MRQ 2017

School of Mathematics and Statistics

MT5836 Galois Theory

Handout III: Splitting Fields and Normal Extensions

3 Splitting Fields and Normal Extensions

Splitting fields

Let F be a field and consider a polynomial $f(X)$ over the field F. Suppose that there is an extension L of F such that, when $f(X)$ is viewed as a polynomial over L, we can factorize it as a product of linear factors:

$$f(X) = c(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n).$$

We shall then say that $f(X)$ *splits* over L. Necessarily, in such a situation, then the roots α_1, α_2, $\dots$, α_n of $f(X)$ are elements of the field L.

Definition 3.1 Let $f(X)$ be a polynomial over some field F. We say that a field K is a *splitting field* for $f(X)$ over F if K is an extension of F satisfying the following properties:

(i) $f(X)$ splits into a product of linear factors over K, and

(ii) if $F \subseteq L \subseteq K$ and $f(X)$ splits over L, then $L = K$.

Thus, a splitting field for a polynomial $f(X)$ over a field F is an extension K of F in which $f(X)$ splits over K but such that $f(X)$ does not split over any proper subfield of K; that is, K is a minimal field over which $f(X)$ splits.

Lemma 3.2 *Let $f(X)$ be a polynomial over a field F and suppose there is some extension L of F such that $f(X)$ splits over L with roots α_1, α_2, $\dots$, α_n. Then*

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

is a splitting field for $f(X)$ over F.

In particular, in the case of a polynomial $f(X)$ over $F = \mathbb{Q}$, we know that $L = \mathbb{C}$ is a suitable extension to use in the lemma since we know from the Fundamental Theorem of Algebra (proved in *Complex Analysis*) that every polynomial over $\mathbb{Q}$ has roots in $\mathbb{C}$ and hence splits over $\mathbb{C}$. We then obtain a splitting field for $f(X)$ over $\mathbb{Q}$ as $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ where α_1, α_2, $\dots$, α_n are the roots of $f(X)$ in $\mathbb{C}$.

Existence of splitting fields

Theorem 3.4 (Existence of Spitting Fields) *Let $f(X)$ be a polynomial of degree n over a field F. Then there is a splitting field K for $f(X)$ over F with degree $|K : F|$ dividing $n!$.*

Uniqueness of splitting fields and related isomorphisms

Lemma 3.5 *Let $\phi\colon F_1 \to F_2$ be an isomorphism between two fields. Let $f(X)$ be an irreducible polynomial in $F_1[X]$ and write $f^{\phi}(X)$ for the polynomial over F_2 obtained by applying ϕ to the coefficients in $f(X)$. Let α be a root of $f(X)$ and β be a root of $f^{\phi}(X)$ in some extensions of F_1 and F_2, respectively. Then there exists an isomorphism $\psi\colon F_1(\alpha) \to F_2(\beta)$ which extends ϕ and maps α to β.*

To say that ψ *extends* ϕ means that $a\psi = a\phi$ for all $a \in F_1$; that is, the restriction $\psi|_{F_1}$ of ψ to F_1 is the isomorphism ϕ we started with.

Theorem 3.6 *Let $\phi\colon F_1 \to F_2$ be an isomorphism between two fields. Let $f(X)$ be any polynomial in $F_1[X]$ and write $f^{\phi}(X)$ for the polynomial over F_2 obtained by applying ϕ to the coefficients in $f(X)$. Let K_1 be a splitting field for $f(X)$ over F_1 and K_2 be a splitting field for $f^{\phi}(X)$ over F_2. Then there exists an isomorphism $\theta\colon K_1 \to K_2$ which extends ϕ.*

To establish uniqueness of splitting fields, we take $F_1 = F_2 = F$ and ϕ to be the identity map in the above theorem. We phrase this uniqueness in terms of the following definition:

Definition 3.7 Let F be a field and let K_1 and K_2 be extensions of F. An *F-isomorphism* from K_1 to K_2 is a field isomorphism $\psi\colon K_1 \to K_2$ such that

$$a\psi = a \qquad \text{for all } a \in F.$$

We then say K_1 and K_2 are *F-isomorphic.*

Corollary 3.8 (Uniqueness of Splitting Fields) *Let $f(X)$ be a polynomial over a field F. Any two splitting fields for $f(X)$ over F are F-isomorphic.*

Definition 3.9 (i) An *automorphism* of a field F is an isomorphism from F to itself.

(ii) Let K be an extension of the field F. An *F-automorphism* of K is an F-isomorphism from K to itself.

Normal extensions

Definition 3.11 An extension K of a field F is a *normal extension* if every irreducible polynomial over F that has at least one zero in K splits over K.

Theorem 3.13 *A finite extension K of a field F is a normal extensions if and only if K is the splitting field of some polynomial over F.*