8 Galois Correspondence

Last Updated: 2026–03–13

Galois theory describes a precise relation between subgroups of a Galois group and intermediate subfields of a Galois field extension. This chapter explains this fundamental correspondence.

8.0 The Basic Correspondence

What maps underlie the Fundamental Theorem of Galois Theory?

8.0.0 Corollary. *Let $K \subseteq M$ and $M \subseteq L$ be Galois field extensions. The group* $\mathrm{Gal}(L/M)$ *is a normal subgroup of* $\mathrm{Gal}(L/K)$*, and restriction to M induces a group isomorphism* $\mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K)$.

Proof. When $K \subseteq M$ is Galois, Theorem 7.2.4 shows that $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. Fix $\sigma \in \mathrm{Gal}(L/K)$. The restriction of σ to M gives the isomorphism $\sigma|_M : M \to \sigma(M)$. Since $K \subseteq M$ is Galois, Theorem 7.2.4 also shows that $\sigma(M) = M$, so $\sigma|_M$ is an automorphism of M. As $\sigma|_K = \mathrm{id}_K$, we see that $\sigma|_M \in \mathrm{Gal}(M/K)$. Hence, the map $\Phi\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ defined by $\sigma \mapsto \sigma|_M$ is a group homomorphism, because $(\sigma \circ \tau)|_M = \sigma|_M \circ \tau|_M$.

For any $\sigma \in \mathrm{Gal}(L/K)$, it follows that

$$\sigma \in \mathrm{Ker}(\Phi) \quad \iff \quad \sigma|_M = \mathrm{id}_M \quad \iff \quad \sigma \in \mathrm{Gal}(L/M)\,,$$

so $\mathrm{Ker}(\Phi) = \mathrm{Gal}(L/M)$. The First Isomorphism Theorem implies that Φ induces $\mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/M) \cong \mathrm{Im}(\Phi)$. Lastly, we have

$$|\mathrm{Im}(\Phi)| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L:K]}{[L:M]} = [M:K] = |\mathrm{Gal}(M/K)|\,,$$

so $\mathrm{Im}(\Phi) = \mathrm{Gal}(M/L)$. □

8.0.1 Remark. Consider the tower $\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq L := \mathbb{Q}(\omega, \alpha)$ of field extensions where $\omega := \exp(2\pi\mathrm{i}/3)$ and $\alpha := \sqrt[3]{2}$. As $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ is a Galois field extension and $\mathrm{Gal}\big(L/\mathbb{Q}(\omega)\big) = \langle\sigma\rangle$ where the map $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ satisfies $\sigma(\omega) = \omega$ and $\sigma(\alpha) = \alpha\omega$, the theorem gives

$$\mathrm{Gal}\big(\mathbb{Q}(\omega)/\mathbb{Q}\big) \cong \mathrm{Gal}(L/\mathbb{Q}) \big/ \langle\sigma\rangle \cong \mathfrak{S}_3 \big/ A_3 \cong \mathbb{Z} \big/ \langle 2\rangle \cong \big\{\mathrm{id}_{\mathbb{Q}(\omega)}, \tau|_{\mathbb{Q}(\omega)}\big\},$$

where $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ satisfies $\tau(\omega) = \omega^2$ and $\tau(\alpha) = \alpha$.

8.0.2 Theorem. *Let $K \subseteq L$ be a Galois field extension.*

(fields) *For every intermediate field $K \subseteq M \subseteq L$, the Galois group* $\mathrm{Gal}(L/M) \subseteq \mathrm{Gal}(L/K)$ *has fixed field* $L^{\mathrm{Gal}(K/M)} = M$*,*

$$|\mathrm{Gal}(L/M)| = [L:M]\,, \quad \textit{and} \quad [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/M)] = [M:K]\,.$$

