Lecture 13 : Normal Extensions

Objectives

(1) Normal extensions and their examples.

(2) Characterization of normal extensions in terms of embeddings and splitting fields.

Key words and phrases: Normal extensions, Galois extensions, Galois group of a Galois extension.

Suppose F is a field and E is a splitting field of $f(x) \in F[x]$. Let $r_1, r_2, \ldots, r_n$ be distinct roots of $f(x)$ in $\overline{F}$. Then $E = F(r_1, r_2, \ldots, r_n)$. Suppose that $a \in E$ and $g(x) =$ irr (a, F). Let $b \in \overline{F}$ be another root of $g(x)$. Then the map $\sigma : F(a) \to F(b)$ given by $\sigma(a) = b$ and $\sigma(c) = c$ for all $c \in F$ is an F-embedding.

Let $\tau : E \to \overline{F}$ be an extension of σ. Then $\tau(r_i) = r_j$ for each i and some j. Hence $\tau(E) \subseteq E$. Since E is a finite dimensional F-vector space and τ is injective, it is also surjective. Hence $\tau(E) = E$. Therefore $b \in E$. This shows that E contains splitting fields of irr (a, F) for all $a \in E$. This property is the defining condition for normal algebraic extensions.

Definition 13.1. *An algebraic extension E/F is called a* **normal extension** *if whenever $f(x) \in F[x]$ is irreducible and has a root in E then $f(x)$ splits into linear factors in $E[x]$.*

Example 13.2. (1) The algebraic closure F^a of a field F is a normal extension of F.

(2) Let ζ be a primitive n^{th} root of unity in $\mathbb{C}$. Then $\mathbb{Q}(\zeta)$ is a normal extension of $\mathbb{Q}$. An element $\alpha \in \mathbb{Q}(\zeta)$ is of the form $g(\zeta)$ for some $g(x) \in \mathbb{Q}[x]$. If β is a root of irr $(\alpha, \mathbb{Q})$ then there is a $\mathbb{Q}-$isomorphism $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ such that $\phi(\alpha) = \beta$. The isomorphism ϕ can be extended to an embedding $\Phi : \mathbb{Q}(\zeta) \to \bar{\mathbb{Q}}$. But $\Phi(\zeta) = \zeta^m$ for some m. Hence $\beta = \phi(f(\zeta)) = f(\zeta^m) \in \mathbb{Q}(\zeta)$. Hence $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a normal extension. Alternatively, note that $\mathbb{Q}(\zeta)$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$.

(3) Every quadratic extension E/F is normal. Let $a \in E \backslash F$. Then irr $(a, F) = f(x) = x^2 + bx + c$ for some $b, c \in F$. Let $f(x) = (x - a)(x - s)$ for some $s \in E$. Hence E is a splitting field of $f(x)$ over F. Hence E/F is a normal extension.,

(4) The extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are normal but the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not a normal extension since the complex roots of irr $(\sqrt[4]{2}, \mathbb{Q})$ are not in $\mathbb{Q}(\sqrt[4]{2})$.

(5) If E/F is a normal extension and K is an intermediate subfield of E/F then E/K is a normal extension.

Lemma 13.3. *Let E/F be an algebraic extension. Let $\sigma : E \to E$ be an $F-$embedding, then σ is an automorphism of E.*

Proof. We need to prove that $\sigma(E) = E$. Let $a \in E$ and $p(x) =$ irr (a, F). Let K be the subfield of E generated by the roots of $p(x)$ in E. Then K is a finite dimensional F-vector space. Since σ is an $F-$embedding, it maps roots of $p(x)$ to its roots. Hence $\sigma(K) \subseteq K$. Since σ is an injective $F-$linear map of the $F-$vector space K, $\dim_F K = \dim_F \sigma(K)$. Hence σ is surjective. $\square$

Theorem 13.4. *Let E/F be an algebraic extension such that $E \subset F^a$. Then the following conditions are equivalent:*
(1) *Every F-embedding $\sigma : E \to F^a$ is an automorphism of E.*
(2) *E is a splitting field of a family of polynomials in $F[x]$.*
(3) *E/F is a normal extension.*

Proof.

$$\begin{tikzcd}
 & F^a \arrow[d, dash] \\
E \arrow[r, "\sigma"] \arrow[d, dash] & \sigma(E) = E \arrow[d, dash] \\
F(a) \arrow[r, "\tau"] \arrow[d, dash] & F(b) \arrow[d, dash] \\
F \arrow[r, "id"] & F
\end{tikzcd}$$

(1) $\Rightarrow$ (2): Let $a \in E$ and $p_a(x) =$ irr (a, F). If $b \in F^a$ is a root of $p_a(x)$ then there is an F-isomorphism $\tau : F(a) \to F(b)$. The embedding $\tau : F(a) \to F^a$ can be extended to an embedding $\sigma : E \to F^a$. But $\sigma(E) = E$. Hence $b \in E$. Thus all roots of $p_a(x)$ are in E. Hence E is a splitting field of the family of polynomials $(p_a(x))_{a \in E}$.

(2) $\Rightarrow$ (3): Let E be a splitting field of $(p_i(x))_{i \in I}$ of polynomials in $F[x]$. Let $a \in E$ and $f(x) =$ irr (a, F). Let b be any other root of $f(x)$ in F^a. Then there is an F-isomorphism $\tau : F(a) \to F(b)$ so that $\tau(a) = b$. The map τ can be extended to an F-embedding $\sigma : E \to F^a$. But σ maps roots of $(p_i(x))_{i \in I}$ to their roots. Hence $\sigma(E) \subset E$. Hence $b \in E$. Thus $f(x)$ splits into linear factors in $E[x]$.

(3) $\Rightarrow$ (1) : Let $\sigma : E \to F^a$ be an F-embedding. Let $a \in E$. Then $p(x) =$ irr (a, F) splits into linear factors in $E[x]$. Since $\sigma(a)$ is a root of $p(x)$, $\sigma(a) \in E$. Hence $\sigma(E) \subseteq E$. By Lemma 13.3, $\sigma(E) = E$. □

Proposition 13.5. *Let E_1, E_2 be subfields of a field E. Let E_1, E_2 be normal extensions of F. Then E_1E_2/F and $E_1 \cap E_2/F$ are normal.*

Proof. Let E_1 and E_2 be normal extensions of F. Let $\sigma : E_1E_2 \to F^a$ be an F-embedding. Then $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2) = E_1E_2$. Similarly observe that $\sigma(E_1 \cap E_2) = \sigma(E_1) \cap \sigma(E_2) = E_1 \cap E_2$. Hence $E_1 \cap E_2$ is a normal extension of F.

□