Let K be a field. Every polynomial $f \in K[X]$ has a splitting field. It is unique up to isomorphism. A polynomial $f \in K[X]$ is called *separable*, if its zeroes in a splitting field are distinct.

Definition. Let $K \subset L$ be a finite extension.
- The extension is called *normal* over K if the minimal polinomial $f \in K[X]$ of any $x \in L$ splits into linear factors in $L[X]$.
- The extension is called *separable*, if every $x \in L$ is separable over K. This means that its minimum polynomial $f \in K[X]$ is separable.
- The extension is called *Galois* if it is both normal and separable.

If the characteristic of K is zero, then any finite extension $K \subset L$ is separable. Indeed, if the minimum polynomial f of $x \in L$ has a double zero, then f divides its derivative f'. Since the degree of f' is strictly smaller than the one of f, the polynomial f' is zero, so that f is constant. This is impossible, since minimum polynomials have degree ≥ 1.

Suppose $K \subset L$ is normal and let E be an intermediate extension $K \subset E \subset L$. Then L is also normal over E. Indeed, for any $x \in L$, its minimum polynomial over E divides the one over K.

Theorem/Criterion. *Let $K \subset L$ be a finite extension. Then the following are equivalent.*
(1) The extension $K \subset L$ is normal.
(2) The field L is the splitting field of some $f \in K[X]$.
(3) For every extension $L \subset M$, the natural map

$$\mathrm{Aut}_K(L) \longrightarrow \mathrm{Hom}_K(L, M)$$

is a bijection.

Proof. (1) $\Rightarrow$ (2) We have $L = K(A)$ for a finite subset $A \subset L$. Let f be the product of the minimum polynomials over K of the elements $a \in A$. Then f splits into a product of linear factors in $L[X]$. Since L is generated by A, this means that L is the splitting field of f.

(2) $\Rightarrow$ (3) The map in (3) is always injective. To prove that it is surjective, let $\sigma : L \longrightarrow M$ be a K-automorphism and let $x \in L$ be a zero of f. Then $\sigma(x)$ is another zero of f in M. Since all zeroes of f are contained in L, this means $\sigma(x) \in L$. The fact that L is generated by the zeroes of f now implies that $\sigma(L) \subset L$, as required.

(3) $\Rightarrow$ (1) Write $L = K(A)$ for a certain finite subset $A \subset L$. Let $x \in L$ and let $f \in K[X]$ denote its minimum polynomial. We apply (3) to the splitting field M of the product of f and the minimum polynomials of the elements in A. Then we have $K \subset L \subset M$. Let $y \in M$ be a zero of f. The K-isomorphism $K(x) \cong K(y)$ that maps x to y extends to a K-automorphism σ of the splitting field M. By (3) its restriction to L is induced by a K-automorphism of L. This means that $y = \sigma(x)$ is contained in L as required.

Lemma. *(Artin-Dedekind) Let $K \subset L$ be a finite extension and let $K \subset M$ be an arbitrary field extension. Then we have*

$$\#\mathrm{Hom}_K(L, M) \leq [L : K].$$

Proof. Let $n = [L : K]$ and let $e_1, \ldots, e_n$ be a K-basis of L. Suppose that there are $n+1$ distinct homomorphisms $\sigma_0, \ldots, \sigma_n \in \mathrm{Hom}_K(L, M)$. Then the $n+1$ vectors

$$\begin{pmatrix} \sigma_i(e_1) \\ \vdots \\ \sigma_i(e_n) \end{pmatrix} \in M^n, \qquad \text{for } i = 0, 1, \ldots, n,$$

are M-linarly dependent. This means that there are $\lambda_0, \ldots, \lambda_n \in M$ not all zero, for which $\sum_{i=0}^n \lambda_i \sigma_i(e_k) = 0$ for $k = 1, \ldots, n$. Since each σ_i is K-linear, this means that the map $\sum_{i=0}^n \lambda_i \sigma_i$ is identically zero on L.

However, such an M-linear relation between field homomorphisms is necessarily trivial. Indeed, assume that

$$\sum_{i=0}^{n} \lambda_i \sigma_i \equiv 0, \qquad \text{in } \mathrm{Hom}_K(L, L),$$

is such a relation with *minimal* number of non-zero coefficients $\lambda_i \in L$. There are at least two non-zero λ_i. We may assume they are λ_0 and λ_1. Let $z \in L$ be such that $\sigma_0(z) \neq \sigma_1(z)$. Subtracting the relations

$$\sigma_0(z) \sum_{i \geq 0} \lambda_i \sigma_i(x) = 0, \qquad \text{for all } x \in L,$$

$$\sum_{i \geq 0} \lambda_i \sigma_i(zx) = 0, \qquad \text{for all } x \in L,$$

gives the relation

$$\sum_{i \geq 1} \lambda_i (\sigma_0(z) - \sigma_i(z)) \sigma_i(x) = 0, \qquad \text{for all } x \in L.$$

Since this relation has fewer non-zero coefficients, all coefficients must be zero. In particular $\lambda_1(\sigma_0(z) - \sigma_1(z)) = 0$. This implies $\lambda_1 = 0$. Contradiction.

