4 Finite Extensions

Copyright © 2026, Gregory G. Smith
Last Updated: 2026–02–02

Under the influence of Emil Artin, linear algebra revolutionizes the understanding of field extensions.

This perspective appears in E. Artin, *Galois Theory*, 2nd edition, Notre Dame Mathematical Lectures, Notre Dame, IN, (1944), 82 pp.

4.0 Degree of an Extension

How can one measure the size of a field extension? For any field extension $K \subseteq L$, multiplication in L gives a scalar multiplication by elements in the subfield K, making L into a K-vector space.

4.0.0 Definition. Let $K \subseteq L$ be a field extension. The field L is a *finite extension* of K if L is a finite-dimensional K-vector space. The *degree* of L over K, denoted by $[L : K]$, is defined by

$$[L : K] := \begin{cases} \dim_K L & \text{if } L \text{ is a finite extension of } K, \\ \infty & \text{otherwise.} \end{cases}$$

4.0.1 Remark. We have $[\mathbb{C} : \mathbb{R}] = 2$ because $1, \mathrm{i}$ is an $\mathbb{R}$-basis for $\mathbb{C}$.

4.0.2 Remark. A field extension $K \subseteq L$ has degree $[L : K] = 1$ if and only if $K = L$. Indeed, we have $[L : K] = 1$ if and only if any nonzero element of L, such as $1 \in L$, is a K-basis for L. Hence, we have $[L : K] = 1$ if and only if $L = \{a \cdot 1_L \mid a \in K\} = K$.

4.0.3 Proposition. *Let $K \subseteq L$ be a field extension and fix $\alpha \in L$.*

(finite) *The element α is algebraic over K if and only if $[K(\alpha) : K] < \infty$.*

(basis) *Assume that $\alpha \in L$ is algebraic over K. When n is the degree of the minimal polynomial of α, the elements $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ form a K-basis for $K(\alpha)$, so $[K(\alpha) : K] = n$.*

Proof. Suppose that α is algebraic over K with minimal polynomial p having degree n. We first show that the elements $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ span the K-vector space $K(\alpha)$. As $K(\alpha) = K[\alpha]$, every element of $K(\alpha)$ is of the form $g(\alpha)$ for some polynomial $g \in K[x]$. Division with remainder of g by p gives $g = qp + (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1})$ for some $q \in K[x]$ and some $a_0, a_1, \dots, a_{n-1} \in K$. Evaluating at α, it follows that $g(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ because $p(\alpha) = 0$. Thus, the elements $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ span $K(\alpha)$ over K.

To prove linear independence of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, suppose that $0 = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ for some $a_0, a_1, \dots, a_{n-1} \in K$. Thus, the element α is a root of $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$. The minimal polynomial p has degree n, so this polynomial must be the zero polynomial. Since $a_j = 0$ for all $0 \leqslant j \leqslant n-1$, the elements $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are linearly independent. Since $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ forms a K-basis for $K(\alpha)$, we have $[K(\alpha) : K] = n$.

It remains to show that $[K(\alpha) : K] < \infty$ implies that α is algebraic. Set $n := [K(\alpha) : K]$. Since $K(\alpha)$ is an n-dimensional K-vector space, any collection of $n+1$ elements in $K(\alpha)$ is linearly dependent. In particular, there exist elements $a_0, a_1, \dots, a_n \in K$, not all zero, such that $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$. It follows that α is a root of the nonzero polynomial $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$. Thus, the element $\alpha \in L$ is algebraic over K. □

4.0.4 Remark. Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since the minimal polynomial of $\sqrt{2}+\sqrt{3}$ is $x^4 - 10x^2 + 1$, we see that $\big[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}\big] = 4$ and every element $\beta \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ has a unique representation of the form
$\beta = a+b(\sqrt{2}+\sqrt{3})+c(\sqrt{2}+\sqrt{3})^2+d(\sqrt{2}+\sqrt{3})^3$ for some $a, b, c, d \in \mathbb{Q}$.

