The Galois correspondence of covering spaces and the analogy to Galois theory

Leonardo Finzi

Acknowledgments

I would like to thank the Painter family for their generous endowment to the University of Pittsburgh mathematics department for the Painter Fellowship and to the University of Pittsburgh mathematics department for selecting me as a 2025 Painter fellow. I would also like to thank my mentors Professor Carl Wang-Erickson and Dr. Mohamed Moakher for selecting the topics of my fellowship and guiding me through them, along with their abundance of help in editing my exposition and their assistance with the proofs.

Contents

1 Introduction **1**

2 A Recollection of Galois Theory **2**

3 Algebraic Topology **7**
3.1 Path Homotopy 7
3.2 The Fundamental Group 9
3.3 Covering Spaces 11

4 The Galois Correspondence of Covering Spaces **16**
4.1 Orbit Categories 16
4.2 The Correspondence 17

5 Concluding Remarks **25**

References **27**

1 Introduction

Given a certain type of mathematical object, it is nice to know if there is a way to describe a maximal object and if that maximal object is unique. Having a maximal object, as well as a minimal object, means that it is possible to determine intermediate objects. With this comes some sort of underlying structure, and if it's nice enough, some sort of underlying order of the objects.

A good example is in Galois theory, where the "largeness" of an intermediate field in a Galois extension can be attributed to how small a certain subgroup of the Galois group is. What is particularly nice is in Galois theory we indeed have a concept of minimal and maximal fields, uniqueness of these fields, and all intermediate fields are easy to find. Specifically, given a Galois extension L/K, we have the following bijective correspondence:

$$\begin{array}{ccc} \{\text{intermediate fields of } L/K\} & \longleftrightarrow & \{\text{subgroups of } \mathrm{Gal}(L/K)\} \\ F & \longmapsto & \mathrm{Gal}(L/F) \\ L^H & \longmapsfrom & H \end{array}$$

The novelty and utility of Galois theory comes from how we can take the generally difficult problem of finding subfields of a Galois extension, and transform it into a group theory problem, of which the latter is much easier.

This bijective correspondence, and in particular a way to discuss minimality and maximality, is analogously present in algebraic topology. If we concern ourselves with certain conditions on a topological space X, and a total space E made of copies of certain subsets of X with a covering map from E to X, we can discuss a type of minimality and maximality of E. We call this pair of a space and map a covering space of X. From this we get a nice identification: Given a covering space of X, we can correspond it to a subgroup of the fundamental group $\pi_1(X, x)$, for some $x \in X$. In addition, we get a Galois-type theory for covering spaces and the fundamental group:

$$\begin{array}{ccc} \{\text{pointed covers of } X\} & \longleftrightarrow & \{\text{subgroups of } \pi_1(X,x)\} \\ Y \xrightarrow{p} X & \longmapsto & p_*(\pi_1(Y,y)) \\ ? & \longmapsfrom & H \end{array}$$

The forward direction arises from an understanding of π_1 as a functor, but as hinted above, it is not obvious if there exists a (two-sided) inverse.

Having covering spaces correspond to subgroups is somewhat interesting, but hav-

ing them correspond *exactly* would be as extraordinary of a result as in Galois theory. It would mean that the problem of finding covering spaces of a space could be done group theoretically rather than purely topologically, of which the latter is significantly harder. We will show that the identification between pointed covers of X and subgroups of $\pi_1(X, x)$ is a bijection and that this bijection respects the order of covering spaces and preserves the structure. In addition, this bijection will classify all covering spaces and maps between covering spaces. Although classifying the objects is important, discussing these morphisms will enrich what we already know about group theory and field theory, and it will be possible to compare this theory in topology to Galois theory via an analogy.

This expository paper discusses the Galois correspondence of covering spaces, by providing exposition on necessary ideas in Galois theory and algebraic topology, proving that the above forward map is a bijection, and outlining the analogy to the Galois correspondence of fields. Section 2 gives an overview of Galois theory of fields to remind the reader of the Galois correspondence. Section 3 develops some of the theory of algebraic topology, and in particular, the fundamental group and covering spaces. Section 4 proves the bijective correspondence using the category of orbits, and provides examples of using the correspondence in both directions. Section 5 will explicitly outline this analogy using an analogy table.