(groups) *For every subgroup $H \subseteq \mathrm{Gal}(L/K)$, its fixed field $K \subseteq L^H \subseteq L$ has Galois group* $\mathrm{Gal}(L/L^H) = H$*,*

$$[L:L^H] = |H|\,, \quad \textit{and} \quad [L^H : K] = [\mathrm{Gal}(L/K) : H]\,.$$

Proof. The first part summaries earlier results. Assuming $K \subseteq L$ is Galois, Proposition 7.0.5 establishes that $M \subseteq L$ is also Galois, and Theorem 7.0.2 shows that $M = L^{\mathrm{Gal}(L/M)}$. Since $M \subseteq L$ and $K \subseteq L$

are Galois, we have $|\mathrm{Gal}(L/M)| = [L : M]$ and $|\mathrm{Gal}(L/K)| = [L : K]$. Using the Tower Theorem, we obtain

$$|\mathrm{Gal}(M/K)| = \left|\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)}\right| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L : K]}{[L : M]} = [M : K]\,.$$

For the second part, let H be a subgroup of $\mathrm{Gal}(L/K)$. It follows that $K \subseteq L^H \subseteq L$ and $H \subseteq \mathrm{Gal}(L/L^H)$ because every $\sigma \in H$ is the identity on L^H. Observe that $L^H \subseteq L$ is a finite separable extension, so the Theorem of the Primitive Element implies that $L = L^H(\alpha)$ for some $\alpha \in L$. Consider

$$h := \prod_{\sigma \in H} (x - \sigma(\alpha))\,.$$

By construction, the coefficients of h are fixed by H, so $h \in L^H[x]$ satisfies $h(\alpha) = 0$. Writing $p \in L^H[x]$ for the minimal polynomial of α over L^H, we deduce that p divides h. Hence, we see that

$$|H| = \deg(h) \geqslant \deg(p) = [L^h(\alpha) : L^H] = [L : L^H]\,.$$

It follows that $[L : L^H] \leqslant |H| \leqslant |\mathrm{Gal}(L/L^H)|$. Proposition 7.0.5 implies that $L^H \subseteq L$ is Galois, so $|\mathrm{Gal}(L/L^H)| = [L : L^H]$, $|H| = |\mathrm{Gal}(L/L^H)|$, and $H = \mathrm{Gal}(L/L^H)$. Using the Tower Theorem, we obtain

$$\left|\frac{\mathrm{Gal}(L/K)}{H}\right| = \frac{|\mathrm{Gal}(L/K)|}{|H|} = \frac{[L : K]}{[L : L^H]} = [L^H : K]\,. \qquad \square$$

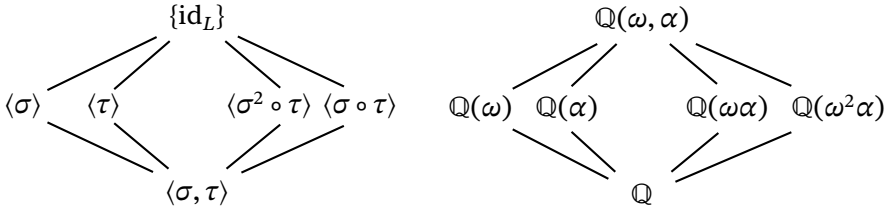
8.0.3 Remark. Consider $\mathbb{Q} \subset L := \mathbb{Q}(\omega, \alpha)$ where $\omega := \exp(2\pi\mathrm{i}/3)$ and $\alpha := \sqrt[3]{2}$. There are automorphisms $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\sigma(\omega) = \omega\,, \qquad \sigma(\alpha) = \omega\alpha\,, \qquad \tau(\omega) = \omega^2\,, \qquad \tau(\alpha) = \alpha\,.$$

and $\langle \sigma, \tau \rangle = \mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_3$.

