Galois Theory

This chapter discusses the interrelation between extension fields and certain groups associated to them, called *Galois groups*. This topic is called *Galois theory* today; it was originally called *Theory of Equations*. Informally, we say that a polynomial is *solvable by radicals* if there is a generalization of the quadratic formula that gives its roots. Galois theory will enable us to prove the theorem of Abel–Ruffini (there are polynomials of degree 5 that are not solvable by radicals) as well as Galois's theorem describing all those polynomials (over a field of characteristic 0) which are solvable by radicals. Another corollary of this theory is a proof of the Fundamental Theorem of Algebra.

Insolvability of the Quintic

Kronecker's Theorem (Theorem A-3.90) says, for each monic $f(x) \in k[x]$ (where k is a field), that there is an extension field K/k and (not necessarily distinct) roots $z_1, \ldots, z_n \in K$ with

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - z_1)\cdots(x - z_n).$$

In Example A-3.92, we displayed the coefficients of f in terms of its roots:

$$\text{(8)} \qquad \begin{cases} a_{n-1} = -\sum_i z_i, \\ a_{n-2} = \sum_{i<j} z_i z_j, \\ a_{n-3} = -\sum_{i<j<k} z_i z_j z_k, \\ \quad \vdots \\ a_0 = (-1)^n z_1 z_2 \cdots z_n. \end{cases}$$

Recall that the ***elementary symmetric functions*** of n variables are the polynomials, for $j = 1, \dots, n$,

$$e_j(y_1, \dots, y_n) = \sum_{i_1 < \cdots < i_j} y_{i_1} \cdots y_{i_j}.$$

Eqs. (8) show that if $z_1, \dots, z_n$ are the roots of $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then

$$e_j(z_1, \dots, z_n) = (-1)^j a_{n-j}.$$

In particular, $-a_{n-1}$ is the sum of the roots of f and $(-1)^n a_0$ is the product of the roots.

Given the coefficients $a_0, \dots, a_{n-1}$ of f, can we find its roots? That is, can we solve the system (8) of n equations in n unknowns? If $n = 2$, the answer is yes: the quadratic formula works. If $n = 3$ or 4, the answer is still yes, for the cubic and quartic formulas work. But if $n \geq 5$, we shall see that no *analogous* solution exists. We do not say that no solution of system (8) exists if $n \geq 5$. Indeed, there are ways of finding the roots of a quintic polynomial if we do not limit ourselves to formulas involving only field operations and extraction of roots. We can find the roots by *Newton's method*: If r is a real root of a polynomial $f(x)$ and x_0 is a "good" approximation to r, then $r = \lim_{n\to\infty} x_n$, where x_n is defined recursively by $x_{n+1} = x_n - f(x_n)/f'(x_n)$ for all $n \geq 0$. There is a method of Hermite finding roots of quintics using elliptic modular functions, and there are methods for finding the roots of many polynomials of higher degree using hypergeometric functions (see King [**62**]).

Abel proved in 1824 that if $n \geq 5$, then there are polynomials of degree n that are not solvable by radicals (as we said earlier, Ruffini proved the same result in 1799, but his proof was very long, it had a gap, and it was not accepted by his contemporaries). The key observation is that symmetry is present.

Definition. Let E/k be an extension field. An ***automorphism*** of E is an isomorphism $\sigma\colon E \to E$; an automorphism σ of E ***fixes*** k if $\sigma(a) = a$ for every $a \in k$.

Note that an extension field E/k is a vector space over k and, if $\sigma\colon E \to E$ fixes k, then σ is a k-linear transformation ($\sigma(ae) = \sigma(a)\sigma(e) = a\sigma(e)$ for all $a \in k$ and $e \in E$). For example, a splitting field of $f(x) = x^2 + 1$ over $\mathbb{Q}$ is $E = \mathbb{Q}(i)$, and complex conjugation $\sigma\colon a \mapsto \overline{a}$ is an example of an automorphism of E fixing $\mathbb{Q}$.

Proposition A-5.1. *Let k be a field, let*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in k[x],$$

and let $E = k(z_1, \dots, z_n)$ be a splitting field of f over k. If $\sigma\colon E \to E$ is an automorphism fixing k, then σ permutes the set of roots $\{z_1, \dots, z_n\}$ of f.

Proof. If z is a root of f, then

$$0 = f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0.$$

Applying σ to this equation gives

$$\begin{aligned} 0 &= \sigma(z)^n + \sigma(a_{n-1})\sigma(z)^{n-1} + \cdots + \sigma(a_1)\sigma(z) + \sigma(a_0) \\ &= \sigma(z)^n + a_{n-1}\sigma(z)^{n-1} + \cdots + a_1\sigma(z) + a_0 \\ &= f(\sigma(z)), \end{aligned}$$

because σ fixes k. Therefore, $\sigma(z)$ is a root of f. Thus, if Ω is the set of all the roots, then $\sigma|\Omega\colon \Omega \to \Omega$, where $\sigma|\Omega$ is the restriction. But $\sigma|\Omega$ is injective (because σ is), so that $\sigma|\Omega$ is a permutation of Ω, by the Pigeonhole Principle. •

We now associate a group to any polynomial $f(x)$.

Definition. The ***Galois group*** of an extension field E/k, denoted by

$$\mathrm{Gal}(E/k),$$

is the set of all those automorphisms of E that fix k.

If $f(x) \in k[x]$ and $E = k(z_1, \ldots, z_n)$ is a splitting field of f over k, then the ***Galois group*** of f over k is defined to be $\mathrm{Gal}(E/k)$.

It is easy to check that $\mathrm{Gal}(E/k)$ is a group with operation composition of functions. Note that the Galois group $\mathrm{Gal}(E/k)$ of a polynomial f is independent of the choice of splitting field E, for any two splitting fields of f over k are isomorphic.

Given a polynomial f, Galois's definition of its Galois group was given in terms of certain permutations of its roots (see [**115**], pp. 295–302). The simpler definition above is due to E. Artin, around 1930. Both definitions yields isomorphic groups.

Lemma A-5.2. *Let $\sigma \in \mathrm{Gal}(E/k)$, where $E = k(z_1, \ldots, z_n)$. If $\sigma(z_i) = z_i$ for all i, then σ is the identity 1_E.*

Proof. We prove this lemma by induction on $n \geq 1$. If $n = 1$, then each $u \in E$ has the form $u = f(z_1)/g(z_1)$, where $f(x)$, $g(x) \in k[x]$ and $g(z_1) \neq 0$. But σ fixes z_1 as well as the coefficients of f and of g, so that σ fixes all $u \in E$. For the inductive step, write $K = k(z_1, \ldots, z_{n-1})$, and note that $E = K(z_n)$ (for $K(z_n)$ is the smallest subfield containing k and $z_1, \ldots, z_{n-1}, z_n$). The inductive step is now just a repetition of the base step with k replaced by K. •

Theorem A-5.3. *If $f(x) \in k[x]$ has degree n, then its Galois group $\mathrm{Gal}(E/k)$ is isomorphic to a subgroup of S_n.*

Proof. Let $X = \{z_1, \ldots, z_n\}$ be the set of roots of f. If $\sigma \in \mathrm{Gal}(E/k)$, then Proposition A-5.1 shows that its restriction $\sigma|X$ is a permutation of X. Define $\varphi\colon \mathrm{Gal}(E/k) \to S_X$ by $\varphi\colon \sigma \mapsto \sigma|X$. To see that φ is a homomorphism, note that both $\varphi(\sigma\tau)$ and $\varphi(\sigma)\varphi(\tau)$ are functions $X \to X$ that agree on each $z_i \in X$: $\varphi(\sigma\tau)\colon z_i \mapsto (\sigma\tau)(z_i)$, while $\varphi(\sigma)\varphi(\tau)\colon z_i \mapsto \sigma(\tau(z_i))$, and these are the same.

The image of φ is a subgroup of $S_X \cong S_n$. The kernel of φ is the set of all $\sigma \in \mathrm{Gal}(E/k)$ with $\sigma|X = 1_X$; that is, σ fixes each of the roots z_i. As σ also fixes k, by the definition of Galois group, and Lemma A-5.2 gives $\ker\varphi = \{1\}$. Therefore, φ is injective. •

We illustrate this result. If $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, then complex conjugation σ is an automorphism of its splitting field $\mathbb{Q}(i)$ (for σ interchanges the roots i and $-i$); since σ fixes $\mathbb{Q}$, we have $\sigma \in G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Now G is a subgroup of the symmetric group S_2, which has order 2; it follows that $G = \langle \sigma \rangle \cong \mathbb{Z}_2$. The reader should regard the elements of any Galois group $\mathrm{Gal}(E/k)$ as generalizations of complex conjugation.

In order to compute the order of the Galois group, we must first discuss *separability*.

Lemma A-5.4. *If k is a field of characteristic 0, then every irreducible polynomial $p(x) \in k[x]$ has no repeated roots.*

Proof. Let $f(x) \in k[x]$ be a (not necessarily irreducible) polynomial. In Exercise A-3.64 on page 74, we saw that f has no repeated roots if and only if $\gcd(f, f') = 1$, where f' is the derivative of f.

Now consider $p(x)$; we may assume that p is monic of degree $d \geq 1$. The highest coefficient dx^{d-1} of the derivative p' is nonzero, because k has characteristic 0, and so $p' \neq 0$. Since p is irreducible, its only divisors are constants and associates; as p' has smaller degree, it is not an associate of p, and so $\gcd(p, p') = 1$. •

Definition. An *irreducible* polynomial $p(x)$ is ***separable*** if it has no repeated roots. An arbitrary polynomial $f(x)$ is ***separable*** if each of its irreducible factors has no repeated roots; otherwise, it is ***inseparable***.

Recall Theorem A-3.87(i): If E/k is an extension field and $\alpha \in E$ is algebraic over k, then there is a unique monic irreducible polynomial $\mathrm{irr}(\alpha, k) \in k[x]$, called its *minimal polynomial*, having α as a root.

Definition. Let E/k be an algebraic extension. An element $\alpha \in E$ is ***separable*** if either α is transcendental over k or α is algebraic over k and its minimal polynomial $\mathrm{irr}(\alpha, k)$ is separable; that is, $\mathrm{irr}(\alpha, k)$ has no repeated roots.

An extension field E/k is ***separable*** if each of its elements is separable; we say that E/k is ***inseparable*** if it is not separable.

In Proposition A-5.47, we shall see that a splitting field of a separable polynomial is a separable extension.

Lemma A-5.4 shows that every extension field E/k is separable if k has characteristic 0. If E is a finite field with p^n elements, then Lagrange's Theorem (for the multiplicative group $E^\times$) shows that every element of E is a root of $g(x) = x^{p^n} - x$. We saw, in the proof of Theorem A-3.95 (the existence of finite fields with p^n elements), that g has no repeated roots. It follows that if $k \subseteq E$, then E/k is separable, for if $\alpha \in E$, then $\mathrm{irr}(\alpha, k)$ is a divisor of g.

Example A-5.5. Here is an example of an inseparable extension. Let $k = \mathbb{F}_p(t) = \mathrm{Frac}(\mathbb{F}_p[t])$, and let $E = k(\alpha)$, where α is a root of $f(x) = x^p - t$; that is, $\alpha^p = t$. In $E[x]$, we have

$$f(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p.$$

If we show that $\alpha \notin k$, then f is irreducible (by Proposition A-3.94), hence $f = \operatorname{irr}(\alpha, k)$ is an inseparable polynomial, and so E/k is inseparable. If, on the contrary, $\alpha \in k$, then there are $g(t), h(t) \in \mathbb{F}_p[t]$ with $\alpha = g/h$. Hence, $g = \alpha h$ and $g^p = \alpha^p h^p = th^p$, so that

$$\deg(g^p) = \deg(th^p) = 1 + \deg(h^p).$$

But $p \mid \deg(g^p)$ and $p \mid \deg(h^p)$, and this gives a contradiction. ◀

Example A-5.6. We now examine roots of unity in fields of different characteristics.

Let n be a positive integer. Theorem A-3.59 says that every finite subgroup of the multiplicative group of a field E is cyclic; hence, the group $\Gamma_n(E)$ of all the nth roots of unity in E is cyclic; any generator of this group, say, ω, is called a *primitive nth root of unity*. Let $f(x) = x^n - 1 \in k[x]$, where k is a field. What is the order of $\Gamma_n(\mathrm{E})$ if E/k is a splitting field of f? If the characteristic of k is 0, we know that f has n distinct roots (by Exercise A-3.64 on page 74, for $\gcd(f, f') = 1$). Thus, $|\Gamma_n(E)| = n$ and a primitive nth root of unity ω has order n. Since every extension field of characteristic 0 is separable, ω is a separable element.

Suppose the characteristic of k is a prime p. Write $n = p^e m$, where $\gcd(m, p) = 1$. If $g(x) = x^m - 1$, then $mx^{m-1} \neq 0$ (because $\gcd(m, p) = 1$) and $\gcd(g, g') = 1$; hence, g has no repeated roots, and E contains m distinct mth roots of unity. We claim that $|\Gamma_n(E)| = m$; that is, there are no other nth roots of unity in E. If β is an nth root of unity, then $1 = \beta^n = (\beta^m)^{p^e}$; that is, β^m is a root of $x^{p^e} - 1$. But $x^{p^e} - 1 = (x - 1)^{p^e}$, because k has characteristic p, so that $\beta^m = 1$. If ω is a primitive nth root of unity, then $\operatorname{irr}(\omega, k) \mid x^m - 1$. Hence, the m roots of $\operatorname{irr}(\omega, k)$ are distinct, and so ω is a separable element in this case as well. ◀

Separability of E/k allows us to find the order of $\operatorname{Gal}(E/k)$.

Theorem A-5.7. *Let $\varphi\colon k \to k'$ be an isomorphism of fields, and let $\varphi_*\colon k[x] \to k'[x]$ be the ring isomorphism of* Corollary A-3.27:

$$\varphi_*\colon g(x) = a_0 + \cdots + a_n x^n \mapsto g_*(x) = \varphi(a_0) + \cdots + \varphi(a_n)x^n.$$

(i) *Let $f(x) \in k[x]$ be separable. If f has splitting field E/k and $f_*(x) = \varphi_*(f) \in k'[x]$ has splitting field E^*/k', then there are exactly $[E : k]$ isomorphisms $\Phi\colon E \to E^*$ that extend φ:*

$$\begin{array}{ccc} E & \overset{\Phi}{\rightarrowtail} & E^* \\ \big| & & \big| \\ k & \xrightarrow[\varphi]{} & k' \,. \end{array}$$

(ii) *If E/k is a splitting field of a separable polynomial f, then*

$$|\operatorname{Gal}(E/k)| = [E : k].$$

Proof.

(i) The proof, by induction on $[E : k]$, modifies that of Lemma A-3.98. The base step $[E : k] = 1$ gives $E = k$, and there is only one extension Φ of φ, namely, φ itself. If $[E : k] > 1$, let $f(x) = p(x)g(x)$, where p is an irreducible factor of largest degree, say, d. We may assume that $d > 1$; otherwise f splits over k and $[E : k] = 1$. Choose a root α of p (note that $\alpha \in E$ because E is a splitting field of $f = pg$). If $\widetilde{\varphi}\colon k(\alpha) \to E^*$ is any extension of φ, then $\varphi(\alpha)$ is a root α^* of $p_*(x)$, by Proposition A-5.1; since f_* is separable, p_* has exactly d roots $\alpha^* \in E^*$. By Lemma A-5.2 and Theorem A-3.87(ii), there are exactly d isomorphisms $\widehat{\varphi} : k(\alpha) \to k'(\alpha^*)$ extending φ, one for each α^*. Now E is also a splitting field of f over $k(\alpha)$, because adjoining all the roots of f to $k(\alpha)$ still produces E; similarly, E^* is a splitting field of $f_*(x)$ over $k'(\alpha^*)$. Now $[E : k(\alpha)] < [E : k]$, because $[E : k(\alpha)] = [E : k]/d$, so that induction shows that each of the d isomorphisms $\widehat{\varphi}$ has exactly $[E : k]/d$ extensions $\Phi\colon E \to E^*$. Thus, we have constructed $[E : k]$ isomorphisms extending φ. But there are no others, because every τ extending φ has $\tau|k(\alpha) = \widehat{\varphi}$ for some $\widehat{\varphi}\colon k(\alpha) \to k'(\alpha^*)$.

(ii) In part (i), take $k = k'$, $E = E^*$, and $\varphi = 1_k$. •

Example A-5.8. The separability hypothesis in Theorem A-5.7(ii) is necessary. In Example A-5.5, we saw that if $k = \mathbb{F}_p(t)$ and α is a root of $x^p - t$, then $E = k(\alpha)$ is an inseparable extension. Moreover, $x^p - t = (x - \alpha)^p$, so that α is the only root of this polynomial. Hence, if $\sigma \in \mathrm{Gal}(E/k)$, then Proposition A-5.1 shows that $\sigma(\alpha) = \alpha$. Therefore, $\mathrm{Gal}(E/k) = \{1\}$, by Lemma A-5.2, and so $|\,\mathrm{Gal}(E/k)| = 1 < p = [E : k]$ in this case. ◀

Corollary A-5.9. *Let E/k be a splitting field of a separable polynomial $f(x) \in k[x]$ of degree n. If f is irreducible, then $n \mid |\,\mathrm{Gal}(E/k)|$.*

Proof. By Theorem A-5.7(ii), $|\,\mathrm{Gal}(E/k)| = [E : k]$. Let $\alpha \in E$ be a root of f. Since f is irreducible, $[k(\alpha) : k] = n$, by Proposition A-3.84(v), and

$$[E : k] = [E : k(\alpha)][k(\alpha) : k] = n[E : k(\alpha)]. \quad \bullet$$

We can now give an example showing that the irreducibility criterion involving reducing the coefficients of a polynomial in $\mathbb{Z}[x]$ mod p may not work.

Proposition A-5.10. *The polynomial $f(x) = x^4 + 1$ is irreducible in $\mathbb{Q}[x]$. yet it factors in $\mathbb{F}_p[x]$ for every prime p.*

Proof. We saw, in Example A-3.103 that f is irreducible in $\mathbb{Q}[x]$.

We show, for all primes p, that $x^4 + 1$ factors in $\mathbb{F}_p[x]$. If $p = 2$, then $x^4 + 1 = (x + 1)^4$, and so we may assume that p is an odd prime. It is easy to check that every square in $\mathbb{Z}$ is congruent to 0, 1, or 4 mod 8 (see Example A-2.24); since p is odd, we must have $p^2 \equiv 1 \bmod 8$, and so[1] $|(\mathbb{F}_{p^2})^\times| = p^2 - 1$ is divisible by 8. By Theorem A-3.59, $(\mathbb{F}_{p^2})^\times$ is a cyclic group, and so it has a (cyclic) subgroup of

[1]Recall that if k is a field, then $k^\times$ denotes the multiplicative group of its nonzero elements.

order 8, by Lemma A-4.89. It follows that $\mathbb{F}_{p^2}$ contains all the 8th roots of unity; in particular, $\mathbb{F}_{p^2}$ contains all the roots of x^4+1, for $x^8-1=(x^4+1)(x^4-1)$). Hence, the splitting field E_p of x^4+1 over $\mathbb{F}_p$ is $\mathbb{F}_{p^2}$, because there is no intermediate field, and $\mathrm{Gal}(E_p/\mathbb{F}_p) = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. But $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, so that $|\mathrm{Gal}(E_p/\mathbb{F}_p)| = 2$. Now x^4+1 is a separable polynomial, by Example A-5.6. Were x^4+1 irreducible in $\mathbb{F}_p[x]$, then Corollary A-5.9 would give $4 \mid |\mathrm{Gal}(E_p/\mathbb{F}_p)| = 2$, a contradiction. Therefore, x^4+1 factors in $\mathbb{F}_p[x]$ for every prime p. •

Here are some computations of Galois groups of specific polynomials in $\mathbb{Q}[x]$.

Example A-5.11.

(i) Let $f(x) = x^3 - 1 \in \mathbb{Q}[x]$. Now $f(x) = (x-1)(x^2+x+1)$, where x^2+x+1 is irreducible (the quadratic formula shows that its roots ω and $\overline{\omega}$ do not lie in $\mathbb{Q}$). The splitting field of f is $\mathbb{Q}(\omega)$, for $\omega^2 = \overline{\omega}$, and so $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Therefore, $|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = 2$, by Theorem A-5.7(ii), and it is cyclic of order 2. Its nontrivial element is complex conjugation.

(ii) Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Now f is irreducible with roots $\pm\sqrt{2}$, so that $E = \mathbb{Q}(\sqrt{2})$ is a splitting field. By Theorem A-5.7(ii), $|\mathrm{Gal}(E/\mathbb{Q})| = 2$. Now every element of E has a unique expression of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$ (Proposition A-3.84(v)); it is easily seen that $\sigma\colon E \to E$, defined by $\sigma\colon a + b\sqrt{2} \mapsto a - b\sqrt{2}$, is an automorphism of E fixing $\mathbb{Q}$. Therefore, $\mathrm{Gal}(E/\mathbb{Q}) = \langle\sigma\rangle$, where σ interchanges $\sqrt{2}$ and $-\sqrt{2}$.

(iii) Let $g(x) = x^3 - 2 \in \mathbb{Q}[x]$. The roots of g are β, $\omega\beta$, and $\omega^2\beta$, where $\beta = \sqrt[3]{2}$, the real cube root of 2, and ω is a primitive cube root of unity. It is easy to see that the splitting field of g is $E = \mathbb{Q}(\beta, \omega)$. Note that

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 3[E : \mathbb{Q}(\beta)],$$

for g is irreducible over $\mathbb{Q}$ (it is a cubic having no rational roots). Now $E \neq \mathbb{Q}(\beta)$, for every element in $\mathbb{Q}(\beta)$ is real, while the complex number ω is not real. Therefore, $[E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})| > 3$. On the other hand, we know that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to a subgroup of S_3, and so we must have $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

(iv) We examined $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ in Example A-3.89, when we saw that f is irreducible; in fact, $f = \mathrm{irr}(\beta, \mathbb{Q})$, where $\beta = \sqrt{2} + \sqrt{3}$. If $E = \mathbb{Q}(\beta)$, then $[E : \mathbb{Q}] = 4$; moreover, E is a splitting field of f, where the other roots of f are $-\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, and $\sqrt{2} - \sqrt{3}$. It follows from Theorem A-5.7(ii) that if $G = \mathrm{Gal}(E/\mathbb{Q})$, then $|G| = 4$; hence, either $G \cong \mathbb{Z}_4$ or $G \cong \mathbf{V}$.

