Chapter 7

Solution of Equations by Radicals

We now establish the fact that we cannot always express the roots of a polynomial by formulae of the form similar to that of the quadratic formula. To be precise, we shall show that the splitting field of a polynomial is what is known as a radical extension if and only if the Galois group is soluble. In Example 7.15, we give an example of a polynomial whose Galois group is not soluble and hence it is not soluble by radicals.

Radical extensions

In this chapter, we consider the question of when there is a formula for the solutions of a polynomial equation analogous to the standard formula for roots of a quadratic polynomial. By a "formula" for the solution, we mean an expression of form similar to, for example,

$$\alpha = \frac{1 + \sqrt[7]{\frac{-2+\sqrt{-3}}{4+\sqrt[5]{5}}}}{2 - \sqrt[3]{17}};$$

that is, formed by repeated use of field operations and taking (various types of) roots. In order to formalize what we mean by these formulae and to make precise what we mean by "solution by radicals", we make the following definition.

Definition 7.1 (i) An extension K of a field F is said to be a *simple radical extension* if $K = F(\alpha)$ for some element $\alpha \in K$ satisfying $\alpha^p \in F$ for some prime number p.

(ii) An extension K of a field F is called a *radical extension* if there is a sequence of intermediate fields
$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$
such that K_i is a simple radical extension of K_{i-1} for $i = 1, 2, \dots, n$.

If K is a radical extenson of F, then

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

where, for each i, some prime power of α_i belongs in the subfield $F(\alpha_1, \alpha_2, \dots, \alpha_{i-1})$. We can therefore view α_i as being a root of an element of $F(\alpha_1, \alpha_2, \dots, \alpha_{i-1})$, so every element of K can be written as a formula involving field operations and pth roots (for a variety of prime numbers p).

The following observations shows that there is no restriction in only permitting pth roots for prime values p.

Lemma 7.2 *Suppose $K = F(\alpha)$ where $\alpha^m \in F$ for some positive integer $m > 1$. Then K is a radical extension of F.*

PROOF: We proceed by induction on m. If m is prime, then by definition K is a simple radical extension of F and there is nothing to prove.

Otherwise $m = kp$ for some positive integer $k > 1$ and some prime p. Put $\beta = \alpha^p$ and consider the chain of subfields

$$F \subseteq F(\beta) \subseteq F(\alpha).$$

(Note $\beta \in F(\alpha)$ as $\beta = \alpha^p$, so $F(\beta) \subseteq F(\alpha)$.) Now $\beta^k = \alpha^{kp} = \alpha^m \in F$, so by induction $F(\beta)$ is a radical extension of F, say

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = F(\beta),$$

where each L_i is a simple radical extension of L_{i-1}. Then

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n = F(\beta) \subseteq F(\alpha) = K$$

and $F(\alpha)$ is a simple radical extension of $F(\beta)$, since $\alpha^p = \beta \in F(\beta)$. We conclude that K is indeed a radical extension of F. This completes the induction step. □

Also note that if K is a radical extension of F, say

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K,$$

where each K_i is a simple radical extension of K_{i-1}; that is, $K_i = K_{i-1}(\alpha_i)$ where $\alpha_i^p \in K_{i-1}$ for some prime p (p depending on i). Thus α_i is algebraic over K_{i-1}, so $|K_i : K_{i-1}|$ is finite and hence, by the Tower Law, K is a finite extension of F. We therefore have established the following additional observation.

Lemma 7.3 *Any radical extension is a finite extension.* □

Definition 7.4 Let $f(X)$ be a polynomial over a field F of characteristic zero. We say that $f(X)$ is *soluble by radicals* if there exists a radical extension of F over which $f(X)$ splits.

Thus, $f(X)$ is soluble by radicals when the splitting field K of $f(X)$ over F is contained in some radical extension L of F. This is then consistent with what we referred to previously as a "formula for a root of a polynomial equation." If $f(X)$ is soluble by radicals, then every root is some element of a radical extension of the base field and hence can be expressed as a formula involving repeated use of field operations and pth roots (for a variety of prime numbers p).