4.0.5 Tower Theorem. *Let $K \subseteq L \subseteq M$ be field extensions.*
(infinite) *If $[L : K] = \infty$ or $[M : L] = \infty$, then $[M : K] = \infty$.*
(finite) *If $[L:K] < \infty$ and $[M:L] < \infty$, then $[M:K] = [M:L][L:K]$.*

Proof. Suppose that $[M:K] < \infty$ and let $\gamma_1, \gamma_2, \dots, \gamma_n$ be a K-basis of M. As M has finite dimension over K, so does every linear subspace in M. In particular, L is a linear subspace of M, so $[L : K] < \infty$. Consider $\alpha \in M$. Since $\gamma_1, \gamma_2, \dots, \gamma_n$ span M over K, there exist $a_1, a_2, \dots, a_n \in K$ such that $\alpha = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_n\gamma_n$. As $K \subseteq L$, the coefficients also lie in L. It follows that $[M : L] < \infty$.

For the second part, let $\ell := [L : K]$ and $m := [M : L]$. Pick the K-basis $\alpha_1, \alpha_2, \dots, \alpha_\ell$ for L, and the L-basis $\beta_1, \beta_2, \dots, \beta_m$ for M. We claim that the ℓm products $\alpha_j\beta_k$ for all $1 \leqslant j \leqslant \ell$ and all $1 \leqslant k \leqslant m$ forms a K-basis for M. We first demonstrate that these products span. Consider $\gamma \in M$. Since $\beta_1, \beta_2, \dots, \beta_m$ span M, there exist $b_1, b_2, \dots, b_m \in L$ such that $\gamma = b_1\beta_1 + b_2\beta_2 + \cdots + b_m\beta_m$. Similarly, for all $1 \leqslant k \leqslant m$, there exist $a_{1,k}, a_{2,k}, \dots, a_{\ell,k} \in K$ such that $b_k = a_{1,k}\alpha_1 + a_{2,k}\alpha_2 + \cdots + a_{\ell,k}\alpha_\ell$. Combining these equations give

$$\gamma = \sum_{k=1}^{m} \left(\sum_{j=1}^{\ell} a_{j,k}\alpha_j \right) \beta_k = \sum_{j=1}^{\ell} \sum_{k=1}^{m} a_{j,k}(\alpha_j\beta_k) .$$

We deduce that the products span M over K.

To prove linear independence, suppose that there exist $a_{j,k} \in K$ such that

$$0 = \sum_{j=1}^{\ell} \sum_{k=1}^{m} a_{j,k}\alpha_j\beta_k = \sum_{k=1}^{m} \left(\sum_{j=1}^{\ell} a_{j,k}\alpha_j \right) \beta_k .$$

Since $\beta_1, \beta_2, \dots, \beta_m$ are linearly independent over L, it follows that

$$0 = \sum_{j=1}^{\ell} a_{j,k}\alpha_j ,$$

for all $1 \leqslant j \leqslant m$. Since $\alpha_1, \alpha_2, \dots, \alpha_\ell$ are also linearly independent over K, we see that $a_{j,k} = 0$ for all $1 \leqslant j \leqslant m$ and all $1 \leqslant k \leqslant \ell$. Thus, the products are linear independent and form a K-basis for M. □

4.0.6 Problem. Compute $\big[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\big]$ two ways.

Solution. Since $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, the elements $1, \sqrt{2}$ form a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Similarly, $x^2 - 3$ is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$, so the elements $1, \sqrt{3}$ form a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. It follows that
$\big[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\big] = \big[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\big]\big[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\big] = (2)(2) = 4 .$
Moreover, $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Since $x^4 - 10x + 1$ is the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$, we also have $\big[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\big] = 4$. □

Copyright © 2026 by Gregory G. Smith

4.1 Algebraic Extensions

How does an elemental property extend to an entire field?

4.1.0 Problem. Let $\omega = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3}) = \exp(2\pi\mathrm{i}/3) \in \mathbb{C}$. Calculate $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}]$.

