GALOIS THEORY AND THE ABEL-RUFFINI THEOREM

MISHAL MRINAL

Abstract. This paper builds up all the requisite knowledge to prove results in Galois Theory aiming at proving the celebrated Abel-Ruffini Theorem about the insolvability of polynomials of degree 5 and higher by radicals. We then make use of Galois Theory to compute explicitly the Galois groups of a certain class of polynomials. We assume basic knowledge of Group Theory and Field Theory, but otherwise this paper is self-contained.

Contents

1. Introduction

Consider the general quadratic

$$ax^2 + bx + c$$

It is a well known fact that for any given quadratic, we can explicitly write down a formula to find its roots, without even knowing a priori what its coefficients are, simply plug them into this formula

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

and we have its roots. Similar formulae involving the elementary operations of $+, -, /, \times, \sqrt{}$ were found for solving the cubic and the quartic by mathematicians, however no progress of this kind was ever made for polynomials of higher degree. In this paper, we prove the celebrated Abel-Ruffini theorem, which established the

impossibility of solving the general polynomial of degree 5 or higher using the basic arithmetic operations.

2. Normal Subgroups and Solvable Groups

Definition 2.1. We say that a subgroup N of G is normal in G if for all $n \in N$, $gng^{-1} \in N$ for all $g \in G$.

Definition 2.2. We say that a group G is solvable if there exists a chain of subgroups (called a subnormal series)

$$\{\text{Identity}\} = G_1 \leq G_2 \leq \ldots \leq G_k = G$$

such that each G_{i-1} is normal in G_i and the quotients G_i/G_{i-1} are all cyclic.

3. Field Extensions

Definition 3.1. If K is a field containing a field F, then K is said to be an extension of F and is denoted by K/F.

Definition 3.2. The degree of an extension K/F, denoted by $[K : F]$ is the dimension of K as a vector space over the field F. If this degree is finite, then the extension is said to be finite, otherwise it is infinite.

The field extensions that we are interested in are those that solve certain polynomial equations over a given field F. For instance, consider the polynomial $x^2 - 2$. This is clearly a polynomial over $\mathbb{Q}$, however, its roots are not in $\mathbb{Q}$. We can adjoin one of its roots, namely $\sqrt{2}$ to the field of rationals to get $\mathbb{Q}(\sqrt{2})$, which is the set of all numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. It is easy to check that this new set is a field, and it in fact contains $\mathbb{Q}$, so it is a field extension of it that contains the roots of the polynomial $x^2 - 2$. The degree of this extension is 2, as we can see that a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$. This example motivates the following definition -

Definition 3.3. We say that an element $\alpha \in K$ is algebraic over a field F if it is the root of some non-zero polynomial over F. The extension K/F is said to be algebraic if every element of K is algebraic over F.

Proposition 3.4. *Let $\alpha \in K$ be algebraic over F. Then there exists a unique, monic irreducible polynomial $m(x)$ over F such that $m(\alpha) = 0$. Any polynomial has α as a root if and only if it is divisible by $m(x)$, i.e $m(x)$ is the polynomial of minimal degree with α as a root.*

Proof. The justification for some of the tools used in this proof relies on ring theory, which we take for granted.

Suppose we have a polynomial $g(x)$ of minimal degree over F such that $g(\alpha) = 0$. We can asssume $g(x)$ is monic, as if it isn't we can simply multiply by a constant factor, which leaves its roots unchanged. Suppose that it is reducible, then there exist polynomials $a(x), b(x)$ both of smaller degree than g such that $g(x) = a(x)b(x)$. This implies that $g(\alpha) = a(\alpha)b(\alpha) = 0$, which implies that either a or b have α as a root, which contradicts the minimality of the degree of g with the property that α is a root.

Suppose that a polynomial $f(x)$ over F has α as a root. By the euclidean algorithm, we know that there exist polynomials $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

where $\deg r(x) < \deg g(x)$. Therefore,

$$f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = 0$$

and so since

$$g(\alpha)q(\alpha) = 0$$

we can conclude that

$$r(\alpha) = 0$$

which implies that $r(x) = 0$, as otherwise we have a contradiction, since the degree of r is lesser than the degree of g. Therefore, $g(x)$ divides any polynomial that has α as a root, and $g(x) = m(x)$, which proves uniqueness.

□

We call $m(x)$ the minimal polynomial of α over F, and it is characterised as the monic, irreducible polynomial of minimal degree that has α as a root. In the example considered earlier, $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. The degree of the minimal polynomial is called the degree of the element α. We take for granted the fact that the degree of extension of some simple extension $F(\alpha)/F$ is the degree of the minimal polynomial of α over F.

Theorem 3.5. *The element α is algebraic over F if and only if $F(\alpha)/F$ is finite.*

Proof. ($\Longrightarrow$) If α is algebraic over F, then the degree of extension of $F(\alpha)$ over F is the degree of the minimal polynomial of α over F, which is finite.
($\Longleftarrow$) Suppose $[F(\alpha) : F] = n$. Then we know that the $n + 1$ elements

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

are linearly dependent. This means that there exist $b_1, b_2, \ldots, b_{n+1}$, where each $b_i \in F$ and are not all 0, such that

$$b_1 + b_2\alpha^1 + \ldots + b_{n+1}\alpha^n = 0$$

so we have found a polynomial over F whose root is α, hence α is algebraic over F. □

Proposition 3.6. *If $[K : F]$ is finite, then the extension K/F is algebraic.*

Proof. Consider some $\alpha \in K$. Then $F(\alpha)$ is a subspace of K if we look at both as vector spaces over F, thus $[F(\alpha) : F] \leq [K : F]$. This implies that $[F(\alpha) : F]$ is finite, and hence is algebraic, which proves that K/F is algebraic. □

We now prove one of the most fundamental theorems of field extensions:

Theorem 3.7 (**Tower Law**)**.** *Suppose we have a tower of field extensions $F \supset K \supset L$, then*

$$[F : L] = [F : K][K : L]$$

Proof. Let $[F : K] = n$ and $[K : L] = m$, and let $\{\alpha_1, \ldots \alpha_n\}$ be a basis for F over K and let $\{\beta_1, \ldots, \beta_m\}$ be a basis for K over L. We claim that $A = \{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for F over L.