We wish to make use of Galois groups and the Fundamental Theorem of Galois Theory in the context of solution by radicals. Accordingly we shall need to be considering normal extensions and so shall make use of the following lemma. Note that separability comes for free since we are now exclusively working over a field of characteristic zero and so can use Corollary 4.9.

Lemma 7.5 *Let K be a radical extension of a field F of characteristic zero. Then there exists an extension L of K such that L is a normal radical extension of F.*

PROOF: Let

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$$

be a sequence of intermediate fields such that each K_i is a simple radical extension of K_{i-1}. Then there exists $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ and prime numbers $p_1, p_2, \dots, p_n$ such that

$$K_i = F(\alpha_1, \alpha_2, \dots, \alpha_i) \qquad \text{and} \qquad \alpha_i^{p_i} = \lambda_i \in K_{i-1}.$$

For each i, let $f_i(X)$ be the minimum polynomial of α_i over F. We construct a chain of fields L_i as follows. Define $L_0 = F$ and then L_1 to be the splitting field of $f_1(X)$ over $K_1 = F(\alpha_1)$. Thus L_1 is obtained from F by adjoining the roots of $f_1(X)$ (one of which is α_1) and also $K_1 \subseteq L_1$.

Suppose that we have constructed L_{i-1} with $K_{i-1} \subseteq L_{i-1}$. Then define L_i to be the splitting field for $f_i(X)$ over $L_{i-1}(\alpha_i)$; that is, L_i is obtained from L_{i-1} by adjoining the roots of $f_i(X)$ (one of which is α_i). In particular,

$$K_i = K_{i-1}(\alpha_i) \subseteq L_{i-1}(\alpha_i) \subseteq L_i.$$

By this inductive method, we have constructed a chain of fields

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_n$$

with $K_i \subseteq L_i$ for each i and such that L_i is obtained by adjoining the roots of $f_i(X)$ to L_{i-1}. As a consequence, L_i is the splitting field of $f_1(X)\, f_2(X) \dots f_i(X)$ over F, so is a normal extension of F (via Theorem 3.13).

We claim that L_i is a radical extension of F. We proceed by induction on i, noting that the result is trivial for $i = 0$ since $L_0 = F$. Therefore assume L_{i-1} is a radical extension of F for some $i \geqslant 1$. We shall prove that L_i is a radical extension of F by constructing the necessary intermediate fields between L_{i-1} and L_i.

Let β_1, β_2, …, β_k be the roots of $f_i(X)$ in L_i, where $\beta_1 = \alpha_i$ without loss of generality. Then by definition

$$L_i = L_{i-1}(\beta_1, \beta_2, \dots, \beta_k).$$

Consider any root β_j. Since $f_i(X)$ is an irreducible polynomial over F, by Lemma 3.5, there is an isomorphism $\psi\colon F(\beta_1) \to F(\beta_j)$ such that $\psi|_F$ is the identity map $F \to F$ and $\beta_1\psi = \beta_j$. Now L_i is the splitting field for $f_1(X)\, f_2(X) \dots f_i(X)$ over both $F(\beta_1)$ and $F(\beta_j)$ (one obtains L_i from these fields by adjoining the other roots of this product). Hence, by Theorem 3.6, there exists an isomorphism $\theta\colon L_i \to L_i$ such that $\theta|_{F(\beta_1)} = \psi$. Thus θ is an element of the Galois group $\mathrm{Gal}(L_i/F)$ and

$$\alpha_i\theta = \beta_1\theta = \beta_1\psi = \beta_j.$$

Now as L_{i-1} is a normal extension of F, by Lemma 6.10 applied to the Galois group $\mathrm{Gal}(L_i/F)$,

$$L_{i-1}\theta \subseteq L_{i-1}.$$

Hence

$$\beta_j^{p_i} = (\alpha_i\theta)^{p_i} = (\alpha_i^{p_i})\theta = \lambda_i\theta \in L_{i-1}.$$

Therefore we have a chain of simple radical extensions:

$$L_{i-1} \subseteq L_{i-1}(\beta_1) \subseteq L_{i-1}(\beta_1, \beta_2) \subseteq \dots \subseteq L_{i-1}(\beta_1, \beta_2, \dots, \beta_k) = L_i.$$

It follows that L_i is a radical extension of L_{i-1} and, by our inductive hypothesis, also then a radical extension of F.