Solution. Consider the field extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\omega, \sqrt[3]{2})$. As $x^3 - 2$ is irreducible over $\mathbb{Q}$, we see that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Recall that $x^2 + x + 1$ has ω and $\overline{\omega} = \omega^2$, neither of which is real. Since $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, the polynomial $x^2 + x + 1$ has no root in this field, so it is the minimal polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$. Hence, we deduce that $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, and

$$[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = (2)(3) = 6\,. \quad \square$$

4.1.1 Definition. A field extension $K \subseteq L$ is called *algebraic* if every element of L is algebraic over K.

4.1.2 Lemma. *Every finite field extension is algebraic. For every field extension $K \subseteq L$ and every element $\alpha \in L$, the degree of the minimal polynomial of α over K divides $[L : K]$.*

There are algebraic extensions that are not finite.

Proof. An element $\alpha \in L$ yields the field extensions $K \subseteq K(\alpha) \subseteq L$. The Tower Theorem 4.0.5 establishes that $[K(\alpha) : K]$ is finite and $[L : K] = [L : K(\alpha)][K(\alpha) : K]$. By Proposition 4.0.3, the degree of the minimal polynomial of α over K equals $[K(\alpha) : K]$. $\square$

4.1.3 Theorem. *For every field extension $K \subseteq L$, we have $[L : K] < \infty$ if and only if there exist elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ such that each α_j is algebraic over K and $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.*

Proof. Suppose that $[L : K]$ is finite. Let $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ be a basis for the K-vector space L. The inclusions

$$L = \{a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \mid a_j \in K\} \subseteq K(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq L$$

demonstrate that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Each α_j is algebraic over K by Lemma 4.1.2.

Suppose that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where each α_j is algebraic over K. Set $L_0 := K$ and $L_r := K(\alpha_1, \alpha_2, \dots, \alpha_r)$ for all $1 \leqslant r \leqslant n$, so that $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n = L$. Corollary 3.0.4 shows that

$$L_r = K(\alpha_1, \alpha_2, \dots, \alpha_r) = \big(K(\alpha_1, \alpha_2, \dots, \alpha_{r-1})\big)(\alpha_r) = L_{r-1}(\alpha_r)\,.$$

Proposition 4.0.3 gives $[L_r : L_{r-1}] = [L_{r-1}(\alpha_r) : L_{r-1}] < \infty$, so every successive extension has finite degree. Repeated use of the Tower Theorem 4.0.5 yields

$$\begin{aligned}[L : K] &= [L : L_{n-1}][L_{n-1} : K] \\ &= [L : L_{n-1}][L_{n-1} : L_{n-2}][L_{n-2} : K] \\ &= [L : L_{n-1}][L_{n-1} : L_{n-2}] \cdots [L_1 : K] < \infty\,. \end{aligned} \quad \square$$

4.1.4 Proposition. *Let $K \subseteq L$ be a field extension. When $\alpha, \beta \in L$ are algebraic over K, their sum $\alpha + \beta$ and their product $\alpha\beta$ are also algebraic.*

Copyright © 2026 by Gregory G. Smith

Proof. Theorem 4.1.3 implies that $K \subseteq K(\alpha, \beta)$ is a finite extension. By Lemma 4.1.2, every element in $K(\alpha, \beta)$ is algebraic over K. In particular, the elements $\alpha + \beta \in K(\alpha, \beta)$ and $\alpha\beta \in K(\alpha, \beta)$ are. □

4.1.5 Corollary. *For every field extension $K \subseteq L$, the subset of algebraic elements over K is a subfield of L containing K.*

Proof. Let $M := \{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$. We have $K \subseteq M$ because $a \in K$ is a root of $x - a \in K[x]$. By Proposition 4.1.4, the subset M is closed under addition and multiplication. Since $-1 \in K$, we see that $\alpha \in M$ implies that $-\alpha = (-1)(\alpha) \in M$. Finally, when $0 \neq \alpha \in M$, there exists $a_0, a_1, \ldots, a_n \in K$ such that $a_0 \neq 0$ and $0 = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n$. Multiplying by $1/(\alpha^n)$ gives $0 = a_0 + a_1\alpha^{-1} + a_2\alpha^{-2} + \cdots + a_{n-1}\alpha^{-n+1} + a_n\alpha^{-n}$. Hence, $1/\alpha$ is a root of $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in K[x]$ and $1/\alpha \in M$. □

4.1.6 Definition. A complex number $z \in \mathbb{C}$ is an *algebraic number* if it is algebraic over $\mathbb{Q}$. The *field of algebraic numbers* is

$$\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ is an algebraic number}\}.$$

An *algebraic integer* is a complex number that is a root of a monic polynomial with integer coefficients.

