An Exploration of Galois Theory with some Classical Results

Olof Klingberg

May 2020

Abstract

Galois theory unites field theory and group theory to solve some field theoretical problems. The aim of this thesis is to provide a concise introduction to the topic, culminating in the proof of the insolubility of the general quintic equation by radicals. Using the developed field theory, a short discussion about geometric constructions is included, in which the impossibility of duplicating the cube, trisecting the angle and squaring the circle is shown.

Contents

1 Introduction

Can the general quintic equation be solved by radicals? This question has puzzled many great mathematicians ever since Girolamo Cardano published a paper containing algebraic solutions to both the cubic and quartic equation in 1545. After nearly 300 years, in 1824, this conundrum was finally solved by the Norwegian Niels Henrik Abel when he proved that such a solution does not exist. The question of whether or not some quintic equations could be solved by radicals then arose, and if so, what was so special about them. The task of answering this was undertaken by the turbulent young Frenchman Évariste Galois. Although it was not discovered until more than a decade after his tragic death following a duel, Galois had found an answer to this in 1832 by introducing the concept of a group and creating a new field of algebra, now called Galois theory in his honour.

Galois theory comprises the theory of field extensions and elementary group theory to define the *Galois Group* over a field extension $F:K$. This is the set of all K-automorphisms over F under composition of maps. It can be seen as a group where the elements are distinct permutations of the zeros of some polynomial over K, and is under certain conditions isomorphic to the symmetry group S_n for some integer n. Galois theory culminates in the exploration of the relationship between the solubility of a polynomial by radicals and the solubility of its associated Galois group.

The theory of field extensions needed for Galois theory also has some unexpected application; it can be used to discuss geometric constructions by manner of unmarked ruler and compass. This connection was famously employed to prove the impossibility of duplicating the cube, trisecting the angle, and squaring the circle, three problems which have puzzled mathematicians ever since Antiquity.

This thesis serves as an unofficial extract of the excellent second edition of Ian Stewart's *Galois Theory* [1]. Unless otherwise specified, all definitions, lemmas, theorems, corollaries, and proofs are from there, subject to reformulation and change of title, that is a lemma in Stewart [1] might in this text be referred as a theorem and so on. The structure also mainly follows that of Stewart [1], with the notable exception that ruler and compass constructions are here covered in the end, instead of straight after discussing field extensions. The information in the brief historical paragraph in the beginning of this section, as well as in the upcoming historical piece on Galois, are also taken from Stewart [1].

To limit the scope of this thesis, some knowledge must regrettably be assumed. This text is mainly aimed at those who have taken a first course in abstract algebra, and for the main results on the solubility of polynomials by radicals, familiarity with concepts such as isomorphisms, fields, soluble, simple, and symmetric groups, and results such as the isomorphism theorems are highly recommended. However, for those who do not possess such knowledge, there might still be some things of interest; the sections on field extensions and geometric constructions are more easily accessible. Before moving into the theory, we shall make a small detour, since any text discussing the work of Galois could be considered incomplete without at least a brief mention of the short, but in many ways extraordinary life he led.

1.1 The Life of Galois

Évariste Galois was born on 25th October 1811 in Bourg-la-Reine near Paris. He entered school at the age of twelve, before which he had been educated solely by his mother. Two years later, he came across Legendre's *Éléments de Géometrie* which he is famously said to have read 'like a novel' and mastered in one reading. His interest in mathematics thus thoroughly peaked, he went through the entrance examination for École Polytechnique, which he failed. Instead, he entered École Normale in 1828.

In the summer of 1830, there was an attempted coup d'état prompting the king to suppress the freedom of the press. An uprising ensued, consequently replacing the king. The students of Polytechnique took part in the protests while the students of École Normale were forbidden to take part and locked in. Galois was infuriated to the point where he wrote a letter attacking the director of the school resulting in his expulsion. In the beginning of 1831, Galois sent a memoir to the Academy of Sciences, receiving no reply. His mathematical career thus coming to a halt, he joined the artillery of the National Guard which soon after disbanded due to charges of conspiracy. At a banquet held in protest, Galois proposed a toast to the king with an open knife in his hand. Those attending interpreted this as a threat to the king's life and Galois was arrested. After being acquitted, Galois received news from the Academy, who rejected his memoir on account of it being incomprehensible. Ten days later, Galois was arrested once more, this time for wearing the uniform of the disbanded artillery and was imprisoned, giving him time to work on his mathematics.

Following his release, Galois experienced his first and only love affair. Although veiled in mystery, letters indicate that Galois was rejected. He took it badly and was soon after challenged to a duel with pistols. On the eve of the duel, 29th May, Galois wrote a letter roughly outlining his discoveries on the connection between groups and polynomial equations. The next day, Galois was shot in the stomach. On 31st May 1832, he died of peritonitis, not yet 21 years old.

Galois's mathematical discoveries lay unnoticed, seemingly lost to the world. It wasn't until 1843 when Joseph Liouville found Galois's work that its importance was recognised.

2 Field Extensions

In this section, we shall examine and discuss various properties of field extensions which we shall need later on, such as what different types of field extensions there are, what is meant by their degree and what it entails.

Definition. If K is a subfield of a field F, then F is a *field extension* of K. We denote this as $F : K$.

We shall regularly refer to a field extension by just calling it an extension.

Definition. Let $K^* : K$ and $F^* : F$ be field extensions. An *isomorphism* between the two is a pair of field isomorphisms (λ, μ), $\lambda : K \to F$ and $\mu : K^* \to F^*$ such that

$$\lambda(k) = \mu(k), \quad \forall k \in K.$$

Note that this is equivalent to saying that $\lambda = \mu|_K$, where $\mu|_K$ denotes the restriction of μ to K. If we identify K with $\lambda(K)$ and K^* with $\mu(K^*)$, then both λ and $\mu|_K$ becomes the identity map.

Now let $F : K$ be a field extension. If $\alpha \in F$ and $\alpha \notin K$, then let $K(\alpha)$ denote the intersection of all subfields of F containing both K and α. Clearly, $K(\alpha)$ is non-empty since it at least contains K. After some consideration, we also realise that $K(\alpha)$ is the smallest subfield of F containing both K and α.

Definition. By the above notation, $K(\alpha) : K$ is called a *simple extension.* Furthermore, we say that $K(\alpha)$ is obtained from K by *adjoining* α to K.

2.1 Transcendental Extensions

Definition. Let $F : K$ be a field extension and let $\alpha \in F$. If there is no non-zero polynomial p over K such that $p(\alpha) = 0$, then α is *transcendental* over K, and $K(\alpha) : K$ is a *simple transcendental extension.*

Theorem 2.1. *Let K be a field. Then the field of fractions $K(t)$ of the polynomial ring $K[t]$ is a simple transcendental extension.*

Proof. Clearly $K(t)$ is a simple extension. If $p(t) = 0$ for some polynomial p over K, then $p = 0$ by the definition of $K(t)$. Thus $K(t) : K$ is a simple transcendental extension. □

To be able to classify all simple transcendental extensions, up to isomorphism, we first need a lemma.

Lemma 2.2. *Let ϕ be a homomorphism from a field K to a ring R with $\phi \neq 0$. Then ϕ is a monomorphism.*

Proof. As is well known, the kernel of ϕ is an ideal in K. However, K is a field and so has no ideals other than 0 and itself. Since $\phi \neq 0$, the kernel of ϕ is not K, so it must be 0. Therefore, ϕ is a monomorphism. □

Theorem 2.3. *Let K be a field and let $K(t) : K$ be as described above. Then the simple transcendental extension $K(\alpha) : K$ is isomorphic to the extension $K(t) : K$. The isomorphism can be chosen to map t to α.*

Proof. Define the map $\phi : K(t) \to K(\alpha)$, where

$$\phi(f(t)/g(t)) = f(\alpha)/g(\alpha),$$

and f, g are polynomials over K. If $g \neq 0$, then $g(\alpha) \neq 0$ since α is transcendental, so that this map makes sense. We have that ϕ is a homomorphism, and since $\phi \neq 0$ it is a monomorphism by Lemma 2.2. All elements of $K(\alpha)$ can be written as $f(\alpha)/g(\alpha)$, so ϕ is also surjective, and hence it is an isomorphism. Moreover, $\phi|_K$ is the identity, and so we have an isomorphism of extensions. Finally, $\phi(t) = \alpha$. □

2.2 Algebraic Extensions

Definition. Let $F : K$ be a field extension and let $\alpha \in F$. If there is a non-zero polynomial p over K such that $p(\alpha) = 0$, then α is *algebraic* over K, and $K(\alpha) : K$ is a *simple algebraic extension.*

Definition. Let $F : K$ be a field extension. If every element in F is algebraic over K, then $F : K$ is an *algebraic extension*, and F is algebraic over K.

The construction of a simple algebraic extension is slightly more difficult compared to that of a simple transcendental extension and requires a couple of lemmas. The goal is to construct a simple algebraic extension from any field K given an irreducible polynomial over K. Let us start with a definition.

Definition. Let $F : K$ be a field extension. If an element $\alpha \in F$ is algebraic over K, then the non-zero monic polynomial m of lowest degree over K such that $m(\alpha) = 0$ is the *minimum polynomial* of α over K.

Lemma 2.4. *Let K be a field. The minimum polynomial m of an algebraic element α over K is irreducible over K. Furthermore, every polynomial p with $p(\alpha) = 0$ is divisible by m.*

Proof. We prove both statements by contradiction.

Suppose m is not irreducible over K. Then there are polynomials g and h over K such that $m = gh$, where the degree of g and h are less than that of m. Since m is the minimum polynomial of α over K, we have $0 = m(\alpha) = g(\alpha)h(\alpha)$. Hence $g(\alpha) = 0$ or $h(\alpha) = 0$, contradicting the definition of m. Therefore, m is irreducible over K.

Now suppose there is a non-zero polynomial p over K not divisible by m such that $p(\alpha) = 0$. By the division algorithm, there are polynomials q and r such that $p = qm + r$, where the degree of r is smaller than that of m, and $r \neq 0$. We then have

$$0 = p(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha).$$

As before, this is a contradiction to the minimality of m. Thus every polynomial p over K such that $p(\alpha) = 0$ is divisible by m. □

Lemma 2.5. *Let m be an irreducible non-constant polynomial over the field K and let I be the ideal of $K[t]$ comprising all multiples of m. Then the quotient ring $K[t]/I$ is a field.*

Proof. Let $I + f$ be a non-zero element of $K[t]/I = T$. Since m is irreducible, f and m are coprime. By a well-known result, there are then polynomials g and h over K such that

$$gf + hm = 1_K.$$

However, since $I + m = I$ is the zero element of R, we have

$$I + 1_K = (I + g)(I + f) + (I + h)(I + m) = (I + g)(I + f),$$

so $(I + g)$ is the inverse of $(I + f)$. Since f was chosen arbitrarily, every element of R has an inverse. Since T is commutative by definition of polynomial multiplication over a field, and since no element of T can be both a unit and a zero divisor, T is a field. □

The sought after construction is now within reach.

Theorem 2.6. *Let K be any field and m a monic irreducible polynomial over K. Then there exists an extension $K(\alpha) : K$ such that the minimum polynomial of α over K is m.*

Proof. As in the proof of Lemma 2.5, let I be the ideal of $K[t]$ comprising all multiples of m. By the same lemma, we know that $K[t]/I = T$ is a field. The goal here is now to set it up in such a way that $T = K(\alpha)$ where the minimum polynomial of α is m.

To this end, we shall define two functions. First, let $\lambda : K \to K[t]$ be the monomorphism that maps every element in K to itself in $K[t]$. Second, let $\mu : K[t] \to T$ be the homomorphism such that $\mu(f) = I + f$ for every $f \in K[t]$. The composite map $\phi = \mu\lambda$ is a homomorphism of fields, and $\phi \neq 0$, so by Lemma 2.2, ϕ is a monomorphism. Let $\alpha = I + t$. We then have $T = \phi(K)(\alpha)$. If we now identify K with its image $\phi(K)$, so that $\phi(\beta)$ is changed to β for every $\beta \in K$, and adjust the definition of addition and multiplication in T accordingly, we get that $K \subseteq T$ and thus $T = K(\alpha)$. It remains to show that m is the minimum polynomial of α over K.

The zero element of T is I and by definition, $m \in I$, so we have $m(\alpha) = I$. If the minimum polynomial of α over K is p, then $p|m$ by Lemma 2.4. However, since m is monic and irreducible, we must have $p = m$. Thus m is the minimum polynomial and the construction is complete. □

The classification of all simple algebraic extensions up to isomorphism is once again a bit more intricate compared to the transcendental case, and we require one more lemma.

Lemma 2.7. *Let $K(\alpha)$:K be a simple algebraic extension where α has minimum polynomial m over K. The every element of $K(\alpha)$ has a unique expression in the form of a polynomial $p(\alpha)$ over K where deg $p <$ deg m.*

Proof. The methodology here is to first prove the existence of such an expression and second, to prove uniqueness.

The set of all elements of the form $f(\alpha)/g(\alpha)$, where f and g are polynomials over K and $g(\alpha) \neq 0$, is a field under regular addition and multiplication of polynomials. It also contains K and α, and lies inside $K(\alpha)$. Therefore, all elements of $K(\alpha)$ can be written in this form. Since $g(\alpha) \neq 0$, m does not divide g. Further, since m is also irreducible, m and g are coprime. Hence there are polynomials p and q over K such that $pg + qm = 1$. This yields

$$1 = p(\alpha)g(\alpha) + q(\alpha)m(\alpha) = p(\alpha)g(\alpha) \Leftrightarrow g(\alpha) = \frac{1}{p(\alpha)},$$

so that

$$f(\alpha)/g(\alpha) = f(\alpha)p(\alpha) = h(\alpha),$$

for some polynomial h over K. Let r be the remainder upon dividing h by m. Then $r(\alpha) = h(\alpha)$ with deg $r <$ deg m. Hence we have proved existence.

Suppose there are two such expressions, with $a(\alpha) = b(\alpha)$ where a and b are polynomials over K. Let $c = a - b$. Then $c(\alpha) = 0$. But since both a and b have lower degree than m, we have deg $c <$ deg m. By the minimality of m, we must have $c = 0$ so that $a = b$, which proves uniqueness. □

Theorem 2.8. *Let $K(\alpha) : K$ and $K(\beta) : K$ be two algebraic extensions where α and β have the same minimum polynomial m over K. Then the two extensions are isomorphic and the isomorphism of the larger fields can be chosen to map α to β.*

Proof. This proof is fairly straight forward. We use Lemma 2.7 to define a map between $K(\alpha)$ and $K(\beta)$, and then we use properties of the minimum polynomial to show that this map is indeed an isomorphism.