Taking $L = L_n$, we now have the required normal radical extension of F that contains $K = K_n$. □

Soluble groups and other group theory

The key theorem of the chapter links radical extensions to what are called soluble groups. Accordingly, we need to introduce enough group theory to work with such groups. We shall omit the proofs, since they belong most naturally in a course on group theory (for example, they appear in the version of *MT5824 Topics in Groups* that I taught in some years).

The definition we require is the following:

Definition 7.6 A group G is called *soluble* (*solvable* in the U.S.) if there are subgroups

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots \geqslant G_d = \mathbf{1} \tag{7.1}$$

such that, for each $i = 1, 2, \ldots, d$, the subgroup G_i is normal in G_{i-1} and the quotient group G_{i-1}/G_i is abelian.

There are multiple equivalent possible definitions for the concept of a soluble group. For example, an equivalent definition is that the derived series of G reaches the trivial subgroup $\mathbf{1}$ after finitely many steps. The concept of commutators and derived subgroups is not essential for the Galois Theory context and we shall stick to soluble groups as given by Definition 7.6. The following observations are straightforward from the above definition:

- An abelian group is soluble: If G is abelian take $G_0 = G$ and $G_1 = \mathbf{1}$ in the definition.
- A non-abelian simple group is not soluble: If G is simple, then $G_1 = \mathbf{1}$ and G is only soluble if it is abelian.

The basic properties of soluble groups that we need are the following:

Proposition 7.7 (i) *If G is soluble, then every subgroup of G is soluble.*

(ii) *If G is soluble, then every quotient group of G is soluble.*

(iii) *If N is a normal subgroup of G such that G/N and N are both soluble, then G is soluble.*

The proofs of these facts are omitted since they belong most naturally in a course on group theory. If H is a subgroup of a soluble group G with a chain of subgroups as in Equation (7.1), then the corresponding chain for H has quotients isomorphic to subgroups of the G_{i-1}/G_i, so are abelian. If N is a normal subgroup of G, then the quotients in the corresponding chain for G/N are quotients of the G_{i-1}/G_i, so are abelian. Finally, for (iii), the quotients for the chain for G are those of G/N together with those for N. (More details are found on the Problem Sheet VII.)

In the context of soluble groups, we shall also need the following observation:

Proposition 7.8 *Let G be a finite soluble group. Then G has a chain of subgroups*

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

such that, for $i = 1, 2, \ldots, n$, H_i is a normal subgroup of H_{i-1} and H_{i-1}/H_i is cyclic of prime order.

Proof: [Slightly sketched] We start with the chain of subgroups

$$G = G_0 > G_1 > G_2 > \cdots > G_d = \mathbf{1}$$

provided by the definition of a soluble group. Suppose some quotient G_{i-1}/G_i is not simple. This means that there is a non-trivial proper normal subgroup and this corresponds to some normal subgroup N of G_{i-1} containing G_i. We then produce a new chain of subgroups

$$G = G_0 > \cdots > G_{i-1} > N > G_i > \cdots > G_d = \mathbf{1}$$

and here N/G_i is a subgroup of G_{i-1}/G_i so is abelian and, by the Third Isomorphism Theorem,

$$G_{i-1}/N \cong \frac{G_{i-1}/G_i}{N/G_i}$$

is abelian as a quotient of an abelian group.

