Chapter 1

Field Extensions

Throughout this chapter k denotes a field and K an extension field of k.

1.1 Splitting Fields

Definition 1.1 A polynomial splits over k if it is a product of linear polynomials in $k[x]$. ◊

Let $\psi : k \to K$ be a homomorphism between two fields. There is a unique extension of ψ to a ring homomorphism $k[x] \to K[x]$ that we also denote by ψ; explicitly,

$$\psi\left(\sum_{i=0}^{n} \lambda_i x^i\right) = \sum_{i=0}^{n} \psi(\lambda_i) x^i.$$

Hence it makes sense to ask if a polynomial in $k[x]$ has a zero in K. Similarly, it makes sense to ask if a polynomial in $k[x]$ splits in $K[x]$.

Definition 1.2 Let $f \in k[x]$ be a polynomial of degree ≥ 1. An extension K/k is called a splitting field for f over k if f splits over K and if L is an intermediate field, say $k \subset L \subset K$, and f splits in $L[x]$, then $L = K$. ◊

The second condition in the definition could be replaced by the requirement that $K = k(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the zeroes of f in K.

The main result in this section is the existence and uniqueness up to isomorphism of splitting fields.

Remarks. 1. If $k \subset L \subset K$, and K is a splitting field for $f \in k[x]$, then K is also a splitting field for f over L. The converse is false as one sees by taking $f = x^2 + 1$ and $k = \mathbb{Q} \subset L = \mathbb{R} \subset K = \mathbb{C}$.

2. Let K be a splitting field for f over k. If F is an extension of K and α is a zero of f in F, then $\alpha \in K$. To see this, write $f = \beta(x - \alpha_1) \ldots (x - \alpha_n)$ with $\beta \in k$ and $\alpha_1, \ldots, \alpha_n \in K$, and observe that $0 = f(\alpha) = \beta(\alpha - \alpha_1) \ldots (\alpha - \alpha_n)$, so $\alpha = \alpha_i$ for some i.

3. Let K be a splitting field for f over k, and let α be a zero of f in K. Then $f = (x - \alpha)g$ for some $g \in K[x]$. Because f splits in K, so does g. Hence K is a splitting field for g over $k(\alpha)$.

Theorem 1.3 *Let k be a field and $f \in k[x]$. Then f has a splitting field, say K/k, and $[K : k] \leq (\deg f)!$.*

Proof. Induction on $n = \deg f$. If $\deg f = 1$, then $f = \alpha x + \beta$ with $\alpha, \beta \in k$, so f already splits in k, so we can take $K = k$.

Suppose that $n > 1$. If f is already split we may take $K = k$, so we may assume that f has an ireducible factor, say g, of degree ≥ 2. By Proposition **??.??**, g has a zero in the extension field $k(\alpha) = k[x]/(g)$; the degree of this extension is $\deg g \leq n$. Now write $f = (x - \alpha)h$ where $h \in k(\alpha)[x]$. Since $\deg h = n - 1$, the induction hypothesis says there is an extension $L/k(\alpha)$ over which h splits, and $[L : k(\alpha)] \leq (n - 1)!$. Certainly f also splits over L, and $[L : k] = [L : k(\alpha)][k(\alpha) : k] \leq n!$. If $\alpha_1, \ldots, \alpha_n$ are the zeroes of f in L, then $k(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f over k. □

The proof of Theorem 1.3 involves a choice of an irreducible factor of f. It is conceivable that choosing a different factor might produce a different splitting field. Before showing that is not the case, and hence that a splitting field is unique up to isomorphism, we need the following lemma.

Lemma 1.4 *Let $\varphi : k \to k'$ be an isomorphism of fields. Let $f \in k[x]$ be irreducible. If α is zero of f in some extension of k and β is an extension of $\varphi(f)$ in some extension of k', then there is an isomorphism $\psi : k(\alpha) \to k'(\beta)$ such that $\psi|_k = \mathrm{id}_k$ and $\psi(\alpha) = \beta$.*

Proof. The map φ extends to an isomorphism $k[x] \to k'[x]$ and sends (f) to $(\varphi(f))$, so induces an isomorphism between the quotient rings by these ideals. The composition of the obvious isomorphisms

$$k(\alpha) \to k[x]/(f) \to k'[x]/(\varphi(f)) \to k'(\beta)$$

is the desired isomorphism. □

Theorem 1.5 *Let k be a field and $f \in k[x]$. Let $\varphi : k \to k'$ be an isomorphism of fields. Let K/k be a splitting field for f, and let K'/k' be an extension such that $\varphi(f)$ splits in K'. Then*

1. *there is a homomorphism $\theta : K \to K'$ such that $\theta|_k = \varphi$;*
2. *if K' is a splitting field for $\varphi(f)$ over k', then $K' \cong K$.*

Proof. (1) We argue by induction on $[K : k]$. Write $f = p_1 \ldots p_n$ as a product of irreducibles $p_i \in k[x]$. Then $\varphi(f) = \varphi(p_1) \ldots \varphi(p_n)$, and each $\varphi(p_i)$ is irreducible in $k'[x]$.

If $[K : k] = 1$, then $K = k$, and we can take $\theta = \varphi$.

Suppose that $[K : k] > 1$. Then some p_i, say p_1, is not linear. Let $\alpha \in K$ be a zero of p_1, and let $\beta \in K'$ be a zero of $\varphi(p_1)$. By Lemma 1.4, there is an isomorphism $\psi : k(\alpha) \to k'(\beta)$ such that $\psi|_k = \varphi$.

Now K is a splitting field for f over $k(\alpha)$, and $\varphi(f)$ splits over $k'(\beta)$. Since $[K : k(\alpha)] < [K : k]$ we can apply the induction hypothesis to obtain $\theta : K \to K'$ such that $\theta|_{k(\alpha)} = \psi$. Hence

(2) Certainly θ is injective, so it remains to show it is surjective. However, if $f = (x - \alpha_1) \dots (x - \alpha_n)$ then $\varphi(f) = (x - \varphi(\alpha_1)) \dots (x - \varphi(\alpha_n))$; since K and K' are splitting fields $K = k(\alpha_1, \dots, \alpha_n)$ and $K' = k'(\varphi(\alpha_1), \dots, \varphi(\alpha_n))$, θ is also surjective, and hence an isomorphism. □

Theorem 1.6 *A polynomial of positive degree has a unique splitting field up to isomorphism.*

1.2 Normal extensions

Definition 2.1 A finite extension K/k is normal if every irreducible polynomial in $k[x]$ that has a zero in K actually splits over K. ◊

Theorem 2.2 *An extension K/k is normal if and only if it is the splitting field of a polynomial.*

Proof. ($\Rightarrow$) Write $K = k(\alpha_1, \dots, \alpha_n)$. The minimal polynomial p_i of α_i has a zero in K so splits in K. Hence $f = p_1 \cdots p_n$ splits in K. But K is generated by the zeroes of f, so K is the splitting field of f over k.

($\Leftarrow$) Suppose $K = k(\alpha_1, \dots, \alpha_n)$ is the splitting field of a degree n polynomial $g \in k$ where $\alpha_1, \dots, \alpha_n$ are the zeroes of g. Let $f \in k[x]$ be irreducible and suppose that $\alpha \in K$ is a zero of f. We must show that f splits in K.

Think of $fg \in K[x]$, and let L be the splitting field for fg over K. Write $f = (x-\alpha)(x-\beta)\dots(x-\omega)$ where $\alpha, \beta \dots, \omega \in L$. Since α and β are zeroes of f, there is an isomorphism $\phi : k(\alpha) \to k(\beta)$ such that $\phi(\alpha) = \beta$ and $\phi|_k = \mathrm{id}_k$ (Lemma 1.4).

Now think of $g \in k(\alpha)[x]$ and $g = \phi(g) \in k(\beta)[x]$. Now K is a splitting field for g over $k(\alpha)$ and $\phi(g)$ splits in $K(\beta)$ so, by Theorem 1.5, there is a map $\theta : K \to K(\beta)$ such that $\theta|_{k(\alpha)} = \phi$. Hence $\theta|_k = \phi|_k = \mathrm{id}_k$ and $\theta(g) = g$. Now $0 = \theta(g(\alpha_i)) = g(\theta(\alpha_i))$ so $\theta(\alpha_i)$ belongs to K. Hence $\theta(K) \subset K$. In particular, $\beta = \theta(\alpha) \in K$; the same argument shows that *all* the zeroes of f belong to K. □

The next result shows that a finite extension K/k can be embedded in a unique smallest normal extension L/k. The extension L/k is called the normal closure of K/k.

Theorem 2.3 *Let K/k be a finite extension. Then there is a finite extension L/K such that*

1. *L is normal over k, and*

2. *if $K \subset F \subset L$ and F is normal over k, then $F = L$, and*

3. *if L'/K is a finite extension such that L' satisfies (1) and (2), then there is a K-isomorphism $\theta : L \to L'$.*

Proof. (1) Write $K = k(\alpha_1, \ldots, \alpha_n)$, let $p_i \in k[x]$ be the minimal polynomial of α_i, set $p = p_1 p_2 \cdots p_n$, and let L be the splitting field of p over K. Then $k \subset K \subset L$, L is the splitting field for p over k, and $[L : k] < \infty$. By Theorem 2.2, L is normal over k.

(2) If $K \subset F \subset L$ and F is normal over k, then each p_i splits in F because it is irreducible and has a zero in F, whence p splits in F, so $F = L$.

(3) If L'/K is a finite extension such that L' satisfies (1) and (2), then each p_i splits in L', so by Theorem 1.5 there is a map $\theta : L \to L'$ such that $\theta|_K = \mathrm{id}_K$. By (2) applied to L', and the inclusions $K \subset \theta(L) \subset L'$, it follows that $\theta(L) = L'$, whence θ is an isomorphism as claimed. □

Example 2.4 Let p be an odd prime. What is the splitting field of $x^p - 2$ over $\mathbb{Q}$ and what is its degree?