First we prove that the elements of A are linearly independent. Suppose that there exist $b_{ij} \in L$, such that

$$\sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}\alpha_i\beta_j = 0$$

Then, making some rearrangements we can rewrite the above expressions as

$$\sum_{i=1}^{n} a_i\alpha_i = 0$$

where

$$a_i = \sum_{j=1}^{m} b_{ij}\beta_j$$

Notice that each a_i is in K, and due to the linear independence of $\{\alpha_1, \dots \alpha_n\}$, we can conclude that each $a_i = 0$. Due to the linear independence of $\{\beta_1, \dots, \beta_m\}$, we can conclude that each b_{ij} must be equal to 0, therefore the elements of A are linearly independent.

Now we prove that the elements of A generate F. Pick some $v \in F$. Then from the fact that $\{\alpha_1, \dots, \alpha_n\}$ generates F, we know that there exist $a_i \in K$ such that

$$\sum_{i=1}^{n} a_i\alpha_i = v$$

Similarly, from the fact that $\{\beta_1, \dots, \beta_m\}$ generate K, we know that there exist $b_{ij} \in L$ such that

$$\sum_{i=1}^{m} b_{ij}\beta_i = a_j$$

Therefore, we have that

$$\sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}\beta_j\alpha_i = v$$

which proves that the elements of A are generating, and so forms a basis. Therefore,

$$[F : L] = nm = [F : K][K : L]$$

□

4. Separable and Inseparable Extensions

Definition 4.1. Let K be a field extension of F. K is called the splitting field for some polynomial $f(x)$ over F if $f(x)$ factors completely into its linear factors over K, and does not factor completely into its linear factors over any proper subfield (i.e K is the "smallest" field with this property)

Definition 4.2. We call an extension K/F normal if and only if for any embedding $\sigma : K \to \overline{F}$ such that $\sigma|_F = Id$ we have $\sigma(K) = K$.

There are infact many different ways to characterise normality - which we take for granted for brevity's sake. The proofs can be found in Chapter V of Lang's *Algebra*.

The following definitions are all equivalent -

(1) Definition 4.2

(2) K is the splitting field of a family of polynomials over F
(3) If an irreducible polynomial $f(X)$ over F has a root $\alpha \in K$, then it splits completely in K

Proposition 4.3. *The degree of extension of the splitting field of a polynomial of degree n over a field F is at most $n!$*

Proof. For any given polynomial $f(x)$ over F of degree n, adjoining a root will generate an extension F_1 of at most degree n over F(and it will be equal to n if and only if $f(x)$ is irreducible over F). Similarly, the degree of extension of adjoining any other root of $f(x)$ will be at most $n-1$ over F_1, and so on. Thus, using the tower law, we can conclude that the degree of extension of the splitting field would be at most $n!$ □

Consider some polynomial $f(x)$ over F. Then, in its splitting field, we may write

$$f(x) = (x-\alpha_1)^{n_1} \dots (x-\alpha_k)^{n_k}$$

where each α_i is distinct, and is in the splitting field of f, and each $n_i \geq 1$. The n_i is called the multiplicity of the root α_i. If $n_i > 1$, then α_i is said to be a multiple root.

Definition 4.4. A polynomial $f(x)$ over F is called separable if it has no multiple roots, otherwise the polynomial is said to be inseparable.

Proposition 4.5. *A polynomial $f(x)$ has a multiple root α if and only if α is also a root of its derivative. i.e, a polynomial is separable if and only if it and its derivative are relatively prime.*

Proof. ($\Longrightarrow$) Let

$$f(x) = (x-\alpha)^n g(x)$$

where $n \geq 2$ and $g(x)$ is some polynomial in the splitting field of f. Then

$$f'(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n g'(x)$$

and clearly, α is a root of $f'(x)$.

($\Longleftarrow$) Suppose that α is a root of $f(x)$ and $f'(x)$. Then we can write

$$f(x) = (x-\alpha)g(x)$$

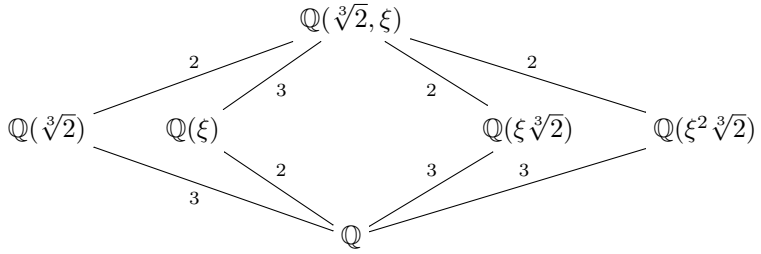
and

$$f'(x) = g(x) + (x-\alpha)g'(x)$$

From the fact that $f'(\alpha) = 0$, we can conclude that $g(\alpha) = 0$, and so α is a multiple root of $f(x)$. □

Example 4.6. Consider the polynomial $x^3 - 2$, which clearly is a polynomial over $\mathbb{Q}$. Note that $\sqrt[3]{2}$ is a root, and furthermore $\xi\sqrt[3]{2}$ is also a root, where ξ is a cube root of unity. It is easy to check that, $\mathbb{Q}(\sqrt[3]{2}, \xi)$ is the splitting field for this polynomial, and by the tower law it is again easy to check that this is a degree 6 extension, as adjoining the cube root of 2 is a degree 3 extension, and adjoining any cube root of unity has the cyclotomic polynomial of degree 2 as its minimal

polynomial and hence is a degree 2 extension. We can thus construct the following Hasse diagram of subfields:



The numbers on the arrow indicate the degree of each subextension from the starting field to the ending field - note that any path from $\mathbb{Q}$ to $\mathbb{Q}(\xi, \sqrt[3]{2})$ has a product of 6 which illustrates the tower law. Furthermore, this lattice of subfields has 6 elements.

5. Galois Theory

5.1. **Group of Automorphisms.**

Definition 5.1. An automorphism of K is an isomorphism $\sigma : K \to K$. We denote the set of all automorphisms of K by $Aut(K)$.

Definition 5.2. An automorphism σ is said to fix a set F, if $\sigma(\alpha) = \alpha$ for all $\alpha \in F$.

Definition 5.3. Let K/F be a field extension. Then let $Aut(K/F)$ denote the set of all automorphisms on K which fix F.

Proposition 5.4. *$Aut(K)$ under composition forms a group, and $Aut(K/F)$ is a subgroup.*

Proof. An identity exists, namely the identity map. For any given automorphism σ, σ^{-1} also exists, and it is the inverse. Composition is associative, and composing two automorphisms gives another automorphism, so $Aut(K)$ forms a group.

