Lecture 24 : Galois Groups of Quartic Polynomials

Objectives

(1) Galois group as a group of permutations.
(2) Irreducibility and transitivity.
(3) Galois groups of quartics.

Keywords and phrases : Transitive subgroups of S_4 Galois groups of quartics, irreducibilty and transitivity.

Galois group as a group of Permutations

Let $f(x) \in F[x]$ be a monic polynomial with distinct roots $r_1, r_2, \ldots, r_n$. Let $E = F(r_1, r_2, \ldots, r_n)$ and $G = G(E/F)$. Any $\sigma \in G$ permutes the roots of $f(x)$. Define $\psi : G = G(E/F) \to S_n$ by $\psi(\sigma) = \sigma|_R$. Then ψ is an injective group homomorphism. The subgroup $\psi(G)$ is called the Galois group of $f(x)$, and it is denoted by G_f. By the FTGT, there is an intermediate subfield of E/F corresponding to $G_f \cap A_n$.

Theorem 24.1. *Let F be a field of characteristic $\neq 2$ and $f(x) \in F[x]$, a monic polynomial of positive degree with distinct roots $r_1, r_2, \ldots, r_n \in F^a$. Put $E = F(r_1, r_2, \ldots, r_n)$. Put $\delta = \Pi_{1 \leq i < j \leq n}(r_i - r_j)$. Then*

$$E^{G_f \cap A_n} = F(\delta).$$

Proof. Any transposition acting on δ maps δ to $-\delta$. Hence all permutations in $G_f \cap A_n$ fix δ. Thus $F(\delta) \subseteq E^{G_f \cap A_n}$. Let $|G_f / G_f \cap A_n| = d$. Then $d \leq 2$. If $d = 1$ then $G_f \cap A_n = G_f$ and so $G_f \subseteq A_n$. Thus $\delta \in F$. Let $d = 2$. Then $G_f \cap A_n \neq G_f$. So G_f has an odd permutation. Hence $\delta \notin F$. Thus $E^{G_f \cap A_n} = F(\delta)$.

□

Definition 24.2. *A subgroup $H \subset S_n$ is called a transitive subgroup if for any $i \neq j \in \{1, 2, \ldots, n\}$, there exists $\sigma \in H$ such that $\sigma(i) = j$.*

Theorem 24.3. *Let $f(x) \in F[x]$ be a polynomial of degree n with n distinct roots $r_1, r_2, \ldots, r_n$ in F^a. Then $f(x)$ is irreducible if and only if G_f is a transitive subgroup of S_n.*

Proof. ($\Leftarrow$) Suppose G_f is a transitive subgroup of S_n. If $f(x)$ is reducible in $F[x]$ then $f(x) = g(x)h(x)$ for some $g, h \in F[x]$ of positive degree. Let $g(r) = h(s) = 0$ where $r, s \in F^a$. Let $\sigma \in G_f$ be a permutation which maps r to s. We may assume that $g(x)$ is irreducible. But then s has to be a root of $g(x)$. Since $f(x)$ has no repeated roots, $h(x)$ is a constant.

($\Rightarrow$) Suppose $f(x)$ is irreducible. Let r, s be roots of $f(x)$. Then there exists an F-isomorphism $\sigma : F(r) \to F(s)$ such that $\sigma(r) = s$. It can be extended to an automorphism of $F(r_1, \ldots, r_n)$. Hence G_f is transitive.

$\square$

Transitive Subgroups of S_4

Let H be a transitive subgroup of S_n. The orbit of action of H on $[n]$ is $[n]$. Thus $n = |\text{ orbit } (1)| = |H|/|\text{ stab } (1)|$. Hence $n \mid |H|$. The orders of possible Galois groups of irreducible separable quartics are $4, 8, 12$ and 24. These groups are listed below.

(1) $C_4 = \{(1234), (13)(24), (1432), (1)\}$.

   A cyclic group of order 4 has two 4-cycles. There are six 4-cycles in S_4. Thus there are three transitive cyclic subgroups of order 4.

(2) Klein 4 -group $V = \{(1), (12)(34), (14)(32), (13)(24)\}$ is a normal subgroup of S_4.

(3) There are 3- Sylow subgroups of order 8. They are all isomorphic to D_4. These are $H_1 = \langle V, (13)\rangle, H_2 = \langle V, (12)\rangle, H_3 = \langle V, (14)\rangle$.

(4) A_4 is the only subgroup of order 12 and it is normal in S_4.

(5) S_4 is the only subgroup of order 24.

