Lecture 14 : Galois group of a Galois Extension I

Objectives

(1) Galois extension and the Galois group of a Galois extension.
(2) Galois group of a finite extension of finite fields and quadratic extensions.
(3) Galois groups of biquadratic extension.
(4) Galois group of a separable cubic polynomial.
(5) Fundamental Theorem of Galois theory (FTGT).

Keywords and phrases: Biquadratic and cubic extensions, fundamental theorem of Galois Theory.

Definition 14.1. *A field extension E/F is called a* **Galois extension** *if it is normal and separable. The* **Galois group of a Galois extension** *E/F denoted by $G(E/F)$ or $Gal(E/F)$ is the group of all F-automorphisms of E under composition of maps.*

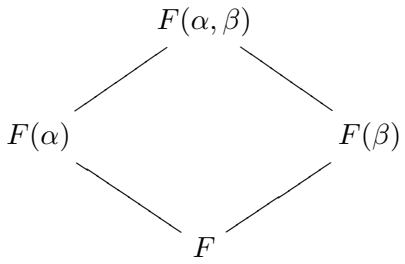
Proposition 14.2. *The Galois group of the Galois extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic group of order n generated by the Frobenious automorphism $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, defined as $\phi(a) = a^q$.*

Proof. Note that ϕ is an $\mathbb{F}_q$-automorphism since any $a \in \mathbb{F}_q$ is a root of $x^q - x$. Let $G = \langle\phi\rangle$. Then $\phi^n(x) = x^{q^n} = x$. Therefore $|G| \leq n$. Suppose $|G| = d$. Then $\phi^d = id$, so $\phi(x) = x^{q^d} = x$. But $x^{q^d} - x$ has atmost q^d roots. Thus $d = n$.

We now show that $G(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\phi\rangle$. Since $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a separable extension, $[\mathbb{F}_{q^n} : \mathbb{F}_q]_s = n$. Hence the number of $\mathbb{F}_q$-automorphisms of $\mathbb{F}_{q^n}$ is n whence $\langle\phi\rangle = G(\mathbb{F}_{q^n}/\mathbb{F}_q)$. □

Example 14.3. Quadratic extensions: Let K/F be a separable quadratic extension. Then for any $\alpha \in K \setminus F$ we have irr $(\alpha, F) = f(x) = x^2 + bx + c$. Let β be another root of $f(x)$. Then $\alpha + \beta = -b$ and $\alpha\beta = c$ and $f(x) = (x - \alpha)(x - \beta) \in K[x]$. Hence K/F is a normal extension. Let $\sigma : K = F(\alpha) \to K$ be a K- automorphism different from id_F. Then $\sigma(\alpha) = \beta$. Thus $G(K/F) = \{id_F, \sigma\}$ is a group of order 2.

Example 14.4. Biquadratic extensions: A field extension K/F is called biquadratic if $[K : F] = 4$ and K is generated by roots of two irreducible quadratic separable polynomials. Let $K = F(\alpha, \beta)$ and $irr(\alpha, F) = x^2 - a$ and $irr(\beta, F) = x^2 - b$.



Since $[F(\alpha, \beta) : F] = 4$, $x^2 - a$ is irreducible over $F(\beta)$ and $x^2 - b$ is irreducible over $F(\alpha)$. Any F- automorphism of K maps α to α or $-\alpha$ and β to β or $-\beta$. Let $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$ and $\tau(\alpha) = \alpha, \tau(\beta) = -\beta$. Then $\sigma\tau = \tau\sigma$ and $\sigma^2 = \tau^2 = id$. Therefore

$$G(K/F) = \{id, \sigma, \tau, \sigma\tau = \tau\sigma\}$$

is the Klein 4-group.

Example 14.5. The Galois group of a separable cubic : Let F be a field of char $\neq 2, 3$. Consider an irreducible cubic polynomial $f(x) = x^3 + px + q \in F[x]$. Thus $f(x)$ has no root in F. Let us observe that $f(x)$ is separable over F. Since $f'(x) = 3x^2 + p$ we have

$$f = \frac{x}{3}(3x^2 + p) + \frac{2p}{3}x + q$$

and hence

$$\gcd(f, f') = \left(\frac{2p}{3}x + q, 3x^2 + p\right).$$

Since f has no root in F, $2px/3 + q$ does not divide $f(x)$. Hence $(f, f') = 1$ and so $f(x)$ is separable. Thus a splitting field E of f must have degree 3 or 6. Let $E = F(\alpha_1, \alpha_2, \alpha_3)$ where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $f(x)$ in E. Then any F- automorphism σ permutes the roots $\alpha_1, \alpha_2, \alpha_3$.