We also saw, in Example A-3.89, that E contains $\sqrt{2}$ and $\sqrt{3}$. If σ is an automorphism of E fixing $\mathbb{Q}$, then $\sigma(\sqrt{2}) = u\sqrt{2}$, where $u = \pm 1$, because $\sigma(\sqrt{2})^2 = 2$. Therefore, $\sigma^2(\sqrt{2}) = \sigma(u\sqrt{2}) = u\sigma(\sqrt{2}) = u^2\sqrt{2} = \sqrt{2}$; similarly, $\sigma^2(\sqrt{3}) = \sqrt{3}$. If α is a root of f, then $\alpha = u\sqrt{2} + v\sqrt{3}$, where $u, v = \pm 1$. Hence,

$$\sigma^2(\alpha) = u\sigma^2(\sqrt{2}) + v\sigma^2(\sqrt{3}) = u\sqrt{2} + v\sqrt{3} = \alpha.$$

Lemma A-5.2 gives $\sigma^2 = 1_E$ for all $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, and so $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbf{V}$.

Here is another way to compute $G = \mathrm{Gal}(E/\mathbb{Q})$. We saw in Example A-3.89 that $E = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ is also a splitting field of $g(x) = (x^2-2)(x^2-3)$ over $\mathbb{Q}$. By Proposition A-3.87(ii), there is an automorphism $\varphi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ taking $\sqrt{2} \mapsto \pm\sqrt{2}$. But $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, as we noted in Example A-3.89, so that x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$. Lemma A-3.98 shows that φ extends to an automorphism $\Phi\colon E \to E$; of course, $\Phi \in \mathrm{Gal}(E/\mathbb{Q})$. There are two possibilities: $\Phi(\sqrt{3}) = \pm\sqrt{3}$. Indeed, it is now easy to see that the elements of $\mathrm{Gal}(E/\mathbb{Q})$ correspond to the four-group, consisting of the identity and the permutations (in cycle notation)

$$\big(\sqrt{2},\ -\sqrt{2}\big)\big(\sqrt{3},\ \sqrt{3}\big),\ \ \big(\sqrt{2},\ -\sqrt{2}\big)\big(\sqrt{3},\ -\sqrt{3}\big),\ \ \big(\sqrt{2},\ \sqrt{2}\big)\big(\sqrt{3},\ -\sqrt{3}\big). \quad \blacktriangleleft$$

Here is a pair of more general computations of Galois groups.

Proposition A-5.12. *If m is a positive integer, k is a field, and E is a splitting field of x^m-1 over k, then $\mathrm{Gal}(E/k)$ is abelian. In fact, $\mathrm{Gal}(E/k)$ is isomorphic to a subgroup of the (multiplicative) group of units $U(\mathbb{Z}_m) = \{[i] \in \mathbb{Z}_m : \gcd(i,m) = 1\}$.*

Proof. By Example A-3.93, $E = k(\omega)$, where ω is a primitive mth root of unity, and so $E = k(\omega)$. The group Γ_m of all roots of $x^m - 1$ in E is cyclic (with generator ω) and, if $\sigma \in \mathrm{Gal}(E/k)$, then its restriction to Γ_m is an automorphism of Γ_m. Hence, $\sigma(\omega) = \omega^i$ must also be a generator of Γ_m; that is, $\gcd(i,m) = 1$, by Theorem A-4.36(ii). It is easy to see that i is uniquely determined mod m, so that the function $\theta\colon \mathrm{Gal}(k(\omega)/k) \to U(\mathbb{Z}_m)$, given by $\theta(\sigma) = [i]$ if $\sigma(\omega) = \omega^i$, is well-defined. Now θ is a homomorphism, for if $\tau(\omega) = \omega^j$, then

$$\tau\sigma(\omega) = \tau(\omega^i) = (\omega^i)^j = \omega^{ij}.$$

Therefore, Lemma A-5.2 shows that θ is injective. •

Remark. We cannot conclude more from the last proposition, for Theorem B-3.15 on page 368 says that every finite abelian group is isomorphic to a subgroup of $U(\mathbb{Z}_m)$ for some integer m. However, if $m = p$ is prime, then $\mathrm{Gal}(E/k)$ is isomorphic to a subgroup of $U(\mathbb{Z}_p)$ which is a cyclic group of order $p-1$; hence, $\mathrm{Gal}(E/k)$ is a cyclic group whose order divides $p-1$. $\blacktriangleleft$

Theorem A-5.13. *If p is prime, then*

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n,$$

and a generator is the ***Frobenius automorphism***

$$\mathrm{Fr}\colon u \mapsto u^p.$$

Proof. Let $q = p^n$, and let $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Since $\mathbb{F}_q$ has characteristic p, we have $(a+b)^p = a^p + b^p$, and so the Frobenius Fr is a homomorphism of fields. As any homomorphism of fields, Fr is injective; as $\mathbb{F}_q$ is finite, Fr must be an automorphism, by the Pigeonhole Principle; that is, $\mathrm{Fr} \in G$ (Fr fixes $\mathbb{F}_p$, by Fermat's Theorem).

If $\pi \in \mathbb{F}_q$ is a primitive element, then $d(x) = \mathrm{irr}(\pi, \mathbb{F}_p)$ has degree n, by Corollary A-3.96, and so $|G| = n$, by Theorem A-5.7(ii). It suffices to prove that

the order j of Fr is not less than n. But if $\mathrm{Fr}^j = 1_{\mathbb{F}_q}$ for $j < n$, then $u^{p^j} = u$ for all of the $q = p^n$ elements $u \in \mathbb{F}_q$, giving too many roots of the polynomial $x^{p^j} - x$. •

The Galois group gives an irreducibility criterion.

Proposition A-5.14. *Let k be a field, let $f(x) \in k[x]$, and let E/k be a splitting field of $f(x)$. If f has no repeated roots, then f is irreducible if and only if* $\mathrm{Gal}(E/k)$ *acts* ***transitively*** *on the roots of f; that is, given any two roots α, β of f, there exists $\sigma \in \mathrm{Gal}(E/k)$ with $\sigma(\alpha) = \beta$.*

Proof. Assume that f is irreducible, and let $\alpha, \beta \in E$ be roots of f. By Theorem A-3.87(i), there is an isomorphism $\varphi : k(\alpha) \to k(\beta)$ with $\varphi(\alpha) = \beta$ and which fixes k. Lemma A-3.98 shows that φ extends to an automorphism Φ of E that fixes k; that is, $\Phi \in \mathrm{Gal}(E/k)$. Now $\Phi(\alpha) = \varphi(\alpha) = \beta$, and so $\mathrm{Gal}(E/k)$ acts transitively on the roots.

Conversely, assume that $\mathrm{Gal}(E/k)$ acts transitively on the roots of f. Let $f = p_1 \cdots p_t$ be a factorization into irreducibles in $k[x]$, where $t \geq 2$. Choose a root $\alpha \in E$ of p_1 and a root $\beta \in E$ of p_2; note that β is not a root of p_1, because f has no repeated roots. By hypothesis, there is $\sigma \in \mathrm{Gal}(E/k)$ with $\sigma(\alpha) = \beta$. Now σ permutes the roots of p_1, by Proposition A-5.1, contradicting β not being a root of p_1. Hence, $t = 1$ and f is irreducible. •

Classical Formulas and Solvability by Radicals

Here is our basic strategy. First, we will translate the classical formulas (giving the roots of polynomials of degree at most 4) into terms of subfields of a splitting field E over k. Second, this translation into the language of fields will further be translated into the language of groups: If there is a formula for the roots of a polynomial, then $\mathrm{Gal}(E/k)$ must be a *solvable* group (which we will soon define). Finally, polynomials of degree at least 5 can have Galois groups that are not solvable. The conclusion is that there are polynomials of degree 5 having no formula analogous to the classical formulas that gives their roots. Without further ado, here is the translation of the existence of a formula for the roots of a polynomial in terms of subfields of a splitting field.

Definition. A ***pure extension*** of ***type*** m is an extension field $k(u)/k$, where $u^m \in k$ for some $m \geq 1$.

An extension field K/k is a ***radical extension*** if there is a tower of intermediate fields

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = K$$

in which each K_{i+1}/K_i is a pure extension.

If $u^m = a \in k$, then $k(u)$ arises from k by adjoining an mth root of a. If $k \subseteq \mathbb{C}$, there are m different mth roots of a, namely, $u, \omega u, \omega^2 u, \ldots, \omega^{m-1} u$, where $\omega = e^{2\pi i/m}$ is a primitive mth root of unity. More generally, if k contains the mth roots of unity, then a pure extension $k(u)$ of type m (that is, $u^m = a \in k$) is a splitting field of $x^m - a$. Not every subfield k of $\mathbb{C}$ contains all the roots of unity;

for example, 1 and -1 are the only roots of unity in $\mathbb{Q}$. Since we seek formulas involving extraction of roots, it will eventually be convenient to assume that k contains appropriate roots of unity.

When we say that there is a ***formula*** for the roots of a polynomial $f(x)$ analogous to the quadratic formula, we mean that there is an expression giving the roots of f in terms of its coefficients; this expression may involve field operations, constants, and extraction of roots, but it should not involve other operations such as cosine, definite integral, or limit, for example. We maintain that the intuitive idea of formula just described is captured by the following definition.

Definition. Let $f(x) \in k[x]$ have a splitting field E. We say that f is ***solvable by radicals*** if there is a radical extension

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

with $E \subseteq K_t$.

By Exercise A-5.1 on page 199, solvability by radicals does not depend on the choice of splitting field.

Example A-5.15.

(i) For every field k and every $n \geq 1$, we show that $f(x) = x^n - 1 \in k[x]$ is solvable by radicals. By Example A-3.93, a splitting field of $x^n - 1$ is $E = k(\omega)$, where ω is a primitive nth root of unity (if $p \mid n$, then a pth power of ω does not equal 1). Thus, E/k is a pure extension and, hence, a radical extension.

(ii) Let p be a prime and let k contain all pth roots of unity (if k has characteristic p, this is automatically true). If $k(u)/k$ is a pure extension of type p, then we claim that $k(u)$ is a splitting field of $f(x) = x^p - u^p$. If k has characteristic p, then $x^p - u^p = (x-u)^p$, and f splits over $k(u)$; otherwise, k contains a primitive pth root of unity, ω, and $f(x) = \prod_i (x - \omega^i u)$. Note that f is separable if characteristic $k \neq p$. ◀

Let us further illustrate this definition by considering the classical formulas for polynomials of small degree.

Quadratics

If $f(x) = x^2 + bx + c$, then the quadratic formula gives its roots as

$$\tfrac{1}{2}\Big(-b \pm \sqrt{b^2 - 4c}\Big).$$

Let $k = \mathbb{Q}(b, c)$. Define $K_1 = k(u)$, where $u = \sqrt{b^2 - 4c}$. Then K_1 is a radical extension of k (even a pure extension), for $u^2 \in k$. Moreover, the quadratic formula implies that K_1 is the splitting field of f, and so f is solvable by radicals.

Cubics

Let $f(X) = X^3 + bX^2 + cX + d$, and let $k = \mathbb{Q}(b, c, d)$. Recall that the change of variable $X = x - \frac{1}{3}b$ yields a new polynomial $\widetilde{f}(x) = x^3 + qx + r \in k[x]$ having

the same splitting field E (for if u is a root of $\widetilde{f}$, then $u - \frac{1}{3}b$ is a root of f); it follows that $\widetilde{f}$ is solvable by radicals if and only if f is. The cubic formula gives the roots of $\widetilde{f}$ as

$$g + h, \quad \omega g + \omega^2 h, \quad \text{and} \quad \omega^2 g + \omega h,$$

where $g^3 = \frac{1}{2}\big(-r + \sqrt{R}\big)$, $h = -q/3g$, $R = r^2 + \frac{4}{27}q^3$, and ω is a primitive cube root of unity. Because of the constraint $gh = -\frac{1}{3}q$, each of these has a "mate," namely, $h = -q/(3g)$, $-q/(3\omega g) = \omega^2 h$, and $-q/(3\omega^2 g) = \omega h$.

Let us show that $\widetilde{f}$ is solvable by radicals. Define $K_1 = k(\sqrt{R})$, where $R = r^2 + \frac{4}{27}q^3$, and define $K_2 = K_1(\alpha)$, where $\alpha^3 = \frac{1}{2}(-r + \sqrt{R})$. The cubic formula shows that K_2 contains the root $\alpha + \beta$ of $\widetilde{f}$, where $\beta = -q/3\alpha$. Finally, define $K_3 = K_2(\omega)$, where $\omega^3 = 1$. The other roots of $\widetilde{f}$ are $\omega\alpha + \omega^2\beta$ and $\omega^2\alpha + \omega\beta$, both of which lie in K_3, and so $E \subseteq K_3$.

A splitting field E need not equal K_3. If $g(x) \in \mathbb{Q}[x]$ is an irreducible cubic all of whose roots are real, then $E \subseteq \mathbb{R}$. As any cubic, g is solvable by radicals, and so there is a radical extension $K_t/\mathbb{Q}$ with $E \subseteq K_t$. The so-called *Casus Irreducibilis* (Theorem A-5.73) says that any radical extension $K_t/\mathbb{Q}$ containing E is not contained in $\mathbb{R}$. Therefore, $E \neq K_t$. In down-to-earth language, any formula for the roots of an irreducible cubic in $\mathbb{Q}[x]$ having all roots real requires the presence of complex numbers!

Quartics

Let $f(X) = X^4 + bX^3 + cX^2 + dX + e$, and let $k = \mathbb{Q}(b, c, d, e)$. The change of variable $X = x - \frac{1}{4}b$ yields a new polynomial $\widetilde{f}(x) = x^4 + qx^2 + rx + s \in k[x]$; moreover, the splitting field E of f is equal to the splitting field of $\widetilde{f}$, for if u is a root of $\widetilde{f}$, then $u - \frac{1}{4}b$ is a root of f. Factor $\widetilde{f}$ in $\mathbb{C}[x]$:

$$\widetilde{f}(x) = x^4 + qx^2 + rx + s = (x^2 + jx + \ell)(x^2 - jx + m),$$

and determine j, ℓ, and m. Now j^2 is a root of the *resolvent cubic* defined on page 7:

$$(j^2)^3 + 2q(j^2)^2 + (q^2 - 4s)j^2 - r^2.$$

The cubic formula gives j^2, from which we can determine m and ℓ, and hence the roots of the quartic.

Define pure extensions

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3,$$

as in the cubic case, so that $j^2 \in K_3$. Define $K_4 = K_3(j)$ (so that $\ell, m \in K_4$). Finally, define $K_5 = K_4\big(\sqrt{j^2 - 4\ell}\big)$ and $K_6 = K_5\big(\sqrt{j^2 - 4m}\big)$ (giving roots of the quadratic factors $x^2 + jx + \ell$ and $x^2 - jx + m$ of $\widetilde{f}(x)$). The quartic formula gives $E \subseteq K_6$.

We have just seen that quadratics, cubics, and quartics in $\mathbb{Q}[x]$ are solvable by radicals. Conversely, let $f(x) \in k[x]$ have splitting field E/k. If $f(x)$ is solvable by

radicals, we claim that there is a formula which expresses its roots in terms of its coefficients. Suppose that

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

is a tower of pure extensions with $E \subseteq K_t$. Let z be a root of f. Now $z \in K_t = K_{t-1}(u)$, where u is an mth root of some element $\alpha \in K_{t-1}$; hence, z can be expressed in terms of u and K_{t-1}; that is, z can be expressed in terms of $\sqrt[m]{\alpha}$ and K_{t-1}. But $K_{t-1} = K_{t-2}(v)$, where some power of v lies in K_{t-2}. Hence, z can be expressed in terms of u, v, and K_{t-2}. Ultimately, z is expressed by a formula analogous to the classical formulas.

Translation into Group Theory

The second stage of the strategy involves investigating the effect of $f(x)$ being solvable by radicals on its Galois group.

Suppose that $k(u)/k$ is a pure extension of type 6; that is, $u^6 \in k$. Now $k(u^3)/k$ is a pure extension of type 2, for $(u^3)^2 = u^6 \in k$, and $k(u)/k(u^3)$ is obviously a pure extension of type 3. Thus, $k(u)/k$ can be replaced by a tower of pure extensions $k \subseteq k(u^3) \subseteq k(u)$ of types 2 and 3. More generally, we may assume, given a tower of pure extensions, that each field is of prime type over its predecessor: if $k \subseteq k(u)$ is of type m, then factor $m = p_1 \cdots p_q$, where the p's are (not necessarily distinct) primes, and replace $k \subseteq k(u)$ by

$$k \subseteq k(u^{m/p_1}) \subseteq k(u^{m/p_1 p_2}) \subseteq \cdots \subseteq k(u).$$

Definition. An extension field E/k is called ***normal*** if it is the splitting field of a polynomial in $k[x]$.

Example A-5.16. If $E/\mathbb{Q}$ is the splitting field of $x^3 - 2$, then E contains $\alpha, \omega\alpha$, and $\omega^2\alpha$, where $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. The extension field $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal (it is the splitting field of $x^3 - 1$), but the extension fields $\mathbb{Q}(\alpha)/\mathbb{Q}$, $\mathbb{Q}(\omega\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\omega^2\alpha)/\mathbb{Q}$ are not normal. Notice that the subfields $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\omega\alpha)$, and $\mathbb{Q}(\omega^2\alpha)$ of E are isomorphic; in fact, the automorphism $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ with $\sigma(\alpha) = \omega\alpha$ is an isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\omega\alpha)$. ◀

Here is a key result allowing us to translate solvability by radicals into the language of Galois groups (it also shows why *normal extension fields* are so called).

Theorem A-5.17. *Let $k \subseteq B \subseteq E$ be a tower of fields. If B/k and E/k are normal extensions, then $\sigma(B) = B$ for all $\sigma \in \mathrm{Gal}(E/k)$, $\mathrm{Gal}(E/B) \lhd \mathrm{Gal}(E/k)$, and*

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k).$$

Proof. Since B/k is a normal extension, it is a splitting field of some $f(x)$ in $k[x]$; that is, $B = k(z_1, \ldots, z_t) \subseteq E$, where $z_1, \ldots, z_t$ are the roots of f. If $\sigma \in \mathrm{Gal}(E/k)$, the restriction of σ to B is an automorphism of B, and it thus permutes $z_1, \ldots, z_t$, by Proposition A-5.1(i) (for σ fixes k); hence, $\sigma(B) = B$. Define $\rho\colon \mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k)$ by $\sigma \mapsto \sigma|B$. It is easy to see, as in the proof of Theorem A-5.3, that ρ is a homomorphism and $\ker \rho = \mathrm{Gal}(E/B)$; thus, $\mathrm{Gal}(E/B) \lhd \mathrm{Gal}(E/k)$. But ρ

is surjective: if $\tau \in \mathrm{Gal}(B/k)$, then Lemma A-3.98 applies to show that there is $\sigma \in \mathrm{Gal}(E/k)$ extending τ (i.e., $\rho(\sigma) = \sigma|B = \tau$). The First Isomorphism Theorem completes the proof. •

The next technical result will be needed when we apply Theorem A-5.17.

Lemma A-5.18.

(i) *If $B = k(u_1, \dots, u_t)/k$ is a finite extension field, then there is a normal extension E/k containing B; that is, E is a splitting field of some $f(x) \in k[x]$. If each u_i is separable over k, then f is a separable polynomial and, if $G = \mathrm{Gal}(E/k)$, then*

$$E = k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G).$$

(ii) *If B/k is a radical extension, then the normal extension E/k is a radical extension.*

Proof.

(i) By Theorem A-3.87(i), there are irreducible polynomials $p_i = \mathrm{irr}(u_i, k) \in k[x]$, for $i = 1, \dots, t$, with $p_i(u_i) = 0$. Define E to be a splitting field of $f(x) = p_1(x) \cdots p_t(x)$ over k. Since $u_i \in E$ for all i, we have $B = k(u_1, \dots, u_t) \subseteq E$. If each u_i is separable over k, then each p_i is a separable polynomial, and hence f is a separable polynomial.

For each pair of roots u and u' of any p_i, Theorem A-3.87(ii) gives an isomorphism $\gamma\colon k(u) \to k(u')$ which fixes k and which takes $u \mapsto u'$. By Lemma A-3.98, each such γ extends to an automorphism $\sigma \in G = \mathrm{Gal}(E/k)$. Thus, f splits over $k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G)$. But E/k is a splitting field of f over k and $k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G) \subseteq E$. Hence,

$$E = k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G),$$

because a splitting field is the smallest field over which f splits.

(ii) Assume now that B/k is a radical extension; say, $B = k(v_1, \dots, v_s)$, where

$$k \subseteq k(v_1) \subseteq k(v_1, v_2) \subseteq \cdots \subseteq k(v_1, \dots, v_s) = B$$

and each $k(v_1, \dots, v_{i+1})/k(v_1, \dots, v_i)$ is a pure extension; of course, $\sigma(B) = k(\sigma(v_1), \dots, \sigma(v_s))$ is a radical extension of k for every $\sigma \in G$. We now show that $E = k(\sigma(v_1), \dots, \sigma(v_s) : \sigma \in G)$ is a radical extension of k. Define

$$B_1 = k(\sigma(v_1) : \sigma \in G).$$

Now if $G = \{1, \sigma, \tau, \dots\}$, then the tower

$$k \subseteq k(v_1) \subseteq k(v_1, \sigma(v_1)) \subseteq k(v_1, \sigma(v_1), \tau(v_1)) \subseteq \cdots \subseteq B_1$$

displays B_1 as a radical extension of k. For example, v_1^m lies in k, and so $\tau(v_1)^m = \tau(v_1^m)$ lies in $\tau(k) = k$; since $k \subseteq k(v_1, \sigma(v_1))$, we have $\tau(v_1)^m \in k(v_1, \sigma(v_1))$. Having defined B_1, define B_{i+1} inductively:

$$B_{i+1} = B_i(\sigma(v_{i+1}) : \sigma \in G).$$

Assume, by induction, that B_i/k is a radical extension and that $\sigma(B_i) \subseteq B_i$ for all $\sigma \in G$. Now B_{i+1}/B_i is a radical extension, for $v_{i+1}^n \in B_i$, and so $\sigma(v_{i+1})^n \in \sigma(B_i) \subseteq B_i$ for each σ. Thus, every B_i is a radical extension of k and, therefore, $E = B_s$ is a radical extension of k. •

We can now give the heart of the translation we have been seeking: a radical extension E/k gives rise to a sequence of subgroups of $\mathrm{Gal}(E/k)$.

Lemma A-5.19. *Let*

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t$$

be a tower with each K_i/K_{i-1} a pure extension of prime type p_i. If K_t/k is a normal extension and k contains all the p_ith roots of unity, for $i = 1, \ldots, t$, then there is a sequence of subgroups

$$\mathrm{Gal}(K_t/k) = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \{1\},$$

with each $G_{i+1} \lhd G_i$ and G_i/G_{i+1} cyclic of prime order p_{i+1} or $\{1\}$.