By Eisenstein's criterion $f = x^p - 2$ is irreducible. Let α be the real p^{th} root of 2. Then f is the minimal polynomial of α over $\mathbb{Q}$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$.

If $\beta \in \mathbb{C}$ is a zero of f, then $(\beta\alpha^{-1})^p = 1$, so $\beta\alpha^{-1}$ is a zero of $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. By **??.??**, the cyclotomic polynomial $x^{p-1} + \cdots + x + 1$ is irreducible. Let $\zeta = e^{2\pi i/p}$. The zeroes of f are $\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{p-1}\alpha$, so the splitting field of f over $\mathbb{Q}$ is $L := \mathbb{Q}(\alpha, \zeta)$.

Since L contains both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta)$ its degree over $\mathbb{Q}$ is divisible by both p and $p - 1$. Hence $p(p-1)$ divides $[L : \mathbb{Q}]$. Let g be the minimal polynomial of α over $\mathbb{Q}(\zeta)$. Then g divides $x^p - 2$ so has degree $\leq p$. Therefore

$$[L : \mathbb{Q}] = [\mathbb{Q}(\zeta)(\alpha) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = (p-1) \deg g \leq (p-1)p,$$

whence $[L : \mathbb{Q}] = p(p-1)$. ◊

1.3 Finite fields

We already saw parts of the next result in Section **??**.

Theorem 3.1 *Let K be a finite field. Then*

1. *$|K| = p^n$ for some positive integer n, where $p = \mathrm{char}\, K$;*

2. *K is the splitting field for $x^{p^n} - x$ over $\mathbb{F}_p$;*

3. *any field of order p^n is isomorphic to K.*

Proof. Since $\operatorname{char} K = p$, $\mathbb{F}_p$ is a subfield of K. Hence K is a finite dimensional vector space over $\mathbb{F}_p$, and so has p^n elements where $n = \dim_{\mathbb{F}_p} K$.

It follows that $K^* := K\backslash\{0\}$ is an abelian group of order $p^n - 1$. Hence $\lambda^{p^n-1} = 1$ for every non-zero $\lambda \in K$. It follows that every element of K is a zero of $x^{p^n} - x$. In other words, $x^{p^n} - x$ has p^n distinct zeroes in K. Hence K is the splitting field for $x^{p^n} - x$ over $\mathbb{F}_p$. It now follows from Theorem 1.5 that any field of order p^n must be isomorphic to K. □

Theorem 3.1 does *not* show that a field of order p^n exists. It just shows what it has to be if it exists.

We will write $\mathbb{F}_{p^n}$ for the field of p^n elements (if it exists!). To prove its existence we will show that $x^{p^n} - x$ has p^n distinct zeroes, and that the set of these zeroes is equal to the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

To see whether a polynomial has repeated zeroes we look at its derivative.

Definition 3.2 The formal derivative of a polynomial $f = a_0 + a_1x + \cdots + a_nx^n$ in $k[x]$ is

$$f' = D(f) := a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

◊

Notice that $D(fg) = f'g + fg'$ and $D(\lambda f) = \lambda f'$ if $\lambda \in k$.

Lemma 3.3 *Let f be a non-zero polynomial in $k[x]$. Then f has a multiple zero in some extension field of k if and only if* $\deg(\gcd(f, f')) \geq 1$.

Proof. ($\Rightarrow$) Let K be an extension of k, and suppose that $\alpha \in K$ is a multiple zero of f. Then $f = (x - \alpha)^2 g$ for some $g \in K[x]$. Hence $x - \alpha$ divides both f and f' in $K[x]$. As remarked on page **??**, the gcd of two polynomials, in this case f and f', is the same in $K[x]$ as in $k[x]$, so that gcd has degree ≥ 1.

($\Leftarrow$) If f and f' have a common factor of degree ≥ 1 in some $K[x]$, then they have a common factor of the form $x - \alpha$ in $K[x]$ with K/k the splitting field of ff'. If we write $f = (x - \alpha)g$, then $f' = (x - \alpha)g' + g$, whence $x - \alpha$ divides g, so α is a multiple zero of f. □

Proposition 3.4 *The polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$ has p^n distinct zeroes in its splitting field.*

Proof. Since the derivative of $x^{p^n} - x$ is 1, the result follows from the previous lemma. □

Lemma 3.5 *Let p be a prime and R a commutative ring in which $p = 0$. Then the map $\phi : R \to R$ defined by $\phi(a) = a^p$ is a ring homomorphism.*

Proof. Certainly $\phi(1) = 1$. It is clear that $\phi(ab) = \phi(a)\phi(b)$, and

$$\phi(a+b) = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.$$

The integers $\binom{p}{i}$ are divisible by p whenever $1 \leq i \leq p-1$, so are zero in R. Hence $\phi(a+b) = \phi(a) + \phi(b)$. □

We call the map ϕ in Lemma 3.5 the Frobenius map.

If K is a field of characteristic p, then ϕ is injective. Hence if K is a *finite* field of characteristic p, then ϕ is also surjective and hence an isomorphism of K with itself. In particular, every element of K is a p^{th} power.

Theorem 3.6 *For each prime p and positive integer n, there is a unique field with p^n elements, namely the splitting field of $x^{p^n} - x$.*

Proof. Let K be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $\phi : K \to K$ be the Frobenius map. Notice that $\alpha \in K$ is a zero of $x^{p^n} - x$ if and only if $\phi^n(\alpha) = \alpha$. Hence, if α and β are zeroes of $x^{p^n} - x$, so are $\alpha \pm \beta$, $\alpha\beta$ and α^{-1}. Hence the zeroes of $x^{p^n} - x$ are a subfield of K. Since K is generated over $\mathbb{F}_p$ by the zeroes of $x^{p^n} - x$, we conclude that K is exactly the set of zeroes of $x^{p^n} - x$. □

Proposition 3.7 *The multiplicative group of non-zero elements in a finite field is cyclic.*

Proof. Suppose that $|K| = p^n$. Write $e = p^n - 1 = q_1^{n_1} \cdots q_t^{n_t}$ as a product of powers of distinct primes. We will show there is an element in $K \backslash \{0\}$ of order e. Define

$$e_i = eq_i^{-1} \qquad \text{and} \qquad d_i = eq_i^{-n_i}.$$

Since $e_i < e$, there is some $\alpha_i \in K$ that is not a zero of $x^{e_i} - 1$. Define $\beta_i = (\alpha_i)^{d_i}$ and $\beta = \beta_1 \cdots \beta_t$. The order of β_i divides $q_i^{n_i}$, but if it were smaller then α_i would be a zero of $x^{e_i} - 1$; hence the order of β_i is $q_i^{n_i}$. It follows that the order of β is e. □

1.4 Separability

Let's begin with a warning: an irreducible polynomial can have multiple zeroes in its splitting field. For example, let $k = \mathbb{F}_p(t)$ be the rational function field over $\mathbb{F}_p$, and let $f = x^p - t \in k[x]$. By Eisenstein's criterion applied to $f \in k[t][x]$, f is irreducible but over the extension field $K = k(t^{1/p})$ we have $f = (x - t^{1/p})^p$. This behavior causes problems.

Definition 4.1 A polynomial $f \in k[x]$ is separable if none of its irreducible factors has a multiple zero in its splitting field.

If every $f \in k[x]$ is separable, we say that k is a perfect field.

Let K be an extension of k An element $\alpha \in K$ is separable over k if its minimal polynomial is separable. We say that K is a separable extension of k if every element in it is separable over k. $\Diamond$

We have just seen that $\mathbb{F}_p(t)$ is not perfect: $t^{1/p}$ is not separable over $\mathbb{F}_p(t)$, and $\mathbb{F}_p(t^{1/p})$ is not a separable extension of $\mathbb{F}_p(t)$.

Lemma 4.2 *If $k \subset F \subset K$ are fields and K/k is separable, so are K/F and F/k.*

Proof. It follows at once form the definition that F/k is separable if K/k is. On the other hand, if $\alpha \in K$ its minimal polynomial over F divides its minimal polynomial over k, so has distinct zeroes. Hence α is separable over F. $\square$

It is quite a bit harder to prove the converse of this lemma.

Proposition 4.3 *Fields of characteristic zero are perfect.*

Proof. Let f be an irreducible polynomial with coefficients in a field of characteristic zero. Since the characteristic is zero, the derivative f' is not zero. Since f is irreducible and $\deg f' < \deg f$, it follows that $\gcd(f, f') = 1$, whence f has no multiple zeroes by Lemma 3.3. $\square$

Theorem 4.4 *A field of characteristic $p > 0$ is perfect if and only if every element of it is a p^{th} power (if and only if the Frobenius map is surjective).*

Proof. Let k be the field in question and write $k^p = \{\alpha^p \mid \alpha \in k\}$.

($\Rightarrow$) Let $\alpha \in k$ and set $f = x^p - \alpha$. Since $f' = 0$, $\gcd(f, f') = f$ so Lemma 3.3 implies that f has a multiple zero. But k is perfect so irreducible polynomials in $k[x]$ do not have multiple zeroes. Hence f is reducible. Write $f = gh$ with $1 \leq \deg g \leq p - 1$. Let K be the splitting field for f over k. If $\lambda \in K$ is a zero of f, then $\lambda^p = \alpha$ so

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

Hence $g = (x - \lambda)^d$ with $1 \leq d \leq p - 1$. But the coefficients of g belong to k, so $\lambda^d \in k$. Also $\lambda^p = \alpha \in k$. Since $(p, d) = 1$, there are integers u and v such that $du + pv = 1$. Hence

$$\lambda = (\lambda^d)^u (\lambda^p)^v \in k.$$

In particular, $\alpha = \lambda^p$ is the p^{th}-power of an element in k.