By Lemma 2.7, all elements of $K(\alpha)$ can be uniquely expressed in the form

$$a = a_0 + a_1\alpha + \cdots + a_n\alpha^n \quad (a_0, \ldots, a_n \in K)$$

where $n = \deg m - 1$. We define the map $\phi : K(\alpha) \to K(\beta)$ by

$$\phi(a) = a_0 + a_1\beta + \cdots + a_n\beta^n.$$

Lemma 2.7 now yields that ϕ is both injective and surjective, so it remains to show that it is a homomorphism. Clearly, we have

$$\phi(a + b) = \phi(a) + \phi(b).$$

To show $\phi(ab) = \phi(a)\phi(b)$, for any $a, b \in K(\alpha)$, let $a = f(\alpha)$, $b = g(\alpha)$, and $ab = h(\alpha)$, where f, g, and h are polynomials over K with degree lower than m. We then need h to be the remainder upon dividing fg by m. We have

$$f(\alpha)g(\alpha) - h(\alpha) = ab - ab = 0.$$

By Lemma 2.4, m divides $fg - h$. Thus there is a polynomial q over K such that

$$fg - h = qm \Leftrightarrow fg = qm + h.$$

Since $\deg h < \deg m$ it follows by the division algorithm that h is the remainder upon dividing fg by m. It follows from this that $f(\beta)g(\beta) = h(\beta)$ since ϕ is a bijection. Thus we have

$$\phi(ab) = \phi(h(\alpha)) = h(\beta) = f(\beta)g(\beta) = \phi(f(\alpha))\phi(g(\alpha)) = \phi(a)\phi(b),$$

and ϕ is an isomorphism. Every element K is a constant polynomial and is therefore mapped to itself, so $\phi|_K$ is the identity and the extensions are isomorphic. Additionally, we have $\phi(\alpha) = \beta$. □

This is an important result for the rigour of later sections and we shall need to invoke this theorem many times. However, we shall also require a more general version of this theorem. We start with a somewhat niche definition.

Definition. Let $\phi : K \to L$ be a monomorphism of fields. We then define the function $\hat{\phi} : K[t] \to L[t]$ by

$$\hat{\phi}(k_0 + k_1t + \cdots + k_nt^n) = \phi(k_0) + \phi(k_1)t + \cdots + \phi(k_n)t^n$$

where $k_0, \ldots, k_n \in K$.

It is easily seen that $\hat{\phi}$ is a monomorphism, and if ϕ is an isomorphism, so is $\hat{\phi}$. The distinction between ϕ and $\hat{\phi}$ is not necessary, since $\phi(k) = \hat{\phi}(k)$ for any $k \in K$. We shall therefore use ϕ for both mappings in the future.

Theorem 2.9. *Let $\phi: K \to K'$ be an isomorphism of fields and let $K(\alpha)$ and $K'(\beta)$ be simple algebraic extensions of K and K' respectively, such that α has minimum polynomial m_α over K and β has minimum polynomial m_β over K'. Suppose that $m_\beta(t) = \phi(m_\alpha(t))$. Then there exists an isomorphism $\psi : K(\alpha) \to K'(\beta)$ such that $\psi|_K = \phi$ and $\psi(\alpha) = \beta$.*

Proof. This proof is basically the same as the proof of the last theorem with some minor adjustments.

All elements of $K(\alpha)$ are of the form $p(\alpha)$ where p is a polynomial over K of lower degree than that of m_α. We define the map $\psi: K(\alpha) \to K'(\beta)$ by $\psi(p(\alpha)) = (\phi(p))(\beta)$. Since ϕ is an isomorphism, ψ is surjective and injective by Lemma 2.7. Moreover, for any $a, b \in K(\alpha)$ we have

$$\begin{aligned}\psi(a+b) &= \psi(a_0 + b_0 + (a_1 + b_1)\alpha + \cdots + (a_n + b_n)\alpha^n)\\ &= \phi(a_0) + \phi(a_1)\beta + \cdots + \phi(a_n)\beta^n + \phi(b_0) + \phi(b_1)\beta + \phi(b_n)\beta^n\\ &= (\phi(a))(\beta) + (\phi(b))(\beta) = \psi(a) + \psi(b).\end{aligned}$$

Now, let $a = f(\alpha)$, $b = g(\alpha)$ and $ab = h(\alpha)$, where f, g, and h are polynomials over K with degree lower than m_α. As before, we have

$$f(\alpha)g(\alpha) - h(\alpha) = 0,$$

and therefore m_α divides $fg - h$, so that h is the remainder upon dividing fg by m_α. By the same reasoning, $\phi(h)$ is the remainder upon dividing $\phi(fg)$ by $\phi(m_\alpha)$. Since $\phi(m_\alpha(t)) = m_\beta(t)$, and ϕ is an isomorphism, we have that

$$\begin{aligned}\psi(ab) &= \psi(h(\alpha)) = (\phi(h))(\beta) = (\phi(fg))(\beta)\\ &= (\phi(f))(\beta)(\phi(g))(\beta) = \psi(a)\psi(b).\end{aligned}$$

Hence ψ is an isomorphism. Since all elements in K are constants, $\psi|_K = \phi$. Finally, consider the polynomial $p(t) = t = 1_K t$ over K. We have

$$\psi(\alpha) = \psi(p(\alpha)) = (\phi(p))(\beta) = (\phi(1_K))(\beta) = p(\beta) = \beta,$$

which concludes the proof. □

2.3 The Degree of an Extension

The degree of an extension is a crucial concept when working with extensions, not least when it comes to geometric construction by means of unmarked ruler and compass, which are discussed in section 5. After this subsection, one has all the necessary tools for section 5 and may, therefore, without complication, skip ahead.

To be able to define the degree of an extension, we first need to make an observation which has been staring us in the face for some time.

Theorem 2.10. *Let $F : K$ be a field extension. Then F is a vector space over K under ordinary addition in F for vectors and ordinary multiplication in F for scalar multiplication.*

Proof. Since both F and K are fields, all the axioms for a vector space are satisfied. □

Definition. Let $F : K$ be a field extension. The *degree* of $F : K$ is the dimension of the vector space F over K. We denote the degree as $[F : K]$.

Definition. A field extension is *finite* if its degree is finite.

We next present a useful tool when determining the degree of an extension, often referred to as the *tower law.*

Theorem 2.11 (The Tower Law)**.** *Let F, M, K be fields such that K is a subfield of M and M is a subfield of F. Then*

$$[F : K] = [F : M][M : K].$$

Proof. Let $(x_i)_{i=1}^m$ be a basis for M over K and let $(y_j)_{j=1}^n$ be a basis for F over M for some integers m and n. Our goal is now to show that x_iy_j is a basis for F over K for $1 \leq i \leq m$ and $1 \leq j \leq n$.

We first show linear independence. Suppose that some linear combination of these elements is zero, that is

$$\sum_{i=1,j=1}^{m,n} k_{ij}x_iy_j = \sum_{j=1}^{n}\Big(\sum_{i=1}^{m} k_{ij}x_i\Big)y_j = 0 \quad (k_{ij} \in K).$$

The coefficients $\sum_{i=1}^m k_{ij}x_i$ lie in M and the y_j are linearly independent over M since they form a basis, so we must have

$$\sum_{i=1}^{m} k_{ij}x_i = 0.$$

However, since the x_i form a basis over K, they are linearly independent over K so we must have $k_{ij} = 0$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Hence the elements x_iy_j are linearly independent for those i and j.

Second, we show that the x_iy_j span F over K. We know that any element $a \in F$ can be written as

$$a = \sum_{j=1}^{n} \lambda_j y_j$$

for some $\lambda_j \in M$ since the y_j span F over M. Similarly, $\lambda_j \in M$ can be written as

$$\lambda_j = \sum_{i=1}^{m} \lambda_{ij}x_i$$

for some $\lambda_{ij} \in K$ since the x_i span M over K. Thus, for any element $a \in F$ we have

$$a = \sum_{i=1,j=1}^{m,n} \lambda_{ij}x_iy_j$$

which shows that the x_iy_j span F over K.

Finally, we need to address what happens if any of the degrees involved are infinite. The interpretation is then the straight forward one. If either $[F : M]$ or $[M : K]$ are infinite, then so is $[F : K]$. Conversely, if $[F : K]$ is infinite, then either $[F : M]$ or $[M : K]$ must also be infinite. □

The tower law is not of much use, however, if we do not know how to get started in calculating the degree of a field extension. In light of this, we present the following convenient fact.

Theorem 2.12. *Let $K(\alpha) : K$ be a simple field extension. If it is transcendental, then $[K(\alpha) : K]$ is infinite. If it is algebraic, then $[K(\alpha) : K] = deg\, m$, where m is the minimum polynomial of α over K.*

Proof. For the transcendental case, we need only note that $1, \alpha, \alpha^2, \ldots$ are linearly independent over K. Hence $[K(\alpha) : K]$ is infinite.

For the algebraic case, we need to determine a basis for $K(\alpha)$ over K. Let deg $m = n$ and consider the set $S = \{1, \alpha, \ldots, \alpha^{n-1}\}$. By Lemma 2.7, any element of $K(\alpha)$ can be written as a polynomial of α of degree lower than n, so the elements of S span $K(\alpha)$ over K. Furthermore, by the uniqueness part of Lemma 2.7, the elements of S are also linearly independent and thus they form a basis. We now have

$$[K(\alpha) : K] = \deg m$$

as required. □

After some consideration, we realise that this result implies that any simple algebraic extension is indeed finite. However, the converse does not hold. Furthermore, algebraic extensions need not be finite, but every finite extension is indeed algebraic.

Theorem 2.13. *Let $F : K$ be field extension. Then $F : K$ is finite if and only if F is algebraic over K and there exists finitely many elements $\alpha_1, \ldots, \alpha_n \in F$ such that $F = K(\alpha_1, \ldots, \alpha_n)$.*

Proof. First, suppose that $F : K$ is a finite extension. Then there is a basis $\{\alpha_1, \ldots, \alpha_n\}$ for F over K, so that every element of F can be obtained as a linear combination of $\alpha_1, \ldots, \alpha_n$, and thus $F = K(\alpha_1, \ldots, \alpha_n)$. It remains to show that $F : K$ is algebraic. To this end, let x be any element of F and note that $[F : K] = n$. The set $\{1, x, \ldots, x^n\}$ contains $n + 1$ elements, so they must be linearly dependent over K. Hence

$$k_0 + k_1 x_1 + \cdots + k_n x^n = 0$$

for some $k_0, \ldots, k_n \in K$, not all zero. Any element x of F is therefore algebraic over K, and thus F is algebraic over K.

Second, suppose instead that $F : K$ is algebraic where $F = K(\alpha_1, \ldots, \alpha_n)$. Here, we use induction on n to show that $F : K$ is finite. If $n = 1$, $F : K$ is a simple algebraic extension, so by Theorem 2.12, $F : K$ is finite. If the statement holds for all $n = k$, then for $n = k + 1$ the tower law yields

$$[F : K] = [K(\alpha_1, \ldots, \alpha_{k+1}) : K(\alpha_1, \ldots, \alpha_k)][K(\alpha_1, \ldots, \alpha_k) : K].$$

Since $F : K$ is an algebraic extension, $[K(\alpha_1, \ldots, \alpha_{k+1}) : K(\alpha_1, \ldots, \alpha_k)]$ is a simple algebraic extension, and again by Theorem 2.12, must be finite. By proceeding in the same manner, the induction step goes through and we have that $[F : K]$ is finite. This concludes the proof. □

2.4 Normal and Separable Extensions

The notions of normality and separability in field extensions are an essential part of Galois theory. Before we can define them, however, we first need to establish the concept of *splitting fields.*

2.4.1 Splitting Fields

Definition. Let K be a field and f a polynomial over K. Then f *splits* over K if it can written as a product of linear factors

$$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n), \quad (k, \alpha_1, \ldots, \alpha_n \in K).$$

If f fulfils this condition, then $\alpha_1, \dots, \alpha_n$ are the zeros of f in K. If F is an extension of K, then f is also a polynomial over F, and it is therefore relevant to examine the case where f splits over F. This motivates the following definition.

Definition. Let K be field and f a polynomial over K. Then an extension Σ of K is a *splitting field* for f over K if

(i) f splits over Σ;

(ii) $\Sigma = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the zeros of f in Σ.

Condition (ii) is equivalent to saying that Σ is the smallest field over which f splits.

We now need to prove the existence of such a field Σ. As stated in (ii) above, such a field Σ is obtained by adjoining zeros of f to K. Recall that we did this for an irreducible polynomial in Theorem 2.6, so we simply split f into irreducible factors and treat them separately.

Theorem 2.14. *Let K be any field and let f be any polynomial over K. Then there exists a splitting field for f over K.*

Proof. We use induction on deg $f = n$. If $n = 1$, then f splits over K and there is nothing to prove. Assume then that there exists a splitting field for f over K for all $n = k$ and let $n = k + 1$. If f splits over K we are done. Suppose therefore that f does not split over K. Then f has an irreducible factor f_1 such that deg $f_1 > 1$. We use Theorem 2.6 to adjoin α_1 to K where α_1 is a zero of f_1. Over $K(\alpha_1)$, we then have $f(t) = (t - \alpha_1)g$, where deg $g = k + 1 - 1 = k$. By the induction hypothesis, there exists a splitting field Σ for g over $K(\alpha_1)$. But Σ is also a splitting field for f over K. Thus the induction step goes through and we are done. □

It remains to determine if there is a unique splitting field for any given f and K. Up to isomorphism, that is indeed the case. However, for the proof of this we first need a lemma which we prove by induction and the use of Theorem 2.9.

Lemma 2.15. *Let $\phi : K \to K'$ be an isomorphism of fields, f a polynomial over K, and Σ any splitting field for f over K. If F is an extension of K' such that $\phi(f)$ splits over F, then there exists a monomorphism $\psi : \Sigma \to F$ such that $\psi|_K = \phi$.*

Proof. We use induction on deg $f = n$. If $n = 1$, then f splits over K, and $\phi(f)$ splits over K' by the definition of ϕ. Then ϕ itself fulfils the requirements of the theorem.

