5 Normality and Separability

Last Updated: 2026–02–08

Certain field extensions possess special structural properties. This chapter studies these important features.

5.0 Normal Extensions

How can we characterize splitting fields among all finite extensions?

5.0.0 Proposition. *Let L be a splitting field for the polynomial $f \in K[x]$, and let $g \in K[x]$ be irreducible. When g has one root in L, the polynomial g splits completely over L.*

Proof. We may assume that the polynomials f and g are monic. Let $L := K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where $f = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. If $\beta \in L$ is a root of g, then g is the minimal polynomial of β, because g is irreducible and monic. We claim that all roots of g lie in L.

Since the elements $\alpha_1, \alpha_2, \dots, \alpha_n$ are algebraic over K, it follows that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n) = K[\alpha_1, \alpha_2, \dots, \alpha_n]$, so $\beta = h(\alpha_1, \alpha_2, \dots, \alpha_n)$ for some $h \in K[x_1, x_2, \dots, x_n]$. Consider the polynomial

$$q(x) := \prod_{\sigma \in \mathfrak{S}_n} \left(x - h(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \dots, \alpha_{\sigma(n)})\right) \in L[x]\,.$$

By construction, all the roots of q lie in L. The factor corresponding to $\sigma = \mathrm{id}$ is $x - h(\alpha_1, \alpha_2, \dots, \alpha_n) = x - \beta$, so β is a root of s. Thus, it suffices to prove that $q \in K[x]$.

To that end, observe that the universal polynomial

$$Q(x) := \prod_{\sigma \in \mathfrak{S}_n} \left(x - h(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})\right)$$

has coefficients in $K[x_1, x_2, \dots, x_n]$, and permuting the indeterminants $x_1, x_2, \dots, x_n$ interchanges the factors of Q. Hence, expanding Q gives the expression

$$Q(x) = \sum_{j=0}^{n!} q_j(x_1, x_2, \dots, x_n)\, x^j\,,$$

where each $q_j \in K[x_1, x_2, \dots, x_n]$ is symmetric. Since the α_j are roots of $f \in K[x]$, we deduce that $q_j(\alpha_1, \alpha_2, \dots, \alpha_n) \in K$. We conclude that

$$q(x) = \sum_{j=0}^{n!} q_j(\alpha_1, \alpha_2, \dots, \alpha_n)\, x^j \in K[x]\,. \qquad \square$$

5.0.1 Remark. The field extension $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for any polynomial in $\mathbb{Q}[x]$. Indeed, $x^3 - 2$ is irreducible over $\mathbb{Q}$ and has a root in this field. However, it does not split completely over this field, because $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ does not contain the complex roots $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ of $x^3 - 2$.

5.0.2 Definition. An algebraic extension $K \subseteq L$ is *normal* if every irreducible polynomial in $K[x]$ that has a root in L splits completely over L.

5.0.3 Problem. Let $n \in \mathbb{Z}$ be positive and set $\zeta := \exp(2\pi\mathrm{i}/n) \in \mathbb{C}$. Verify that the field extension $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ is normal.

Solution. The element ζ is a primitive nth root of unity, so it is the root of the polynomial $x^n - 1 \in \mathbb{Q}[x]$. The field $\mathbb{Q}(\zeta)$ contains all power ζ^j where $0 \leqslant j < n$, and these are precisely the roots of $x^n - 1$. Hence, $\mathbb{Q}(\zeta)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$. Since splitting fields are normal extensions, it follows that $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ is normal. □

5.0.4 Proposition. *An algebraic field extension $K \subseteq L$ is normal if and only if, for every $\alpha \in L$, the minimal polynomial of α over K splits completely over L.*

Proof. Suppose that $\alpha \in L$. Let $p \in K[x]$ be the minimal polynomial of α over K. As p is irreducible and has $\alpha \in L$ as a root, normality implies that every root of p lies in L, so p splits completely over L.