($\Leftarrow$) Suppose to the contrary that k is not perfect. Let $f = \sum \alpha_j x^j$ be an irreducible polynomial in $k[x]$ having a repeated zero in some extension field. Then $\deg(\gcd(f, f')) \geq 1$ but f is irreducible so $\gcd(f, f') = f$. Hence $f' = 0$. It follows that $\alpha_j = 0$ if p does not divide j. Hence $f = \beta_0 + \beta_1 x^p + \beta_2 x^{2p} + \cdots$. By hypothesis there are elements $\gamma_i \in k$ such that $\gamma_i^p = \beta_i$ so $f = (\gamma_0 + \gamma_1 x + \gamma_2 x^2 + \cdots)^p$. This contradicts the irreducibility of f. We conclude that k must be perfect. $\square$

Corollary 4.5 *A finite field is perfect.*

Every algebraic extension of a finite field, and every extension of a characteristic zero field is a separable extension.

Definition 4.6 If $K = k(\alpha)$ we say that K is a simple extension of k and that α is a primitive element of K over k. $\Diamond$

For example, if $(n, d) = 1$ then $\alpha = e^{2\pi id/n}$ is a primitive element for the extension of $\mathbb{Q}$ obtained by adjoining all n^{th} roots of one.

Theorem 4.7 (The primitive element theorem) *A finite separable extension is simple. In particular, if k is finite or of characteristic zero every finite extension of k is of the form $k(\alpha)$.*

Proof. Let K be a finite separable extension of k.

Suppose k is finite. Then K is also finite so its multiplicative group $K\backslash\{0\}$ is cyclic by Proposition 1.3.7. If α is a generator of this group, then $K = k(\alpha)$.

Suppose k is infinite. By induction it suffices to show that a finite separable extension of the form $k(\alpha, \beta)$ is equal to $k(\gamma)$ for a suitable γ.

Let f and g be the minimal polynomials of α and β over k. Write $m = \deg f$ and $n = \deg g$, and let $\{\alpha = \alpha_1, \ldots, \alpha_m\}$ and $\{\beta = \beta_1, \ldots, \beta_n\}$ be the zeroes of f and g respectively. Since the extension is separable, these zeroes are distinct.

Consider the mn equations

$$(\alpha - \alpha_i) + (\beta - \beta_j)X = 0, \qquad 1 \le i \le m, 1 \le j \le n.$$

Since k is infinite there is some $\lambda \in k$ that is not a solution to any of these equations. Define $\gamma := \alpha + \beta\lambda$.

Notice that β is a common zero of the polynomials $g(x)$ and $f(\gamma - \lambda x)$ in $k(\gamma)[x]$. If $\xi \neq \beta$ were another common zero lying in some extension field of K, then $g(\xi) = f(\gamma - \lambda\xi) = 0$, so $\xi = \beta_j$ for some $j > 1$ and $\gamma - \lambda\xi = \alpha_i$ for some i, whence $\alpha + \beta\lambda - \lambda\beta_j = \alpha_i$ thus contradicting the choice of λ. Hence $\gcd(g(x), f(\gamma - \lambda x)) = x - \beta$. In particular, $x - \beta \in k(\gamma)[x]$ by the remark on page **??**, so $\beta \in k(\gamma)$. Hence $\alpha = \gamma - \lambda\beta$ is also in $k(\gamma)$, and we conclude that $k(\alpha, \beta) = k(\gamma)$. $\square$

Corollary 4.8 *If K/k is a finite, normal, separable extension, then K is the splitting field of an irreducible separable polynomial over k.*

Proof. By the Primitive Element Theorem, $K = k(\alpha)$. Let f be the minimal polynomial of α. Then f is separable and irreducible of degree $[K : k]$. Since f has one zero in K and K/k is normal, f splits in K. Hence K is the splitting field for f. $\square$

1.5 Automorphisms of separable extensions

The notion of separabilty was defined in terms of individual elements. However, it eventually proves more useful to be able to characterize whether or not an extension K/k is separable in terms of automorphisms of K. We shall see that non-separable extensions are more rigid than separable ones in the sense that they possess far fewer automorphisms.

The next example illustrates the matter.

Example 5.1 The extension $K/k = \mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ is not separable. If ϕ is an automorphism of this extension then $\phi(t^{1/p})$ has the same minimal polynomial as $t^{1/p}$, namely $x^p - t = (x - t^{1/p})^p$, so $\phi(t^{1/p}) = t^{1/p}$, whence $\phi = \mathrm{id}_K$. Hence $\mathrm{Aut}(K/k) = \{1\}$. ◊

Compare this to a separable extension like $\mathbb{Q}(\sqrt{2})$ where there is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2})$ sending $\sqrt{2} \to -\sqrt{2}$. Of course, $\mathbb{Q}(\sqrt[3]{\ })$ does not have any automorphisms but for a rather different reason: although the minimal polynomial of $\sqrt[3]{2}$ has three distinct zeroes, only one of them is in $\mathbb{Q}(\sqrt[3]{2})$. Hence to really understand the difference between separable and non-separable extensions from the perspective of automorphisms we should focus on separable extensions that are normal.

Proposition 5.2 *Let $k(\alpha)$ be a degree d extension of k and let $f \in k[x]$ be the minimal polynomial of α. Let $\phi : k \to F$ be a homomorphism, and suppose that $\phi(f)$ splits over F.*

1. *If α is separable over k there are exactly d distinct extensions of ϕ to maps $\phi_i : k(\alpha) \to F$ such that $\phi_i|_k = \phi$.*

2. *If α is not separable there are $< d$ such extensions.*

Proof. Let $\beta_1, \ldots, \beta_n$ be the distinct zeroes of f in F. Then $n \leq d = \deg f$ and $n = d$ if and only if α is separable over k.

Any homomorphism $\psi : k(\alpha) \to F$ that extends ϕ is completely determined by $\psi(\alpha)$. But $\psi(\alpha) = \beta_i$ for some i, so there are at most n different ψs. By Lemma 1.4, there *is* such an extension for all i. Hence there are exactly n extensions of ϕ, and the result follows. □

Theorem 5.3 *Let K/k be a degree d extension and let $\phi : k \to F$ be a homomorphism. Suppose the minimal polynomials of all the elements in K split in F.*

1. *If K/k is separable there are exactly d distinct extensions of ϕ to maps $\phi_i : K \to F$ such that $\phi_i|_k = \phi$.*

2. *If K/k is not separable there are $< d$ such extensions.*

Proof. (1) By the Primitive Element theorem $K = k(\alpha)$, so the result follows from part (1) of Proposition 5.2.

(2) We argue by induction on d. Since K/k is not separable, $d > 1$. Let $\alpha \in K$ be non-separable over k. Set $s = [k(\alpha) : k]$ and $t = [K : k(\alpha)]$, so $st = d$ and $t < d$.

Every extension of ϕ to K can be obtained in two steps: first extend ϕ to $k(\alpha)$, then extend the extension from $k(\alpha)$ to K. By part (2) of Proposition 5.2, there are $< s$ extensions of ϕ to $k(\alpha)$, and by the induction hypothesis and (1), each of those extensions has $\leq t$ extensions to K, giving a total of $< d$ extensions of ϕ to K. □

Theorem 5.4 *The following conditions on a finite extension K/k are equivalent:*

1. *K/k is a normal and separable;*
2. *$|\operatorname{Aut}(K/k)| = [K : k]$;*
3. *$K^{\operatorname{Aut}(K/k)} = k$.*

If K/k is normal but not separable, then $|\operatorname{Aut}(K/k)| < [K : k]$.

Proof. The final sentence in the statement of this theorem follows from Theorem 5.3(2).

(1) $\Rightarrow$ (2) If we set $F = K$, then the hypotheses of Theorem 5.3(1) hold and the conclusion of that result gives (2).

(2) $\Leftrightarrow$ (3) Artin's Theorem says that

$$[K : K^{\operatorname{Aut}(K/k)}] = |\operatorname{Aut}(K/k)|,$$

so (2) and (3) are equivalent.

(2) $\Rightarrow$ (1) Write $d = [K : k]$ and let $\phi_1, \ldots, \phi_d$ be the distinct elements in $\operatorname{Aut}(K/k)$. If F denotes the normal closure of K, then the hypotheses of Theorem 5.3 hold, and each ψ_i may be considered as a map $\phi_i : K \to F$ that extends the inclusion $\phi : k \to F$. The conclusion of Theorem 5.3 then shows that K/k is separable.

By the Primitive Element Theorem, $K = k(\alpha)$ for some $\alpha \in K$. Let $p \in k[x]$ be the minimal polynomial of α. Since the ϕ_is are distinct, the elements $\phi_1(\alpha), \ldots, \phi_d(\alpha)$ are distinct. Hence p has $d = \deg p$ distinct zeroes in K, whence K is a splitting field for p. Hence K/k is normal. □

Theorem 5.5 *An extension generated by separable elements is separable.*

Proof. Let $K = k(\alpha_1, \ldots, \alpha_n)$ and suppose that each α_i is separable over k. We argue by induction on n. If $n = 0$, there is nothing to do, so suppose that $k' = k(\alpha_1, \ldots, \alpha_{n-1})$ is separable over k, set $\alpha = \alpha_n$ so that $K = k'(\alpha)$ and consider the extensions k'/k and K/k'.

Let F be the normal closure of k' over k (see page 3). Let $\phi : k \to F$ be the inclusion; the hypotheses of Theorem 5.3 now hold, so there are exactly $[k' : k]$ distinct homomorphisms $\phi_i : k' \to F$ such that $\phi_i|_k = \mathrm{id}_k$.

