and y are k-conjugates and so there exists a k-automorphism $\overline{\sigma} \in \mathrm{Gal}(\overline{k}|k)$ such that $\overline{\sigma}(x) = y$. Then, since $\overline{\sigma}|_K : K \longrightarrow \overline{k}$ is an k-embedding, we have $y = \overline{\sigma}(x) = \overline{\sigma}|_K(x) \in (\overline{\sigma}|_K)(K) \subseteq K$ by (iv).

The most useful criterion to show that a field extension is normal is the following:

3.A.2 Corollary Let $K|k$ be an algebraic field extension. Then $K|k$ is normal if and only if K is a splitting field of $\{\mu_x \mid x \in K\} \subseteq k[X]$ over k.

3.A.3 Corollary Every quadratic field extension is normal.

Proof Let $K|k$ be a field extension with $[K:k] = 2$. Then for every $x \in K \setminus k$, $\deg \mu_x = 2$ and hence $\mu_x = (X - x)(X - y)$ with $y \in K$. Therefore K is a splitting field of $\{\mu_x \mid x \in K\}$ over k.

3.A.4 Corollary Let $K|k$ be a normal field extension and let $k \subseteq L \subseteq K \subseteq E$ $\subseteq \overline{k}$ be a chain of fields. If $\sigma : L \longrightarrow E$ be a k-embedding, then $\sigma(L) \subseteq K$.

Proof Since $K|L$ is algebraic, $\sigma : L \longrightarrow E \hookrightarrow \overline{k}$ can be extended to a k-embedding $\tau : K \longrightarrow \overline{k}$. Now, by 3.A.1 $\tau(K)=K$ and hence $\sigma(L) = \tau(L) \subseteq \tau(K) = K$.

3.A.5 (see page 3A/5)

The next theorem shows that every algebraic field extension is contained in a smallest normal field extension.

3.A.6 Theorem Let $K|k$ be an algebraic field extension. Then there exists a unique (upto a k-isomorphism) smallest normal extension $N|k$ with $K \subseteq N$. Moreover, if $K|k$ is finite, then $N|k$ is also finite. If $\overline{k}$ is an algebraic closure of k with $K \subseteq \overline{k}$, then N is the compositum of $\sigma_1(K), \dots, \sigma_n(K)$, where $\sigma_1, \dots, \sigma_n$ are all distinct k-embeddings of K into $\overline{k}$.

Proof Note that $\overline{k}$ is normal over k and if N_1, N_2 are normal extension of k with $K \subseteq N_1 \subseteq \overline{k}$, $K \subseteq N_2 \subseteq \overline{k}$, then $N_1 \cap N_2$ is also normal extension of k containing K. In particular,

$$N = \bigcap_{\substack{K \subseteq \tilde{N} \subseteq \overline{k} \\ \tilde{N}|k \text{ normal}}} \tilde{N}$$

is a smallest normal extension of k and $K \subseteq N$.

Now, assume that $K|k$ is finite. Then $\sigma(K) \subseteq N$ for every k-embedding $\sigma : K \longrightarrow \overline{k}$ by 3.A.4. We note that there are at most $[K:k]$ distinct k-embeddings

3.A.5 Corollary. Let $K|k$ and $L|k$ be algebraic extensions with $K, L \subseteq \bar{k}$. Then:

(1) If both $K|k$ and $L|k$ are normal, then $KL|k$ and $K \cap L|k$ are normal.

(2) If $K|k$ is normal, then $LK|L$ is normal and the Galois group $\mathrm{Gal}(LK|L)$ is isomorphic to a subgroup of the Galois group $\mathrm{Gal}(K|K \cap L)$.

Proof (1) It is clear from 3.A.1 that $K \cap L|k$ is normal if both $K|k$ and $L|k$ are normal. Let $\sigma : KL \longrightarrow \bar{L}$ be a k-embedding. Then $\overset{\text{by 3.A.1}}{}$ $\sigma(K) = K$ and $\sigma(L) = L$, since both $K|k$ and $L|k$ are normal. Therefore $\sigma(KL) = KL$ and hence $KL|k$ is normal by 3.A.1.