Consider two automorphisms σ and τ that fix the field F. Then $\sigma\tau$ and σ^{-1} also fix F, which by the subgroup test allows us to conclude that $Aut(K/F)$ is a subgroup. □

Proposition 5.5. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in Aut(K/F)$, $\sigma(\alpha)$ is a root of the minimal polynomial for $\alpha \in F$, i.e $Aut(K/F)$ permutes the roots of the minimal polynomial of α over F.*

Proof. Suppose we have that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$$

where each $a_i \in F$. Then applying the automorphism σ to both sides, we get

$$\begin{aligned}
&\sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0) = 0\\
&\sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \ldots + \sigma(a_0) = 0\\
&\sigma(\alpha^n) + a_{n-1}\sigma(\alpha^{n-1}) + \ldots + a_0 = 0\\
&(\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \ldots + a_0 = 0
\end{aligned}$$

and so $\sigma(\alpha)$ satisfies the same polynomial. We use the fact that σ fixes F in the third inequality, and the fact that σ is multiplicative in the last equality. □

We can even associate to each group of automorphisms a field extension.

Proposition 5.6. *Let $H \leq Aut(K)$ be a subgroup of automorphisms of K. Then the set F of all the elements of K fixed by all elements of H forms a subfield of K.*

Proof. Consider some $\sigma \in H$ and $a, b \in F$. Then $h(a \pm b) = h(a) \pm h(b) = a \pm b$, $h(ab) = h(a)h(b) = ab$ and $h(a^{-1}) = (h(a))^{-1} = a^{-1}$, thus F is closed and so is a subfield. □

We call the subfield fixed by all the elements of a subgroup H of $Aut(K)$ the fixed field of H.

Theorem 5.7 (**Inclusion-reversing**). *The correspondence between field extensions to groups and groups to field extensions is inclusion reversing -*

(1) if $F_1 \subset F_2 \subset K$ are two subfields of K, then $Aut(K/F_2) \leq Aut(K/F_1)$ and
(2) If $H_1 \leq H_2 \leq Aut(K)$ are two subgroups with fixed fields F_1 and F_2 respectively, then $F_2 \subset F_1$.

Proof. For the first part, since any automorphism σ fixing F_2 also fixes F_1, σ will be in $Aut(K/F_1)$ also, so $Aut(K/F_2) \leq Aut(K/F_1)$.

Similarly, Since any element of H_1 is also an element of H_2, we know that all elements of H_1 also fix F_2, which implies that $F_2 \subset F_1$. □

Definition 5.8. Let K/F be any finite extension. K is said to be Galois over F if $|Aut(K/F)| = [K : F]$. In this case the group of automorphisms is called the Galois group of K/F and is denoted $Gal(K/F)$.

5.2. **Characterisation of Galois Extensions.**

Definition 5.9. A character χ of a group G whose values are in a field L is a homomorphism from G to the multiplicative group of L:

$$\chi : G \to L^{\times}$$

We map into the multiplicative group of L so that $\chi(g) \neq 0$ for all $g \in G$.

Definition 5.10. The characters $\chi_1, \chi_2, \ldots, \chi_n$ of G are said to be linearly independent over L if they are linearly independent as functions on G, i.e, there is no non-trivial relation

$$a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0 \qquad (a_1, a_2, \ldots, a_n \in L, \text{not all equal to } 0)$$

Theorem 5.11 (**Linear Independence of Characters**). *If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G, then they are linearly independent over L.*

Proof. Suppose that the characters were linearly dependent. Then there exist non-trivial relations as defined in the previous definition. Consider a relation which has the minimal number of non-zero terms. Then WLOG, let $a_1, a_2, \ldots, a_m$ be the non-zero coefficients of this relation, such that

$$a_1\chi_1 + \ldots a_m\chi_m = 0$$

Pick some $g \in G$ such that $\chi_1(g) \neq \chi_m(g)$. We know that such a g exists as these characters are distinct. Then for all $g' \in G$ we have that

$$a_1\chi_1(gg') + \ldots + a_m\chi_m(gg') = 0$$

Note that for all $g' \in G$

$$a_1\chi_1(g') + \ldots + a_m\chi_m(g') = 0$$

and so

$$a_1\chi_1(g')\chi_m(g) + \ldots + a_m\chi_m(g')\chi_m(g) = 0$$

Subtracting this equation from the previous one, we get

$$\begin{aligned} &a_1\chi_1(g')\chi_m(g) + \ldots + a_m\chi_m(g')\chi_m(g) - (a_1\chi_1(gg') + \ldots + a_m\chi_m(gg')) = 0 \\ &\implies [\chi_m(g) - \chi_1(g)]a_1\chi_1(g') + \ldots + [\chi_m(g) - \chi(m)]a_m\chi_m(g') = 0 \\ &\implies [\chi_m(g) - \chi_1(g)]a_1\chi_1(g') + \ldots [\chi_m(g) - \chi_{m-1}(g)]a_{m-1}\chi_{m-1}(g') = 0 \end{aligned}$$

notice that the first term is non-zero and so we have found a non-trivial relation on the characters with even fewer non-zero terms than we started, a contradiction. So, the characters are linearly independent. □

For our purposes, consider a homomorphism σ between fields L and K, and note that σ is a homomorphism between the multiplicative groups $L^\times$ and $K^\times$, so σ can be viewed as a character on $K^\times$ with values in L.

Note that thinking of σ as a character loses no information when compared to thinking of σ as a function between fields. This is because restricting K to its multiplicative group does not lead to any loss of information as we know that for any homomorphism of fields, the zero element maps to zero.

We now prove a fundamental relation about finite extensions and the order of the subgroup associated to them.