Suppose that, for each $\alpha \in L$, the minimal polynomial of α over K splits completely in L. Let $f \in K[x]$ be an irreducible having a roots $\alpha \in L$. It follows that f is the minimal polynomial of α over K. By hypothesis, f splits completely over L. Therefore, every irreducible polynomial in $K[x]$ that has a root in L splits in L, which is precisely the definition of normality. □

5.0.5 Theorem. *Let $K \subseteq L$ be a field extension. The field L is the splitting field for some $f \in K[x]$ if and only if the field extension $K \subseteq L$ is normal and finite.*

Proof. Suppose that L is the splitting field of the polynomial f over K. Proposition 5.0.0 implies that L is normal, and Theorem 4.2.4 implies that L is finite.

Conversely, suppose that the field extension $K \subseteq L$ is normal and finite. Finiteness implies that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where each α_j is algebraic over K. For all $1 \leqslant j \leqslant n$, let $p_j \in K[x]$ be the minimal polynomial of α_j, and set $f = p_1 p_2 \cdots p_n$. We claim that L is the splitting field of f over K.

First observe that every p_j splits completely over L because $K \subseteq L$ is normal and $p_j \in K[x]$ is irreducible with a root $\alpha_j \in L$. It follows that f splits completely over L. Let $L' \subseteq L$ be the subfield of L generated by K and the roots of f. As the roots of f include $\alpha_1, \alpha_2, \dots, \alpha_n$, we see that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq L' \subseteq L$. Therefore, we deduce that $L' = L$ and L is the splitting field of f over K. □

5.0.6 Remark. The algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ is normal and infinite. By definition, $\overline{\mathbb{Q}}$ contains every root of every polynomial in $\mathbb{Q}[x]$. In particular, if an irreducible polynomial $f \in \mathbb{Q}[x]$ has one root in $\overline{\mathbb{Q}}$, then all of its roots lie in $\overline{\mathbb{Q}}$. Hence, every irreducible polynomial over $\mathbb{Q}$ that has a root in $\overline{\mathbb{Q}}$ splits completely, so this field extension is normal. You will prove on a problem set that $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$.

5.1 Separable Extensions

When does a polynomial have distinct roots? Given $f \in K[x]$ with splitting field $K \subseteq L$, we have $f = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, for some $a_0 \in K$ and some $\alpha_1, \alpha_2, \dots, \alpha_n \in L$. Let $\beta_1, \beta_2, \dots, \beta_r$ be the distinct elements of L among $\alpha_1, \alpha_2, \dots, \alpha_n$ and let m_j be the number of times $x - \beta_j$ appears in the factorization of f:

$$f = a_0(x-\beta_1)^{m_1}(x-\beta_2)^{m_2}\cdots(x-\beta_r)^{m_r}\,.$$

These definitions are independent of the splitting field, because all splitting fields of f over K are isomorphic.

The *multiplicity* of β_j is $m_j \in \mathbb{N}$, and the root β_j is *simple* if $m_j = 1$.

5.1.0 Definition. A polynomial $f \in K[x]$ is called *separable* if it is nonconstant and its roots in a splitting field are all simple.

In other words, f is separable if its has distinct roots.

5.1.1 Proposition. *For every monic nonconstant polynomial $f \in K[x]$, the following are equivalent.*

(separable) *The polynomial f is separable.*
(discriminant) *The discriminant $\Delta(f)$ is nonzero.*
(derivative) *The polynomial f and its derivative f' are coprime.*

Being coprime or relative prime means $\gcd(f, f') = 1$.

Proof. When $\deg(f) = 1$, the discriminant is $\Delta(f) = 1$, and $f' \in K^\times$, so all three conditions hold. We may assume that $n := \deg(f) > 1$.

For the equivalence of the first two conditions, let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of f in some splitting field. The formula

$$\Delta(f) = \prod_{1 \leqslant j < k \leqslant n} (\alpha_j - \alpha_k)^2\,,$$

shows that $\Delta(f) \neq 0$ if and only if $\alpha_j \neq \alpha_k$ for all $j < k$.