We claim that the symmetric group $\mathfrak{S}_3$ has six subgroups. The trivial group is the unique group of order 1, and $\mathfrak{S}_3$ is the unique group of order 6. Each transposition generates a subgroup of order 2, so there are three such subgroups. The 3-cycles generate a subgroup; since $(3\ \ 1\ \ 2) = (3\ \ 2\ \ 1)^{-1}$, there is only one subgroup of order 3. Since the order of any subgroup divides 6, this list is complete.

From the maps between intermediate fields and subgroups, the subgroups of $\mathrm{Gal}(L/\mathbb{Q})$ and the intermediates fields are



Notice that

$$(\sigma^2 \circ \tau)(\omega\alpha) = \sigma^2(\tau(\omega)\tau(\alpha)) = \sigma^2(\omega^2\alpha) = \sigma(\alpha) = \omega\alpha\,,$$
$$(\sigma \circ \tau)(\omega^2\alpha) = \sigma(\tau(\omega)^2\tau(\alpha)) = \sigma(\omega\alpha) = \sigma(\omega)\sigma(\alpha) = \omega^2\alpha\,.$$

8.1 Fundamental Theorem of Galois Theory

What is the Galois correspondence?

8.1.0 Fundamental Theorem of Galois Theory. *For every Galois field extension $K \subseteq L$, the maps between intermediate fields $K \subseteq M \subseteq L$ and subgroups $H \subseteq \mathrm{Gal}(L/K)$ defined by*

$$M \mapsto \mathrm{Gal}(L/M) \qquad \text{and} \qquad H \mapsto L^H$$

reverse inclusions and are mutual inverses. Furthermore, if a subfield M corresponds to a subgroup H under these maps, then M is Galois over K if and only if H is normal in $\mathrm{Gal}(L/K)$.

Much like the Correspondence Theorem for rings or groups, this theorem describes an isomorphism of posets.

Proof. Composing maps in one way gives

$$M \mapsto \mathrm{Gal}(L/M) \mapsto L^{\mathrm{Gal}(L/M)} = K$$

by the first part of Theorem 8.0.2. Going the other way gives

$$H \mapsto L^H \mapsto \mathrm{Gal}(L/L^H) = H$$

by the second part of Theorem 8.0.2. This proves that these maps are mutual inverses.

Consider field extensions $M_1 \subseteq M_2 \subseteq L$. For each $\sigma \in \mathrm{Gal}(L/M_2)$, we have $\sigma|_{M_1} = \mathrm{id}_{M_1}$, so we obtain $\sigma_{M_1} = \mathrm{id}_{M_1}$, $\sigma \in \mathrm{Gal}(L/M_1)$, and $\mathrm{Gal}(L/M_2) \subseteq \mathrm{Gal}(L/M_1)$. Thus, the map $M \mapsto \mathrm{Gal}(L/M)$ is inclusion reversing.

Similarly, consider nested subgroups $H_1 \subseteq H_2 \subseteq \mathrm{Gal}(L/K)$. For every $\alpha \in L^{H_2}$, we have $\sigma(\alpha) = \alpha$ for all $\sigma \in H_2$. Hence, $\sigma(\alpha) = \alpha$ for all $\sigma \in H_1 \subseteq H_2$, so $\alpha \in L^{H_1}$ and $L^{H_2} \subseteq L_{H_1}$. Therefore, the map $H \mapsto L^H$ is inclusion reversing.

The final assertion follows from Corollary 8.0.0. □

8.1.1 Problem. Describe the intermediate fields of the Galois field extension $\mathbb{Q} \subseteq L := \mathbb{Q}(\mathrm{i}, \alpha)$ where $\alpha := \sqrt[4]{2}$.

Solution. The Galois group is generated by σ, τ satisfying $\sigma(\mathrm{i}) = \mathrm{i}$, $\sigma(\alpha) = \mathrm{i}\alpha$, $\tau(\mathrm{i}) = -\mathrm{i}$, and $\tau(\alpha) = \alpha$. Moreover, $\mathrm{Gal}(L/\mathbb{Q})$ is the dihedral group of order 8.