Proof. For each i, define $G_i = \mathrm{Gal}(K_t/K_i)$. It is clear that

$$\mathrm{Gal}(K_t/k) = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \{1\}$$

is a sequence of subgroups. Now $K_1 = k(u)$, where $u^{p_1} \in k$; since k contains all the p_1th roots of unity, Example A-5.15(ii) says that K_1/k is a splitting field of the polynomial $f(x) = x^{p_1} - u^{p_1}$. Theorem A-5.17 now applies: $G_1 = \mathrm{Gal}(K_t/K_1)$ is a normal subgroup of $G_0 = \mathrm{Gal}(K_t/k)$ and $G_0/G_1 \cong \mathrm{Gal}(K_1/k)$. Now Example A-5.15(ii) also says that if characteristic $k \neq p_1$, then f is separable. By Theorem A-5.7(ii), $G_0/G_1 \cong \mathbb{Z}_{p_1}$. If characteristic $k = p_1$, then Example A-5.8 shows that $G_0/G_1 \cong \mathrm{Gal}(K_1/k) = \{1\}$. This argument can be repeated for each i. •

We have been led to the following definitions.

Definition. A ***normal series***[2] of a group G is a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \{1\}$$

with each G_{i+1} a normal subgroup of G_i; the ***factor groups*** of this series are the quotient groups

$$G_0/G_1,\ G_1/G_2,\ \ldots,\ G_{t-1}/G_t.$$

The ***length*** of this series is the number of nontrivial factor groups.

A group G is called ***solvable*** if it has a normal series each of whose factor groups is abelian.

In this language, Lemma A-5.19 says that $\mathrm{Gal}(K_t/k)$ is a solvable group if K_t/k is a radical extension and k contains appropriate roots of unity.

[2]This terminology is not quite standard. We know that normality is not transitive; that is, if $H \subseteq K$ are subgroups of a group G, then $H \lhd K$ and $K \lhd G$ do not force $H \lhd G$. A subgroup $H \subseteq G$ is called a ***subnormal subgroup*** if there is a chain $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = H$ with $G_i \lhd G_{i-1}$ for all $i \geq 1$. Normal series as defined in the text are called ***subnormal series*** by some authors; they reserve the name *normal series* for those series in which each G_i is a normal subgroup of the big group G.

Example A-5.20.

(i) Every abelian group is solvable.

(ii) Let us see that S_4 is a solvable group. Consider the chain of subgroups

$$S_4 \supseteq A_4 \supseteq \mathbf{V} \supseteq W \supseteq \{1\},$$

where $\mathbf{V}$ is the four-group and W is any subgroup of $\mathbf{V}$ of order 2. Note, since $\mathbf{V}$ is abelian, that W is a normal subgroup of $\mathbf{V}$. Now $|S_4/A_4| = |S_4|/|A_4| = 24/12 = 2$, $|A_4/\mathbf{V}| = |A_4|/|\mathbf{V}| = 12/4 = 3$, $|\mathbf{V}/W| = |\mathbf{V}|/|W| = 4/2 = 2$, and $|W/\{1\}| = |W| = 2$. Since each factor group is a cyclic group (of prime order), hence is abelian, S_4 is solvable. In Example A-5.24, we shall see that S_5 is not a solvable group.

(iii) A nonabelian simple group G, for example, $G = A_5$, is not solvable, for its only proper normal subgroup is $\{1\}$, and $G/\{1\} \cong G$ is not abelian. ◀

The awkward hypothesis about roots of unity in the next lemma will soon be removed.

Lemma A-5.21. *Let k be a field, let $f(x) \in k[x]$ be solvable by radicals, and let $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$ be a tower with K_i/K_{i-1} a pure extension of prime type p_i for all i. If K_t contains a splitting field E of f and k contains all the p_ith roots of unity, then the Galois group* $\mathrm{Gal}(E/k)$ *is a quotient of a solvable group.*

Proof. By Lemma A-5.18, we may assume that K_t is a normal extension of k. The hypothesis on k allows us to apply Lemma A-5.19 to see that $\mathrm{Gal}(K_t/k)$ is a solvable group. Since E and K_t are splitting fields over k, Theorem A-5.17 shows that $\mathrm{Gal}(K_t/E) \lhd \mathrm{Gal}(K_t/k)$ and $\mathrm{Gal}(K_t/k)/\mathrm{Gal}(K_t/E) \cong \mathrm{Gal}(E/k)$, as desired. •

Proposition A-5.22. *Every quotient of a solvable group G is itself a solvable group.*

Proof. Let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t = \{1\}$ be a sequence of subgroups as in the definition of solvable group. If $N \lhd G$, we must show that G/N is solvable. Now G_iN is a subgroup of G for all i, and so there is a sequence of subgroups

$$G = G_0N \supseteq G_1N \supseteq \cdots \supseteq G_tN = N \supseteq \{1\}.$$

To see that this is a normal series, we claim, with obvious notation, that

$$(g_in)G_{i+1}N(g_in)^{-1} \subseteq g_iG_{i+1}Ng_i^{-1} = g_iG_{i+1}g_i^{-1}N \subseteq G_{i+1}N.$$

The first inclusion holds because $n(G_{i+1}N)n^{-1} \subseteq NG_{i+1}N \subseteq (G_{i+1}N)(G_{i+1}N) = G_{i+1}N$ (for $G_{i+1}N$ is a subgroup). The equality holds because $Ng_i^{-1} = g_i^{-1}N$ (for $N \lhd G$, and so its right cosets coincide with its left cosets). The last inclusion holds because $G_{i+1} \lhd G_i$.

The Second Isomorphism Theorem gives

$$\frac{G_i}{G_i \cap (G_{i+1}N)} \cong \frac{G_i(G_{i+1}N)}{G_{i+1}N} = \frac{G_iN}{G_{i+1}N},$$

the last equation holding because $G_iG_{i+1} = G_i$. Since $G_{i+1} \lhd G_i \cap G_{i+1}N$, the Third Isomorphism Theorem gives a surjection $G_i/G_{i+1} \to G_i/[G_i \cap G_{i+1}N]$, and so the composite is a surjection $G_i/G_{i+1} \to G_iN/G_{i+1}N$. As G_i/G_{i+1} is abelian, its image is also abelian. Therefore, G/N is a solvable group. •

Proposition A-5.23. *Every subgroup H of a solvable group G is solvable.*

Proof. Since G is solvable, there is a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_t = \{1\}$$

with G_i normal in G_{i-1} and G_{i-1}/G_i abelian for all i. Consider the sequence of subgroups

$$H = H \cap G_0 \supseteq H \cap G_1 \supseteq \cdots \supseteq H \cap G_t = \{1\}.$$

This is a normal series: if $h_{i+1} \in H \cap G_{i+1}$ and $g_i \in H \cap G_i$, then $g_ih_{i+1}g_i^{-1} \in H$, for $g_i, h_{i+1} \in H$; also, $g_ih_{i+1}g_i^{-1} \in G_{i+1}$ because G_{i+1} is normal in G_i. Therefore, $g_ih_{i+1}g_i^{-1} \in H \cap G_{i+1}$, and so $H \cap G_{i+1} \lhd H \cap G_i$. Finally, the Second Isomorphism Theorem gives

$$\begin{aligned}(H \cap G_i)/(H \cap G_{i+1}) &= (H \cap G_i)/[(H \cap G_i) \cap G_{i+1}] \\ &\cong G_{i+1}(H \cap G_i)/G_{i+1}.\end{aligned}$$

But the last quotient group is a subgroup of G_i/G_{i+1}. Since every subgroup of an abelian group C is abelian, it follows that the factor groups $(H \cap G_i)/(H \cap G_{i+1})$ are also abelian. Therefore, H is a solvable group. •

Example A-5.24. In Example A-5.20(ii), we showed that S_4 is a solvable group. On the other hand, if $n \geq 5$, then the symmetric group S_n is not solvable. Otherwise, each of its subgroups would also be solvable. But $A_5 \subseteq S_5 \subseteq S_n$, and the simple group A_5 is not solvable, by Example A-5.20(iii). ◀

Proposition A-5.25. *If $H \lhd G$ and both H and G/H are solvable groups, then G is solvable.*

Proof. Since G/H is solvable, there is a normal series,

$$G/H \supseteq K_1^* \supseteq K_2^* \supseteq \cdots \supseteq K_m^* = \{1\},$$

having abelian factor groups. By the Correspondence Theorem for Groups, there are subgroups K_i of G,

$$G \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_m = H,$$

with $K_i/H = K_i^*$ and $K_{i+1} \lhd K_i$ for all i. By the Third Isomorphism Theorem,

$$K_i^*/K_{i+1}^* \cong K_i/K_{i+1}$$

for all i, and so K_i/K_{i+1} is abelian for all i.

Since H is solvable, there is a normal series

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_q = \{1\}$$

having abelian factor groups. Splice these two series together,

$$G \supseteq K_1 \supseteq \cdots \supseteq K_m = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_q = \{1\},$$

to obtain a normal series of G having abelian factor groups (note that $H \lhd G$ implies $H_0 = H = K_m$). •

Corollary A-5.26. *If H and K are solvable groups, then $H \times K$ is solvable.*

Proof. The result follows from Proposition A-5.25 because $(H \times K)/H \cong K$. •

There is a subtle point; when is a group G *not* solvable? By definition, G is solvable if it has a normal series with abelian factor groups; hence, G is not solvable if it has no such normal series. It is not enough to display one normal series having a nonabelian factor group; perhaps another normal series does have all its factor groups abelian. But we have to be a bit more careful. After all, S_3 is a solvable group, for the factor groups of the normal series

$$S_3 \supseteq A_3 \supseteq \{1\}$$

are $\mathbb{Z}_2, \mathbb{Z}_3$. On the other hand, $S_3 \supseteq \{1\}$ is another normal series whose factor group(s) is not abelian. This suggests that we look at the longest normal series.

Definition. A ***composition series*** of a group is a normal series all of whose nontrivial factor groups are simple. The list of nontrivial factor groups of a composition series is called the list of ***composition factors*** of G. The ***length*** of a composition series is the number of nontrivial factor groups.

A finite group G is solvable if it has a normal series with abelian factor groups (many define a finite group to be solvable if it has a normal series with all factor groups cyclic). Exercise A-5.9 on page 200 says that G is solvable if and only if it has a normal series all of whose factor groups are cyclic of prime order. As groups of prime order are simple groups, this normal series is a composition series and the cyclic groups are its composition factors.

A group need not have a composition series; for example, the abelian group $\mathbb{Z}$ has no composition series.

Proposition A-5.27. *Every finite group G has a composition series.*

Proof. Let G be a *least criminal*; that is, assume that G is a finite group of smallest order that does not have a composition series. Now G is not simple, otherwise $G \supsetneq \{1\}$ is a composition series. Hence, G has a proper normal subgroup H. Since G is finite, we may assume that H is a maximal normal subgroup, so that G/H is a simple group. But $|H| < |G|$, so that H has a composition series: say, $H = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq \{1\}$. Hence, $G \supsetneq H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq \{1\}$ is a composition series for G, a contradiction. •

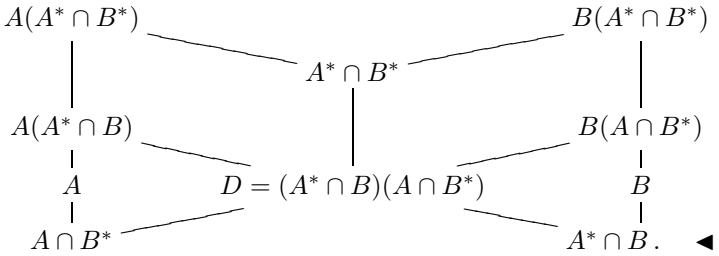
We begin with a technical result that generalizes the Second Isomorphism Theorem; it is useful when comparing different normal series of a group.

Lemma A-5.28 (Zassenhaus Lemma). *Given four subgroups $A \lhd A^*$ and $B \lhd B^*$ of a group G, then $A(A^* \cap B) \lhd A(A^* \cap B^*)$, $B(B^* \cap A) \lhd B(B^* \cap A^*)$, and there is an isomorphism*

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

Remark. The isomorphism is symmetric in the sense that the right side is obtained from the left by interchanging the symbols A and B.

The Zassenhaus Lemma is sometimes called the *Butterfly Lemma* because of the following picture. I confess that I have never liked this picture; it doesn't remind me of a butterfly, and it doesn't help me understand or remember the proof:



Proof. We claim that $(A \cap B^*) \lhd (A^* \cap B^*)$: that is, if $c \in A \cap B^*$ and $x \in A^* \cap B^*$, then $xcx^{-1} \in A \cap B^*$. Now $xcx^{-1} \in A$ because $c \in A$, $x \in A^*$, and $A \lhd A^*$; but also $xcx^{-1} \in B^*$, because $c, x \in B^*$. Hence, $(A \cap B^*) \lhd (A^* \cap B^*)$; similarly, $(A^* \cap B) \lhd (A^* \cap B^*)$. Therefore, the subset D, defined by $D = (A \cap B^*)(A^* \cap B)$, is a normal subgroup of $A^* \cap B^*$, because it is generated by two normal subgroups.

Using the symmetry in the remark, it suffices to show that there is an isomorphism

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \to \frac{A^* \cap B^*}{D}.$$

Define $\varphi : A(A^* \cap B^*) \to (A^* \cap B^*)/D$ by $\varphi : ax \mapsto xD$, where $a \in A$ and $x \in A^* \cap B^*$. Now φ is well-defined: if $ax = a'x'$, where $a' \in A$ and $x' \in A^* \cap B^*$, then $(a')^{-1}a = x'x^{-1} \in A \cap (A^* \cap B^*) = A \cap B^* \subseteq D$; hence, $xD = x'D$. Also, φ is a homomorphism: $axa'x' = a''xx'$, where $a'' = a(xa'x^{-1}) \in A$ (because $A \lhd A^*$), and so $\varphi(axa'x') = \varphi(a''xx') = xx'D = \varphi(ax)\varphi(a'x')$. It is routine to check that φ is surjective and that $\ker \varphi = A(A^* \cap B)$. The First Isomorphism Theorem completes the proof. •

The Zassenhaus Lemma implies the Second Isomorphism Theorem: if S and T are subgroups of a group G with $T \lhd G$, then $TS/T \cong S/(S \cap T)$; set $A^* = G$, $A = T$, $B^* = S$, and $B = S \cap T$.

Here are two composition series of $G = \langle a \rangle$, a cyclic group of order 30 (note that normality of subgroups is automatic because G is abelian). The first is

$$G = \langle a \rangle \supseteq \langle a^2 \rangle \supseteq \langle a^{10} \rangle \supseteq \{1\};$$

the factor groups of this series are $\langle a \rangle / \langle a^2 \rangle \cong \mathbb{Z}_2$, $\langle a^2 \rangle / \langle a^{10} \rangle \cong \mathbb{Z}_5$, and $\langle a^{10} \rangle / \{1\} \cong \langle a^{10} \rangle \cong \mathbb{Z}_3$ (see Example A-4.80 on page 166). Another normal series is

$$G = \langle a \rangle \supseteq \langle a^5 \rangle \supseteq \langle a^{15} \rangle \supseteq \{1\};$$

the factor groups of this series are $\langle a \rangle / \langle a^5 \rangle \cong \mathbb{Z}_5$, $\langle a^5 \rangle / \langle a^{15} \rangle \cong \mathbb{Z}_3$, and $\langle a^{15} \rangle / \{1\} \cong \langle a^{15} \rangle \cong \mathbb{Z}_2$. Notice that the same factor groups arise, although the order in which they arise is different. We will see that this phenomenon always occurs: different

composition series of the same group have the same factor groups. This is the *Jordan–Hölder Theorem*, and the next definition makes its statement more precise.

Definition. Two normal series of a group G are ***equivalent*** if there is a bijection between the lists of nontrivial factor groups of each so that corresponding factor groups are isomorphic.

The Jordan–Hölder Theorem says that any two composition series of a group are equivalent. It is more efficient to prove a more general theorem, due to Schreier.

Definition. A ***refinement*** of a normal series of a group G is a normal series $G = N_0 \supseteq \cdots \supseteq N_k = \{1\}$ having the original series as a subseries.

In other words, a refinement of a normal series is a normal series obtained from the original one by inserting more subgroups.

Notice that a composition series admits only insignificant refinements; one can merely repeat terms (if G_i/G_{i+1} is simple, then it has no proper nontrivial normal subgroups and, hence, there is no intermediate subgroup L with $G_i \supsetneq L \supsetneq G_{i+1}$ and $L \lhd G_i$). Therefore, any refinement of a composition series is equivalent to the original composition series.

Theorem A-5.29 (Schreier Refinement Theorem). *Any two normal series*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

and

$$G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = \{1\}$$

of a group G have equivalent refinements.

Proof. We insert a copy of the second series between each pair of adjacent terms in the first series. In more detail, for each $i \geq 0$, define

$$G_{ij} = G_{i+1}(G_i \cap N_j)$$

(this is a subgroup, by Proposition A-4.69(i), because $G_{i+1} \lhd G_i$). Since $N_0 = G$, we have

$$G_{i0} = G_{i+1}(G_i \cap N_0) = G_{i+1}G_i = G_i,$$

and since $N_k = \{1\}$, we have

$$G_{ik} = G_{i+1}(G_i \cap N_k) = G_{i+1}.$$

Therefore, the series of G_i is a subsequence of the series of G_{ij}:

$$\cdots \supseteq G_i = G_{i0} \supseteq G_{i1} \supseteq G_{i2} \supseteq \cdots \supseteq G_{ik} = G_{i+1} \supseteq \cdots .$$

Similarly, the second series of N_j is a subsequence of the series

$$N_{ji} = N_{j+1}(N_j \cap G_i).$$

Both doubly indexed sequences have nk terms. For each i, j, the Zassenhaus Lemma, for the four subgroups $G_{i+1} \lhd G_i$ and $N_{j+1} \lhd N_j$, says both subsequences are normal series, hence are refinements, and there is an isomorphism

$$\frac{G_{i+1}(G_i \cap N_j)}{G_{i+1}(G_i \cap N_{j+1})} \cong \frac{N_{j+1}(N_j \cap G_i)}{N_{j+1}(N_j \cap G_{i+1})};$$

that is,

$$G_{i,j}/G_{i,j+1} \cong N_{j,i}/N_{j,i+1}.$$

The association $G_{i,j}/G_{i,j+1} \mapsto N_{j,i}/N_{j,i+1}$ is a bijection showing that the two refinements are equivalent. •

Theorem A-5.30 (Jordan–Hölder Theorem[3]). *Any two composition series of a group G are equivalent. In particular, the length of a composition series, if one exists, is an invariant of G.*

Proof. As we remarked earlier, any refinement of a composition series is equivalent to the original composition series. It now follows from Schreier's Theorem that any two composition series are equivalent. •

We have resolved the subtle point: if a finite group G has one composition series with a factor group not of prime order, then G is not solvable, for the Jordan-Hölder Theorem say that every composition series of G has such a factor group.

The importance of the Jordan-Hölder Theorem, for group theory as well as for other branches of mathematics, is that it shows that valuable information about a group (or a topological space or a ring, for example) can be retrieved from an analog of a normal series. In light of the next proof, the theorem can be viewed as a kind of unique factorization result; here is a new proof of the Fundamental Theorem of Arithmetic.

Corollary A-5.31. *Every integer $n \geq 2$ has a factorization into primes, and the prime factors and their multiplicities are uniquely determined by n.*

Proof. Since the group $\mathbb{Z}_n$ is finite, it has a composition series; let $S_1, \ldots, S_t$ be the factor groups. Now an abelian group is simple if and only if it is of prime order, by Proposition A-4.92; since $n = |\mathbb{Z}_n|$ is the product of the orders of the factor groups (Exercise A-5.7 on page 199), we have proved that n is a product of primes. Moreover, the Jordan–Hölder Theorem gives the uniqueness of the (prime) orders of the factor groups and their multiplicities. •

Example A-5.32.

(i) Nonisomorphic groups can have the same composition factors. For example, both $\mathbb{Z}_4$ and $\mathbf{V}$ have composition series whose factor groups are $\mathbb{Z}_2$, $\mathbb{Z}_2$.

(ii) Let $G = \mathrm{GL}(2, \mathbb{F}_4)$ be the general linear group of all 2×2 nonsingular matrices with entries in the field $\mathbb{F}_4$ with four elements. Now $\det\colon G \to (\mathbb{F}_4)^\times$, where $(\mathbb{F}_4)^\times \cong \mathbb{Z}_3$ is the multiplicative group of nonzero elements of $\mathbb{F}_4$. Since $\ker \det = \mathrm{SL}(2, \mathbb{F}_4)$, the special linear group consisting of those matrices of determinant 1, there is a normal series

$$G = \mathrm{GL}(2, \mathbb{F}_4) \supseteq \mathrm{SL}(2, \mathbb{F}_4) \supseteq \{1\}.$$

[3] In 1868, Jordan proved that the orders of the factor groups of a composition series depend only on G and not on the composition series; in 1889, Hölder proved that the factor groups themselves, up to isomorphism, do not depend on the composition series.

The factor groups of this normal series are $\mathbb{Z}_3$ and $\mathrm{SL}(2,\mathbb{F}_4)$. It is true that $\mathrm{SL}(2,\mathbb{F}_4)$ is a nonabelian simple group (in fact, $\mathrm{SL}(2,\mathbb{F}_4) \cong A_5$), and so this series is a composition series. We cannot yet conclude that G is not solvable, for the definition of solvability requires that there be some composition series, not necessarily this one, having factor groups of prime order. However, the Jordan–Hölder Theorem says that if one composition series of G has all its factor groups of prime order, then so does every other composition series. We may now conclude that $\mathrm{GL}(2,\mathbb{F}_4)$ is not a solvable group. ◀

Exercises

∗ **A-5.1.** Prove that solvability by radicals does not depend on the choice of splitting field: if E/k and E'/k are splitting fields of $f(x) \in k[x]$ and there is a radical extension K_t/k with $E \subseteq K_t$, prove that there is a radical extension K'_r/k with $E' \subseteq K'_r$.

∗ **A-5.2.** Let $f(x) \in E[x]$ be monic, where E is a field, and let $\sigma\colon E \to E$ be an automorphism. If f splits and σ fixes every root of $f(x)$, prove that σ fixes every coefficient of f.

∗ **A-5.3. (Accessory Irrationalities)** Let E/k be a splitting field of $f(x) \in k[x]$ with Galois group $G = \mathrm{Gal}(E/k)$. Prove that if k^*/k is an extension field and E^* is a splitting field of f over k^*, then $\sigma \mapsto \sigma|E$ is an injective homomorphism $\mathrm{Gal}(E^*/k^*) \to \mathrm{Gal}(E/k)$.

Hint. If $\sigma \in \mathrm{Gal}(E^*/k^*)$, then σ permutes the roots of f, so that $\sigma|E \in \mathrm{Gal}(E/k)$.

A-5.4. (i) Let K/k be an extension field, and let $f(x) \in k[x]$ be a separable polynomial. Prove that f is a separable polynomial when viewed as a polynomial in $K[x]$.