Proposition 5.12. *Let $G = \{Id\,, \sigma_2, \ldots, \sigma_n\}$ be a group whose fixed field is F. Then*

$$[K : F] = n = |G|$$

Proof. We do a proof by contradiction. Suppose that $[K : F] \neq n$.
Case 1: $n > [K : F]$. Suppose that $[K : F] = m$, and let $\omega_1, \ldots, \omega_m$ be a basis for K over F. Consider the system of equations

$$\begin{aligned} &Id(\omega_1)x_1 + \ldots + \sigma_n(\omega_1)x_n = 0 \\ &\vdots \\ &Id(\omega_m)x_1 + \ldots + \sigma_n(\omega_m)x_n = 0 \end{aligned}$$

We have m equations in n variables, therefore a non-trivial solution $\beta_1, \ldots \beta_n$, $\beta_i \in K$, exists. Consider some $a_1, \ldots, a_m \in F$. We know that all automorphisms in G fix all these elements, so we have the system of equations

$$\begin{aligned} &Id(a_1\omega_1)\beta_1 + \ldots + \sigma_n(a_1\omega_1)\beta_n = 0 \\ &\vdots \\ &Id(a_m\omega_m)\beta_1 + \ldots + \sigma_n(a_m\omega_m)\beta_n = 0 \end{aligned}$$

Adding all the equations we get the equation

$$Id(a_1\omega_1 + \dots a_m\omega_m)\beta_1 + \dots + \sigma_n(a_1\omega_1 + \dots + a_m\omega_m)\beta_n = 0$$

Note that the coefficients of all the β_i are in K, so we can replace them with some $\alpha \in K$, and we get the equation

$$Id(\alpha)\beta_1 + \dots + \sigma_n(\alpha)\beta_n = 0$$

a contradiction, as we have shown that the characters are linearly dependent, since our choices of a_i are not all zero.
Case 2: $n < [K : F]$. We are yet to use the fact that G is a group, which we make use of here. We know that there exist $n + 1$ linearly independent elements in K over F. Let $\alpha_1, \dots, \alpha_{n+1}$ denote these elements. Consider the system of equations

$$\begin{aligned} Id(\alpha_1)x_1 + \dots + Id(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \dots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

We have n equations in $n+1$ variables, and so we know that there exists a non-trivial solution $\beta_1, \dots, \beta_{n+1}$, $\beta_i \in K$. We know that at least one of these β_i is not in F as otherwise the first equation implies that $\alpha_1, \dots, \alpha_{n+1}$ are not linearly independent. Amongst all the solutions, pick the solution with the minimum number of non-zero elements, and let $\beta_1, \dots, \beta_r$ denote the non-zero elements of the solution set, where $\beta_1 \notin F$, WLOG. We also regard $\beta_r = 1$, by dividing all the equations by β_r.
Then we have the system of equations

$$\sigma_j(\alpha_1)\beta_1 + \dots + \sigma_j(\alpha_r) = 0 \qquad (j \in [n], \text{ and } \sigma_1 = Id)$$

Since $\beta_1 \notin F$, we know that there exists an automorphism $\sigma' \in G$ such that $\sigma'(\beta_1) \neq \beta_1$. Applying σ' to the equations, we get

$$\sigma'\sigma_j(\alpha_1)\sigma(\beta_1) + \dots + \sigma'\sigma_j(\alpha_r) = 0$$

Now we make use of the property that G forms a group - all the $\sigma'\sigma_j$ terms are in fact rearrangements of the σ_i where $i \in [n]$. Thus we can define a numbering $\sigma'\sigma_j = \sigma_i$, and we can rewrite the equation as

$$\sigma_i(\alpha_1)\sigma'(\beta_1) + \dots + \sigma_i(\alpha_r) = 0$$

Now we subtract the previous system that we first introduced with this new system, to obtain the new system

$$[\sigma'(\beta_1) - \beta_1]\sigma_i(\alpha_1) + \dots + [\sigma'(\beta_{r-1} - \beta_{r-1}]\sigma_i(\alpha_{r-1}) = 0$$

and since $\sigma'(\beta_1) - \beta_1 \neq 0$, we have found a non-trivial solution with even fewer zeroes than we started with, a contradiction.

Therefore, $[K : F] = n$. □

We now introduce another characterisation of Galois Extensions

Proposition 5.13. *The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irreducible polynomial over F which has a root in K splits completely in K.*

Proof. ($\implies$) Let $G = Gal(K/F)$ and let $p(x)$ be an irreducible polynomial, which has a root $\alpha \in K$. Consider the elements

$$\alpha, \sigma_1(\alpha), \ldots, \sigma_n(\alpha)$$

where each $\sigma_i \in G$. Let

$$\alpha_1, \alpha_2, \ldots, \alpha_r$$

be the distinct elements from the previous list of elements. Note that since G is a group, if we apply $\tau \in G$ to the set of automorphisms $\{ \mathrm{Id}, \sigma_1, \ldots, \sigma_n\}$, then we get the same set as G is a group. Thus applying any automorphism $\tau \in G$ on the distinct elements results in the same set.

Thus consider the polynomial

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_r)$$

As we established, any automorphism shuffles the roots of this polynomial, and so its coefficients are fixed by them, and so lie in the fixed field of the automorphisms, which is F in our case. Since $p(x)$ is irreducible, and has α as a root, it is the minimal polynomial for α over F(we can assume that $p(x)$ is monic). Thus as we proved in proposition 3.4, $p(x)$ must divide $f(x)$ over F. It is also clear from proposition 5.5 that since applying automorphisms to α shuffles between the roots of $p(x)$, $f(x)$ must divide $p(x)$ over K. So $f(x) = p(x)$, thus $p(x)$ is separable and all its roots lie in K. □

Definition 5.14. Let K/F be a Galois Extension. If $\alpha \in K$, then the set of all elements $\sigma(\alpha)$ for all $\sigma \in Gal(K/F)$ are called the conjugates of α over F.

Now notice that we have multiple characterisations of Galois extensions -

(1) A Galois extension is a finite, normal and separable extension.
(2) A Galois extension is an extension for which the the order of the group of automorphisms fixing the base field is equal to the degree of extension.
(3) A Galois extension is the splitting field of some separable polynomial over the base field.
(4) An extension K/F is Galois when the field fixed by $Aut(K/F)$ is exactly F(the field could be larger in other cases).

Some of the above implications are not proven in this section for the sake of brevity. We are now ready to prove the Fundamental Theorem of Galois Theory.

5.3. **The Fundamental Theorem of Galois Theory.**

Theorem 5.15 (**The Fundamental Theorem of Galois Theory**). *Let K/F be a Galois extension, and let $G = Gal(K/F)$. Then there is a bijection between all subfields E of K containing F, and the subgroups H of G, given by the correspondence*

$$E \longrightarrow \{\textit{The elements of } G \textit{ fixing } E\}$$

and

$$\{\textit{The fixed field of } H\} \longleftarrow H$$

Under this correspondence, we have the following properties -

(1) (Inclusion reversing) If E_1, E_2 correspond to H_1 and H_2 respectively then $E_1 \subset E_2$ if and only if $H_2 \leq H_1$.
(2) $[K : E] = |H|$ and $[E : F] = |G : H|$

(3) *K/E is always Galois, with Galois Group $Gal(K/E) = H$*
(4) *E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group*

$$Gal(E/F) \cong G/H$$

.