We claim that the group $\mathrm{Gal}(L/\mathbb{Q})$ has ten subgroups. The trivial group is the unique group of order 1, and $\mathrm{Gal}(L/\mathbb{Q})$ is the unique group of order 8. Each element of order 2 (there are four reflections and one subgroup of order 2 of generated by a rotation) generates a subgroup of order 2, so there are five such subgroups. The cyclic subgroup $\langle\sigma\rangle$ has order 4. Two other subgroups of order 4 arise from pairs of non-involutions (and their square). Since the order of any subgroup divides 8, this list is complete.

We next determine the corresponding fixed fields. Applying σ and τ to the $\mathbb{Q}$-basis $1, \alpha, \alpha^2, \alpha^3, \mathrm{i}, \mathrm{i}\alpha, \mathrm{i}\alpha^2, \mathrm{i}\alpha^3$ of $\mathbb{Q}(\mathrm{i}, \alpha)$, we see that

$$\sigma \leftrightarrow \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&-1&0&0&0&0 \end{bmatrix}, \quad \tau \leftrightarrow \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&-1 \end{bmatrix}.$$

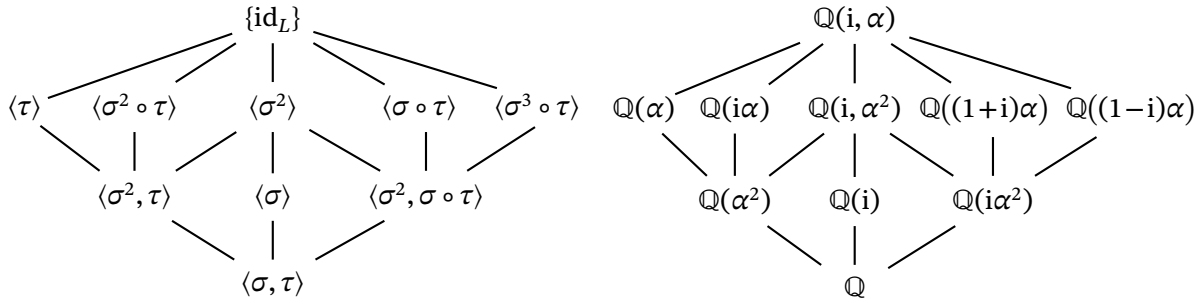
The 1-eigenspace of σ is spanned by $\{1, \mathrm{i}\}$ and 1-eigenspace of τ is spanned by $\{1, \alpha, \alpha^2, \alpha^3\}$, so $L^{\langle\sigma\rangle} = \mathbb{Q}(\mathrm{i})$ and $L^{\langle\tau\rangle} = \mathbb{Q}(\alpha)$. Moreover, matrix multiplication gives

$$\sigma\circ\tau \leftrightarrow \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&0&0&0&0&-1\\ 0&0&0&0&-1&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&-1&0&0&0&0 \end{bmatrix}, \quad \sigma^3\circ\tau \leftrightarrow \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&-1&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&-1&0&0&0\\ 0&-1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0&0 \end{bmatrix}.$$

The 1-eigenspace of $\sigma\circ\tau$ is spanned by $\{1, \alpha + \mathrm{i}\alpha, \mathrm{i}\alpha^2, -\alpha^3 + \mathrm{i}\alpha^3\}$ and 1-eigenspace of $\sigma^3\circ\tau$ is spanned by $\{1, -\alpha + \mathrm{i}\alpha, \mathrm{i}\alpha^2, \alpha^3 + \mathrm{i}\alpha^3\}$, so we see that $L^{\langle\sigma\circ\tau\rangle} = \mathbb{Q}\big((1+\mathrm{i})\alpha\big)$ and $L^{\langle\sigma^3\circ\tau\rangle} = \mathbb{Q}\big((1-\mathrm{i})\alpha\big)$. Similar calculations show that the 1-eigenspaces of σ^2 and $\sigma^2\circ\tau$ are spanned by $\{1, \alpha^2, \mathrm{i}, \mathrm{i}\alpha^2\}$ and $\{1, \alpha^2, \mathrm{i}\alpha, \mathrm{i}\alpha^3\}$ respectively, so $L^{\langle\sigma^2\rangle} = \mathbb{Q}(\mathrm{i}, \alpha^2)$ and $L^{\langle\sigma^2\circ\tau\rangle} = \mathbb{Q}(\mathrm{i}\alpha)$. Finally, we have