By hypothesis α is separable over k and hence over k'. By Proposition 5.2 applied to $k'(\alpha)$, there are exactly $[k'(\alpha) : k']$ extensions of each ϕ_i to homomorphisms $K = k'(\alpha) \to F$. This gives a total of $[k' : k].[k'(\alpha) : k'] = [K : k]$ homomorphisms $\psi : K \to F$ such that $\psi|_k = \mathrm{id}_k$. By part (2) of Theorem 5.3, K/k is separable. □

Corollary 5.6 *The splitting field of a separable polynomial is a separable extension.*

Proof. Let $f \in k[x]$ be a separable polynomial. Its splitting field is generated by the zeroes of the irreducible factors of f, and by hypothesis these zeroes are separable. Theorem 5.5 implies that this splitting field is separable over k. □

Chapter 2

Galois Theory

The fundamental idea of Galois theory is to study an extension K/k through analysis of its automorphism group $\mathrm{Aut}(K/k)$.

2.1 The Galois correspondence

Definition 1.1 A finite, normal, separable extension K/k is called a Galois extension. We then write

$$\mathrm{Gal}(K/k) = \mathrm{Aut}(K/k),$$

and call this the Galois group of the extension. ◊

We restate Theorem 1.5.4.

Theorem 1.2 *The following are equivalent:*

1. *K/k is Galois;*
2. *$|\mathrm{Aut}(K/k)| = [K : k]$;*
3. *$K^{\mathrm{Aut}(K/k)} = k$.*

Lemma 1.3 *Let K/k be a Galois extension and F an intermediate field. Then*

1. *K/F is a Galois extension, and*
2. *$\{\psi \in \mathrm{Gal}(K/k) \mid \psi|_F = \mathrm{id}_F\} = \mathrm{Gal}(K/F)$.*

Proof. (1) Because K/k is normal it is a splitting field for some $f \in k[x] \subset F$. Then K/F is a splitting field for f over F, and hence normal. By Lemma 1.4.2, K/F is separable.

(2) Because K/F is a Galois extension we can speak of its Galois group. There is a natural injective group homomorphism $\mathrm{Gal}(K/F) \to \mathrm{Gal}(K/k)$ and the image is as claimed. □

Theorem 1.4 (The Galois correspondence) *Suppose K/k is a Galois extension. There is an order-reversing bijection*

$$\{\textit{intermediate fields } F,\ k \subset F \subset K\} \longleftrightarrow \{\textit{subgroups of } \mathrm{Gal}(K/k)\}$$

implemented by

$$F \mapsto \mathrm{Gal}(K/F)$$

and

$$K^H \leftarrow H.$$

Proof. To prove these maps are mutual inverses we must show that

$$F = K^{\mathrm{Gal}(K/F)} \qquad \text{and} \qquad H = \mathrm{Gal}(K/K^H).$$

The first equality is given by Theorem 5.4. If H is a subgroup of $\mathrm{Gal}(K/k)$, then K/K^H is a Galois extension and $H \subset \mathrm{Gal}(K/K^H)$, so

$$|H| = [K : K^H] = |\,\mathrm{Gal}(K/K^H)|.$$

Hence $H = \mathrm{Gal}(K/K^H)$.

"Order-reversing" means that if $H \subset H'$, then $K^H \supset K^{H'}$. Actually, the lattices involved in the bijection are anti-isomorphic.

□

Remarks. Consider a Galois extension K/k and an intermediate extension $k \subset F \subset K$.

1. We will always think of $\mathrm{Gal}(K/F)$ as the subgroup of $\mathrm{Gal}(K/k)$ consisting of automorphisms of K/k that are the identity on F.

2. Notice that $[F : k] = |\,\mathrm{Gal}(K/k)|/|\,\mathrm{Gal}(K/F)|$.

3. Since $\mathrm{Gal}(K/k)$ is finite it has only a finite number of subgroups. Hence there are only a finite number of intermediate extensions F. This is not apriori obvious because one has intermediate extensions $k(\alpha)$ for all $\alpha \in K$ and there are infinitely many choices for α if k is infinite. For example, it is not at all obvious why only finitely many different extensions of $\mathbb{Q}$ appear as $\mathbb{Q}(a\sqrt[5]{2} + b\sqrt[7]{-11} + c\sqrt[3]{17})$ as $a, b, c \in \mathbb{Z}$ vary!

Theorem 1.5 *Let K/k be a Galois extension. Then*

1. *F/k is normal if and only if $\mathrm{Gal}(K/F)$ is a normal subgroup of $\mathrm{Gal}(K/k)$.*
2. *If F/k is normal, then $\mathrm{Gal}(F/k) \cong \mathrm{Gal}(K/k)/\,\mathrm{Gal}(K/F)$.*

Proof. (1) ($\Leftarrow$) Let H be a normal subgroup of $\mathrm{Gal}(K/k)$. To show that K^H/k is normal, it suffices to show that every irreducible polynomial $f \in k[x]$ having one zero $\alpha \in K^H$ actually splits in K^H.

Certainly f splits in K so we must show all its zeroes are in K^H. Let $\beta \in K$ be a zero of f. Then there is $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha) = \beta$. If $\eta \in H$, then $\sigma^{-1}\eta\sigma \in H$, so $\alpha = \sigma^{-1}\eta\sigma(\alpha) = \sigma^{-1}\eta(\beta)$, whence $\eta(\beta) = \sigma(\alpha) = \beta$. Therefore $\beta \in K^H$.

($\Rightarrow$) Suppose that F/k is normal. Because K/k is separable, F/k is separable. Hence F/k is a Galois extension.

Let $\alpha \in F$ and let $p \in k[x]$ be its minimal polynomial. Then p splits in F. Hence, if $\sigma \in \mathrm{Gal}(K/k)$, then $\sigma(\alpha) \in F$ because it is a zero of p. Hence $\sigma(F) \subset F$ for all $\sigma \in \mathrm{Gal}(K/k)$. Now, if $\eta \in H$, then $\sigma^{-1}\eta\sigma(\alpha) = \sigma^{-1}\sigma(\alpha) = \alpha$, so $\sigma^{-1}\eta\sigma|_F = \mathrm{id}_F$. In other words, $\sigma^{-1}\eta\sigma \in \mathrm{Gal}(K/F)$. Hence $\mathrm{Gal}(K/F)$ is a normal subgroup of $\mathrm{Gal}(K/k)$.

(2) Using the equality between the order of a Galois group and the degree of the corresponding extension this is just a restatement of the fact that $[K : k] = [K : F][F : k]$. □

Remark. Consider $k \subset F \subset K$ and suppose that K/k and F/k are Galois. By the proof of the previous theorem, if $\sigma \in \mathrm{Gal}(K/k)$, $\sigma(F) \subset F$, so there is a group homomorphism $\Phi : \mathrm{Gal}(K/k) \to \mathrm{Gal}(F/k)$, $\Phi(\sigma) = \sigma|_F$. Obviously, $\ker\Phi = \mathrm{Gal}(K/F)$. By part (2) of Theorem 1.5, Φ is surjective. This says, as we already know, that any $\eta \in \mathrm{Gal}(F/k)$ can be extended to and automorphism of K/k in $[K : F]$ different ways.

2.2 Elementary examples

Example 2.1 The Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is the cyclic group of order n generated by the Frobenius automorphism $\sigma(a) = a^p$.

Since $\mathbb{F}_{p^n}$ is the splitting field for $x^{p^n} - x$ over $\mathbb{F}_p$, it is a normal extension. It is a separable extension also because $\mathbb{F}_p$ is finite. Hence $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension of degree n.

The Frobenius automorphism is an automorphism of any field of characteristic p, and it fixes the elements of $\mathbb{F}_p$ because $\mathbb{F}_p - \{0\}$ is a group of order $p-1$ (so $a^{p-1} = a$ for all $0 \neq a \in \mathbb{F}_p$). Hence $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Now, $\sigma^r(a) = a^{p^r}$, so $\sigma^n = 1$. However, if $\sigma^r = 1$, then $a^{p^r} = a$ for all $a \in \mathbb{F}_{p^n}$, so every element in $\mathbb{F}_{p^n}$ is a zero of $x^{p^r} - x$; the degree of a polynomial is at least as big as its number of zeroes, so $p^r \geq |\mathbb{F}_{p^n}| = p^n$, whence $r \geq n$. It follows that the order of σ is n, so the subgroup of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ has order $\geq n$. However, $|\mathrm{Gal}(\mathbb{F}^{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle.$$

where σ is the Frobenius automorphism. ◊

Example 2.2 If $n = mr$, the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is the cyclic group of order r generated by the m^{th} power of the Frobenius automorphism. In other words,

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle\sigma^m\rangle$$

where $\sigma^m(a) = a^{p^m}$. ◊

Example 2.3 The splitting field of $f = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is a Galois extension and $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4$. There are only two groups with four elements, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

There are elements σ, τ in $\mathrm{Gal}(K/\mathbb{Q})$ defined by

$$\begin{aligned} \sigma(\sqrt{2}) &= -\sqrt{2} \qquad \sigma(\sqrt{3}) = \sqrt{3} \\ \tau(\sqrt{2}) &= \sqrt{2} \qquad \tau(\sqrt{3}) = -\sqrt{3}, \end{aligned}$$

so $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Its subgroup lattice is This is easy to compute. For example, if $H = \{1, \sigma\tau\}$, then $K^H = \mathbb{Q}(\sqrt{6})$. $\Diamond$

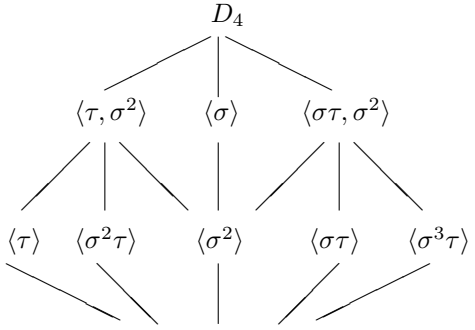
Example 2.4 Let K be a splitting field for $f = x^4 - 2 \in \mathbb{Q}[x]$.

