6 Galois Groups

The field automorphisms that fix a base field reveal many algebraic aspects of a field extension. This chapter explores this principle.

6.0 Definition of the Galois Group

How is group theory connected to field theory?

6.0.0 Definition. The *Galois group* of the field extension $K \subseteq L$ is

$$\operatorname{Gal}(L/K) := \left\{ \sigma \colon L \to L \;\middle|\; \begin{array}{l} \sigma \text{ is a field automorphism,} \\ \text{and } \sigma(a) = a \text{ for all } a \in K \end{array} \right\}.$$

In other words, $\operatorname{Gal}(L/K)$ is consists of all K-algebra automorphisms of L, or equivalently, all ring homomorphisms of L that restrict to the identity on the subfield K.

We first justify the nomenclature.

6.0.1 Proposition. *For every field extension $K \subseteq L$, the set $\operatorname{Gal}(L/K)$ is a group under composition.*

Proof. The automorphisms of every mathematical object forms a group. By definiton, composition is associative. The identity map $\mathrm{id}_L \colon L \to L$ satisfies $\sigma \circ \mathrm{id}_L = \sigma = \mathrm{id}_L \circ \sigma$ for all $\sigma \in \operatorname{Gal}(L/K)$, and is its own inverse. The definition of an automorphism asserts that, for every automorphism $\sigma \colon L \to L$, there exists field homomorphism $\tau \colon L \to L$ such that $\sigma \circ \tau = \mathrm{id}_L = \tau \circ \sigma$.

Regarding L as field, we verify that $\operatorname{Gal}(L/K)$ is a subgroup of all field automorphisms. For all automorphism $\sigma, \tau \in \operatorname{Gal}(L/K)$ and every $a \in K$, we have $a = \mathrm{id}_L(a) = (\tau^{-1} \circ \tau)(a) = \tau^{-1}\big(\tau(a)\big) = \tau^{-1}(a)$ and $(\sigma \circ \tau^{-1})(a) = \sigma\big(\tau^{-1}(a)\big) = \sigma(a) = a$, so $\sigma \circ \tau^{-1} \in \operatorname{Gal}(L/k)$. We conclude that $\operatorname{Gal}(L/K)$ is a subgroup of $\operatorname{Aut}(L)$. □

Regarding L as a K-algebra, one sees immediately that $\operatorname{Gal}(L/K)$ is a group. However, one still needs to know that being a K-algebra homomorphism is equivalent to being a ring homomorphism that restricts to the identity on K.

6.0.2 Proposition. *Let $K \subseteq L$ be a finite field extension, and fix the automorphism $\sigma \in \operatorname{Gal}(L/K)$.*

(evaluation) *For every polynomial $f \in K[x_1, x_2, \dots, x_n]$, we have*

$$\begin{aligned}(\sigma \circ \mathrm{ev}_\beta)(f) &= \sigma\big(f(\beta_1, \beta_2, \dots, \beta_n)\big) \\ &= f\big(\sigma(\beta_1), \sigma(\beta_2), \dots, \sigma(\beta_n)\big) = \mathrm{ev}_{\sigma(\beta)}(f)\,.\end{aligned}$$

(roots) *For every nonconstant $f \in K[x]$ having $\alpha \in L$ as a root, the image $\sigma(\alpha)$ is also a root of f in L.*

(uniqueness) *When $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, the map σ is determined by its values on $\alpha_1, \alpha_2, \dots, \alpha_n$.*

Proof. The first part is immediate because the map σ is compatible with addition and multiplication, and restricts to the identity on the coefficient field K.

The hypothesis $f(\alpha) = 0$ gives $f\big(\sigma(a)\big) = \sigma\big(f(a)\big) = \sigma(0) = 0$, which shows that $\sigma(\alpha) \in L$ is also a root of f.

As $L = K[\alpha_1, \alpha_2, \dots, \alpha_n]$, every element $\beta \in L$ can be written as $\beta = f(\alpha_1, \alpha_2, \dots, \alpha_n)$ for some $f \in K[x_1, x_2, \dots, x_n]$. Observe that $\sigma(\beta) = \sigma\big(f(\alpha_1, \alpha_2, \dots, \alpha_n)\big) = f\big(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)\big)$, so the map $\sigma \colon L \to L$ is uniquely determined by $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)$. □