Define $\psi : G(E/F) \to S_3$ by $\psi(\sigma) = p_\sigma$ where p_σ is the corresponding permutation. It is easy to check that ψ is an injective group homomorphism.

Hence $G(E/F) \simeq S_3$ or A_3. Let us see how disc $(f(x))$ determines the Galois group. We identify $G(E/F)$ with a subgroup of S_3. Let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3).$$

Then $\delta^2 = \text{ disc } (f(x)) = -(4p^3 + 27q^2) \in F$. Hence $[F(\delta) : F] \leq 2$. If disc $(f(x))$ is not perfect square in F then $2 \mid [E : F]$. hence $G(E/F) = S_3$. If disc (f) is a square in F then $\delta \in F$ and hence $G(K/F)$ cannot have any odd permutations since these do not fix δ. Thus $G(E/F) = A_3$. For example, if $f(x) = x^3 + x + 1$, then disc $(f) = -31$. Therefore $G(E/F) = S_3$. If $f(x) = x^3 - 3x + 1$, then $G(E/F) = A_3$ as disc $(f) = 3^4$.

The Fundamental Theorem of Galois Theory

Let F be a field. We know that a Splitting field E of a polynomial $f(x) \in F[x]$ is a normal extension of F. If $f(x)$ is separable then E/F is separable. Thus a splitting field of a separable polynomial $f(x) \in F[x]$ is a Galois extension of F. Conversely if E/F is a finite Galois extension then by the Primitive Element Theorem there is an $a \in E$ such that $E = F(a)$. Since E/F is normal, E is a splitting field of irr (a, F). Thus a finite extension E/F is Galois if and only if E is a splitting field of a separable polynomial $f(x)$ over F. We say in this case that $G(E/F)$ is the Galois group of $f(x)$. Since any two splitting fields of $f(x)$ are F-isomorphic, we write $G(E/F) = G_f$.

Definition 14.6. *Let G be a group of automorphism of a field E. Then*

$$E^G = \{a \in E \mid \sigma(a) = a \text{ for all } \sigma \in G\}$$

is called the **fixed field of G acting on E.**

Theorem 14.7 (**Fundamental Theorem of Galois Theory (FTGT)).** *Let E/F be a finite Galois extension. Consider the sets:*

$\mathcal{I} = \{K \mid K \text{ is an intermediate field of } E/F\}$ and $\mathcal{G} = \{H \mid H < G(E/F)\}$.

(i) *The maps:*

$$K \mapsto G(E/K) \text{ and } H \mapsto E^H$$

give a one-to-one correspondence, called the **Galois correspondence** *between $\mathcal{I}$ and $\mathcal{G}$.*

(ii) *K/F is Galois if and only if $G(E/K) \lhd G(E/F)$ and in this case*

$$G(K/F) \simeq \tfrac{G(E/F)}{G(E/K)}.$$

(iii) $[E : K] = |G(E/K)|$.

The FTGT will be proved in several steps. We shall prove parts of it for infinite Galois extensions.

Theorem 14.8. *Let E/F be a Galois extension with $G = G(E/F)$. Then*
(1) $F = E^G$.
(2) *Let K be an intermediate subfield of E/F. Then E/K is Galois and the map $K \mapsto G(E/K)$ is an injective map from $\mathcal{I}$ to $\mathcal{G}$.*

Proof. (1) Let $a \in E^G$. Let $\sigma : F(a) \to \overline{F}$ be an F-embedding. Let $\tau : E \to \overline{F}$ be an extension of σ. Since E/F is Galois, τ is an automorphism of E. Hence $\tau(a) = a$. Therefore $[F(a) : F]_s = 1$. But E/F is separable, so $F(a)/F$ is also separable. Thus $[F(a) : F]_s = [F(a) : F] = 1$. So $a \in F$.
(2) Let K be an intermediate subfield of E/F. Then E/K is separable as E/F is so. Let $\sigma : E \to \overline{K} = \overline{F}$ be a K-embedding. Then it is also an F-embedding. As E/F is normal, σ is an automorphism of E. Thus E/K is a Galois extension. Let $H = G(E/K)$. Then by (1), we have $K = E^H$. Let K and K' be intermediate subfields of E/F. If $H = G(E/K)$ and $H' = G(E/K')$ then $K = E^H$ and $K' = E^{H'}$. Hence the map $K \mapsto G(E/K)$ is an injective map.

□