GALOIS THEORY AND THE FUNDAMENTAL THEOREM OF ALGEBRA

SRIRAM ANANTHAKRISHNAN

Abstract. The Fundamental Theorem of Algebra, as the name suggests, is one of the most important theorems in all of mathematics. While its seemingly obvious statement is intuitive to most, proving it is quite involved and may be done through somewhat disconnected areas of mathematics. In this paper, we will explore how developing the fundamental machinery of Galois Theory can yield a rather simple proof of the theorem. Hence, while the Fundamental Theorem of Algebra is seemingly unrelated to the theory of groups and fields, the following paper illustrates the power of Galois Theory as a uniting force of groups and fields in solving often seemingly unrelated problems.

Contents

1. Introduction

In this paper, we will develop the main results of Galois Theory, which allows us to examine relations between field theory and finite group theory. Specifically, it allows us to associate **Galois Extensions**, a special type of algebraic extension, to a group, namely the **Galois Group**. Using these notions, the Fundamental Theorem of Algebra boils down to proving that any nontrivial Galois extension of $\mathbb{C}$ must be $\mathbb{C}$ itself - which is somewhat straightforward.

2. Basic Group Theory

Central to Galois Theory is the idea of a special type of algebraic field extension called the **Galois Extension**, and these are related to a group called the **Galois Group**. To fully develop the results of Galois Theory, we must first develop some

Date: DEADLINES: Draft AUGUST 14 and Final version AUGUST 28, 2024.

results in basic group theory, as well as field theory, which will be covered in the next section.

Recall that a **Group** is an algebraic structure consisting of a set and a binary operation $(G, \star)$. All groups have the following properties:

(1) $\star$ is associative. Namely, for any $a, b, c \in G$, we have $(a \star b) \star c = a \star (b \star c)$.
(2) The group is closed under $\star$. In other words, for any $a, b \in G$, $a \star b \in G$.
(3) Every element $g \in G$ has an inverse g^{-1}, and there always exists an identity element e in G, such that $g \star g^{-1} = e$, and $g \star e = g$ for all $g \in G$.

We say that a group is **abelian** if $\star$ is commutative, and that it is **finite** if it has a finite number of elements. Note that the number of elements in a group is denoted as its **order**.

Next, given two groups G and H, we define a **homomorphism** between the groups as a mapping $f : G \to H$ that preserves the relationships between elements. Specifically, for any homomorphism f, $f(g_1 \star g_2) = f(g_1) \star f(g_2)$.

If f is a bijection, then we say that it is an **isomorphism**. Importantly, we say that two groups G and H are **isomorphic** if there exists an isomorphism between them. We'll use the notation $G \cong H$ to denote this relation.

If f is a bijection whose domain and codomain are the same group, then we say that f is an **automorphism**. Specifically, for any group G, an isomorphism $f : G \to G$ is an automorphism.

Example 2.1. Consider the cyclic group $G = \{g^k \mid 1 \leq k \leq n\}$, where $g^n = e$ (here, we use exponentiation to denote repeated composition of $\star$).

An automorphism $f : G \to G$ would be any mapping such that $f(g) = g^\ell$, where $\gcd(\ell, n) = 1$. Otherwise, the image of G under f would be some smaller subgroup of G.

Example 2.2. Consider the group G of all permutations of $\{1, 2, \cdots n\}$. Then, for any permutation $\{a_1, a_2, \cdots a_n\}$, the function $f(i) = a_i$ that maps elements in index i to index a_i is an automorphism.

Automorphisms are highly important in Galois Theory. As we will see later, the aforementioned **Galois Group** is actually a group of automorphisms.

Definition 2.3. For any group, field, or ring R, we denote by $\mathrm{Aut}(R)$ the set of all automorphisms f from $R \to R$. Moreover, this set forms a group.

Example 2.4. Consider the cyclic group $G = \{g^k \mid 1 \leq k \leq n\}$. We will describe the automorphism group of G.

As seen above, any valid automorphism f maps the generator g of G to some element g^ℓ, where $\gcd(\ell, n) = 1$. This is because, for any k, $f(g^k) = f(g)^k = g^{\ell k}$. It suffices to show that the set $\{\ell, 2\ell, \cdots n\ell\}$ (where elements are taken modulo n) is a permutation of $\{1, 2, \ldots n\}$.

Indeed, if two elements $i\ell$ and $j\ell$ were equal, then $(i-j)\ell \equiv 0 \pmod{n}$. However, this cannot be the case as this would imply $i \equiv j \pmod{n}$. This implies that the set $\{\ell, \ldots n\ell\}$ has n distinct elements modulo n, which in turn implies that it is a permutation of $\{1, 2, \ldots n\}$.