It remains to verify the equivalence of the first and last conditions. Let L be a splitting field of f over K, so

$$f = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in L[x]\,.$$

For a fixed index j, write $f = (x-\alpha_j)g_j$ and $h_j = \prod_{k\neq j}(x-\alpha_k)$. Differentiating, we obtain $f'(x) = (x-\alpha_j)g_j' + g_j$ by the product rule. Evaluating at α_j gives

$$f'(\alpha_j) = g_j(\alpha_j) = \prod_{k\neq j}(\alpha_j - \alpha_k)\,,$$

If the third conditions fails, then f and f' have a common factor h of positive degree. Since h divides f, we must have $h(\alpha_j) = 0$ for some j, which implies that h divides f' and $f'(\alpha_j) = 0$. It follows that $0 = f'(\alpha_j) = \prod_{k\neq j}(\alpha_j - \alpha_k)$, so $\alpha_j = \alpha_k$ for some $j \neq k$. If the third conditions holds, then $1 = pf + qf'$ for some $p, q \in K[x]$. Evaluating at α_j gives $1 = q(\alpha_j)f'(\alpha_j)$, so $f'(\alpha_j) \neq 0$. It follows that $\prod_{k\neq j}(\alpha_j - \alpha_k)$ is nonzero for all j, so $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct. □

5.1.2 Problem. Let $\mathbb{F}_2 := \mathbb{Z}/\langle 2\rangle$ be the field with two elements. Prove that $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible and separable.

Solution. Since $(0)^2+(0)+1 = 1$ and $(1)^2+1+1 = 1$, this polynomial has no roots in $\mathbb{F}_2$, so it is irreducible. Since $f' = 2x+1 = 1$, we have $\gcd(f, f') = 1$, so this polynomial is separable. □

5.1.3 Definition. Let $K \subseteq L$ be an algebraic extension.

(element) The element $\alpha \in L$ is *separable* over K if its minimal polynomial over K is separable.

(extension) The field extension $K \subseteq L$ is *separable* if every $\alpha \in L$ is separable over K.

5.1.4 Problem. Show that $f := x^n - 1 \in K[x]$ is not separable if and only if the characteristic of the base field K divides n.

Solution. The polynomial f is separable if and only if f is coprime to $f' = nx^{n-1}$. When $n \neq 0$ in K, the only irreducible factor of f' is x which does not divide f. Thus, f is coprime to f'. When $n = 0$ in K, the derivative f' is identically zero, so f divides f'. Thus, f is not coprime to f'. We conclude that $x^n - 1 \in K[x]$ fails to be separable if and only if the characteristic of the field K divides n. □

5.1.5 Lemma. *An irreducible polynomial $f \in K[x]$ having degree n is separable if either of the following conditions is satisfied:*

(zero) *K has characteristic zero.*

(positive) *K has positive characteristic p and p does not divide n.*

Proof. Let $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ where $n > 0$ and $a_0 \neq 0$. It follows that $f' = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}$. Either condition implies that $n \neq 0$ in K, so $na_0 \neq 0$. Hence, f' is nonzero and has degree $n-1$. Since f is irreducible, its only divisors (up to constant multiples) are 1 and f, so $g := \gcd(f, f')$ must be 1 or f. However, g divides f' and $f' \neq 0$ imply that $\deg(g) \leqslant \deg(f') = n-1$. We deduce that g cannot be a multiple of f, so $\gcd(f, g') = 1$. □

5.1.6 Lemma. *A polynomial is separable if and only if it is a product of irreducible polynomials, each of which is separable and no two of which are multiples of each other.*

Proof. Suppose that $f \in K[x]$ is separable. If a factor of f has multiple roots in a splitting field, then the same is true for f. Thus, any irreducible factor of f must be separable. If the irreducible factorization of f includes two factors that are multiples of each other, then the product of these factors would be an inseparable divisor of f. Hence, the factorization of f must consist of separable, irreducible polynomials no two of which are multiples of each other.

Conversely, let $f = g_1g_2 \cdots g_r$ where $g_1, g_2, \ldots, g_r$ are separable and irreducible, and no two are multiples of each other. In the splitting field of f, each g_j has distinct roots. Suppose that g_j and g_k share a root α for some $j \neq k$. Since g_j and g_j are irreducible, this would imply that each was a constant times the minimal polynomial of α, which is a contradiction. Hence, f is separable. □

5.1.7 Proposition. *Assume that the field K has characteristic zero. Any irreducible polynomial in $K[x]$ is separable. Every algebraic extension of K is separable. A nonconstant $f \in K[x]$ is separable if and only if f is a product of irreducibles, no two of which are multiples of each other.*

5.2 Theorem of the Primitive Element

Which field extension can be realized by adjoining a single element?