Set $\alpha = 2^{1/4}$. The zeroes of f are $\pm\alpha$ and $\pm i\alpha$ so $K = \mathbb{Q}(\alpha, i) = \mathbb{Q}(\alpha)(i)$, whence $[K : \mathbb{Q}] = 8$. Hence $G = \mathrm{Gal}(K/\mathbb{Q})$ has eight elements. Elements of G must permute the zeroes of f, so G is a subgroup of the symmetric group S_4. Since α and $i\alpha$ have the same minimal polynomial over $\mathbb{Q}(i)$, namely $x^4 - 2$, there is a $\sigma \in G$ such that $\sigma(i) = i$ and $\sigma(\alpha) = i\alpha$. Similarly, there is a $\tau \in G$ such that $\tau(\alpha) = \alpha$ and $\tau(i) = -i$.

We will now show that G is isomorphic to the dihedral group D_4, the symmetry group of the square. A straighforward calculation shows that $\sigma^4 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$, so there is a homomorphism $D_4 \to G$. Notice that $\sigma^2 \neq 1$; since a non-trivial normal subgroup of D_4 contains σ^2, the map $D_4 \to G$ is injective and hence surjective. Thus $G = \langle \sigma, \tau \rangle \cong D_4$.

Before determining the intermediate fields we make some calculations. Since $\sigma^2(\alpha) = -\alpha$, $\sigma^2(\alpha^2) = \alpha^2$. Also $\sigma\tau(i) = -i$, $\sigma\tau(\alpha) = i\alpha$, and $\sigma\tau(i\alpha) = \alpha$, so $\sigma\tau(\alpha + i\alpha) = \alpha + i\alpha$.

The subgroup lattice of G is



As we said above, every non-trivial normal subgroup of D_4 contains σ^2. Since $D_4/\langle \sigma^2 \rangle \cong \mathbb{Z}_4$, the non-trivial normal subgroups of G are $\langle \sigma^2 \rangle$ and those of index two, namely

$$\{1, \sigma^2\},\ \{1, \sigma, \sigma^2, \sigma^3\},\ \{1, \sigma^2, \tau, \tau\sigma^2\},\ \{1, \sigma^2, \tau\sigma, \tau\sigma^3\}.$$

The corresponding intermediate fields are the normal extensions of $\mathbb{Q}$, namely

$$\begin{aligned} K^{\langle\sigma^2\rangle} &= \mathbb{Q}(i, \alpha^2) = \mathbb{Q}(i, \sqrt{2}), \\ K^{\langle\sigma\rangle} &= \mathbb{Q}(i), \\ K^{\langle\tau,\sigma^2\rangle} &= K^{\langle\sigma^2\rangle} \cap K^{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2}), \\ K^{\langle\sigma\tau,\sigma^2\rangle} &= \mathbb{Q}(i\sqrt{2}). \end{aligned}$$

The other intermediate fields are

$$\begin{aligned} K^{\langle\tau\rangle} &= \mathbb{Q}(\alpha), \\ K^{\langle\sigma\tau\rangle} &= \mathbb{Q}((1+i)\alpha), \\ K^{\langle\sigma^2\tau\rangle} &= \mathbb{Q}(i\alpha), \\ K^{\langle\sigma^3\tau\rangle} &= \mathbb{Q}((1-i)\alpha), \end{aligned}$$

all of which are degree four extensions of $\mathbb{Q}$. ◊

Exercises.
Let β be an element of $\mathbb{F}_4$ that is not in $\mathbb{F}_2$.

1. Find the minimal polynomial of β over $\mathbb{F}_2$.
2. Show that $x^2 + (\beta + 1)x + 1$ is irreducible in $\mathbb{F}_4[x]$.
3. Is the cubic $x^3 + x^2 + \beta \in \mathbb{F}_4[x]$ irreducible? If not, find its factors.
4. Show that $\mathbb{F}_{16}$ contains an element α that is a primitive fifth root of one over $\mathbb{F}_2$, and that $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$. Find the minimal polynomial of α over $\mathbb{F}_4$, and show that α^4 is the other zero of this polynomial.
5. Show that α is a zero of $x^3 + x^2 + \beta \in \mathbb{F}_4[x]$.
6. Show that the Galois group of $x^5 - 1$ over $\mathbb{F}_4$ is $\mathbb{Z}_2$.
7. Factor $x^4 + x^3 + x^2 + x + 1$ over $\mathbb{F}_4$.
8. You have shown above that $\mathbb{F}_{16} = \mathbb{F}_4(\alpha)$ where α is a primitive fifth root of 1. Does there exist an element $\alpha \in \mathrm{Gal}(x^5 - 1/\mathbb{F}_4)$ such that $\sigma(\alpha) = \alpha^2$?

2.3 Polynomials of degree ≤ 4

In this section we determines the Galois groups of quadratics, cubics, and quartics.

Notation. The Galois group of a separable polynomial $f \in k[x]$ is $\mathrm{Gal}(f/k) := \mathrm{Gal}(K/k)$ where K is a splitting field of f.

Definition 3.1 A subgroup H of the symmetric group S_n is transitive if, given any $i, j \in \{1, \ldots, n\}$, there is an $\eta \in H$ such that $\eta(i) = j$. ◊

Lemma 3.2 *Let $f \in k[x]$ be a separable, irreducible, polyomial of degree n. Then* $\mathrm{Gal}(f/k)$ *is a transitive subgroup of the symmetric group S_n, and n divides* $|\mathrm{Gal}(f/k)|$.

Proof. Let K be the splitting field of f and write $K = k(\alpha_1, \ldots, \alpha_n)$ where the α_i are the distinct zeroes of f. Because f is irreducible it is the minimal polynomial of each α_i, so $[k(\alpha) : k] = \deg f = n$. Hence n divides $[K : k] = |\mathrm{Gal}(K/k)|$.

If $\sigma \in \mathrm{Gal}(K/k)$, then the minimal polynomial of $\sigma(\alpha_i)$ is the same as the minimal polynomial of α_i so is f. Hence $\sigma(\alpha_i) = \alpha_j$ for some j. Hence $\mathrm{Gal}(K/k)$ permutes the zeroes of f and this gives a homomorphism $\mathrm{Gal}(K/k) \to S_n$. It is injective because if σ is the identity on the α_is it is the identity on $k(\alpha_1, \ldots, a_n)$. Because α_i and α_j have the same minimal polynomial there is an automorphism of K sending α_i to α_j. Hence $\mathrm{Gal}(K/k)$ is a transitive subgroup of the symmetric group. □

The discriminant. Let $f \in k[x]$ be a monic, irreducible, separable polynomial. The element

$$\delta(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

depends (up to a sign) on the order in which we label the zeroes of f, so is not an invariant of f. However, the discriminant of f, which is defined to be

$$D(f) := \delta(f)^2 = \prod_{1 \le i \ne j \le n} (\alpha_i - \alpha_j)$$

is independent of the labelling of the zeroes of f.

If $\tau \in S_n$ is a transposition, then $\tau(\delta) = -\delta$ and $\tau(D) = D$.

It follows that D is invariant under $\mathrm{Gal}(f/k)$, so belongs to $K^{\mathrm{Gal}(K/k)} = k$.

Lemma 3.3 *Let $f \in k[x]$ be monic, irreducible, and separable. Then* $\mathrm{Gal}(f/k)$ *is contained in the alternating group if and only if the discriminant $D(f)$ is a square in k.*

Proof. Clearly $D(f)$ is a square in k if and only if $\delta(f)$ belongs to k; if and only if $\delta(f)$ is fixed by every element of $\mathrm{Gal}(f/k)$. But $\delta(f)$ is fixed by even permutations and sent to $-\delta(f)$ by odd permutations, so $\delta(f) \in k$ if and only if $\mathrm{Gal}(f/k)$ consists of even permutations. □

Quadratic Polynomials. Let $f = (x - \alpha)(x - \beta) = x^2 + bx + c \in k[x]$. Then $b = -(\alpha + \beta)$ and $c = \alpha\beta$. The discriminant is

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

Since $S_2 \cong \mathbb{Z}_2$, $\mathbb{A}_2 = \{1\}$. The lemma says that $\mathrm{Gal}(f/k)$ is trivial if and only if $D(f)$ is a square, i.e., if and only if $b^2 - 4c$ is a square in k. In other words f splits in k if and only if $b^2 - 4c$ is a square, a result known to the ancients.

Cubic Polynomials. If $f = x^3 + ax^2 + bx + c$, a tedious computation gives

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

You should do this tedious computation at least once in your life: write $f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, express each of a, b, and c in terms of $\alpha_1, \alpha_2, \alpha_3$, then multiply out $D(f) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$ and rewrite it in terms of a, b, c.

We can always make a linear change of variable to bring a cubic polynomial into the form $f = x^3 + px + q$. Doing so, the discriminant takes the simpler form

$$-4p^3 - 27q^2.$$

The only transitive subgroups of S_3 are S_3 itself and A_3, so the Galois group of an irreducible, separable cubic is either S_3 or $A_3 \cong \mathbb{Z}_3$, with the two possibilities being determined by whether $D(f)$ is or is not a square in k.

Quartic Polynomials. The transitive subgroups of S_4 are:

S_4
the six conjugates of $\langle(1234)\rangle \cong \mathbb{Z}_4$
the three conjugates of $H = \langle(1234), (13)(24)\rangle \cong D_4$
A_4
$V = \{1, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The last two are the only ones contained in A_4.