6.0.3 Corollary. *The Galois group of a finite field extension is finite.*

Proof. Let $K \subseteq L$ be a finite field extension. In particular, there are $\alpha_1, \alpha_2, \dots, \alpha_n \in L$, algebraic over K, such that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Each $\sigma \in \operatorname{Gal}(L/K)$ is uniquely determined by $\sigma(\alpha_1)$, $\sigma(\alpha_2)$, $\dots$, $\sigma(\alpha_n)$. If $p_j \in K[x]$ is the minimal polynomial of α_j, then there are at most $\deg(p_j)$ possibilities for $\sigma(\alpha_j)$ because $\sigma(\alpha_j)$ is a root of p_j. □

6.0.4 Problem. Show that the Galois group of $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is trivial.

Solution. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, which has $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ as roots. The last two are not real, so do not lie in L. Hence, every $\sigma \in \operatorname{Gal}(L/K)$ must satisfy $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. As σ is uniquely determined by $\sigma(\sqrt[3]{2})$, it must be the identity map. □

6.0.5 Problem. Let K be a field of positive characteristic p, and let L be the splitting field of $f = x^p - t \in K(t)[x]$ over the function field $K(t)$. Show that the group $\operatorname{Gal}\big(L/K(t)\big)$ is trivial.

Solution. When $\alpha \in L$ is a root of f, it follows that $L = K(t, \alpha)$ and $f = (t - \alpha)^p$. Since f has a single root of multiplicity p, we again deduce that $\operatorname{Gal}\big(L/K(t)\big) = \{\mathrm{id}_L\}$. □

6.0.6 Problem. Show that the Galois group of the field extension $\mathbb{R} \subset \mathbb{C}$ is the cyclic group of order 2.

Solution. Let $\tau \colon \mathbb{C} \to \mathbb{C}$ denote complex conjugation: $\tau(z) := \overline{z}$ for all $z \in \mathbb{C}$. It is a ring automorphism because $\tau \circ \tau = \mathrm{id}_{\mathbb{C}}$. As $\tau(a) = a$ for all $a \in \mathbb{R}$, we have $\tau \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})$ and $|\operatorname{Gal}(\mathbb{C}/\mathbb{R})| \geqslant 2$.

Since the roots of $x^2 + 1$ are $\pm\mathrm{i}$, every $\sigma \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})$ satisfies either $\sigma(\mathrm{i}) = \mathrm{i}$ or $\sigma(\mathrm{i}) = -\mathrm{i}$, so $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ has at most two elements. We conclude that $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \tau\} \cong \mathbb{Z}\big/\langle 2\rangle$. □

6.0.7 Problem. Show that the Galois group of $\mathbb{Q} \subset L := \mathbb{Q}(\sqrt{2})$ is the cyclic group of order 2.

Solution. Every map $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$ satisfies $\sigma(\sqrt{2}) = \pm\sqrt{2}$, so we see that $|\operatorname{Gal}(L/\mathbb{Q})| \leqslant 2$. For all $a, b \in \mathbb{Q}$, one verifies that $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism of L. □

6.0.8 Proposition. *Let $K \subseteq L_1$ and $K \subseteq L_2$ be finite field extensions. Every field isomorphism $\varphi \colon L_1 \to L_2$ that restricts to the identity on K induces a group isomorphism* $\operatorname{Gal}(\varphi) \colon \operatorname{Gal}(L_1/K) \to \operatorname{Gal}(L_2/K)$ *defined by $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ for all* $\sigma \in \operatorname{Gal}(L_1/K)$.

Proof. The composition of isomorphisms is also an isomorphism, so $\varphi \circ \sigma \circ \varphi^{-1}$ is an automorphism of L_2. Since σ and φ restrict to the identity on K, we see that $\varphi \circ \sigma \circ \varphi^{-1} \in \operatorname{Gal}(L_2/K)$, and the map $\operatorname{Gal}(\varphi)$ is well-defined. For all $\sigma, \sigma' \in \operatorname{Gal}(L_1/K)$, we have

$$(\varphi \circ \sigma \circ \varphi^{-1}) \circ (\varphi \circ \sigma' \circ \varphi^{-1}) = \varphi \circ (\sigma \circ \sigma') \circ \varphi^{-1},$$

so the induced map is a group homomorphism. Finally, the map from $\operatorname{Gal}(\varphi^{-1}) \colon \operatorname{Gal}(L_2/K) \to \operatorname{Gal}(L_1/K)$ defined by $\tau \mapsto \varphi^{-1} \circ \tau \circ \varphi$ for all $\tau \in \operatorname{Gal}(L_2/L)$ is the inverse of $\operatorname{Gal}(\varphi)$. □

6.1 Galois groups of splitting fields

How can we understand some concrete Galois groups?