We repeat this process until we cannot proceed any further. (This must eventually stop since G is finite so has only finitely many subgroups.) Our final product is a chain of subgroups

$$G = H_0 > H_1 > H_2 > \cdots > H_n = \mathbf{1}$$

such that each H_i is a normal subgroup of H_{i-1} and H_{i-1}/H_i is both abelian and simple; that is, they are all cyclic of prime order. □

We also state one further fact from group theory that we need. For those that have covered Sylow's Theorem in a previous course can deduce it from that theorem. (It is basically an easier first case of that theorem.)

Theorem 7.9 (Cauchy's Theorem) *Let G be a finite group and p be a prime number that divides the order of G. Then G contains an element of order p.*

Deduction from Sylow's Theorem: Let P be a Sylow p-subgroup of G. The hypothesis ensures $P \neq \mathbf{1}$ and then if g is a non-identity element of P it has order p^k for some $k > 0$. Now $g^{p^{k-1}}$ has order p. □

Examples of polynomials with abelian Galois groups

When considering radical extensions of a field, we involve a number of intermediate fields, each of which is a simple radical extension of the previous one. Consequently, we shall first consider the special case of a simple radical extension $F(\alpha)$ of a field F. Here we know that $\alpha^p = \lambda$ for some $\lambda \in F$ and some prime number p. Accordingly the following two lemmas provide us with the detailed information that we need and in both cases we observe that the resulting Galois group is abelian (and hence link with our definition of soluble group above).

Lemma 7.10 *Let F be a field of characteristic zero and let K be the splitting field of $X^p - 1$ over F, where p is a prime number. Then the Galois group $\mathrm{Gal}(K/F)$ is abelian.*

Proof: Let $f(X) = X^p - 1$. The formal derivative is $Df(X) = pX^{p-1}$, so $f(X)$ and $Df(X)$ has no common factors of degree $\geqslant 1$. Hence the roots of $f(X)$ in K are distinct. Consider the set Z of roots of $f(X)$ in K. If $\alpha, \beta \in Z$, then

$$(\alpha\beta)^p = \alpha^p\beta^p = 1 \qquad \text{and} \qquad (1/\alpha)^p = 1/\alpha^p = 1,$$

so Z is closed under multiplication and division. Hence Z is a subgroup of K^* of order p. It is therefore cyclic, so there is a generator ε for Z. The roots of $f(X)$ are then ε, ε^2, …, ε^{p-1} and 1, so

$$K = F(\varepsilon).$$

Any $\phi \in \mathrm{Gal}(K/F)$ is then determined by its effect on ε and it must map ε to a root of $f(X)$; that is, to a power of ε. Let $\phi, \psi \in \mathrm{Gal}(K/F)$, say

$$\phi \colon \varepsilon \mapsto \varepsilon^i \qquad \text{and} \qquad \psi \colon \varepsilon \mapsto \varepsilon^j,$$

for some i and j. Then

$$\varepsilon\phi\psi = (\varepsilon^i)\psi = (\varepsilon\psi)^i = (\varepsilon^j)^i = \varepsilon^{ij}$$

and $\varepsilon\psi\phi = \varepsilon^{ij}$ similarly. Since these automorphisms are determined by their effect on ε, we conclude $\phi\psi = \psi\phi$, as required. □

Lemma 7.11 *Let F be a field of characteristic zero in which $X^n - 1$ splits. Let $\lambda \in F$ and let K be the splitting field for $X^n - \lambda$ over F. Then the Galois group $\mathrm{Gal}(K/F)$ is abelian.*

Proof: Fix one root α of $X^n - \lambda$ in K. Since $X^n - 1$ splits over F, any other root of $X^n - \lambda$ in K has the form $\varepsilon\alpha$ where ε is a root of $X^n - 1$. Thus $K = F(\alpha)$.