5.2.0 Theorem of the Primitive Element. *Consider a finite extension $K \subseteq L := K(\alpha_1, \alpha_2, \dots, \alpha_n)$. When each α_j is separable over K, there exists $\alpha \in L$ separable over K such that $L = K(\alpha)$. Moreover, when the base field K is infinite, the element α can be chosen to be of the form $\alpha := c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$ for some $c_1, c_2, \dots, c_n \in K$.*

Given a field extension $K \subseteq L$, an element $\alpha \in L$ is *primitive* if $L = K(\alpha)$.

Proof. Assume that K is infinite. We proceed by induction on n. When $n = 2$, we have $L = K(\alpha_1, \alpha_2)$. For all $1 \leqslant j \leqslant 2$, let $p_j \in K[x]$ be the minimal polynomial of α_j over K, and set $d_j := \deg(p_j)$. In a splitting field of p_1p_2, the separability of α_1, α_2 implies that p_1 has distinct roots $\beta_1, \beta_2, \dots, \beta_{d_1}$ and p_2 has distinct roots $\gamma_1, \gamma_2, \dots, \gamma_{d_2}$. Since K is infinite, we can find $\lambda \in K$ such that

$$\lambda \neq \frac{\beta_j - \beta_k}{\gamma_s - \gamma_r} \text{ for all } 1 \leqslant j, k \leqslant d_1 \text{ and all } 1 \leqslant s, r \leqslant d_2 \text{ such that } s \neq r.$$

It follows that $\beta_k + \lambda\gamma_s \neq \beta_j + \lambda\gamma_r$ for all $(r, s) \neq (j, k)$. In particular, we have $\beta_1 + \lambda\gamma_1 \neq \beta_j + \lambda\gamma_k$ for all $1 \leqslant j \leqslant d_1$ and all $1 \leqslant k \leqslant d_2$.

We claim that $K(\beta_1 + \lambda\gamma_1) = K(\beta_1, \gamma_1)$. As $K(\beta_1 + \lambda\gamma_1) \subseteq K(\beta_1, \gamma_1)$, it suffices to show that $\beta_1, \gamma_1 \in K(\beta_1 + \lambda\gamma_1)$. By construction, $p_2(x)$ vanishes at γ_1 and lies in $K[x] \subseteq K(\beta_1 + \lambda\gamma_1)[x]$, and the translate $p_1(\beta_1 + \lambda\gamma_1 - \lambda x)$ vanishes at γ_1 and lies in $K(\beta_1 + \lambda\gamma_1)[x]$. We examine the greatest common divisor of p_2 and $p_1(\beta_1 + \lambda\gamma_1 - \lambda x)$. If it were 1, then there exists $f_1, f_2 \in K(\beta_1 + \lambda\gamma_1)[x]$ such that

$$f_2(x)p_2(x) + f_1(x)p_1(\beta_1 + \lambda\gamma_1 - \lambda x) = 1\,.$$

Evaluating at γ_1 yields the contradiction $0 = 1$. Hence, we have $h := \gcd\big(p_2(x), p_1(\beta_1 + \lambda\gamma_1 - \lambda x)\big) \in K(\beta_1 + \lambda\gamma_1)[x]$ has positive degree. If the degree were greater than 1, then h dividing p_2 implies that for some $2 \leqslant j \leqslant m$, γ_j would be a root of h. Since h divides the translate $p_1(\beta_1 + \lambda\gamma_1 - \lambda x)$, γ_j must also be a root of this translate. Since the roots of p_1 are $\beta_1, \beta_2, \dots, \beta_{d_1}$, we have $\beta_1 + \lambda\gamma_1 - \lambda\gamma_j = \beta_k$ for some $1 \leqslant k \leqslant d_1$ which contradicts our choice of λ. Thus, h has degree 1 and $h = x - \gamma_1$ because γ_1 is a root. However, we also know that $h \in K(\beta_1 + \lambda\gamma_1)[x]$, so $\gamma_1 \in K(\beta_1 + \lambda\gamma_1)$. We thereby deduce that $\beta_1 = (\beta_1 + \lambda\gamma_1) - \lambda\gamma_1 \in K(\beta_1 + \lambda\gamma_1)$.

Let $p \in K[x]$ denote the minimal polynomial over $\beta_1 + \lambda\gamma_1$ over K. We need to show that p is separable. Consider

$$q(x) = \prod_{k=1}^{d_2} p_1(x - \lambda\gamma_k)\,.$$

Observe that $\beta_1 + \lambda\gamma_1$ is a root of q. Since $p_1 \in K[x]$, $\lambda \in K$, and $\gamma_1, \gamma_2, \dots, \gamma_{d_2}$ are roots of $p_2 \in K[x]$, one verifies that $q \in K[x]$. It follows that p divides q in $K[x]$, which implies that

$$q(x) = \prod_{k=1}^{d_2} \prod_{j=1}^{d_1} (x - (\beta_j + \lambda\gamma_k))\,.$$

As q has distinct roots, p is separable, which proves that $\beta_1 + \lambda\gamma_1$ is separable over K.

Now, suppose that $n > 2$ and $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ where each α_j is separable over K. By the induction hypothesis, there exist $c_1, c_2, \dots, c_{n-1} \in K$ such that $K(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) = K(\alpha_0)$ where $\alpha_0 := c_1\alpha_1 + c_2\alpha_2 + \cdots + c_{n-1}\alpha_{n-1}$ is separable over K. It follows that

$$L = K(\alpha_1, \alpha_2, \dots, \alpha_n) = \big(K(\alpha_0)\big)(\alpha_n) = K(\alpha_0, \alpha_n)\,.$$

By the proof for $n = 2$, we have $K(\alpha_0, \alpha_n) = K(\alpha_0 + \lambda a_n)$ for some $\lambda \in K$ where $\alpha_0 + \lambda\alpha_n$ is separable over K. Setting $c_n = \lambda$, we see that $\alpha_0 + \lambda\alpha_n = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$ is the desired separable primitive element. □

5.2.1 Remark. The proof is very different when K is a finite field.

5.2.2 Corollary. *Let $K \subseteq L$ be a finite field extension.*

(extension) *When the field extension $K \subseteq L$ is separable, there exists an element $\alpha \in L$ such that $L = K(\alpha)$.*

(base) *When the base field K has characteristic zero, there exists $\alpha \in L$ such that $L = K(\alpha)$. When $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, the element α can be chose to be of the form*

$$\alpha := c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

where $c_1, c_2, \dots, c_n \in K$.

Proof. Since the field extension $K \subseteq L$ is finite, there are elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ algebraic over K such that $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. In the first case, each α_j is separable because $K \subseteq L$ is separable, so we are done by Theorem of the Primitive Element. □

5.2.3 Remark. Consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. For all $\lambda \neq 0$ in $\mathbb{Q}$, the element $\sqrt{2} + \lambda\sqrt{3}$ is a primitive element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

5.2.4 Problem. Let K be a field of characteristic p. Consider the field extension $K(s,t) \subset L$ where L is the splitting field of the polynomial $(x^p - s)(x^p - t) \in K(s,t)[x]$. Show that L has no primitive element.

Solution. By hypothesis, there exists $\alpha, \beta \in L$ such that $\alpha^p = s$ and $\beta^p = t$. One verifies that $\big[L : K(s,t)\big] = p^2$.

Suppose that $\gamma \in L$. Since $L = \big(K(t_1, t_2)\big)(\alpha, \beta) = \big(K(t_1, t_2)\big)[\alpha, \beta]$, we write $\gamma = \sum_{j,k} c_{j,k}\alpha^j\beta^k$where $c_{j,k} \in K(s,t)$. It follows that

$$\gamma^p = \left(\sum_{j,k} c_{j,k}\alpha^j\beta^k\right)^p = \sum_{j,k} c_{j,k}^p\alpha^{jp}\beta^{kp} = \sum_{j,k} c_{j,k}^p s^j t^k \in K(s,t)\,.$$

Hence, γ is a root of $x^p - \gamma^p \in K(s,t)[x]$, so $\big[K(s,t)(\gamma) : K(s,t)\big] \leqslant p$. We conclude that $L \neq K(x,t)(\gamma)$ for any $\gamma \in L$. Therefore, L has no primitive element. □