Assume that the statement holds for all $n = k$ and let $n = k + 1$. Over Σ, we then have

$$f(t) = k(t - \alpha_1) \cdots (t - \alpha_{k+1}).$$

Now the minimum polynomial m of α_1 over K is an irreducible factor of f. Since ϕ is an isomorphism, $\phi(m)$ divides $\phi(f)$ which splits over F. Over F we therefore have

$$\phi(m(t)) = k(t - \beta_1) \cdots (t - \beta_r)$$

where $\beta_1, \dots, \beta_r \in F$. Over K', $\phi(m)$ is irreducible and must therefore be the minimum polynomial of β_1 over K'. By Theorem 2.9, there is an isomorphism $\psi_1 : K(\alpha_1) \to K'(\beta_1)$, such that $\psi_1|_K = \phi$ and $\psi_1(\alpha_1) = \beta_1$. We now have that Σ is a splitting field for the polynomial $g(t) = f(t)/(t - \alpha_1)$ over $K(\alpha_1)$. Since deg $g = k$, the induction hypothesis yields that there exists a monomorphism $\psi : \Sigma \to F$ such that $\psi|_{K(\alpha_1)} = \psi_1$. But then $\psi|_K = \psi_1|_K = \phi$. This concludes the proof. □

Theorem 2.16. *Let $\phi : K \to K'$ be an isomorphism of fields. Let Σ be splitting field for f over K, Σ' a splitting field for $\phi(f)$ over K'. Then there is an isomorphism $\psi : \Sigma \to \Sigma'$ such that $\psi|_K = \phi$. In other words, the extensions $\Sigma : K$ and $\Sigma' : K'$ are isomorphic.*

Proof. By Lemma 2.15, there is a monomorphism $\psi : \Sigma \to \Sigma'$ such that $\psi|_K = \phi$. Because of this and the fact that ϕ is an isomorphism, we have that $\psi(\Sigma)$ is a splitting field for $\phi(f)$ over K'. But $\psi(\Sigma)$ is contained in Σ' since ψ is a monomorphism, and Σ' is also a splitting field for $\phi(f)$ over K', so we must have $\psi(\Sigma) = \Sigma'$. Hence ψ is surjective and an isomorphism. □

2.4.2 Normal Extensions

Definition. Let $F : K$ be a field extension. If every irreducible polynomial over K with at least one zero in F splits over F, then $F : K$ is *normal.*

Theorem 2.17. *A field extension $F : K$ is normal and finite if and only if F is a splitting field for some polynomial over K.*

Proof. Since we are dealing with an *if and only if* statement, the proof comprises two parts.

First, suppose that $F : K$ is normal and finite. By Theorem 2.13, $F = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n$ algebraic over K. Let m_i be the minimum polynomial of α_i over K and let $f = m_1 \cdots m_n$. Every m_i is irreducible over K and has a zero α_i in F, so by normality, each m_i splits over F. Hence f splits over F. Since F is generated by K and the zeros of f, F is a splitting field for f over K.

Second, suppose that F is a splitting field for some polynomial f over K. Since F is then generated by K and the zeros of f, $F : K$ is finite. It remains to show that it is also normal. The goal is to show that an irreducible polynomial g over K with a zero in F splits over F. Let Σ be a splitting field for fg over F, and thus also a splitting field for g over F. Let β_1 and β_2 be zeros of g in Σ. We now claim that

$$[F(\beta_1) : F] = [F(\beta_2) : F].$$

Here, we make use of a certain trick. Since for $i = 1$ and 2, $F \subseteq F(\beta_i)$, and $K \subseteq K(\beta_i)$, we have by the tower law

$$[F(\beta_i) : F][F : K] = [F(\beta_i) : K] = [F(\beta_i) : K(\beta_i)][K(\beta_i) : K]. \tag{2.1}$$

Since β_1 and β_2 have the same minimum polynomial g over K, we have by Theorem 2.12 that $[K(\beta_1){:}K] = [K(\beta_2){:}K]$, and by Theorem 2.8, $K(\beta_1)$ and $K(\beta_2)$ are isomorphic. Furthermore, $F(\beta_i)$ is a splitting field for f over $K(\beta_i)$. Hence, the extensions $F(\beta_i) : K(\beta_i)$ are isomorphic by Theorem 2.16, and thus they have the same degree. Substituting this in equation (2.1) yields

$$\begin{aligned} [F(\beta_1) : F][F : K] &= [F(\beta_1) : K(\beta_1)][K(\beta_1) : K] \\ &= [F(\beta_2) : K(\beta_2)][K(\beta_2) : K] = [F(\beta_2) : F][F : K]. \end{aligned}$$

After cancellation, we obtain

$$[F(\beta_1) : F] = [F(\beta_2) : F]$$

as claimed.

If $\beta_1 \in F$, we have that $[F(\beta_1) : F] = 1 = [F(\beta_2) : F]$, and so $\beta_2 \in F$. Hence $F : K$ is normal. □

2.4.3 Separable Extensions

Definition. Let f be an irreducible polynomial over K. Then f is *separable* over K if it has no multiple zeros in a splitting field. If f is not separable over K, it is *inseparable* over K.

We can extend the notion of separability to arbitrary polynomials, algebraic elements and entire extensions.

Definition. Any polynomial over a field K is *separable* over K if all its irreducible factors are separable over K.

Let $F : K$ be a field extension. An algebraic element $\alpha \in F$ is *separable* over K if its minimum polynomial over K is separable over K.

An algebraic extension $F : K$ is a *separable extension* if every $\alpha \in F$ is separable over K.

If $F : M$ and $M : K$ are field extensions such that $K \subseteq M \subseteq F$, we say that M is an *intermediate field* of $F : K$. Often we omit specifying what extension M is an intermediate field of since it is usually clear from the context. Next, we show that separability in algebraic extensions carries over to intermediate fields.

Theorem 2.18. *Let $F : K$ be a separable algebraic extension and let M be an intermediate field. Then $F : M$ and $M : K$ are separable.*

Proof. Since every algebraic element $\alpha \in F$ is separable over K, we must have that all algebraic elements in M are separable over K, and thus $M : K$ is separable.

Let $\alpha \in F$ and let m_K and m_M be the minimum polynomials of α over K and over M respectively. By Theorem 2.4, we have that $m_M | m_K$ over M. But α is separable over K so m_K is separable over K, hence m_M is separable over M. Therefore, $F : M$ is a separable extension and we are done. □

While on the topic of multiple zeros of polynomials, we shall now investigate how we can detect such using differentiation. For polynomials over $\mathbb{R}$ this detection method is standard. For polynomials over arbitrary fields, we first need to formally define what differentiation is.

Definition. Let K be a field and

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n$$

a polynomial over K. Then the *formal derivative* of f is the polynomial

$$Df = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}.$$

Just as in the case of the standard derivative in $\mathbb{R}$, we have some properties of D. Simple computation show that for any polynomials f and g over K

$$D(f + g) = Df + Dg, \quad D(fg) = Df \cdot g + f \cdot Dg$$

and if $k \in K$, then

$$D(k) = 0, \quad D(kf) = k \cdot Df.$$

These allow us to give a useful criterion for the existence of multiple zeros without knowing what they are.

Theorem 2.19. *Let $f \neq 0$ be a polynomial over a field K. Then f has multiple zeros in a splitting field if and only if f and Df have a common factor of degree ≥ 1 over K.*

Proof. First, suppose that f has a repeated zero in a splitting field Σ, so that over Σ

$$f(t) = (t - \alpha)^2 g(t)$$

for some g over Σ and some $\alpha \in \Sigma$. Then

$$Df = 2(t - \alpha)g + (t - \alpha)^2 Dg = (t - \alpha)(2g + (t - \alpha)Dg)$$

so that f and Df have a common factor $(t - \alpha)$ over Σ. We have that $f(\alpha) = 0$ and $(Df)(\alpha) = 0$ so when considered as polynomials over K, they must both be divisible by the minimum polynomial of α over K by Theorem 2.4. Thus f and Df have a common factor of degree ≥ 1.

Second, suppose that f has no multiple zeros. We shall use induction on $\deg f = n$ to show that f and Df are coprime over Σ, hence also coprime over K. If $n = 1$, then Df is a constant and so coprime to the polynomial f. If $n = k + 1$, then $f(t) = (t - \alpha)g(t)$ where $\deg g = k$ and $(t - \alpha) \nmid g(t)$. Then

$$Df = g + (t - \alpha)Dg.$$

Since $(t - \alpha) \nmid g(t)$, we must have that a factor of g divides Dg if f and Df are not to be coprime. But by induction, g and Dg are coprime, and hence, so are f and Df. This completes the proof. □

3 Galois Theory

In this section, we shall begin by introducing some of the basic concepts in Galois theory, such as *Galois extensions* and *Galois groups*. We shall then need to do some interim study on field degrees, group orders, and monomorphisms to then be able to present the fundamental theorem of Galois theory which concerns what is known as the *Galois correspondence*. Finally, we shall conclude the section by reviewing some results from group theory, which will be needed for the upcoming section.

3.1 Underlying Definitions

We already have all that is required to define the Galois extension.

Definition. If $F : K$ is a finite separable normal field extension, then $F : K$ is a *Galois extension*.

For the definition of the Galois group, a preceding definition and a lemma are necessary.

Definition. Let K be a subfield of the field F. An automorphism ϕ of F is a *K-automorphism* of F if

$$\phi(k) = k, \quad \forall k \in K.$$

Note that an *automorphism* is an isomorphism between a mathematical object and itself. In the above case, ϕ can be seen as an automorphism of the extension $F : K$, rather than just of the large field.

Lemma 3.1. *Let $F : K$ be a field extension. The set of all K-automorphisms of F form a group under composition of maps.*

Proof. Composition of maps is associative, so it remains to prove closure under operation, existence of identity, and existence of inverse. Let ϕ and ψ be K-automorphisms of F. Clearly, $\phi\psi$ is then an automorphism. Furthermore, $\phi(\psi(k)) = \phi(k) = k$, for all $k \in K$, so $\phi\psi$ is a K-automorphism and we have closure under operation. The identity map on F is a K-automorphism. Finally, ϕ^{-1} is an automorphism of F, and for all $k \in K$ we have $k = \phi^{-1}(\phi(k)) = \phi^{-1}(k)$, so ϕ^{-1} is a K-automorphism. Thus, the set of all K-automorphisms of F form a group under composition of maps. □

Definition. Let $F : K$ be a field extension. The *Galois group* of $F : K$, denoted $\Gamma(F : K)$, is the group of all K-automorphisms of F under composition of maps.

To prepare for what is known as the *Galois correspondence*, we need to examine the relationship between intermediate fields and subgroups of the associated Galois group. We shall return to this correspondence later on.

Definition. Let $F : K$ be a field extension and let M be an intermediate field. Then $M^* = \Gamma(F : M)$ is the group of all M-automorphisms of F.

We have that K^* is the whole Galois group, and that F^* comprises one element, namely the identity map on F. Furthermore if N is another intermediate field and $M \subseteq N$, we have that $M^* \supseteq N^*$, since all automorphisms fixing all elements of N certainly also fix all elements of M.

Conversely, we also associate a set to a subgroup of $\Gamma(F : K)$.

Definition. Let $F : K$ be a field extension and H a subgroup of $\Gamma(F : K)$. We then let $H^\dagger = \{x \in F \,|\, \phi(x) = x \;\forall \phi \in H\}$.

For us to have a correspondence between the maps * and †, we need $H^\dagger$ to be an intermediate field. This is indeed the case, which we show in the following lemma.

Lemma 3.2. *$F : K$ be a field extension and H a subgroup of $\Gamma(F : K)$. Then $H^\dagger$ is a subfield of F containing K.*

Proof. Let $x, y \in H^\dagger$ and $\phi \in H$. Since ϕ is an automorphism, we have

$$\phi(x + y) = \phi(x) + \phi(y) = x + y.$$

Similarly, $H^\dagger$ is closed under multiplication. Since ϕ fixes all elements $x, y \in H^\dagger$, and all x, y are in the field F, the other axioms for a field are also fulfilled so that $H^\dagger$ is a subfield of F. Since $\phi \in \Gamma(F : K)$, we have $\phi(k) = k$ for all $k \in K$, and hence $H^\dagger$ contains K. □

Definition. With notation as above, $H^\dagger$ is the *fixed field* of H.

In this case, we note that $K \subseteq \Gamma(F : K)^\dagger$. Once again, we have reverse inclusions. If H and G are subgroups of $\Gamma(F : K)$ and $H \subseteq G$, then $H^\dagger \supseteq G^\dagger$, since all elements in $G^\dagger$ are fixed by all automorphisms in G, and thus certainly also by all automorphisms in H. Furthermore, if M is an intermediate field we have

$$\begin{aligned} M &\subseteq M^{*\dagger} \\ H &\subseteq H^{\dagger *}, \end{aligned} \tag{3.1}$$

since every element of M is fixed by the automorphisms that fixes all of M, and every automorphism of H fix all elements that are fixed by all of H.

To give a taste of what is to come, let $\mathscr{F}$ be the set of all intermediate fields of $F : K$ and $\mathscr{G}$ be the set of all subgroups of $\Gamma(F : K)$. We then have the two maps

$$\begin{aligned} ^* &: \mathscr{F} \to \mathscr{G} \\ ^\dagger &: \mathscr{G} \to \mathscr{F} \end{aligned}$$

satisfying (3.1). When both of these are bijections we refer to this as the aforementioned *Galois correspondence.* We shall later see that this is, in fact, the case when we are dealing with a Galois extension, but we are not ready to prove it yet.

3.2 Fixed Fields and Subgroups

The goal in this subsection is to show that if H is a subgroup of $\Gamma(F : K)$, where $F : K$ is a Galois extension, then $H^{\dagger *} = H$. Our method will be to show that H and $H^{\dagger *}$ are finite groups of the same order and, since we know that $H \subseteq H^{\dagger *}$, conclude that $H^{\dagger *} = H$.

3.2.1 Degrees and Group Orders

Keeping our goal described above in mind, we shall first determine $[H^\dagger : K]$ in terms of the order of H. We need this to later compute the order of $H^{\dagger *}$. For this, we require a couple of lemmas. We begin with one attributed to Dedekind.