6.1.0 Theorem. *When L is the splitting field of a separable polynomial in $K[x]$, the Galois group of $K \subseteq L$ has order* $|\mathrm{Gal}(L/K)| = [L : K]$.

Proof. The hypotheses guarantee that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the distinct roots of a separable polynomial over K. In particular, each α_j is separable over K. By the Theorem of the Primitive Element, there exists an element $\beta \in L$, separable over K, such that $L = K(\beta)$. Let $p \in K[x]$ be the minimal polynomial of β; it is separable because β is. Since $L = K(\beta)$, Proposition 4.0.3 implies that $[L : K] = m$ where $m := \deg(p)$. To prove the theorem, it suffices to show that $\mathrm{Gal}(L/K)$ has m elements.

As L is a splitting field and $\beta \in L$ is a root of p, normality shows that all the roots of p lie in L. The separability of p ensures these roots $\beta = \beta_1, \beta_2, \dots, \beta_m$ are distinct. Since β_1 and β_j are roots of the same irreducible polynomial over K, Proposition 4.2.7 produces an automorphism $\sigma_j : L \to L$ such that $\sigma_j(\beta_1) = \beta_j$ and $\varphi|_L = \mathrm{id}_K$. It follows that $\sigma_1, \sigma_2, \dots, \sigma_m \in \mathrm{Gal}(L/K)$. Observe that $\sigma_j \neq \sigma_k$ when $j \neq k$ because $\sigma_j(\beta_1) = \beta_j \neq \beta_k = \sigma_k(\beta_1)$, so this Galois group has at least m distinct elements. Proposition 6.0.2 implies that every automorphism $\sigma \in \mathrm{Gal}(L/K)$ is uniquely determined by $\sigma(\beta) \in \{\beta_1, \beta_2, \dots, \beta_m\}$, which means $\sigma = \sigma_j$ for some $1 \leqslant j \leqslant m$. □

6.1.1 Remark. The "splitting field" and the "separable" hypotheses are both necessary. For instance, the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ has a trivial Galois group, but this field extension is not a splitting field. Similarly, let K be a field of positive characteristic p, and let L be the splitting field of $f = x^p - t \in K(t)[x]$ over the function field $K(t)$. The field extension $K(t) \subset L$ has a trivial Galois group, but this field extension is inseparable.

6.1.2 Problem. Show that the Galois group of $\mathbb{Q} \subset L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the Klein four-group.

Solution. By Proposition 6.0.2, the map $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is uniquely determined by $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$, which implies that $|\mathrm{Gal}(L/\mathbb{Q})| \leqslant 4$. Because L is the splitting field of the separable polynomial $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$, all of the above sign combination occur. Hence, there exist $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\sigma(\sqrt{2}) = \sqrt{2}\,, \quad \sigma(\sqrt{3}) = -\sqrt{3}\,, \quad \tau(\sqrt{2}) = -\sqrt{2}\,, \quad \tau(\sqrt{3}) = \sqrt{3}\,,$$

and $\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}_L, \sigma, \tau, \sigma \circ \tau\} \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$. □

6.1.3 Definition. The *affine group* $\mathrm{Aff}(K^n)$ of the finite-dimensional K-vector space K^n is the group, under composition, of all affine transformations $\mathbf{v} \mapsto \mathbf{A}\mathbf{v}+\mathbf{b}$ for some invertible matrix $\mathbf{A} \in \mathrm{GL}(n, K)$ and some vector $\mathbf{b} \in K^n$.

6.1.4 Problem. For every prime $p \in \mathbb{Z}$, the affine group $\operatorname{Aff}(\mathbb{F}_p)$ has order $p(p-1)$, and the map $v \mapsto av + b$ corresponds to the matrix

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

Solution. There are p choices for $b \in \mathbb{F}_p$, and there are $p-1$ choices for a unit $a \in \operatorname{GL}(1, \mathbb{F}_p) = \mathbb{F}_p^\times$. Moreover, we have

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v \\ 1 \end{bmatrix} = \begin{bmatrix} av + b \\ 1 \end{bmatrix}. \qquad \square$$

6.1.5 Proposition. *Let $p \in \mathbb{Z}$ be a prime and let $\zeta := \exp(2\pi \mathrm{i}/p) \in \mathbb{C}$ be a primitive pth root of unity. For the splitting field*

$$L := \mathbb{Q}\Big(\sqrt[p]{2}, \zeta \sqrt[p]{2}, \zeta^2 \sqrt[p]{2}, \dots, \zeta^{p-1} \sqrt[p]{2}\Big) = \mathbb{Q}\Big(\zeta, \sqrt[p]{2}\Big)$$

of $x^p - 2 \in \mathbb{Q}[x]$, the Galois group $\operatorname{Gal}(L/\mathbb{Q})$ is isomorphic to $\operatorname{Aff}(\mathbb{F}_p)$.