Hence, as the rest of the automorphism is uniquely determined by where we map the generator, we may characterize the set of all automorphisms of G by where the generator maps to. In this case, we have $g \to g^\ell$ with $\gcd(\ell, n) = 1$.

We'll now show that the set $\text{Aut}(G)$ forms a group. First, note that for any $\sigma_1, \sigma_2 \in \text{Aut}(G)$, $\sigma_1 \circ \sigma_2$ is also a bijection, and has domain G and range G. Hence, $\sigma_1 \circ \sigma_2 \in G$.

Moreover, for any $\sigma \in \text{Aut}(R)$ that satisfies $\sigma(g_i) = g_k$, the function $\sigma^{-1}(g_k) = g_i$ is also an automorphism, as is the identity function, and so $\text{Aut}(R)$ is a group.

We have discussed functions between groups, so now we discuss cosets and Lagrange's Theorem, which give us ways to "split apart" groups into smaller subgroups.

Definition 2.5. Let H be a subgroup of G and let g be a fixed element of G. We say that the set $gH = \{gh \mid h \in H\}$ the **left coset** of H. Similarly, $Hg = \{hg \mid h \in H\}$ is called the **right coset** of H. We say that these are cosets of G *modulo* H.

Consider the set of all left cosets gH of G. It's relatively simple to show that any two cosets are disjoint, which in turn implies that the set of left cosets partitions G. Similarly, the set of right cosets partitions G.

In general, the set of all left cosets of G modulo H is called the **quotient** G/H. We denote the size of this set by $[G : H]$, called the **index** of H in G.

Because the set of cosets partition G, and because each coset has $|H|$ elements, we have the following relation:

Theorem 2.6 (Lagrange's Theorem). *Let G be a finite group and H be a subgroup of G. We have*

$$|G| = [G : H]|H|.$$

In particular, this implies that the order of H divides the order of G for all subgroups H of G.

While this is a really nice result and gives great insight into subgroups themselves, the true power of taking the quotient of two groups arises when we introduce the concept of a **normal subgroup**.

Definition 2.7. Let $H \subset G$ be a subgroup and let $g \in G$. Then $g^{-1}Hg$ is a subgroup, called a *conjugate* of H. We say that g *normalizes* H if $g^{-1}Hg = H$. If this property holds for *all* $g \in G$, then H is called a **normal subgroup** of G.

Normal subgroups are important for the following reason. Suppose that $H \lhd G$, and we consider G/H, i.e., the set of left cosets of G in H. Consider any two g_1H and g_2H, and consider their product g_1Hg_2H. Because H is normal, $gHg^{-1} = H$ for any $g \in G$, meaning $gH = Hg$ (that is, all left and right cosets are equal).

Hence, we may write

$$g_1Hg_2H = g_1(Hg_2)H = g_1g_2HH = g_1g_2H,$$

which is another coset. That is, the set of all cosets under a normal subgroup is closed under composition. It's easy to show that this resulting set of cosets actually forms a group, and so we denote these groups as **quotient groups**, or factor groups.

Importantly, when H is *not* a normal subgroup, the set of cosets G/H is not necessarily a subgroup of G.

Definition 2.8 (Image and Kernel). Suppose $f : G \to H$ is a homomorphism.

(1) We denote the *kernel* of f as

$$\ker(f) = \{g \in G \mid f(g) = e\},$$

the set of elements of g that map to the identity of H under f.

(2) We denote the *image* of f as

$$\mathrm{Im}(f) = \{h \in H \mid h = f(g), g \in G\}.$$

In other words, the image of f is the set of all elements in $h \in H$ for which there exists some $g \in G$ satisfying $f(g) = h$.

Combining the above few notions gives the **First Isomorphism Theorem**.

Theorem 2.9 (First Isomorphism Theorem). *Let $f : G \to H$ be a homomorphism. Then, ker(f) is a normal subgroup of H, Im(f) is a subgroup of H. Moreover,*

(1) $G/ker(f) \cong Im(f)$

(2) Suppose further that $H \lhd G$. There now exists a homomorphism $f : G \to G/H$ such that $ker(f) = H$ and $Im(f) = G/H$.

In other words, if we consider the set of cosets of G with respect to the kernel of f, this set is isomorphic to the image of f, which encapsulates the relationship between image and kernel of any homomorphism. The second half of the theorem follows from the first part, except with the reverse notion that $H = \ker f$.

Although we do not need many fundamental results from Group Thoery, we'll introduce *Sylow's Theorem*, which is useful in proving the Fundamental Theorem of Algebra.