Calculation of Galois group of quartic polynomials

Let F be a field of $char \neq 2, 3$. Let $f(x) = x^4 + b_1x^3 + b_2x^2 + b_3x + b_4 \in F[x]$ be separable. By the change $y = x + \frac{b_1}{4}$ we may assume that there is no x^3 term. This change does not alter the Galois group and the discriminant. So let $f(x) = x^4 + bx^2 + cx + d \in F[x]$ be an irreducible polynomial with roots r_1, r_2, r_3, r_4 in a splitting field E of $f(x)$ over F. We write $G_f \subset S_4$. So $G_f \simeq G(E/F)$. Set

$$\underline{t} = \{t_1 = r_1r_2 + r_3r_4, t_2 = r_1r_3 + r_2r_4, t_3 = r_1r_4 + r_2r_4\}.$$

Proposition 24.4. $E^{G_f \cap V} = F(\underline{t})$ *and* $G(F(\underline{t})/F) = \frac{G_f}{G_f \cap V}$.

Proof. Clearly, $F(t_1, t_2, t_3) \subseteq E^{G_f \cap V}$. The element t_1 is fixed by $H_1 = \langle (12), V) \rangle$, a dihedral group of order 8 in S_4. Moreover

$$S_4 = H_1 \cup (13)H_1 \cup (14)H_1.$$

Thus H_1 is the stabilizer of t_1. Similarly, $H_2 =$ Stab $(t_2) = \langle (13), V) \rangle$, $H_3 =$ Stab $(t_3) = \langle (14), V) \rangle$. Since $V = H_1 \cap H_2 \cap H_3$, if $\sigma \in G_f$ fixes t_1, t_2, t_3 then $\sigma \in V$. Hence $G(E/F(\underline{t})) \subseteq G_f \cap V$ which gives $F(\underline{t}) \supseteq E^{G_f \cap V}$. We know that $F(t_1, t_2, t_3)$ is the splitting field of the resolvent cubic over F, hence it is Galois. Thus $G(F(\underline{t})/F) \simeq \frac{G_f}{G_f \cap V}$. $\square$

Proposition 24.5. *The resolvent cubic of a separable irreducible quartic has a root in F if and only if $G_f \subseteq D_4$.*

Proof. Let $t_1 \in F$. Then $G(E/F(t_1)) = G_f = G_f \cap H_1 \Rightarrow G_f \subseteq H_1$. Conversely if $G_f \subset H_i$ for some i say $i = 1$, then each $\sigma \in G_f$ fixes t_1 and hence $t_1 \in E^{G_f} = F$. $\square$

Theorem 24.6. *Let $f(x)$ be an irreducible separable quartic over a field F of char $F \neq 2$ and $E = F(r_1, r_2, r_3, r_4)$ be a splitting field where $r_1, \ldots, r_4$ are the roots of $f(x)$. Let $r(x)$ denote resolvent cubic of $f(x)$.*

(1) *If $r(x)$ is irreducible in $F[x]$ and disc $(r(x)) \notin F^2$ then $G_f \simeq S_4$.*

(2) *If $r(x)$ is irreducible in $F[x]$ and disc $(r(x)) \in F^2$ then $G_f \simeq A_4$.*

(3) *If $r(x)$ splits completely in $F[x]$ then $G_f \simeq V$.*

(4) *Let $r(x)$ have one root in F. Then*
   - (a) *If $f(x)$ is irreducible over $F(\underline{t})$ then $G_f \simeq D_4$.*
   - (b) *If $f(x)$ is reducible over $F(\underline{t})$ then $G_f \simeq C_4$.*

Proof. Since $f(x)$ is irreducible over F, G_f is a transitive subgroup of S_4. Hence $|G_f| = 4, 8, 12$, or 24, $|G_f \cap V| = 1, 2$ or 4, and $|G_f/G_f \cap V| = |G_{r(x)}| = 1, 2, 3, 6$. Thus $|G_f \cap V| > 1$. We also have $|V \cap G_f| \times |\frac{G_f}{V \cap G_f}| = |G_f|$. Thus $\{2, 4\} \times \{1, 2, 3, 6\} = \{4, 8, 12, 24\}$.

(1) If $r(x)$ is irreducible over F and disc $(r(x)) \in F^2$ then $G_{r(x)} \simeq A_3$. Hence $|G_f/G_f \cap V| = 3$. Hence $|G_f| = 12$ and therefore $G_f \simeq A_4$.

(2) If $r(x)$ is irreducible over F and disc $(r(x))$ is not a square in F, then $G_{r(x)} \simeq S_3$. Hence $|G_f/G_f \cap V| = 6$. Thus $|G_f| = 12$ or 24. If $|G_f| = 12$ then $G_f \simeq A_4$ and $|G_f/G_f \cap V| = 3$ which is a contradiction. Hence $G_f \simeq S_4$.

(3) If $r(x)$ has all its roots in F, then $E^{G_f \cap V} = F = E^{G_f}$. Thus $G_f \subseteq V$. Since $4 \mid |G_f|$, $G_f = V$.

(4) Now let $r(x)$ have exactly one root in F. Then $[F(\underline{t}) : F] = 2 = |G_f/G_f \cap V|$. Thus $|G_f| = 4$ or 8.