Example 3.4 Let

$$f = x^4 + ax^2 + b \in \mathbb{Q}[x]$$

be irreducible and suppose that $k/\mathbb{Q}$ is an extension that does not contain a zero of f. Because f is a quadratic in x^2 its zeroes are $\{\pm\alpha, \pm\beta\}$ in its splitting field. We will show that

$$\mathrm{Gal}(f/k) \cong \begin{cases} \mathbb{Z}_4 & \text{if } \alpha\beta^{-1} - \beta\alpha^{-1} \in k \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{if } \alpha\beta \in k \\ D_4 & \text{otherwise.} \end{cases}$$

Let's write $G = \mathrm{Gal}(f/k)$.

Notice that G can not contain a 3-cycle because such an element would fix one of the zeroes, say α, but would not fix $-\alpha$. That is absurd. Hence G can not equal to S_4 or A_4.

To compute the discriminant notice that

$$x^4 + ax^2 + b = (x^2 - \alpha^2)(x^2 - \beta^2) = x^4 - (\alpha^2 + \beta^2)x^2 + \alpha^2\beta^2$$

so $-a = \alpha^2 + \beta^2$ and $b = \alpha^2\beta^2$. Therefore

$$\begin{aligned}\delta &= (\alpha+\alpha)(\alpha-\beta)(\alpha+\beta)(-\alpha-\beta)(-\alpha+\beta)(-\beta-\beta)\\ &= -4\alpha\beta(\alpha^2-\beta^2)^2\\ &= -4\alpha\beta\big(b^2-4a\big).\end{aligned}$$

Hence $a\beta \in k \iff \delta \in k \iff G \subset A_4 \iff G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Claim: if $\phi := \alpha\beta^{-1} - \alpha^{-1}\beta$ belongs to k, G does not contain a product of two disjoint 2-cycles. Proof: Suppose to the contrary G contained such an element. Looking at the list of possible G above, G would therefore have to contain all products of disjoint 2-cycles. Hence G would contain the automorphism σ such that $\sigma(\alpha) = \beta$. But $\sigma(\phi) = -\phi$, so $\phi \notin k$. This is a contradiction, so the claim must hold. $\Diamond$ It follows from the claim that $G \cong \mathbb{Z}_4$ if $\phi \in k$.

The following 4-cycles can not belong to G:

$$\begin{aligned}&\alpha \mapsto -\alpha \mapsto -\beta \mapsto \beta,\\ &\alpha \mapsto \beta \mapsto -\beta \mapsto -\alpha,\\ &\alpha \mapsto -\beta \mapsto \beta \mapsto -\alpha,\end{aligned}$$

The other three 4-cycles all fix ϕ, so if $G \cong \mathbb{Z}_4$, then $\phi \in k$. Thus, $\phi \in k \iff G \cong \mathbb{Z}_4$. $\Diamond$

2.4 Generic Polynomials

The symmetric group S_n acts on the polynomial ring $k[t_1, \ldots, t_n]$ in the obvious way:

$$\sigma(t_i) := t_{\sigma(i)}.$$

We extend the action by requiring σ to act as the identity on k and to be an automorphism of the polynomial ring. Thus, if $\sigma = (123)$, then the action of σ on a polynomial f is given by replacing each t_1 by t_2, each t_2 by t_3, and each t_3 by t_1, and leaving the other t_js untouched.

The action extends to the function field $k(t_1, \ldots, t_n)$.

A polynomial f which is invariant under S_n, that is, $\sigma(f) = f$ for all $\sigma \in S_n$, is called a symmetric polynomial. The invariants $k[t_1, \ldots, t_n]^{S_n}$ form a subring of $k[t_1, \ldots, t_n]$. Among the invariants are the elementary symmetric polynomials

defined as follows:

$$\begin{aligned}
\varepsilon_0 &= 1\\
\varepsilon_1 &= t_1 + \cdots + t_n\\
\varepsilon_2 &= \sum_{p<q} t_p t_q = t_1t_2 + t_1t_3 + \cdots + t_2t_3 + \cdots + t_{n-1}t_n\\
\varepsilon_3 &= \sum_{p<q<r} t_p t_q t_r\\
&\vdots \quad\quad \vdots\\
\varepsilon_n &= t_1t_2\cdots t_n.
\end{aligned}$$

Theorem 4.1 *1.* $k[t_1, \cdots, t_n]^{S_n} = k[\varepsilon_1, \cdots, \varepsilon_n]$;

2. $k[\varepsilon_1, \cdots, \varepsilon_n]$ *is a polynomial ring in* n *variables;*

3. $k(t_1, \cdots, t_n)$ *is a Galois extension of* $k(\varepsilon_1, \cdots, \varepsilon_n)$ *with Galois group* S_n.

Part (1) of Theorem 4.1 says that every polynomial that is invariant under the action of the symmetric group can be written as a polynomial in the elementary symmetric polynomials $\varepsilon_1, \cdots, \varepsilon_n$. For example, the polynomials $t_1^d + \cdots + t_n^d$ are obviously invariant. We have

$$t_1^2 + \cdots + t_n^2 = \varepsilon_1^2 - 2\varepsilon_2.$$

Try finding analogous expressions for $d = 3, 4, \ldots$.

Lemma 4.2 *Let* $f = (x - t_1)\cdots(x - t_n) \in k(t_1, \ldots, t_n)[x]$. *Then*

$$f = x^n - \varepsilon_1 x^{n-1} + \varepsilon_2 x^{n-2} - \cdots + (-1)^{n-1}\varepsilon_{n-1}x + (-1)^n\varepsilon_n.$$

Proof. Straightforward. □

We can view these previous two results in another way. Let $s_1, \ldots, s_n$ be indeterminates over k, and consider the field $k(s_1, \ldots, s_n)$. The general polynomial of degree n is

$$f = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^{n-1}s_{n-1}x + (-1)^n s_n.$$

It belongs to $k(s_1, \ldots, s_n)[x]$.

Theorem 4.3 $\mathrm{Gal}(f/k(s_1, \ldots, s_n)) \cong S_n$.

Proof. Let $t_1, \ldots, t_n$ be indeterminates and $\varepsilon_1, \cdots, \varepsilon_n$ the elementary symmetric polynomials in $t_1, \ldots, t_n$. By Theorem 4.1, $k(s_1, \ldots, s_n)$ is isomorphic to the subfield $k(\varepsilon_1, \cdots, \varepsilon_n)$ of $K = k(t_1, \cdots, t_n)$. We identify $k(s_1, \ldots, s_n)$ with $k(\varepsilon_1, \cdots, \varepsilon_n)$. By Lemma 4.2, f splits over K. In fact $f = (x - t_1)\cdots(x - t_n)$, so $K/k(s_1, \ldots, s_n)$ is the splitting field of f. By Theorem 4.1(3), the Galois group of f is isomorphic to S_n. □

Corollary 4.4 (Abel, Galois) *Let $n \geq 5$. The general polynomial of degree n is not solvable by radicals.*

Proof. We will prove this in the next chapter—a polynomial is solvable by radicals if and only if its Galois group is solvable. However, the symmetric group S_n is not solvable if $n \geq 5$. □

Chapter 3

Solvability by radicals

A polynomial $f \in k[x]$ is solvable by radicals if the zeroes of f are given by a "formula" that involves only $+$, $-$, $\times$, $\div$, n^{th} roots, and elements of k and the coefficients of f. The paradigmatic example is that the zeroes of $ax^2 + bx + c$ are given by

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

provided that $a \neq 0$ and $\operatorname{char} k \neq 2$. (What happens when $\operatorname{char} k = 2$?)

The formula for the zeroes of a quadratic polynomial was known to several ancient civilizations. A formula for the cubics was not found until the 16th century, and is generally credited to Scipio Ferro and Niccolo Tartaglia, although the first published solution appeared in a book by Cardano. The zeroes of $x^3 + px + q$ are

$$A - B,\ \omega A - \omega^2 B,\ \omega^2 A - \omega B,$$

where ω is a primitive cube root of unity, say $\frac{1}{2}(-1 + \sqrt{-3})$, and

$$A = \sqrt[3]{-\frac{q}{2}} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}$$

$$B = \sqrt[3]{+\frac{q}{2}} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^2}$$

and the cube roots are chosen so that $AB = -3p$. That is quite some formula! Notice though that if p and q belong to some field k, the three zeroes belong to the field $k(\omega, \alpha, A, B)$ where $\alpha = \sqrt{-3D}$ and $A^3, B^3 \in k(\omega, \alpha)$. In other words the zeroes belong to a field K that is obtained by successively adjoining roots of elements.

One very interesting aspect of this formula, an aspect that was a great puzzle at the time, is that the three roots could all be real numbers even if $\sqrt{-3D}$ is *not* a real number.

This was soon followed by a general solution to the quartic, and attention soon shifted to the quintic. Despite intense efforts during the 17th century no general solution was found and the suspicion then arose that there might not be

a formula for the solution to the general quintic. This was confirmed by Ruffini and Abel.

3.1 Roots of unity

The polynomials $x^n - 1$ and their Galois groups are of fundamental importance. Understanding them is a necessary preparation for Galois's theorem that (with a proviso on the characteristic of the field) a polynomial is solvable by radicals if and only if its Galois group is solvable.