This proves the lemma.

Definition. Let $K \subset L$ be finite. Then the *separability degree* of L over K is defined by

$$[L : K]_{\mathrm{sep}} = \#\mathrm{Hom}_K(L, M), \qquad \text{for any normal extension } L \subset M.$$

To see that this definition does not depend on the choice of the field M, we write $L = K(A)$ for some finite set $A \subset L$. Then the product f of the minimum polynomials over K of $a \in A$ splits completely in $M[X]$. Let $E \subset M$ be the subfield generated by those zeroes. Then E is a splitting field of f over K. For every $a \in A$ and every $\sigma \in \mathrm{Hom}_K(L, M)$ the element $\sigma(a)$ is in E. Since L is generated over K by A, this means that $\sigma(L) \subset E$ for every $\sigma \in \mathrm{Hom}_K(L, M)$. It follows that $\mathrm{Hom}_K(L, M) = \mathrm{Hom}_K(L, E)$. This shows that $[L : K]_{\mathrm{sep}}$ only depends on the splitting field E and not on the choice of M.

The separability degree satisfies $[L : K]_{\text{sep}} \leq [L : K]$. This follows from the Artin-Dedekind Lemma. The separability degree is multiplicative in the sense that for finite extensions $K \subset E \subset L$ we have

$$[L : K]_{\text{sep}} \ = \ [L : E]_{\text{sep}} \cdot [E : K]_{\text{sep}}.$$

To see this, write $L = K(A)$ and let M be a splitting field of the product of the minimum polynomials over K of the elements $a \in A$. Then M is normal over K and hence also over E and L. For every $\sigma \in \text{Hom}_K(L, M)$, the isomorphism $\sigma : L \longrightarrow \sigma(L)$ extends to an automorphism $M \longrightarrow M$. This shows that the natural map

$$\text{Aut}_K(M) \ \longrightarrow \text{Hom}_K(L, M)$$

is surjective. Two automorphisms in $\text{Aut}_K(L)$ have the same image if and only if their quotient fixes L. Therefore we have

$$\#\text{Hom}_K(L, M) \ = \ \#\text{Aut}_K(M)/\#\text{Aut}_L(M).$$

There are similar formulas for $\#\text{Hom}_K(E, M)$ and $\#\text{Hom}_E(L, M)$. Multiplying the together, the cardinalities of the automorphism groups cancel out and the result follows.

Theorem/Criterion. *Let $K \subset L$ be a finite extension. The following are equivalent.*
(1) The extension $K \subset L$ is separable.
(2) We have $L = K(A)$ for some finite set of separable elements $A \subset L$.
(3) We have $[L : K]_{\text{sep}} = [L : K]$.

Proof. (1) $\Rightarrow$ (2) This is trivial.

(2) $\Rightarrow$ (3) If L is of the form $K(a)$ for some separable element a, then the minimum polynomial $f \in K[X]$ of a has $\deg f$ zeroes in any normal extension $L \subset M$. This means that $[L : K]_{\text{sep}} = \#\text{Hom}_K(L, M) = [L : K]$ as required.

In general, we write L as a successive extension, adjoining one separable element at the time. Since each element is separable over K, it is also separable over any larger field $K \subset E \subset L$. Therefore we can invoke the result for extensions generated by one single element. The fact that both the degree and the separability degree are multiplicative, implies the result in general.

(3) $\Rightarrow$ (1) Let $a \in L$. Then we have

$$K \subset K(a) \subset L$$

By Artin we have $[K(a) : K]_{\text{sep}} \leq [K(a) : K]$ and $[L : K(a)]_{\text{sep}} \leq [L : K(a)]$. Since both the degree and the separaibility degree are multiplicative, the hypothesis $[L : K]_{\text{sep}} = [L : K]$ implies $[K(a) : K]_{\text{sep}} = [K(a) : K]$. So, for every normal extension $L \subset M$ there are as many K-homomorphism $K(a) \longrightarrow M$ as the degree of the minimum polynomial f of a. This is only possible if all zeroes of f in M are distinct. So f is separable, as required.