(2) Let $\sigma : LK \longrightarrow \bar{k}$ be a L-embedding. Then $\sigma|K : K \longrightarrow \bar{k}$ is a k-embedding and hence $\sigma(K) = K$ by 3.A.1. Since $\sigma(L) = L$, it follows that $\sigma(LK) = LK$ and hence $LK|L$ is normal by 3.A.1.
The map $\varphi : \mathrm{Gal}(LK|L) \longrightarrow \mathrm{Gal}(K/K \cap L)$ defined by $\sigma \longmapsto \sigma|K$ is a group homomorphism and $\sigma \in \mathrm{Ker}\,\varphi \iff \sigma|K = id_K \iff \sigma = id_{LK}$, since $\sigma|L = id_L$. Therefore φ is injective.

$\sigma_1, \cdots, \sigma_n : K \longrightarrow \bar{k}$. Let N_1 be the compositum of $\sigma_1(K), \cdots, \sigma_n(K)$ over k. Then $N_1 \subseteq N$. Further, we shall show that N_1 is normal over; this will prove $N = N_1$. Let $\tau : N_1 \longrightarrow \bar{k}$ be an k-embedding. Then $\tau \circ \sigma_i : K \longrightarrow \sigma_i(K) \subseteq N_1 \xrightarrow{\tau} k$ is also a k-embedding of K into $\bar{k}$ and so $\tau\sigma_i(K) \subseteq N_1$, i.e. $\tau(N_1) \subseteq N_1$, since N_1 is generated by $\sigma_1(K) \cup \cdots \cup \sigma_n(K)$ over k. This proves that N_1 is normal over k.

3.A.7 Definition Let $K|k$ be a field extension and let $\bar{k}$ be an algebraic closure of k with $K \subseteq \bar{k}$. The smallest subfield N of $\bar{k}$ containing K such that $N|k$ is normal is called the normal closure of K over k in $\bar{k}$.

3.A.8 (see page 3A/7)

3.A.9 Theorem Let $K|k$ be a normal field extension. Then every k-embedding $\sigma : L \longrightarrow \bar{K}$ of an intermediate field $k \subseteq L \subseteq K$ into the algebraic closure $\bar{K}$ of K can be extended to an k-automorphism of K.

Proof First extend σ to a k-automorphism τ of $\bar{K}$. By 3.A.1 $\tau|K$ is an automorphism of K, since $K|k$ is normal.

3.A.10 Corollary Every k-embedding $\sigma : K \longrightarrow \bar{k}$ of an algebraic extension $K|k$ into the algebraic closure $\bar{k}$ of k can be extended to an k-automorphism $\tau : N \longrightarrow N$ of the normal closure N of K in $\bar{k}$, i.e. to an element in $\mathrm{Gal}(N|k)$.

Proof Since $\bar{N} = \bar{k}$, apply 3.A.9.

3.A.8 Corollary Let $k \subseteq K \subseteq K'$ be algebraic field extensions of k with $K' \subseteq \overline{k}$ (= an algebraic closure of k) and let N, N' be normal closures of K, K' (in $\overline{k}$) over k, respectively. Then $N \subseteq N'$.

Proof Immediate, since $N'|k$ is normal and $K \subseteq K' \subseteq N'$

3.A.11 Corollary Let $K|k$ be a normal field extension and let L be an intermediate field of $K|k$, i.e. $k \subseteq L \subseteq K$. Then $K|L$ is normal. Further $L|k$ is normal $\Longleftrightarrow$ $\sigma(L) = L$ for every $\sigma \in \mathrm{Gal}(K|k)$.

Proof Every L-embedding of K is also k-embedding and hence $K|L$ is normal by 3.A.1. Let $L|k$ be normal and let $\sigma \in \mathrm{Gal}(K|k)$. Then $\sigma(L) = L$ by 3.A.1. Conversely suppose that $\sigma(L) = L$ for every $\sigma \in \mathrm{Gal}(K|k)$. Let $\overline{K}$ be an algebraic closure of K and $\tau : L \longrightarrow \overline{K}$ be a k-embedding. By 3.A.9 can be extended to $\sigma \in \mathrm{Gal}(K|k)$. Now, by hypothesis $\sigma(L) = L$ and hence $L|k$ is normal by 3.A.1.