Lemma 3.3 (Dedekind)**.** *Let K and F be fields. Then every set of distinct monomorphisms $K \to F$ is linearly independent over F.*

Proof. We aim to prove this by contradiction. Suppose therefore that a set of distinct monomorphisms $\lambda_1, \ldots, \lambda_n$ from K to F are linearly dependent. That means that there are elements $a_1, \ldots, a_n \in F$, not all zero, such that

$$a_1\lambda_1(x) + \cdots + a_n\lambda_n(x) = 0 \tag{3.2}$$

for all $x \in K$. Of all equations of the form (3.2) that hold, with all $a_i \neq 0$, there must be at least one where the number n of terms is least. We choose notation so that equation (3.2) is such an equation.

There exists $y \in K$ such that $\lambda_1(y) \neq \lambda_n(y)$ since $\lambda_1 \neq \lambda_n$, and so $y \neq 0$. Equation (3.2) holds for all $x \in K$, so we can replace x with yx. This yields, for all $x \in K$,

$$a_1\lambda_1(yx) + \cdots + a_n\lambda_n(yx) = a_1\lambda_1(y)\lambda_1(x) + \cdots + a_n\lambda_1(y)\lambda_n(x) = 0. \tag{3.3}$$

The first equality follows from the fact that all λ_i are monomorphisms. If we now multiply equation (3.2) by $\lambda_1(y)$ and then subtract equation (3.3), we obtain

$$a_2(\lambda_1(y) - \lambda_2(y))\lambda_2(x) + \cdots + a_n(\lambda_1(y) - \lambda_n(y))\lambda_n(x) = 0.$$

The coefficient of $\lambda_n(x)$ is $a_n(\lambda_1(y) - \lambda_n(y)) \neq 0$, so we have an equation of the form (3.2) with at most $n-1$ terms. This is a contradiction to the minimality of n, and thus no equation of the form (3.2) with non-zero coefficients exists. This concludes the proof. □

The second lemma is a useful principle from group theory.

Lemma 3.4. *Let G be a group whose distinct elements are $g_1, \ldots, g_n$, and let $g \in G$. Then, as i varies from 1 to n, the elements gg_i run through the whole of G, each element of G occurring precisely once.*

Proof. If $h \in G$, then $g^{-1}h = g_i$ for some i, so that $h = gg_i$. If $gg_j = gg_i$, we then have $g_j = g^{-1}gg_j = g^{-1}gg_i = g_i$. Hence the mapping $g_j \to gg_j$ is a bijection $G \to G$, from which the result follows. □

A corollary to the next theorem will end our current endeavour.

Theorem 3.5. *Let G be a finite subgroup of the group of automorphisms of a field K and let K_0 be the fixed field of G. Then*

$$[K : K_0] = |G|.$$

Proof. Let $g_1, \ldots, g_n$ be the elements of G where g_1 is the identity. Then $|G| = n$. The methodology of this proof will be to first show that $[K : K_0] \geq n$, and then to show that $[K : K_0] \leq n$ which will allow us to conclude that $[K : K_0] = n$. We prove both of these statements by contradiction.

To this end, suppose that $[K : K_0] = m < n$. Let $\{a_1, \ldots, a_m\}$ be a basis for K over K_0. Consider the system of m homogeneous linear equations

$$g_1(a_i)x_1 + \cdots + g_n(a_i)x_n = 0, \quad i = 1, \ldots, m,$$

in the n unknowns $x_1, \ldots, x_n$. Since $n > m$, this is an underdetermined system of homogeneous equations so that there is a non-trivial solution. Hence, there are elements $y_1, \ldots, y_n \in K$, not all zero, such that

$$g_1(a_i)y_1 + \cdots + g_n(a_i)y_n = 0 \tag{3.4}$$

for $i = 1, \ldots, m$. For any element $k \in K$ we have

$$k = \alpha_1 a_1 + \cdots + \alpha_m a_m, \quad \alpha_1, \ldots, \alpha_m \in K_0.$$

Using (3.4), picking any i, we have

$$\begin{aligned} g_1(k)y_1 + \cdots + g_n(k)y_n &= g_1\left(\sum_{j=1}^{m} \alpha_j a_j\right)y_1 + \ldots + g_n\left(\sum_{j=1}^{m} \alpha_j a_j\right)y_n \\ &= \sum_{j=1}^{m} \alpha_j g_1(a_j)y_1 + \cdots + \sum_{j=1}^{m} \alpha_j g_n(a_j)y_n \\ &= \sum_{j=1}^{m} \alpha_j (g_1(a_j)y_1 + \cdots + g_n(a_j)y_n) \\ &= 0. \end{aligned}$$

Hence the distinct automorphisms $g_1, \ldots, g_n$ are linearly dependent. This is a contradiction to Lemma 3.3. Therefore $m \geq n$.

Now suppose $[K : K_0] > n$. Then there exists a set of $n + 1$ elements of K linearly independent over K_0. Let $\{a_1, \ldots, a_{n+1}\}$ be such a set. Consider the system of n homogeneous linear equations

$$g_i(a_1)x_1 + \cdots + g_i(a_{n+1})x_{n+1} = 0, \quad i = 1, \ldots, n,$$

in the $n + 1$ unknowns $x_1, \ldots, x_{n+1}$. As before, this is an underdetermined system, so there exist $y_1, \ldots, y_{n+1}$, not all zero, such that

$$g_i(a_1)y_1 + \cdots + g_i(a_{n+1})y_{n+1} = 0 \tag{3.5}$$

for $i = 1, \ldots, n$. As in the proof of Lemma 3.3, we choose $y_1, \ldots, y_{n+1}$ so that as many terms as possible are zero, and renumber so that

$$y_1, \ldots, y_r \neq 0, \quad y_{r+1}, \ldots, y_{n+1} = 0.$$

The system of equations (3.5) now becomes

$$g_i(a_1)y_1 + \cdots + g_i(a_r)y_r = 0 \tag{3.6}$$

for $i = 1, \ldots, n$. Let $g \in G$, and operate by g on (3.6). This yields

$$gg_i(a_1)g(y_1) + \cdots + gg_i(a_r)g(y_r) = 0, \quad i = 1, \ldots, n,$$

which by Lemma 3.4 as i varies, is equivalent to

$$g_i(a_1)g(y_1) + \cdots + g_i(a_r)g(y_r) = 0 \tag{3.7}$$

for $i = 1, \ldots, n$. If we now multiply the equations (3.6) by $g(y_1)$ and equations (3.7) by y_1, and then subtract, we obtain

$$g_i(a_2)(g(y_1)y_2 - y_1 g(y_2)) + \cdots + g_i(a_r)(g(y_1)y_r - y_1 g(y_r)) = 0.$$

This is a system of equations like (3.6) but with fewer terms, so we have a contradiction unless all the coefficients

$$g(y_1)y_j - y_1 g(y_j), \quad j = 1, \ldots, r,$$

are zero. If this is the case, then

$$g(y_1)y_j - y_1g(y_j) = 0 \quad \Leftrightarrow \quad g(y_1)y_j = y_1g(y_j) \quad \Leftrightarrow \quad y_1^{-1}y_j = g(y_1^{-1}y_j),$$

for all $g \in G$, so that $y_1^{-1}y_j \in K_0$. Hence there exist $z_1, \dots, z_r \in K_0$ such that $y_j = y_1z_j$ for $j = 1, \dots, r$. With $i = 1$, equation (3.6) then becomes

$$a_1y_1z_1 + \cdots + a_ry_1z_r = 0,$$

since g_1 is the identity. Because $y_1 \neq 0$, we can divide by y_1 to obtain

$$a_1z_1 + \cdots + a_rz_r = 0.$$

This shows that the a_i are linearly dependent over K_0, which is a contradiction to our original assumption. Hence $[K : K_0] \leq n$.

Combining the first and second part, we can conclude that $[K : K_0] = n$, and the proof is complete. □

Corollary 3.6. *Let $G = \Gamma(F : K)$ where $F : K$ is a finite extension and let H be a finite subgroup of G. Then*

$$[H^\dagger : K] = [F : K]/|H|.$$

Proof. Since $H^\dagger$ is an intermediate field, we have $[F : K] = [F : H^\dagger][H^\dagger : K]$ by the tower law. By Theorem 3.5, we have $[F : H^\dagger] = |H|$. Combining these two yields $[H^\dagger : K] = [F : K]/|H|$ as required. □

We now need to do some work on auto- and monomorphisms. To be able to treat these more generally, we shall also introduce the notion of a *normal closure.*

3.2.2 Automorphisms and Monomorphisms

We begin with a generalisation of the K-automorphism, the K-monomorphism.

Definition. Let K be a subfield of the fields M and F. Then a *K-monomorphism* of M into F is a map $\phi : M \to F$ which is a monomorphism between fields such that $\phi(k) = k$ for all $k \in K$.

Evidently, if $K \subseteq M \subseteq F$, then any K-automorphism of F restricted to M is a K-monomorphism $M \to F$. We are interested in reversing the process.

Theorem 3.7. *Let $F : K$ be a finite and normal field extension and let M be a field such that $K \subseteq M \subseteq F$. Further, let ψ be any K-monomorphism $M \to F$. Then there exists a K-automorphism ϕ of F such that $\phi|_M = \psi$.*

Proof. Since $F : K$ is finite, F is a splitting field for a polynomial f over K by Theorem 2.17. Hence, it is simultaneously a splitting field for f over M and for f over $\psi(M)$. The latter is true since $\psi(M) \subseteq F$, and since $\psi(f) = f$. We have that ψ is an isomorphism between M and $\psi(M)$, so by Theorem 2.16 there exists an isomorphism ϕ:$F \to F$ such that $\phi|_M = \psi$. Thus ϕ is an automorphism of F. Furthermore, since $\phi|_K = \psi|_K$ is the identity, ϕ is a K-automorphism of F. □

This allows us to construct K-automorphisms in the following manner.

Theorem 3.8. *Let $F : K$ be a finite and normal field extension and let α, β be zeros in F of the irreducible polynomial p over K. Then there exists a K-automorphism ϕ of F such that $\phi(\alpha) = \beta$.*

Proof. By Theorem 2.8 there is an isomorphism ψ:$K(\alpha) \to K(\beta)$ such that $\psi|_K$ is the identity and $\psi(\alpha) = \beta$. By Theorem 3.7, ψ extends to a K-automorphism ϕ of F. □

3.2.3 Normal Closures

When we are dealing with extensions that are not normal, we can try to obtain normality by making the extensions larger. This is the thought behind normal closures.

Definition. Let $F:K$ be an algebraic extension. A *normal closure* of $F:K$ is an extension N of F such that

(i) $N:K$ is normal;

(ii) if $F \subseteq M \subseteq N$ and $M:K$ is normal, then $M=N$.

Similar to our definition of a splitting field, N is the smallest extension of F which is normal over K.

Next, we show the existence and uniqueness of a normal closure, which we shall prove using the existence and uniqueness of a splitting field.

Theorem 3.9. *Let $F:K$ be a finite extension. Then there exists a normal closure N of $F:K$. If N' is another normal closure, then the extensions $N:K$ and $N':K$ are isomorphic.*

Proof. First, we show existence. Since $F:K$ is finite, $F=K(\alpha_1,\dots,\alpha_r)$ for some integer r by Theorem 2.13. Let m_i be the minimum polynomial of α_i over K and let N be a splitting field for $f=m_1\cdots m_r$ over F. Then N is also a splitting field for f over K so that by Theorem 2.17, $N:K$ is normal and finite. Suppose that there is another field L such that $F \subseteq L \subseteq N$ where $L:K$ is normal. Each polynomial m_i has a zero $\alpha_i \in L$, so f splits over L by normality. By the definition of a splitting field, $L=N$. Hence, N is a normal closure.

Now suppose that N and N' are both normal closures. The above polynomial f splits over N and N', so both N and N' contain a splitting field for f over K. These splitting fields contain F and are normal over K by Theorem 2.17. Combining this with the definition of N and N', we must have that the splitting fields are equal to N and N' respectively. By the uniqueness of splitting fields (Theorem 2.16), $N:K$ and $N':K$ are isomorphic. □

The next two results will show that we only need to concern ourselves with a normal closure of a given extension when discussing monomorphisms. The first is a simple lemma.

Lemma 3.10. *Let $K \subseteq F \subseteq N \subseteq L$ where $F:K$ is finite and N is a normal closure of $F:K$. Further, let ψ be any K-monomorphism $F \to L$. Then $\psi(F) \subseteq N$.*

Proof. Let $\alpha \in F$. Then α has minimum polynomial m over K and

$$0 = m(\alpha) = \psi(m(\alpha)) = m(\psi(\alpha)).$$

Thus $\psi(\alpha)$ is a zero of m which implies that $\psi(\alpha) \in N$ since $N:K$ is normal. The choice of α is arbitrary so $\psi(F) \subseteq N$. □

The second result is a bit more intricate and provides a sort of converse to our lemma.

Theorem 3.11. *Let $F:K$ be a finite extension. The following statements are then equivalent:*

(i) $F:K$ is normal.

(ii) There exists a normal extension N of K containing F such that every K-monomorphism $\psi: F \to N$ is a K-automorphism of F.

(iii) For every extension L of K containing F, every K-monomorphism $\psi: F \to L$ is a K-automorphism of F.

Proof. Our methodology here will be to show that (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (iii). $F : K$ is normal so F is a normal closure of $F : K$. Additionally, $F \subseteq F$, and thus $\psi(F) \subseteq F$ by Lemma 3.10. Since ψ is also a monomorphism and a linear map between two finite dimensional vector spaces, F and $\psi(F)$, over the same field K, we have that $\psi(F) = F$. Hence ψ is a K-automorphism of F, and every K-monomorphism $\psi : F \to L$, for any extension L, is a K-automorphism of F.

(iii) $\Rightarrow$ (ii). Let N be a normal closure for $F : K$, which exists by Theorem 3.9. Then it follows from (iii) that N has the properties described in (ii).

(ii) $\Rightarrow$ (i). Suppose f is any irreducible polynomial over K with a zero α in F. Then f splits over N by normality, and if β is a zero of f in N, then there exists a K-automorphism ϕ of N such that $\phi(\alpha) = \beta$ by Theorem 3.8. By assumption in (ii), ϕ is a K-automorphism of F, so that

$$\beta = \phi(\alpha) \in \phi(F) = F.$$

Hence any irreducible polynomial f with at least one zero in F splits over F and $F : K$ is a normal extension. □

The third result is of a more computational nature.