Definition 1.1 An element ζ in a field is called a primitive n^{th} root of unity if $\zeta^n = 1$ but $\zeta^i \neq 1$ for every $1 \leq i \leq n-1$. $\Diamond$

Proposition 1.2 *Let k be a field of characteristic $p > 0$. If p divides n, then k does not contain a primitive n^{th} root of unity.*

Proof. Write $n = pd$. Then $x^n - 1 = (x^d - 1)^p$, so every n^{th} root of unity is a d^{th} root of unity. $\square$

In particular, if $\operatorname{char} k$ divides n, no extension of k can contain a primitive n^{th} root of unity. The next proposition shows that if $\operatorname{char} k$ does not divide n then there is an extension of k containing a primitive n^{th} root of unity.

Lemma 1.3 *The n^{th} roots of unity form a cyclic subgroup of the multiplicative group of a field.*

Proof. The set Γ of n^{th} roots of unity in k is a subgroup of the multiplicative group $k^\times = k - \{0\}$. Let $m > 0$ be minimal such that $a^m = 1$ for all $a \in \Gamma$. Then $|\Gamma| \leq m$ because $x^m - 1$ has at most m zeroes in k. However, $\Gamma \cong \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_t}$ for some integers a_i, so m is the least common multiple of the a_is, whence $m \leq a_1 \cdots a_t = |\Gamma|$. Hence $|\Gamma| = m$, so the a_is are relatively prime and $\Gamma \cong \mathbb{Z}_m$. $\square$

Proposition 1.4 *If the characteristic of k does not divide n, then*

1. *$x^n - 1$ is separable over k;*
2. *the splitting field of $x^n - 1$ contains a primitive n^{th} root of unity;*
3. *$\operatorname{Gal}(x^n - 1/k)$ is abelian;*
4. *$\operatorname{Gal}(x^n - 1/k)$ is isomorphic to a subgroup of the group of units in $\mathbb{Z}/(n)$.*

Proof. (1) and (2). Since $\operatorname{char} k$ does not divide n, the derivative of $x^n - 1$ is non-zero, hence relatively prime to $x^n - 1$. Thus $x^n - 1$ has n distinct zeroes and these form a cyclic group $\{1, \omega, \ldots, \omega^{n-1}\}$ by Lemma 1.3. In particular, ω is a primitive n^{th} root of unity.

(3) and (4) Let K denote the splitting field of $x^n - 1$. If $\sigma \in \mathrm{Gal}(K/k)$, then $\sigma(\omega)$ is also a zero of $x^n - 1$, so $\sigma(\omega) = \omega^{i(\sigma)}$ for a unique $i(\sigma) \in \mathbb{Z}_n$. A simple calculation shows that the map i:$\mathrm{Gal}(K/k) \to \mathbb{Z}_n$, $\sigma \mapsto i(\sigma)$, satisfies $i(\sigma\tau) = i(\sigma)i(\tau)$ and $i(\sigma^{-1}) = i(\sigma)^{-1}$, so is a homomorphism to the group of units in $\mathbb{Z}_n$. □

Corollary 1.5 *If* $\mathrm{char}\, k$ *does not divide* n*, then there is a Galois extension of* k *generated by a primitive* n^{th} *root of unity, say* ζ*, and* $\mathrm{Gal}(k(\zeta)/k)$ *is cyclic.*

Proof. □

Corollary 1.6 *Let* p *be a prime and* k *a field of characteristic not* p*. Then* $\mathrm{Gal}(x^p - 1/k)$ *is isomorphic to a subgroup of* $\mathbb{Z}_{p-1}$*.*

Proof. The group of units in the ring $\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_{p-1}$ by Proposition 1.3.7. □

Example 1.7 $\mathrm{Gal}(x^5 - 1/\mathbb{F}_4) \cong \mathbb{Z}_2$.

It is easy to see that $f = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. Hence if α is a zero of f, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$. The four distinct zeroes of f are $\alpha, \alpha^2, \alpha^3, \alpha^4$, so $\mathbb{F}_2(\alpha)$ is the splitting field for f over $\mathbb{F}_2$ and $\mathbb{F}_2(\alpha)$ is a Galois extension of $\mathbb{F}_2$. Since $\mathbb{F}_2(\alpha) \cong \mathbb{F}_{16}$, it has a subfield isomorphic to $\mathbb{F}_4$, and $[\mathbb{F}_2(\alpha) : \mathbb{F}_4] = 2$. Hence $\mathbb{F}_2(\alpha)$ is the splitting field of the separable polynomial $x^5 - 1$ over $\mathbb{F}_4$, and $\mathrm{Gal}(x^5 - 1/\mathbb{F}_4) = \mathrm{Gal}(\mathbb{F}_2(\alpha)/\mathbb{F}_4) \cong \mathbb{Z}_2$.

Over $\mathbb{F}_4$, f is no longer irreducible: we can write $\mathbb{F}_4 = \{0, 1, \beta, \beta + 1\}$ with $\beta^2 = \beta + 1$; then $f = (x^2 + \beta x + 1)(x^2 + (\beta + 1)x + 1)$. ◊

3.2 Solvability by radicals

First the formality.

Definition 2.1 A polynomial $f \in k[x]$ is solvable by radicals if there is a chain of field extensions

$$k = K_0 \subset K_1 \subset \cdots \subset K_r \tag{2-1}$$

of the form

$$K_{i+1} = K_i\big(\sqrt[n_i]{a_i}\big)$$

for various positive integers n_i and elements $a_i \in K_i$, $0 \le i \le r - 1$, such that f splits in K_r.

In this situation we call each K_{i+1}/K_i a simple radical extension, K_r/k a radical extension, and (2-1) a radical sequence. ◊

Definition 2.2 We call K/k a cyclic extension if it is Galois with cyclic Galois group. ◊

Theorem 2.3 *Let k be a field containing a primitive n^{th} root of unity. Then K/k is a cyclic extension of degree n if and only if $K = k(\sqrt[n]{a})$ for some $a \in k$.*

Proof. ($\Leftarrow$) Let $\zeta \in k$ be a primitive n^{th} root of 1. Suppose that $K = k(\alpha)$ where $\alpha = \sqrt[n]{a}$. Then K/k is the splitting field of the polynomial $x^n - a \in k[x]$ because it has n distinct zeroes $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ in K.

If $\sigma \in \mathrm{Gal}(K/k)$, then $\sigma(\alpha) = \zeta^{i(\sigma)}\alpha$ for some $i(\sigma) \in \mathbb{Z}_n$. The map $\sigma \mapsto i(\sigma)$ is a homomorphism $\mathrm{Gal}(K/k) \to \mathbb{Z}_n$. But it is also injective, and hence an isomorphism because $|\mathrm{Gal}(K/k)| = [K : k] = n = |\mathbb{Z}_n|$.

($\Rightarrow$) Suppose $\mathrm{Gal}(K/k) = \langle\sigma\rangle \cong \mathbb{Z}_n$. By Dedekind's Proposition **??**, the distinct maps $\mathrm{id}_K, \sigma, \sigma^2, \ldots, \sigma^{n-1} : K \to K$ are linearly independent over K. Hence there is some $\beta \in K$ such that

$$\alpha := \beta + \zeta^{-1}\sigma(\beta) + \cdots + \zeta^{1-n}\sigma^{n-1}(\beta)$$

is non-zero. Now $\sigma(\alpha) = \alpha\zeta$ so α^n is invariant under σ, hence invariant under $\mathrm{Gal}(K/k)$. Thus $\alpha^n = a \in k$. Because $x^n - a \in k[x]$ has n distinct zeroes $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ in K, it is separable over k and splits in K.

Every element of $\mathrm{Gal}(K/k)$ sends $k(\alpha)$ to $k(\alpha)$, so restriction gives a homomorphism $\mathrm{Gal}(K/k) \to \mathrm{Gal}(k(\alpha)/k)$, $\phi \mapsto \phi|_{k(\alpha)}$, which is clearly injective. Hence $[k(\alpha) : k] \geq n$, and it follows that $K = k(\alpha) = k(\sqrt[n]{a})$. □

Lemma 2.4 *Let F/k be an extension. If $f \in k[x]$ is separable, then* $\mathrm{Gal}(f/F)$ *is isomorphic to a subgroup of* $\mathrm{Gal}(f/k)$.

Proof. First observe that f remains separable over F because its irreducible factors over F divide its irreducible factors over k, and therefore have no repeated zeroes.

Let $L = F(\alpha_1, \ldots, \alpha_n)$ be a splitting field for f over F, where $\alpha_1, \ldots, \alpha_n$ are the zeroes of f. Then $K := k(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f over k.

If $\sigma \in \mathrm{Gal}(L/F) = \mathrm{Gal}(f/F)$, then each $\sigma(\alpha_i)$ is a zero of f so equal to some α_j. Hence $\sigma(K) \subset K$. The map $\sigma \mapsto \sigma|_K$ is a group homomorphism $\mathrm{Gal}(f/F) \to \mathrm{Gal}(K/k) = \mathrm{Gal}(f/k)$. This map is injective because if $\sigma|_K = \mathrm{id}_K$, then $\sigma_(\alpha_i) = \alpha_i$ for all i whence $\sigma = \mathrm{id}_L$. □

Theorem 2.5 *Let $f \in k[x]$ and suppose that* $\mathrm{char}\, k$ *does not divide* $\deg f$. *If* $\mathrm{Gal}(f/k)$ *is solvable, then f is solvable by radicals.*

Proof. Set $n = (\deg f)!$. By Proposition 1.4, there is an extension F/k generated by a primitive n^{th} root of unity. By Lemma 2.4, $\mathrm{Gal}(f/F)$ is isomorphic to a subgroup of $\mathrm{Gal}(f/k)$ so is also solvable. Since F/k is a radical extension, it suffices to show that f is solvable by radicals over F. Hence we can, and will, assume that k contains a primitive n^{th} root of unity.