(ii) Let k be a field, and let $f(x), g(x) \in k[x]$. Prove that if both f and g are separable polynomials, then their product fg is also a separable polynomial.

A-5.5. Let k be a field and let $f(x) \in k[x]$ be a separable polynomial. If E/k is a splitting field of f, prove that every root of f in E is a separable element over k.

A-5.6. (i) Let K/k be an extension field that is a splitting field of a polynomial $f(x) \in k[x]$. If $p(x) \in k[x]$ is a monic irreducible polynomial with no repeated roots and

$$p(x) = g_1(x) \cdots g_r(x) \text{ in } K[x],$$

where the g_i are monic irreducible polynomials in $K[x]$, prove that all the g_i have the same degree. Conclude that $\deg(p) = r \deg(g_i)$.

Hint. In some splitting field E/K of pf, let α be a root of g_i and β be a root of g_j, where $i \neq j$. There is an isomorphism $\varphi\colon k(\alpha) \to k(\beta)$ with $\varphi(\alpha) = \beta$, which fixes k and which admits an extension to $\Phi\colon E \to E$. Show that $\Phi|K$ induces an automorphism of $K[x]$ taking g_i to g_j.

(ii) Let E/k be a finite extension field. Prove that E/k is a normal extension if and only if every irreducible $p(x) \in k[x]$ having a root in E splits in $E[x]$. (Compare with Theorem A-5.42 which uses a separability hypothesis.)
Hint. Use part (i).

∗ **A-5.7.** Let G be a finite group with normal series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}.$$

Prove that $|G| = \prod_i |G_{i-1}|/|G_i|$; that is, the order of G is the product of the orders of the factor groups.

A-5.8. (i) Give an example of a group G having a subnormal subgroup that is not a normal subgroup.

(ii) Give an example of a group G having a subgroup that is not a subnormal subgroup.

∗ **A-5.9.** (i) Prove that a finite solvable group $G \neq \{1\}$ has a normal subgroup of index p for some prime p.

(ii) Prove that a finite group is solvable if and only if it has a normal series all of whose factor groups are cyclic of prime order.

A-5.10. Prove that the following statements are equivalent for $f(x) = ax^2+bx+c \in \mathbb{Q}[x]$.

(i) f is irreducible in $\mathbb{Q}[x]$.

(ii) $\sqrt{b^2-4ac}$ is not rational.

(iii) $\mathrm{Gal}(\mathbb{Q}(\sqrt{b^2-4ac})/\mathbb{Q})$ has order 2.

∗ **A-5.11.** Let k be a field, let $f(x) \in k[x]$ be a polynomial of degree p, where p is prime, and let E/k be a splitting field of f. Prove that if $\mathrm{Gal}(E/k) \cong \mathbb{Z}_p$, then f is irreducible.

Hint. Show that f has no repeated roots, and use Proposition A-5.14.

∗ **A-5.12.** Generalize Theorem A-5.13: prove that if E is a finite field and $k \subseteq E$ is a subfield, then $\mathrm{Gal}(E/k)$ is cyclic.

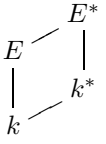
Fundamental Theorem of Galois Theory

We return to fields, for we can now give the main criterion that a polynomial be solvable by radicals.

Theorem A-5.33 (Galois). *Let $f(x) \in k[x]$, where k is a field, and let E be a splitting field of f over k. If f is solvable by radicals, then its Galois group* $\mathrm{Gal}(E/k)$ *is a solvable group.*

Remark. The converse of this theorem is false if k has characteristic $p > 0$ (Theorem A-5.66), but it is true when k has characteristic 0 (Corollary A-5.63). ◀

Proof. Let $p_1, \ldots, p_t$ be the types of the pure extensions occurring in the radical extension arising from f being solvable by radicals. Define m to be the product of all these p_i, define E^* to be a splitting field of $x^m - 1$ over E, and define $k^* = k(\Omega)$, where Ω is the set of all mth roots of unity in E^*. Now E^*/k^* is a normal extension, for it is a splitting field of f over k^*, and so $\mathrm{Gal}(E^*/k^*)$ is solvable, by Lemma A-5.21. Consider the tower $k \subseteq k^* \subseteq E^*$:



since k^*/k is normal, Theorem A-5.17 gives $\mathrm{Gal}(E^*/k^*) \lhd \mathrm{Gal}(E^*/k)$ and

$$\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/k^*) \cong \mathrm{Gal}(k^*/k).$$

Now $\mathrm{Gal}(E^*/k^*)$ is solvable, while $\mathrm{Gal}(k^*/k)$ is abelian, hence solvable; therefore, $\mathrm{Gal}(E^*/k)$ is solvable, by Proposition A-5.25. Finally, we may use Theorem A-5.17 once again, for the tower $k \subseteq E \subseteq E^*$ satisfies the hypothesis that both E and E^* are normal (E^* is a splitting field of $(x^m - 1)f(x)$). It follows that $\mathrm{Gal}(E^*/k)/\mathrm{Gal}(E^*/E) \cong \mathrm{Gal}(E/k)$, and so $\mathrm{Gal}(E/k)$, being a quotient of a solvable group, is solvable. •

Recall that if k is a field and $E = k(y_1, \ldots, y_n) = \mathrm{Frac}(k[y_1, \ldots, y_n])$ is the field of rational functions, then the *general polynomial of degree n* over k is

$$(x - y_1)(x - y_2)\cdots(x - y_n).$$

Galois's Theorem is strong enough to prove that there is no generalization of the quadratic formula for the general quintic polynomial.

Theorem A-5.34 (Abel–Ruffini). *If $n \geq 5$, the general polynomial*

$$f(x) = (x - y_1)(x - y_2)\cdots(x - y_n)$$

over a field k is not solvable by radicals.

Proof. In Example A-3.92, we saw that if $E = k(y_1, \ldots, y_n)$ is the field of all rational functions in n variables with coefficients in a field k, and if $F = k(a_0, \ldots, a_{n-1})$, where the a_i are the coefficients of $f(x)$, then E is the splitting field of f over F.

We claim that $\mathrm{Gal}(E/F) \cong S_n$. Recall Exercise A-3.38 on page 54: If A and R are domains and $\varphi\colon A \to R$ is an isomorphism, then $a/b \mapsto \varphi(a)/\varphi(b)$ is an isomorphism $\mathrm{Frac}(A) \to \mathrm{Frac}(R)$. Now if $\sigma \in S_n$, then Theorem A-3.25 gives an automorphism $\widetilde{\sigma}$ of $k[y_1, \ldots, y_n]$, defined by $\widetilde{\sigma}\colon f(y_1, \ldots, y_n) \mapsto f(y_{\sigma 1}, \ldots, y_{\sigma n})$; that is, $\widetilde{\sigma}$ just permutes the variables. Thus, $\widetilde{\sigma}$ extends to an automorphism σ^* of $E = \mathrm{Frac}(k[y_1, \ldots, y_n])$, and Eqs. (8) on page 179 show that σ^* fixes F; hence, $\sigma^* \in \mathrm{Gal}(E/F)$. Using Lemma A-5.2, it is easy to see that $\sigma \mapsto \sigma^*$ is an injection $S_n \to \mathrm{Gal}(E/F)$, so that $|S_n| \leq |\mathrm{Gal}(E/F)|$. On the other hand, Theorem A-5.3 shows that $\mathrm{Gal}(E/F)$ can be imbedded in S_n, giving the reverse inequality $|\mathrm{Gal}(E/F)| \leq |S_n|$. Therefore, $\mathrm{Gal}(E/F) \cong S_n$. But S_n is not a solvable group if $n \geq 5$, by Example A-5.24, and so Theorem A-5.33 shows that f is not solvable by radicals. •

Some quintics in $\mathbb{Q}[x]$ are solvable by radicals; for example, Example A-5.15 says that $x^5 - 1$ is solvable by radicals. Here is an explicit example of a quintic polynomial in $\mathbb{Q}[x]$ which is not solvable by radicals.

Corollary A-5.35. *$f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ is not solvable by radicals.*

Proof. By Eisenstein's criterion (Theorem A-3.111), f is irreducible over $\mathbb{Q}$. We now use some calculus. There are exactly two real roots of the derivative $f'(x) = 5x^4 - 4$, namely, $\pm\sqrt[4]{4/5} \sim \pm .946$, and so f has two critical points. Now $f(\sqrt[4]{4/5}) < 0$ and $f(-\sqrt[4]{4/5}) > 0$, so that f has one relative maximum and one relative minimum. It follows easily that f has exactly three real roots.

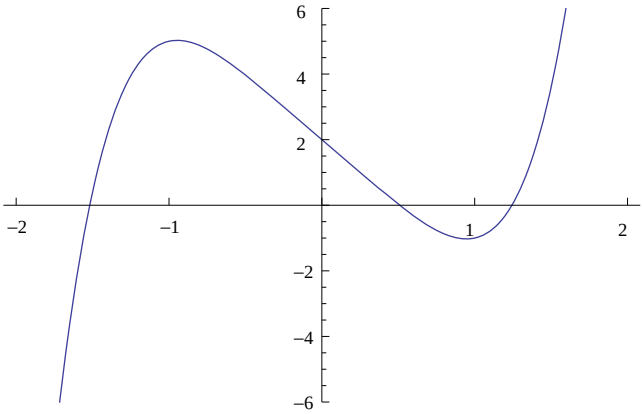


Figure A-5.1. $f(x) = x^5 - 4x + 2$.

Let $E/\mathbb{Q}$ be the splitting field of f contained in $\mathbb{C}$. The restriction of complex conjugation to E, call it τ, interchanges the two complex roots while it fixes the three real roots. Thus, if X is the set of five roots of $f(x)$, then τ is a transposition in S_X. The Galois group $\mathrm{Gal}(E/\mathbb{Q})$ of f is isomorphic to a subgroup $G \subseteq S_X$. Corollary A-5.9 gives $|G| = [E : \mathbb{Q}]$ divisible by 5, so that G contains an element σ of order 5, by Cauchy's Theorem (FCAA [**94**], p. 200). (If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.) Now σ must be a 5-cycle, for the only elements of order 5 in $S_X \cong S_5$ are 5-cycles. But Exercise A-5.13 on page 221 says that S_5 is generated by any transposition and any 5-cycle. Since $G \supseteq \langle \sigma, \tau \rangle$, we have $G = S_X$. By Example A-5.24, $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$ is not a solvable group, and Theorem A-5.33 says that f is not solvable by radicals. •

Let E be a field and let $\mathrm{Aut}(E)$ be the group of all (field) automorphisms of E (see Exercise A-5.16 on page 222). If k is any subfield of E, then the Galois group $\mathrm{Gal}(E/k)$ is a subgroup of $\mathrm{Aut}(E)$, and so it acts on E. We have already seen several theorems about Galois groups whose hypothesis involves a normal extension E/k. It turns out that the way to understand normal extensions E/k is to examine them in the context of this action of $\mathrm{Gal}(E/k)$ on E and separability.

What elements of E are fixed by every σ in some subset H of $\mathrm{Aut}(E)$?

Definition. If E is a field and H is a subset[4] of $\mathrm{Aut}(E)$, then the ***fixed field*** of H is defined by

$$E^H = \{a \in E : \sigma(a) = a \text{ for all } \sigma \in H\}.$$

[4]The most important instance of a fixed field E^H arises when H is a subgroup of $\mathrm{Aut}(E)$, but we will meet cases in which it is merely a subset; for example, $H = \{\sigma\}$.

It is easy to see that if $\sigma \in \mathrm{Aut}(E)$, then $E^\sigma = \{a \in E : \sigma(a) = a\}$ is a subfield of E; in fact, $E^\sigma = E^{\langle\sigma\rangle}$ It follows that E^H is a subfield of E, for

$$E^H = \bigcap_{\sigma \in H} E^\sigma.$$

Example A-5.36. If k is a subfield of E and $G = \mathrm{Gal}(E/k)$, then $k \subseteq E^G$, but this inclusion can be strict. For example, let $E = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. If $\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$, then σ must fix $\mathbb{Q}$, and so it permutes the roots of $f(x) = x^3 - 2$. But the other two roots of f are not real, so that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Lemma A-5.2 gives $\sigma = 1_G$; that is, $E^G = E$. Note that E is not a splitting field of f. ◀

The proof of the following proposition is almost obvious.

Proposition A-5.37. *If E is a field, then the function from subsets of* $\mathrm{Aut}(E)$ *to subfields of E, given by $H \mapsto E^H$, is* ***order-reversing****: if $H \subseteq L \subseteq \mathrm{Aut}(E)$, then $E^L \subseteq E^H$.*

Proof. If $a \in E^L$, then $\sigma(a) = a$ for all $\sigma \in L$. Since $H \subseteq L$, it follows, in particular, that $\sigma(a) = a$ for all $\sigma \in H$. Hence, $E^L \subseteq E^H$. •

Our immediate goal is to determine the degree $[E : E^G]$, where $G \subseteq \mathrm{Aut}(E)$. To this end, we introduce the notion of characters.

Definition. A ***character***[5] of a group G in a field E is a (group) homomorphism $\sigma\colon G \to E^\times$, where $E^\times$ denotes the multiplicative group of nonzero elements of the field E.

If $\sigma \in \mathrm{Aut}(E)$, then its restriction $\sigma|E^\times\colon E^\times \to E^\times$ is a character in E. In particular, if k is a subfield of E, then every $\sigma \in \mathrm{Gal}(E/k)$ gives a character in E.

Definition. Let E be a field and let G be a group. A list $\sigma_1, \ldots, \sigma_n$ of characters of G in E is ***independent*** if, whenever $\sum_i c_i\sigma_i(x) = 0$, for $c_1, \ldots, c_n \in E$ and all $x \in G$, then all the $c_i = 0$.

In Example A-7.14(iii), we saw that the set V of all the functions from a set X to a field E is a vector space over E: addition of functions is defined by

$$\sigma + \tau\colon x \mapsto \sigma(x) + \tau(x),$$

and scalar multiplication is defined, for $c \in E$, by

$$c\sigma\colon x \mapsto c\sigma(x).$$

Independence of characters, as just defined, is linear independence in the vector space V when X is the group G.

[5] This definition gives a special case of *character* in representation theory: if $\sigma\colon G \to \mathrm{GL}(n, E)$ is a homomorphism, then its ***character*** $\chi_\sigma\colon G \to E$ is defined, for $x \in G$, by

$$\chi_\sigma(x) = \mathrm{tr}(\sigma(x)),$$

where the trace, $\mathrm{tr}(A)$, of an $n \times n$ matrix A is the sum of its diagonal entries. If $n = 1$, then $\mathrm{GL}(1, E) = E^\times$ and $\chi_\sigma(x) = \sigma(x)$ is called a ***linear character***.

Proposition A-5.38 (Dedekind). *Every list $\sigma_1, \dots, \sigma_n$ of distinct characters of a group G in a field E is independent.*

Proof. The proof is by induction on $n \geq 1$. The base step $n = 1$ is true, for if $c\sigma(x) = 0$ for all $x \in G$, then either $c = 0$ or $\sigma(x) = 0$; but $\sigma(x) \neq 0$, because $\operatorname{im}\sigma \subseteq E^\times = E - \{0\}$.

Assume that $n > 1$; if the characters are not independent, there are $c_i \in E$, not all zero, with

$$c_1\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(x) + c_n\sigma_n(x) = 0 \tag{9}$$

for all $x \in G$. We may assume that all $c_i \neq 0$, for if some $c_i = 0$, then the inductive hypothesis can be invoked to reach a contradiction. Multiplying by c_n^{-1} if necessary, we may assume that $c_n = 1$. Since $\sigma_n \neq \sigma_1$, there exists $y \in G$ with $\sigma_1(y) \neq \sigma_n(y)$. In Eq. (9), replace x by yx to obtain

$$c_1\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(y)\sigma_n(x) = 0,$$

for $\sigma_i(yx) = \sigma_i(y)\sigma_i(x)$. Now multiply this equation by $\sigma_n(y)^{-1}$ to obtain the equation

$$c_1\sigma_n(y)^{-1}\sigma_1(y)\sigma_1(x) + \cdots + c_{n-1}\sigma_n(y)^{-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(x) = 0.$$

Subtract this last equation from Eq. (9) to obtain a sum of $n - 1$ terms:

$$c_1\big[1 - \sigma_n(y)^{-1}\sigma_1(y)\big]\sigma_1(x) + c_2\big[1 - \sigma_n(y)^{-1}\sigma_2(y)\big]\sigma_2(x) + \cdots = 0.$$

By induction, each of the coefficients $c_i[1 - \sigma_n(y)^{-1}\sigma_i(y)] = 0$. Now $c_i \neq 0$, and so $\sigma_n(y)^{-1}\sigma_i(y) = 1$ for all $i < n$. In particular, $\sigma_n(y) = \sigma_1(y)$, contradicting the definition of y. •

Lemma A-5.39. *If $G = \{\sigma_1, \dots, \sigma_n\}$ is a set of n distinct automorphisms of a field E, then*

$$[E : E^G] \geq n.$$

Proof. Suppose, on the contrary, that $[E : E^G] = r < n$, and let $\alpha_1, \dots, \alpha_r$ be a basis of E/E^G. Consider the homogeneous linear system over E of r equations in n unknowns:

$$\begin{aligned}
\sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n &= 0,\\
\sigma_1(\alpha_2)x_1 + \cdots + \sigma_n(\alpha_2)x_n &= 0,\\
\vdots \qquad\quad \vdots \qquad\quad & \vdots\\
\sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n &= 0.
\end{aligned}$$

Since $r < n$, there are more unknowns than equations, and Corollary A-7.12 gives a nontrivial solution $(c_1, \dots, c_n)$ in E^n.

We are now going to show that $\sigma_1(\beta)c_1 + \cdots + \sigma_n(\beta)c_n = 0$ for every $\beta \in E^\times$, which will contradict the independence of the characters $\sigma_1|E^\times, \dots, \sigma_n|E^\times$. Since $\alpha_1, \dots, \alpha_r$ is a basis of E over E^G, each $\beta \in E$ can be written

$$\beta = \sum b_i\alpha_i,$$

where $b_i \in E^G$. Multiply the ith row of the system by $\sigma_1(b_i)$ to obtain the system with ith row

$$\sigma_1(b_i)\sigma_1(\alpha_i)c_1 + \cdots + \sigma_1(b_i)\sigma_n(\alpha_i)c_n = 0.$$

But $\sigma_1(b_i) = b_i = \sigma_j(b_i)$ for all i, j, because $b_i \in E^G$. Thus, the system has ith row

$$\sigma_1(b_i\alpha_i)c_1 + \cdots + \sigma_n(b_i\alpha_i)c_n = 0.$$

Adding all the rows gives

$$\sigma_1(\beta)c_1 + \cdots + \sigma_n(\beta)c_n = 0,$$

contradicting the independence of the characters. •

Proposition A-5.40. *If* $G = \{\sigma_1, \ldots, \sigma_n\}$ *is a subgroup of* $\mathrm{Aut}(E)$*, then*

$$[E : E^G] = |G|.$$

Proof. In light of Lemma A-5.39, it suffices to prove that $[E : E^G] \leq |G|$. If, on the contrary, $[E : E^G] > n$, there is a linearly independent list $\omega_1, \ldots, \omega_{n+1}$ of vectors in E over E^G. Consider the system of n equations in $n+1$ unknowns:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} &= 0, \\ \vdots \qquad\qquad & \quad \vdots \\ \sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} &= 0. \end{aligned}$$

Corollary A-7.12 gives nontrivial solutions over E, which we proceed to normalize. Choose a nontrivial solution $(\beta_1, \ldots, \beta_r, 0, \ldots, 0)$ having the smallest number r of nonzero components (by reindexing the ω_i, we may assume that all nonzero components come first). Note that $r \neq 1$, lest $\sigma_1(\omega_1)\beta_1 = 0$ imply $\beta_1 = 0$, contradicting $(\beta_1, 0, \ldots, 0)$ being nontrivial. Multiplying by its inverse if necessary, we may assume that $\beta_r = 1$. Not all $\beta_i \in E^G$, lest the row corresponding to $\sigma = 1_E$ violate the linear independence of $\omega_1, \ldots, \omega_{n+1}$. Our last assumption is that β_1 does not lie in E^G (this, too, can be accomplished by reindexing the ω_i); thus, there is some σ_k with $\sigma_k(\beta_1) \neq \beta_1$. Since $\beta_r = 1$, the original system has jth row (after renumbering the rows)

$$\sigma_j(\omega_1)\beta_1 + \cdots + \sigma_j(\omega_{r-1})\beta_{r-1} + \sigma_j(\omega_r) = 0. \tag{10}$$

Apply σ_k to this system to obtain

$$\sigma_k\sigma_j(\omega_1)\sigma_k(\beta_1) + \cdots + \sigma_k\sigma_j(\omega_{r-1})\sigma_k(\beta_{r-1}) + \sigma_k\sigma_j(\omega_r) = 0.$$

Since G is a group, $\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n$ is just a permutation of $\sigma_1, \ldots, \sigma_n$. Setting $\sigma_k\sigma_j = \sigma_i$, the system has ith row

$$\sigma_i(\omega_1)\sigma_k(\beta_1) + \cdots + \sigma_i(\omega_{r-1})\sigma_k(\beta_{r-1}) + \sigma_i(\omega_r) = 0.$$

Subtract this from the ith row of Eq. (10) to obtain a new system with ith row

$$\sigma_i(\omega_1)\big[\beta_1 - \sigma_k(\beta_1)\big] + \cdots + \sigma_i(\omega_{r-1})\big[\beta_{r-1} - \sigma_k(\beta_{r-1})\big] = 0.$$

Since $\beta_1 - \sigma_k(\beta_1) \neq 0$, we have found a nontrivial solution of the original system having fewer than r nonzero components, a contradiction. •

These ideas give a result needed in the proof of the Fundamental Theorem of Galois Theory.

Theorem A-5.41. *If G and H are finite subgroups of* $\mathrm{Aut}(E)$ *with* $E^G = E^H$, *then* $G = H$.

Proof. We first show that $\sigma \in \mathrm{Aut}(E)$ fixes E^G if and only if $\sigma \in G$. Clearly, σ fixes E^G if $\sigma \in G$. Suppose, conversely, that σ fixes E^G but $\sigma \notin G$. If $|G| = n$, then

$$n = |G| = [E : E^G],$$

by Proposition A-5.40. Since σ fixes E^G, we have $E^G \subseteq E^{G\cup\{\sigma\}}$. But the reverse inequality always holds, by Proposition A-5.37, so that $E^G = E^{G\cup\{\sigma\}}$. Hence,

$$n = [E : E^G] = [E : E^{G\cup\{\sigma\}}] \geq |G \cup \{\sigma\}| = n + 1,$$

by Lemma A-5.39, a contradiction.

If $\sigma \in H$, then σ fixes $E^H = E^G$, and hence $\sigma \in G$; that is, $H \subseteq G$; the reverse inclusion is proved the same way, and so $H = G$. •

Here is the characterization we have been seeking. Recall that a normal extension is a splitting field of some polynomial; we now characterize splitting fields of separable polynomials.