Theorem 3.12. *Let $F : K$ be a finite separable extension of degree n. Then there are exactly n distinct K-monomorphisms of F into a normal closure N.*

Proof. We use induction on $[F : K] = n$. If $n = 1$, then $F = K$ and the identity map is the only distinct K-monomorphism of F into N. Thus the statement holds for $n = 1$.

Assume that the statement holds for all $n = k$. Let $n = k + 1$ and let $\alpha \in F \setminus K$ with minimum polynomial m over K. Then

$$\deg m = [K(\alpha) : K] = r > 1,$$

since $\alpha \notin K$. The irreducible polynomial m has one zero in the normal extension N, so it splits over N, and since m is also separable, it has the distinct zeros $\alpha_1, \dots, \alpha_r$. By the induction hypothesis, there are precisely s distinct $K(\alpha)$-monomorphisms $\rho_1, \dots, \rho_s : F \to N$, where

$$s = [F : K(\alpha)] = [F : K]/[K(\alpha) : K] = (k + 1)/r,$$

by the tower law. Now since $N : K$ is a normal and finite extension, we have by Theorem 3.8 that there are r distinct K-automorphisms $\psi_1, \dots, \psi_r$ of N such that $\psi_i(\alpha) = \alpha_i$. Consider the maps

$$\phi_{ij} = \psi_i \rho_j.$$

It is easily verified that they are $k + 1 = rs$ distinct K-monomorphisms $F \to N$. We show that these exhaust the K-monomorphisms $F \to N$.

Let $\psi : F \to N$ be a K-monomorphism. Since $0 = \psi(m(\alpha)) = m(\psi(\alpha))$, we have that $\psi(\alpha)$ is a zero of m in N. Hence $\psi(\alpha) = \alpha_i$ for some integer $1 \leq i \leq r$. The map $\phi = \psi_i^{-1}\psi$ is a $K(\alpha)$-monomorphism of $F : N$, since ψ_i^{-1} and ψ both fix K and

$$\phi(\alpha) = \psi_i^{-1}\psi(\alpha) = \psi_i^{-1}(\alpha_i) = \alpha.$$

Now, by induction, we have precisely s distinct $K(\alpha)$-monomorphisms $\rho_1, \dots, \rho_s$, so $\phi = \rho_j$ for some integer $1 \leq j \leq s$. Hence,

$$\psi = \psi_i \phi = \psi_i \rho_j.$$

Thus all K-monomorphisms $F \to N$ are of the form $\psi_i \rho_j$, and the theorem is proved. □

This enables us to calculate the order of the Galois group of a Galois extension.

Corollary 3.13. *Let $F : K$ be a Galois extension of degree n. Then $|\Gamma(F : K)| = n$.*

Proof. By Theorem 3.12 there are precisely n distinct K-monomorphisms of F into a normal closure N, and hence into any normal extension of F. Since $F : K$ is normal, we have, by Theorem 3.11, that every K-monomorphism $F \to N$ is a K-automorphism of F. Hence there are precisely n distinct K-automorphisms of F, and thus $|\Gamma(F : K)| = n$. □

This leads us to another important result.

Theorem 3.14. *If $F : K$ is a Galois extension with Galois group G, then K is the fixed field of G.*

Proof. Let K_0 be the fixed field of G and let $[F : K] = n$. Then $|G| = n$ by Corollary 3.13. By Theorem 3.5, $[F : K_0] = |G| = n$. Since K_0 is a fixed field of G we have $K \subseteq K_0$, and so we must have $K = K_0$. □

There is a converse to this, that is if K is the fixed field of the Galois group G of a finite extension, then we have a Galois extension. We need this result as well to ensure that the Galois correspondence is a bijection. Before we can prove it, however, we require a result similar in both statement and proof to Theorem 3.12.

Theorem 3.15. *Let $K \subseteq F \subseteq L$ be fields such that $L : K$ is finite and $[F : K] = n$. Then there are at most n K-monomorphisms $F \to L$.*

Proof. Let N be a normal closure of $L : K$. Then $N : K$ is finite by Theorem 3.9. Every K-monomorphism $F \to L$ is also a K-monomorphism $F \to N$ and we may therefore assume that L is a normal extension of K by replacing L with N. We now use induction on $[F : K]$ as in the proof of Theorem 3.12 with some alterations. First, by induction we have s' distinct $K(\alpha)$-monomorphisms $F \to N$ where $s' \leq s$. Second, we may lack separability, so we have r' K-automorphisms of N where $r' \leq r$ since the zeros in N need not be distinct. The rest of the argument goes through. □

Note that if we do not have separability, then there are fewer than n K-monomorphisms $F \to L$ since $r' < r$ for some choice of α.

We can now prove the converse of Theorem 3.14 when $F : K$ is finite.

Theorem 3.16. *If $F : K$ is a finite extension with Galois group G such that K is the fixed field of G, then $F : K$ is a Galois extension.*

Proof. First we show that $F : K$ is separable and second, that $F : K$ is normal.

K is the fixed field of G, so by Theorem 3.5, $[F : K] = |G|$. Let $|G| = n$. Then there are precisely n distinct K-automorphisms of F, which are K-monomorphisms $F \to F$, namely the elements of G. But as noted just above, if $F : K$ is not separable, there are fewer than n K-monomorphisms $F \to F$. Therefore, $F : K$ must be separable.

Let N be an extension of K containing F and let ψ be a K-monomorphism $F \to N$. Since N contains F, every element of G defines a K-monomorphism $F \to N$, and thus there are n K-monomorphisms $F \to N$ which are automorphisms of F. But by Theorem 3.15, we can have at most n distinct ψ, so ψ must be one of these automorphisms of F. Since condition (iii) in Theorem 3.11 is now fulfilled, we have that $F : K$ is normal by the same theorem.

$F : K$ is then a finite separable normal extension and thus it is a Galois extension. □

3.3 The Fundamental Theorem of Galois Theory

We are almost ready to properly establish the properties of the Galois correspondence between a field extension and its Galois group. Before we can state and fully prove the main theorem, however, we need a lemma.

Lemma 3.17. *Let $F\!:\!K$ be a field extension and let M be an intermediate field. Furthermore, let ψ be a K-automorphism of F. Then*

$$(\psi(M))^* = \psi M^* \psi^{-1}.$$

Proof. Let $M' = \psi(M)$, $\phi \in M^*$, and $x_1 \in M'$. Then $x_1 = \psi(x)$ for some $x \in M$, and we have

$$(\psi\phi\psi^{-1})(x_1) = \psi\phi(x) = \psi(x) = x_1,$$

so that

$$\psi M^* \psi^{-1} \subseteq M'^*.$$

Similarly $\psi^{-1} M'^* \psi \subseteq M^*$. Thus we have

$$\begin{aligned} \psi M^* \psi^{-1} &\subseteq M'^* \\ \psi M^* \psi^{-1} &\supseteq M'^* \end{aligned}$$

and hence also $M'^* = (\psi(M))^* = \psi M^* \psi^{-1}$. □

Theorem 3.18 (Fundamental Theorem of Galois Theory)**.** *Let $F : K$ be a Galois extension of degree n with Galois group G. Furthermore, let $\mathscr{F}$ be the set of all intermediate fields of $F : K$ and $\mathscr{G}$ the set of all subgroups of $\Gamma(F : K)$. Then the following statements hold true.*

(i) $|G| = n$.

(ii) The maps * and † are mutual inverses and set up an order-reversing one-to-one correspondence between $\mathscr{F}$ and $\mathscr{G}$.

(iii) If M is an intermediate field, then

$$[F : M] = |M^*|$$

and $[M : K]$ is the index of M^* in G.

(iv) An intermediate field M is a normal extension of K if and only if M^* is a normal subgroup of G.

(v) If an intermediate field M is a normal extension of K, then $\Gamma(M : K)$ is isomorphic to the quotient group G/M^*.

Proof. (i). This is just a restatement of Corollary 3.13.

(ii). Let $M \in \mathscr{F}$. We then have that $F : M$ is separable by Theorem 2.18. Additionally, since $F : K$ is normal and finite, F is a splitting field for some polynomial over K by Theorem 2.17, and therefore also a splitting field for the same polynomial over M, so that

$$M^{*\dagger} = M. \tag{3.8}$$

Now consider $H \in \mathscr{G}$. We know that $H \subseteq H^{\dagger *}$. By equation (3.8), we have that $H^{\dagger * \dagger} = (H^\dagger)^{*\dagger} = H^\dagger$. This, combined with Theorem 3.5, yields

$$|H| = [F : H^\dagger] = [F : H^{\dagger * \dagger}] = |H^{\dagger *}|.$$

Since both H and $H^{\dagger *}$ are finite groups and $H \subseteq H^{\dagger *}$, we must have that

$$H = H^{\dagger *}.$$

So for any $M \in \mathscr{F}$ and $H \in \mathscr{G}$, we have that $M^{*\dagger} = M$ and $H = H^{\dagger *}$, from which statement (ii) follows.

(iii). $F : K$ is a Galois extension, so by Corollary 3.13, $[F : M] = |M^*|$. By the tower law,

$$|M^*| = [F : M] = \frac{[F : K]}{[M : K]} \quad \Leftrightarrow \quad [M : K] = \frac{[F : K]}{|M^*|} = \frac{|G|}{|M^*|},$$

which, by the well-known theorem of Lagrange, is equal to the index of M^* in G since both groups are finite.

(iv). First, suppose that $M : K$ is normal and let $\psi \in G$. Then $\psi|_M$ is a K-monomorphism $M \to F$. Since $M : K$ is normal and $M \subseteq F$, we have that $\psi|_M$ is a K-automorphism of M by (iii) in Theorem 3.11. Hence $\psi(M) = M$. By Lemma 3.17, $M^* = (\psi(M))^* = \psi M^* \psi^{-1}$, so that $M^* \lhd G$.

Now suppose that $M^* \lhd G$ and let ψ be any K-monomorphism $M \to F$. By Theorem 3.7, there exists a K-automorphism ϕ of F such that $\psi|_M = \phi$. Now $\phi \in G$ so $\phi M^* \phi^{-1} = M^*$ since $M^* \lhd G$. Lemma 3.17 then tells us that $(\phi(M))^* = \phi M^* \phi^{-1} = M^*$. By statement (ii), we can apply the map † to both sides to get $\phi(M) = M$. Hence $\psi(M) = M$, so that ψ is a K-automorphism of M. By (ii) in Theorem 3.11 $M : K$ is normal.

(v). Let $\widetilde{G}$ be the Galois group of the normal extension $M : K$. We define the map $\phi : G \to \widetilde{G}$ by

$$\phi(\lambda) = \lambda|_M, \quad \lambda \in G.$$

We have that $\lambda|_M$ is a K-monomorphism $M \to F$, but since $M : K$ is normal, statement (ii) in Theorem 3.11 tells us that $\lambda|_M$ is a K-automorphism of M. Hence ϕ is a group homomorphism. By Theorem 3.7, there is a K-automorphism λ of F for every K-monomorphism $\mu : M \to F$, and thus in particular of for every K-automorphism of M, such that $\lambda|_M = \mu$. Therefore, ϕ is surjective. Furthermore, we observe that $\ker(\phi) = M^*$. We can employ elementary group theory to see that

$$\widetilde{G} = \operatorname{Im}(\phi) \cong G/\ker(\phi) = G/M^*.$$

All parts of the theorem are now proved. □

The importance of this theorem does not necessarily lie in its intrinsic merit, but rather in its potential to be used as a tool. It allows us to utilise results from group theory when dealing with polynomials and field extensions which dramatically expands our arsenal. Because of this, we shall need to review some results form elementary group theory before delving into the discussion of solutions of equations by radicals.

3.4 Results from Group Theory

This subsection requires some basic knowledge about group theory to be properly comprehended. The relevant theory, that is all necessary definitions, theorems, and proofs, should be included in most texts on group theory, for example Bhattacharya et al. [2], or Hungerford [3].

To facilitate the understanding of future proofs, we recall then isomorphism theorems, omitting the proofs.

Theorem 3.19 (The Isomorphism Theorems). *Let G, H, and T be groups.*

(i) If $\phi : G \to H$ is a homomorphism, then

$$G/ker(\phi) \cong im(\phi).$$

(ii) If H is a subgroup of G and $T \lhd G$, then

$$H/(T \cap H) \cong HT/T.$$

(iii) If H and T are normal subgroups of G with $T \subseteq H$, then $H/T \lhd G/T$, and

$$(G/T)/(H/T) \cong G/H.$$

These are the first, second, and third isomorphism theorems, respectively. We shall really only need these to prove the next theorem, which tells us how the property of solubility relates between a group and its subgroups.

3.4.1 Soluble Groups

Let us begin by recalling the definition of a soluble group.

Definition. A group G is *soluble* if there is a finite series of subgroups G_i of G such that

$$\langle e_G \rangle = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

for $i = 0, \cdots, n-1$, where $\langle e_G \rangle$ is the group generated by the identity in G and G_{i+1}/G_i is abelian for all i.

Theorem 3.20. *Let G be a group, H a subgroup of G, and T a normal subgroup of G.*

(i) If G is soluble, then H is soluble.

(ii) If G is soluble, then G/T is soluble.

(iii) If T and G/T are soluble, then G is soluble.

Proof. (i). Let G have a finite series of subgroups as described as in the definition and let $H_i = G_i \cap H$. Then H has the a series

$$\langle e_G \rangle = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H.$$

This stems from the fact that if $G_i \lhd G_{i+1}$, then $(G_i \cap H) \lhd (G_{i+1} \cap H)$ because $(G_i \cap H) \subseteq G_i$ and $(G_{i+1} \cap H) \subseteq G_{i+1}$. We now need to show that the factors H_{i+1}/H_i are abelian. Since $G_i \lhd G_{i+1}$, we have by the second isomorphism theorem that

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{(G_{i+1} \cap H)G_i}{G_i}.$$

The latter group is a subgroup of G_{i+1}/G_i, which is abelian, so must itself be abelian. Thus H_{i+1}/H_i is abelian for all i, and H is soluble.

(ii). Define G_i as before. Then G/T has a series

$$T/T = G_0T/T \lhd G_1T/T \lhd \ldots \lhd G_nT/T = G/T.$$

A typical quotient is

$$\frac{G_{i+1}T/T}{G_iT/T}$$

which, by the third isomorphism theorem, is isomorphic to

$$\frac{G_{i+1}T}{G_iT} = \frac{G_{i+1}(G_iT)}{G_iT} \cong \frac{G_{i+1}}{(G_iT) \cap G_{i+1}} \cong \frac{G_{i+1}/G_i}{((G_iT) \cap G_{i+1})/G_i}.$$

The first isomorphy follows from the second isomorphism theorem, and the second isomorphy from the third isomorphism theorem. The last group is a quotient group of G_{i+1}/G_i, which is abelian, so must itself be abelian. Hence G/T is soluble.

