AN INTRODUCTION TO GALOIS THEORY AND THE ABEL-RUFFINI THEOREM

DHRUV KOHLI

Abstract. This paper sets out to explain Galois theory and at the end prove the Abel-Ruffini Theorem, which was partially proved in 1799 by Paolo Ruffini and then completed by Niels Henrik Abel in 1823. Évariste Galois independently proved the theorem, with his proof published posthumously in 1846. This paper will first introduce key concepts of algebra, then build upon these to introduce Galois Theory and its extensions. Finally, we conclude by proving the Abel-Ruffini Theorem using previously established mathematical concepts.

Contents

1. Introduction

This paper culminates by proving the Abel-Ruffini Theorem with a few side quests on the way.

Theorem 1.1. *There is no solution in radicals to general polynomial equations of degree five or greater with arbitrary coefficients.*

For there to be a solution in radicals for a general polynomial equation of degree n, there needs to be an explicit formula for the roots of the polynomial using the operations $+, -, /, \times$, and $\sqrt[n]{}$. An example of this would be the quadratic equation that finds the roots of a second-degree polynomial. The Abel-Ruffini Theorem proves that there is no explicit formula using our basic operations to find the roots of a polynomial with a degree of 5 or greater.
Before we begin, I suggest the reader have a good understanding of the basics of group theory, fields, the Fundamental Theorem of Symmetric Polynomials, polynomial properties, and roots of unity.

2. Contextual Definitions

Definition 2.1. A polynomial $p \in F(x_1, ..., x_n)$ is symmetric if for every permutation $(x_{r(1)}, ..., x_{r(n)})$ of the variables $(x_1, ..., x_n)$, we have

$$p(x_{r(1)}, ..., x_{r(n)}) = p(x_1, ..., x_n).$$

Definition 2.2. A subgroup N of a group G is normal in G if for all $n \in N$ and $g \in G$, we have $gng^{-1} \in N$.

Definition 2.3. A group G is defined as solvable if it has a subnormal series whose factor groups are all abelian. If there are subgroups

$$1 = G_0 \triangleleft G_1 \triangleleft ... \triangleleft G_k = G$$

such that for all $j = 1, 2, ...k$, G_{j-1} is normal in G_j and the quotients G_j/G_{j-1} are all abelian, then G is solvable.

Definition 2.4. The degree of a field extension E/F is the dimension of E as a vector space over F. If E/F is finite, then $[E : F]$ denotes the degree of E/F.

Definition 2.5. A polynomial $f \in F[x]$ is irreducible over F if it is nonconstant and cannot be factored into polynomials of strictly lower degree with coefficients in F.

Definition 2.6. A characteristic of a ring R is the smallest number of the ring's multiplicative identity that it takes to add together to get to the additive identity. If no such number exists, then the ring has characteristic 0. An example of this is that in $5\mathbb{Z}$it take 5 ones to get back to 0, and so it is characteristic 5, written $char(5\mathbb{Z}) = 5$.

Definition 2.7. An nth root of unity z, with $n \in \mathbb{N}$, is a number z such that $z^n = 1$ in a given field F that we are working in. An nth root is primitive if for any $m \in \mathbb{N}$ and $m < n$, $z^m \neq 1$.

3. Finite Extension Fields and Splitting Fields

Definition 3.1. Let F be a field. An extension field E of F is a field such that $F \subset E$. We call F the ground field with respect to E. This relationship is denoted by E/F.

Definition 3.2. Let E/F be a field extension, then E may be considered as a vector space over F, and the dimension of this vector space is called the field extension and is denoted by $[E : F]$.

Example 3.3. The complex numbers, $\mathbb{C}$, is an extension field of the real numbers, $\mathbb{R}$, with $\mathbb{R}(i) = \mathbb{C}$. This is due to all elements of $\mathbb{C}$ being of the form $a + bi$ with $a, b \in \mathbb{R}$. The degree of the field extension is 2, written as $[E : F] = 2$.

Definition 3.4. Let F be a field and S its basis. For an element $a \notin F$, we create a basis $B = S \cup a$ and denote the field with basis B as $F(a)$. For example $\mathbb{R}(i) = \mathbb{C}$ as the basis of $\mathbb{R}$ is 1 and that of of $\mathbb{C}$ is $\{1, i\}$.

Definition 3.5. Let F be a field. The set of all polynomials of coefficients in F is denoted $F[X]$.

Definition 3.6. An element $\alpha \in E$ is algebraic over a field F if it is the root of some non-zero polynomial over F. The extension E/F is algebraic if all elements of E are algebraic over F.

Example 3.7. For example, we have $\sqrt{5} \notin \mathbb{Q}$ as algebraic over $\mathbb{Q}$ since it is a root of the polynomial $g(x) = x^2 - 5$ who's coefficients are all rational numbers.

Definition 3.8. For a field F and its extension E, we have E/F as an algebraic extension if every element of E is algebraic over F. For example, we have $\mathbb{C}/\mathbb{R}$ as an algebraic extension since all polynomials with coefficients in $\mathbb{R}$ of degree n will always have all n of their roots in $\mathbb{C}$ but not always in $\mathbb{R}$. A such polynomial is $f(x) = x^2 + 1$, with roots i and $-i$.

Definition 3.9. For a field F and its extension E, we call E/F a transcendental extension if it is not an algebraic extension. We thus have an element in E, δ, such that there are no polynomial with coefficients in F such that δ is a root of such a polynomial. We call δ a transcendental element of E/F.

Proposition 3.10. *Let α be algebraic over F. We know there exists a polynomial $p(x)$ such that $p(x)$ is the polynomial of lowest degree with α as a root. A polynomial has α as a root if and only if it is divisible by $p(x)$.*

Proof. We will first show that if a polynomial $f(x)$ has α as a root, it is divisible by $p(x)$ through a proof by contradiction. Let a polynomial $f(x)$ have α as a root but is not a multiple of $p(x)$. We can then write $f(x)$ as $f(x) = p(x) \cdot q(x) + r(x)$ with $q(x)$ and $r(x)$ non-zero polynomials and $r(x)$ of lower degree than $p(x)$. We then know $f(\alpha) = p(\alpha) \cdot q(\alpha) + r(\alpha) = 0 \implies r(\alpha) = 0$. This contradicts $p(x)$ being the minimal polynomial with α as a root. We can thus conclude that $f(x)$ must this be divisible by $p(x)$.

Now showing the other direction, we let a polynomial $f(x)$ be divisible by $p(x)$ such that $f(x) = p(x) \cdot a(x)$ with $a(x)$ a polynomial. Then $f(\alpha) = p(\alpha) \cdot a(\alpha) = 0 \cdot a(\alpha) = 0$ so α is a root of $f(x)$. □

Definition 3.11. Let E/F be a field extension, and α an element of E. The element α has a minimal polynomial when α is algebraic over F. Then the minimal polynomial of α is defined as the polynomial of least degree among all polynomials in $F[x]$ having α as a root.

Theorem 3.12. *An element α is algebraic over F if and only if $[F(\alpha) : F]$ is finite. Using an abuse of notation in the future, this will be said as $F(\alpha)/F$ is finite.*

Proof. We first show that if α is algebraic over F then $[F(\alpha) : F]$ is finite. We know that if α is algebraic over F, then there exists a lowest degree polynomial that has α as a root. Let the degree of this polynomial be n. We can then use the elements $1, \alpha, \cdots, \alpha^{n-1}$ to form a basis for $F(\alpha)$ over F, and so $[F(\alpha) : F] = n$ and thus $[F(\alpha) : F]$ is finite.