Theorem A-5.42. *If E/k is a finite extension field with Galois group $G = \mathrm{Gal}(E/k)$, then the following statements are equivalent.*

(i) *E is a splitting field of some separable polynomial $f(x) \in k[x]$.*

(ii) *$k = E^G$.*

(iii) *If a monic irreducible $p(x) \in k[x]$ has a root in E, then it is separable and splits in $E[x]$.*

Proof.

(i) $\Rightarrow$ (ii) By Theorem A-5.7(ii), $|G| = [E : k]$. But Proposition A-5.40 gives $|G| = [E : E^G]$; hence,

$$[E : k] = [E : E^G].$$

Since $k \subseteq E^G$, we have $[E : k] = [E : E^G][E^G : k]$, so that $[E^G : k] = 1$ and $k = E^G$.

(ii) $\Rightarrow$ (iii) Let $p(x) \in k[x]$ be a monic irreducible polynomial having a root α in E, and let the distinct elements of the set $\{\sigma(\alpha) \colon \sigma \in G\}$ be $\alpha_1, \ldots, \alpha_n$. Define $g(x) \in E[x]$ by

$$g(x) = \prod (x - \alpha_i).$$

Now each $\sigma \in G$ permutes the α_i, so that each σ fixes each of the coefficients of g (for they are elementary symmetric functions of the roots); that is, the coefficients of g lie in $E^G = k$. Hence, g is a polynomial in $k[x]$ which, by construction, has no repeated roots. Now p and g have a common root in E, and so their gcd in $E[x]$ is not 1, by Corollary A-3.72. Since p is irreducible, it must divide g. Therefore, p has no repeated roots; that is, p is separable. Finally, $g = p$, for they are monic polynomials of the same degree having the same roots. Hence, p splits in $E[x]$.

(iii) $\Rightarrow$ (i) Choose $\alpha_1 \in E$ with $\alpha_1 \notin k$. Since E/k is a finite extension field, α_1 must be algebraic over k; let $p_1(x) = \mathrm{irr}(\alpha_1, k) \in k[x]$ be its minimal polynomial. By hypothesis, p_1 is a separable polynomial that splits over E; let $K_1 \subseteq E$ be its splitting field. If $K_1 = E$, we are done. Otherwise, choose $\alpha_2 \in E$ with $\alpha_2 \notin K_1$. By hypothesis, there is a separable irreducible $p_2(x) \in k[x]$ having α_2 as a root that splits in $E[x]$. Let $K_2 \subseteq E$ be the splitting field of $p_1 p_2$, a separable polynomial in $k[x]$. If $K_2 = E$, we are done; otherwise, repeat this construction. This process must end with $K_m = E$ for some m because E/k is finite. Thus, E is a splitting field of the separable polynomial $p_1 \cdots p_m \in k[x]$. •

Definition. A finite extension field E/k is a ***Galois extension***[6] if it satisfies any of the equivalent conditions in Theorem A-5.42.

Example A-5.43. If B/k is a finite separable extension and E/B is the radical extension of B constructed in Lemma A-5.18, then Theorem A-5.42(i) shows that E/k is a Galois extension. ◄

Corollary A-5.44. *If E/k is a finite Galois extension and B is an* ***intermediate field*** *(that is, a subfield B with $k \subseteq B \subseteq E$), then E/B is a Galois extension.*

Proof. We know that E is a splitting field of some separable polynomial $f(x) \in k[x]$; that is, $E = k(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f. Since $k \subseteq B \subseteq E$, we have $E = B(\alpha_1, \ldots, \alpha_n)$, and $f \in B[x]$. •

We do not say that if E/k is a finite Galois extension and B/k is an intermediate field, then B/k is a Galois extension, for this may not be true. In Example A-5.11(iii), we saw that $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field of $x^3 - 2$ over $\mathbb{Q}$, where ω is a primitive cube root of unity, and so it is a Galois extension. However, the intermediate field $B = \mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension, for $x^3 - 2$ is an irreducible polynomial having a root in B, yet it does not split in $B[x]$.

The next proposition determines when an intermediate field B is a Galois extension.

Definition. Let E/k be a Galois extension and let B be an intermediate field. A ***conjugate*** of B is an intermediate field of the form

$$\sigma(B) = \{\sigma(b) : b \in B\}$$

for some $\sigma \in \mathrm{Gal}(E/k)$.

Proposition A-5.45. *If E/k is a finite Galois extension, then an intermediate field B is a Galois extension of k if and only if B has no conjugates other than B itself.*

Proof. Assume that $\sigma(B) = B$ for all $\sigma \in G$, where $G = \mathrm{Gal}(E/k)$. Let $p(x) \in k[x]$ be an irreducible polynomial having a root β in B. Since $B \subseteq E$ and E/k is Galois, $p(x)$ is a separable polynomial and it splits in $E[x]$. If $\beta' \in E$ is another root of $p(x)$, there exists an isomorphism $\sigma \in G$ with $\sigma(\beta) = \beta'$ (for G acts transitively

[6] Infinite extension fields may be Galois extensions; we shall define them in Course II.

on the roots of an irreducible polynomial, by Proposition A-5.14). Therefore, $\beta' = \sigma(\beta) \in \sigma(B) = B$, so that $p(x)$ splits in $B[x]$. Therefore, B/k is a Galois extension.

The converse follows from Theorem A-5.17: since B/k is a splitting field of some (separable) polynomial $f(x)$ over k, it is a normal extension. •

We have looked at symmetric polynomials of several variables; we now consider rational functions in several variables. In Example A-3.92, we considered $E = k(y_1, \ldots, y_n)$, the rational function field in n variables with coefficients in a field k, and its subfield $K = k(a_0, \ldots, a_{n-1})$, where

$$f(x) = (x - y_1)(x - y_2) \cdots (x - y_n) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

is the general polynomial of degree n over k. We saw that E is a splitting field of f over K, for it arises from K by adjoining to it all the roots of f, namely, $Y = \{y_1, \ldots, y_n\}$. Since every permutation of Y extends to an automorphism of E, by Theorem A-3.25, we may regard S_n as a subgroup of $\mathrm{Aut}(E)$. The elements of K are called the *symmetric functions* in n variables over k.

Definition. A rational function $g(y_1, \ldots, y_n)/h(y_1, \ldots, y_n) \in k(y_1, \ldots, y_n)$ is a ***symmetric function*** if it is unchanged by permuting its variables: for every $\sigma \in S_n$, we have $g(y_{\sigma 1}, \ldots, y_{\sigma n})/h(y_{\sigma 1}, \ldots, y_{\sigma n}) = g(y_1, \ldots, y_n)/h(y_1, \ldots, y_n)$.

The *elementary symmetric functions* are the *polynomials*, for $j = 1, \ldots, n$:

$$e_j(y_1, \ldots, y_n) = \sum_{i_1 < \cdots < i_j} y_{i_1} \cdots y_{i_j}.$$

We have seen that if a_j is the jth coefficient of the general polynomial of degree n, then $a_j = (-1)^j e_{n-j}(y_1, \ldots, y_n)$. We now prove that $K = k(e_1, \ldots, e_n) = E^{S_n}$.

Theorem A-5.46 (Fundamental Theorem of Symmetric Functions). *If k is a field, every symmetric function in $k(y_1, \ldots, y_n)$ is a rational function in the elementary symmetric functions $e_1, \ldots, e_n$.*

Proof. Let $K = k(e_1, \ldots, e_n) \subseteq E = k(y_1, \ldots, y_n)$. As we saw in Example A-3.92, E is the splitting field of the general polynomial $f(x)$ of degree n:

$$f(x) = \prod_{i=1}^{n} (x - y_i).$$

As f is a separable polynomial, E/K is a Galois extension. We saw, in the proof of the Abel–Ruffini Theorem, that $\mathrm{Gal}(E/K) \cong S_n$. Therefore, $E^{S_n} = K$, by Theorem A-5.42. But $g(y_1, \ldots, y_n)/h(y_1, \ldots, y_n) \in E^{S_n}$ if and only if it is unchanged by permuting its variables; that is, it is a symmetric function. •

There is a useful variation of Theorem A-5.46. The ***Fundamental Theorem of Symmetric Polynomials*** says that every symmetric *polynomial* $f \in k[x_1, \ldots, x_n]$ lies in $k[e_1, \ldots, e_n]$; that is, f is a polynomial (not merely a rational function) in the elementary symmetric functions. There is a proof of this in van der Waerden [**118**], pp. 78–81, but we think it is more natural to prove it using the Division Algorithm for polynomials in several variables (in Course II).

Definition. If A and B are subfields of a field E, then their ***compositum***, denoted by

$$A \vee B,$$

is the intersection of all the subfields of E containing $A \cup B$.

It is easy to see that $A \vee B$ is the smallest subfield of E containing both A and B. For example, if E/k is an extension field with intermediate fields $A = k(\alpha_1, \ldots, \alpha_n)$ and $B = k(\beta_1, \ldots, \beta_m)$, then their compositum is

$$k(\alpha_1, \ldots, \alpha_n) \vee k(\beta_1, \ldots, \beta_m) = k(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m).$$

Proposition A-5.47.

(i) *Every finite Galois extension is separable.*

(ii) *If E/k is a (not necessarily finite) algebraic extension and $S \subseteq E$ is a (possibly infinite) set of separable elements, then $k(S)/k$ is separable.*

(iii) *Let E/k be a (not necessarily finite) algebraic extension, where k is a field, and let A and B be intermediate fields. If both A/k and B/k are separable, then their compositum $A \vee B$ is also a separable extension of k.*

Proof.

(i) If $\beta \in E$, then $p(x) = \mathrm{irr}(\beta, k) \in k[x]$ is an irreducible polynomial in $k[x]$ having a root in E. By Theorem A-5.42(iii), p is a separable polynomial (which splits in $E[x]$). Therefore, β is separable over k, and E/k is separable.

(ii) Let us first consider the case when S is finite; that is, $B = k(\alpha_1, \ldots, \alpha_t)$ is a finite extension field, where each α_i is separable over k. By Lemma A-5.18(i), there is an extension field E/B that is a splitting field of some separable polynomial $f(x) \in k[x]$; hence, E/k is a Galois extension, by Theorem A-5.42(i). By part (i), E/k is separable; that is, for all $\alpha \in E$, the polynomial $\mathrm{irr}(\alpha, k)$ has no repeated roots. In particular, $\mathrm{irr}(\alpha, k)$ has no repeated roots for all $\alpha \in B$, and so B/k is separable.

We now consider the general case. If $\alpha \in k(S)$, then Exercise A-3.81 on page 89 says that there are finitely many elements $\alpha_1, \ldots, \alpha_n \in S$ with $\alpha \in B = k(\alpha_1, \ldots, \alpha_n)$. As we have just seen, B/k is separable, and so α is separable over k. As α is an arbitrary element of $k(S)$, it follows that $k(S)/k$ is separable.

(iii) Apply part (ii) to the subset $S = A \cup B$, for $A \vee B = k(A \cup B)$. •

We are now going to show, when E/k is a finite Galois extension, that the intermediate fields are classified by the subgroups of $\mathrm{Gal}(E/k)$.

We begin with some general definitions.

Definition. A set X is a ***partially ordered set*** if it has a binary relation $x \preceq y$ defined on it that satisfies, for all $x, y, z \in X$,

(i) *Reflexivity*: $x \preceq x$;

(ii) *Antisymmetry*: if $x \preceq y$, and $y \preceq x$, then $x = y$;

(iii) *Transitivity*: if $x \preceq y$ and $y \preceq z$, then $x \preceq z$.

An element c in a partially ordered set X is an ***upper bound*** of a pair $a, b \in X$ if $a \preceq c$ and $b \preceq c$; an element $d \in X$ is a ***least upper bound*** of a, b if d is an upper bound and $d \preceq c$ for every upper bound c of a and b. ***Lower bounds*** and ***greatest lower bounds*** are defined similarly, everywhere reversing the inequalities.

We shall return to partially ordered sets in Course II when we discuss Zorn's Lemma, inverse limits, and direct limits. Here, we are more interested in special partially ordered sets called *lattices*.

Definition. A ***lattice*** is a partially ordered set $\mathcal{L}$ in which every pair of elements $a, b \in \mathcal{L}$ has a greatest lower bound $a \wedge b$ and a least upper bound $a \vee b$.

Example A-5.48.

(i) If U is a set, define $\mathcal{L}$ to be the family of all the subsets of U, and define a partial order $A \preceq B$ by $A \subseteq B$. Then $\mathcal{L}$ is a lattice, where $A \wedge B = A \cap B$ and $A \vee B = A \cup B$.

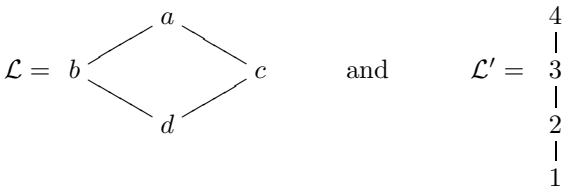
(ii) If G is a group, define $\mathcal{L} = \mathrm{Sub}(G)$ to be the family of all the subgroups of G, and define $A \preceq B$ to mean $A \subseteq B$; that is, A is a subgroup of B. Then $\mathcal{L}$ is a lattice, where $A \wedge B = A \cap B$ and $A \vee B$ is the subgroup generated by $A \cup B$.

(iii) If E/k is an extension field, define $\mathcal{L} = \mathrm{Int}(E/k)$ to be the family of all the intermediate fields, and define $K \preceq B$ to mean $K \subseteq B$; that is, K is a subfield of B. Then $\mathcal{L}$ is a lattice, where $A \wedge B = A \cap B$ and $A \vee B$ is the compositum of A and B.

(iv) If n is a positive integer, define $\mathrm{Div}(n)$ to be the set of all the positive divisors of n. Then $\mathrm{Div}(n)$ is a partially ordered set if one defines $d \preceq d'$ to mean $d \mid d'$. Here, $d \wedge d' = \gcd(d, d')$ and $d \vee d' = \mathrm{lcm}(d, d')$. ◀

Definition. Let $\mathcal{L}$ and $\mathcal{L}'$ be partially ordered sets. A function $f\colon \mathcal{L} \to \mathcal{L}'$ is called ***order-reversing*** if $a \preceq b$ in $\mathcal{L}$ implies $f(b) \preceq f(a)$ in $\mathcal{L}'$.

Example A-5.49. There exist lattices $\mathcal{L}$ and $\mathcal{L}'$ and an order-reversing bijection $\varphi\colon \mathcal{L} \to \mathcal{L}'$ whose inverse $\varphi^{-1}\colon \mathcal{L}' \to \mathcal{L}$ is not order-reversing. For example, consider the lattices



The bijection $\varphi\colon \mathcal{L} \to \mathcal{L}'$, defined by

$$\varphi(a) = 1, \quad \varphi(b) = 2, \quad \varphi(c) = 3, \quad \varphi(d) = 4,$$

is an order-reversing bijection, but its inverse $\varphi^{-1}\colon \mathcal{L}' \to \mathcal{L}$ is not order-reversing, because $2 \preceq 3$ but $c = \varphi^{-1}(3) \not\preceq \varphi^{-1}(2) = b$. ◀

The De Morgan laws say that if A and B are subsets of a set X, then

$$(A \cap B)' = A' \cup B' \quad \text{and} \quad (A \cup B)' = A' \cap B',$$

where A' denotes the complement of A. These identities are generalized in the next lemma.

Lemma A-5.50. *Let $\mathcal{L}$ and $\mathcal{L}'$ be lattices, and let $\varphi\colon \mathcal{L} \to \mathcal{L}'$ be a bijection such that both φ and φ^{-1} are order-reversing. Then*

$$\varphi(a \wedge b) = \varphi(a) \vee \varphi(b) \quad \textit{and} \quad \varphi(a \vee b) = \varphi(a) \wedge \varphi(b).$$

Proof. Since $a, b \preceq a \vee b$, we have $\varphi(a \vee b) \preceq \varphi(a), \varphi(b)$; that is, $\varphi(a \vee b)$ is a lower bound of $\varphi(a), \varphi(b)$. It follows that $\varphi(a \vee b) \preceq \varphi(a) \wedge \varphi(b)$.

For the reverse inequality, surjectivity of φ gives $c \in \mathcal{L}$ with $\varphi(a) \wedge \varphi(b) = \varphi(c)$. Now $\varphi(c) = \varphi(a) \wedge \varphi(b) \preceq \varphi(a), \varphi(b)$. Applying φ^{-1}, which is also order-reversing, we have $a, b \preceq c$. Hence, c is an upper bound of a, b, so that $a \vee b \preceq c$. Therefore, $\varphi(a \vee b) \succeq \varphi(c) = \varphi(a) \wedge \varphi(b)$. A similar argument proves the other half of the statement. •

Recall Example A-5.48: if G is a group, then $\mathrm{Sub}(G)$ is the lattice of all its subgroups and, if E/k is an extension field, then $\mathrm{Int}(E/k)$ is the lattice of all the intermediate fields.

Theorem A-5.51 (Fundamental Theorem of Galois Theory). *Let E/k be a finite*[7] *Galois extension with Galois group $G = \mathrm{Gal}(E/k)$.*

(i) *The function $\gamma\colon \mathrm{Sub}(\mathrm{Gal}(E/k)) \to \mathrm{Int}(E/k)$, defined by*

$$\gamma\colon H \mapsto E^H,$$

is an order-reversing bijection whose inverse,

$$\delta\colon \mathrm{Int}(E/k) \to \mathrm{Sub}(\mathrm{Gal}(E/k)),$$

is the order-reversing bijection

$$\delta\colon B \mapsto \mathrm{Gal}(E/B).$$

(ii) *For every $B \in \mathrm{Int}(E/k)$ and $H \in \mathrm{Sub}(\mathrm{Gal}(E/k))$,*

$$E^{\mathrm{Gal}(E/B)} = B \quad \textit{and} \quad \mathrm{Gal}(E/E^H) = H.$$

(iii) *For every $H, K \in \mathrm{Sub}(\mathrm{Gal}(E/k))$ and $A, B \in \mathrm{Int}(E/k)$,*

$$E^{H \vee K} = E^H \cap E^K,$$
$$E^{H \cap K} = E^H \vee E^K,$$
$$\mathrm{Gal}(E/(A \vee B)) = \mathrm{Gal}(E/A) \cap \mathrm{Gal}(E/B),$$
$$\mathrm{Gal}(E/(A \cap B)) = \mathrm{Gal}(E/A) \vee \mathrm{Gal}(E/B).$$

(iv) *For every $B \in \mathrm{Int}(E/k)$ and $H \in \mathrm{Sub}(\mathrm{Gal}(E/k))$,*

$$[B : k] = [G : \mathrm{Gal}(E/B)] \quad \textit{and} \quad [G : H] = [E^H : k].$$

[7] There is a generalization to infinite Galois extensions in Course II.

(v) *If* $B \in \mathrm{Int}(E/k)$*, then* B/k *is a Galois extension if and only if* $\mathrm{Gal}(E/B)$ *is a normal subgroup of* G*.*

Proof.

(i) Proposition A-5.37 proves that γ is order-reversing, and it is also easy to prove that δ is order-reversing. Now injectivity of γ is proved in Theorem A-5.41, so that it suffices to prove that $\gamma\delta\colon \mathrm{Int}(E/k) \to \mathrm{Int}(E/k)$ is the identity;[8] it will follow that γ is a bijection with inverse δ. If B is an intermediate field, then $\delta\gamma\colon B \mapsto E^{\mathrm{Gal}(E/B)}$. But E/E^B is a Galois extension, by Corollary A-5.44, and so $E^{\mathrm{Gal}(E/B)} = B$, by Theorem A-5.42.

(ii) This is just the statement that $\gamma\delta$ and $\delta\gamma$ are identity functions.

(iii) These statements follow from Lemma A-5.50.

(iv) By Theorem A-5.7(ii) and the fact that E/B is a Galois extension,

$$[B : k] = [E : k]/[E : B] = |G|/|\,\mathrm{Gal}(E/B)| = [G : \mathrm{Gal}(E/B)].$$

Thus, the degree of B/k is the index of its Galois group in G. The second equation follows from this one; take $B = E^H$, noting that (ii) gives $\mathrm{Gal}(E/E^H) = H$:

$$[E^H : k] = [G : \mathrm{Gal}(E/E^H)] = [G : H].$$

(v) It follows from Theorem A-5.17 that $\mathrm{Gal}(E/B) \lhd G$ when B/k is a Galois extension (both B/k and E/k are normal extensions). For the converse, let $H = \mathrm{Gal}(E/B)$, and assume that $H \lhd G$. Now $E^H = E^{\mathrm{Gal}(E/B)} = B$, by (ii), and so it suffices to prove that $\sigma(E^H) = E^H$ for every $\sigma \in G$, by Proposition A-5.45. Suppose now that $a \in E^H$; that is, $\eta(a) = a$ for all $\eta \in H$. If $\sigma \in G$, then we must show that $\eta(\sigma(a)) = \sigma(a)$ for all $\eta \in H$; that is, $\sigma(a) \in E^H$. Now $H \lhd G$ says that if $\eta \in H$ and $\sigma \in G$, then there is $\eta' \in H$ with $\eta\sigma = \sigma\eta'$ (of course, $\eta' = \sigma^{-1}\eta\sigma$). But

$$\eta\sigma(a) = \sigma\eta'(a) = \sigma(a),$$

because $\eta'(a) = a$, as desired. Therefore, $B/k = E^H/k$ is Galois. •

Example A-5.52. We use our discussion of $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ in Example A-5.16 to illustrate the Fundamental Theorem. The roots of $f(x)$ are $\alpha_1 = \beta$, $\alpha_2 = \omega\beta$, and $\alpha_3 = \omega^2\beta$, where $\beta = \sqrt[3]{2}$ and ω is a primitive cube root of unity. By Example A-5.11(iii), the splitting field is $E = \mathbb{Q}(\beta, \omega)$ and $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

Figure A-5.2 shows the lattice of subgroups of $\mathrm{Gal}(E/\mathbb{Q})$: σ_{ij} denotes the automorphism that interchanges α_i, α_j, where $i, j \in \{1, 2, 3\}$, and fixes the other root; τ denotes the automorphism sending $\alpha_1 \mapsto \alpha_2$, $\alpha_2 \mapsto \alpha_3$, and $\alpha_3 \mapsto \alpha_1$. Figure A-5.3 shows the lattice of intermediate fields (without the Fundamental Theorem, it would not be obvious that these are the only such).

We compute fixed fields. If $\sigma = \sigma_{12}$, what is $E^{\langle\sigma\rangle}$? Now

$$\sigma(\alpha_1) = \sigma(\beta) = \omega\beta \quad \text{and} \quad \sigma(\alpha_2) = \sigma(\omega\beta) = \beta.$$

[8] If $f\colon X \to Y$ and $g\colon Y \to X$, then $gf = 1_X$ implies that g is surjective and f is injective.

