Advanced Algebra I

SPLITTING FIELDS AND NORMAL EXTENSIONS

In this section, we are going to prove the existence and uniqueness of splitting fields. And we introduce the notion of normal extension.

Proposition 0.1. *Let K be a field. And S be a set of polynomial in $K[x]$. Then*

1. *There is a splitting of S over K.*
2. *Any two splitting field are isomorphic.*
3. *If F_1, F_2 are two splitting fields in a fixed algebraic closure $\overline{K}$, then $F_1 = F_2$.*

Proof. In an algebraic closure $\overline{K}$, we pick all roots of polynomials of S, say $\{u_i\}_{i \in I}$. Then $K(u_i)_{i \in I}$ is a splitting field.

Let F_1 and F_2 be two splitting fields, one has an embedding $\sigma : K \to \overline{F_2} = \overline{K}$. This embedding can be extended to $\tilde{\sigma} : F_1 \to \overline{F_2}$ by the extension theorem. One can prove that image of $\tilde{\sigma}$ is in F_2. Hence one has an injective homomorphism $\tilde{\sigma} : F_1 \to F_2$. Similarly there is another one $\tilde{\tau} : F_2 \to F_1$. It's easy to show that these give the isomorphism. □

Proposition 0.2. *Let N be an algebraic extension over K contained in $\overline{K}$. Then the following are equivalent:*

1. *Any K-embedding $\sigma : N \to \overline{K}$ induces an K-automorphism of N.*
2. *N is a splitting field of some $S \subset K[x]$ over K.*
3. *Every irreducible polynomial in $K[x]$ having a root in N splits in N.*

Proof. For (1) ⇒ (2), (3), we prove that for every $u \in N$, with minimal polynomial $p(x)$, then $v \in N$ for every root of $p(x)$. To this end, start with an isomorphism $\sigma : K(u) \to K(v)$. By extension theorem, one can extend it to an embedding $N \to \overline{K(v)} = \overline{K}$. The embedding is an automorphism by (1). Thus, $v = \sigma(u) \in N$.

(3) ⇒ (2) is trivial.

For (2) ⇒ (1). Suppose that N is a splitting field of S over K. Let u be a root of $f(x) \in S$. Let $\sigma : N \to \overline{K}$ be any K-embedding. It's clear that $\sigma(u)$ is a root of $f(x)$, hence $\sigma(u) \in N$. Thus $\sigma(N) \subset N$. Since σ is injective and N/K is algebraic, σ is in fact an isomorphism. □

The property of being normal is not as well-behaved as begin algebraic or finite. For example, it's not preserve after "extension"

Example 0.3. *If F/E and E/K are normal, then F/K is not necessarily normal. For example, take $F = \mathbb{Q}(\sqrt[4]{2}), E = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}$. It's easy to see that a degree 2 extension is always normal, however, $\mathbb{Q}(\sqrt[4]{2})$ is not normal over $\mathbb{Q}$.*

Also let's consider $K \subset E \subset F$. Then F is normal over K implies that F is normal over E. But it doesn't imply that E is normal over K. For example, take $F = \mathbb{Q}(\sqrt[4]{2}, i), E = \mathbb{Q}(\sqrt[4]{2}), K = \mathbb{Q}$

Being normal is preserved by "lifting" and "compositum"

Proposition 0.4. *Let E, F be extensions over K and contained in a field L. If E/K is normal then EF/F is normal. Moreover, if both $E/K, F/K$ are normal, then EF/K is normal.*

Proof. In order to show that EF is normal over F, we look at F-embedding $\sigma : EF \to \overline{F}$. Since σ is identity on F, hence on K. By the extension theorem and the proof of the previous Proposition, one can show that $\sigma_{|E}$ is an automorphism. Hence $\sigma(E) = E$. It follows that

$$\sigma(EF) = \sigma(E)F = EF.$$

Thus EF is normal over F.

Suppose now that $E/K, F/K$ are normal. Let $\sigma : EF \to \overline{K}$ be a K-embedding. We have that $\sigma_{|E}, \sigma_{|F}$ are K-embeddings. One sees that $\sigma(E) = E$ and $\sigma(F) = F$ by the normal assumption. If follows that

$$\sigma(EF) = \sigma(E)\sigma(F) = EF.$$

□