(a) Suppose $f(x)$ is irreducible over $F(\underline{t})$. Then

$$[E : F(\underline{t})] = |G_f \cap V| \geq 4 \Rightarrow |G_f| = 8 \Rightarrow G_f \simeq D_4.$$

(b) Suppose $f(x)$ is reducible over $F(\underline{t})$. If $G_f \simeq D_4$ then

$$[E : F] = 8 \Rightarrow [E : F(\underline{t})] = 4.$$

Hence $G(E/F(\underline{t})) = V$ which is transitive. Hence $f(x)$ is irreducible over $F(\underline{t})$. This is a contradiction. So $|G_f| = 4$. If $G_f = V$ then $G_{r(x)} = G_f/G_f \cap V = \{1\}$. But $|G_{r(x)}| = 2$. Thus $G_f \simeq C_4$. $\square$

Example 24.7. (1) ($G_f = V$) Let $f(x) = x^4+1 \in \mathbb{Q}[x]$. Then the resolvent cubic is $r(x) = x(x-2)(x+2)$. Since $f(x)$ is irreducible over $\mathbb{Q}$, $G_f = V$.

(2) ($G_f = C_4$) Consider $f(x) = x^4 + 5x^2 + 5$ which is irreducible over $\mathbb{Q}$ by Eisenstein criterion. Then

$$r(x) = x^3 - 5x^2 - 20x + 100 = (x-5)(x - 2\sqrt{5})(x + \sqrt{5}).$$

Thus $t_1 = 5,\ t_2 = 2\sqrt{5},\ t_3 = -2\sqrt{5}$. Hence $F(\underline{t}) = \mathbb{Q}(\sqrt{5})$ and

$$x^4 + 5x^2 + 5 = \left(x^2 + \tfrac{5+\sqrt{5}}{2}\right)\left(x^2 - \tfrac{5-\sqrt{5}}{2}\right).$$

Therefore $f(x)$ is reducible over $F(\underline{t})$. Thus $G_f \simeq C_4$.

(3) ($G_f = S_4$) Consider $f(x) = x^4 - x + 1$. Then $f(x)$ is irreducible modulo 2, and hence it is irreducible over $\mathbb{Q}$. The resolvent cubic $r(x) = x^3 - 4x - 1$ is irreducible over $\mathbb{Q}$ and disc $(r(x)) = 229 \notin \mathbb{Q}^2$. Hence $G_f = S_4$.

(4) ($G_f = D_4$) The polynomial $f(x) = x^4 - 3$ is irreducible over $\mathbb{Q}$ and $r(x) = x(x + i2\sqrt{3})(x - i2\sqrt{3})$. Therefore $F(\underline{t}) = \mathbb{Q}(i\sqrt{3})$. Hence

$$f(x) = (x^2 - \sqrt{3})(x^2 + \sqrt{3}) = (x - i\sqrt[4]{3})(x + i\sqrt[4]{3})(x + \sqrt[4]{3})(x - \sqrt[4]{3}).$$

Thus $f(x)$ has no root in $\mathbb{Q}(i\sqrt{3})$. The splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt[4]{3})$ which is a degree 8 extension of $\mathbb{Q}$. Hence $G_f = D_4$.

(5) ($G_f = A_4$) Let $f(x) = x^4 - 8x + 12$. Then $r(x) = x^3 - 48x - 64$. Using Eisenstein's criterion, $f(x)$ is irreducible over $\mathbb{Q}$. Since disc $(r(x)) = 2^{12}3^4$ is a perfect square in $\mathbb{Q}$, $G_f = A_4$.

Example 24.8. Let p be a prime number and $f(x) = x^4 + px + p$. Then $r(x) = x^3 - 4px - p^2$. Possible roots of $r(x)$ in $\mathbb{Q}$ are ± 1, $\pm p$, $\pm p^2$. Check that ± 1, $\pm p^2$ are not roots for any p. But $r(p) = p^2(p-5)$ and $r(-p) = p^2(3-p)$. Hence $r(x)$ has a rational root if and only if $p = 3, 5$. For $p \neq 3, 5$, the resolvent cubic is irreducible over $\mathbb{Q}$. Check that disc $(f(x)) = p^3(256 - 27p)$ is never a perfect square in $\mathbb{Q}$. Let G be the Galois group of $f(x)$. Then $G = S_4$ if $p \neq 3, 5$.

If $p = 3$ then $r(x) = (x+3)(x^2 - 3x - 3)$. Hence the splitting field L of $r(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{21})$. Check that $x^4 + 3x + 3$ is irreducible over $\mathbb{Q}(\sqrt{21})$. Hence $G = D_4$.

Now let $p = 5$. The resolvent cubic of $f(x) = x^4 + 5x + 5$ is $r(x) = x^3 - 20x - 25 = (x-5)(x^2 + 5x + 5)$. Hence the splitting field of $r(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{5})$. Check that $f(x)$ has two roots in $\mathbb{Q}(\sqrt{5})$. Hence the Galois group is C_4.