2 A Recollection of Galois Theory

This section will review Galois theory up to what is referred to as the Galois correspondence to best understand the importance of the main result to be best understood. If Galois theory is very unfamiliar, a good additional reference would be [1].

A field $(K, +, \cdot)$ is an algebraic structure where $(K, +)$ is an abelian group, $(K/\{0\}, \cdot)$ is a group, $0 \neq 1$, distribution over multiplication and addition holds, and multiplication by 0 yields 0. If the addition and multiplication are unambiguous, for simplicity, we just write K is a field. Examples of fields include $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}/p\mathbb{Z}$, for a prime p. If a field $(L, +, \cdot)$ contains a subset K such that $(K, +, \cdot)$ is also a field, then we say that K is a *subfield* and that L is a *field extension* of K, denoted L/K. We call $[L : K] = \dim_K L$ the *degree* of the extension L/K. If the degree of L/K is finite, then we say L/K is a *finite extension*. The degree of any field extension is multiplicative, i.e., given fields $K \subseteq F \subseteq L$, $[L : K] = [L : F][F : K]$.

We can also build larger fields from a base field in addition to deducing subfields of an extension. Recall that a number α is *algebraic* over a field K if there is a

polynomial with coefficients in K that has root α.[1] If K is a field and α is an algebraic number, then $K(\alpha) = \{a + b\alpha \mid a, b \in K\}$ is a vector space over K, and in particular, is the smallest field containing K and α. We say $K(\alpha)/K$ is an *algebraic field extension*. We can also *adjoin* more algebraic numbers to K to form larger algebraic field extensions. Examples of algebraic extensions are $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{R}(i)$. Note that if the algebraic number adjoined to a field is in the field, then the field extension is trivial. For example, $\mathbb{Q}(3) = \mathbb{Q}$ since $3 \in \mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, 3\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ since $3\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Definition 2.1. Let K be a field and $p(x) \in K[x]$ a polynomial. We say $p(x)$ is **reducible** over K if $p(x) = f(x)g(x)$, where $f(x), g(x) \in K[x]$ with degree at least 1. If a polynomial is not reducible over K, then it is **irreducible** over K. If α is algebraic over K, then a **minimal polynomial** of α over K is a monic, irreducible polynomial $p(x) \in K[x]$ which has a root α.

Although minimal polynomials were defined ambiguously, it should be noted that a minimal polynomial of α is unique. Because they are unique, we can use them to compute the degree of an algebraic extension. If K is a field and α is algebraic over K with n-degree minimal polynomial $p(x)$, then $[K(\alpha) : K] = n$, since $K(\alpha)$ is generated as a K-vector space by the basis $\{1, \alpha, ..., \alpha^{n-1}\}$. For example, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

We can view irreducible polynomials over K in a different way. We can write any polynomial as $p(x) = \prod_{i=1}^{n}(x - r_i) \in K[x]$, where each $r_i \in \bar{K}$, the algebraic closure of K, is a root of $p(x)$ with degree n. If we adjoin a root r_1 of $p(x)$ to K, then we can factor out the $x - r_1$ term from $p(x)$, and we are left with a polynomial $p_1(x) \in K(r_1)$ and degree $n-1$.[2] We can adjoin another root of $p(x)$, say r_2, to factor out a linear term of $p_1(x)$, and we are left with $p_2(x) \in K(r_1, r_2)$ and degree $n - 2$. Continuing in this way, we can completely split $p(x)$ into n linear terms in the field $K(r_1, ..., r_n)$. Though, it is possible that we may have added too many "copies" of a root, so to speak. For example, in $\mathbb{Q}$, i has minimal polynomial $x^2 + 1$. The roots of $x^2 + 1$ are $\pm i$, so we may think that $x^2 + 1$ will first split completely in $\mathbb{Q}(i, -i)$. But $-i = (-1)i \in \mathbb{Q}(i)$, so $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$. This notion of splitting is fundamental to Galois theory, and is expressed explicitly in the following definition.

Definition 2.2. Let K be a field. If L is a field extension of K such that there exists an irreducible polynomial $p(x)$ that can be factored into linear terms in $L[x]$, and

[1] This α can be in K, but it does not have to be!

[2] A non-obvious part of this discussion is showing that $p_1(x) \in K(r_1)$. To see this, one has to utilize symmetric polynomials, which are necessary to develop Galois theory properly, but are not discussed here.

there is no intermediate field in which this is possible, then L is a **splitting field** of $p(x)$. In such cases, we say the extension L/K is **normal**.