Now any $\phi \in \mathrm{Gal}(K/F)$ is determined by its effect on α and must map α to a root of $X^n - \lambda$. Hence if $\phi, \psi \in \mathrm{Gal}(K/F)$, they have the form

$$\phi \colon \alpha \mapsto \varepsilon\alpha \qquad \text{and} \qquad \psi \colon \alpha \mapsto \eta\alpha$$

where $\varepsilon, \eta \in F$ are roots of $X^n - 1$. Now

$$\alpha\phi\psi = (\varepsilon\alpha)\psi = \varepsilon\eta\alpha,$$

since ψ fixes ε (as $\varepsilon \in F$). Similarly $\alpha\psi\phi = \varepsilon\eta\alpha$. Hence $\phi\psi = \psi\phi$, as required. □

Galois groups of normal radical extensions

We now have the ingredients needed to prove our first result about the Galois group of a normal radical extension.

Theorem 7.12 *Let F be a field of characteristic zero and K be a normal radical extension of F. Then the Galois group* $\mathrm{Gal}(K/F)$ *is soluble.*

Corollary 7.13 (Galois) *Let $f(X)$ be a polynomial over a field F of characteristic zero. If $f(X)$ is soluble by radicals then the Galois group of $f(X)$ over F is soluble.*

Proof: By assumption, the splitting field K for $f(X)$ over F is contained in some radical extension of F. By applying Lemma 7.5, we pass to the situation where

$$F \subseteq K \subseteq L$$

and L is a *normal* radical extension of F. Theorem 7.12 then tells us that $\mathrm{Gal}(L/F)$ is a soluble group. However, K is a normal extension of F, so part (iv) of the Fundamental Theorem of Galois Theory (Theorem 6.7) tells us that

$$\mathrm{Gal}(f(X)) = \mathrm{Gal}(K/F) \cong \frac{\mathrm{Gal}(L/F)}{L^*},$$

which is a quotient of a soluble group, hence soluble by Proposition 7.7(ii). This establishes the corollary. □

Proof of Theorem 7.12: We proceed by induction on the degree $|K : F|$. Note that if $|K : F| = 1$, then $\mathrm{Gal}(K/F) = \mathbf{1}$, so is certainly soluble. Assume $|K : F| > 1$ and let

$$F = F_0 \subset F_1 \subset \cdots \subset F_k = K$$

be a chain of intermediate fields such that F_i is a simple radical extension of F_{i-1}, say $F_i = F_{i-1}(\alpha_i)$. We may assume that $F_i \neq F_{i-1}$ for all i. We shall now construct some normal extensions of F inside K from the element α_1 with $F_1 = F(\alpha_1)$. This will enable us to apply induction.

Suppose $\alpha_1^p = \lambda \in F$ for some prime number p and let $g(X)$ be the minimum polynomial of α_1 over F. Note that $g(X)$ divides $X^p - \lambda$. Since $g(X)$ has a root in K and K is a normal extension of F, $g(X)$ must split in K. Now $\alpha_1 \notin F$, so $\deg g(X) \geqslant 2$ and, moreover by use of Proposition 4.6, $g(X)$ is separable and so has distinct roots. Let β be a root of $g(X)$ in K with $\beta \neq \alpha_1$. Put $\varepsilon = \beta/\alpha_1$. Then $\varepsilon \neq 1$ and

$$\varepsilon^p = \beta^p/\alpha_1^p = \lambda/\lambda = 1.$$

Thus ε is an element of order p in the multiplicative group of K, so the polynomial $X^p - 1$ splits in K with roots ε, ε^2, ..., ε^{p-1} and 1. Let $L = F(\varepsilon)$, which is then the splitting field of $X^p - 1$ over F.

Then let $M = L(\alpha_1) \subseteq K$. Now the roots of $X^p - \lambda$ in K are α_1, $\varepsilon\alpha_1$, ..., $\varepsilon^{p-1}\alpha_1$, all of which belong to M. Consequently, $M = L(\alpha_1)$ is the splitting field for $X^p - \lambda$ over L (and also over F).