It follows that an extension of the form $K \subset E \subset L$ is separable if and only if both $K \subset E$ and $E \subset L$ are separable.

Theorem/Criterion. *Let $K \subset L$ be a finite extension. The following are equivalent:*
(1) The extension $K \subset L$ is Galois;
(2) The field K is the fixed field of $\mathrm{Aut}_K(L)$;
(3) There a subgroup $G \subset \mathrm{Aut}(L)$ whose fixed field is K;
(4) The field L is the splitting field of some separable polynomial in $K[X]$.

Proof. (1) $\Rightarrow$ (2) We put $G = \mathrm{Aut}_K(L)$. The group G is *also* equal to $\mathrm{Aut}_{L^G}(L)$. Therefore we have

$$\#G = \#\mathrm{Hom}_{L^G}(L,L) \leq [L : L^G] \leq [L : K] \overset{(*)}{=} [L : K]_{\mathrm{sep}} \overset{(*)}{=} \#\mathrm{Hom}_K(L,L) = \#G.$$

The equalities $(*)$ follow from the fact that $K \subset L$ is normal and separable. It follows that we have equality everywhere. In particular, we obtain the equalities $L^G = K$ and $\#G = [L : K]$.

The implication (2) $\Rightarrow$ (3) is trivial. For (3) $\Rightarrow$ (4) we write $L = K(A)$ for some finite set $A \subset L$. By adding more elements to A, we may assume it to be G-stable. Then the polynomial $\prod_{a \in A}(X - a)$ has coefficients in $L^G = K$ and its splitting field is equal to L. It has distinct zeroes in L, so it is separable.

(4) $\Rightarrow$ (1) The field L is a splitting field. So it is normal by the criterion for normality. Since f is separable, so are the minimum polynomials of its zeroes. It follows by the separability criterion that $K \subset L$ is also separable. Therefore $K \subset L$ is Galois, as required.

The group $\mathrm{Aut}_K(L)$ is the *Galois group of L over K* and is denoted by $\mathrm{Gal}(L/K)$.

Theorem. *(Main Theorem of Galois theory). Let $K \subset L$ be a finite Galois extension with Galois group G. Then the following two maps*

$$\begin{array}{ccc} \{\textit{subfields } K \subset E \subset L\} & \longleftrightarrow & \{\textit{subgroups } H \subset G\} \\ E & \mapsto & \mathrm{Aut}_E(L), \\ L^H & \leftarrow & H. \end{array}$$

are inverse to one another. Moreover,
(a) for each subgroup H we have $[L : L^H] = \#H$;
(b) for each subfield E we have $\#\mathrm{Aut}_E(L) = [L : E]$.
(c) for any subfield E the extension $E \subset L$ is Galois with Galois group $\mathrm{Aut}_E(L)$. The extension $K \subset E$ is Galois if and only if $\mathrm{Aut}_E(L) \subset G$ is a normal subgroup. In this case $\mathrm{Gal}(E/K) = G/\mathrm{Aut}_E(L)$.

Proof. We have $H \subset \mathrm{Aut}_{L^H}(L)$ and $E \subset L^{\mathrm{Aut}_E(L)}$. Since we have

$$\begin{aligned} [L : L^{\mathrm{Aut}_E(L)}] &\overset{(a)}{=} \#\mathrm{Aut}_E(L) \overset{(b)}{=} [L : E], \\ \#\mathrm{Aut}_{L^H}(L) &\overset{(b)}{=} [L : L^H] \overset{(a)}{=} \#H, \end{aligned}$$

it suffices to prove the statements (a), (b) to establish. the Galois correspondence

By the criterion $L^H \subset L$ is Galois with Galois group H. Therefore $[L : L^H] = \#H$ and (a) follows. Part (b) and the first statement in (c) follow from the fact that the extension $E \subset L$ is normal and separable and therefore Galois. If the subgroup $H = \mathrm{Aut}_E(L)$ in very last statement is normal in G, then G/H acts on $E = L^H$ and its field of invariants is K. By the criterion E is Galois over K with Galois group G/H. Conversely, suppose that $E = L^H$ and that $K \subset E$ is Galois. By the criterion of normality, any $\sigma \in \mathrm{Aut}_K(L)$ restricts to an automorphism of E. This means that $\sigma^{-1}H\sigma$ fixes E, so that $\sigma^{-1}H\sigma \subset H$ and H is normal in G. The natural homomorphism $G/H \longrightarrow \mathrm{Aut}_K(E)$ is an isomorphism.

This proves the theorem.