From what was previously discussed, any polynomial over a field K has a splitting field, namely K adjoined with all the roots of the polynomial. Looking back at the example of x^2+1, although x^2+1 splits completely into linear terms in $\mathbb{Q}(i,\sqrt{5})$, $\mathbb{Q}(i)$ is the splitting field of x^2+1 over $\mathbb{Q}$ because $\mathbb{Q}(i) \subset \mathbb{Q}(i,\sqrt{5})$.

Definition 2.3. Let L/K be a field extension. If every element of L has a minimal polynomial over K such that the roots of the minimal polynomial are distinct, then we say the extension L/K is **separable**.

Combining these two concepts, we arrive at a crucial concept for Galois theory.

Definition 2.4. If an extension L/K is normal and separable, we say L/K is **Galois**.

Example. Consider the extension $\mathbb{Q} \subset \mathbb{Q}(i,\sqrt[4]{2})$ and the subfields $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(i,\sqrt[4]{2})$. The minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is x^4-2, which has roots $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. $\pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$, but $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$. Though, all four roots are in $\mathbb{Q}(i,\sqrt[4]{2})$, since both $\sqrt[4]{2}$ and i must be added so that x^4-2 can split. There is also no smaller field where x^4-2 splits completely. Thus, the extension is normal and separable, since all four roots are distinct, so $\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q}$ is Galois.

To get to the heart of Galois theory, there is one more concept we must recall. For a field L, we call an isomorphism $\sigma : L \to L$ an **automorphism** of L. Automorphisms of L, since they are bijective, can be thought of as permutations of elements of L. It turns out that when conditions are nice enough, the distinct automorphisms of a field are relatively easy to compute.

Definition 2.5. Let L/K be Galois. Define the **Galois group** by

$$\mathrm{Gal}(L/K) := \{\sigma : L \to L \mid \sigma(k) = k,\ \forall k \in K\}.$$

That is, the Galois group is the group of automorphisms on L that act as the identity when restricted to elements of K. The field that is fixed by an element of $\mathrm{Gal}(L/K)$ is called a **fixed field**.

The Galois group, as described, is a group under function composition. Using what we know about Galois extensions, we can compute the Galois group for a given extension. For example, if $K(\alpha)/K$ is Galois, then every element in $K(\alpha)$ is a K-linear combination of $\{1,\alpha,...,\alpha^n\}$. So, if $\sigma \in \mathrm{Gal}(L/K)$, then for $x \in K(\alpha)$, $\sigma(x) = \sigma(a_0+a_1\alpha+...+a_{n-1}\alpha^{n-1}) = a_0+a_1\sigma(\alpha)+...+a_{n-1}\sigma(\alpha)^{n-1}$, since σ fixes elements

of K and is a homomorphism. Hence, each σ is defined on where it takes α. In particular, the automorphisms in the Galois group permute the roots of the minimal polynomials over K of the adjoined elements. In addition, it can be shown that $|\mathrm{Gal}(L/K)| = [L : K]$, which, again, can be easily computed by looking at the degree of minimal polynomials.

Example. Consider again $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt[4]{2})$. The automorphisms of $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ are completely determined by where they take i and $\sqrt[4]{2}$. In particular, since $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8$, we have 8 automorphisms:

$$\sigma_{1-} : i \mapsto i, \quad \sigma_{2-} : i \mapsto -i$$

$$\sigma_{-1} : \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad \sigma_{-2} : \sqrt[4]{2}, \mapsto i\sqrt[4]{2} \quad \sigma_{-3} : \sqrt[4]{2}, \mapsto -\sqrt[4]{2} \quad \sigma_{-4} : \sqrt[4]{2} \mapsto -i\sqrt[4]{2},$$

In fact, these automorphisms are generated by σ_{12} and σ_{21}. These can be thought of as a rotation by 180 degrees (or a flip) of a square and a rotation by 90 degrees of a square, respectively. So

$$\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}) = \langle \sigma_{12}, \sigma_{21} \rangle \cong D_4 = \langle s, r \mid s^2 = r^4 = e \rangle.$$

Proposition 2.6. *Let L/K be Galois. Let G be a subgroup of Gal(L/K). Then the field fixed by G is an intermediate subfield of the extension L/K. We denote this field L^G.*

Given an intermediate field $K \subseteq F \subseteq L$, where L/K is Galois, what can we say about the extension L/F? Since L/K is separable, moving to an extension of K does not change separability in the higher field, so L/F is still separable. Since L/K is normal, then some minimal polynomial $p(x)$ splits completely in L. This polynomial may split more in F, but L will still split it completely. So L/F is also normal and hence Galois, and $\mathrm{Gal}(L/F)$ is sensible to write. From the definition of the Galois group, $\mathrm{Gal}(L/F)$ is a subgroup of $\mathrm{Gal}(L/K)$.