Now consider the chain of fields

$$F \subseteq L \subseteq M \subseteq K. \tag{7.2}$$

We first apply Lemma 7.10 to the extension $L = F(\varepsilon)$ of F and conclude that $\mathrm{Gal}(L/F)$ *is abelian.* We also apply Lemma 7.11 to the extension $M = L(\alpha_1)$ of L and conclude that $\mathrm{Gal}(M/L)$ *is abelian.* We also know that $\alpha_1 \in M$, so $M \neq F$. Hence the degree $|K : M|$ is strictly smaller than $|K : F|$. Now K is a normal extension of F, so it is a normal extension of M. Also we have

$$M = M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k = K$$

where $M_i = M_{i-1}(\alpha_i)$ and some prime power of α_i lies in $F_{i-1} \subseteq M_{i-1}$. Hence K is a radical extension of M. We now apply induction to conclude that $\mathrm{Gal}(K/M)$ *is soluble.*

Now let us turn to the Galois group $G = \mathrm{Gal}(K/F)$. We shall apply the Fundamental Theorem of Galois Theory (Theorem 6.7). Applying the Galois correspondence to the fields appearing in Equation (7.2) yields subgroups of G:

$$\mathbf{1} \leqslant M^* \leqslant L^* \leqslant G,$$

where $M^* = \mathrm{Gal}(K/M)$ and $L^* = \mathrm{Gal}(K/L)$ occurring as subgroups of G. We have observed M^* is soluble. Now M is a normal extension of L (as the splitting field of $X^p - \lambda$), so by part (iv) of the Fundamental Theorem of Galois Theory, $M^* \trianglelefteqslant L^* = \mathrm{Gal}(K/L)$ and

$$L^*/M^* \cong \mathrm{Gal}(M/L),$$

which is abelian, so soluble. Finally, L is a normal extension of F (as the splitting field of $X^p - 1$), so $L^* \trianglelefteqslant G$ and

$$G/L^* \cong \mathrm{Gal}(L/F),$$

which is abelian, so soluble. Now applying Proposition 7.7(iii) twice, we conclude that $G = \mathrm{Gal}(K/F)$ is soluble, completing the induction. □

A polynomial which is insoluble by radicals

In the example below we give an example of a polynomial that is not soluble by radicals. We do this by demonstrating that its Galois group is not soluble, with use of the following lemma, and then making use of Corollary 7.13.

Lemma 7.14 *Let p be a prime and $f(X)$ be an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose that $f(X)$ has precisely two non-real roots in $\mathbb{C}$. Then the Galois group of $f(X)$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_p.*

Proof: By adjoining the roots of $f(X)$ found in $\mathbb{C}$, we can construct a splitting field K for $f(X)$ contained in $\mathbb{C}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$, the Galois group of $f(X)$ over $\mathbb{Q}$. By Lemma 6.14, we may regard G as a subgroup of the symmetric group on Ω, the set of roots of $f(X)$ in K. We know $|\Omega| = p$, so the symmetric group on Ω is (isomorphic to) S_p.

Now by part (i) of the Fundamental Theorem of Galois Theory (Theorem 6.7),

$$|G| = |K : \mathbb{Q}|.$$

Let α be one of the roots of $f(X)$. Then $|K : \mathbb{Q}|$ is divisible by $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f(X) = p$. Hence, by Cauchy's Theorem, G possesses an element of order p. However, an element of order p in S_p must be a p-cycle, so G contains a p-cycle σ. By taking a suitable power of σ, we can assume that $\sigma = (\alpha_1 \ \alpha_2 \dots \alpha_p)$ where α_1 and α_2 are the two non-real roots of $f(X)$.

Observe, in addition, that complex conjugation must permute the roots of $f(X)$, so induces some $\mathbb{Q}$-automorphism τ in G. This must fix the $p-2$ real roots of $f(X)$ and hence must swap the two non-real roots. Thus τ is the transposition $(\alpha_1 \ \alpha_2)$.