$$L^{\langle\sigma^2,\tau\rangle} = L^{\langle\sigma^2\rangle} \cap L^{\langle\tau\rangle} = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\mathrm{i}, \alpha^2) = \mathbb{Q}(\alpha^2)\,,$$
$$L^{\langle\sigma^2,\sigma\circ\tau\rangle} = L^{\langle\sigma^2\rangle} \cap L^{\langle\sigma\circ\tau\rangle} = \mathbb{Q}(\mathrm{i}, \alpha^2) \cap \mathbb{Q}\big((1-\mathrm{i})\alpha\big) = \mathbb{Q}(\mathrm{i}\alpha^2)\,.$$

Hence, the subgroups of $\mathrm{Gal}(L/\mathbb{Q})$ and the intermediates fields are



Observe that the degree of the field extensions correspond to the dimensions of the 1-eigenspaces. □

8.1.2 Proposition. *For every finite separable field extension $K \subseteq L$, there are only finitely many intermediate fields $K \subseteq M \subseteq L$.*

Proof. By Proposition 7.1.2, there exists an field extension $L \subseteq L'$ such that $K \subseteq L'$ is Galois. The Fundamental Theorem of Galois Theory implies that the subfields of L' containing K correspond to subgroups of $\mathrm{Gal}(L'/K)$. Since the group $\mathrm{Gal}(L'/K)$ is finite, it has finitely many subgroups, so there are finitely many subfields of L' that contain K. As every intermediate field M is a subfield of L' containing K, the desired finiteness follows. □

8.1.3 Remark. Let K be a field of characteristic p, and consider the finite field extension $K(s,t) \subseteq L$, where L is the splitting field of $(x^p - s)(x^p - t) \in K(s,t)[x]$. This purely inseparable field extension has no primitive element and $L = K(s,t)(\alpha, \beta)$ where $\alpha^P = s$ and $\beta^p = t$. Every intermediate field $K(s,t) \subset K(\alpha + \lambda\beta) \subset L$ is distinct as λ ranges over the distinct elements of $K(s,t)$. Since $K(s,t)$ is finite, we see that there are infinitely many intermediate fields.

8.2 First Applications

What are some of the more appealing applications of the Galois correspondence? Let K be a field. Recall that, for the polynomial $f = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in K[x]$ in a splitting field L of f, its discriminant is

$$\Delta(f) = \prod_{j<k}(\alpha_j - \alpha_k)^2 \in K\,.$$

Moreover, the polynomial f is separable if and only if $\Delta(f) \neq 0$. Set

$$\sqrt{\Delta(f)} = \prod_{j<k}(\alpha_j - \alpha_k) \in L\,.$$

8.2.0 Lemma. *Assume that the field K has characteristic not equal to 2. Let L be the splitting field of a separable polynomial $f \in K[x]$ of degree n. When $\sigma \in \mathrm{Gal}(L/K)$ corresponds to $\tau \in \mathfrak{S}_n$, we have*

$$\sigma\Big(\sqrt{\Delta(f)}\Big) = \mathrm{sgn}(\tau)\sqrt{\Delta(f)}\,.$$

Moreover, the image of $\mathrm{Gal}(L/K)$ lies in the alternating group A_n if and only if $\sqrt{\Delta(f)} \in K$, or equivalently $\Delta(f)$ is the square of an element in K.