We will now show that if $[F(\alpha) : F]$ is finite then α is algebraic over F. Now let $[F(\alpha) : F] = n$. There exist $b_0, ..., b_n$ with $b_i \in F$ and they are not all equal to 0. Notice that we can have

$$b_0 + b_1\alpha + ... + b_n\alpha^n = 0$$

since $1, \alpha, ..., \alpha^n$ are linearly dependent over $F(\alpha)$. It then follows that we can construct a polynomial $g(x)$ of degree n, such that $g(\alpha) = 0$. We have thus found a non-zero polynomial which has α as a root and thus α is algebraic over F. □

Corollary 3.13. *If $[E : F]$ is finite, then E/F is algebraic (every element of E is algebraic over F).*

Proof. Let us take an arbitrary $\alpha \in E$ and set $[E : F] = n$ for some finite n. We have

$$F(\alpha) \subset E \implies [F(\alpha) : F] \leq [E : F] = n.$$

It this follows from the previous theorem that since $[F(\alpha) : F]$ is finite, α is algebraic over F. Due to our arbitrary selection for α, this is the case for all $\alpha \in E$ and so E/F is an algebraic extension. □

Theorem 3.14 (Tower Law)**.** *Given three fields, K, L, and M such that $K \subset L \subset M$, if L/K and M/L are both finite then M/K is finite. In this case we have*

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

Proof. We shall first show that if L/K and M/L are both finite then M/K is finite. Let us have $[M : L] = l$ and $[L : K] = k$ for some finite l and k in $\mathbb{N}$. We can then find a basis $u_1, ..., u_k$ of L over K and a basis $w_1, ..., w_l$ of M over L. We will now show that the elements of the form $u_m w_n$, for m ranging through $1, 2, ..., k$ and n ranging through $1, 2, ..., l$, of which there are $l \cdot k$ many, form a basis of M/K.
If x is an element of M then since the w_n form a basis for M over L, we can find elements a_i in L such that:

$$x = \sum_{n=1}^{l} a_n w_n.$$

Furthermore, since the u_m form a basis for L over K, we can find elements $b_{m,n}$ in K such that for each n,

$$a_n = \sum_{m=1}^{k} b_{m,n} u_m.$$

Putting this together we have:

$$x = \sum_{n=1}^{l} (\sum_{m=1}^{k} b_{m,n} u_m) w_n = \sum_{n=1}^{l} \sum_{m=1}^{k} b_{m,n} (u_m w_n).$$

Thus, x is a linear combination of coefficients from K and the multiplication of the other bases, thus they span M over K.
We now check for linear independence. We have

$$0 = \sum_{n=1}^{l} \sum_{m=1}^{k} b_{m,n} (u_m w_n) = \sum_{n=1}^{l} (\sum_{m=1}^{k} b_{m,n} u_m) w_n$$

and since the w_n are linearly independent over L, we must have

$$\sum_{m=1}^{k} b_{m,n} u_m = 0$$

for each n, Since the u_m are linearly independent the only solution is for all $b_{m.n} = 0$ and thus the elements $u_m w_n$ are linearly independent over K. In conclusion these elements will form a basis for M/K and so we must have

$$[M : K] = l \cdot k = [M : L][L : K].$$

and so if L/K and M/L are both finite then M/K is finite.

□

Definition 3.15. An extension field E of F is called the splitting field for a polynomial p over F if p factors into its linear factors over E, and E is the smallest field with such a property. We can thus write

$$p(x) = c \cdot \prod_{i=1}^{deg(p)} (x - \alpha_i)$$

with $c \in F$, $(x - a_i) \in E[x]$ and a_i not necessarily distinct roots of $p(x)$.

Lemma 3.16. *Let F be a field. The following are then equivalent:*

1) The field F is algebraically closed.
2) Every irreducible polynomial over F is linear.
3) Every non-constant polynomial over F has at least one root.
4) Every non-constant polynomial over F is a product of linear factors.

Proof.

$1 \implies 2$ If F is algebraically closed, we want to show that every irreducible polynomial over F must be linear. We know that if there is an irreducible polynomial of degree greater than 1, it will generate a nontrivial finite field extension. By this logic, we can thus conclude that every polynomial over F is linear.

$2 \implies 3$ If every irreducible polynomial over F is linear, then every irreducible polynomial must have a root. We can factor any non-constant polynomial over F into linear polynomials and so they must have at least one root.

$3 \implies 4$ Let every non-constant polynomial have at least one root in F and $p \in F[X]$ be a non-constant polynomial. If $p(\alpha) = 0$, with α as a root in F, then we know that $p(x) = (x - a)q(x)$ for some polynomial $q \in F[X]$. We can generalize this idea by induction on the degree of a polynomial that any polynomial of degree ≥ 1 can be written as a product of $c(x - \alpha_i)$ with the α_i as roots and c a constant in F.

$4 \implies 1$ Let every non-constant polynomial over F be a product of linear factors and E/F an algebraic extension. We then know that all sub-extensions $F(\alpha_i)/F$ of E are simply F and so we have $F = E$ and thus F is algebraically closed. □

Definition 3.17. Let F be a field and E an extension field of F:

1) We say an irreducible polynomial p over F is separable if it relatively prime to its derivative p'.
2) For $\alpha \in E$ algebraic over F, α is said to be separable over F if its minimal polynomial is separable over F.
3) If E is an algebraic field extension of F, E is said to be separable over F if every element of E is seperable over F.

Corollary 3.18. *Let F be a field. An irreducible polynomial p over F is separable if and only if all roots of p are distinct in the algebraic closure of F, E.*

Proof. Suppose p and its derivative p' have a common root $\alpha \in E$, then $p = (x-\alpha)q$ for some polynomial q. We then can write p' as: $p' = q + (x-\alpha)q'$. We then also know α is a root for q, and so this implies that p has a repeated root α. We can thus conclude if p and p' are relatively prime, then all roots of p are distinct.
Conversely, if p has a repeated root α, then $(x-\alpha)^2$ divides p and so $(x-\alpha)$ also divides p' making α a root of both p' and p. □

Corollary 3.19. *A polynomial $p(x)$ in $F[X]$ is separable if it has no multiple roots in any field containing F. An algebraic field extension E of F is separable if the minimal polynomial over every element in E over F is separable.*

Proof. For the first part of the statement, this follows directly from the previous corollary as any elements of F will be in its extensions, and so a repeated root will remain. Thus for a polynomial $p(x)$ in $F[X]$ to be separable it must have no multiple roots in any field containing F.
For the second part of the statement, we know that a field extension E of F is separable if each of its elements is separable over F. In addition, since it is algebraic we know that for each element α in E there is a polynomial in $F[X]$ with α as a root and so a minimal polynomial exists. Furthermore, we know that an element is said to be separable if its minimal polynomial is separable over F is separable. Using the first statement and the given definitions, it then follows that an algebraic field extension E of F is separable if the minimal polynomial over every element in E over F is separable. □

Theorem 3.20. *Let $f(x)$ be any polynomial of degree n over F and $\overline{f}(x)$ the corresponding polynomial over an isomorphic field $\overline{F}$. If E is the splitting field of $f(x)$ over F and $\overline{E}$ is the splitting field of $\overline{f}(x)$ over $\overline{F}$, then we can extend the isomorphism between F and $\overline{F}$ to E and $\overline{E}$.*

Proof. Let f have q roots in F, then we can factor f as such:

$$f(x) = c(x-\alpha_1)(x-\alpha_2)...(x-\alpha_q)P_1(x)P_2(x)...P_s(x),$$

with each P_i being an irreducible factor in F of degree greater than 1. Since F and $\overline{F}$ are isomorphic we can factorize $\overline{f}$ similarly over $\overline{F}$:

$$\overline{f}(x) = \overline{c}(x-\overline{\alpha}_1)(x-\overline{\alpha}_2)...(x-\overline{\alpha}_q)\overline{P}_1(x)\overline{P}_2(x)...\overline{P}_s(x).$$

We shall use a proof by induction.

Let us first look at the case of F having all roots of f with $q = n$. It then follows that $E = F$ is the splitting field of $f(x)$, meaning that $\overline{E} = \overline{F}$ is also the splitting field of $\overline{f}(x)$, and so the isomorphism is extended to E and $\overline{E}$.

We will now prove that if this theorem is true for $q+1$ linear factors, it is also true for q linear factors, giving us our induction. Let the theorem be true for $q+1$ linear factors and $f(x)$ has q linear factors in F. We have $P_1(x)$ that splits in E and $\overline{P}_1(x)$ that splits in $\overline{E}$ which have respective roots α_{q+1} and $\overline{\alpha}_{q+1}$. We can then construct the extension fields by adjoining each root to the base field and extend the isomorphism of F and $\overline{F}$ to these fields by a transformation that sends

α_{q+1} to $\overline{\alpha}_{q+1}$ and vice-versa. Since the isomorphism of $F(\alpha_{q+1})$ and $\overline{F}(\overline{\alpha}_{q+1})$ also contains that of F and $\overline{F}$, the mapping between $f(x)$ and $\overline{f}(x)$ remains. We now have $F(\alpha_{q+1})$ and $\overline{F}(\overline{\alpha}_{q+1})$ as ground fields. We can now factor $f(x)$ and $\overline{f}(x)$ once again, but will obtain one new linear factor each, $(x-\alpha_{q+1})$ and $(x-\overline{\alpha}_{q+1})$ respectively, in their respective new ground fields. We thus see that $f(x)$ possesses at least $q+1$ factors in $F(\alpha_{q+1})$. The splitting field of $f(x)$ over $F(\alpha_{q+1})$ will be E since it does not split in any other smaller field. The same ideas can be extended to $\overline{f}(x)$ and so we can conclude the isomorphism between $F(\alpha_{q+1})$ and $\overline{F}(\overline{\alpha}_{q+1})$ can be extended to E and $\overline{E}$ which are the respective splitting fields of $f(x)$ and $\overline{f}(x)$. We have thus finished our proof by induction.

□

4. Automorphisms

Definition 4.1. An automorphism of a field F is a map $\sigma : F \to F$ that preserves the field operations. The set of all automorphisms of F, denoted $\mathcal{A}ut(F)$, forms a group. This is otherwise thought of an isomorphism from F to itself.

Definition 4.2. An automorphism, σ, of E fixes a field F if for all $\alpha \in F, \sigma(\alpha) = \alpha$. The set of all automorphisms of E that fix F is denoted $\mathcal{A}ut_F(E)$.

Proposition 4.3. *Let E/F be a field extension. Then $\mathcal{A}ut(E)$ under composition forms a group of which $\mathcal{A}ut_F(E)$ is a subgroup.*

Proof. We first have an identity which is the identity map as it is an automorphism, as for any ϕ which is an automorphism, $Id \circ \phi = \phi \circ Id = \phi$. Now to show that we have closure.

The composition of two bijective maps is also a bijective map, further if both maps have the same codomain and domain in common (G), the composition of the maps will also maintain these codomains and domains, so we must have a bijective map to itself. Now to show it is a homomorphism, with the automorphisms ϕ_1 and ϕ_2, we have:

$$\begin{aligned}(\phi_1 \circ \phi_2)(ab) &= \phi_1(\phi_2(ab)) = \phi_1(\phi_2(a)\phi_2(b)) \\ &= \phi_1(\phi_2(a))\phi_1(\phi_2(b)) = (\phi_1 \circ \phi_2)(a)(\phi_1 \circ \phi_2)(b).\end{aligned}$$

This is the case since $\phi_2(x) \in G$ as it is an automorphism. We thus have an isomorphism which maps to itself and so an automorphism. We thus have closure under composition.

Any element of this group has an inverse which will also be an automorphism since the domain and codomain are the same and the map is bijective, so the inverse map is also a bijective map and will exist. It will also be a homomorphism as it will maintain the properties due to being the inverse. Since we then have an isomorphism which maps from itself to itself as the codomoain and domain are the same, it will also be an automorphism. Finally, to show associativity we have the automorphisns f,g, and h with:

$$(f \circ (g \circ h))(x) = f(g(h(x))) = ((f \circ g) \circ h)(x).$$

We can thus conclude set of automorphisms forms a group under composition.

Let us have any two automorphisms in $\mathcal{A}ut(E)$, σ and τ that fix F. It follows that $\sigma \circ \tau$ will fix F and furthermore so will σ^{-1}. The identity will necessarily fix F as well, and we will have associativity as automorphisms are associative as shown earlier. We thus conclude that $\mathcal{A}ut_F(E)$ meets the conditions of being a subgroup of $\mathcal{A}ut(E)$. □

Proposition 4.4. *Let a polynomial $f(x)$ over F possess an irreducible factor $p(x)$ with distinct roots $\alpha_1, ..., \alpha_n \in E, (n \geq 2)$. If we switch any α_i and α_j by transformation, we obtain an isomorphism mapping $F(\alpha_i)$ to $F(\alpha_j)$ and leaving F fixed. This isomorphism can be extended to give an automorphism of E.*

Lemma 4.5. *Let us factor any polynomial $f(x)$ of degree n into irreducible polynomials over F which has an arbitrary q distinct roots in F, so*

$$f(x) = c(x - \alpha_1)(x - \alpha_2)...(x - \alpha_q)P_1(x)P_2(x)...P_s(x),$$

with P_i as factors of degree greater than 1. If E is the splitting field of $f(x)$ over F and all $P_i(x)$ have only distinct roots in E, then no elements other than those of F remain fixed in $\mathcal{A}ut_F(E)$.

Proof. To prove this we shall use a proof by induction.

For $q = n$ we then have $F = E$ and so our lemma holds.
We will now show that if the theorem is true for $q + 1$ roots, then it is also true for q roots.

We must first show that $F(\alpha_{q+1})$ meets the criterion for the theorem. Assume the theorem is true for $q + 1$ linear factors, so we can extend our field F to $F(\alpha_{q+1})$ since α_{q+1} is a root of a polynomial. We will now factorize $f(x)$ in the field $F(\alpha_{q+1})$, which gives

$$f(x) = c(x - \alpha_1)...(x - \alpha_{q+1})(x - \beta_1)...(x - \beta_s)Q_1(x)...Q_u(x).$$

Within this, β_i are new roots found in our extension and Q_k are nonlinear irreducible polynomials that are factors of the $P_i(x)$ of the previous factorization. We know E is the splitting field of $f(x)$ over $F(\alpha_{q+1})$ and since $Q_k(x)$ is a factor of $P_i(x)$ the splitting of $Q_k(x)$ in E contains distinct roots since no factor appears twice in the splitting of $P_i(x)$ of which $Q_k(x)$ is a factor. Due to the criteria being met we know that if $a \in E$ is fixed by $\mathcal{A}ut_{F(\alpha_{q+1})}(E)$ then $a \in F(\alpha_{q+1})$.

Finally, we shall do the inductive step of the theorem. Suppose $a \in \mathcal{A}ut_F(E)$, then we know that a is also fixed under all automorphisms that leave the elements of $F(\alpha_{q+1})$ fixed, and so we have $a \in F(\alpha_{q+1})$. Let us create the polynomial $P_1(x)$ of degree m, and since $a \in F(\alpha_{q+1})$ we can write it as

$$a = c_0 + c_1\alpha_{q+1} + ... + c_{m-1}\alpha_{q+1}^{m-1}$$

for $c_l \in F$ and α_i as the t roots of $P_1(x)$. We also know that there are no repeated factors of $P_1(x)$in E and so we have:

$$P_1(x) = (x - \alpha_{q+1})(x - \alpha_{q+2})...(x - \alpha_{q+m}).$$

By proposition 4.4, the m transformations between α_{q+1} and α_{q+j} provide automorphisms which leave F fixed. However, we know that a is fixed under all these automorphisms and thus can be written in m different manners (the α_{q+1} gets switched with a α_{q+j}). We can thus create a polynomial

$$h(x) = (c_0 - a) + c_1x + ... + c_{m-1}x^{m-1}$$

of degree $m-1$ with m distinct roots, which is only possible for $h(x)=0$. Thus, all the coefficients of the polynomial are equal to 0 and so we know $a=c_0$ and so we must have $a \in F$ and thus all fixed elements of $\mathcal{A}ut_F(E)$ are in F.

□

Theorem 4.6. *Let U be a field containing:*

1) The ground field, F.

2) The splitting field of any polynomial defined over F, E.

3) An intermediate field between E and F, K

4) An extension field of F which is isomorphic to K in a mapping such that F remains fixed, K'.

We then have $K' \subset E$ and the isomorphism mapping K to K' is an automorphism of E.

Proof. Let us first denote our mapping from K to K' that leaves F fixed as ϕ. Let E be the splitting field of the polynomial $f(x)$ over F such that

$$E = F(\alpha_1, ..., \alpha_n),$$

with α_i as a root of $f(x)$. Since $F \subset K \subset E$, E is also the splitting field of $f(x)$ over K. We also know that $f(x)$ is a polynomial in K' and the splitting field of $f(x)$ over K' is the field E', with

$$E' = F(\alpha_1', ..., \alpha_n').$$

Furthermore, by theorem 3.14, we know the isomorphism mapping K to K' can be extended to E and E', so $\phi(E) = E'$. Let us denote any element of K as u, and $\phi(u) = u'$. By definition $u \in E$ so u is of the form

$$u = g(\alpha_1, ..., \alpha_n),$$

with ϕ a polynomial with coefficients in F. Similarly, we can express u' as

$$u' = g(\alpha_1', ..., \alpha_n'),$$

with the $\alpha_i' = \phi(\alpha_i)$. Since we have a finite field extension of the fixed field F through the adjoinment of the α_i', by Corollary 3.7, they must also be roots of $f(x)$ and thus our original α_i in a different permutation. Thus, we see that for any

$$u' \in K', u' \in E \implies K' \subset E,$$

and $E = E'$ since there can only be one splitting field of $f(x)$ over K'. We can thus conclude that our isomorphism is an automorphism of E and so $\phi \in \mathcal{A}ut(E)$.

□

5. Linear Independence of Characters

Definition 5.1. A primitive element of a finite field F_q of order q is a generator of the multiplicative group of the field.

Definition 5.2. For an abelian group G, a character of G is a group homomorphism from G to the multiplicative group of a field F:

$$\chi : G \to F^\times.$$

Definition 5.3. The characters $\chi_1, ..., \chi_n$, with $\chi_i : G \to F^\times$, of a group G are said to be linearly independent over F if they are linearly independent as functions on G. This means that if we have $a_1\chi_1(g) + ... + a_n\chi_n(g) = 0$ for any $g \in G$ with $a_1, ..., a_n \in F$, if and only if $a_1 = ... = a_n = 0$.

Lemma 5.4. *Let F be a field, G a group, and $\chi_1, ..., \chi_n : G \to F$ be distinct homomorphisms of monoids where F is regarded as a monoid by multiplication. Then $\chi_1, ..., \chi_n$ are linearly independent over F.*

Proof. We shall look at linear independence in a slightly different manner. If $a_1, ..., a_n$ are not all zero, then $\sum a_i\chi_i(g) \neq 0$ for some $g \in G$. We shall do a proof by induction.

For the case of $n = 1$, we have $g = e$, with e as the identity element of G and $\chi_1(e) = 1$, and so we must have $a_1 = 0$ if $a_1\chi_1(e) = 0$.

We notice that if any a_i is equal to 0 in $\sum a_i\chi_i(g) = 0$, we can simply take off the corresponding χ_i and relabel to work with one less element and so on until all $a_i \neq 0$. We thus only need to look at the case where all $a_i \neq 0$. Now suppose we have our lemma stand for $n > 1$, and from above we can reduce our case to have all $a_i \neq 0$. Let us now add the element $a_{n+1}\chi_{n+1}(g) \neq 0$, we then have $\sum_{i=1}^{n+1} a_i\chi_i(g) = 0$ if and only if $-a_{n+1}\chi_{n+1}(g) = \sum_{i=1}^{n} a_i\chi_i(g)$. We will now show why this is not possible through a proof by contradiction. Now let us divide by $-a_{n+1}$ and relabel our $a_k = \frac{a_i}{-a_{n+1}} \neq 0$ and $\chi_i = \chi_k$ accordingly. We thus have

$$\chi_{n+1}(g) = \sum_{k=1}^{n} a_k\chi_k(g)$$

for all $g \in G$. Let us now fix an $h \in G$, and due to all χ being homomorphisms we have $\chi(h)\chi(g) = \chi(hg)$ for any $g \in G$. It then follows that

$$\chi_{n+1}(gh) = \chi_{n+1}(h) \cdot \sum_{k=1}^{n} a_k\chi_k(g)$$

and

$$\chi_{n+1}(gh) = \sum_{k=1}^{n} a_k\chi_k(gh).$$

Setting these equal, it then follows that

$$0 = \chi_{n+1}(h) \cdot \sum_{k=1}^{n} a_k\chi_k(g) - \sum_{k=1}^{n} a_k\chi_k(gh) = \sum_{k=1}^{n} a_k\chi_k(g)(\chi_{n+1}(h) - \chi_k(h)).$$

Since all our $a_k\chi(g) \neq 0$, the only way this sum is equal to 0 is if $\chi_{n+1}(h) = \chi_k(h) = \chi_i(h)$ for all $k \leq n$, and since h was arbitrarily fixed, this implies that $\chi_i = \chi_{n+1}$ for $i \leq n$. We thus have reached a contradiction since we had our χ_i as distinct homomorphisms which is not the case. We have thus proved our inductive step since our sum is not equal to 0 unless all our $a_i = 0$. We can thus conclude our lemma and so our χ_i are linearly independent over F. □

Theorem 5.5. *If $\chi_1, ..., \chi_n : G \to F^\times$ are distinct characters of G, then they are linearly independent over F.*

Proof. Our characters and $F^\times$ fulfill the conditions set by lemma 5.4, and thus are proven to be linearly independent over F. □

Theorem 5.6. *Let E/F and K/F be extension fields, and $\sigma_1, ..., \sigma_n : K \to E$ be distinct morphisms of extensions of F. Then $\sigma_1, ..., \sigma_n$ are linearly independent over E.*

Proof. Since our σ_i meet the criteria set by lemma 5.4 when we apply it to the restriction of σ_i to the group of units we have linear independence. □

6. Galois Theory

Definition 6.1. For any subset H of $\mathcal{A}ut_F(E)$, the fixed field of H is

$$E^H := \{x \in E | \forall h \in H, h(x) = x\}.$$

Lemma 6.2. *Let F be a field, $\alpha \in \overline{F}$ be an element in the algebraic closure of F, and $p(x)$ its minimal polynomial over F. We then have:*

$$F(\alpha) \cong F[X]/\langle p(x) \rangle.$$

Proof. Let $\psi : F[X] \to F(\alpha)$ be the homomorphisms which fixed F and maps x to α. We see that the kernel of ψ will be all the polynomials which vanish alpha, and so those generated by $p(x)$. We thus conclude that $Ker(\psi) = \langle p(x) \rangle$, and so by the first isomorphism theorem we must have $F(\alpha) \cong F[X]/\langle p(x) \rangle$. □

Theorem 6.3. *Let $\overline{F}$ denote the algebraic closure of F. A finite extension E/F is said to be normal if and only if any of the following equivalent conditions hold:*

1) Every irreducible polynomial $f(x)$ over F with a root in E splits into its linear factors in E.

2) For all $\alpha \in E$, the minimal polynomial of α over F has E as its splitting field.

3) $\sigma(E) = E$ for all $\sigma \in \mathcal{A}ut_F(E)$, with $\mathcal{A}ut_F(E)$ as the set of embeddings of E in $\overline{F}$ which fix F point wise.

Proof. We will show the equivalence of these definitions.

$1 \implies 2$ Since E/F is finite, it is algebraic by Corollary 3.13, and thus we know every $\alpha \in E$ will be a root of some polynomial over F. We thus know the minimal polynomial of α will split in E. It thus follows that for all $\alpha \in E$, the minimal polynomial of α over F has E as its splitting field.

$2 \implies 1$ Take any irreducible polynomial $f(x)$ over F with at least one root in E. It then follows that there must be the roots $alpha_i \in E$ such that $f(x)$ is composed by the minimal polynomial of the α_i. However, by 3, we know that the minimal polynomial of each of these α_i splits in E, and so we must have $f(x)$ splitting in E as well.

$1 \implies 3$ Suppose every irreducible polynomial $f(x)$ over F with a root in E splits completely in E, we want to show this implies $\sigma(E) = E$ for all $\sigma \in \mathcal{A}ut_F(E)$. Now let us have an arbitrary $\alpha \in E$ and $\sigma : E \to \overline{F}$ an abritrary embedding of E fixing F. We want to show that $\sigma(\alpha) \in E$. Let $p(x)$ be the minimal polynomial of α over F. Since σ fixes F, we must have $\sigma(\alpha)$ as a root of $p(x)$. since $\alpha \in E$, we have all the roots of $p(x)$ in E, and consequently, $\sigma(\alpha) \in E$. We can thus conclude that we would then have $\sigma(E) = E$ for all $\sigma \in \mathcal{A}ut_F(E)$ due to our abritrary choices of $\alpha \in E$ and $\sigma \in \mathcal{A}ut_F(E)$.

$3 \implies 1$ We will now show that if for all $\sigma \in \mathcal{A}ut_F(E)$, $\sigma(E) = E$, then every irreducible polynomial $f(x)$ over F with a root in E splits completely in E. Let us once again take an arbitrary $\alpha \in E$ and let $p(x)$ be it minimal polynomial over F. We want to show that for every root β of $p(x)$, there exists an embedding σ_β of E in $\overline{F}$ such that $\sigma_\beta(\alpha) = \beta$. Let us consider the intermediate field $K = F(\alpha) \subset E$, by the previous Lemma, we know that we have an automorphism τ_β for each β such that $\tau_\beta(\alpha) = \beta$ and τ_β fixes F. We can then extend these isomorphisms to an embedding σ_β of E in $\overline{F}$ such that $\sigma_\beta \upharpoonright K = \tau_\beta$ with $\upharpoonright$ denoting the truncation of σ_β to K. Since we have $\sigma_\beta(E) = E$ for each root β, it thus follows that all roots of $p(x)$ are in E. □

Theorem 6.4. *The correspondence between field extensions to groups and groups to field extensions is inclusion reversing;*

1) if $F_1 \subset F_2 \subset E$, then $\mathcal{A}ut_{F_2}(E) \leq \mathcal{A}ut_{F_1}(E)$.

2) if $H_2 \leq H_1 \leq \mathcal{A}ut(E)$ with respective fixed fields F_2 and F_1, then $F_1 \subset F_2$.

Proof. 1) Since any automorphism, σ fixing F_2 will also fix F_1, we have $\sigma \in \mathcal{A}ut_{F_1}(E)$ and so $\mathcal{A}ut_{F_2}(E) \leq \mathcal{A}ut_{F_1}(E)$.

2) We have $H_2 \leq H_1$ with H_1 fixing F_1. It then follows that all elements of H_2 will also fix F_1. However, we do not necessarily have all elements of H_1 fixing F_2. It then follows that all the elements fixing F_2 fix F_1, but not all the elements fixing F_1 fix F_2. We can thus conclude $F_1 \subset F_2$. □

Theorem 6.5. *Let G be a finite group of automorphisms $\sigma_1, ..., \sigma_n$ of the field E, and $E^G = F$. Then any element of $\alpha \in E$ is a root of a polynomial equation over F, so E is an algebraic field extension of F.*

Proof. Consider our group of automorphisms $\sigma_1, ..., \sigma_n$ and the image of α through them, $\sigma_i(\alpha)$. Let us take all α_i such that $\alpha_i = \sigma_i(\alpha)$ with each α_i distinct (let us say there are $m \leq n$ of them). By definition, α will be one of the α_i since we will have one of our σ_i as the identity. Let us now look at

$$\sigma_i\sigma_1(\alpha), \sigma_i\sigma_2(\alpha), ..., \sigma_i\sigma_m(\alpha)$$

for an arbitrary $i \leq n$. Notice that $\sigma_i\sigma_k$ for $k \leq m$ will simply be another element of the group $\sigma_1, ..., \sigma_n$. It then follows that $\sigma_i\sigma_1(\alpha), \sigma_i\sigma_2(\alpha), ..., \sigma_i\sigma_m(\alpha)$ will simply be another permutation of our α_k which will all be distinct since if not we would have two σ_k same which is not possible. We thus have the distinct elements of α_k in a different arrangement. Let us create the polynomial

$$\phi(x) = \prod_{k=1}^{n}(x - \alpha_k).$$

Using the fact that $\sigma_i\sigma_1(\alpha), \sigma_i\sigma_2(\alpha), ..., \sigma_i\sigma_m(\alpha)$ is a different arrangement of the α_k, we now know

$$\sigma_i(\phi(x)) \prod_{k=1}^{m} \sigma_i(x - \alpha_k) = \prod_{k=1}^{m}(x - \sigma_i(\alpha_k)) = \phi(x).$$

The coefficients of $\phi(x)$ remain unchanged and so they must be fixed elements and thus elements of F, and the roots of $\phi(x)$ are the α_k. We thus have them as algebraic, and we know that our arbitrary $\alpha \in E$ is amongst them, and so α is the root of some polynomial equation over F. Due to the arbitrary nature of our chosen α we conclude any element of $\alpha \in E$ is a root of a polynomial equation over F and E is an algebraic field extension. □

Theorem 6.6. *The extension E/F is normal if and only if E is the splitting field of a separable polynomial over F.*

Proof. Assume E is the splitting field of a separable polynomial $p(x)$ over F. By lemma 4.5, we know that F is the fixed field under the group of all automorphisms which leave every element of F fixed, thus we know that E/F is normal.

Assume E/F is normal, with $[E : F] = n$, then there is a basis B of n elements of E/F and E is obtained from F by adjoining each of the n elements of B. Since the degree of E/F is finite, each element of B serves as a root of an irreducible separable polynomials $p_i(x)$ over F. The polynomial $f(x) = p_1(x)p_2(x)...p_n(x)$ splits in E since each factor will also split in E among the roots denoted by the elements of B. We can thus see that E must be the smallest field than can split $f(x)$ and thus is the splitting field.

□

Corollary 6.7. *If E/F is normal and if K is any field such that $F \subset K \subset E$ then E/K is normal.*

Proof. E is the splitting field of $p(x)$ over F and thus is the splitting field of the same seprable polynomial over K which as shown above indicates E/K is normal. □

Lemma 6.8. *For any finite group of automorphisms H of E the following hold:*
1) E/E^H is separable
2) E/E^H is normal
3) $[E : E^H] = |H|$
4) $H = \mathcal{A}ut_{E^H}(E)$.

Proof. 1) Let us take any $\alpha \in E/E^H$ and $\alpha_1, ..., \alpha_n$ as its orbit by H. It then follows that α will be a root of the polynomial

$$g(x) = \prod_i (x - \alpha_i) \in E^H[X]$$

since all the α_i are unique, $g(x)$ is relatively prime to its derivative and thus separable. We thus have α as a root of a separable polynomial over E^H. Since our choice of α was arbitrary, it thus follows that this is the case for any $\alpha \in E/E^H$ and so we have E/E^H as separable.

2) Let us consider an arbitrary polynomial $p(x) \in E^H[X]$ with a root $\alpha \in E$. For any automorphism $\sigma \in H$, we must have $\sigma(\alpha)$ as another root of $p(x)$ since the coefficients of $p(x)$ in E^H are fixed by σ. Since H is a finite group, all roots must lie in E and so $p(x)$ split into its linear factors in E. Thus by Theorem 6.3 we know that E/E^H must be normal.

3) We know that automorphisms act transitively on the roots of polynomials, and by the orbit-stabilizer theorem, the size of H is equal to the number of distinct images of an element $\alpha \in E$ under the action of H. This will be the degree of the minimal polynomial of α over E^H which will be equal to $[E : E^H]$. We can thus

conclude that $|H| = [E : E^H]$.

4) We want to show that $\mathcal{A}ut_{E^H}(E) \subset H$. Let us consider any $\sigma \in \mathcal{A}ut_{E^H}(E)$ which will permute the roots of any polynomial over E^H in E. Since H is the full set of automorphisms fixing E^H, and all elements of $\mathcal{A}ut_{E^H}(E)$ fix E^H, it thus follows that $\mathcal{A}ut_{E^H}(E) \subset H$. Similarly, all elements in H fix E^H and are automorphisms of E, and so $H \subset \mathcal{A}ut_{E^H}(E)$ which concludes that $\mathcal{A}ut_{E^H}(E) = H$. □

Theorem 6.9 (Definition of Galois extensions and groups)**.** *
Let us have a finite field extension E/F and $G = \mathcal{A}ut_F(E)$, then all the following conditions imply each other and when they hold E/F is called a Galois extension and G its Galois group (denoted by $Gal(E/F)$):
1) E/F is normal and separable
2) E is the splitting field of a separable polynomial $p \in F[X]$
3) $|G| = [E : F]$
4) F is the fixed field of G,

Proof.
$1 \iff 2$ If E is normal then by definition it is the splitting field of a polynomial $F[X]$ which will have no multiple factors over F and so is also separable. Conversely, if E is the splitting field then E/F is normal and $E = F[\alpha_1, ..., \alpha_n]$ with α as the n distinct roots and so E/F is separable.

$1 \implies 4$ By the definition, we know that G will fix F. We now want to show that only the elements of F are fixed and those that aren't will be moved. We assume that E/F is normal and separable. By Theorem 6.6, we know that since E/F is normal, E is the splitting field of an irreducible polynomial $p(x)$ over F. Furthermore, since it is separable, we know that the minimal polynomial of any of its elements is separable (so have no repeated roots as per Corollary 3.19). We can now use Lemma 4.5 as we know if E is the splitting field of $p(x)$ over F and it is separable. It thus follows that no elements other than those of F remain fixed in $\mathcal{A}ut_F(E)$.

$4 \implies 1$ We have F as the fixed field of $G = \mathcal{A}ut_F(E)$ and so it follows that $E^G = F$. In addition,G is a finite group of automorphisms of E, so we can then apply Lemma 6.8 and so we know that in this case E/E^G is normal and separable.

$4 \implies 3$ As in the previous part, we can apply Lemma 6.8 and so we know that E/F is of degree $|G|$, otherwise written as $[E : F] = |G|$.

$3 \implies 4$ We know that $[E : F] = |G| = [E : E^G]$, and so it directly follows that F and E^G are equivalent up to isomorphism, thus $F = E^G$ is the fixed field of G. □

Corollary 6.10. *Let $F \subset K \subset E$ with E/F Galois, then E/K is Galois.*

Proof. We know that if E/F is a Galois extension. By Theorem 6.9 part 2 it then follows that E is the splitting field of a separable polynomial $p(x)$ over F. Since $F \subset K \subset E$, E is the splitting field of the same $p(x)$ over K as well and so using Theorem 6.9 it thus follows that E/K is Galois. □

Theorem 6.11 (Fundamental Theorem of Galois Theory)**.** *
Let E/F be a Galois extension, with Galois group $G = Gal(E/F)$. To each intermediary field K of E/F, we associate the group $G_K = \mathcal{A}ut_K(E) = Gal(E/K)$ and to each subgroup $H < G$ we associate the fixed field E^H. The following 4 statements hold:

1) There is a bijection between the set of intermediary fields and the set of subgroups of G.

2) If $K \subset K'$ are subfields of E/F, then $[K' : K] = [G_K : G'_K]$,

3) If $H' < H < G$ are subgroups of G, then $[H : H'] = [E^{H'} : E^H]$.

4) If K is an intermediary field of E/F and $\sigma \in G$, then $\sigma(K)$ is an intermediary field of E/F and $G_{g(K)} = \sigma G_K \sigma^{-1}$, otherwise written as $Gal(E/\sigma(K)) = \sigma Gal(E/K)\sigma^{-1}$

5) If $H < G$, then $E^{gHg^{-1}} = g(E^H)$.

6) For $F \subset K \subset E$, we have K/F is normal if and only if G_K is a normal subgroup of G, in which case $Gal(K/F) \cong G/G_K$.

Proof. .

1) From Lemma 6.8, we can see that we can map any group of automorphisms, H, so any subgroup of G, to the field E^H. In our specific case, using Theorem 6.3 we know that $H \subset G$ and so it follows that $F \subset E^H \subset E$ and so it is an intermediary field of E/K. This is a one to one mapping, so injective, and for every intermediary field, there will exist a subgroup of G that fix it, so we have surjectivity as well. We have thus constructed a bijection between the set of intermediary fields and the set of subgroups of G.

2) We know that for any intermediary fields, K and K', since E/F is Galois, we have E/K and E/K' as Galois as well by Corollary 6.10. It then follows from Theorem 6.9 part 3 that $G_K = [E : K]$ and $G_{K'} = [E : K']$. Furthermore, using the Tower Law (Theorem 3.14) and Lagrange's Theorem (Theorem TBD), we know that

$$[K' : K] = \frac{[E : K]}{[E : K']} = \frac{G_K}{G_{K'}} = [G_k : G'_k].$$

We can thus conclude $[K' : K] = [G_K : G'_K]$.

3) By part 1, we have established a bijection between the set of intermediary fields and the set of subgroups of G. We can thus map H' and H to their respective intermediary fields, $E^{H'}$ and E^H, where using Theorem 6.3 we know that $E^H \subset E^{H'}$. Having fulfilled the conditions, we can apply part 2 to get $[H : H'] = [E^{H'} : E^H]$.

4) We know that for any $\sigma \in G$, $\sigma(K)$ will leave F fixed and might permute the elements of K with other elements in E but not in F. It would then follows that all elements of F will be in $\sigma(K)$ as it was fixed, $\sigma(K)$ maps to some sub-field of E. We thus conclude that $F \subset \sigma(K) \subset E$ and so $\sigma(K)$ is an intermediary field of E/F for any $\sigma \in G$.

We now set out to prove the second part of the statement. We know that σ sends K to $\sigma(K)$, and so σ^{-1} send $\sigma(K)$ to K, in addition any element $h \in G_K$

will fix K. Knowing this, let us look at how $\sigma h\sigma^{-1}$ acts on $\sigma(K)$ for any $h \in G_K$:

$$\sigma h\sigma^{-1}(\sigma(K)) = \sigma h(K) = \sigma(K).$$

We thus see this leaves $\sigma(K)$ for any $h \in G_K$ and so it follows that $\sigma G_K\sigma^{-1} \subset G_{\sigma(K)}$. We now want to show that $G_{\sigma(K)} \subset \sigma G_K\sigma^{-1}$. Let us take an arbitrary automorphism $\tau \in G_{\sigma(K)}$. We know that τ will fix every element of $\sigma(K)$, now let us look at how $\sigma^{-1}\tau\sigma$ acts on K:

$$\sigma^{-1}\tau\sigma(K) = \sigma^{-1}\sigma(K) = K \implies \sigma^{-1}\tau\sigma \in G_K \implies \tau \in \sigma G_K\sigma^{-1}.$$

Since our choice of τ was arbitrary, we thus know that $G_{\sigma(K)} \subset \sigma G_K\sigma^{-1}$ and can conclude $G_{\sigma(K)} = \sigma G_K\sigma^{-1}$, otherwise written as $Gal(E/\sigma(K)) = \sigma Gal(E/K)\sigma^{-1}$.

5) As it is defined, we know that $H = Gal(E/E^H)$, furthermore, using part 4 we know that $gHg^{-1} = Gal(E/g(E^H))$. Due to the bijective nature of of the mapping between the set of subgroups of G and the intermediary fields, we know that if two groups are the same, so are their fixed fields. Equipped with this, we can thus cocnlude that $E^{gHg^{-1}} = g(E^H)$ since $gHg^{-1} = Gal(E/g(E^H))$.

6) As per Theorem 6.3, we know that K/F is normal if and only if for every $\sigma \in G$, $\sigma(K) = K$. Suppose that K/F is normal. We then define the map

$$\psi : G \to G_K$$

by sending σ to the restriction ϕ of σ to K. As K/F is normal, ϕ is an automorphism of F/K. It is quite apparent and easy to check that ψ is a homomorphism of groups, and G_K is clearly the kernel, and thus normal in G. It then follows that G/G_K is isomorphic to a subgroup of $Gal(K/F)$. However by the Tower Law and Theorem 6.9 we see:

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

We can thus conclude that $Gal(K/F) \cong G/G_K$.

Now going the other way, suppose G_K is normal in G. Take an arbitrary $x \in K$, let $\phi \in G$, and set $y = \phi(x)$. As G_K stabilizes x, then $G_K = \phi G_K\phi^{-1}$ stabilizes y. However, as $G_K = \mathcal{A}ut_K(E)$, the only elements of E stabilized by all of G_K are only those of K. Thus we must have $y \in K$, and so $\phi(K) = K$ for every $\phi \in G_K$ and so K/F is normal. □

7. Radical Extensions

Definition 7.1. Let E be a field and F and K subfields of E. The composite of F and K is said to be the intersection of all subfields of E containing both F and K. This relationship is denoted FK.

Definition 7.2. Let K/F be a separable field extension. If K is contained in a field extension E which is Galois over F and is the smallest field to do so, then E is the Galois closure of K over F.

Definition 7.3. The extension E/F is a cyclic extension if its Galois group is cyclic.

Definition 7.4. A radical extension is a field extension obtained by adjoining roots of elements. For example $\mathbb{Q}(\sqrt{2})$ is a radical extension of $\mathbb{Q}$. More generally, if F is a field and $\alpha \in F$, the field $F(\alpha^{1/n})$ obtained by adjoining an nth root of α is a radical extension of F.
Let E be an extension of F generated by a sequence of radical extensions:

$$F \subset F_1 \subset F_2 \subset ... \subset F_n = E,$$

where each $F_{i+1} = F_i(\alpha_i^{1/n_i})$ for some $\alpha_i \in F_i$ and $n_i \in \mathbb{Z}$. Then E is a radical extension of F.

Theorem 7.5. *Let E/F be a Galois extension of fields whose Galois group is $\mathbb{Z}/n\mathbb{Z}$. Let us assume that the characteristic of F is relatively prime with n and that F contains a primitive nth root of 1. We then know that $E = F(z^n)$ with $z^n \in F$.*

Proof. Let $\xi \in F$ be a primitive nth root of 1 and σ a generator of $Gal(E/F)$. We can consider our σ as a linear operator in F, and so $\sigma^n - 1 = 0$. Applying lemma 5.4, we know that there cannot be a polynomial p over F of degree less than n such that $p(\sigma) = 0$. We thus know that the minimal polynomial of σ is $x^n - 1$. Since ξ is a root of $x^n - 1$, there exists a $z \in E$ such that $\sigma(z) = \xi z$. Furthermore, this z will satisfy $z^n \in F$ since $\sigma(z^n) = (\xi z)^n = z^n$. In addition, we see the that $z, \sigma(z), ..., \sigma^{n-1}(z), \xi z, ..., \xi^{n-1}z$ are all distinct. This helps us conclude that z generates E over F and thus we know $E = F(z)$. □

Lemma 7.6. *Let F be a field containing the nth 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. Since F contains the nth roots of unity, it is the splitting field of $x^n - a$ and thus the extension $F(\sqrt[n]{a})$ is Galois over F. For any automorphism $\sigma \in Gal(F(\sqrt[n]{a})/F)$, we know $\sigma(F(\sqrt[n]{a}))$ as a root of the polynomial and so

$$\sigma(F(\sqrt[n]{a})) = \xi_\sigma F(\sqrt[n]{a})$$

where ξ_σ is some nth root of unity. Let us now consider the map $Gal(F(\sqrt[n]{a})/F) \rightarrow u_n$ given by $\sigma \rightarrow \xi_\sigma$ with u_n as the group of the nth root of unity. We can also see that this map is a homomorphism since

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

This map is also an injection since its kernel is the identity map due to it fixing $\sqrt[n]{a}$. □

Definition 7.7. For $\alpha \in E$ and any nth root of unity ξ, we have the Lagrange resolvent $(\alpha, \xi) \in E$ by $(\alpha, \xi) = \alpha + \xi\sigma(\alpha) + ... + \xi^{n-1}\sigma^{n-1}(\alpha)$ for $\sigma \in Gal(E/F)$

Corollary 7.8. *The Lagrange resolvent $(\alpha, \xi)^n$ will be fixed by all elements of $Gal(E/F)$ and in $(\alpha, \xi)^n \in F$.*

Proof. Let $\sigma \in Gal(E/F)$, then we know:

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

Thus, $\sigma(\alpha, \xi)^n = (\xi^{-1})^n (\alpha, \xi)^n = (\alpha, \xi)^n$.
We have thus shown that for any $\sigma \in Gal(E/F)$, $(\alpha, \xi)^n$ is fixed, and thus $(\alpha, \xi)^n \in F$.

□

Theorem 7.9. *Let α be contained in a root extension such that α is an element of a field K that can be obtained by a succession of radical extensions:*

$$F = K_0 \subset ... \subset K_q = E,$$

where each $K_{i+1} = K_i(\sqrt[n]{a_i})$ for $\alpha_i \in K$. Then, α is contained in a root extension which is Galois over F such that each K_{i+1}/K_i is cyclic.

Proof. Let C be the Galois closure of K over F. We then have

$$\sigma(F) = \sigma(K_0) \subset ... \subset \sigma(K_q) = \sigma(K),$$

for any $\sigma \in Gal(C/F)$ with each $\sigma(K_{i+1})/\sigma(K_i)$ is a radical extension generated by $\sigma(\sqrt[n_i]{a_i})$. The composite of root extensions is a root extension so the composite of all $\sigma(K) \forall \sigma \in Gal(E/F)$ is a root extension with E as the composite of these fields. We must then have α contained in a root extension. We then extend the N_ith roots of unity for all roots $\sqrt[n_i]{a_i})$ of the radical extension K/F to F which we will now call F' and obtain the composite extensions

$$F' = K_0F \subset ... \subset K_qF = KF' = E'$$

which is composition of Galois extensions by definition and so E'/F is also a Galois extension. By lemma 7.5 we know, since the base field of each extension $F'K_{i+1}/F'K_i$ is a radical extension which contains the roots of unity, each extension $F'K_{i+1}/F'K_i$ is cyclic. We have thus shown that for each α as described, we have E'/F as a Galois extension that fits the criteria demanded.