Theorem 2.10 (Sylow's Theorem). *Let G be a finite group of order $p^m\alpha$, such that p is a prime and* $\gcd(p, \alpha) = 1$. *We call a p-**Sylow** subgroup a subgroup of G of order p^m, and a p-group a subgroup whose only prime divisor is p. Then,*

(1) G necessarily has a p-Sylow subgroup

(2) All p-Slyow subgroups are conjugate. That is, for all p-Sylow groups H and K, there exists $g \in G$ satisfying $g^{-1}Hg = K$.

(3) Any p-subgroup of G is contained in the p-Sylow subgroup

(4) The number of p-Sylow subgroups is congruent to 1 *modulo p, and divides $|G|$, meaning it divides α.*

While this is a seemingly contrived theorem at first glance, Sylow's theorem is useful in a multitude of problems where we care about the orders of groups. As seen later, this holds in the proof of the Fundamental Theorem of Algebra.

3. Necessary Theory on Field Extensions

Definition 3.1. (Ring) Recall that a **ring** is a set R, armed with two binary operations $(+, \times)$, such that

(1) $(F, +)$ is an abelian group

(2) $\times$ is associative

(3) For any $x, y, z \in F$, $x(y + z) = xy + xz$.

(4) There exists an element $1 \in F$ such that $1x = x1 = x$, i.e., a multiplicative identity.

A **Field** is a ring armed with the property that the set $R - \{0\}$ is a group under multiplication.

Importantly, for any ring R, we define the **polynomial ring** $R[x]$ as the set of all polynomials with coefficients in R.

For example, $x^2 + 2x + 3 \in \mathbb{Z}[x]$, but $0.5x^2 + 2x + 3 \in \mathbb{Q}[x]$ and not $\mathbb{Z}[x]$.

We are concerned about the roots of such polynomials. For example,

Example 3.2. Consider the roots of the polynomial $f(x) = x^2 + x + 1 \in \mathbb{Z}[x]$. By the quadratic formula, we find

$$x = \frac{-1 \pm i\sqrt{3}}{2} \notin \mathbb{Z}.$$

This has two complex roots, but no roots in $\mathbb{Z}$.

This leads us to the following observation: for many polynomials with coefficients in a certain field, there exist roots not in said field. To further explore these types of relations, we must introduce the following notions.

Definition 3.3. Given a field K and a subfield k, we say that K is an **extension** of K, and written K/k.

For example, $\mathbb{R}$ is an extension of $\mathbb{Q}$. We can think of field extensions in the following way: let's say we start with a field, and call it the **ground field**. When we try to extend this field, we would add an element, say, α, that's not already in the field. However, once we add α, we correspondingly add α^{-1}, $-\alpha$, and all linear combinations of α with elements of the ground field.

In other words, we can think about adding elements to the field as adding a *vector space* with element α and scalar multiplication supplied by the ground field. This can be formalized in the following way.

Suppose we consider some field extension K/k as a vector space over k, i.e., where each element of K is a linear combination of the elements in k. We denote the **degree of the extension** as the dimension of K over k, and use the notation $|K : k|$ to do so.

The previous notion is more clear with a few examples.

Example 3.4. We will consider $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{C}/\mathbb{R}$.

(1) If we denote by $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, then this field has degree 2 over $\mathbb{Q}$, since the vector space has basis vectors $\{1, \sqrt{2}\}$ over a scalar field $\mathbb{Q}$.

(2) Notice that every element in $\mathbb{C}$ can be written as $x + yi$, where $x, y \in \mathbb{R}$. This is a vector space with basis $\{1, i\}$, which has dimension 2, and scalar multiplication supplied by $\mathbb{R}$. In other words, $\mathbb{C}/\mathbb{R}$ is a vector space of dimension 2.

In this regard, we denote a **finite field extension** K/k as an extension such that $|K : k| < \infty$. Note that an infinite field extension may be something like $\mathbb{R}/\mathbb{Q}$, since no finite vector space of elements in $\mathbb{R}$ with scalar multiplication in $\mathbb{Q}$ span $\mathbb{R}$.

For a given field F and any finite field extension F' of degree n, we may write $F' = F(\alpha_1, \dots \alpha_n)$, where we add elements in the following manner:

(1) Start with F. Adjoin α_1 as described before.
(2) Next, write $F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2)$, which means we adjoin α_2 to $F(\alpha_1)$.
(3) Do this iteratively. That is, keep adjoining elements to the field until we have our desired extension.