Proof. We first prove that the correspondence is bijective. To prove that there is an injection from subgroups to fields, suppose we have two subgroups of G_1, G_2 of G such that $G_1 \neq G_2$, with fixed fields F_1, F_2 respectively. We claim that $F_1 \neq F_2$. Suppose that $F_1 = F_2$, then we know that all elements of G_1 also fix the field F_2, which implies that $G_1 \leq G_2$. By the same reasoning, we can conclude that $G_2 \leq G_2$, which implies that $G_1 = G_2$, a contradiction, hence $F_1 \neq F_2$. So the correspondence is injective from subgroups to fields.

To establish surjectivity, we know from the fact that K/F is Galois that it is the splitting field of some separable polynomial $f(x)$ over F. Since E contains F, $f(x)$ is also a polynomial over E, and so K/E is also Galois. This implies that E is the fixed field of $Aut(K/E) \leq G$. So the group of automorphisms of every subfield of K containing F arises as the subgroup of G, which proves the correspondence is surjective, and hence is bijective.
We already proved (1) in 5.7.

To prove (2), we make use of the tower law. Suppose that $E = K^H$, i.e, the field that is fixed by the subgroup H of G. Then we know from 5.12 that $[K : E] = |H|$. From the tower law, we know that

$$[K : F] = [K : E][E : F] = |G|$$

which implies that

$$|H|[E : F] = |G|$$

$$[E : F] = \frac{|G|}{|H|} = |G : H|$$

To Prove (3), we proceed by proving that every finite automorphism fixing E is contained in H, which would prove that K/E is Galois. We know that $|H| \leq Aut(K/E) \leq [K : E]$, as the fixed field of the group may be larger than E. By 5.12, we know that $[K : E] = |H|$, and therefore, we must have that $|H| = [K : E]$, and so the extension K/E is Galois, with Galois group $Gal(K/E)$.

To prove (4), we make use of the fact that a Galois Extension is a finite, normal and separable extension. Let E/F be a Galois extension. Recall that E/F is a normal extension if and only if for all $\sigma \in Gal(K/F)$, $\sigma(E) = E$. Therefore, we can define the map

$$f : Gal(K/F) \to Gal(E/F)$$

defined as

$$f(\sigma) = \sigma|_E$$

By definition, since the extension E/F is normal, the restriction of σ to E defines an automorphism. We claim that f is a homomorphism between groups. To verify

this, consider $\sigma, \tau \in Gal(K/F)$. Then note that

$$f(\sigma \circ \tau) = (\sigma \circ \tau)|_E$$

which is an automorphism on E, and we have the fact that

$$(\sigma \circ \tau)|_E = \sigma|_E \circ \tau|_E = f(\sigma) \circ f(\tau)$$

which follows due to the fact that all of these restrictions are automorphisms on E, so f is in fact a group homomorphism. We also claim that H is the kernel of this homomorphism. Consider some $\sigma \in H$

$$f(\sigma) = \sigma|_E = Id$$

since E is the fixed field of H. Since H is the kernel of some homomorphism of $Gal(K/F)$, it is a normal subgroup of it.
From properties of normal subgroups, G/H is isomorphic to some subgroup of $Gal(E/F)$. Note that by the tower law

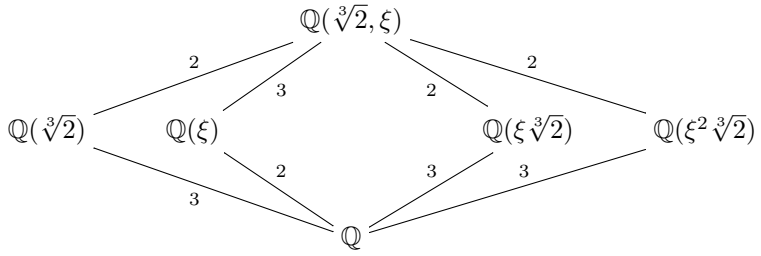
$$|Gal(E/F)| = [E : F] = \frac{[K : F]}{[K : E]} = \frac{|Gal(K/F)|}{|Gal(K/E)|} = \frac{|G|}{|H|} = |G : H|$$

and so

$$Gal(E/F) \cong G/H$$

For the other direction, suppose that H is a normal subgroup in $Gal(E/F)$, and consider some $\sigma \in G$ and some $q \in E$. Let $p = \sigma(q)$. Due to the normality of H, we know that q is stabilised by H, and so p is stabilised by $\sigma H \sigma^{-1} = H$. By the bijective correspondence that we just established, the only elements of K that are stabilised by all of H are those in the field E, which implies that $\sigma(E) \subset E$, and since it is an automorphism, $\sigma(E) = E$, which proves that the extension is normal. □

Example 5.16. Consider the same polynomial $x^3 - 2$ as in example 4.6. Recall the Hasse diagram of subfields.



This extension is Galois as it is the splitting field of the separable, irreucible polynomial $x^3 - 2$ over $\mathbb{Q}$. By what we have just proven, we should be able to construct a corresponding lattice of subgroups. Now note that since an automorphism is completely determined by its action on the generators, we have only the following possibilities for where each $\sigma \in Gal(\mathbb{Q}(\xi, \sqrt[3]{2}))$ can send the generators

$$\sigma(\xi) \in \{\xi, \xi^2\} \qquad \sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}\}$$

which gives us 6 possibilities for the automorphisms. Note that the identity automorphism corresponds to the entire field $\mathbb{Q}(\xi, \sqrt[3]{2})$ as it fixes everything, and the whole group corresponds to $\mathbb{Q}$ as we know that it is the fixed field by definition.