□

8. Abel-Ruffini Theorem

Lemma 8.1. *The symmetric group, A_n, is simple for $n \geq 5$.*

Proof. Let us show that A_n is a simple group for $n \geq 5$. I will first show that A_5 is a simple group. Let us first look at the elements inside A_5. We have the identity, 20 3-cycles, 24 5-cycles, and 15 order 2. Let us now look at the centrilizers of elements for each order type. For order 3, we look at $(1, 2, 3)$ who's centralizer is $e, (1, 2, 3), (1, 3, 2)$ in A_5 which is 3 elements and so the conjugacy class of $(1, 2, 3)$ has $60/3 = 20$ elements and so is the set of all the $3 - cycles$. Similarly, for the product of our 2 cycles, take for example $(1, 2)(3, 4)$ will have 4 elements in the centralizer and so the conjugacy class will be 15 elements and so all the other order 2 elements. For our order 5 we look at the centralizer of $(1, 2, 3, 4, 5)$ who's centralizer will have 5 elements, and so the conjugacy class of this has 12 elements. We can get the other 12 elements through some creative shifting to get the whole class other conjugacy class of another element of order 5. We thus have classes with 1, 12, 12, 15, and 20 elements. Now we know that for N normal subgroup of G then N is equal to the union of the disjoint conjugacy classes. We know that the order of N must divide the order of A_5 so 60 and will be made from a sum of 1, 12, 12, 15, and 20 with a need for the identity element in it so we need to add the 1. This only divides 60 for $|N| = 1$ or $|N| = 60$ and so the only possible normal subgroups are the trivial subgroup and A_5.

Now moving on to the general case of A_n for $n > 5$. We first quickly show that A_n is generated by the $3-cycles$, which is the case since the product of any 2 transpositions is a product of $3-cycles$ and since any element in A_n is a product of even number of transpositions this solves. Let τ_1 and τ_2 be transpositions which move a common number a so $\tau_1\tau_2 = (a,b)(a,c) = (a,c,b)$ and so we are done. No supposing that they have no moving elements in common, with $\tau_1\tau_2 = (a,b)(c,d) = (d,a,c)(a,b,d)$ and so we are done. We thus have A_n generated by the $3-cycles$. We next show that the 3-cycles form their own class. We see the number of $3-cycles$ will be $\frac{n(n-1)(n-2)}{3}$ and we then look at the centralizer of $(1,2,3)$. We know it will be in $S_n \subset S_3 \times S_{n-3} \cap A_n = Z/3 \times A_{n-3}$, and so it follows that the centralizer has $\frac{3(n-3)!}{2}$ elements and so the order of the class of $(1,2,3)$ is $\frac{n!}{2}/\frac{3(n-3)!}{2} = \frac{n(n-1)(n-2)}{3}$ and so the class of $(1,2,3)$ is all the 3-cycles and form their own class. Now suppose we have a normal subgroup, N, of G with $N \neq \{e\}$. Let $\sigma \in N$ with $|\sigma| = m > 1$. Choose smallest $p|m$, if $p \neq m$ then replace $\sigma^{\frac{m}{p}}$, and so we now have $|\sigma| = p$ prime, thus σ is the product of disjoint $p - cycles$. If any of these is a 2,3, or 5 cycle we are done since if there is a $3-cycle$, then the 3-cycles class is in N and so $N = A_n$, if there is a 5 cycle as done for A_5 we can transform it into 3-cycles, and finally if there is a 2 cycle this isn't possible since that is an odd permutation so we can rule it out. Now if this is not the case, we will conjugate and multiply since a normal subgroup is closed under both.

Now for $p = 2$, we conjugate by (a,b,c) with $\sigma = (a,b)(c,d)...$ and so $w = (b,c)(a,d)....$ For the cycles not showing they will be their own inverse, and so $\sigma w = (a,b)(c,d)(b,c)(a,d) = (a,c)(b,d)$ which we know how to turn into $3-cycles$ and so we are done.

For $p = 3$, we have $\sigma = (abd)(def)...$ which we conjugate by (abd) to get $w = (bdc)(aef)...$ and $w^{-1} = (bcd)(afe)()^{-1}...$ and so since the terms not shown cancel $w^{-1}\sigma = (bcd)(afe)(abc)(def) = (acfbd)$ and so we are done.

Now for $p > 3$, we know that we can break the larger elements such that a 3-cycle must appear. We thus have a $3-cycle$ and so for all the case where we have $N \neq \{e\}$ we must have $N = A_n$ and thus A_n must be simple for $n \geq 5$.

□

Lemma 8.2. *The symmetric group, S_n, is not solvable for $n \geq 5$.*

Proof. To show that S_n is not solvable for $n \geq 5$, we use the fact that the alternating group A_n is simple for $n \geq 5$. The derived series of S_n starts with A_n, because A_n is generated by commutators in S_n. Since A_n is simple for $n \geq 5$, it has no nontrivial normal subgroups other than itself. This implies that the derived series of S_n is $S_n \triangleright A_n \triangleright e$, where A_n cannot be further decomposed into simpler normal subgroups. As A_n is non-abelian and cannot be reduced to the trivial group through commutators, S_n cannot be broken down into a series of abelian groups, hence S_n is not solvable for $n \geq 5$.

□

Lemma 8.3. *A polynomial f is solvable by radicals if and only if its Galois group is solvable.*

Proof. Let $p(x)$ be a solvable polynomial by radicals. For each root of p, there exists an extension field $F(\alpha)$. Through the composition of these fields we have an extension field that is Galois and will have all the roots of our polynomial, let us call such a field E. By theorem 6.11, we can attribute to each $H_i < G$, subgroup of $Gal(E/F)$, a corresponding subfield K_i of E/F, and we know

$$Gal(K_{i+1}/K_i) = H^{i+1}/H_i,$$

and thus our group G is solvable since each quotient will be abelian due to it being cyclic.

Let $p(x)$ have a Galois group G which is solvable. By the fundamental Theorem of Galois theory, we will have a chain of fixed subfields each fixed by a subgroup of G, with

$$F = K_0 \subset ... \subset K_q = E$$

where by definition 2.2 since each group is solvable then each group is cyclic and thus by the Galois correspondence each extension K_{i+1}/K_i is cyclic. We then extend by the n_ith roots of unity to F and obtain the field F' and after composing this with the chain of subfields, we have

$$F' = F'K_0 \subset ... \subset F'K_q = F'E$$

and the cyclicity remains of degree dividing n_i. We have a base field which contains the roots of unity, so each extension is a radical extension and so our $p(x)$ must be solvable by radicals. □

Theorem 8.4 (Abel-Ruffini Theorem)**.** *
For $n \geq 5$, the general polynomials of degree n is not solvable in the radicals.

Proof. The general polynomial equation of degree n is of the form

$$0 = x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$$

where a_i are the distinct indeterminates and the equation defined over the field

$$F = \mathbb{Q}(a_1, ..., a_n).$$

We will now show that the Galois group over F of the equation is the symmetric group S_n which is not solvable for $n \geq 5$.

Let us have the x_i be new indeterminates aimed to be our roots, now consider the polynomial

$$p(x) = x^n + b_1x^{n-1} + ... + b_{n-1}x + b_n = (x - x_1)...(x - x_n).$$

Let us now look at the fields $H = \mathbb{Q}(x_1, ..., x_n)$ and its subfield $K = \mathbb{Q}(b_1, ..., b_n)$. The permutation of the x_i induce automorphisms of H, and by Vieta's formulas, every element of K us a symmetric function of the x_i and thus will be the fixed field of all the automorphisms and so we conclude that $Gal(H/K) = S_n$. By the fundamental Theorem of Symmetric Polynomials, we know that b_i are algebraic independent and so the map will send each a_i to the corresponding b_i and so there is an isomorphism from F to K. Thus the Galois group of a general equation is the symmetric group and thus unsolvable. We can now conclude the general polynomial equation of degree $n \geq 5$ cannot be solved in radicals. □

Acknowledgments

I would like to thank my mentor, Chengyang Bao, for her exceptional encouragement and patience. I would also like to thank Daniil Rudenko for the invaluable lessons he taught me regarding group theory and the interconnected nature of mathematics, which led me to writing this paper. Finally, thank you Peter May for reading this and encouraging me to make the English more understandable.

bibliography

References

[1] Serge Lang. Algebra. Springer-Verlag. 2002.
[2] Emil Artin. Algebra with Galois Theory. American Mathematical Society. 2007.
[3] Stacks project authors. The Stacks project. https://stacks.math.columbia.edu. 2022.
[4] David S. Dummit. Richard M. Foote. Abstract Algebra. Wiley. 1999.
[5] David A. Cox. Galois Theory. Wiley. 2012.