Proof. When $n = 1$, the result is trivial, so we may assume that $n \geqslant 2$. Proposition 1.2.4 shows that $\sqrt{\Delta} := \prod_{j<k}(x_j - x_k) \in K[x_1, x_2, \ldots, x_n]$ satisfies $\tau(\sqrt{\Delta}) = \mathrm{sgn}(\tau)\sqrt{\Delta}$ for all $\tau \in \mathfrak{S}_n$. It follows that

$$\prod_{j<k}(x_{\tau(j)} - x_{\tau(k)}) = \mathrm{sgn}(\tau)\prod_{j<k}(x_j - x_k)\,.$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ be the roots of f. Since the evaluation map $K[x_1, x_2, \ldots, x_n] \to L$ sending x_j to α_j is a ring homomorphism,so

$$\prod_{j<k}(\alpha_{\tau(j)} - \alpha_{\tau(k)}) = \mathrm{sgn}(\tau)\prod_{j<k}(\alpha_j - \alpha_k) = \mathrm{sgn}(\tau)\sqrt{\Delta(f)}\,.$$

We also have $\sigma(\alpha_j) = \alpha_{\tau(j)}$, which implies that

$$\prod_{j<k}(\alpha_{\tau(j)} - \alpha_{\tau(k)}) = \sigma\Big(\sqrt{\Delta(f)}\Big)\,.$$

For the second part, observe that $K \subseteq L$ is Galois, so K is the fixed field of $\mathrm{Gal}(L/K)$. Hence, we obtain

$$\begin{aligned}
\sqrt{\Delta(f)} \in K \quad &\iff \quad \sigma\Big(\sqrt{\Delta(f)}\Big) = \sqrt{\Delta(f)} \quad \text{for all } \sigma \in \mathrm{Gal}(L/K) \\
&\iff \quad \mathrm{sgn}(\tau)\Big(\sqrt{\Delta(f)}\Big) = \sqrt{\Delta(f)} \quad \text{for all } \sigma \in \mathrm{Gal}(L/K)\,,
\end{aligned}$$

where τ is the permutation corresponding to σ. Since $\Delta(f) \neq 0$ and K has characteristic different from 2, the last condition is equivalent to $\mathrm{sgn}(\tau) = 1$ for all τ. This complete the proof because $\mathrm{sgn}(\tau) = 1$ if and only if $\tau \in A_n$. □

8.2.1 Proposition. *Assume that the field K has characteristic not equal to 2. Let $f \in K[x]$ be a monic irreducible separable cubic. When L is the splitting field of f over K, its Galois group is*

$$\mathrm{Gal}(L/K) \cong \begin{cases} \mathbb{Z}\big/\langle 3\rangle & \text{if } \Delta(f) \text{ is a square in } K, \\ \mathfrak{S}_3 & \text{otherwise.} \end{cases}$$

Proof. The order $|\mathrm{Gal}(L/K)|$ is divisible by 3 because f is irreducible and separable. We also have an injective group homomorphism $\mathrm{Gal}(L/K) \to \mathfrak{S}_3$. Since the only subgroups of $\mathfrak{S}_3$ of order divisible by 3 are $\mathfrak{S}_3$ and A_3, the claim follows from lemma. □

Consider the universal extension of degree n

$$K(e_1, e_2, \dots, e_n) \subset K(x_1, x_2, \dots, x_n)$$

where $e_1, e_2, \dots, e_n$ are the elementary symmetric polynomials. The field $K(x_1, x_2, \dots, x_n)$ is the splitting field of

$$\widetilde{f} = x^n - e_1 x^{n-1} + \cdots + (-1)^j e_j x^{n-j} + \cdots (-1)^n e_n = \prod_{j=1}^{n} (x - x_j),$$

and $\mathrm{Gal}\big(K(x_1, x_2, \dots, x_n) \,\big/\, K(e_1, e_2, \dots, e_n)\big) \cong \mathfrak{S}_n$. Set

$$\sqrt{\Delta} := \prod_{1 \leqslant j < k \leqslant n} (x_j - x_k).$$

8.2.2 Theorem. *A rational function $f \in K(x_1, x_2, \dots, x_n)$ is invariant under $\mathfrak{S}_n$ if and only if $f \in K(e_1, e_2, \dots, e_n)$. Moreover, assuming that the characteristic of K is not 2, the function $f \in K(x_1, x_2, \dots, x_n)$ is invariant under A_n if and only if there exists $g, h \in K(e_1, e_2, \dots, e_n)$ such that $f = g + h\sqrt{\Delta}$.*