3.A.12 Corollary Let $K|k$ and $L|k$ be normal field extensions with $L \subseteq K \subseteq \overline{k}$ (an algebraic closure of k). Then

$$\mathrm{Gal}(K|k) / \mathrm{Gal}(K|L) \simeq \mathrm{Gal}(L|k)$$

$\mathrm{Gal}(K|L)$ is normal in $\mathrm{Gal}(K|k)$ and the quotient group

Proof Let $\varphi : \mathrm{Gal}(K|k) \longrightarrow \mathrm{Gal}(L|k)$ be the map defined by $\sigma \longmapsto \sigma|L$ (note that since $L|k$ is normal, $\sigma|L \in \mathrm{Gal}(L|k)$ by 3.A.1). Clearly φ is a group homomorphism and $\ker\varphi = \mathrm{Gal}(K/L)$. Therefore $\mathrm{Gal}(K/L)$ is a normal subgroup of $\mathrm{Gal}(K/k)$. Further, since every k-automorphism of L can be extended to an k-automorphism of K by 3.A.9 and hence the image of $\varphi = \mathrm{Gal}(L/k)$. Therefore (by isomorphism theorem of groups) φ induces a group isomorphism

$$\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L) \xrightarrow{\approx} \mathrm{Gal}(L/k).$$

Exercises

1. Let $K|k$ be an algebraic extension and let L be an intermediate field of $K|k$, i.e. $k \subseteq L \subseteq K$.

(a) If $K|k$ is normal, then $K|L$ is also normal

(b) If $L|k$ is normal, then L is stable under $\mathrm{Gal}(K|k)$, i.e. $\sigma(L) \subseteq L$ for every $\sigma \in \mathrm{Gal}(K|k)$.

(c) If $K|k$ is normal, then $L|k$ is normal $\iff$ L is stable under $\mathrm{Gal}(K|k)$. Moreover, in this case

$$\mathrm{Gal}\left(K \big| L^{\mathrm{Gal}(K|k)}\right) \cong \mathrm{Gal}(L|k)$$

(d) If $K|L$ and $L|k$ are normal, then $K|k$ need not be normal (Let $x \in \mathbb{R}$ be a real 4-th root of 2 and consider $\mathbb{Q} \subseteq \mathbb{Q}(x^2) \subseteq \mathbb{Q}(x)$).

2. Let $K|k$ be an algebraic extension. Then:

(a) $K|k$ is normal $\iff$ for every normal extension $N|k$ with $K \subseteq N$ and for every k-embedding $\sigma : K \longrightarrow N$ of K into N, we have $\sigma(K) \subseteq K$.

(b) If every element of K belongs to some intermediate field L of $K|k$ with $L|k$ normal, then $K|k$ is normal.

3. Let $K|k$ be a normal field extension and let $f \in k[X]$ be an irreducible polynomial over k.

(a) Let $g, h \in K[X]$ be irreducible factors of f in $K[X]$. Show that there exists $\sigma \in \mathrm{Gal}(K|k)$ such that $\sigma(h) = g$. Further, show by an example that the normality of $K|k$ is necessary.

(b) Suppose that f is not irreducible over K. Then show that f factors over K into irreducible polynomials of the same degree. In particular, if f has a zero in K, then f splits into linear factors over K.

4. Let $K|k$ be a normal extension. Suppose that $x, x', y, y' \in K$ and $\mu_x = \mu_{x'}$, $\mu_y = \mu_{y'}$. Determine whether or not there is an k-automorphism $\sigma \in Gal(K|k)$ such that $\sigma(x) = x'$ and $\sigma(y) = y'$.

5. Let $K|k$ and $L|k$ be normal extensions with $K \subseteq \overline{k}$, $L \subseteq \overline{k}$ and $k = K \cap L$. Show that every k-automorphism $\sigma : K \longrightarrow K$ can be extended to an L-automorphism $\tau : KL \longrightarrow KL$.

6. Let $K|k$ be a finite Galois extension and let $x \in k$ If $\sigma(x) \neq x$ for all $\sigma \in Gal(K|k)$, then show tha $K = k(x)$.