Let K/k be a splitting field of f, and choose a solvable series

$$\mathrm{Gal}(K/k) = G_0 \supset G_1 \supset \ldots \supset G_r = \{1\}$$

such that each G_i/G_{i+1} is cyclic. Define $K_i := K^{G_i}$ to obtain a sequence of fields

$$k = K_0 \subset K_1 \subset \ldots \subset K_r = K$$

with each K_{i+1}/K_i a cyclic extension whose degree, d say, divides n. Since K_i contains a primitive n^{th} root of unity, $K_{i+1} = K_i\big(\sqrt[d]{a}\big)$ for some $a \in K_i$ by Theorem 2.3. Hence K is a radical extension of k. □

Lemma 2.6 *The normal closure of a radical extension is a radical extension.*

Proof. Let $K = k(\alpha_1, \ldots, \alpha_r)$ be a radical extension. We argue by induction on r. Thus, we assume that the normal closure, say L', of $K' = k(\alpha_1, \ldots, \alpha_{r-1})$ is a radical extension of k.

The normal closure of K, say L, must contain L', so is equal to the normal closure of $L'(\alpha_r)$. Notice that $L'(\alpha_r)$ is a radical extension of L', so is a radical extension of k. Let f be the minimal polynomial of α_n over L' and let $\beta_1, \ldots, \beta_d$ be the zeroes of f in L. Then $L = L'(\beta_1, \ldots, \beta_d)$. Since $L'(\beta_i) \cong L'(\alpha_r)$, $L'(\beta_i)$ is a radical extension of k. Since L is generated by the fields $L'(\beta_i)$, the second remark above implies that L is a radical extension of k. □

Remark. We need a more precise version of Lemma 2.6. With the notation in its proof, suppose that $\alpha_i^{n_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$ for all i. Then L is built from k by adjoining only n_i^{th} roots too.

Theorem 2.7 *Suppose that $f \in k[x]$ is solvable by radicals, say by taking various n_i^{th} roots of unity. If* $\operatorname{char} k$ *does not divide any of the n_is, then* $\operatorname{Gal}(f/k)$ *is solvable.*

Proof. Let n be the least common multiple of the various n_is. Then $\operatorname{char} k$ does not divide n. By Lemma 2.6 and the hypothesis, there is a radical Galois extension L/k in which f splits, and the remark after that Lemma shows that L involves adjoining only n^{th} roots. Let K/L be the splitting field for $x^n - 1$ where $n = [L : k]$.

Let F/k be the splitting field of f. Since

$$\operatorname{Gal}(f/k) \cong \frac{\operatorname{Gal}(K/k)}{\operatorname{Gal}(K/F)}$$

it suffices to show that $\operatorname{Gal}(K/k)$ is solvable.

Now K contains a primitive n^{th} root of unity, say ζ, and we have a chain

$$k \subset k(\zeta) = K_0 \subset K_1 \subset \cdots \subset K_r = K$$

in which each $K_{i+1} = K_i\big(\sqrt[d]{a_i}\big)$ for some $a_i \in K_i$ and some integer d_i dividing n. By Theorem 2.3, K_{i+1}/K_i is a cyclic extension.

Now $k(\zeta)/k$ is Galois with abelian Galois group, and

$$\operatorname{Gal}(k(\zeta)/k) \cong \frac{\operatorname{Gal}(K/k)}{\operatorname{Gal}(K/k(\zeta))}$$

so $\mathrm{Gal}(K/k)$ is solvable if and only if $\mathrm{Gal}(K/k(\zeta))$ is solvable.

Let G_i be the subgroup of $\mathrm{Gal}(K/k(\zeta))$ corresponding to K_i. Then there is a chain

$$\mathrm{Gal}(K/k(\zeta)) = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

in which G_{i+1} is normal in G_i because K_{i+1}/K_i is normal, and G_i/G_{i+1} is cyclic because K_{i+1}/K_i is cyclic. □

Example 2.8 Let $k = \mathbb{F}_p(t)$ be the rational function field over the field of p elements. If $f = x^p - x - t \in k[x]$, then $\mathrm{Gal}(f/k) \cong \mathbb{Z}_p$, so is solvable. However, f is not solvable by radicals.

Let α be a zero of f. Then

$$(\alpha+1)^p - (\alpha+1) - t = \alpha^p + 1 - \alpha - 1 - t = 0$$

so $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1$ are the distinct zeros of f. Hence f is separable. The splitting field of f is $k(\alpha)$ and the minimal polynomial of α is f, so $[k(\alpha) : k] = p$. Hence the Galois group is $\mathbb{Z}_p$.

♢

The proof of the next result uses Cauchy's Theorem, which will be proved later, and a technical result on the symmetric group that will also be proved later. In particular, we use the fact that the symmetric group S_n is not solvable if $n \geq 5$.

Theorem 2.9 *Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree, say p. If f has exactly two non-real zeroes, then $\mathrm{Gal}(f/\mathbb{Q}) \cong S_p$. In particular, if $p \geq 5$, then f is not solvable by radicals.*

Proof. By the Fundamental Theorem of Algebra f splits in $\mathbb{C}$. Let K be the splitting field for f over $\mathbb{Q}$, and set $G = \mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q})$. By Lemma 2.4, the action of G on the zeroes of f gives an injective group homomorphism $G \to S_p$.

By Lemma 3.2, p divides $[K : \mathbb{Q}] = |G|$ so, by Cauchy's Theorem, G has an element σ of order p. This must be a p-cycle, say $\sigma = (12\ldots p)$. Complex conjugation is a $\mathbb{Q}$-automorphism of $\mathbb{C}$, so restricts to a $\mathbb{Q}$-automorphism of K. But conjugation fixes the $p-2$ real zeroes of f, and permutes the two non-real zeroes so is a 2-cycle. Let's assume this transposition is $(1n)$.

Notice that σ^n is again a p-cycle and $\sigma^n = (1\,n\,2n{-}1\,\cdots)$, so after relabelling we can assume that G contains $(12\ldots p)$ and (12). But these two elements generate all of S_p so $G = S_p$. □

Exercise. In S_4, (13) and (1234) do *not* generate S_4, so check the "without loss of generality" claim in the last sentence of the proof—you need to use the fact that p is prime.

Example 2.10 The polynomial $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals. By Eisenstein's criterion f is irreducible. Since $f'(x) = 5x^4 - 6$ has only two real zeroes, say $\pm\alpha$, f has at most three real zeroes by Rolle's Theorem. Since $f(-\alpha) > 0 > f(\alpha)$ and $f(x) to \pm\infty$ as $x \to \pm\infty$, f has three real zeroes. Hence $\mathrm{Gal}(f/\mathbb{Q}) \cong S_5$. ◊

3.3 Cyclotomic polynomials

Definition 3.1 For each positive integer n define

$$\zeta_n := e^{2\pi i/n}.$$

We call $\mathbb{Q}(\zeta_n)$ the n^{th} cyclotomic extension of $\mathbb{Q}$.

The minimal polynomial of ζ_n over $\mathbb{Q}$ is called the n^{th} cyclotomic polynomial and is denoted by $\Phi_n(x)$. ◊

Claim: $\mathbb{Q}(\xi_m, \xi_n) = \mathbb{Q}(\xi_\ell)$ where $\ell = \mathrm{lcm}\{m, n\}$. To see this, first write $\ell = ma = nb$ where $(a, b) = 1$. Then ξ_ℓ^a is a primitive n^{th} root of unity, so $\xi_n \in \mathbb{Q}(\xi_\ell)$. Similarly, $\xi_m \in \mathbb{Q}(\xi_\ell)$. So it remains to prove that $\xi_\ell \in \mathbb{Q}(\xi_m, \xi_n)$. It suffices to show that $\mathbb{Q}(\xi_m, \xi_n)$ contains a primitive ℓ^{th} root of unity. Notice that $\xi_\ell^a = \xi_n$ and $\xi_\ell^b = \xi_m$. There are integers c and d such that $1 = ac + bd$. Hence $\xi_\ell = \xi_n^c \xi_m^d$. ◊

We write

$$\mu_n := \{\text{the group of } n^{\text{th}} \text{ roots of unity}\} \subset \mathbb{C}.$$

There is an isomorphism of groups $\mathbb{Z}_n \to \mu_n$ defined by $a \mapsto \xi_n^a$. If $1 \le a < n$, ξ_n^a is a primitive d^{th} root of unity where $d = \gcd(a, n)$.

If we view $\mathbb{Z}_n$ as a ring and write U_n for its group of units, then ξ_n^a is a primitive n^{th} root of unity if and only if $a \in U_n$. Hence the set of primitive n^{th} roots of unity is the image in μ_n of U_n.

Lemma 3.2 *The n^{th} cyclotomic polynomial is*

$$\Phi_n(x) = \prod_{\substack{\xi \in \mu_n \\ \xi \text{ primitive}}} (x - \xi) = \prod_{\substack{1 \le a < n \\ \gcd(a,n)=1}} (x - \xi_n^a)$$

Proof. It is clear that these two products are equal.

□

Definition 3.3 The Euler ϕ-function $\phi : \mathbb{N} \to \mathbb{N}$ is defined by

$$\phi(n) := \text{the number of integers } 1 \le m \le n \text{ such that } (m, n) = 1.$$

◊

Corollary 3.4 *Let n be a positive integer. Then*

1. $\deg \Phi_n(x) = \phi(n)$;
2. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$;
3. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is isomorphic to the group of units in* $\mathbb{Z}_n$.

Proof. The set $U_n := \{m \mid 1 \leq m \leq n \text{ and } (m, n) = 1\}$ has cardinality $\phi(n)$. The set U_n has two other descriptions: it is the set of m such that ζ_n^m is a primitive n^{th} root of unity; its image in $\mathbb{Z}_n$ is the group of units. The map $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{Z}_n$, $\sigma \mapsto i(\sigma)$ defined by $\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$, is an isomorphism to U_n. □