Proof. Since $K(e_1, e_2, \dots, e_n) \subset K(x_1, x_2, \dots, x_n)$ is a Galois extension, Theorem 8.0.2 implies that $K(e_1, e_2, \dots, e_n)$ is the fixed field of the Galois group $\mathrm{Gal}\big(K(x_1, x_2, \dots, x_n) \,\big/\, K(e_1, e_2, \dots, e_n)\big) = \mathfrak{S}_n$ acting on L, which proves the first part.

For the second part, set $M := L^{A_n}$ be the fixed field of the subgroup A_n. Since A_n has index 2 in $\mathfrak{S}_n$, Theorem 8.0.2 implies that $K(e_1, e_2, \dots, e_n) \subset M$ is a field extension of degree 2. Since $\tau\big(\sqrt{\Delta}\big) = \mathrm{sgn}(\tau)\sqrt{\Delta}$ for all $\tau \in \mathfrak{S}_n$, we see that $\sqrt{\Delta} \in M$, so

$$K(e_1, e_2, \dots, e_n) \subset K(e_1, e_2, \dots, e_n)\big[\sqrt{\Delta}\big] \subseteq M\,.$$

By the Tower Theorem, it follows that

$$\begin{aligned} 2 &= [M : K] \\ &= \Big[M : K(e_1, e_2, \dots, e_n)\big[\sqrt{\Delta}\big]\Big]\Big[K(e_1, e_2, \dots, e_n)\big[\sqrt{\Delta}\big] : K(e_1, e_2, \dots, e_n)\Big]. \end{aligned}$$

Since $\sqrt{\Delta} \notin K$, we see that $M = K(e_1, e_2, \dots, e_n)\big[\sqrt{\Delta}\big]$. Since $\sqrt{\Delta}$ is a primitive element of $K \subset M$, we conclude that

$$M = \{g + h\sqrt{\Delta} \mid g, h \in K(e_1, e_2, \dots, e_n)\}. \qquad \square$$

8.2.3 Theorem. *For every finite group G, there exists a Galois extension whose Galois group is isomorphic to G.*

Proof. Let G be a finite group of order n and let K be an arbitrary field. The universal extension of degree n,

$$K(e_1, e_2, \dots, e_n) \subseteq L := K(x_1, x_2, \dots, x_n),$$

is a Galois extension with Galois group $\mathrm{Gal}\big(L/K(e_1, e_2, \dots, e_n)\big) \cong \mathfrak{S}_n$. Since G is isomorphic to a subgroup of $\mathfrak{S}_n$, it follows that G is also isomorphic to a subgroup H of this Galois group. Hence, the fixed field of H is an intermediate field $K(e_1, e_2, \dots, e_n) \subseteq L^H \subseteq L$, and the Fundamental Theorem of Galois Theory demonstrates that $L^H \subseteq L$ is a Galois extension with $\mathrm{Gal}(L/L^H) = H \cong G$. Therefore, $L^H \subseteq L$ is the desired extension. $\square$

In the field extension constructed in Theorem 8.2.3, the smaller field depends on the group. The *inverse Galois problem for* $\mathbb{Q}$ asks which finite groups arise as the Galois group for a finite extension of $\mathbb{Q}$. Many cases are known. For example, every simple sporadic group, except possibly the Mathieu group of order 23, is "realizable over $\mathbb{Q}$."