(iii). There exist two series, since both T and G/T are soluble,

$$\langle e_G \rangle = T_0 \lhd T_1 \lhd \ldots \lhd T_r = T$$

$$T/T = G_0/T \lhd G_1/T \lhd \ldots \lhd G_s/T = G/T$$

with abelian quotients. Consider the series of G given by

$$\langle e_G \rangle = T_0 \lhd T_1 \lhd \ldots \lhd T_r = T = G_0 \lhd \ldots \lhd G_s = G.$$

Then a quotient is either T_{i+1}/T_i, which is abelian, or G_{i+1}/G_i which, by the third isomorphism theorem, is isomorphic to

$$\frac{G_{i+1}/T}{G_i/T},$$

which again is abelian. Hence G is soluble. □

3.4.2 Simple Groups

We turn our attention to *simple* groups which, in a sense, can be regarded as the opposite of soluble groups. Let us once again begin by quickly recalling the definition.

Definition. A group G is *simple* if its only normal subgroups are $\langle e_G \rangle$ and G.

We now classify all groups which are both simple and soluble. Recall that all cyclic groups are abelian, that every subgroup of an abelian group is normal and that a cyclic group of prime order is simple.

Theorem 3.21. *A soluble group is simple if and only if it is cyclic of prime order.*

Proof. First, suppose that G is a simple soluble group. Then G has a series

$$\langle e_G \rangle = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G.$$

By deleting repeats, we may assume that $G_{i+1} \neq G_i$. The G_{n-1} is a proper normal subgroup of G, so $G_{n-1} = \langle e_G \rangle$ since G is simple. Hence $G_n/G_{n-1} = G$, which is abelian. Every subgroup of an abelian group is normal and every element in G generates a cyclic subgroup, so must therefore generate either $\langle e_G \rangle$ or G. Hence G is simple and cyclic, so is therefore of prime order.

Now suppose that G is a soluble cyclic group of prime order. Then G is also simple. □

Our last little excursion into reviewing results from group theory will be concerning the alternating and symmetric groups. Recall that the symmetric group S_n is the group of all permutations of a set of n elements and that the alternating group A_n is the group of all even permutations of S_n. The proof presented here is more similar in structure to the proof by Hungerford [3], rather than that of Stewart [1].

Theorem 3.22. *If $n \geq 5$, then the alternating group A_n is simple.*

Proof. This proof is rather long, so we shall split it up into two parts. Suppose that $(1) \neq T \lhd A_n$. Our methodology will be to first show that if T contains one 3-cycle, then it contains all 3-cycles and that the 3-cycles generate A_n, so that we must have $T = A_n$. Second, we shall show that T indeed contains a 3-cycle which regrettably will require some arduous case study. It is here we shall need $n \geq 5$.

According to our plan above, suppose then that T contains a 3-cycle which we may assume to be (123). Now for any integer $k > 3$, the cycle $(32k) = (2k)(3k)$ is even, so lies in A_n. Since $T \lhd A_n$, we have that

$$(32k)(123)(32k)^{-1} = (32k)(123)(3k2) = (1k2)$$

lies in T, and hence also that $(1k2)^2 = (12k) \in T$ for all $k \geq 3$. Now the symmetric group S_n is generated by all 2-cycles of the form $(1i)$ for $i = 2, \ldots, n$. Since A_n is the set of all even products of these, it is generated by all elements of the form $(1ij)$, where $1 < i < j$. But for $2 < i < j$, we have

$$(1ij) = (1j2)(12i)(12j) = (12j)^{-1}(12i)(12j),$$

so that A_n is generated by all the cycles $(12k)$ and hence $T = A_n$.

We now need to show that T must contain at least one 3-cycle. As mentioned above, we shall do this by splitting it into three cases. Every element of T is a product of disjoint cycles.

1. Some element of T contains a cyclic factor of length ≥ 4.
2. All disjoint cyclic factors of elements of T are of length ≤ 3 and at least one is of length 3.
3. All disjoint cyclic factors of elements of T are of length ≤ 2.

These cases exhaust the possibilities of the structure of T.

1. Suppose that T contains an element of the form $\sigma = (123 \ldots r)\tau$, where $r \geq 4$ and τ is a product of cycles disjoint from each other and from $(123 \ldots r)$. Now let $\delta = (123) = (12)(23) \in A_n$. Since $T \lhd A_n$, we have that $\sigma^{-1}(\delta\sigma\delta^{-1}) \in T$. Furthermore, (123) and $(123 \ldots r)$ commutes with τ since they are disjoint. Thus

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(1r \ldots 32)\big((123)(123 \ldots r)\tau(123)^{-1}\big)\\ &= \tau^{-1}\tau(1r \ldots 32)(123)(123 \ldots r)(132)\\ &= (13r)\end{aligned}$$

and T contains a 3-cycle.

2. (a) Suppose that T contains an element of the form $\sigma = (123)(456)\tau$, where τ is a product cycles disjoint from each other, from (123) and from (456). Now let $\delta = (124) \in A_n$. As in case (1), $\sigma^{-1}(\delta\sigma\delta^{-1}) \in T$, so that T contains

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= \tau^{-1}(456)^{-1}(123)^{-1}\big((124)(123)(456)\tau(124)^{-1}\big)\\ &= \tau^{-1}\tau(465)(132)(124)(123)(456)(142)\\ &= (14263)\end{aligned}$$

and hence also a 3-cycle by case (1).

(b) Suppose that T contains an element of the form $\sigma = (123)\tau$, where τ is a possibly empty product of 2-cycles disjoint from each other and from (123). Then

$$\sigma^2 = (123)\tau(123)\tau = (123)(123)\tau\tau = (123)(123) = (132)$$

lies in T, so that T contains a 3-cycle.

3. Here we may suppose that T contains an element of the form $\sigma = (12)(34)\tau$, where τ is a product of 2-cycles disjoint from each other, from (12) and from (34). Let $\delta = (123) \in A_n$. Then

$$\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(34)(12)(123)(12)(34)\tau(132) = (13)(24) = \pi \in T.$$

Since $n \geq 5$, there is an element $\rho = (13k) \in A_n$, where $k \geq 5$. Then $\pi(\rho\pi\rho^{-1}) \in T$. But

$$\pi(\rho\pi\rho^{-1}) = (13)(24)(13k)(13)(24)(1k3) = (13k),$$

so T contains a 3-cycle.

Hence T must contains a 3-cycle, so that by the first part of this proof $T = A_n$. Thus A_n has no proper normal subgroups for $n \geq 5$ and is therefore simple. □

We now connect this result to the full symmetric group S_n.

Corollary 3.23. *The symmetric group S_n is not soluble if $n \geq 5$.*

Proof. If S_n were soluble, then the subgroup A_n would be soluble by Theorem 3.20 and simple by Theorem 3.22. Hence A_n is of prime order by Theorem 3.21. But $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$ is not prime if $n \geq 5$, so we have a contradiction. Thus, S_n is not soluble for $n \geq 5$. □

We conclude this section by reviewing one final result concerning the symmetric group.

Theorem 3.24. *The symmetric group S_n is generated by the cycles $(12\ldots n)$ and (12) for any positive integer n.*

Proof. Let $\sigma = (12\ldots n)$ and $\tau = (12)$, and let G be the group generated by σ and τ. Then

$$\sigma\tau\sigma^{-1} = (12\ldots n)(12)(1n\ldots 2) = (23) \in G$$

and hence

$$\sigma(23)\sigma^{-1} = (12\ldots n)(23)(1n\ldots 2) = (34) \in G.$$

Thus G contains all 2-cycles $(m-1, m)$ for $m = 2, \ldots, n$. Then G contains

$$(12)(23)(12) = (13), \quad (13)(34)(13) = (14), \ldots$$

and therefore all 2-cycles $(1m)$. But then G contains all $(1m)(1r)(1m) = (mr)$. Every element of S_n is a product of 2-cycles, so we must have $G = S_n$. □

4 Solutions of Equations by Radicals

We are now ready to connect all of this perhaps seemingly unrelated theory and apply it to the solution of equations by radical expressions. We shall then be able to show the insolubility of general quintic equation.

4.1 Radical Extensions

We have not yet defined properly what the 'solubility by radicals' of polynomials actually means. It seems high time to do something about this. We begin with field extensions.

Definition. Let $F : K$ be a field extension. Then $F : K$ is a *radical extension* if $F = K(\alpha_1, \dots, \alpha_n)$ where, for each $i = 1, \dots, n$, there is an integer $m(i)$ such that

$$\alpha_i^{m(i)} \in K(\alpha_1, \dots, \alpha_{i-1}) \quad \text{for} \quad i \geq 2$$

and $\alpha_1^{m(1)} \in K$.

We say that the α_i together form a *radical sequence* for $F : K$.

Before we can make the connection with zeros of polynomials, we need to address the *characteristic* of a field. We define it as done in Hungerford [3].

Definition. Let F be a field. Then F is of *characteristic* n if $n1_F = 0$ for some positive integer n. If no such n exists, F is of characteristic 0.

We shall only concern ourselves with fields of characteristic zero.

Definition. Let f be a polynomial over a field K of characteristic zero and let Σ be a splitting for f over K. Then f is *soluble by radicals* if there exists a field L containing Σ such that $L : K$ is a radical extension.

There are two things to note here; first, $\Sigma : K$ need not be radical and second, this definition implies that if f has one zero expressible by radicals, then all zeros must be, by an argument based on Theorem 2.8.

We now want to prove that if K is a field of characteristic zero, then the extension $F : K$ has a soluble Galois group if there is field L such that $L : K$ is radical. This is not straight forward, and we shall need to do some preliminary work in the form of a sequence of lemmas, first concerning separability of irreducible polynomials over fields of characteristic zero.

Lemma 4.1. *If K is a field of characteristic zero, then every irreducible polynomial over K is separable over K.*

Proof. We shall prove this by contradiction. Suppose, therefore, that f is an irreducible polynomial over K which is inseparable over K. Since f then has multiple zeros in a splitting field, f and Df must have a common factor of degree ≥ 1 over K by Theorem 2.19. But f is irreducible and Df is of smaller degree than f, so we must have $Df = 0$. Thus if

$$f(t) = a_0 + \cdots + a_m t^m,$$

then $na_n = 0$ for all integers $n > 0$. Over a field of characteristic zero, this is equivalent to $a_n = 0$ for all n, so that every irreducible polynomial f is a constant polynomial, which is a contradiction. Thus, f is separable over K. □

Lemma 4.2. *Let $F : K$ be a radical extension and let N be a normal closure of $F : K$. Then $N : K$ is a radical extension.*

Proof. Let $F = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_i^{m(i)} \in K(\alpha_1, \dots, \alpha_{i-1})$ for $i = 2, \dots, n$, and $\alpha_1^{m(1)} \in K$. Let f_i be the minimum polynomial of α_i over K. Then $N \supseteq F$ is a splitting field for $f_1 \cdots f_n$. For every zero $\beta_{ij} \in N$ of f_i, there is an isomorphism $\phi : K(\alpha_i) \to K(\beta_{ij})$ by Theorem 2.8. Furthermore, since $N : K$ is normal, we have by Theorem 3.8 that ϕ extends to a K-automorphism ψ of N. Since α_i is radical over K, so is β_{ij}, and therefore also N. □

Let us now move to situations where we have abelian Galois groups.

Lemma 4.3. *Let K be a field of characteristic zero and let F be a splitting field for the polynomial $t^p - 1$ over K, where p is prime. Then $\Gamma(F : K)$ is a abelian.*

Proof. The derivative of $t^p - 1$ is pt^{p-1}, so the polynomial has no multiple zeros in in F by Theorem 2.19. Furthermore, a quick investigation shows that its zeros form a group G under multiplication. All the zeros are distinct, so G has order p, and since p is prime, G is cyclic. Let ε be the generator of this group. Then $F = K(\varepsilon)$, so that any K-automorphism of F is determined by its effect on ε. Moreover, K-automorphisms of F permute the zeros of $t^p - 1$. Hence any $\sigma_i \in \Gamma(F : K)$ is of the form

$$\sigma_i : \varepsilon \to \varepsilon^i.$$

But then

$$\sigma_i \sigma_j(\varepsilon) = \varepsilon^{ij} = \varepsilon^{ji} = \sigma_j \sigma_i(\varepsilon),$$

so that $\Gamma(F : K)$ is abelian. □

Lemma 4.4. *Let K be a field of characteristic zero over which $t^n - 1$ splits. Further, let $k \in K$ and let F be a splitting field for $t^n - k$ over K. Then $\Gamma(F : K)$ is abelian.*

Proof. Let α be any zero of $t^n - k$ and let ε be a zero of $t^n - 1$. Since $t^n - 1$ splits over K, we have n distinct zeros of $t^n - 1$ in K by the proof of Lemma 4.3. Thus, the general zero of $t^n - k$ is $\varepsilon\alpha$. Hence $F = K(\alpha)$ and any K-automorphism of F is determined by its effect on α. Let σ and τ be in $\Gamma(F : K)$. Then

$$\sigma : \alpha \to \varepsilon\alpha$$
$$\tau : \alpha \to \eta\alpha$$

where ε and η are in K, whence

$$\sigma\tau(\alpha) = \varepsilon\eta\alpha = \eta\varepsilon\alpha = \tau\sigma(\alpha),$$

and $\Gamma(F : K)$ is abelian. □

Lemma 4.5. *Let K be a field of characteristic zero and let $F : K$ be a normal and radical extension. Then $\Gamma(F : K)$ is soluble.*

Proof. We shall prove this by induction, however, we first need to make an observation. Suppose that $F = K(\alpha_1, \dots, \alpha_n)$, where $\alpha_i^{m(i)} \in K(\alpha_1, \dots, \alpha_{i-1})$ and $\alpha_1^{m(1)} \in K$. By inserting extra elements α_j when necessary, we may assume that $m(i)$ is prime for all i. In particular, there is a prime p such that $\alpha_1^p \in K$. Using this observation, we shall now prove the statement using induction on n.

If $n = 0$, then $F = K$ and $\Gamma(F : K)$ contains only the identity map, so is soluble.