4.1.7 Theorem. *Let $K \subseteq L \subseteq M$ be field extensions and assume that L is algebraic over K. For every $\beta \in M$ that is algebraic over L, the element β is algebraic over K.*

Proof. Let β be a root of $f = \alpha_0x^n + \alpha_1x^{n-1} + \cdots \alpha_n \in L[x]$ where $\alpha_0, \alpha_1, \ldots, \alpha_n \in L$ are not all zero and each β_j is algebraic over K. Theorem 4.1.3 shows that $L' := K(\alpha_1, \alpha_1, \ldots, \alpha_n)$ is a finite extension of K. Since $f \in L'[x]$, the element β is algebraic over L', and the field extension $K \subseteq L'(\beta)$ is finite. The Tower Theorem 4.0.5 gives $[L'(\beta) : K] = [L'(\beta) : L'][L' : K] < \infty$. Therefore, the field extension $K \subseteq L'(\beta)$ is finite and algebraic, so β is algebraic over K. □

4.1.8 Remark. Every complex solution of the equation

$$x^{11} - (\sqrt{2} + \sqrt{5})x^5 + 3\sqrt[4]{12}x^3 + (1 + 3\mathrm{i})x + \sqrt[5]{17}$$

lies in $\overline{\mathbb{Q}}$, because the coefficients are algebraic over $\mathbb{Q}$.

4.1.9 Corollary. *Let $K \subseteq L \subseteq M$ be a chain of field extensions. When M is algebraic over L and L is algebraic over K, M is algebraic over K.*

Proof. Follows immediately from Corollary 4.1.5. □

4.1.10 Proposition. *Every nonconstant polynomial in $\overline{\mathbb{Q}}[x]$ has a root in the field $\overline{\mathbb{Q}}$ of algebraic numbers.*

We call $\overline{\mathbb{Q}}$ the *algebraic closure* of $\mathbb{Q}$.

Proof. Let $f \in \overline{\mathbb{Q}}[x]$ be a nonconstant polynomial. Since $\overline{\mathbb{Q}} \subset \mathbb{C}$, the Fundamental Theorem of Algebra establishes that f has a root $\alpha \in \mathbb{C}$. The element α is algebraic over $\overline{\mathbb{Q}}$ because $f \in \overline{\mathbb{Q}}[x]$. By construction, the field $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$, so α is algebraic over $\mathbb{Q}$ by Theorem 4.1.7. Thus f has the root $\alpha \in \overline{\mathbb{Q}}$. □

Copyright © 2026 by Gregory G. Smith

4.2 Splitting Fields

What is the smallest field extension over which a polynomial splits completely? The following definition capture the basic idea.

4.2.0 Definition. Let $f \in K[x]$ have positive degree $n \in \mathbb{N}$. A field extension $K \subseteq L$ is a *splitting field* of f over K if
(splitting) $f = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ for some $a_0 \in K$ and some $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, and
(minimal) $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

4.2.1 Remark. The finite extension field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ of $\mathbb{Q}$ is a splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$.

4.2.2 Remark. The field $\mathbb{Q}(\mathrm{i}, \sqrt[4]{2})$ is a splitting field of x^4-2 over $\mathbb{Q}$.

4.2.3 Remark. A splitting field of $f \in K[x]$ depends on both the polynomial f and the field K. For instance, a splitting field of x^2+1 over $\mathbb{Q}$ is $\mathbb{Q}(\mathrm{i})$, a splitting field of x^2+1 over $\mathbb{R}$ is $\mathbb{C}$, and a splitting field of x^2+1 over $\mathbb{C}$ is $\mathbb{C}$.