Now we know that $(\alpha_1 \ \alpha_2)$ and $(\alpha_1 \ \alpha_2 \dots \alpha_p)$ generate the symmetric group S_p and hence we conclude $G = S_p$. □

Example 7.15 *The quintic polynomial $f(X) = X^5 - 9X + 3$ over $\mathbb{Q}$ is not soluble by radicals.*

Proof: By Eisenstein's Criterion (with $p = 3$), $f(X)$ is irreducible over $\mathbb{Q}$. Now

$$f(-2) = -11, \qquad f(-1) = 11, \qquad f(1) = -5, \qquad f(2) = 17.$$

Hence, by the Intermediate Value Theorem, $f(X)$ has at least three real roots (one between -2 and -1, one between -1 and 1 and one between 1 and 2). The derivative of $f(X)$ is

$$f'(X) = 5X^4 - 9,$$

so $f'(X)$ has exactly two real roots, so $f(X)$ has two turning points. There must be a turning point between every pair of real roots (Rolle's Theorem), so $f(X)$ has *exactly* three real roots and therefore two non-real roots. Now Lemma 7.14 tells us that

$$\mathrm{Gal}(f(X)) \cong S_5,$$

the symmetric group of degree 5. Now the alternating group A_5 is a non-abelian simple group and is therefore not soluble. Hence, using Proposition 7.7(i), the Galois group of $f(X)$ over $\mathbb{Q}$ is not soluble and, by Corollary 7.13, $f(X)$ is not soluble by radicals. □

Thus for this particular quintic polynomial, we cannot express the roots using formulae involving field operations and pth roots.

Galois's Great Theorem

We finish the chapter by establish the converse of Corollary 7.13; that is, we shall show that if the Galois group of a polynomial is soluble then the polynomial is soluble by radicals. We begin with a special case, which can be viewed as a base step of an induction argument.

Lemma 7.16 *Let K be a finite normal extension of a field F of characteristic zero and suppose that $X^p - 1$ splits in F (for some prime p). If $\mathrm{Gal}(K/F)$ is cyclic of order p then $K = F(\alpha)$ for some α satisfying $\alpha^p \in F$.*

Thus the lemma shows that, under the given hypotheses, K is a simple radical extension of F.

Proof: By the Theorem of the Primitive Element (Theorem 4.11), $K = F(\beta)$ for some $\beta \in F$. We know that the roots of $X^p - 1$ in K are $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ and 1, for some $\varepsilon \in F$. Let ϕ be a generator for $G = \mathrm{Gal}(K/F)$. Set

$$\alpha = \beta + \varepsilon(\beta\phi) + \varepsilon^2(\beta\phi^2) + \dots + \varepsilon^{p-1}(\beta\phi^{p-1}).$$

Then, noting $\varepsilon\phi = \varepsilon$ since ϕ is an F-automorphism and $\varepsilon \in F$,

$$\begin{aligned}\alpha\phi &= \beta\phi + \varepsilon(\beta\phi^2) + \varepsilon^2(\beta\phi^3) + \cdots + \varepsilon^{p-1}\beta \\ &= \varepsilon^{-1}\alpha,\end{aligned}$$

so

$$(\alpha^p)\phi = (\alpha\phi)^p = (\varepsilon^{-1}\alpha)^p = \alpha^p.$$

Hence $\alpha^p \in \mathrm{Fix}_K(G) = F$ (by Lemma 6.8).

Since $\varepsilon \neq 1$, we have $\alpha\phi \neq \alpha$, so $\alpha \notin F$. Thus

$$F \subsetneqq F(\alpha) \subseteq K.$$

Now by part (i) of the Fundamental Theorem of Galois Theory (Theorem 6.7),

$$|K : F| = |G| = p$$

so, using the Tower Law, $F(\alpha) = K$, as required. □

Theorem 7.17 (Galois's Great Theorem) *Let $f(X)$ be a polynomial over a field F of characteristic zero. Then $f(X)$ is soluble by radicals if and only if the Galois group of $f(X)$ over F is soluble.*

Proof: One direction of this theorem is, of course, already established as Corollary 7.13. It remains to establish the converse.