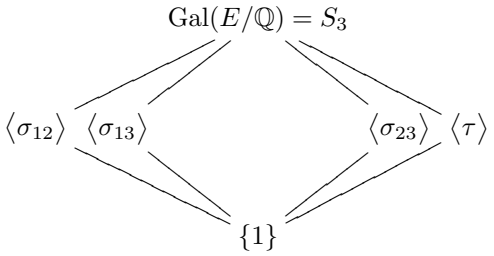


Figure A-5.2. Sub(Gal($E/\mathbb{Q}$)).

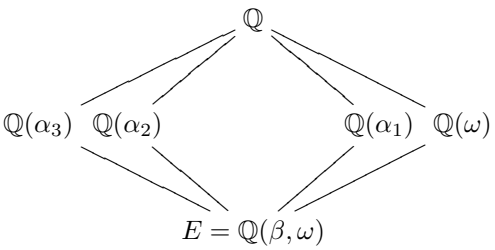


Figure A-5.3. Sub(Gal($E/\mathbb{Q}$)) and Int($E/\mathbb{Q}$).

Hence,

$$\sigma(\alpha_2/\alpha_1) = \sigma(\omega\beta/\beta) = \sigma(\omega).$$

On the other hand,

$$\sigma(\alpha_2/\alpha_1) = \sigma(\alpha_2)/\sigma(\alpha_1) = \beta/\omega\beta = \omega^2.$$

Therefore, $\sigma(\omega) = \omega^2$, so that $\omega \notin E^{\langle\sigma\rangle}$. Since the only candidates for $E^{\langle\sigma\rangle}$ are $\mathbb{Q}(\alpha_3)$, $\mathbb{Q}(\alpha_2)$, $\mathbb{Q}(\alpha_1)$, and $\mathbb{Q}(\omega)$, we conclude that $E^{\langle\sigma\rangle} = \mathbb{Q}(\alpha_3)$.

What is $E^{\langle\tau\rangle}$? We note that it contains no root α_i, for τ moves each of them. On the other hand,

$$\sigma(\omega) = \sigma(\alpha_2/\alpha_1) = \sigma(\alpha_2)/\sigma(\alpha_1) = \omega^2\beta/\omega\beta = \omega,$$

so that $\omega \in E^{\langle\tau\rangle}$. Thus, $E^{\langle\tau\rangle} = \mathbb{Q}(\omega)$, for it is not any of the other intermediate fields . Note, as the Fundamental Theorem predicts, that $\mathbb{Q}(\omega)/\mathbb{Q}$ is a normal extension, for it corresponds to the normal subgroup $\langle\tau\rangle$ of Gal($E/\mathbb{Q}$); that is, $A_3 \lhd S_3$ (of course, $\mathbb{Q}(\omega)/\mathbb{Q}$ is the splitting field of $x^3 - 1$). ◀

Here are some corollaries.

Theorem A-5.53. *If E/k is a finite Galois extension whose Galois group is abelian, then every intermediate field is a Galois extension.*

Proof. Every subgroup of an abelian group is a normal subgroup. •

Corollary A-5.54. *A finite Galois extension E/k has only finitely many intermediate fields.*

Proof. The finite group $\mathrm{Gal}(E/k)$ has only finitely many subgroups. •

Definition. An extension field E/k is a ***simple extension*** if there is $u \in E$ with $E = k(u)$.

The following theorem characterizes simple extensions.

Theorem A-5.55 (Steinitz). *A finite extension field E/k is simple if and only if it has only finitely many intermediate fields.*

Proof. Assume that E/k is a simple extension, so that $E = k(u)$; let $p(x) = \mathrm{irr}(u, k) \in k[x]$ be its minimal polynomial. If B is any intermediate field, let

$$q(x) = \mathrm{irr}(u, B) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n \in B[x]$$

be the minimal polynomial of u over B, and define

$$B' = k(b_0, \ldots, b_{n-1}) \subseteq B.$$

Note that q is an irreducible polynomial over the smaller field B'. Now

$$E = k(u) \subseteq B'(u) \subseteq B(u) \subseteq E,$$

so that $B'(u) = E = B(u)$. Hence, $[E : B] = [B(u) : B]$ and $[E : B'] = [B'(u) : B']$. But each of these is equal to $\deg(q)$, by Proposition A-3.84(v), so that $[E : B] = \deg(q) = [E : B']$. Since $B' \subseteq B$, it follows that $[B : B'] = 1$; that is,

$$B = B' = k(b_0, \ldots, b_{n-1}).$$

We have characterized B in terms of the coefficients of q, a monic divisor of $p(x) = \mathrm{irr}(u, k)$ in $E[x]$. But p has only finitely many monic divisors, and hence there are only finitely many intermediate fields.

Conversely, assume that E/k has only finitely many intermediate fields. If k is a finite field, then we know that E/k is a simple extension (take u to be a primitive element); therefore, we may assume that k is infinite. Since E/k is a finite extension field, there are elements $u_1, \ldots, u_n$ with $E = k(u_1, \ldots, u_n)$. By induction on $n \geq 1$, it suffices to prove that $E = k(u, v)$ is a simple extension. Now there are infinitely many elements $c \in E$ of the form $c = u + tv$, where $t \in k$, for k is now infinite. Since there are only finitely many intermediate fields, there are, in particular, only finitely many fields of the form $k(c)$. By the Pigeonhole Principle, there exist distinct $t, t' \in k$ with $k(c) = k(c')$, where $c' = u + t'v$. Clearly, $k(c) \subseteq k(u, v)$. For the reverse inclusion, the field $k(c) = k(c')$ contains $c - c' = (t - t')v$, so that $v \in k(c)$ (because $t - t' \in k$ and $t - t' \neq 0$). Hence, $u = c - tv \in k(c)$, and so $k(c) = k(u, v)$. •

An immediate consequence is that every Galois extension is simple; in fact, even more is true.

Theorem A-5.56 (Theorem of the Primitive Element). *If B/k is a finite separable extension, then there is $u \in B$ with $B = k(u)$.*

In particular, if k has characteristic 0, then every finite extension field B/k is a simple extension.

Proof. By Example A-5.43, the radical extension E/k constructed in Lemma A-5.18 is a Galois extension having B as an intermediate field, so that Corollary A-5.54 says that the extension field E/k has only finitely many intermediate fields. It follows at once that the extension field B/k has only finitely many intermediate fields, and so Steinitz's Theorem says that B/k has a primitive element. •

The Theorem of the Primitive Element was known to Lagrange, and Galois used a modification of it to construct the original version of the Galois group.

We now turn to finite fields.

Theorem A-5.57. *The finite field $\mathbb{F}_q$, where $q = p^n$, has exactly one subfield of order p^d for every divisor d of n, and no others.*

Proof. First, $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension, for it is a splitting field of the separable polynomial $x^q - x$ (all the roots of $x^q - x$ are distinct). Now $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic of order n, by Theorem A-5.13. Since a cyclic group of order n has exactly one subgroup of order d for every divisor d of n, by Lemma A-4.89, it follows that G has exactly one subgroup H of index n/d. Therefore, there is only one intermediate field, namely, E^H, with $[E^H : \mathbb{F}_p] = [G : H] = n/d$, and $E^H = \mathbb{F}_{p^{n/d}}$. •

The Fundamental Theorem of Algebra was first proved by Gauss in 1799. Here is an algebraic proof which uses the Fundamental Theorem of Galois Theory as well as a two group theoretic results we will prove in Part 2: If p^k is the largest power of a prime p dividing the order of a finite group G, then G contains a subgroup of order p^k (this is one of the Sylow Theorems); Every group of order p^k contains a subgroup of order p^d for every $d \leq k$.

We assume only that $\mathbb{R}$ satisfies a weak form of the Intermediate Value Theorem: If $f(x) \in \mathbb{R}[x]$ and there exist $a, b \in \mathbb{R}$ such that $f(a) > 0$ and $f(b) < 0$, then f has a real root.

(i) *Every positive real number r has a real square root.*
If $f(x) = x^2 - r$, then $f(1 + r) = (1 + r)^2 - r = 1 + r + r^2 > 0$, and $f(0) = -r < 0$.

(ii) *Every quadratic $g(x) \in \mathbb{C}[x]$ has a complex root.*
First, every complex number z has a complex square root: when z is written in polar form $z = re^{i\theta}$, where $r \geq 0$, then $\sqrt{z} = \sqrt{r}e^{i\theta/2}$. The quadratic formula gives the (complex) roots of g.

(iii) *The field $\mathbb{C}$ has no extension fields of degree* 2.
Such an extension field would contain an element whose minimal polynomial is an irreducible quadratic in $\mathbb{C}[x]$; but item (ii) shows that no such polynomial exists.

(iv) *Every $f(x) \in \mathbb{R}[x]$ having odd degree has a real root.*
Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{R}[x]$. Define $t = 1 + \sum |a_i|$. Now $|a_i| \leq t - 1$ for all i and, if $h(x) = f(x) - x^n$, then $|h(t)| < t^n$:

$$\begin{aligned} |h(t)| &= \left|a_0 + a_1t + \cdots + a_{n-1}t^{n-1}\right| \\ &\leq (t-1)\left(1 + t + \cdots + t^{n-1}\right) = t^n - 1 < t^n. \end{aligned}$$

Therefore, $-t^n < -|h(t)| \le h(t)$ and $0 = -t^n + t^n < h(t) + t^n = f(t)$. A similar argument shows that $|h(-t)| < t^n$, so that

$$f(-t) = h(-t) + (-t)^n < t^n + (-t)^n.$$

When n is odd, $(-t)^n = -t^n$, and so $f(-t) < t^n - t^n = 0$. Therefore, the Intermediate Value Theorem provides a real number $r \in (-t, t)$ with $f(r) = 0$; that is, f has a real root.

(v) *There is no extension field $E/\mathbb{R}$ of odd degree > 1.*

If $u \in E$, then its minimal polynomial $\mathrm{irr}(u, \mathbb{R})$ must have even degree, by item (iv), so that $[\mathbb{R}(u) : \mathbb{R}]$ is even. Hence $[E : \mathbb{R}] = [E : \mathbb{R}(u)][\mathbb{R}(u) : \mathbb{R}]$ is even.

Theorem A-5.58 (Fundamental Theorem of Algebra). *Every nonconstant $f(x)$ in $\mathbb{C}[x]$ has a complex root.*

Proof. If $g(x) = \sum a_i x^i \in \mathbb{C}[x]$, define $\overline{g}(x) = \sum \overline{a}_i x^i$, where $\overline{a}_i$ is the complex conjugate of a_i. Now $g\overline{g} = \sum c_k x^k$, where $c_k = \sum_{i+j=k} a_i \overline{a}_j$; hence, $\overline{c}_k = c_k$ and $g\overline{g} \in \mathbb{R}[x]$. We claim that if $g\overline{g}$ has a (complex) root, say z, then g must have a root. Since $g(z)\overline{g}(z) = 0$, either $g(z) = 0$ and z is a root of g, or $\overline{g}(z) = 0$. In the latter case, z is a root of $\overline{g}$, and so $\overline{z}$ is a root of g. In either event, g has a root.

It now suffices to prove that every nonconstant monic polynomial $f(x)$ with real coefficients has a complex root. Let $E/\mathbb{R}$ be a splitting field of $(x^2 + 1)f(x)$; of course, $\mathbb{C}$ is an intermediate field. Since $\mathbb{R}$ has characteristic 0, $E/\mathbb{R}$ is a Galois extension; let $G = \mathrm{Gal}(E/\mathbb{R})$ be its Galois group. Now $|G| = 2^m \ell$, where $m \ge 0$ and ℓ is odd. By the Sylow Theorem quoted above, G has a subgroup H of order 2^m; let $B = E^H$ be the corresponding intermediate field. By the Fundamental Theorem of Galois Theory, the degree $[B : \mathbb{R}]$ is equal to the index $[G : H] = \ell$. But we have seen, in item (v), that $\mathbb{R}$ has no extension field of odd degree greater than 1; hence $\ell = 1$ and G is a 2-group (that is, $|G|$ is a power of 2). Now $E/\mathbb{C}$ is also a Galois extension, and $\mathrm{Gal}(E/\mathbb{C}) \subseteq G$ is also a 2-group. If this group is nontrivial, then it has a subgroup K of index 2. By the Fundamental Theorem once again, the intermediate field E^K is an extension field of $\mathbb{C}$ of degree 2, contradicting item (iii). We conclude that $[E : \mathbb{C}] = 1$; that is, $E = \mathbb{C}$. But E is a splitting field of f over $\mathbb{C}$, and so f has a complex root. •

We now prove the converse of Galois's Theorem (which holds only in characteristic 0): if the Galois group of a polynomial $f(x)$ is solvable, then $f(x)$ is solvable by radicals. In order to prove that certain extension fields are pure extensions, we will use the *norm*.

Definition. If E/k is a Galois extension and $u \in E^\times$, the nonzero elements of E, define the ***norm*** $N\colon E^\times \to E^\times$ by

$$N(u) = \prod_{\sigma \in \mathrm{Gal}(E/k)} \sigma(u).$$

For example, if $E = \mathbb{Q}(i)$, then $\mathrm{Gal}(E/\mathbb{Q}) = \langle \tau \rangle$, where $\tau\colon z \mapsto \overline{z}$ is complex conjugation, and $N(u) = z\overline{z}$.

Here are some preliminary properties of the norm, whose simple proofs are left to the reader.

(i) If $u \in E^\times$, then $N(u) \in k^\times$ (because $N(u) \in E^G = k$).

(ii) $N(uv) = N(u)N(v)$, so that $N\colon E^\times \to k^\times$ is a homomorphism.

(iii) If $a \in k^\times \subseteq E^\times$, then $N(a) = a^n$, where $n = [E\colon k]$.

(iv) If $\sigma \in G$ and $u \in E^\times$, then $N(\sigma(u)) = N(u)$.

Given a homomorphism, we always ask about its kernel and image. The image of the norm is not easy to compute; the next result (which was the ninetieth theorem in Hilbert's 1897 exposition of algebraic number theory) computes the kernel of the norm in a special case.

Theorem A-5.59 (Hilbert's Theorem 90). *Let E/k be a Galois extension whose Galois group $G = \mathrm{Gal}(E/k)$ is cyclic of order n, say, with generator σ. If $u \in E^\times$, then $N(u) = 1$ if and only if there exists $v \in E^\times$ with $u = v\sigma(v)^{-1}$.*

Proof. If $u = v\sigma(v)^{-1}$, then

$$N(u) = N(v\sigma(v)^{-1}) = N(v)N(\sigma(v)^{-1}) = N(v)N(\sigma(v))^{-1} = N(v)N(v)^{-1} = 1.$$

Conversely, let $N(u) = 1$. Define "partial norms" in $E^\times$:

$$\begin{aligned}
\delta_0 &= u,\\
\delta_1 &= u\sigma(u),\\
\delta_2 &= u\sigma(u)\sigma^2(u),\\
&\vdots\\
\delta_{n-1} &= u\sigma(u)\cdots\sigma^{n-1}(u).
\end{aligned}$$

Note that $\delta_{n-1} = N(u) = 1$. It is easy to see that

$$u\sigma(\delta_i) = \delta_{i+1} \text{ for all } 0 \le i \le n-2. \tag{11}$$

By independence of the characters $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$, there exists $y \in E$ with

$$\delta_0 y + \delta_1\sigma(y) + \cdots + \delta_{n-2}\sigma^{n-2}(y) + \sigma^{n-1}(y) \neq 0;$$

call this sum v. Using Eq. (11), we easily check that

$$\begin{aligned}
\sigma(v) &= \sigma(\delta_0)\sigma(y) + \sigma(\delta_1)\sigma^2(y) + \cdots + \sigma(\delta_{n-2})\sigma^{n-1}(y) + \sigma^n(y)\\
&= u^{-1}\delta_1\sigma(y) + u^{-1}\delta_2\sigma^2(y) + \cdots + u^{-1}\delta_{n-1}\sigma^{n-1}(y) + y\\
&= u^{-1}\Big(\delta_1\sigma(y) + \delta_2\sigma^2(y) + \cdots + \delta_{n-1}\sigma^{n-1}(y)\Big) + u^{-1}\delta_0 y\\
&= u^{-1}v.
\end{aligned}$$

Hence, $\sigma(v) = u^{-1}v$ and $u = v/\sigma(v)$. •

Corollary A-5.60. *Let E/k be a Galois extension of prime degree p. If k contains a primitive pth root of unity ω, then $E = k(z)$, where $z^p \in k$, and so E/k is a pure extension of type p.*

Proof. The Galois group $G = \mathrm{Gal}(E/k)$ has order p, hence is cyclic; let σ be a generator. Observe that $N(\omega) = \omega^p = 1$, because $\omega \in k$. By Hilbert's Theorem 90, we have $\omega = z\sigma(z)^{-1}$ for some $z \in E$. Hence $\sigma(z) = \omega^{-1}z$. Thus, $\sigma(z^p) = (\omega^{-1}z)^p = z^p$, and so $z^p \in E^G$, because σ generates G; since E/k is Galois, however, we have $E^G = k$, so that $z^p \in k$. Note that $z \notin k$, lest $\omega = 1$, so that $k(z) \neq k$ is an intermediate field. Therefore $E = k(z)$, because $[E : k] = p$ is prime, and hence E has no proper intermediate fields. •

We confess that we have presented Hilbert's Theorem 90 not only because of its corollary, which will be used to prove Galois's theorem below, but also because it is a well-known result that is an early instance of homological algebra.

Here is an elegant proof of Corollary A-5.60 which does not use Hilbert's Theorem 90.

Proposition A-5.61 (= Corollary A-5.60). *Let E/k be a Galois extension of prime degree p. If k contains a primitive pth root of unity ω, then $E = k(z)$, where $z^p \in k$, and so E/k is a pure extension of type p.*

Proof (Houston). Since E/k is a Galois extension of degree p, its Galois group $G = \mathrm{Gal}(E/k)$ has order p, and hence it is cyclic: $G = \langle\sigma\rangle$. We view $\sigma\colon E \to E$ as a linear transformation. Now σ satisfies the polynomial $x^p - 1$, because $\sigma^p = 1_E$, by Lagrange's Theorem. But σ satisfies no polynomial of smaller degree, lest we contradict independence of the characters $1, \sigma, \sigma^2, \ldots, \sigma^{p-1}$. Therefore, $x^p - 1$ is the minimal polynomial of σ, and so every pth root of unity is an eigenvalue of σ. Since $\omega^{-1} \in E$, by hypothesis, there is some eigenvector $z \in E$ of σ with $\sigma(z) = \omega^{-1}z$ (note that $z \notin k$ because it is not fixed by σ). Hence, $\sigma(z^p) = (\sigma(z))^p = (\omega^{-1})^p z^p = z^p$, from which it follows that $z^p \in E^G = k$. Now $p = [E : k] = [E : k(z)][k(z) : k]$; since p is prime and $[k(z) : k] \neq 1$, we have $[E : k(z)] = 1$; that is, $E = k(z)$, and so E/k is a pure extension. •

Theorem A-5.62 (Galois). *Let k be a field of characteristic 0, let E/k be a Galois extension, and let $G = \mathrm{Gal}(E/k)$ be a solvable group. Then E can be imbedded in a radical extension of k.*

Proof. Since G is solvable, Exercise A-5.9 on page 200 says that it has a normal subgroup H of prime index, say, p. Let ω be a primitive pth root of unity, which exists in some extension field because k has characteristic 0.

Case (i): $\omega \in k$. We prove the statement by induction on $[E : k]$. The base step is obviously true, for $k = E$ is a radical extension of itself. For the inductive step, consider the intermediate field E^H. Now E/E^H is a Galois extension, by Corollary A-5.44, and $H = \mathrm{Gal}(E/E^H)$ is solvable, being a subgroup of the solvable group G. Since $[E : E^H] < [E : k]$, the inductive hypothesis gives a radical tower $E^H \subseteq R_1 \subseteq \cdots \subseteq R_t$, where $E \subseteq R_t$. Now E^H/k is a Galois extension, for $H \lhd G$, and its index $[G : H] = p = [E^H : k]$, by the Fundamental Theorem. Corollary A-5.60 now applies to give $E^H = k(z)$, where $z^p \in k$; that is, E^H/k is a pure extension. Hence, the radical tower above can be lengthened by adding the prefix $k \subseteq E^H$, thus displaying R_t/k as a radical extension containing E.

Case (ii): General case. Let $k^* = k(\omega)$, and define $E^* = E(\omega)$. We claim that E^*/k is a Galois extension. Since E/k is a Galois extension, it is the splitting field of some separable $f(x) \in k[x]$, and so E^* is a splitting field over k of $f(x)(x^p - 1)$. But $x^p - 1$ is separable, because k has characteristic 0, and so E^*/k is a Galois extension. Therefore, E^*/k^* is also a Galois extension, by Corollary A-5.44. Let $G^* = \mathrm{Gal}(E^*/k^*)$. By Exercise A-5.3 on page 199 (Accessory Irrationalities), there is an injection $\psi\colon G^* \to G = \mathrm{Gal}(E/k)$, so that G^* is solvable, being isomorphic to a subgroup of a solvable group. Since $\omega \in k^*$, the first case says that there is a radical tower $k^* \subseteq R_1^* \subseteq \cdots \subseteq R_m^*$ with $E \subseteq E^* \subseteq R_m^*$. But $k^* = k(\omega)$ is a pure extension, so that this last radical tower can be lengthened by adding the prefix $k \subseteq k^*$, thus displaying R_m^*/k as a radical extension containing E. •

Corollary A-5.63 (Galois). *If k is a field of characteristic 0 and $f(x) \in k[x]$, then f is solvable by radicals if and only if the Galois group of f is a solvable group.*

Remark. A counterexample in characteristic p is given in Theorem A-5.66. ◀

Proof. Let E/k be a splitting field of f and let $G = \mathrm{Gal}(E/k)$. Since G is solvable, Theorem A-5.62 says that there is a radical extension R/k with $E \subseteq R$; that is, f is solvable by radicals. The converse is Theorem A-5.33. •

We now have another proof of the existence of the classical formulas.

Corollary A-5.64. *Let $f(x) \in k[x]$, where k has characteristic 0. If $\deg(f) \leq 4$, then f is solvable by radicals.*

Proof. If G is the Galois group of f, then G is isomorphic to a subgroup of S_4. But S_4 is a solvable group, and so every subgroup of S_4 is also solvable. By Corollary A-5.63, f is solvable by radicals. •

Suppose we know the Galois group G of a polynomial $f(x) \in \mathbb{Q}[x]$ and that G is solvable. Can we use this information to find the roots of f? The answer is affirmative; we suggest the reader look at the book by Gaal [**40**] to see how this is done.

In 1827, Abel proved that if the Galois group of a polynomial $f(x)$ is commutative, then f is solvable by radicals (of course, Galois groups had not yet been defined). This result was superseded by Galois's Theorem, proved in 1830 (for abelian groups are solvable), but it is the reason why abelian groups are so called.