Proof. The minimal polynomial of ζ over $\mathbb{Q}$ is $x^{p-1} + x^{p-2} + \cdots + 1$, and the roots of this polynomial are ζ^j for all $1 \leqslant j \leqslant p-1$. Furthermore, the minimal polynomial of $\sqrt[p]{2}$ over $\mathbb{Q}$ is $x^p - 2$ by the Eisenstein criterion, and its roots are $\sqrt[p]{2}, \zeta \sqrt[p]{2}, \zeta^2 \sqrt[p]{2}, \dots, \zeta^{p-1} \sqrt[p]{2}$. The Tower Theorem implies that $[L : \mathbb{Q}]$ is divisible by both p and $p-1$. Since $\gcd(p, p-1) = 1$, we conclude that $[L : \mathbb{Q}] = p(p-1)$. It follows that $\operatorname{Gal}(L/\mathbb{Q})$ is group of order $p(p-1)$.

To analyze this Galois group, consider a map $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$. By Proposition 6.0.2, the automorphism σ is uniquely determined by

$$\sigma(\zeta) \in \{\zeta, \zeta^2, \dots, \zeta^{p-1}\}, \quad \sigma(\sqrt[p]{2}) \in \Big\{\sqrt[p]{2}, \zeta \sqrt[p]{2}, \zeta^2 \sqrt[p]{2}, \dots, \zeta^{p-1} \sqrt[p]{2}\Big\}.$$

In other words, for all $1 \leqslant j \leqslant p-1$ and all $0 \leqslant k \leqslant p-1$, there exists an automorphism $\sigma_{j,k} : L \to L$ such that

$$\sigma_{j,k}(\zeta) = \zeta^j, \qquad \sigma_{j,k}(\sqrt[p]{2}) = \zeta^k \sqrt[p]{2}$$

The number of possible pairs (j, k) is $(p-1)p = |\operatorname{Gal}(L/\mathbb{Q})|$, so all possible pairs must occur. Since ζ^j depends only on the congruence class of j module p, we regard the pair of subscripts as an element in the product $\mathbb{F}_p^\times \times \mathbb{F}_p$.

To determine the group structure, we compute the composition of $\sigma_{j,k}$ and $\sigma_{r,s}$. Observe that

$$\begin{aligned} (\sigma_{j,k} \circ \sigma_{r,s})(\zeta) &= \sigma_{j,k}(\zeta^r) = \big(\sigma_{j,k}(\zeta)\big)^r = (\zeta^j)^r = \zeta^{jr}, \\ (\sigma_{j,k} \circ \sigma_{r,s})(\sqrt[p]{2}) &= \sigma_{j,k}(\zeta^s \sqrt[p]{2}) = \big(\sigma_{j,k}(\zeta)\big)^s \sigma_{j,k}(\sqrt[p]{2}) \\ &= (\zeta^j)^s (\zeta^k \sqrt[p]{2}) = \zeta^{js+k} \sqrt[p]{2}. \end{aligned}$$

This computation establishes that $\sigma_{j,k} \circ \sigma_{r,s} = \sigma_{jr, js+k}$. Thus, the map $\sigma_{j,k} \mapsto jv + k$ defines an isomorphism $\operatorname{Gal}(L/\mathbb{Q}) \cong \operatorname{Aff}(\mathbb{F}_p)$, because $j(rv + s) + k = jrv + (js + k)$. $\square$

6.2 Permutations of the Roots

How are Galois groups realized as permutation groups?

6.2.0 Definition. Let K be a field, and let L be the splitting field of a separable polynomial $f \in K[x]$ of degree n. Factoring gives

$$f = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where $0 \neq a_0 \in K$ and $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ are distinct roots. The *permutation map* $\rho \colon \operatorname{Gal}(L/K) \to \mathfrak{S}_n$ is defined as follows. For each $\sigma \in \operatorname{Gal}(L/K)$, Proposition 6.0.2 implies that $\sigma(\alpha_j)$ is a root of f, so $\sigma(\alpha_j) = \alpha_{\tau(j)}$ for some $\tau(j) \in [n] := \{1, 2, \dots, n\}$. Observe that the index $\tau(j)$ is uniquely determined because $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct. The map $\tau \colon [n] \to [n]$ is bijective because σ is. In other words, the map τ is a permutation, and $\tau \in \mathfrak{S}_n$.