Consider the automorphisms τ, π, where

$$\tau(\xi) = \xi^2 \text{ and } \tau(\sqrt[3]{2}) = \sqrt[3]{2}$$

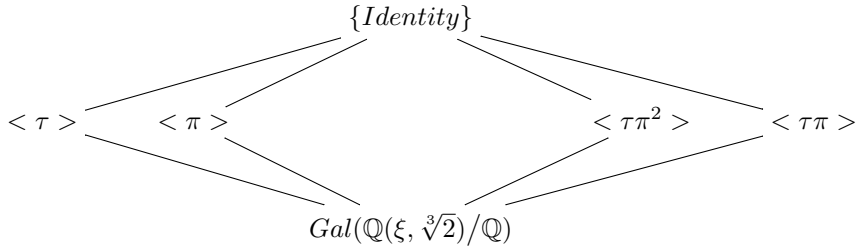
and

$$\pi(\xi) = \xi \text{ and } \pi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$$

Note that τ is an element of order 2, which fixes the subfield $\mathbb{Q}(\sqrt[3]{2})$ and π is an element of order 3 which fixes the subfield $\mathbb{Q}(\xi)$.
Now note that $\tau\pi$ is another element of order 3, and it fixes the subfield $\mathbb{Q}(\xi^2\sqrt[3]{2})$. We can check this by noticing that the field

$$\mathbb{Q}(\xi, \sqrt[3]{2}) = \{a + b\xi + c\xi^2 + d\sqrt[3]{2} + e\xi\sqrt[3]{2} + f\xi^2\sqrt[3]{2} \mid a, b, c, d, e, f \in \mathbb{Q}\}$$

and seeing that the action of $\tau\pi$ only fixes elements of $\mathbb{Q}(\xi^2\sqrt[3]{2})$. Similarly, we see that the fixed field for $\tau\pi^2$ is $\mathbb{Q}(\xi\sqrt[3]{2})$, and so we have our lattice of subgroups as follows :



The notation $< \sigma >$ means the subgroup generated by σ. Note that the lattice of subgroups is in some sense reversed as the "smallest" group is at the top of lattice, as opposed to the lattice of subfields where the largest field is at the top. This is due to the inclusion-reversing nature of the Galois correspondence. The fact that the number of subgroup matches the degree of extension shows that this extension is Galois.

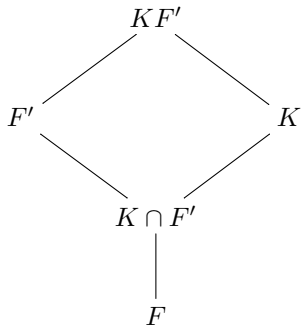
5.4. **Composite Extensions.**

Definition 5.17. Let K_1 and K_2 be fields. The composite of K_1 and K_2 is the intersection of all fields that contain K_1 and K_2 as subfields (i.e, the composite is the "smallest" field with this property), and this is denoted as K_1K_2.

Proposition 5.18. *Let K/F be a Galois extension and F'/F be any finite extension. Then the extension KF'/F' is Galois and*

$$Gal(KF'/F') \cong Gal(K/K \cap F')$$

This can be illustrated as



Proof. Since K/F is Galois, it is the splitting field of some separable polynomial $f(X)$ over F. Similarly, we can view $f(X)$ as a polynomial over F' and conclude that since KF'/F' is the splitting field of this polynomial the extension is Galois. To prove the isomorphism relation - consider the map

$$\phi : Gal(KF'/F') \to Gal(K/F)$$

given by

$$\sigma \to \sigma|_K$$

We know that this map is well-defined as by definition since $K/K \cap F'$ is a Galois hence normal extension, and so any embedding that fixes F, which is precisely what σ does, will give us an automorphism of K. Note that

$$\ker \phi = \{\sigma \in Gal(KF'/F') \mid \sigma|_K = 1\}$$

and so any element of the kernel must fix F' and K, and hence fixes their composite, which means that only the identity map is in the kernel, which proves that ϕ is an injection.

Let H be the image of ϕ on $Gal(K/F)$ and K^H denote its fixed field, which is a subfield of K containing F. Note that the restriction to F' for any element of H results in the identity, so K^H in fact contains $K \cap F'$. Note that the composite $K^H F'$ is fixed by all elements of $Gal(KF'/F')$, and so by the Galois correspondence we can conclude that $F' = K^H F'$, which implies that $K^H \subset F'$ and so $K^H \subset K \cap F'$, which proves that $K^H = K \cap F'$, and so by the Fundamental theorem we can conclude that $H = Gal(K/K \cap F')$ Thus we have that

$$\phi : Gal(KF'/F') \to Gal(K/K \cap F')$$

is an isomorphism. □

Note that a simple corollary follows from this result, due to the equality that $[KF' : K] = [F' : K \cap F']$ -

$$[KF' : F] = [KF' : F'][F' : F] = [K : K \cap F'][F' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}$$

We now prove a major result that will be useful in proving the Abel-Ruffini theorem.

Theorem 5.19. *Let K_1/F and K_2/F be Galois extensions. Then*

1. *The extension $K_1 \cap K_2/F$ is Galois.*
2. *The group $Aut(K_1K_2/F)$ is Galois and is isomorphic to the subgroup*

$$H = \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

of the direct product $Gal(K_1/F) \times Gal(K_2/F)$.

Proof. For the first part, let $p(X)$ be a polynomial over F such that a root α lies in $K_1 \cap K_2$. Since both of the extensions K_1/F and K_2/F are Galois, it follows that all the roots of $p(X)$ lie in both these extensions, and hence in their intersection. Thus, $K_1 \cap K_2/F$ is Galois, as it is a finite, normal and separable extension.
For the second part let K_1 be the splitting field of the polynomial $f_1(X)$ over F and let $f_2(x)$ be the corresponding polynomial for K_2. Then the composite K_1K_2 is the splitting field for the squarefree part of the product $f_1(X)f_2(X)$ and hence is Galois.

Consider the map

$$\phi : Gal(K_1K_2/F) \to Gal(K_1/F) \times Gal(K_2/F)$$

given by

$$\sigma \to (\sigma|_{K1}, \sigma|_{K2})$$

which is a homomorphism. The kernel is trivial as the map must be trivial on both K_1 and K_2 and hence on their composite, so ϕ is injective. Note that the image of ϕ lies in H.
For every $\sigma \in Gal(K_1/F)$ there exist exactly $|Gal(K_2/K_1 \cap K_2|$ elements $\tau \in Gal(K_2/F)$ such that $\tau|_{K_1 \cap K_2} = \sigma|_{K_1 \cap K_2}$ This implies that

$$|H| = |Gal(K_1/F)||Gal(K_2/K_1 \cap K_2)|$$

which allows us to conclude that

$$|H| = \frac{|Gal(K_1/F)||Gal(K_2/F)|}{|Gal(K_1 \cap K_2/F)|}$$

and by the corollary, we can conclude that $|H| = |Gal(K_1K_2/F)|$, which establishes the isomorphism. □

5.5. **Kummer Theory and Radical Extensions.**

Definition 5.20. Let E/F be a finite separable extension. Then E is contained in an extension K which is Galois over F, and which is minimal in the sense that any other such extension has K as a subfield. Then K is called the Galois Closure of E over F.