A deep theorem of Feit and Thompson (1963) says that every group of odd order is solvable. It follows that if k is a field of characteristic 0 and $f(x) \in k[x]$ is a polynomial whose Galois group has odd order or, equivalently, whose splitting field has odd degree over k, then f is solvable by radicals.

The next theorem gives an example showing that the converse of Galois's Theorem is false in prime characteristic.

Lemma A-5.65. *The polynomial $f(x) = x^p - x - t \in \mathbb{F}_p[t]$ has no roots in $\mathbb{F}_p(t)$, the field of rational functions over $\mathbb{F}_p$.*

Proof. If there is a root α of $f(x)$ lying in $\mathbb{F}_p(t)$, then there are $g(t), h(t) \in \mathbb{F}_p[t]$ with $\alpha = g/h$; we may assume that $\gcd(g,h) = 1$. Since α is a root of f, we have $(g/h)^p - (g/h) = t$; clearing denominators, there is an equation

$$g^p - h^{p-1}g = th^p$$

in $\mathbb{F}_p[t]$. Hence, $g \mid th^p$. Since $\gcd(g,h) = 1$, we have $g \mid t$, so that $g(t) = at$ or $g(t)$ is a constant, say, $g(t) = b$, where $a, b \in \mathbb{F}_p$. Transposing $h^{p-1}g$ in the displayed equation shows that $h \mid g^p$; but $\gcd(g,h) = 1$ forces h to be a constant. We conclude that if $\alpha = g/h$, then $\alpha = at$ or $\alpha = b$. In the first case,

$$\begin{aligned} 0 &= \alpha^p - \alpha - t \\ &= (at)^p - (at) - t \\ &= a^p t^p - at - t \\ &= at^p - at - t \quad \text{(by Fermat's Theorem)} \\ &= t(at^{p-1} - a - 1). \end{aligned}$$

Hence, $at^{p-1} - a - 1 = 0$. But $a \neq 0$, and this contradicts t being transcendental over $\mathbb{F}_p$. In the second case, $\alpha = b \in \mathbb{F}_p$. But b is not a root of f, for $f(b) = b^p - b - t = -t$, by Fermat's Theorem. Thus, no root α of f can lie in $\mathbb{F}_p(t)$. •

Theorem A-5.66. *Let $k = \mathbb{F}_p(t)$, where p is prime. The Galois group of $f(x) = x^p - x - t$ over k is cyclic of order p, but f is not solvable by radicals over k.*

Proof. Let α be a root of f. It is easy to see that the roots of f are $\alpha + i$, where $0 \leq i < p$, for Fermat's Theorem gives $i^p = i$ in $\mathbb{F}_p$, and so

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) - t = \alpha^p + i^p - \alpha - i - t = \alpha^p - \alpha - t = 0.$$

It follows that f is a separable polynomial and that $k(\alpha)$ is a splitting field of f over k. We claim that f is irreducible in $k[x]$. Suppose that $f = gh$, where

$$g(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in k[x]$$

and $0 < d < \deg(f) = p$; then g is a product of d factors of the form $x - (\alpha + i)$. Now $-c_{d-1} \in k$ is the sum of the roots: $-c_{d-1} = d\alpha + j$, where $j \in \mathbb{F}_p$, and so $d\alpha \in k$. Since $0 < d < p$, however, $d \neq 0$ in k, and this forces $\alpha \in k$, contradicting Lemma A-5.65. Therefore, f is an irreducible polynomial in $k[x]$. Since $\deg(f) = p$, we have $[k(\alpha) : k] = p$ and, since f is separable, $|\operatorname{Gal}(k(\alpha)/k)| = [k(\alpha) : k] = p$. Therefore, $\operatorname{Gal}(k(\alpha)/k) \cong \mathbb{Z}_p$.

It will be convenient to have certain roots of unity available. Define

$$\Omega = \{\omega : \omega^q = 1, \text{where } q \text{ is a prime and } q < p\}.$$

We claim that $\alpha \notin k(\Omega)$. On the one hand, if $n = \prod_{q<p} q$, then Ω is contained in the splitting field of $x^n - 1$, and so $[k(\Omega) : k] \mid n!$, by Theorem A-5.3. It follows that $p \nmid [k(\Omega) : k]$. On the other hand, if $\alpha \in k(\Omega)$, then $k(\alpha) \subseteq k(\Omega)$ and $[k(\Omega) : k] = [k(\Omega) : k(\alpha)][k(\alpha) : k] = p[k(\Omega) : k(\alpha)]$. Hence, $p \mid [k(\Omega) : k]$, and this is a contradiction.

If f were solvable by radicals over $k(\Omega)$, there would be a radical extension

$$k(\Omega) = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_r$$

with $k(\Omega, \alpha) \subseteq B_r$. We may assume, for each $i \geq 1$, that B_i/B_{i-1} is of prime type; that is, $B_i = B_{i-1}(u_i)$, where $u_i^{q_i} \in B_{i-1}$ and q_i is prime. There is some $j \geq 1$ with $\alpha \in B_j$ but $\alpha \notin B_{j-1}$. Simplifying notation, we set $u_j = u$, $q_j = q$, $B_{j-1} = B$, and $B_j = B'$. Thus, $B' = B(u)$, $u^q = b \in B$, $\alpha \in B'$, and $\alpha, u \notin B$. We claim that $f(x) = x^p - x - t$, which we know to be irreducible in $k[x]$, is also irreducible in $B[x]$. By Accessory Irrationalities (Exercise A-5.3 on page 199), restriction gives an injection $\mathrm{Gal}(B(\alpha)/B) \to \mathrm{Gal}(k(\alpha)/k) \cong \mathbb{Z}_p$. If $\mathrm{Gal}(B(\alpha)/B) = \{1\}$, then $B(\alpha) = B$ and $\alpha \in B$, a contradiction. Therefore, $\mathrm{Gal}(B(\alpha)/B) \cong \mathbb{Z}_p$, and f is irreducible in $B[x]$, by Exercise A-5.11 on page 200.

Since $u \notin B'$ and B contains all the qth roots of unity, Proposition A-3.94 shows that $x^q - b$ is irreducible in $B[x]$, for it does not split in $B[x]$. Now $B' = B(u)$ is a splitting field of $x^q - b$, and so $[B' : B] = q$. We have $B \subsetneq B(\alpha) \subseteq B'$, and

$$q = [B' : B] = [B' : B(\alpha)][B(\alpha) : B].$$

Since q is prime, $[B' : B(\alpha)] = 1$; that is, $B' = B(\alpha)$, and so $q = [B(\alpha) : B]$. As α is a root of the irreducible polynomial $f(x) = x^p - x - t \in B[x]$, we have $[B(\alpha) : B] = p$; therefore, $q = p$. Now $B(u) = B' = B(\alpha)$ is a separable extension, by Proposition A-5.47, for α is a separable element. It follows that $u \in B'$ is also a separable element, contradicting $\mathrm{irr}(u, B) = x^q - b = x^p - b = (x - u)^p$ having repeated roots.

We have shown that f is not solvable by radicals over $k(\Omega)$. It follows that f is not solvable by radicals over k, for if there were a radical extension $k = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_t$ with $k(\alpha) \subseteq R_t$, then $k(\Omega) = R_0(\Omega) \subseteq R_1(\Omega) \subseteq \cdots \subseteq R_t(\Omega)$ would show that f is solvable by radicals over $k(\Omega)$, a contradiction. •

Exercises

∗ **A-5.13.** (i) Let $\sigma, \tau \in S_5$, where σ is a 5-cycle and τ is a transposition. Prove that $S_5 = \langle \sigma, \tau \rangle$; that is, S_5 is generated by σ, τ.

(ii) Show that S_6 contains a 6-cycle σ and a transposition τ which generate a proper subgroup of S_6.

∗ **A-5.14.** Let k be a field, let $f(x) \in k[x]$ be a separable polynomial, and let E/k be a splitting field of f. Assume further that there is a factorization $f(x) = g(x)h(x)$ in $k[x]$, and that B/k and C/k are intermediate fields that are splitting fields of g and h, respectively.

(i) Prove that $\mathrm{Gal}(E/B), \mathrm{Gal}(E/C)$ are normal subgroups of $\mathrm{Gal}(E/k)$.

(ii) Prove that $\mathrm{Gal}(E/B) \cap \mathrm{Gal}(E/C) = \{1\}$.

(iii) If $B \cap C = k$, prove that $\mathrm{Gal}(E/B)\,\mathrm{Gal}(E/C) = \mathrm{Gal}(E/k)$.
Hint. Use the Fundamental Theorem of Galois Theory, along with Proposition A-4.83 and Theorem A-5.17, to show, in this case, that

$$\mathrm{Gal}(E/k) \cong \mathrm{Gal}(B/k) \times \mathrm{Gal}(C/k).$$

(Note that $\mathrm{Gal}(B/k)$ is not a subgroup of $\mathrm{Gal}(E/k)$.)

(iv) Use (iii) to give another proof that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbf{V}$, where $E = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ (see Example A-3.89 on page 81).

(v) Let $f(x) = (x^3-2)(x^3-3) \in \mathbb{Q}[x]$. If $B/\mathbb{Q}$ and $C/\mathbb{Q}$ are the splitting fields of x^3-2 and x^3-3 inside $\mathbb{C}$, prove that $\mathrm{Gal}(E/\mathbb{Q}) \ncong \mathrm{Gal}(B/\mathbb{Q}) \times \mathrm{Gal}(C/\mathbb{Q})$, where E is the splitting field of f contained in $\mathbb{C}$.

A-5.15. Let k be a field of characteristic 0, and let $f(x) \in k[x]$ be a polynomial of degree 5 with splitting field E/k. Prove that f is solvable by radicals if and only if $[E:k] < 60$.

∗ **A-5.16.** Let E be a field and let $\mathrm{Aut}(E)$ be the group of all (field) automorphisms of E. Prove that $\mathrm{Aut}(E) = \mathrm{Gal}(E/k)$, where k is the prime field of E.

A-5.17. Let E/k be a Galois extension with $\mathrm{Gal}(E/k)$ cyclic of order n. If $\varphi\colon \mathrm{Int}(E/k) \to \mathrm{Div}(n)$ is defined by $\varphi(L) = [L:k]$, prove that φ is an order-preserving lattice isomorphism (see Example A-5.48(iv)).

A-5.18. Use Theorem A-5.57 to prove that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $m \mid n$.

A-5.19. Find all finite fields k whose subfields form a *chain*; that is, if k' and k'' are subfields of k, then either $k' \subseteq k''$ or $k'' \subseteq k'$.

A-5.20. (i) Let k be an infinite field, let $f(x) \in k[x]$ be a separable polynomial, and let $E = k(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f. Prove that there are $c_i \in k$ so that $E = k(\beta)$, where $\beta = c_1\alpha_1 + \cdots + c_n\alpha_n$.

Hint. Use the proof of Steinitz's Theorem.

(ii) **(Janusz)** Let k be a finite field and let $k(\alpha,\beta)/k$ be finite. If $k(\alpha) \cap k(\beta) = k$, prove that $E = k(\alpha+\beta)$. (This result is false in general. For example, N. Boston used the computer algebra system MAGMA to show that there are primitive elements α of $\mathbb{F}_{2^6}$ and β of $\mathbb{F}_{2^{10}}$ such that $\mathbb{F}_2(\alpha,\beta) = \mathbb{F}_{2^{30}}$ while $\mathbb{F}_2(\alpha+\beta) = \mathbb{F}_{2^{15}}$.)
Hint. Use Proposition A-3.74(ii).

A-5.21. Let E/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/k)$. Define the ***trace*** $T\colon E \to E$ by

$$T(u) = \sum_{\sigma \in G} \sigma(u).$$

(i) Prove that $\mathrm{im}\, T \subseteq k$ and that $T(u+v) = T(u) + T(v)$ for all $u, v \in E$.

(ii) Use independence of characters to prove that T is not identically zero.

A-5.22. Let E/k be a Galois extension with $[E:k] = n$ and with cyclic Galois group $G = \mathrm{Gal}(E/k)$, say, $G = \langle\sigma\rangle$. Define $\tau = \sigma - 1_E$, and prove that $\mathrm{im}\,\tau = \ker T$, where $T\colon E \to E$ is the trace. Conclude, in this case, that the ***Trace Theorem*** is true:

$$\ker T = \{a \in E : a = \sigma(u) - u \text{ for some } u \in E\}.$$

Hint. Show that $\ker\tau = k$, so that $\dim(\mathrm{im}\,\tau) = n-1 = \dim(\ker T)$.

A-5.23. Let k be a field of characteristic $p > 0$, and let E/k be a Galois extension having a cyclic Galois group $G = \langle\sigma\rangle$ of order p. Using the Trace Theorem, prove that there is an element $u \in E$ with $\sigma(u) - u = 1$. Prove that $E = k(u)$ and that there is $c \in k$ with $\mathrm{irr}(u,k) = x^p - x - c$. (This is an additive version of Hilbert's Theorem 90.)

Hint. If u is a root of $g(x) = x^p - x - c$, then so is $u+i$ for $0 \le i \le p-1$. But $\mathrm{irr}(u,k) = \prod_{i=0}^{p-1} x - (u+i)$.

Calculations of Galois Groups

We now show how to compute Galois groups of polynomials of low degree. The *discriminant* of a polynomial will be useful, as will some group-theoretic theorems we will cite when appropriate.

If $f(x) \in k[x]$ is a monic polynomial having a splitting field E/k, then there is a factorization in $E[x]$:

$$f(x) = \prod_i (x - \alpha_i),$$

where $\alpha_1, \ldots, \alpha_n$ is a list of the roots of f (with repetitions if f has repeated roots).

Definition. Define

$$\Delta = \Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j),$$

and define the ***discriminant*** to be

$$D = D(f) = \Delta^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

The product $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$ has one factor $\alpha_i - \alpha_j$ for each distinct pair of indices (i, j) (the inequality $i < j$ prevents a pair of indices from occurring twice). It is clear that f has repeated roots if and only if its discriminant $D(f) = 0$. Each $\sigma \in \mathrm{Gal}(E/k)$ permutes the roots, and so σ permutes all the distinct pairs. However, it may happen that $i < j$ while the subscripts involved in $\sigma(\alpha_i) - \sigma(\alpha_j)$ are in reverse order. For example, suppose the roots of a cubic are α_1, α_2, and α_3. If there is $\sigma \in G$ with $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_1$, and $\sigma(\alpha_3) = \alpha_3$ (that is, σ is a transposition), then

$$\begin{aligned}\sigma(\Delta) &= \big(\sigma(\alpha_1) - \sigma(\alpha_2)\big)\big(\sigma(\alpha_1) - \sigma(\alpha_3)\big)\big(\sigma(\alpha_2) - \sigma(\alpha_3)\big)\\ &= (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) = -(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) = -\Delta.\end{aligned}$$

Each term $\alpha_i - \alpha_j$ occurs in $\sigma(\Delta)$, but with a possible sign change. We conclude, for all $\sigma \in \mathrm{Gal}(E/k)$, that $\sigma(\Delta) = \pm\Delta$. It is natural to consider Δ^2 rather than Δ, for Δ depends not only on the roots of $f(x)$, but also on the order in which they are listed, whereas $D = \Delta^2$ does not depend on the ordering. For a connection between discriminants and the alternating group A_n, see the footnote on page 141. In fact, $\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta$.

Proposition A-5.67. *If $f(x) \in k[x]$ is a separable polynomial, then its discriminant $D(f)$ lies in k.*

Proof. Let E/k be a splitting field of f; since f is separable, Theorem A-5.42 applies to show that E/k is a Galois extension. Each $\sigma \in \mathrm{Gal}(E/k)$ permutes the roots $\alpha_1, \ldots, \alpha_n$ of f, and $\sigma(\Delta) = \pm\Delta$, as we have just seen. Therefore,

$$\sigma(D) = \sigma(\Delta^2) = \sigma(\Delta)^2 = (\pm\Delta)^2 = D,$$

so that $D \in E^G$. But E/k is a Galois extension, so that $E^G = k$ and $D \in k$. •

If $f(x) = x^2 + bx + c \in k[x]$, where k is a field of characteristic $\neq 2$, then the quadratic formula gives the roots of f:

$$\alpha = \tfrac{1}{2}\big(-b + \sqrt{b^2 - 4c}\big) \quad \text{and} \quad \beta = \tfrac{1}{2}\big(-b - \sqrt{b^2 - 4c}\big).$$

It follows that

$$D = \Delta^2 = (\alpha - \beta)^2 = b^2 - 4c.$$

If f is a cubic with roots α, β, γ, then

$$D = \Delta^2 = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2;$$

it is not obvious how to compute the discriminant D from the coefficients of f (see Theorem A-5.68(ii) below).

Recall our discussion of the classical formulas for cubics and quartics. For each $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in k[x]$, the change of variable x to $x - \frac{1}{n}c_{n-1}$ produces a ***reduced*** polynomial $\widetilde{f}$; that is, one with no x^{n-1} term. This change of variable is always possible if k has characteristic 0; it is also possible if the characteristic is p and $p \nmid n$.

If $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in k[x]$ and $\beta \in k$ is a root of $\widetilde{f}$, then

$$0 = \widetilde{f}(\beta) = f(\beta - \tfrac{1}{n}c_{n-1}).$$

Hence, β is a root of $\widetilde{f}$ if and only if $\beta - \frac{1}{n}c_{n-1}$ is a root of f.

Theorem A-5.68. *Let k be a field of characteristic* 0.

(i) *A polynomial $f(x) \in k[x]$ and its reduced polynomial $\widetilde{f}(x)$ have the same discriminant: $D(f) = D(\widetilde{f})$.*

(ii) *The discriminant of a reduced cubic $\widetilde{f}(x) = x^3 + qx + r$ is*

$$D = D(\widetilde{f}) = -4q^3 - 27r^2.$$

Proof.

(i) If the roots of $f = \sum c_i x^i$ are $\alpha_1, \ldots, \alpha_n$, then the roots of $\widetilde{f}$ are $\beta_1, \ldots, \beta_n$, where $\beta_i = \alpha_i + \frac{1}{n}c_{n-1}$. Therefore, $\beta_i - \beta_j = \alpha_i - \alpha_j$ for all i, j,

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j) = \prod_{i<j}(\beta_i - \beta_j) = \Delta(\widetilde{f}),$$

and so the discriminants, which are the squares of these, are equal.

(ii) The cubic formula gives the roots of $\widetilde{f}$ as

$$\alpha = g + h, \quad \beta = \omega g + \omega^2 h, \quad \text{and} \quad \gamma = \omega^2 g + \omega h,$$

where $g = \big[\frac{1}{2}\big(-r + \sqrt{R}\big)\big]^{1/3}$, $h = -q/3g$, $R = r^2 + \frac{4}{27}q^3$, and ω is a cube root of unity. Because $\omega^3 = 1$, we have

$$\begin{aligned}\alpha - \beta &= (g + h) - (\omega g + \omega^2 h)\\ &= (g - \omega^2 h) - (\omega g - h)\\ &= (g - \omega^2 h) - (g - \omega^2 h)\omega\\ &= (g - \omega^2 h)(1 - \omega).\end{aligned}$$

Similar calculations give

$$\alpha - \gamma = (g + h) - (\omega^2 g + \omega h) = (g - \omega h)(1 - \omega^2)$$

and

$$\beta - \gamma = (\omega g + \omega^2 h) - (\omega^2 g + \omega h) = (g - h)\omega(1 - \omega).$$

It follows that

$$\Delta = (g - h)(g - \omega h)(g - \omega^2 h)\omega(1 - \omega^2)(1 - \omega)^2.$$

By Exercise A-5.24 on page 232, we have $\omega(1 - \omega^2)(1 - \omega)^2 = 3i\sqrt{3}$; moreover, the identity

$$x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2),$$

with $x = g/h$, gives

$$(g - h)(g - \omega h)(g - \omega^2 h) = g^3 - h^3 = \sqrt{R}$$

(we saw that $g^3 - h^3 = \sqrt{R}$ on page 5). Therefore, $\Delta = 3i\sqrt{3}\sqrt{R}$, and

$$D = \Delta^2 = -27R = -27r^2 - 4q^3. \quad \bullet$$

Remark. Let k be a field, and let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in k[x]$ have degrees $m \geq 1$ and $n \geq 1$, respectively. Their ***resultant*** is defined as

$$\operatorname{Res}(f, g) = \det(M),$$

where $M = M(f, g)$ is the $(m + n) \times (m + n)$ matrix

$$M = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & \\ & a_m & a_{m-1} & \cdots & a_1 & a_0 & \\ & & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ & & & \cdots & & & \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & b_n & b_{n-1} & \cdots & b_1 & b_0 & \\ & & b_n & b_{n-1} & \cdots & b_1 & b_0 \\ & & & \cdots & & & \end{bmatrix};$$

there are n rows for the coefficients a_i of f and m rows for the coefficients b_j of g; all the entries other than those shown are assumed to be 0. It can be proved that $\operatorname{Res}(f, g) = 0$ if and only if f and g have a nonconstant common divisor (Jacobson [**51**], p. 309). We mention the resultant here because the discriminant can be computed in terms of it:

$$D(f) = (-1)^{n(n-1)/2}\operatorname{Res}(f, f'),$$

where $f'(x)$ is the derivative of f (see van der Waerden [**118**], pp. 83–88, or Dummit–Foote [**28**], pp. 600–602). ◀

Here is a way to use the discriminant in computing Galois groups.

Proposition A-5.69. *Let k be a field of characteristic $\neq 2$, let $f(x) \in k[x]$ be a polynomial of degree n with no repeated roots, and let $D = \Delta^2$ be its discriminant. Let E/k be a splitting field of f, and let $G = \mathrm{Gal}(E/k)$ be regarded as a subgroup of S_n (as in* Theorem A-5.3*).*

(i) *If $H = A_n \cap G$, then $E^H = k(\Delta)$.*

(ii) *G is a subgroup of A_n if and only if $\Delta = \sqrt{D} \in k$.*

Proof.

(i) The Second Isomorphism Theorem gives $H = (G \cap A_n) \lhd G$ and

$$[G : H] = [G : A_n \cap G] = [A_n G : A_n] \leq [S_n : A_n] = 2.$$

By the Fundamental Theorem of Galois Theory (which applies because f has no repeated roots, hence is separable), $[E^H : k] = [G : H]$, so that $[E^H : k] = [G : H] \leq 2$. By Exercise A-5.28 on page 232, we have $k(\Delta) \subseteq E^{A_n}$, and so $k(\Delta) \subseteq E^H$, for H is contained in A_n. Therefore,

$$[E^H : k] = [E^H : k(\Delta)][k(\Delta) : k] \leq 2.$$

There are two cases. If $[E^H : k] = 1$, then each factor in the displayed equation is 1; in particular, $[E^H : k(\Delta)] = 1$ and $E^H = k(\Delta)$. If $[E^H : k] = 2$, then $[G : H] = 2$ and there exists $\sigma \in G$, $\sigma \notin A_n$, so that $\sigma(\Delta) = -\Delta$. Now $\Delta \neq 0$, because f has no repeated roots, and $-\Delta \neq \Delta$, because k does not have characteristic 2. Hence, $\Delta \notin E^G = k$ and $[k(\Delta) : k] > 1$. It follows from the displayed inequality that $[E^H : k(\Delta)] = 1$ and $E^H = k(\Delta)$.