Example 3.5. Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. We can now write any element $z \in \mathbb{Q}(\sqrt{2})(\sqrt{3})$ as

$$z = (x + y\sqrt{2}) + (a + b\sqrt{2})\sqrt{3} = x + y\sqrt{2} + a\sqrt{3} + b\sqrt{6},$$

where $x, y, a, b \in \mathbb{Q}$. Considering this as a vector space, this has basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, and so the extension has degree 4.

It would only make sense to adjoin elements to fields that are actually roots of polynomials. As such, we introduce the following notion.

Definition 3.6. Given an extension F' of F, we say that $\alpha \in F'$ is **algebraic** if there exists a nonconstant polynomial $p(x) \in F[x]$ satisfying $p(\alpha) = 0$.

For example, i is algebraic over $\mathbb{Q}$, since it is a root to $x^2 + 1$. We say that F' is an **algebraic extension** of F if every element of F' is algebraic over F. If $\alpha \in F$ is not algebraic, then it is called **transcendental**, and the corresponding extension is also transcendental. An example of a transcendental number over the integers would be π.

Before returning to polynomials, we'll first establish an important result regarding algebraic extensions.

Theorem 3.7. *Every finite extension F' of F is algebraic.*

Proof. Take any $\alpha \in F'$, and let $n = [F' : F]$. Note that any set of $n + 1$ elements in F' is linearly dependent, because the basis for F' has n elements. Hence, $\{1, \alpha, \dots \alpha^n\}$ is a linearly dependent set, so there exist $f_0, \dots f_n \in F$ such that

$$f_0 + f_1\alpha + \cdots + f_n\alpha^n = 0.$$

This is a polynomial in $F[x]$, meaning α is algebraic. □

We'll also need an important lemma, which introduces the concept of a **minimal polynomial**. Before this, however, we make the following clear.

Definition 3.8. A polynomial $f(x) \in F[x]$ is **irreducible** if it has no roots in F.

For example, $x^2 + 2$ is irreducible over $\mathbb{Q}$, and so is $x^2 + x + 1$.

Lemma 3.9. *If $\alpha \in F'$ is algebraic over F, then there exists a unique monic irreducible polynomial $p(x) \in F[x]$ of minimal degree such that $p(\alpha) = 0$. This polynomial will be denoted by $irr(\alpha, F)$.*

Proof. [2] Because α is algebraic, any polynomial $p(x) \in F[x]$ with α as a root can be factored into a product of irreducible polynomials in F. One of these polynomials must have α as a root. Hence, assume that p is irreducible and monic. Suppose now that there exists another monic irreducible polynomial $g(x)$, with $g(\alpha) = 0$. We have $\deg p(x) \leq \deg g(x)$. Hence, we may write

$$g(x) = p(x)q(x) + r(x) \iff g(\alpha) = p(\alpha)q(\alpha) + r(\alpha),$$

by the division algorithm. This, in turn, implies $r(\alpha) = 0$. However, the degree of r is less than the degree of p, contradicting minimality, which implies $r(x) \equiv 0$. Hence, $g(x) = p(x)r(x)$, meaning g is not irreducible. As such, p is unique. □

Next, let's analyze the relationship between an algebraic number, its minimal polynomial, and the corresponding finite extension given by adjoining said number to a field, in essence unifying what we introduced above.

Theorem 3.10. *Given a simple extension $F' = F(\alpha)$, where α is algebraic, let n be the degree of its minimal polynomial $irr(\alpha, F)$. Then, $|F' : F| = n$ i.e., the extension has degree n. This also implies that the extension is finite.*

Proof. Suppose we let

$$\operatorname{irr}(\alpha, F) = f_0 + f_1\alpha + \cdots + f_n\alpha^n = 0.$$

This implies that the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent. However, $A = \{1, \alpha, \cdots \alpha^{n-1}\}$ must be linearly independent, since the degree of the minimal polynomial is n. In other words, A spans F' with scalars over F, and since A has n elements, the extension has dimension n. □

Here are a few more short results. For proofs, refer to [2]

(1) Given algebraic numbers α and β, $\alpha \pm \beta$, $\alpha\beta$, and α/β are all algebraic.
(2) Given an extension F'/F, the set of elements in F' that are algebraic over F is called the **algebraic closure** of F in F'. This set is also a field. Note that, if we consider a set generated by any set of algebraic numbers, every element in the resulting generated set is also algebraic from (1), which gives insight as to how field extensions contain purely algebraic numbers.

Now, we return to polynomials. From what we just established, field extensions induce, in a sense, new roots. This was formalized by Kronecker.