6.2.1 Proposition. *Let L be the splitting field of a separable polynomial $f \in K[x]$ of degree n. The permutation map $\rho \colon \operatorname{Gal}(L/K) \to \mathfrak{S}_n$ is an injective group homomorphism.*

Proof. Suppose that $\sigma, \sigma' \in \operatorname{Gal}(L/K)$ corresponds to $\tau, \tau' \in \mathfrak{S}_n$. This means that $\sigma(\alpha_j) = \alpha_{\tau(j)}$ and $\sigma'(\alpha_j) = \alpha_{\tau'(j)}$ for all $1 \leqslant j \leqslant n$. It follows that $(\sigma \circ \sigma')(\alpha_j) = \sigma\big(\sigma'(\alpha_j)\big) = \sigma(\alpha_{\tau'(j)}) = \alpha_{\tau(\tau'(j))} = \alpha_{(\tau \circ \tau')(j)}$. Hence, $\sigma \circ \sigma'$ corresponds to $\tau \circ \tau'$, which shows that ρ is a group homomorphism. Since $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ and $\sigma \in \operatorname{Gal}(L/K)$ is determined by its values on $\alpha_1, \alpha_2, \dots, \alpha_n$, the map ρ is injective. □

6.2.2 Corollary. *When L is the splitting field of a separable polynomial $f \in K[x]$ of degree n, its degree $[L : K]$ divides $n!$.*

Proof. The permutation map $\rho \colon \operatorname{Gal}(L/K) \to \mathfrak{S}_n$ identifies the Galois group with a subgroup of the symmetric group, so the Lagrange Theorem establishes that $|\operatorname{Gal}(L/K)|$ divides $n!$. Under the given hypothesese, $[L : K] = |\operatorname{Gal}(L/K)|$. □

6.2.3 Problem. Describe the image of $\rho \colon \operatorname{Gal}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big) \to \mathfrak{S}_4$.

Solution. Problem 6.1.2 shows that $\operatorname{Gal}(L/\mathbb{Q}) = \{\mathrm{id}_L, \sigma, \tau, \sigma \circ \tau\}$ where the automorphisms $\sigma, \tau \in \operatorname{Gal}(L/\mathbb{Q})$ are defined by

$$\sigma(\sqrt{2}) = \sqrt{2}\,, \quad \sigma(\sqrt{3}) = -\sqrt{3}\,, \quad \tau(\sqrt{2}) = -\sqrt{2}\,, \quad \tau(\sqrt{3}) = \sqrt{3}\,.$$

Set $\alpha_1 := \sqrt{2}$, $\alpha_2 := -\sqrt{2}$, $\alpha_3 := \sqrt{3}$, and $\alpha_4 := -\sqrt{3}$. Since σ fixes α_1, α_2 and interchanges α_3, α_4, we have $\rho(\sigma) = (4 \;\; 3) \in \mathfrak{S}_4$. Similarly, τ fixes α_2, α_3 and interchanges α_1, α_2, we have $\rho(\sigma) = (2 \;\; 1) \in \mathfrak{S}_4$. Thus, $\operatorname{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, (3 \;\; 4), (2 \;\; 1), (2 \;\; 1)(4 \;\; 3)\} \subset \mathfrak{S}_4$. □

6.2.4 Problem. Show that the Galois group of $\mathbb{Q} \subset L := \mathbb{Q}\big(\omega, \sqrt[3]{2}\big)$ is the symmetric group $\mathfrak{S}_3$.

Solution. The field L is the splitting field of the separable polynomial $x^3 - 2 \in \mathbb{Q}[x]$. There exists $\sigma, \tau \in \operatorname{Gal}(L/\mathbb{Q})$ such that

$$\sigma\big(\sqrt[3]{2}\big) = \omega \sqrt[3]{2}\,, \quad \sigma(\omega) = \omega\,, \quad \tau\big(\sqrt[3]{2}\big) = \sqrt[3]{2}\,, \quad \tau(\omega) = \omega^2\,.$$

Enumerating the roots as $\alpha_1 := \sqrt[3]{2}$, $\alpha_2 := \omega \sqrt[3]{2}$, and $\alpha_3 := \omega^2 \sqrt[3]{2}$, we have $\rho(\sigma) = (3 \;\; 2 \;\; 1)$ and $\rho(\tau) = (3 \;\; 2)$, so $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_3$. □

6.2.5 Definition. A subgroup $H \subseteq \mathfrak{S}_n$ is *transitive* if, for every pair $(j,k) \in [n] \times [n]$, there exists $\tau \in H$ such that $\tau(j) = k$.