Assume that the statement holds for all $n = k$ and let $n = k + 1$. If $\alpha_1 \in K$, then $F = K(\alpha_2, \dots, \alpha_{k+1})$ and $\Gamma(F : K)$ is soluble by induction.

Suppose, therefore, that $\alpha_1 \notin K$. Let f be the minimum polynomial of α_1 over K. Since $F : K$ is normal, f splits over F, and since K is of characteristic zero, $F : K$ is separable by Theorem 4.1, so that f has no repeated zeros. Since $\alpha_1 \notin K$, the degree of f is at least 2. Let β be a zero of f different from α_1 and let $\varepsilon = \alpha_1/\beta$. We have that $\alpha_1^p \in K$ so α_1 is a zero of the polynomial $g = t^p - \alpha_1^p$ over K. We must therefore have that $f|g$. Since $f(\beta) = 0$, $g(\beta) = 0$, from which it follows that $\alpha_1^p = \beta^p$. Hence, $\varepsilon^p = 1$. Furthermore, $\varepsilon \neq 1$. Thus, ε has order p in the multiplicative group of F, so the elements $1, \varepsilon, \ldots, \varepsilon^{p-1}$ are distinct pth roots of unity in F, since $(\varepsilon^k)^p = (\varepsilon^p)^k = 1^k = 1$, for any integer k. Hence, $t^p - 1$ splits over F.

We shall now consider an intermediate field and treat the Galois groups of various extensions related to this intermediate field to show that the induction step goes through. To this end, let M be a splitting field for $t^p - 1$ over K and a subfield of F, so that $M = K(\varepsilon)$. Before proceeding, we observe that $F : K$ is finite and normal by assumption, but also separable by Lemma 4.1, since K is of characteristic zero, hence $F : M$ is also finite, normal and separable, so that Theorem 3.18 applies to both extensions.

Since $t^p - 1$ splits over M and $\alpha_1^p \in M$, the proof of Lemma 4.4 implies that $M(\alpha_1)$ is a splitting field for $t^p - \alpha_1^p$ over M. Thus $M(\alpha_1) : M$ is normal, and by Lemma 4.4, $\Gamma(M(\alpha_1) : M)$ is abelian. By (v) in Theorem 3.18, we have that

$$\Gamma(M(\alpha_1) : M) \cong \Gamma(F : M)/\Gamma(F : M(\alpha_1)).$$

Now

$$F = M(\alpha_1)(\alpha_2, \ldots, \alpha_n),$$

so that $F : M(\alpha_1)$ is a normal radical extension. By induction $\Gamma(F : M(\alpha_1))$ is soluble. Since $\Gamma(M(\alpha_1) : M)$ is trivially soluble, we have, by (iii) in Theorem 3.20, that $\Gamma(F : M)$ is soluble.

The intermediate field M is a splitting field for $t^p - 1$ over K, so $M : K$ is normal. By Lemma 4.3, $\Gamma(M : K)$ is abelian and hence, also soluble. Applying (v) in Theorem 3.18, we have that

$$\Gamma(M : K) \cong \Gamma(F : K)/\Gamma(F : M).$$

Again, by (iii) in Theorem 3.20, we have that $\Gamma(F : K)$ is soluble, completing the induction step. □

We can now prove the desired result.

Theorem 4.6. *Let K be a field of characteristic zero and let $K \subseteq F \subseteq L$ such that $L : K$ is radical. Then $\Gamma(F : K)$ is a soluble group.*

Proof. Let K_0 be the fixed field of $\Gamma(F : K)$, and let N be a normal closure of $L : K_0$. Then

$$K \subseteq K_0 \subseteq F \subseteq L \subseteq N.$$

Since $L : K$ is radical, so is $L : K_0$, and by Lemma 4.2, so is $N : K_0$. Since $N : K_0$ is a also normal, $\Gamma(N : K_0)$ is soluble by Lemma 4.5.

By Theorem 3.16, $F : K_0$ is a Galois extension, so that by (v) in Theorem 3.18,

$$\Gamma(F : K_0) \cong \Gamma(N : K_0)/\Gamma(N : F).$$

Theorem 3.20 then implies that $\Gamma(F : K_0)$ is soluble. But $F : K_0$ is a Galois extension, so $\Gamma(F : K_0) = \Gamma(F : K)$, and thus $\Gamma(F : K)$ is soluble. □

Before we can restate this result in terms of polynomials, we first define the Galois group of a polynomial.

Definition. Let f be a polynomial over a field K with splitting field Σ over K. The *Galois group* of f over K is $\Gamma(\Sigma : K)$.

Let G be the Galois group of the polynomial f over the field K. If $\alpha \in \Sigma$ is a zero of f, then $f(\alpha) = 0$, so for any $g \in G$ we have

$$f(g(\alpha)) = g(f(\alpha)) = 0.$$

Hence, each element $g \in G$ induces a permutation g' on the set of zeros of f, so that distinct elements of G induces different permutations, since Σ is generated by the zeros of f and F. The map $g \to g'$ is a group monomorphism from G to the set of all permutations of the zeros of f. This is equivalent to saying that G is the group of permutations on the zeros of f. This means that we can restate Theorem 4.6 as:

Theorem 4.7. *Let f be a polynomial over a field K of characteristic zero. If f is soluble by radicals, then the Galois group of f over K is a soluble group.*

Thus to find a polynomial not soluble by radicals it is enough to find one whose Galois group is not soluble.

4.2 The General Polynomial

To prove the insolubility of the quintic equation over $\mathbb{Q}$, we shall first show that the *general polynomial* of degree $n \geq 5$ over $\mathbb{Q}$ is not soluble by radicals. This implies that there is no general formula by which all quintic equations can be solved, contrary to the situation for quadratic, cubic and quartic equations. However, this does *not* imply that all quintic polynomials are insoluble by radicals; all quintic equations might be soluble by radicals, only the solutions might look so different that they cannot be expressed in one formula. We shall, therefore, then provide an example of a specific quintic polynomial which has an insoluble Galois group

To be able to define the general polynomial of some degree, we need to consider a different notion of finiteness so that we can treat transcendental extensions.

Definition. An extension $F : K$ is *finitely generated* if $F = K(\alpha_1, \dots, \alpha_n)$ where n is finite.

Here, the α_i can be either algebraic or transcendental over K.

Definition. Let $t_1, \dots, t_n$ be transcendental elements over a field K, all lying in some extension F of K. Then they are *independent* if there is no non-trivial polynomial p over K such that

$$p(t_1, \dots, t_n) = 0$$

in F.

Lemma 4.8. *Let $F : K$ be a finitely generated extension. Then there exists an intermediate field M such that*

(i) $M = K(\alpha_1, \dots, \alpha_r)$ where the α_i are independent transcendental elements over K;

(ii) $F : M$ is a finite extension.

Proof. Let $F = K(\beta_1, \dots, \beta_n)$. If all the β_j are algebraic over K, then $F : K$ is finite by Theorem 2.13 and we may take $M = K$. If not, then some β_i is transcendental over K. Let α_1 be such an element. If $F : K(\alpha_1)$ is not finite, there exists some β_j transcendental over $K(\alpha_1)$. Let α_2 be such a β_j. We may proceed in this manner until $M = K(\alpha_1, \dots, \alpha_r)$ is such that $F : M$ is finite. By construction, the α_i are independent transcendental elements over K. □

Continuing down this road, a result due to Steinitz tells us that the number r of independent transcendental elements is independent of choice of M.

Lemma 4.9 (Steinitz)**.** *With the notation of Lemma 4.8, if there is another intermediate field $N = K(\beta_1, \dots, \beta_s)$ such that $\beta_1, \dots, \beta_s$ are independent transcendental elements over K and $F : N$ is finite, then $r = s$.*

Proof. Since $F{:}M$ is finite and $\beta_1 \in F$, β_1 is algebraic over M, there is a non-trivial polynomial p such that

$$p(\beta_1, \alpha_1, \dots, \alpha_r) = 0.$$

Some α_i must occur in this equation. Without loss of generality, we can take it to be α_1. Then α_1 is algebraic over $K(\beta_1, \alpha_2, \dots, \alpha_r)$ and $F : K(\beta_1, \alpha_2, \dots, \alpha_r)$ is finite. Continuing in this way, we get that

$$F : K(\beta_1, \dots, \beta_r)$$

is finite. Now if $s > r$, then β_{r+1} must be algebraic over $K(\beta_1, \dots, \beta_r)$, which is a contradiction, and so $s \leq r$. Repeating the argument with β_i and α_i interchanged, we get $r \leq s$. Hence, $r = s$. □

Definition. The number r in Lemma 4.8 is the *transcendence degree* of $F : K$.

Before proceeding, we must make a note on *symmetric polynomials.*

Definition. A polynomial $f(t_1, \dots, t_n)$ in n variables is *symmetric* if

$$f(t_1, \dots, t_n) = f(t_{\sigma(t_1)}, \dots, t_{\sigma(t_n)})$$

for every permutation σ of the set $\{1, \dots, n\}$.

There is a special type of symmetric polynomial, which is of considerable interest to us.

Definition. The rth *elementary symmetric polynomial*

$$s_r(t_1, \dots, t_n)$$

in the indeterminates $t_1, \dots, t_n$ is the sum of all possible distinct products with r factors of the elements $t_1, \dots, t_n$, so that

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n \\ s_2 &= t_1t_2 + t_1t_3 + \cdots + t_{n-1}t_n \\ &\vdots \\ s_n &= t_1t_2 \cdots t_n. \end{aligned}$$

If K is a field and if $t_1, \dots, t_n$ are independent transcendental elements over K, then the symmetric group S_n can be made to act as a K-automorphism of $K(t_1, \dots, t_n)$ by defining

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

for all $\sigma \in S_n$. Distinct elements of S_n give rise to distinct K-automorphisms.

Now let M be the fixed field of S_n. Then it is clear that M contains all the symmetric polynomials in the t_i, and so, in particular, all the elementary symmetric polynomials $s_r(t_1, \dots, t_n)$.

Lemma 4.10. *With the above notation, $M = K(s_1, \ldots, s_n)$.*

Proof. We shall first show that

$$[K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)] \leq n!$$

and second, that

$$[K(t_1, \ldots, t_n) : M] = n!$$

Finally, we shall observe that $K(s_1, \ldots, s_n) \subseteq M$ so that we, in fact, must have an equality.

For the first part we use induction on n. If $n = 1$, then $[K(t_1) : K(s_1)] = 1$ since $s_1(t_1) = t_1$.

Assume that the statements holds for all $n = k$ and let $n = k + 1$. Consider the double extension

$$K(t_1, \ldots, t_{k+1}) \supseteq K(s_1, \ldots, s_{k+1}, t_{k+1}) \supseteq K(s_1, \ldots, s_{k+1}).$$

We shall calculate the degree in our induction hypothesis by calculating the degree of each of these extensions and then use the tower law. Let

$$f(t) = t^{k+1} - s_1 t^k + \ldots + (-1)^{k+1} s_{k+1} = (t - t_1) \ldots (t - t_{k+1}),$$

so that $f(t_{k+1}) = 0$, and thus

$$[K(s_1, \ldots, s_{k+1}, t_{k+1}) : K(s_1, \ldots, s_{k+1})] \leq k + 1,$$

by Theorem 2.12 and Lemma 2.4. Now if we let $s'_1, \ldots, s'_k$ be the elementary symmetric polynomials in $t_1, \ldots, t_k$, we have

$$\begin{aligned} s_i &= t_1 \ldots t_i + \ldots + t_{k-i+2} \ldots t_{k+1} \\ &= t_{k+1}(t_1 \ldots t_{i-1} + \ldots + t_{k-i+2} \ldots t_k) + (t_1 \ldots t_i + \ldots + t_{k+1-i} \ldots t_k) \\ &= t_{k+1} s'_{i-1} + s'_i \end{aligned}$$

so that

$$K(s_1, \ldots, s_{k+1}, t_{k+1}) = K(t_{k+1}, s'_1, \ldots, s'_k).$$

By induction we now have

$$\begin{aligned} &[K(t_1, \ldots, t_{k+1}) : K(s_1, \ldots, s_{k+1}, t_{k+1}] \\ &\qquad = [K(t_{k+1})(t_1, \ldots, t_k) : K(t_{k+1})(s'_1, \ldots, s'_k)] \leq k! \end{aligned}$$

so that by the tower law

$$\begin{aligned} &[K(t_1, \ldots, t_{k+1}) : K(s_1, \ldots, s_{k+1})] \\ &\quad = [K(t_1, \ldots, t_{k+1}) : K(s_1, \ldots, s_{k+1}, t_{k+1})][K(s_1, \ldots, s_{k+1}, t_{k+1}) : K(s_1, \ldots, s_{k+1})] \\ &\quad \leq k!(k + 1) = (k + 1)! \end{aligned}$$

and the induction step goes through.

Since S_n is a group of K-automorphisms of $K(t_1, \ldots, t_n)$ we have, by Theorem 3.5, that

$$[K(t_1, \ldots, t_n) : M] = |S_n| = n!$$

As mentioned above, the fixed field M of S_n contains all symmetric polynomials in the t_i, and thus M must also contain $K(s_1, \ldots, s_n)$. We therefore have $M = K(s_1, \ldots, s_n)$. □

Corollary 4.11. *Every symmetric polynomial in $t_1, \dots, t_n$ over K can be written as a rational expression in $s_1, \dots, s_n$.*

Proof. The statement follows directly from the previous lemma, since symmetric polynomials lie inside the fixed field of S_n. □

Lemma 4.12. *With notation as above, $s_1, \dots, s_n$ are independent transcendental elements over K.*

Proof. We know from the proof of Lemma 4.10 that $K(t_1, \dots, t_n)$ is a finite extension of $K(s_1, \dots, s_n)$. Hence, $K(t_1, \dots, t_n)$ has transcendence degree n over K. Since $K(s_1, \dots, s_n)$ is an intermediate field of $K(s_1, \dots, s_n) : K$, it also has transcendence degree n over K. If the s_i were to be dependent, then the transcendence degree of $K(s_1, \dots, s_n)$ over K would be smaller than n. Therefore the s_i must be independent transcendental elements over K. □

We can now assign a meaning to the title of this subsection.

Definition. Let K be a field and let $s_1, \dots, s_n$ be independent transcendental elements over K. The *general polynomial of degree* n over K is the polynomial

$$t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n$$

over the field $K(s_1, \dots, s_n)$.