Theorem 3.11. *(Kronecker) Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial over F. Then there exists a finite extension F' of F where $f(x)$ has a root.*

A relatively simple proof that uses *quotient rings* is presented in [1]. However, for our purposes, we need not introduce the notion of a quotient ring, so we'll leave the proof in the references.

Importantly, Kronecker's theorem shows that we can essentially adjoin roots to a field. Specifically, given an algebraic integer α that is a root of some polynomial in $F[x]$, the extension $F' = F(\alpha)$ is the result of adjoining the root of some polynomial to F. As such, we may say that polynomials induce algebraic extensions.

Specifically, if we can find an extension that contains one root of some polynomial, then we may factor said polynomial into a product of a linear term and a polynomial of smaller degree - for which we can again find some root. This process of root discovery allows us to factor the polynomial into the product of n linear terms, where the roots may or may not be within the ground field.

Definition 3.12. [3] Let k be a field and let $f \in k[X]$ be a polynomial of degree n. An extension K/k is called a **splitting field** if

$$f(x) = c\prod_{i=1}^{n}(X - \alpha_i),$$

for $\alpha_i \in K$ and $c \in k$.

Example 3.13. The splitting field of $\mathbb{R}$ is $\mathbb{C}$, by the Fundamental Theorem of Algebra.

Furthermore, note that the Fundamental Theorem of Algebra is equivalent to the statement that $\mathbb{C}$ is its own splitting field, or in other words **algebraically closed** (we'll use this terminology more in the next section). From here, we may begin to get a sense of why such fields are of importance.

We are finally ready to introduce the necessary machinery of Galois Theory to accomplish our proof.

4. Galois Extensions

Recall from the introduction that Galois Theory formalizes the interplay between groups and fields. Specifically, we associate certain types of algebraic field extensions called **Galois Extensions** to a **Galois Group**. We'll introduce each shortly. First, we build the necessary theory to define a Galois extension.

Definition 4.1. (Normality) We say that an extension K/k is a **normal extension** if K is a splitting field over k.

Note that this is just a difference in terminology. All normal extensions are simply splitting fields. Next, define a **simple root** of a polynomial as a root α of multiplicity 1. If this root has multiplicity > 1, then it is called a **multiple root**.

Definition 4.2. (Separability) Suppose K/k is a finite extension with $\alpha \in K$. Then α is **separable** over k if α is a *simple* root of $\mathrm{irr}(\alpha, F)$. If all $\alpha \in K$ are separable over k, then K is called a **separable extension** of k.

In this regard, we may also extend this definition to polynomials. Specifically, we say that a polynomial $f(x) \in K[x]$ is separable if all of its roots have multiplicity 1 in the splitting field.

Example 4.3. Consider the following few polynomials [4]:

(1) $f(x) = x^2 - x$ is separable over $\mathbb{R}[x]$ because it has roots $0, 1$.
(2) $f(x) = x^3 - 2$ is separable over $\mathbb{C}$ since it has distinct complex roots.
(3) However, $f(x) = x^3 - 2$ is *not* separable over $F_3[x]$ (i.e., the set of polynomials with integer coefficients modulo 3), since $f(x) = x^3 - 2 \equiv (x+1)^3$ over $F_3[x]$, which has multiple roots.

These examples make more clear the definition of separable extensions. Specifically, from [4],

Example 4.4. $\sqrt{2}$ and $\sqrt{3}$ are both separable over $\mathbb{Q}$, since their minimal polynomials $x^2 - 2$ and $x^2 - 3$ have distinct roots over $\mathbb{Q}$. Note that this implies that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is separable.

If we try to test extensions of, say, $\mathbb{Q}$, we find that it is difficult to actually construct an extension that is not separable. As it turns out, separability is often a nice consequence of a certain property of a field.

Definition 4.5. Suppose (1) is the multiplicative identity of a field. A field F has **characteristic** n if n is the least positive integer such that $(n)(1) = 0$ in F. If no n exists, then we say that F has characteristic 0.

Note that $\mathbb{R}$ $\mathbb{Q}$, and $\mathbb{C}$ all have characteristic 0. The field F_2 has characteristic 2, since $1+1 \equiv 0+0 \equiv 0 \pmod 2$. Similarly, all fields of the form $F_p = \{0, 1, \cdots p-1\}$ have characteristic p.

Theorem 4.6. *In general, we have the following:*

(1) The characteristic of any field is either 0 *or prime.*
(2) Any extension of a field of characteristic 0 *must be separable. Specifically, all extensions of* $\mathbb{Q}, \mathbb{Z},$ *or* $\mathbb{R}$ *are separable.*

While not obvious why separability is of importance just yet, we'll also need one more theorem, called the **Primitive Element Theorem**. However, before proving this theorem, we will need the following lemma.