Definition 5.21. The extension K/F is said to be cyclic if it is Galois with a cyclic Galois group.

For this section, we assume that all fields are of Characteristic 0.

Proposition 5.22. *Let F be a field which contains the n^{th} roots of unity. Then the extension $F(\sqrt[n]{a})$ for $a \in F$ is a cyclic extension over F of degree dividing n.*

Proof. The extension $F(\sqrt[n]{a})$ is Galois over F if F contains the n^{th} roots of unity as it is the splitting field of the polynomial $x^n - a$. For any $\sigma \in Gal(F(\sqrt[n]{a})/F)$, we have that $\sigma(F(\sqrt[n]{a}))$ is another root of the polynomial, and so $\sigma(F(\sqrt[n]{a})) = \xi_\sigma F(\sqrt[n]{a})$, where ξ_σ is some n^{th} root of unity.

Consider the map

$$Gal(F(\sqrt[n]{a})/F) \to \mu_n$$

given by

$$\sigma \to \xi_\sigma$$

where μ_n is the group of the n^{th} roots of unity. Note that

$$\sigma_a\sigma_b = \xi_a\xi_b = \xi_{ab} = \sigma_{ab}$$

and so this map is a homomorphism. Also, the kernel of this map is precisely the identity map as it fixes $\sqrt[n]{a}$, and so this map is an injection. □

We now want to characterise these radical extensions. Consider a cyclic extension K/F of degree n over a field F containing the n^{th} roots of unity. Let σ be the generator for $Gal(K/F)$.

Definition 5.23. For $\alpha \in K$ and any n^{th} root of unity ξ, define the *Lagrange Resolvent* $(\alpha, \xi) \in K$ by

$$(\alpha, \xi) = \alpha + \xi\sigma(\alpha) + \xi^2\sigma^2(\alpha) + \ldots + \xi^{n-1}\sigma^{n-1}(\alpha)$$

The resolvent is important in this case as if we apply σ to the above definition, we get

$$\begin{aligned}\sigma(\alpha, \xi) &= \sigma(\alpha) + \xi\sigma^2(\alpha) + \ldots + \xi^{n-1}\sigma^n(\alpha) \\ &= \sigma(\alpha) + \xi\sigma^2(\alpha) + \ldots + \xi^{-1}\alpha \\ &= \xi^{-1}(\alpha + \ldots + \xi^{n-1}\sigma^{n-1}(\alpha)) \\ &= \xi^{-1}(\alpha, \xi)\end{aligned}$$

and so

$$\sigma(\alpha, \xi)^n = (\xi^{-1})^n(\alpha, \xi)^n = (\alpha, \xi)^n$$

and so $(\alpha, \xi)^n$ is fixed by all elements of $Gal(K/F)$ which means that it lies in F.

From the linear independence of characters, and the fact that σ is chosen to be a generator of $Gal(K/F)$, we know that there exists some $\alpha \in K$ such that $(\alpha, \xi) \neq 0$. Thus we can conclude that for this choice of α, $\sigma^i(\alpha)$ does not fix (α, ξ) for any $i \in [n]$, and so the resolvent cannot lie in any proper subfield of K, which implies that $K = F((\alpha, \xi))$, so we have proven that any cylic extension of degree n over a field F which contains the n^{th} roots of unity is of the form $F(\sqrt[n]{a})$ for some $a \in F$.

Definition 5.24. An element α that is algebraic over F can be expressed by radicals if α is an element of a field K which can be obtained by a succession of simple radical extensions

$$F = K_0 \subset K_1 \subset \ldots \subset K_i \subset \ldots \subset K_q = F$$

where each $K_{i+1} = K_i(\sqrt[n]{a_i})$ for some $a_i \in K_i$. A polynomial $f(x)$ over F can be solved by radicals if all its roots can be solved for in terms of radicals.

Lemma 5.25. *If α is contained in a root extension of K as outlined above, then α is contained in a root extension which is Galois over F and where each extension K_{i+1}/K_i is cyclic.*

Proof. Let M be the Galois closure of K over F. Then for any $\sigma \in Gal(M/F)$ we have the chain of subfields

$$\sigma(F) = \sigma(K_0) \subset \sigma(K_1) \subset \ldots \subset \sigma(K_q) = \sigma(K)$$

where each $\sigma(K_{i+1})/\sigma(K_i)$ is a simple radical extension as it is generated by the element $\sigma(\sqrt[n_i]{a_i})$. Since the composite of two root extensions is a root extension, it follows that the composite of all $\sigma(K)$ for all $\sigma \in Gal(L/F)$ is also a root extension. Since the composite of all these fields is exactly L, we can conclude that α is contained in a root extension.

We now make use of Kummer Theory and adjoin to F the n_i^{th} roots of unity for all the roots $\sqrt[n_i]{a_i}$ of the simple radical extensions in the Galois root extensions of K/F to obtain the field F', and we get the composite extensions

$$F' = K_0F \subset K_1F \subset \ldots \subset K_qF = KF'$$

Note that $F'K/F$ is a Galois extension as it is the composition of Galois extensions. Each extension $F'K_{i+1}/F'K_i$ is a simple radical extension, and since the base field contains the appropriate roots of unity, by the previous proposition, each successive extension is cyclic. Therefore $F'K/F$ is a Galois extension with the required properties. □

5.6. **Abel-Ruffini Theorem.**

Theorem 5.26. *A polynomial $f(x)$ is solvable by radicals if and only if its Galois group is solvable.*

Proof. This theorem is the crux of Galois's proof of the Abel-Ruffini theorem.

($\Longrightarrow$) Let the polynomial $f(x)$ be solvable by radicals. For each root α_i of f, we know by 5.21 that an extension with the given properties exists. We take the composition of each of these fields to obtain another field L over which the polynomial is Galois and contains all the roots of the polynomial. Let G_i be the subgroups corresponding to the K_i of the field. Then since

$$Gal(K_{i+1}/K_i) = G_{i+1}/G_i$$

we have that our group G is solvable, since each of the quotients are cyclic and thus abelian.

