Lecture 15 : Galois group of a Galois Extension II

Objectives

(1) Artin's Theorem about fixed field of a finite group of automorphisms.
(2) Behavior of Galois group under isomorphisms.
(3) Normal subgroups of the Galois groups and their fixed fields.

Keywords and phrases: Fixed field, Galois correspondence, normal subgroups of Galois group.

The next theorem is perhaps the most important ingredient of the **Fundamental Theorem of Galois Theory** (FTGT). We will need the following

Lemma 15.1. *Let E/F be a separable algebraic extension. suppose that for all $\alpha \in E, \deg\ irr\,(\alpha, F) \leq n$. Then $[E : F] \leq n$.*

Proof. Let $\beta \in E$ be such that $\deg \operatorname{irr}(\beta, F)$ is maximal among $\deg \operatorname{irr}(\alpha, F)$ for $\alpha \in E$. We claim that $E = F(\beta)$. Suppose $E \neq F(\beta)$ and choose $\alpha \in E \setminus F(\beta)$. Then $F(\alpha, \beta)$ is a finite separable extension. By the Primitive Element Theorem, there exists $\eta \in F(\alpha, \beta)$ such that $F(\alpha, \beta) = F(\eta)$. But then $\deg \eta > \deg \beta$. □

The above lemma is not true without separability assumption. For example, $deg_F\ \alpha \leq p$ for all $\alpha \in k(u, v)$, where $F = k(u^p, v^p)$, where k is a field of char $p > 0$. But $[k(u, v) : k(u^p, v^p)] = p^2$.

Theorem 15.2 (**Emil Artin**). *Let E be a field and G a finite group of automorphisms of E. Then*

(1) *E/E^G is a finite Galois extension.*

(2) *$G(E/E^G) = G$.* (3) *$[E : E^G] = |G|$.*

Proof. (1) Let $\alpha \in E$ and $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ and $S = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$. Suppose $|S| = r$. Without loss of generality let $S = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$. If

$\tau \in G$ then $\tau\sigma_1(\alpha), \ldots, \tau\sigma_r(\alpha)$ are distinct. Hence $S = \tau(S)$. So τ restricted to S is a permutation of S. Consider the polynomial

$$f(x) = (x - \sigma_1(\alpha))(x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_r(\alpha)).$$

The coefficient of $f(x)$ are elementary symmetric functions of $\sigma_1(\alpha) \ldots, \sigma_r(\alpha)$. Since $\tau(S) = S$ these elementary symmetric functions are in E^G. Thus $f(x) \in E^G[x]$ is a separable polynomial and $f(\alpha) = 0$. Hence E/E^G is a separable and normal extension. Moreover for all $\alpha \in E$, deg irr $(\alpha, E^G) \leq |G|$. Hence $[E : E^G] \leq |G|$. Thus E/E^G is a finite Galois extension.

(2) and (3) : Since E/E^G is a finite separable extension, $[E : E^G]$ is the number of E^G-embeddings of $E \to E^a$. These embeddings are automorphisms of E as E/E^G is a normal extension. Using (1) and the fact that $G \subseteq G(E/E^G)$, we get

$$|G| \leq |G(E/E^G)| = [E : E^G] \leq |G|.$$

Thus $|G| = |G(E/E^G)| = [E : E^G]$ and so $G = G(E/E^G)$. □

Theorem 15.3. *Let E/F be a Galois extension with Galois group G. Let K_1 and K_2 be intermediate subfields of E/F and $H_1 = G(E/K_1)$, $H_2 = G(E/K_2)$. Let (H_1, H_2) denote the smallest subgroup containing H_1 and H_2. Then*

$$K_1K_2 = E^{H_1 \cap H_2}, \quad K_1 \cap K_2 = E^{(H_1, H_2)}, \quad \text{and } K_1 \subseteq K_2 \iff H_1 \supseteq H_2.$$

Proof. Since E/K_i is Galois for $i = 1, 2$, we have $K_i = E^{H_i} \subset E^{H_1 \cap H_2}$ for $i = 1, 2$. Therefore $K_1K_2 \subset E^{H_1 \cap H_2}$. Conversely, if $\sigma \in G$ fixes K_1K_2 then it fixes K_1 and K_2, consequently $\sigma \in H_1 \cap H_2$. Hence $G(E/K_1K_2) \subseteq H_1 \cap H_2$. Hence $K_1K_2 \supseteq E^{H_1 \cap H_2}$. The remaining statements are obvious. □

Behavior of Galois groups under isomorphisms

Proposition 15.4. *Let E/F be a Galois extension. Let $\lambda : E \to \lambda(E)$ be an isomorphism of fields. Then*

(1) *$\lambda(E)/\lambda(F)$ is a Galois extension.*

(2) *$G(\lambda(E)/\lambda(F)) = \lambda G(E/F)\lambda^{-1} \simeq G(E/F)$.*

Proof. (1) Since E/F is Galois, E is a splitting field of a family of separable polynomials $\{f_i(x) \in F[x] \mid i \in \Lambda\}$. Then $\lambda(E)$ is a splitting field of of the family of polynomials: $\{f_i^{\lambda}(x) \in \lambda(F)[x] \mid i \in \Lambda\}$. Hence $\lambda(E)$ is a Galois extension of $\lambda(F)$.

(2) Define $\psi : G(E/F) \to G(\lambda E/\lambda F)$ by the rule $\sigma \mapsto \lambda\sigma\lambda^{-1}$.

$$\begin{array}{ccccccc} \lambda(E) & \xrightarrow{\lambda^{-1}} & E & \xrightarrow{\sigma} & E & \xrightarrow{\lambda} & \lambda(E) \\ | & & | & & | & & | \\ \lambda(F) & \xrightarrow{\lambda^{-1}} & F & \longrightarrow & F & \xrightarrow{\lambda} & \lambda(F) \end{array}$$

The inverse of ψ is given by the rule $\tau \mapsto \lambda^{-1}\tau\lambda$. Hence ψ is an isomorphism. □

Theorem 15.5. *Let E/F be a Galois extension. Let K be an intermediate subfield of E/F. Then*

(1) *K/F is Galois if and only if $G(E/K) \lhd G(E/F)$.*

(2) *If K/F is Galois, then $G(K/F) \simeq G(E/F)/G(E/K)$*

Proof. (1) and (2) : Let K/F be Galois. Define

$$\psi : G(E/F) \to G(K/F) \text{ by } \psi(\sigma) = \sigma|_K.$$

Since K is a normal extension of F, $\sigma|_K \in G(K/F)$. Since

$$\text{Kernel } \psi = \{\sigma \in G(E/F) \mid \sigma|_K = id_K\} = G(E/K),$$

$G(E/K)$ is a normal subgroup of $G(E/F)$.

Conversely, let $G(E/K) \lhd G(E/F)$. Let $\lambda : E \to E$ be any F-automorphism. We show that $\lambda K = K$. Now

$$\lambda G(E/K)\lambda^{-1} = G(E/\lambda K) = G(E/K),$$

provided $\lambda \in G(E/F)$. Thus $\lambda K = K$. Let $\sigma : K \to F^a$ be an F-embedding. Then σ can be extended to an embedding $\tau : E \to F^a$. Since E/F is Galois, $\tau(E) = E$. Thus $\sigma(K) = K$. Hence K/F is Galois.

□