Lemma 4.7 (number of automorphisms fixing a ground field)**.** *Suppose K/F is a finite separable field extension. Then the number of automorphisms of K fixing F is equal to the degree $|K : F|$.*

The proof of this lemma is quite involved. Consult [5] for a detailed explanation.

Theorem 4.8 (Primitive Element Theorem)**.** *If K is a finite separable extension of F, then K is a simple extension. In other words, $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. We'll show that if $K = F(\alpha, \beta)$, then $K = F(\gamma)$. Any more variables, and we simply induct down.

Clearly, we must have $\gamma = \alpha + c\beta$ for some $c \in F$, since $F(\alpha + c\beta) \subset F(\alpha, \beta)$. Now, let $|F(\alpha, \beta) : F| = n$. Now, from Lemma 4.7, are n distinct automorphisms $\sigma_1, \ldots \sigma_n$ that fix F.

Claim: There exists $c > 0$ such that $\sigma_1(\alpha + c\beta), \ldots \sigma_n(\alpha + c\beta)$ are distinct.

To see this, consider

$$p(x) = \prod_{i<j}(\sigma_i(\alpha + x\beta) - \sigma_j(\alpha + x\beta)).$$

Note that this is not zero unless $\sigma_i(\beta) = \sigma_j(\beta)$ and $\sigma_i(\alpha) = \sigma_j(\beta)$. However, as α, β, and F span K, it follows that $\sigma_i = \sigma_j$, which cannot be true.

Hence, for some c, $\sigma_i(\alpha + c\beta) - \sigma_j(\alpha + c\beta) \neq 0$ for all pairs (i, j). It follows that $\sigma_i(\alpha + c\beta)$ is distinct for all $1 \leq i \leq n$, meaning that there are n distinct automorphisms that fix F over $F(\alpha + c\beta)$. However, this implies that $|F(\alpha + c\beta) : F| = n$, which means $F(\alpha + c\beta) \equiv F(\alpha, \beta)$, as desired. □

Finally,

Definition 4.9. A **Galois Extension** of F is a finite, separable, normal extension.

In other words, any Galois extension K over F satisfies the following properties:

(1) The number of automorphisms over K fixing F is equal to $|K : F|$.
(2) K is a splitting field over F, and moreover every algebraic number in K is a simple root of its minimal polynomial.

5. Galois Groups

In the previous section, we discussed automorphisms of field extensions, specifically, those that fixed their ground field. It turns out that these extensions have a very special name.

Definition 5.1. If K is a Galois Extension of F, then the **Galois Group** of K over F is equal to the set of automorphisms over K that fix F. This is denoted as $\mathrm{Gal}(K/F)$.

In a similar manner, it makes sense to "go backwards". Essentially, given a set of automorphisms H, we denote by K^H as the subfield of K that is fixed by H. In the case of a Galois group, we have that $\mathrm{Gal}(K/K^H) = H$. This notation will show up in later definitions, which is why we introduce it here.

Moreover, from **Lemma 4.7**, $|\mathrm{Gal}(K/F)| = |K : F|$. We also have the following lemma, where a proof can be found in [2]:

Lemma 5.2. *Suppose $F \subset E \subset K$ with K Galois over F (i.e., K/F is a Galois extension). Then,*

1. *K is galois over E, and Gal$(K/E) \subset$ Gal(K/F). Note that as Gal(K/E) is a group, the latter is actually a subgroup of the former.*
2. *If H is a subgroup of Gal(K/F), then $E = K^H$ satisfies $F \subset E \subset K$. Recall also that we must have Gal$(K/E) = H$.*

Since we have dealt extensively with polynomials, it also makes sense to define the **Galois Group for polynomials**. Specifically,

Definition 5.3. Let f be irreducible over F and K be the splitting field of F. Then, K is Galois over F, and the group $\text{Gal}(K/F)$ called the **Galois Group of the polynomial**.

In other words, if we take the splitting field of some polynomial, then consider the Galois Group of said splitting field over the ground field, we are left with the Galois Group of the polynomial.

Now consider some arbitrary automorphism σ in $\text{Gal}(K/F)$. If we consider some $f \in K[x]$ with roots $\alpha_1, \dots \alpha_n$, then

$$\sigma(f) = \sum_{i=0}^{n} f_i(\sigma(x))^i.$$

In other words, for any root α_i, $\sigma(\alpha_i)$ is also a root. Hence, σ must permute the roots $\{\alpha_1, \cdots \alpha_n\}$.