Suppose that f has Galois group G which is solvable. Then we obtain another chain of subfields where each K_i corresponds to the group fixed by the subgroup G_i

$$F = K_0 \subset K_1 \subset \ldots \subset K_q = K$$

where each extension K_{i+1}/K_i are cyclic if K is cyclic by the definition of solvable groups and the Galois Correspondence. We then adjoin the n_i^{th} roots of unity to F to obtain the field F' and then compose them to the chain of subfields to obtain

$$F' = F'K_0 \subset \ldots \subset F'K_q = F'K$$

and we still have $F'K_{i+1}/F'K_i$ as a cyclic extension of degree dividing n_i. We now have a chain of extensions where the base field contains the required roots of unity, so each extension is a simple radical extension by the proof of the result following the definition of Lagrange resolvents, which implies that the polynomial is solvable by radicals. □

The Abel-Ruffini Theorem now follows easily -

Theorem 5.27 (**Abel-Ruffini**). *The general polynomial of degree n is not solvable by radicals for $n \geq 5$.*

Proof. Recall that the general polynomial

$$f(x) = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$$

has Galois group S_n, and it is a well-known fact that for $n \geq 5$, S_n is not solvable, and so the general polynomial is not solvable by radicals. □

6. Some Computations using Galois Theory

We call a rational function $f(x_1, x_2, \ldots, x_n)$ symmetric if under all permutations of its inputs, the value of the expression remains unchanged.

Note that the coefficients of the general polynomial

$$(x - x_1)(x - x_2)\ldots(x - x_n)$$

remain unchanged upon any permutation of the roots, and we can actually obtain a whole class of expressions for these coefficients in terms of the roots of the polynomials given by

$$\begin{aligned} s_1 &= x_1 + \ldots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + x_2x_4 + \ldots x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2\ldots x_n \end{aligned}$$

which are all symmetric. We take for granted the most important theorem regarding these symmetric functions - that any symmetric function in $x_1, \ldots, x_n$ can in fact be represented as a rational function in $s_1, \ldots, s_n$. We are interested in giving a condition for a polynomial of degree 4 to have Galois group S_4 - i.e any root permutation is contained in the Galois group of that polynomial.

Definition 6.1. If a polynomial $f(X)$ over F factors over its splitting field as

$$f(X) = (X - r_1)\ldots(X - r_n)$$

then we define the discriminant of the polynomial as

$$disc(f) = \prod_{i<j}(r_j - r_i)$$

Notice that the discriminant is a symmetric function. We take for granted the following theorem -

Theorem 6.2. *The Galois group of a polynomial $f(X)$ over a field F is a subgroup of A_n if any only if its discriminant is a perfect square.*

Now consider a monic irreducible polynomial $f(X) = X^4 + aX^3 + bX^2 + cX + d$ over a field F. We can write the polynomial in terms of its roots r_1, r_2, r_3, r_4 as

$$f(X) = X^4 + aX^3 + bX^2 + cX + d = (X - r_1)(X - r_2)(X - r_3)(X - r_4)$$

We want to create an expression that under all root permutations only takes on 3 values, so that we can associate a cubic polynomial with that expression.

$$x_1x_2 + x_3x_4$$

is such an expression, as under all 24 permutations of S_4, we see that the expression only takes on the values

$$\begin{aligned} &x_1x_2 + x_3x_4 \\ &x_1x_3 + x_2x_4 \\ &x_1x_4 + x_2x_3 \end{aligned}$$

and so the cubic polynomial

$$(X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3))$$

is symmetric and thus has all its coefficients in F by the Galois Correspondence. It is natural to ask what the coefficients of the polynomial are when we equate the coefficients to $X^3 + AX^2 + BX + C$. Equating coefficients we see that

$$A = -(r_1r_2 + r_3r_4 + r_1r_3 + r_2r_4 + r_1r_4 + r_3r_2) = -b$$

where b is the coefficient of the polynomial $f(X)$ that we defined above. The other coefficients are messier to compute so we skip working for the sake of brevity, but we see that

$$B = ac - 4d$$

and

$$C = -(a^2d + c^2 - 4bd)$$

where a, b, c, d are as defined in our original polynomial $f(X)$. This polynomial is called the cubic resolvent of $f(X)$ and is denoted by $R_3(X)$. There is a very important relation between these two polynomials -

Theorem 6.3. *A quartic polynomial $f(X)$ and its cubic resolvent have the same discriminant.*

Proof. Note that the difference between any 2 roots of the cubic resolvent are of the form

$$(r_1r_2 + r_3r_4) - (r_1r_3 + r_2r_4) = (r_1 - r_4)(r_2 - r_3)$$

and doing the same for the other two expressions we see that the determinants do match. □

We now have a criterion to test if the Galois group of a given quartic is S_4 or A_4(it could be other transitive subgroups of S_4 but we limit our exploration to these 2 cases).

Theorem 6.4. *If the discriminant of our quartic is not a square and its cubic resolvent is irreducible over F, then the Galois group of the polynomial is S_4. If the discriminant of our quartic is a square and its cubic resolvent is irreducible over F, then the Galois group of the polynomial is A_4.*

Proof. In the first case, since the discriminant is not a square, $G \not\leq A_4$ by theorem 6.2. Since the cubic resolvent is irreducible, adjoining a root of it generates a degree 3 extension over F, and thus by the Galois correspondence implies that the order of the subgroup is divisible by 3. The irreducibility of the original polynomial implies that the order of the group is also divisible by 4. This means that the Galois group is either A_4 or S_4, and so S_4 is the Galois group.

For the second case, Since the discriminant is a perfect square, we know that the Galois group $G \leq A_4$, and by the same argument as above we can narrow the choices of the Galois group to be S_4 or A_4, leaving A_4 as the only possible choice. □

Acknowledgments

It is a pleasure to thank my mentor Gal Porat for his patience, encouragement and help in tackling some of the more involved proofs of Galois Theory. I would also like to thank Prof. May for organising and giving me the opportunity to participate and learn a lot of interesting Mathematics in this REU - it made for an extremely fun summer.

References

[1] David S. Dummit, Richard M. Foote. Abstract Algebra. *Wiley*. 1999.
[2] Serge Lang. Algebra. *Springer-Verlag*. 2002.
[3] Keith Conrad. Galois Groups of Cubics and Quartics (Not in Characteristic 2). https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf