3 Field Extensions

Last Updated: 2026–01–29

The structure of certain types of field extensions form a key part of Galois theory. We develop the relevant mathematical language.

3.0 Adjoining elements

How can we describe subrings and subfields of a field extension?

3.0.0 Notation. Let $K \subseteq L$ be a field extension. For all field elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$, we define

$$\begin{aligned} K[\alpha_1, \alpha_2, \dots, \alpha_n] &:= \{h(\alpha_1, \alpha_2, \dots, \alpha_n) \mid h \in K[x_1, x_2, \dots, x_n]\}, \\ K(\alpha_1, \alpha_2, \dots, \alpha_n) &:= \left\{\tfrac{\alpha}{\beta} \mid \alpha, \beta \in K[\alpha_1, \alpha_2, \dots, \alpha_n] \text{ with } \beta \neq 0\right\} \\ &= \left\{h(\alpha_1, \alpha_2, \dots, \alpha_n) \mid h \in K(x_1, x_2, \dots, x_n)\right\}. \end{aligned}$$

Although we overload the mathematical meaning of parentheses and brackets, this does not seem to cause any significant confusion.

3.0.1 Lemma. *The set $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ is the smallest subfield of L that contains K and the elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$.*

Proof. By construction, the set $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ is the image of the evaluation map from $K(x_1, x_2, \dots, x_n)$ to L sending x_j to α_j for all $1 \leqslant j \leqslant n$. It follows that $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ is a subfield of L because the image of a unit is also a unit; see MATH 210.

Suppose that the subfield $K' \subseteq L$ contains the underlying field K and the elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$. Since K' is closed under both addition and multiplication, we have $f(\alpha_1, \alpha_2, \dots, \alpha_n) \in K'$ for all $f \in K[x_1, x_2, \dots, x_n]$. In other words, there exists a ring extension $K[\alpha_1, \alpha_2, \dots, \alpha_n] \subset K'$. The universal property for fraction fields establishes that $K(\alpha_1, \alpha_2, \dots, \alpha_n) \subset K'$. □

The canonical injection η from $K[x_1, x_2, \dots, x_n]$ to $K(x_1, x_2, \dots, x_n)$ sends x_j to $x_j/1$. The universal property of fraction fields asserts that, for any ring homomorphism $\psi\colon K[x_1, x_2, \dots, x_n] \to L$ such the image of any nonzero element is a unit, there exists a unique ring homomorphism $\widehat{\psi}$ from $K(x_1, x_2, \dots, x_n)$ to L such that $\psi = \widehat{\psi} \circ \eta$.

3.0.2 Remark. Since $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ is a subfield of L containing K, we have a chain $K \subset K(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq L$ of field extensions. We say that the field $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ is obtained from K by *adjoining* the elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$.

3.0.3 Problem. Show that $x^4 - 2 \in \mathbb{Q}[x]$ splits completely over the field $L := \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \mathrm{i}\sqrt[4]{2}, -\mathrm{i}\sqrt[4]{2})$ and that $L = \mathbb{Q}(\mathrm{i}, \sqrt[4]{2})$.

Solution. Over $\mathbb{C}$, we have

$$\begin{aligned} x^4 - 2 &= (x^2 - \sqrt{2})(x^2 + \sqrt{2}) \\ &= (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \mathrm{i}\sqrt[4]{2})(x + \mathrm{i}\sqrt[4]{2}). \end{aligned}$$

It follows that $L := \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \mathrm{i}\sqrt[4]{2}, -\mathrm{i}\sqrt[4]{2})$ is the smallest field over which $x^4 - 2$ splits completely.

We have $L \subseteq K := \mathbb{Q}(\mathrm{i}, \sqrt[4]{2})$ because the field K contains $\mathbb{Q}$, and the elements $\pm\sqrt[4]{2}$ and $\pm\mathrm{i}\sqrt[4]{2}$. Since L contains both $\mathbb{Q}$ and $\sqrt[4]{2}$, and

$$\mathrm{i} = \frac{\mathrm{i}\sqrt[4]{2}}{\sqrt[4]{2}} \in L,$$

we conclude that $K \subseteq L$ and $L = K$. □

3.0.4 Corollary. *For every field extension $K \subseteq L$ and all field elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$, we have*

$$K(\alpha_1, \alpha_2, \dots, \alpha_n) = (K(\alpha_1, \alpha_2, \dots, \alpha_r))(\alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$$

for all $1 \leqslant r < n$.

This corollary implies that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This incremental perspective can be very useful.

Proof. The field on the right is constructed by first adjoining the elements $\alpha_1, \alpha_2, \dots, \alpha_r \in L$ to K to produce $K(\alpha_1, \alpha_2, \dots, \alpha_r)$ and then adjoining $\alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n \in L$ to the field $K(\alpha_1, \alpha_2, \dots, \alpha_r)$. Since this field contains K and the elements $\alpha_1, \alpha_2, \dots, \alpha_n$, Lemma 3.0.1 gives $K(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq (K(\alpha_1, \alpha_2, \dots, \alpha_r))(\alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n)$. Conversely, the field $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ contains the underlying field K and the elements $\alpha_1, \alpha_2, \dots, \alpha_r \in L$, so Lemma 3.0.1 shows that

$$K(\alpha_1, \alpha_2, \dots, \alpha_r) \subseteq K(\alpha_1, \alpha_2, \dots, \alpha_n)\,.$$

Since the field $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ contains $K(\alpha_1, \alpha_2, \dots, \alpha_r)$ and the elements $\alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n \in L$, Lemma 3.0.1 also shows that

$$(K(\alpha_1, \alpha_2, \dots, \alpha_r))(\alpha_{r+1}, \alpha_{r+2}, \dots, \alpha_n) \subseteq K(\alpha_1, \alpha_2, \dots, \alpha_n)\,. \qquad \square$$

3.0.5 Proposition. *Let $K \subseteq L$ be a field extension. For all $\alpha \in L$, the element α is algebraic over K if and only if $K[\alpha] = K(\alpha)$.*

Proof. When $\alpha \in L$ is algebraic over K, Lemma 2.2.7 establishes that $K[\alpha] \cong K[x] \big/ \langle p \rangle$ where $p \in K[x]$ is the minimal polynomial of α. Knowing that minimal polynomials are irreducible, it follows that $K[\alpha]$ is a field. Since $K(\alpha)$ is the smallest subfield of L containing K and α, we deduce that $K(\alpha) = K[\alpha]$. The opposite inclusion always holds, so $K(\alpha) = K[\alpha]$ with $\alpha \in L$ is algebraic over K.

For the other implication, suppose that $K[\alpha] = K(\alpha)$. We may assume that $\alpha \neq 0$ because 0 is obviously algebraic over K. The membership $1/\alpha \in K(\alpha) = K[\alpha]$ implies that

$$\frac{1}{\alpha} = a_0 + a_1\alpha + \cdots + a_m\alpha^m\,,$$

for some $a_0, a_1, \dots, a_m \in K$. Hence, we obtain

$$0 = -1 + a_0\alpha + a_1\alpha^2 + \cdots + a_m\alpha^{m+1}\,,$$

proving that α is algebraic over K. $\square$

3.0.6 Corollary. *Let $K \subseteq L$ be an extension. When $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ are algebraic over K, we have $K[\alpha_1, \alpha_2, \dots, \alpha_n] = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.*

Proof. It suffices to prove that the subring $K[\alpha_1, \alpha_2, \dots, \alpha_n]$ is a field. We proceed by induction on n. The base case $n = 1$ is precisely Proposition 3.0.5. Suppose that $n > 1$. The induction hypothesis asserts that $K[\alpha_1, \alpha_2, \dots, \alpha_{n-1}] = K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$. Since $\alpha_n \in L$ is algebraic over K, there exists a nonconstant $f \in K[x]$ such that $f(\alpha_n) = 0$. Regarding f as having coefficients in $K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$, we see that α_n is algebraic over $K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$. Proposition 3.0.5 gives $K(\alpha_1, \alpha_2, \dots, \alpha_{n-1})[\alpha_n] = (K(\alpha_1, \alpha_2, \dots, \alpha_{n-1}))(\alpha_n)$ and Corollary 3.0.4 gives $(K(\alpha_1, \alpha_2, \dots, \alpha_{n-1}))(\alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. $\square$

3.0.7 Remark. Since $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, every element in the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a polynomial in $\sqrt{2}, \sqrt{3}$ with coefficients in $\mathbb{Q}$. The equations

$$\sqrt{2}^{2k} = 2^k\,, \quad \sqrt{2}^{2k+1} = 2^k\sqrt{2}\,, \quad \sqrt{3}^{2k} = 3^k\,, \quad \sqrt{3}^{2k+1} = 3^k\sqrt{3}\,,$$

imply that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$.

3.1 Irreducible Polynomials

How can we determine if a given polynomial is irreducible? Since minimal polynomials are always irreducible, irreducibility plays a prominent role in field theory.

To get an idea of how factoring is done, we describe an algorithm for deciding whether $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.

3.1.0 Corollary. *For any reducible $f \in \mathbb{Z}[x]$ having positive degree, there exists $g, h \in \mathbb{Z}[x]$ such that $f = gh$ where $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$.*

Comment on proof. See MATH 210. □

To determine the irreducibility of a given polynomial $f \in \mathbb{Z}[x]$, set $n := \deg(f) > 0$. Observe that, if $f(j) = 0$ for some $0 \leqslant j \leqslant n-1$, then $x - j$ is a factor of f and we know that f is reducible. Thus, we may assume that $f(0), f(1), \dots, f(n-1)$ are nonzero. Create a set of polynomials as follows:

Fix an integer $0 < d < n$.
Fix divisors $a_0, a_1, \dots, a_d \in \mathbb{Z}$ of $f(0), f(1), \dots, f(d) \in \mathbb{Z}$.
Use the Lagrange interpolation formula to construct $g \in \mathbb{Q}[x]$ such that $\deg(g) \leqslant d$ and $g(j) = a_j$ for all $0 \leqslant j \leqslant d$.
Accept g if $\deg(g) = d$ and $g \in \mathbb{Z}[x]$; otherwise reject it.

Doing this for all $0 < d < n$ and all divisors of $f(0), f(1), \dots, f(d)$ defines a set of polynomials $g \in \mathbb{Z}[x]$.

3.1.1 Proposition. *This set of polynomials $g \in \mathbb{Z}[x]$ is finite. Moreover, the polynomial f is irreducible over $\mathbb{Q}$ if and only if it is not divisible by any of the polynomials in this set.*

Proof. Since we may assume that $f(0), f(1), \dots, f(d)$ are nonzero, each $f(j)$ has only finitely many divisors. Hence, there are only finitely many choices for $a_0, a_1, \dots, a_d \in \mathbb{Z}$. Since g is uniquely determined by the a_j, there are only finitely many such g's.

We claim that f is reducible if and only if it is divisible by one of theses polynomials. One direction is obvious. For the other direction, suppose that f is reducible. By Corollary 3.1.0, there exists $g, h \in \mathbb{Z}[x]$ such that $f = g\,h$ and $\deg(g) = d$ where $0 < d < n$. Set $a_i := g(i)$ for $0 \leqslant j \leqslant d$. Observe that a_j divides $f(j)$ because $f(j) = g(j)\,h(j)$. The Lagrange interpolation formula produces $\widetilde{g} \in \mathbb{Q}[x]$ of degree at most d such that $\widetilde{g}(j) = a_j$ for all $0 \leqslant i \leqslant d$. Since $g - \widetilde{g}$ has degree at most d and vanishes at $d+1$ points, it must by the zero polynomial. Hence, $g = \widetilde{g}$ is on our list. □

From a computational point of view, this algorithm is dreadful. The first polynomial time algorithm for factoring rational polynomials appears in A.K. Lenstra, H.W. Lenstra, L. Lovász, László, *Factoring polynomials with rational coefficients*, Math. Ann., **261** (1982) 515–534.

3.1.2 Eisenstein Criterion. *Let n be a positive integer and consider the polynomial $f = a_0x^n + a_1x^{n-1} + \cdots a_n \in \mathbb{Z}[x]$. Whenever there exists a prime $p \in \mathbb{Z}$ such that p does not divide a_0, p divides $a_1, a_2, \dots, a_n$, and p^2 does not divide a_n, the polynomial f is irreducible over $\mathbb{Q}$.*

Comment on proof. See MATH 210. □

Theodor Schönemann first published a version of this criterion in 1846. Gotthold Eisenstein published a somewhat different version in the same journal in 1850.

3.1.3 Problem. For all integers $n \geqslant 2$ and any prime p, prove that $x^n + px + p$ is irreducible over $\mathbb{Q}$.

Solution. For the prime p, the Eisenstein criterion implies that f is irreducible over $\mathbb{Q}$. □

3.1.4 Problem. For every prime integer p, prove that

$$f := x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Q}[x]$.

Solution. Since $(x-1)f(x) = x^p - 1$, the ring isomorphism given by $x \mapsto y + 1$ yields

$$yf(y+1) = (y+1)^p - 1 = y^p + \tbinom{p}{1} y^{p-1} + \tbinom{p}{2} y^{p-2} + \cdots + \tbinom{p}{p-1} y\,.$$

We have $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$. When $i < p$, the prime integer p is not a factor of $i!$, so $i!$ divides the product $(p-1)(p-2)\cdots(p-i+1)$ which implies that $\binom{p}{i}$ is divisible by p. Dividing the expansion of $yf(y+1)$ by y shows that $f(y+1)$ satisfies the hypothesis of the Eisenstein criterion. Therefore, the polynomial

$$y^{p-1} + \tbinom{p}{1} y^{p-2} + \tbinom{p}{2} y^{p-3} + \cdots + \tbinom{p}{p-1}$$

is irreducible. We conclude that f is irreducible. □

3.1.5 Proposition. *Let K be a field. For every prime integer $p \in \mathbb{Z}$, the polynomial $f = x^p - a \in K[x]$ is irreducible over K if and only if f has no roots in K.*

Proof. Suppose that f has a root $\alpha \in K$. It follows that $x - \alpha \in K[x]$ is a factor, so f is reducible.

Suppose that f is reducible. By Theorem 2.0.6, there exists a field extension $K \subseteq L$ over which f splits completely:

$$f = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_p)$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_p \in L$. If $\alpha_1 = 0$, then f has a root in K, so we may assume that $\alpha_1 \neq 0$. For all $1 \leqslant j \leqslant p$, set $\zeta_j = \alpha_j/\alpha_1$. Since $\alpha_j^p = a$, we see that

$$\zeta_j^p = \frac{\alpha_j^p}{\alpha_1^p} = \frac{a}{a} = 1\,.$$

It follows that $\alpha_j = \zeta_j \alpha_1$ where ζ_j is a pth root of unity. Hence, we obtain $f = (x - \zeta_1\alpha_1)(x - \zeta_2\alpha_1)\cdots(x - \zeta_p\alpha_1)$.

Now, suppose that $f = gh$ where $g, h \in K[x]$, $r := \deg(g) < p$, and $s := \deg(h) < p$. We may assume that both g and h are monic. Since $K[x]$ is a unique factorization domain, the polynomial g must be a product of r of the linear factors. After relabeling if necessary, we may assume that $g = (x - \zeta_1\alpha_1)(x - \zeta_2\alpha_1)\cdots(x - \zeta_r\alpha_1)$. Since the constant term of g lies in K, this implies that $\zeta\alpha_1^r \in K$ where $\zeta = \zeta_1\zeta_2\cdots\zeta_r$. Notice that $\zeta^p = 1$. Since $0 < r < p$ and p is prime, there exists $k, \ell \in \mathbb{Z}$ such that $kr + ellp = 1$. It follows that

$$\zeta^k\alpha_1 = \zeta^k\alpha_1^{kr+\ell p} = (\zeta\alpha_1^r)^k(\alpha_1^p)^\ell \in K\,.$$

Hence, we see that $(\zeta^k\alpha_1)^p = (\zeta^p)^k\alpha_1^p = a$ which shows that $\zeta^k\alpha_1$ is a root of $f = x^p - a$ lying in K. □

Let K be a subfield of $\mathbb{R}$ and let p be an odd prime. For all $a \in K$, define $\sqrt[p]{a}$ to be the real pth root of a. Since p is odd, $\sqrt[p]{a}$ is the only real pth root of a. Proposition 3.1.5 establishes that $x^p - a$ is irreducible over K if and only if $\sqrt[p]{a} \notin K$.