Note that even though we say that the polynomial is over K it is really over $K(s_1, \dots, s_n)$.

Theorem 4.13. *Let K be a field and let f be the general polynomial of degree n over K. Further, let Σ be a splitting for f over $K(s_1, \dots, s_n)$. Then the zeros $t_1, \dots, t_n$ of f in Σ are independent transcendental elements over K, and $\Gamma(\Sigma : K(s_1, \dots, s_n))$ is the symmetric group S_n.*

Proof. We have that $\Sigma : K(s_1, \dots, s_n)$ is finite by Theorem 2.17, so the transcendence degree of Σ over K is equal to that of $K(s_1, \dots, s_n)$ over K, namely n. By the definition of a splitting field, $\Sigma = K(t_1, \dots, t_n)$ and thus, the t_i are independent transcendental elements over K, since the transcendence degree of Σ over K would be smaller than n otherwise. Since the t_i are independent transcendental elements over K and the zeros of the general polynomial f over K, the s_i must be the elementary symmetric polynomials.

As previously established, S_n acts as a group of K-automorphisms of Σ, and by Lemma 4.10, the fixed field of S_n is $K(s_1, \dots, s_n)$. Now by Theorem 3.16 $\Sigma : K(s_1, \dots, s_n)$ is a Galois extension, and hence its degree is $|S_n| = n!$ by Theorem 3.5. By (i) in Theorem 3.18 $G = |\Gamma(\Sigma : K(s_1, \dots, s_n))| = n!$ and since it also contains S_n, we must have $G = S_n$. □

The insolubility of the general quintic is now finally within our grasp.

Theorem 4.14. *Let K be a field of characteristic zero and let $n \geq 5$. Then the general polynomial of degree n over K is not soluble by radicals.*

Proof. By Theorem 4.13 the Galois group of f over $K(s_1, \dots, s_n)$ is the symmetric group S_n. Since S_n is not soluble by Theorem 3.23, the general polynomial of degree n is not soluble by radicals by Theorem 4.7. □

What remains now is to exhibit an example of a quintic polynomial which is not soluble by radicals. For this, we need the associated Galois group to be insoluble. For practical purposes, we first need a lemma.

Lemma 4.15. *Let f be an irreducible polynomial of degree p over $\mathbb{Q}$ where p is prime. If f has precisely two non-real zeros in $\mathbb{C}$, then the Galois group of f over $\mathbb{Q}$ is the symmetric group S_p.*

For the proof of this theorem, we shall need to invoke a theorem in group theory by Cauchy; it states that if a prime p divides the order of a finite group, then the finite group contains an element of order p. For reasons of brevity, we shall omit the proof of this. The full statement and proof of the theorem is presented in, for example, Stewart [1].

Proof. By the fundamental theorem of algebra, $\mathbb{C}$ contains a splitting field Σ for f over $\mathbb{Q}$. Let G be the Galois group of f over $\mathbb{Q}$. Then G is a subgroup of S_p. When constructing Σ from $\mathbb{Q}$, we first adjoin a zero, which is an element of degree p, so that $[\Sigma : \mathbb{Q}]$ is divisible by p. By (i) in Theorem 3.18, p divides the order of G. By the aforementioned theorem by Cauchy, G contains an element of order p. However, the only elements of S_p of order p are the p-cycles.

Complex conjugation is a $\mathbb{Q}$-automorphism of $\mathbb{C}$, and therefore induces a $\mathbb{Q}$-automorphism of Σ. It leaves the $p - 2$ real zeros of f fixed while permuting the two non-real ones. Thus G contains a 2-cycle.

We may choose notation so that the 2-cycle is (12) and, taking a power of the p-cycle if necessary, so that the p-cycle is $(12 \dots p)$. By Theorem 3.24, these generate the whole of S_p, and thus, $G = S_p$. The lemma is proved. □

Theorem 4.16. *The polynomial $t^5 - 6t + 3$ over $\mathbb{Q}$ is not soluble by radicals.*

Once again, we shall need the use of a result omitted in this text; namely the well-known Eisenstein's criterion. Its statement and proof are also presented in Stewart [1].

Proof. Let $f(t) = t^5 - 6t + 3$. By Eisenstein's criterion, f is irreducible over $\mathbb{Q}$. We shall show that f has precisely three real zeros, each with multiplicity 1, so that we may invoke Lemma 4.15.

Since f is irreducible and $\mathbb{Q}$ is of characteristic zero, f is separable over $\mathbb{Q}$ by Lemma 4.1, so that f has no repeated zeros. We have $f(-2) = -17$, $f(-1) = 8$, $f(0) = 3$, $f(1) = -2$, and $f(2) = 23$. By Rolle's theorem, the zeros of f are separated by zeros of Df, which has two real zeros $\pm \sqrt[4]{6/5}$, so that f has at most three real zeros. But since a continuous function on the real line cannot change sign without passing through 0, f has at least three zeros. Thus f has precisely three real zeros.

Since 5 is prime, the Galois group of f is S_5 by Lemma 4.15. By Corollary 3.23, S_5 is not soluble, so that f is not soluble by radicals by Theorem 4.7. □

5 Geometric Constructions

We shall end by discussing another application of the theory of field extensions; namely impossible geometric constructions by unmarked ruler and compass. In order to make the seemingly strange leap between these two subjects, we must first establish what can be done with the tools at our disposal.

Assume that we are given a set P_0 of points in the Euclidean plane $\mathbb{R}^2$. There are then two possible operations we can perform.

(a) ***Operation 1*** (ruler): Draw a straight line through any two points in P_0.

(b) ***Operation 2*** (compass): With centre at a point in P_0, draw a circle with radius equal to the distance between any pair of points in P_0.

Definition. Points are *constructible in one step* from P_0 if they are points of intersection of any distinct lines or circles which are drawn using operations 1 or 2.

A point $r \in \mathbb{R}^2$ is *constructible* from P_0 if there is a finite sequence

$$r_1, \dots, r_n = r$$

of points of $\mathbb{R}^2$ such that, for each $i = 1, \dots, n$, the point r_i is constructible in one step from the set

$$P_0 \cup \{r_1, \dots, r_{i-1}\}.$$

It turns out that given coordinates a and b, we can with operations 1 and 2 construct $a+b$, $a-b$ and ab. If b is non-zero, we can also construct a/b, and if $a > 0$, we can construct $\sqrt{a}$. Since we can perform all field operations, the connection to field theory follows in a natural way. When constructing new points, we consider the subfield of $\mathbb{R}$ generated by the x- and y-coordinates of the points given and already constructed. Now let K_0 be the subfield of $\mathbb{R}$ generated by the coordinates of the points in P_0. If r_i is a constructible point with coordinates (x_i, y_i), then we define the associated field K_i to be

$$K_i = K_{i-1}(x_i, y_i),$$

that is the field obtained from adjoining x_i and y_i to the field K_{i-1}. This yields

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}.$$

Lemma 5.1. *With notation as above, x_i and y_i are zeros in K_i of quadratic polynomials in K_{i-1}.*

Proof. There are three possible cases: line meets line, line meets circle, and circle meets circle. Each one is dealt with using coordinate geometry. We shall only show the case 'line meets circle'.

Let A, B, and C be points with coordinates in K_{i-1} which are (a_1, a_2), (b_1, b_2), and (c_1, c_2), respectively. We draw the line AB and the circle with centre C and radius r, as can be seen in Figure 1. Note that $r^2 \in K_{i-1}$ by the Pythagorean theorem, since r is the distance between two points whose coordinates are in K_{i-1}. The equation of the line AB is

$$\frac{x - a_1}{b_1 - a_1} = \frac{y - a_2}{b_2 - a_2} \tag{5.1}$$

and of the circle

$$(x - c_1)^2 + (y - c_2)^2 = r^2. \tag{5.2}$$

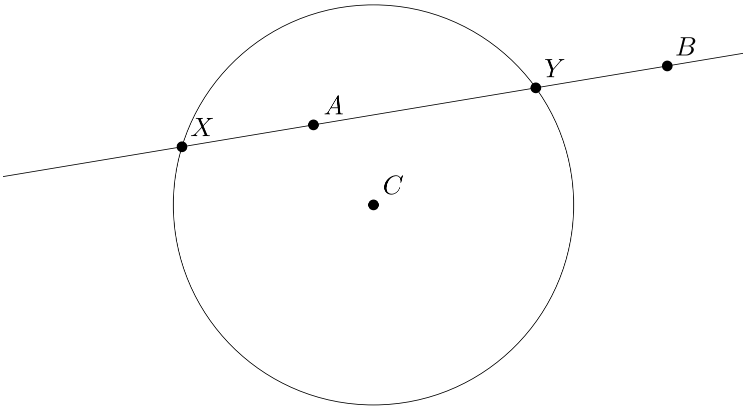

Figure 1: Line meets circle.

If we substitute equation (5.1) into equation (5.2) we obtain

$$(x - c_1)^2 + \left(\frac{(x - a_1)}{(b_1 - a_1)} (b_2 - a_2) + a_2 - c_2 \right)^2 = r^2$$

so that the x-coordinates of the intersection points X and Y are zeros of a quadratic polynomial over K_{i-1}. The same is true for the y-coordinates. □

A field extension created by adjoining the zeros of a quadratic polynomial has degree 2. The fact that our geometric constructions are results of repetitions of such processes motivates our next theorem which is key in the upcoming impossibility proofs.

Theorem 5.2. *Let $r = (x, y)$ be a point constructible from a subset P_0 of $\mathbb{R}^2$, and let K_0 be the subfield of $\mathbb{R}$ generated by the coordinates of the points in P_0. Then the degrees*

$$[K_0(x) : K_0] \quad \textit{and} \quad [K_0(y) : K_0]$$

are powers of 2.

Proof. We employ the accumulated notation. By Lemma 5.1 and Theorem 2.12 we have

$$[K_{i-1}(x_i) : K_{i-1}] = 1 \text{ or } 2.$$

If the quadratic polynomial over K_{i-1}, of which x_i is a zero, is irreducible, then the degree is 2; otherwise it is 1. Similarly,

$$[K_{i-1}(y_i) : K_{i-1}] = 1 \text{ or } 2.$$

By the tower law, we therefore have

$$\begin{aligned} [K_{i-1}(x_i, y_i) : K_{i-1}] &= [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}] \\ &= 1, 2 \text{ or } 4. \end{aligned}$$

Hence $[K_{i-1}(x_i, y_i) : K_{i-1}] = [K_i : K_{i-1}]$ is a power of 2.

An easy proof by induction using the above conclusion and the tower law shows that $[K_n : K_0]$ is a power of 2. But, once again using the tower law,

$$[K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0]$$

from which it follows that $[K_0(x) : K]$ is a power of 2. By the same reasoning, $[K_0(y) : K_0]$ is a power of 2. □

5.1 Impossibility Proofs

We shall shortly resolve three classical construction problems by showing that the constructions are impossible; the construction of a cube with twice the volume of a given one, the trisection of the angle $\pi/3$, and the construction of a square equal in area to that of a given circle. However, one crucial note must first be made. For these three proofs, we shall use two results not included in this thesis; one that is easy to prove, and one that is much more difficult. The first is Eisenstein's criterion, which we have used once before, and the second is the transcendence of π over $\mathbb{Q}$ which was famously proved by Lindemann. The full statement and proof of both of these results are presented in Stewart [1].

Theorem 5.3. *The cube cannot be duplicated using constructions by means of unmarked ruler and compass.*

Proof. We are given a cube and without loss of generality, we may take the side of that cube to be the unit interval on the x-axis. We may therefore further assume that $P_0 = \{(0,0),(1,0)\}$, so that $K_0 = \mathbb{Q}$. If we were able to duplicate the cube, then we should be able to construct the point $(\alpha, 0)$, where $\alpha = \operatorname{Re}\sqrt[3]{2}$, and so $[\mathbb{Q}(\alpha):\mathbb{Q}]$ would be a power of 2 by Theorem 5.2. But α is a zero of the polynomial t^3-2 over $\mathbb{Q}$, which is irreducible over $\mathbb{Q}$, so that t^3-2 is the minimum polynomial of α over $\mathbb{Q}$. Hence $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ by Theorem 2.12, which is a contradiction to Theorem 5.2. Thus, the cube cannot be duplicated. □

Theorem 5.4. *The angle $\pi/3$ cannot be trisected using constructions by means of unmarked ruler and compass.*

Proof. Trisecting the angle $\pi/3$ is equivalent to constructing the angle $\pi/9$, which in turn is equivalent to constructing the point $(\alpha, 0)$ given the points $(0,0)$ and $(1,0)$, where $\alpha = \cos(\pi/9)$. From this we can construct $(\beta, 0)$ where $\beta = 2\cos(\pi/9)$. We recall the trigonometric formula

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

If we put $\theta = \pi/9$, then $\cos(3\theta) = 1/2$, so that

$$\frac{1}{2} = 2(2\cos^3(\pi/9)) - 3\cos(\pi/9) = 2\beta^3 - \frac{3\beta}{2} \quad \Leftrightarrow \quad \beta^3 - 3\beta - 1 = 0.$$

Now let $f(t) = t^3 - 3t - 1$. Since

$$f(t+1) = t^3 + 3t^2 - 3$$

is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, so is $f(t)$, and so f is the minimum polynomial of β over $\mathbb{Q}$. Thus $[\mathbb{Q}(\beta):\mathbb{Q}] = 3$, a contradiction to Theorem 5.2. □

Theorem 5.5. *The circle cannot be squared using constructions by means of unmarked ruler and compass.*

Proof. We may assume that the given circle has radius 1 and thus, area π. The problem is then equivalent to constructing $(0, \sqrt{\pi})$ from the points $(0,0)$ and $(0,1)$. If such a construction exists, then we can use it to construct $(0, \pi)$, which by Theorem 5.2 implies that $[\mathbb{Q}(\pi):\mathbb{Q}]$ is a power of 2, and thus in particular that π is algebraic over $\mathbb{Q}$. This is a contradiction by Lindemann's theorem. Such a construction is therefore impossible. □

References

[1] Stewart, I. *Galois Theory.* Second edition. Chapman and Hall Ltd, London (1989)

[2] Bhattacharya, P.B., Jain, S.K. and Nagpaul, S.R. *Basic Abstract Algebra.* Second edition. Cambridge University Press (1994)

[3] Hungerford, T.W. *Abstract Algebra: An Introduction.* Third edition. International edition. Brooks/Cole, Cengage Learning (2014)