6.2.6 Remark. The subgroup $\{\mathrm{id}_{[4]}, (2\;\;1), (4\;\;3), (2\;\;1)(4\;\;3)\} \subseteq \mathfrak{S}_4$ is no transitive, because not element of the subgroup sends 1 to 3.

6.2.7 Proposition. *Let L be the splitting field of a separable polynomial $f \in K[x]$ of degree n. The image of $\rho \colon \mathrm{Gal}(K/L) \to \mathfrak{S}_n$ is transitive if and only if f is irreducible over K.*

Proof. Suppose that f is irreducible and $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ are its distinct roots. By Proposition 4.2.7, there exists an automorphism $\sigma \colon L \to L$ such that $\sigma(\alpha_j) = \alpha_k$ and $\varphi|_K = \mathrm{id}_K$. Hence, $\sigma \in \mathrm{Gal}(L/K)$ and $\rho(\sigma) \in \mathfrak{S}_n$ sends j to k. Thus, the image of the Galois group is a transitive subgroup of $\mathfrak{S}_n$.

Suppose that $\rho\big(\mathrm{Gal}(L/K)\big) \subseteq \mathfrak{S}_n$ is transitive. Let h be an irreducible factor of f. It suffices to show that $\deg(h) \geqslant n$. Writing $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ for the distinct roots of f, there exists an index j such that $h(\alpha_j) = 0$. Choose any $k \in [n] := \{1, 2, \dots, n\}$. By transitivity, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha_j) = \alpha_k$. Since the coefficients of h are in K, we see that $\sigma(\alpha_j) = \alpha_k$ is also a root of h. Since the index k as arbitrary and $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct, it follows that h has at least n roots, which implies that $\deg(h) \geqslant n$. $\square$

6.2.8 Definition. Fix positive $n \in \mathbb{N}$ and a field K. Let $e_1, e_2, \dots, e_n$ be the elementary symmetric polynomials in $K[x_1, x_2, \dots, x_n]$. The *universal polynomial of degree n* is

$$\begin{aligned} \widetilde{f} &= (x - x_1)(x - x_2) \cdots (x - x_n) \\ &= x^n - e_1 x^{n-1} + \cdots + (-1)^r e_r x^{n-r} + \cdots + (-1)^n e_n \,. \end{aligned}$$

The coefficients of $\widetilde{f}$ lie in $K(e_1, e_2, \dots, e_n)$ and its splitting field is $K(x_1, x_2, \dots, x_n)$. The extension $K(e_1, e_2, \dots, e_n) \subset K(x_1, x_2, \dots, x_n)$ is the *universal field extension of degree n*.

6.2.9 Theorem. *The universal field extension of degree n is the splitting field of a separable polynomial and*

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

Sketch of Proof. The function field $K(x_1, x_2, \dots, x_n)$ is the splitting field of $\widetilde{f} \in K(e_1, e_2, \dots, e_n)[x]$, and this polynomial is separable because its roots $x_1, x_2, \dots, x_n$ are distinct indeterminants.

The group $\mathfrak{S}_n$ acts on the ring $K[x_1, x_2, \dots, x_n]$ by permuting the variables. For every $\tau \in \mathfrak{S}_n$, the map $f \mapsto \tau(f)$ is an automorphism of the ring $K[x_1, x_2, \dots, x_n]$. Moreover, this automorphism extends to an automorphism of its field $K(x_1, x_2, \dots, x_n)$ of fractions. Since the elementary symmetric polynomials are fixed by the $\mathfrak{S}_n$-action, this automorphism is the identity on the subfield $K(e_1, e_2, \dots, e_n)$. In other words, the map $f \mapsto \tau(f)$ is an element of $\mathrm{Gal}(L/K)$. Under $\rho \colon \mathrm{Gal}(L/K) \to \mathfrak{S}_n$, this automorphism maps to τ. Since τ is an arbitrary element of $\mathfrak{S}_n$, the map ρ is surjective. $\square$