4.2.4 Theorem. *Let $f \in K[x]$ be a polynomial of positive degree n. For every splitting field K of f over K, we have $[L : K] \leqslant n!$.*

This bound is sharp, meaning there are cases where equality occurs.

Proof. We proceed by induction on n. When $n = 1$, the polynomial $f = ax + b$ has $-b/a \in K$ as a root, so $L = K$ and $[L : K] \leqslant 1!$.

Suppose that $n > 1$. Let $L := K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a splitting field of f over K and consider $g \in L[x]$ determined by $f = (x-\alpha_1)g$. Division with remainder implies that $g \in K(\alpha_1)[x]$. The roots of g are obviously $\alpha_2, \alpha_3, \ldots, \alpha_n$, so that a splitting field of g over $K(\alpha_1)$ is given by $(K(\alpha_1))(\alpha_2, \alpha_3, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_n) = L$. Since $g \in K(\alpha_1)[x]$ has degree $n-1$, the induction hypothesis implies that $[L : K(\alpha_1)] \leqslant (n-1)!$. By the Tower Theorem 4.0.5, we have

$$[L : K] = [L : K(\alpha_1)][K(\alpha_1) : K] \leqslant (n-1)!\,[K(\alpha_1) : K].$$

By Proposition 4.0.3, we also know that $[K(\alpha_1) : K]$ is the degree of the minimal polynomial of α_1 over K. Since $f(\alpha_1) = 0$, we deduce that $[K(\alpha_1) : K] \leqslant n$ and $[L : K] \leqslant n!$. □

To study the uniqueness of splitting fields, we consider slightly more general situation.

4.2.5 Theorem. *Assume that $\varphi : K_1 \to K_2$ is an isomorphism of fields. For every $f \in K_1[x]$, let L_1 be a splitting field of f over K_1 and let L_2 be a splitting field of the image $\varphi(f) \in K_2[x]$ over K_2. There exists a field isomorphism $\widehat{\varphi} : L_1 \to L_2$ such that $\varphi = \widehat{\varphi}|_{K_1}$.*

$$\begin{array}{ccc} L_1 & \xrightarrow[\cong]{\widehat{\varphi}} & L_2 \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\cong]{\varphi} & K_2 \end{array}$$

Figure 4.1: Commutative diagram arising from Theorem 4.2.5

Proof. We proceed by induction on $n := \deg(f)$. When $n = 1$, the polynomial $f = ax+b$ has $-b/a \in K_1$ as a root, so $L_1 = K_1$. Similarly, $\varphi(f) = \varphi(a)x + \varphi(b)$ has $-\varphi(b)/\varphi(a) \in K_2$ as a root, so $L_2 = K_2$. Hence, in the base case, we take $\widehat{\varphi} = \varphi$.

Suppose that $n > 1$. Let $L_1 := K_1(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a splitting field of f over K_1 where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f. Consider the

Copyright © 2026 by Gregory G. Smith

chain $K_1 \subseteq K_1(\alpha_1) \subseteq L_1$, where the field extension $K(\alpha_1) \subseteq L_1$ is a splitting field for the polynomial $g := f/(x - \alpha_1)$. Let $p_1 \in K_1[x]$ be the minimal polynomial of α_1. It follows that p_1 is an irreducible factor of $f \in K_1[x]$ because α_1 is a root of f. Hence, we obtain $K_1(\alpha_1) = K_1[\alpha_1] \cong K_1[x]\big/\langle p_1\rangle$ where $\alpha_1 \mapsto x + \langle p_1\rangle$.