(ii) The following are equivalent: $G \subseteq A_n$; $H = G \cap A_n = G$; $E^H = E^G = k$. Since $E^H = k(\Delta)$, by part (i), $E^H = k$ is equivalent to $k(\Delta) = k$; that is, $\Delta = \sqrt{D} \in k$. •

We can now show how to compute Galois groups of polynomials over $\mathbb{Q}$ of low degree.

If $f(x) \in \mathbb{Q}[x]$ is quadratic, then its Galois group has order either 1 or 2 (because the symmetric group S_2 has order 2). The Galois group has order 1 if f splits; it has order 2 if f does not split; that is, if f is irreducible.

If $f(x) \in \mathbb{Q}[x]$ is a cubic having a rational root, then its Galois group G is the same as that of its quadratic factor. Otherwise f is irreducible; since $|G|$ is now a multiple of 3, by Corollary A-5.9, and $G \subseteq S_3$, it follows that either $G \cong A_3 \cong \mathbb{Z}_3$ or $G \cong S_3$.

Proposition A-5.70. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic with Galois group G and discriminant D.*

(i) *f has exactly one real root if and only if $D < 0$, in which case $G \cong S_3$.*

(ii) *f has three real roots if and only if $D > 0$. In this case, either $\sqrt{D} \in \mathbb{Q}$ and $G \cong \mathbb{Z}_3$ or $\sqrt{D} \notin \mathbb{Q}$ and $G \cong S_3$.*

Proof. Note first that $D \neq 0$, for irreducible polynomials over $\mathbb{Q}$ have no repeated roots because $\mathbb{Q}$ has characteristic 0. Let $E/\mathbb{Q}$ be the splitting field of f.

(i) Suppose that f has one real root α and two complex roots: $\beta = u + iv$ and $\overline{\beta} = u - iv$, where $u, v \in \mathbb{R}$. Since $\beta - \overline{\beta} = 2iv$ and $\alpha = \overline{\alpha}$, we have

$$\Delta = (\alpha - \beta)(\alpha - \overline{\beta})(\beta - \overline{\beta}) = (\alpha - \beta)(\overline{\alpha - \beta})(\beta - \overline{\beta}) = 2iv|\alpha - \beta|^2,$$

and so $D = \Delta^2 = -4v^2|\alpha - \beta|^4 < 0$. Now $E \neq \mathbb{Q}(\alpha)$, because $\beta \in E$ is not real, so that $[E : \mathbb{Q}] = 6$ and $G \cong S_3$.

(ii) If f has three real roots, then Δ is real (by definition), $D = \Delta^2 > 0$, and $\sqrt{D}$ is real. By Proposition A-5.69(ii), $G \cong A_3 \cong \mathbb{Z}_3$ if and only if $\sqrt{D}$ is rational, and $G \cong S_3$ if $\sqrt{D}$ is irrational. •

Example A-5.71. The polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is irreducible, by Eisenstein's Criterion. Its discriminant is $D = -108$, and so its Galois group is S_3, by part (i) of the proposition.

The polynomial $x^3 - 4x + 2 \in \mathbb{Q}[x]$ is irreducible, by Eisenstein's Criterion; its discriminant is $D = 148$, and so it has three real roots. Since $\sqrt{148} = 2\sqrt{37}$ is irrational, the Galois group is S_3.

The polynomial $f(x) = x^3 - 48x + 64 \in \mathbb{Q}[x]$ is irreducible, by Theorem A-3.101 (it has no rational roots); the discriminant is $D = 2^{12}3^4$, and so f has three real roots. Since $\sqrt{D} = 2^6 3^2$ is rational, the Galois group is $A_3 \cong \mathbb{Z}_3$. ◀

The following corollary can sometimes be used to compute a splitting field of a polynomial even when we do not know all of its roots.

Corollary A-5.72. *Let $f(x) = x^3 + qx + r \in \mathbb{C}[x]$ have discriminant D and roots u, v and w. If $F = \mathbb{Q}(q, r)$, then $F(u, \sqrt{D})$ is a splitting field of f over F.*

Proof. Let $E = F(u, v, w)$ be a splitting field of f, and let $K = F(u, \sqrt{D})$. Now $K \subseteq E$, for the definition of discriminant gives $\sqrt{D} = \pm(u - v)(u - w)(v - w) \in E$. For the reverse inclusion, it suffices to prove that $v \in K$ and $w \in K$. Since $u \in K$ is a root of f, there is a factorization

$$f(x) = (x - u)g(x) \text{ in } K[x].$$

Now the roots of the quadratic g are v and w, so that

$$g(x) = (x - v)(x - w) = x^2 - (v + w)x + vw.$$

Since g has its coefficients in K and $u \in K$, we have

$$g(u) = (u - v)(u - w) \in K.$$

Therefore,

$$\begin{aligned} v - w &= (u - v)(u - w)(v - w)/(u - v)(u - w) \\ &= \pm\sqrt{D}/(u - v)(u - w) \in K. \end{aligned}$$

On the other hand, $v + w \in K$, because it is a coefficient of g and $g(x) \in K[x]$. But we have just seen that $v - w \in K$; hence, $v, w \in K$ and $E = F(u, v, w) \subseteq K = F(u, \sqrt{D})$. Therefore, $F(u, v, w) = F(u, \sqrt{D})$. •

In Example A-1.4 on page 6, we observed that the cubic formula giving the roots of $f(x) = x^3 + qx + r$ involves $\sqrt{R}$, where $R = r^2 + 4q^3/27$. Thus, when R is negative, every root of f involves complex numbers. Since every cubic f has at least one real root, this phenomenon disturbed mathematicians of the sixteenth century, and they spent much time trying to rewrite specific formulas to eliminate complex numbers. The next theorem shows why such attempts were doomed to fail. On the other hand, these attempts ultimately led to a greater understanding of numbers in general and of complex numbers in particular.

Theorem A-5.73 (Casus Irreducibilis). *If $f(x) = x^3 + qx + r \in \mathbb{Q}[x]$ is an irreducible cubic having three real roots u, v, and w, then any radical extension $K_t/\mathbb{Q}$ containing the splitting field of f is not real; that is, if $K_t \subseteq \mathbb{C}$, then $K_t \not\subseteq \mathbb{R}$.*

Proof. Let $F = \mathbb{Q}(q, r)$, let $E = F(u, v, w)$ be a splitting field of f, and let

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

be a radical tower with $E \subseteq K_t$.

Since all the roots u, v and w are real,

$$D = \Big((u - v)(u - w)(v - w)\Big)^2 \geq 0,$$

and so $\sqrt{D}$ is real. There is no loss in generality in assuming that $\sqrt{D}$ has been adjoined first:

$$K_1 = F(\sqrt{D}).$$

We claim that f remains irreducible in $K_1[x]$. If not, then K_1 contains a root of f, say, u. Now $w \in K_1(v)$, because $x - w = f(x)/(x - u)(x - v) \in K_1(v)[x]$, and hence $E \subseteq K_1(v)$. The reverse inclusion holds, for E contains v and $\sqrt{D} = (u-v)(u-w)(v-w)$; thus, $E = K_1(v)$. Now $[E : K_1] \leq 2$ and $[K_1 : F] \leq 2$, so that $[E : F] = [E : K_1][K_1 : F]$ is a divisor of 4. By Theorem A-3.88, the irreducibility of f over F gives $3 \mid [E : F]$. This contradiction shows that f is irreducible in $K_1[x]$.

We may assume that each pure extension K_{i+1}/K_i in the radical tower is of prime type. As f is irreducible in $K_1[x]$ and splits in $K_t[x]$ (because $E \subseteq K_t$), there is a first pure extension K_{j+1}/K_j with f irreducible in $K_j[x]$ and factoring in $K_{j+1}[x]$. By hypothesis, $K_{j+1} = K_j(\alpha)$, where α is a root of $x^p - c$ for some prime p and some $c \in K_j$. By Proposition A-3.94, either $x^p - c$ is irreducible over K_j or c is a pth power in K_j. In the latter case, we have $K_{j+1} = K_j$, contradicting f being irreducible over K_j but not over K_{j+1}. Therefore, $x^p - c$ is irreducible over K_j, so that

$$[K_{j+1} : K_j] = p.$$

Since f factors over K_{j+1}, there is a root of f lying in it, say,

$$u \in K_{j+1};$$

hence, $K_j \subseteq K_j(u) \subseteq K_{j+1}$. But f is an irreducible cubic over K_j, so that $3 \mid [K_{j+1} : K_j] = p$, by Theorem A-3.88. It follows that $p = 3$ and

$$K_{j+1} = K_j(u).$$

Now K_{j+1} contains u and $\sqrt{D}$, so that $K_j \subseteq E = F(u, \sqrt{D}) \subseteq K_{j+1}$, by Corollary A-5.72. Since $[K_{j+1} : K_j]$ has no proper intermediate subfields (Corollary A-5.9 again), we have $K_{j+1} = E$. Thus, K_{j+1} is a splitting field of f over K_j, and hence K_{j+1} is a Galois extension of K_j. The polynomial $x^3 - c$ (remember that $p = 3$) has a root, namely α, in K_{j+1}, so that Theorem A-5.42 says that K_{j+1} contains the other roots $\omega\alpha$ and $\omega^2\alpha$ as well, where ω is a primitive cube root of unity. But this gives $\omega = (\omega\alpha)/\alpha \in K_{j+1}$, which is a contradiction because ω is not real while $K_{j+1} \subseteq K_t \subseteq \mathbb{R}$. •

Before examining quartics, we cite a property of S_4 which is proved using a group-theoretic theorem of Sylow: If d is a divisor of $|S_4| = 24$, then S_4 has a subgroup of order d; moreover, $\mathbf{V}$ and $\mathbb{Z}_4$ are nonisomorphic subgroups of order 4, but any two subgroups of order $d \neq 4$ are isomorphic. We conclude that the Galois group G of a quartic is determined, up to isomorphism, by its order unless $|G| = 4$.

Consider a (reduced) quartic $f(x) = x^4 + qx^2 + rx + s \in \mathbb{Q}[x]$; let $E/\mathbb{Q}$ be its splitting field and let $G = \mathrm{Gal}(E/\mathbb{Q})$ be its Galois group (by Exercise A-5.25(ii) on page 232, a polynomial and its reduced polynomial have the same Galois group). If f has a rational root α, then $f(x) = (x - \alpha)c(x)$, and its Galois group is the same as that of the cubic factor c; but Galois groups of cubics have already been discussed. Suppose that $f = h\ell$ is the product of two irreducible quadratics; let α be a root of h and let β be a root of ℓ. If $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, then Exercise A-5.14(iii) on page 221 shows that $G \cong \mathbf{V}$, the four-group; otherwise, $\alpha \in \mathbb{Q}(\beta)$, so that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha, \beta) = E$, and G has order 2.

We are left with the case of f irreducible. The basic idea now is to compare G with the four-group $\mathbf{V}$, namely, the normal subgroup of S_4,

$$\mathbf{V} = \big\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\big\},$$

so that we can identify the fixed field of $\mathbf{V} \cap G$. If the four roots of f are α_1, α_2, α_3, α_4 (Proposition A-5.75(ii) shows that these are distinct), consider the numbers:

$$\begin{cases} u &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \\ v &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \\ w &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3). \end{cases} \tag{12}$$

It is clear that if $\sigma \in \mathbf{V} \cap G$, then σ fixes u, v, and w. Conversely, if $\sigma \in S_4$ fixes $u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, then

$$\sigma \in \mathbf{V} \cup \big\{(1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\big\}.$$

However, none of the last four permutations fixes both v and w, and so $\sigma \in G$ fixes each of u, v, w if and only if $\sigma \in \mathbf{V} \cap G$. Therefore,

$$E^{\mathbf{V} \cap G} = \mathbb{Q}(u, v, w).$$

Definition. The ***resolvent cubic*** of $f(x) = x^4 + qx^2 + rx + s$ is

$$g(x) = (x - u)(x - v)(x - w),$$

where u, v, w are the numbers defined in Eqs. (12).

Proposition A-5.74. *The resolvent cubic of* $f(x) = x^4 + qx^2 + rx + s$ *is*

$$g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2.$$

Proof. If $f(x) = (x^2 + jx + \ell)(x^2 - jx + m)$, then we saw, in our discussion of the quartic formula on page 7, that j^2 is a root of

$$h(x) = x^3 + 2qx^2 + (q^2 - 4s)x - r^2,$$

a polynomial differing from the claimed expression for g only in the sign of its quadratic and constant terms. Thus, a number β is a root of h if and only if $-\beta$ is a root of g.

Let the four roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of f be indexed so that α_1, α_2 are the roots of $x^2 + jx + \ell$ and α_3, α_4 are the roots of $x^2 - jx + m$. Then $j = -(\alpha_1 + \alpha_2)$ and $-j = -(\alpha_3 + \alpha_4)$; therefore,

$$u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -j^2$$

and $-u$ is a root of h since $h(j^2) = 0$.

Now factor f into two quadratics, say,

$$f(x) = (x^2 + \widetilde{j}x + \widetilde{\ell})(x^2 - \widetilde{j}x + \widetilde{m}),$$

where α_1, α_3 are the roots of the first factor and α_2, α_4 are the roots of the second. The same argument as before now shows that

$$v = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -\widetilde{j}^2;$$

hence $-v$ is a root of h. Similarly, $-w = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$ is a root of h. Therefore,

$$h(x) = (x + u)(x + v)(x + w),$$

and so

$$g(x) = (x - u)(x - v)(x - w)$$

is obtained from h by changing the sign of the quadratic and constant terms. •

Proposition A-5.75. *Let* $f(x) \in \mathbb{Q}[x]$ *be a quartic polynomial.*

(i) *The discriminant* $D(f)$ *is equal to the discriminant* $D(g)$ *of its resolvent cubic* g.

(ii) *If* f *is irreducible, then* g *has no repeated roots.*

Proof.

(i) One checks easily that

$$u - v = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 = -(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

Similarly,

$$u - w = -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) \quad \text{and} \quad v - w = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4).$$

We conclude that

$$D(g) = [(u - v)(u - w)(v - w)]^2 = \Big[-\prod_{i<j}(\alpha_i - \alpha_j)\Big]^2 = D(f).$$

(ii) If f is irreducible, then it has no repeated roots (it is separable because $\mathbb{Q}$ has characteristic 0), and so $D(f) \neq 0$. But $D(g) = D(f) \neq 0$, and so g has no repeated roots. •

In the notation of Eqs. (12) on page 229, if f is an irreducible quartic, then, by (ii) above, u, v, w are distinct, and our discussion there gives $E^{\mathbf{V}\cap G} = \mathbb{Q}(u, v, w)$, where $G = \mathrm{Gal}(E/\mathbb{Q})$ is the Galois group of f. We can almost compute G; there is one ambiguous case. The resolvent cubic contains much information about the Galois group of the irreducible quartic from which it comes.

Proposition A-5.76. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quartic. Let G be its Galois group, D its discriminant, $g(x)$ its resolvent cubic, and m the order of the Galois group of g.*

(i) *If $m = 6$, then $G \cong S_4$. In this case, g is irreducible and $\sqrt{D}$ is irrational.*

(ii) *If $m = 3$, then $G \cong A_4$. In this case, g is irreducible and $\sqrt{D}$ is rational.*

(iii) *If $m = 1$, then $G \cong \mathbf{V}$. In this case, g splits in $\mathbb{Q}[x]$.*

(iv) *If $m = 2$, then $G \cong D_8$ or $G \cong \mathbb{Z}_4$. In this case, g has an irreducible quadratic factor.*

Proof. We have seen that $E^{\mathbf{V}\cap G} = \mathbb{Q}(u, v, w)$. By the Fundamental Theorem of Galois Theory,

$$[G : \mathbf{V} \cap G] = [E^{\mathbf{V}\cap G} : \mathbb{Q}] = [\mathbb{Q}(u, v, w) : \mathbb{Q}] = |\,\mathrm{Gal}(\mathbb{Q}(u, v, w)/\mathbb{Q})| = m.$$

Since f is irreducible, $|G|$ is divisible by 4, by Corollary A-5.9, and the group-theoretic statements follow from Exercise A-5.31 on page 233. Finally, in the first two cases, $|G|$ is divisible by 12, and Proposition A-5.69(ii) shows whether $G \cong S_4$ or $G \cong A_4$. The conditions on g in the last two cases are easy to see. •

Example A-5.77.

(i) Let $f(x) = x^4 - 4x + 2 \in \mathbb{Q}[x]$; f is irreducible, by Eisenstein's criterion. (Alternatively, we can see that f has no rational roots, using Theorem A-3.101, and then show that f has no irreducible quadratic factors by examining conditions imposed on its coefficients.) By Proposition A-5.74, the resolvent cubic is

$$g(x) = x^3 - 8x + 16.$$

Now g is irreducible (for $g(x) = x^3 + 2x + 1$ in $\mathbb{F}_5[x]$, and the latter polynomial is irreducible because it has no roots in $\mathbb{F}_5$). The discriminant of g is -4864, so that Theorem A-5.70(i) says that the Galois group of g is S_3, hence has order 6. Theorem A-5.76(i) now shows that $G \cong S_4$.

(ii) Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$; f is irreducible, by Example A-3.89. By Proposition A-5.74, the resolvent cubic is

$$x^3 + 20x^2 + 96x = x(x + 8)(x + 12).$$

In this case, $\mathbb{Q}(u, v, w) = \mathbb{Q}$ and $m = 1$. Therefore, $G \cong \mathbf{V}$. (This should not be a surprise once we recall Example A-3.89, for f is the irreducible polynomial of $\alpha = \sqrt{2} + \sqrt{3}$, where $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.) ◀

An interesting open question is the ***inverse Galois problem***: Which finite abstract groups G are isomorphic to $\mathrm{Gal}(E/\mathbb{Q})$, where $E/\mathbb{Q}$ is a Galois extension? Hilbert proved that the symmetric groups S_n are such Galois groups, and Shafarevich proved that every solvable group is a Galois group (see Neukirk-Schmidt-Wingberg [**84**], Chapter IX §6). After the classification of the finite simple groups, it was shown that most simple groups are Galois groups. For more information, the reader is referred to Malle–Matzat [**74**] and Serre [**107**].

Exercises

∗ **A-5.24.** Prove that $\omega(1-\omega^2)(1-\omega)^2 = 3i\sqrt{3}$, where $\omega = e^{2\pi i/3}$.

∗ **A-5.25.** (i) Prove that if $a \neq 0$, then $f(x)$ and $af(x)$ have the same discriminant and the same Galois group. Conclude that it is no loss in generality to restrict our attention to monic polynomials when computing Galois groups.

(ii) Let k be a field of characteristic 0. Prove that a polynomial $f(x) \in k[x]$ and its reduced polynomial $\widetilde{f}(x)$ have the same Galois group.

A-5.26. (i) Let k be a field of characteristic 0. If $f(x) = x^3 + ax^2 + bx + c \in k[x]$, then its reduced polynomial is $x^3 + qx + r$, where

$$q = b - \tfrac{1}{3}a^2 \quad \text{and} \quad r = \tfrac{2}{27}a^3 - \tfrac{1}{3}ab + c.$$

(ii) Show that the discriminant of f is

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

A-5.27. Find the Galois group of the cubic polynomial arising from the castle problem in Exercise A-1.1 on page 8.

∗ **A-5.28.** If $\sigma \in S_n$ and $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, where k is a field, define

$$(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n}).$$

(i) Prove that $(\sigma, f(x_1, \ldots, x_n)) \mapsto \sigma f$ is an action of S_n on $k[x_1, \ldots, x_n]$ (see Example A-4.55(ii) on page 152).

(ii) Let $\Delta = \Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$ (on page 223, we saw that $\sigma\Delta = \pm\Delta$ for all $\sigma \in S_n$). If $\sigma \in S_n$, prove that $\sigma \in A_n$ if and only if $\sigma\Delta = \Delta$.
Hint. Define $\varphi\colon S_n \to G$, where G is the multiplicative group $\{1, -1\}$, by

$$\varphi(\sigma) = \begin{cases} 1 & \text{if } \sigma\Delta = \Delta, \\ -1 & \text{if } \sigma\Delta = -\Delta. \end{cases}$$

Prove that φ is a homomorphism, and that $\ker\varphi = A_n$.

A-5.29. Prove that if $f(x) \in \mathbb{Q}[x]$ is an irreducible quartic whose discriminant has a rational square root, then the Galois group of f has order 4 or 12.

A-5.30. Let $f(x) = x^4 + rx + s \in \mathbb{Q}[x]$ have Galois group G.

(i) Prove that the discriminant of f is $-27r^4 + 256s^3$.

(ii) Prove that if $s < 0$, then G is not isomorphic to a subgroup of A_4.

(iii) Prove that $f(x) = x^4 + x + 1$ is irreducible and that $G \cong S_4$.

∗ **A-5.31.** Let G be a subgroup of S_4 with $|G|$ a multiple of 4; define $m = |G/(G \cap \mathbf{V})|$.

(i) Prove that m is a divisor of 6.

(ii) If $m = 6$, then $G = S_4$; if $m = 3$, then $G = A_4$; if $m = 1$, then $G = \mathbf{V}$; if $m = 2$, then $G \cong D_8$, $G \cong \mathbb{Z}_4$, or $G \cong \mathbf{V}$.

∗ **A-5.32.** Let G be a subgroup of S_4, and let G act transitively on $X = \{1, 2, 3, 4\}$. If $|G/(\mathbf{V} \cap G)| = 2$, prove that $G \cong D_8$ or $G \cong \mathbb{Z}_4$. (If we merely assume that G acts transitively on X, then $|G|$ is a multiple of 4 (Corollary A-5.9). The added hypothesis $|G/(\mathbf{V} \cap G)| = 2$ removes the possibility $G \cong \mathbf{V}$ when $m = 2$.)

A-5.33. Compute the Galois group over $\mathbb{Q}$ of $x^4 + x^2 - 6$.

A-5.34. Compute the Galois group over $\mathbb{Q}$ of $f(x) = x^4 + x^2 + x + 1$.

Hint. Use Example A-3.105 to prove irreducibility of f, and prove irreducibility of the resolvent cubic by reducing mod 2.

A-5.35. Compute the Galois group over $\mathbb{Q}$ of $f(x) = 4x^4 + 12x + 9$.

Hint. Prove that f is irreducible in two steps: first show that it has no rational roots, and then use Descartes's method (on page 3) to show that f is not the product of two quadratics over $\mathbb{Q}$.