Now, we are finally able to discuss the **Fundamental Theorem of Galois Theory**.

6. The Fundamental Theorem of Galois Theory

Pretty much all of the fundamental results of Galois Theory can be united into a singular theorem, which is as follows:

Theorem 6.1 (Fundamental Theorem of Galois Theory [2])**.** *Let K be a Galois extension of F with Galois group $G =$ Gal(K/F). Then, for each intermediate field $K \subset E \subset F$, let $\tau(E)$ be the subgroup of G fixing E. Then:*

1. *τ is a bijection between intermediate fields containing F and subgroups of G - in other words, we may biject some subgroup of G to some intermediate field of K (recall that an intermediate field is a subfield of K that contains F).*
2. *If H is a subgroup of G and $E = K^H$, then $\tau(E) = H$. Hence, the bijection described above maps E to H.*
3. *$|G| = |K : F|$*
4. *$|E : F| = |G : \tau(E)|$. That is, the degree of the intermediate field extension is equal to the index of the corresponding subgroup (in this case, $\tau(E)$) in the Galois group.*
5. *E is Galois over F if and only if $\tau(E)$ is a normal subgroup of G. In this case,*
$$\text{Gal}(E/F) \cong G/\tau(E) \cong \text{Gal}(K/F)/\text{Gal}(K/E).$$

The first part of the theorem is an excellent contextualization of the interplay between groups and fields. Here, we are saying that there is a fixed function τ such that we may map any subgroup of G to any intermediate field E. Note that when $E = K^H$, E is the subfield of K fixed by H, so $\tau(E) = H$.

Next, we recall that $|G| = |K : F|$ by Lemma 4.7, and (4) is simply an extension of 3 to a more general case.

Lastly, (5) follows from the First isomorphism theorem, discussed in section 2. Note that the result in (4) follows from the left-hand isomorphism in (5)

While we won't need (5) here, we'll present a toy example that illustrates the fundamental results of Galois Theory by relating automorphism groups to fixed intermediate fields, from [2].

Example 6.2. Consider the group $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that this is a Galois extension since $\mathbb{Q}$ has characteristic 0. Next, note that $|Q(\sqrt{2}, \sqrt{3}) : \mathbb{Q}|$ has degree 4, since $|Q(\sqrt{2}) : Q| = 2$ (as it has minimal polynomial $x^2 - 2$), and $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$, which is also a degree 2 extension over $\mathbb{Q}(\sqrt{2})$.

Hence, we would expect $\mathrm{Gal}(K/\mathbb{Q})$ to have degree 4. Indeed, let's enumerate them:

$$\sigma_1 : \sqrt{2} \to \sqrt{2}, \qquad \sqrt{3} \to \sqrt{3}$$
$$\sigma_2 : \sqrt{2} \to -\sqrt{2}, \qquad \sqrt{3} \to -\sqrt{3}$$
$$\sigma_3 : \sqrt{2} \to -\sqrt{2}, \qquad \sqrt{3} \to \sqrt{3}$$
$$\sigma_4 : \sqrt{2} \to \sqrt{2}, \qquad \sqrt{3} \to -\sqrt{3}$$

Now, note that $\sigma_2 = \sigma_3 \circ \sigma_4$, so if we let $\sigma_1 = e$, the identity, $\sigma_3 = \sigma$, and $\sigma_4 = \tau$, then $\sigma_2 = \sigma\tau$. Hence, the group representation is $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. Moreover, note that each element has order 2.

Next, let's list subgroups, and their corresponding fixed fields:

(1) If we let $H = \{1\}$, then the fixed field is K.
(2) If we let $H = \{1, \sigma\}$, then the fixed field is $\mathbb{Q}(\sqrt{3})$
(3) Similarly, if we let $H = \{1, \tau\}$, then the fixed field is $\mathbb{Q}(\sqrt{2})$.
(4) Lastly, let us consider $H = \{1, \sigma\tau\}$. This fixes neither $\sqrt{2}$ nor $\sqrt{3}$. However, note that $\sqrt{6} = (-\sqrt{2})(-\sqrt{3})$, so $\mathbb{Q}(\sqrt{6})$ is fixed, which is an extension of order 2 over $\mathbb{Q}$ as expected.

The above example illustrates the relationship between Galois groups and intermediate Galois extensions, which will be useful in providing proof for the Fundamental Theorem of Algebra.