We next find a root of $\varphi(f) \in K_2[x]$ corresponding to α_1. Overloading the symbol φ, the isomorphism $\varphi : K_1 \to K_2$ determines the the ring isomorphism $\varphi : K_1[x] \to K_2[x]$ that sends f to $\varphi(f)$, sends factors to factors, and sends irreducibles to irreducibles. Thus, p_1 maps to an irreducible factor p_2 of $\varphi(f)$. As $\varphi(f)$ splits completely over L_2, so does p_2. This allows one to label the roots of $\varphi(f)$ as $\beta_1, \beta_2, \ldots, \beta_n \in L_2$ where β_1 is a root of p_2. Hence, we have field extensions $K_2 \subseteq K_2(\beta_1) \subseteq L_2$ where $K_2(\beta_1)$ is a splitting field for the polynomial $g_2 := \varphi(f)/(x - \beta_1)$. As before, we deduce that $K_2(\beta_1) = K_2[\beta_1] \cong K_2[x]\big/\langle p_2\rangle$ that sends β_1 to $x + \langle p_2\rangle$.

The isomorphism $\varphi : K_1[x] \to K_2[x]$ takes p_1 to p_2, so it induces an isomorphism of quotient rings from $K_1[x]/\langle p_1\rangle$ to $K_2[x]/\langle p_2\rangle$ that takes $x + \langle p_1\rangle$ to $x + \langle h_2\rangle$ and that restricts to the isomorphism φ on the coefficient fields. Combined with the earlier isomorphisms, we have a field isomorphism $\varphi_1 : K_1(\alpha_1) \to K_2(\beta_1)$. Since φ_1 takes α_1 to β_1 and f to $\varphi(f)$, it also takes g_1 to g_2.

It remains to prove the existence of the isomorphism $\widehat{\varphi} : L_1 \to L_2$. Since $g_1 = f_1/(x - \alpha_1)$ has degree $n - 1$, the induction hypothesis yields applied to g_1 and φ_1 produces the isomorphism $\widehat{\varphi_1} : L_1 \to L_2$ whose restriction to $K_1(\alpha_1)$ is φ_1. Since φ_1 itself restricts to φ on K_1, the isomoprhism $\widehat{\varphi_1}$ is the required field isomorphism. □

4.2.6 Corollary. *For all splitting fields L_1 and L_2 of $f \in K[x]$ over K, there exists a field isomorphism $\psi : L_1 \to L_2$ that is the identity on K.* □

4.2.7 Proposition. *Let L be a splitting field of a polynomial in $K[x]$. For every irreducible $p \in K[x]$ with roots $\alpha, \beta \in L$, there exists a field isomorphism $\sigma : L \to L$ that is the identity on K and takes α to β.*

Proof. The isomorphism $K(\alpha) = K[\alpha] \cong K[x]\big/\langle p\rangle$ is the identity on K and sends α to $x + \langle p\rangle$. Similarly, $K(\beta) = K[\beta] \cong K[x]\big/\langle p\rangle$ is the identity on K and sends β to $x + \langle p\rangle$. Combining these produces the field isomorphism $\varphi : K(\alpha) \to K(\beta)$ such that $\varphi(\alpha) = \beta$ and φ is the identity on K.

Suppose that L is a splitting field of $f \in K[x]$. Since $f \in K(\alpha)[x]$ and $f \in K(\beta)[x]$, the field L is a splitting field of f over both $K(\alpha)$ and $K(\beta)$. Hence, Theorem 4.2.5 give the field isomorphism $\widehat{\varphi} : L \to L$ such that its restriction to $K(\alpha)$ is φ. Since φ is the identity on K and maps α to β, $\sigma := \widehat{\varphi}$ is the desired field isomorphism. □

4.2.8 Remark. The field $L := \mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$. This polynomial is irreducible over $\mathbb{Q}$ and has $\pm\sqrt{2} \in L$ as roots. Proposition 4.2.7 implies that there is a field isomorphism $\sigma : L \to L$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$.

$$\begin{array}{ccc} L_1 & \xrightarrow[\cong]{\widehat{\varphi}} & L_2 \\ \uparrow & & \uparrow \\ K & \xrightarrow[\cong]{\mathrm{id}_K} & K \end{array}$$

Figure 4.2: Commutative diagram arising from Corollary 4.2.6

Copyright © 2026 by Gregory G. Smith