Let K be the splitting field of $f(X)$ over F and assume that $G = \mathrm{Gal}(K/F)$ is a soluble group. We shall establish the existence of a radical extension of F that contains the splitting field K. We proceed by induction on the order of G. If $G = \mathbf{1}$, then $K = F$ (by part (i) of the Fundamental Theorem of Galois Theory (Theorem 6.7)) and certainly then K is a radical extension of F.

Assume then that G is non-trivial and let

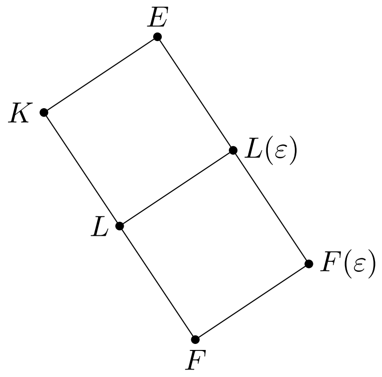
$$G = G_0 > G_1 > G_2 > \cdots > G_k = \mathbf{1}$$

be a chain of subgroups as provided by Proposition 7.8. Thus we are assuming, in particular, G_1 is a normal subgroup of G and G/G_1 is a cyclic group of order p for some prime p. Let

$$L = G_1^* = \mathrm{Fix}_K(G_1).$$

Now $G_1 = G_1^{**} = L^* = \mathrm{Gal}(K/L)$, by the Galois Correspondence (part (ii) of the Fundamental Theorem). Since G_1 is a proper subgroup of G, we may apply induction to conclude that there is a radical extension E of L containing K. By adjoining an element $\varepsilon \neq 1$ such that $\varepsilon^p = 1$ to E, if necessary, we may also assume that $X^p - 1$ splits in E.

The situation now is that we have various fields as shown in the following diagram:



We shall complete the proof by showing that E is a radical extension of F.

Now E is a radical extension of L, so it is certainly a radical extension of $L(\varepsilon)$ (by adjoining the same elements to $L(\varepsilon)$ as were adjoined to L to construct the intermediate fields). By construction, $F(\varepsilon)$ is a simple radical extension of F, so we need to show $L(\varepsilon)$ is a radical extension of $F(\varepsilon)$.

As G_1 is a normal subgroup of G, we know L is a normal extension of F (by part (iv) of the Fundamental Theorem of Galois Theory (Theorem 6.7)), so it is the splitting field for some polynomial $g(X)$ over F. Hence $L(\varepsilon)$ is the splitting field for $g(X)$ over $F(\varepsilon)$, so $L(\varepsilon)$ is a normal extension of $F(\varepsilon)$. Now

$$|L(\varepsilon) : F| = |L(\varepsilon) : F(\varepsilon)| \cdot |F(\varepsilon) : F| = |L(\varepsilon) : L| \cdot |L : F|,$$

by two applications of the Tower Law (Theorem 2.4), and so $p = |G|/|L^*| = |L : F|$ divides $|L(\varepsilon) : F(\varepsilon)| \cdot |F(\varepsilon) : F|$. Now, since $\varepsilon^p = 1$ and $\varepsilon \neq 1$, the minimum polynomial of ε over F divides

$$X^{p-1} + X^{p-2} + \cdots + X + 1,$$

so $|F(\varepsilon) : F| \leqslant p - 1$. We deduce that p divides $|L(\varepsilon) : F(\varepsilon)|$.

On the other hand, if $L = F(\alpha)$ by use of the Theorem of the Primitive Element (Theorem 4.11), then $L(\varepsilon) = F(\varepsilon, \alpha)$ and the minimum polynomial of α over $F(\varepsilon)$ divides that over F, so $|L(\varepsilon) : F(\varepsilon)| \leqslant |L : F| = p$.

Hence $|L(\varepsilon) : F(\varepsilon)| = p$ and we see that $\mathrm{Gal}(L(\varepsilon)/F(\varepsilon))$ is cyclic of order p (using part (i) of the Fundamental Theorem of Galois Theory). Now Lemma 7.16 shows $L(\varepsilon)$ is a simple radical extension of $F(\varepsilon)$, which completes the proof of the theorem. □