7. The Fundamental Theorem of Algebra

Theorem 7.1 (Fundamental Theorem of Algebra)**.** *Every polynomial $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

Before we begin the proof, let's write this in the language of Galois Theory. If we strictly consider polynomials $f \in \mathbb{C}[x]$ and their roots, we know that there exists some extension of that contains all of the roots of f. However, if f has a root r in $\mathbb{C}$, then $g(x) = f(x)/(x - r)$ is also a polynomial in $\mathbb{C}$. By the hypothesis, this must also have a root in $\mathbb{C}$, and so on. Hence, every root in f must be in $\mathbb{C}$.

In other words, if we consider a Galois extension K of $\mathbb{C}$, it must be $\mathbb{C}$ itself. This is what we will prove.

Proof. Before we look at extensions of $\mathbb{C}$, let's first look at extensions of $\mathbb{R}$. Specifically, let K be a Galois extension of $\mathbb{R}$ satisfying $|K : \mathbb{R}| = q$, where q is odd.

Because K is Galois and finite, it is also a simple extension, from the Primitive Element Theorem.

Hence, we may write $K = R(\alpha)$ for some algebraic α. It follows that the minimal polynomial of α has odd degree q. Write

$$\operatorname{irr}(\alpha, \mathbb{R}) = a_q x^q + \cdots + a_0.$$

If we take $x \to -\infty$, this polynomial tends to $-\infty$ since x^q is negative. On the other hand, as $x \to \infty$, $\operatorname{irr}(\alpha, \mathbb{R}) \to \infty$. Since the polynomial is continuous, some $x \in \mathbb{R}$ is a root. However, this means that the polynomial is not irreducible over $\mathbb{R}$, a contradiction.

Hence, there exist no odd degree extensions over $\mathbb{R}$. We now turn back to extensions of $\mathbb{C}$. Suppose K is a Galois extension of $\mathbb{C}$. We may write $K = \mathbb{C}(\alpha)$. We note that if K has degree 2, then α is the root of a quadratic, but by the quadratic formula, the roots of any quadratic are necessarily complex, which means that the polynomial is not irreducible over $\mathbb{C}$. Hence, K cannot have degree 2.

Now, we turn back to $\mathbb{R}$. Let K be the Galois extension satisfying $|K : \mathbb{R}| = 2^m q$, where $m > 0$ and $\gcd(q, 2) = 1$. Then, the Galois group $G = \operatorname{Gal}(K/\mathbb{R})$ has order $2^m q$. Now recall **Sylow's Theorem** (Theorem 2.9). From this, we note that G necessarily has a subgroup G' of order 2^m.

However, recall that Galois Theory allows us to relate subgroups of the Galois group to intermediate fields E satisfying $\mathbb{R} \subset E \subset K$. Specifically, from part (4) of the Fundamental Theorem of Galois Theory, we have

$$|E : \mathbb{R}| = |G : \tau(E)| = q,$$

because $G/\tau(E)$ has order $\frac{2^m q}{2^m}$ by Lagrange's Theorem.

However, as q is odd, and no odd degree extensions exist over $\mathbb{R}$, we must have $q = 1$, i.e., $E = \mathbb{R}$. Hence, $|K : \mathbb{R}| = 2^m$. It follows that $|K : \mathbb{C}| = 2^{m-1}$. If $m > 1$, then by Sylow again, an intermediate field extension must exist of degree 2. However, we have already established that this is impossible. Hence, $m = 1$, meaning $K = \mathbb{C}$, as desired. □

This proof illustrates the power of Galois Theory in relating groups and fields. Most importantly, we are able to relate respective *degrees* of extensions to orders of quotient groups using the notion of automorphism groups. We have used these relationships to prove the Fundamental Theorem of Algebra, but Galois Theory can also be used to verify a multitude of other seemingly unrelated problems. For example, Galois Theory was famously used to prove that there exists no closed form solution to any polynomial of degree greater than 4, which came from

8. Acknowledgements

I would like to thank my mentor, Aadrita Laha, for guiding me on topic selection and for her invaluable help in supplying resources and other relevant information in my writing of this paper. I would also like to thank Prof. Peter May for graciously inviting me to participate in the UChicago Math REU and providing me an opportunity to learn lots of awesome math.

9. Bibliography

References

[1] https://kconrad.math.uconn.edu/blurbs/galoistheory/rootirred.pdf

[2] Benjamin Fine, Peter Rosenberger The Fundamental Theorem of Algebra

[3] M. Pavan Murthy et. al Galois Theory Tata Institute of Fundamental Research, 1965

[4] https://kconrad.math.uconn.edu/blurbs/galoistheory/separable1.pdf Separability fundamental-galois https://www.math.purdue.edu/ jlipman/553/Galois.pdf The Fundamental Theorem of Galois Theory

[5] https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorr.pdf The Galois Correspondence