Given this and Proposition 2.6, we have a correspondence called the *Galois correspondence*. It says subgroups of $\mathrm{Gal}(L/K)$ correspond to fixed fields, and intermediate fields of L/K correspond to subgroups of $\mathrm{Gal}(L/K)$. Theorem 2.7 tells us that this correspondence is bijective.

Theorem 2.7 (The Fundamental Theorem of Galois Theory)**.** *Let L/K be Galois and let $K \subseteq F \subseteq L$.*

1. *There is a unique subgroup G of Gal(L/K) such that $F = L^G$.*

2. *L/F is a normal extension if and only if the corresponding G is a normal subgroup of $Gal(L/K)$.*

3. *For the corresponding G, $[L : F] = |G|$.*

In other words, understanding subfields of a Galois extension boils down to finding subgroups of the Galois group, and vice-versa. Although the correspondence is bijective, there is a slight difference in inclusion. Since $L = L^{\{id\}}$ and $K = L^{\mathrm{Gal}(L/K)}$, the relationship is *inclusion-reversing*, meaning $H \subseteq H'$ implies $L^{H'} \subseteq L^H$. In other words, the smaller a subgroup of the Galois group is, the larger the corresponding intermediate field, and the larger a subgroup of the Galois group is, the smaller the corresponding intermediate field is.

To show the power of this theorem, consider the following example:

Example. Earlier, we computed the Galois group of the Galois extension $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$, which was $D_4 = \langle s, r \mid s^2 = r^4 = e \rangle$, the group of symmetries of a square. To find the subfields of the Galois extension, we can look at the subgroups of $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ as shown in Figure 1.

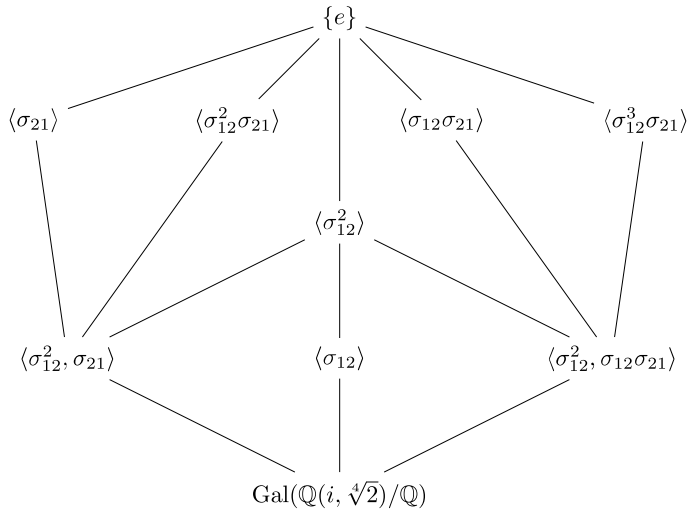


Figure 1: The subgroups of $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}) \cong D_4$.

Understanding the structure of $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$, we can now write the intermediate fields of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ in the exact same way (reversing the inclusion), as shown in Figure 2. There are many techniques to compute the fixed fields, but a good way is to see which combinations of roots of the minimal polynomial is fixed by the generating automorphisms. For example, $\sigma_{12} \circ \sigma_{21}(\sqrt[4]{2} + i\sqrt[4]{2}) = i\sqrt[4]{2} + \sqrt[4]{2}$, so $\langle \sigma_{12}\sigma_{21} \rangle$ fixes $(1+i)\sqrt[4]{2}$ and thus $\mathbb{Q}(i, \sqrt[4]{2})^{\langle \sigma_{12}\sigma_{21} \rangle} = \mathbb{Q}((1+i)\sqrt[4]{2})$.

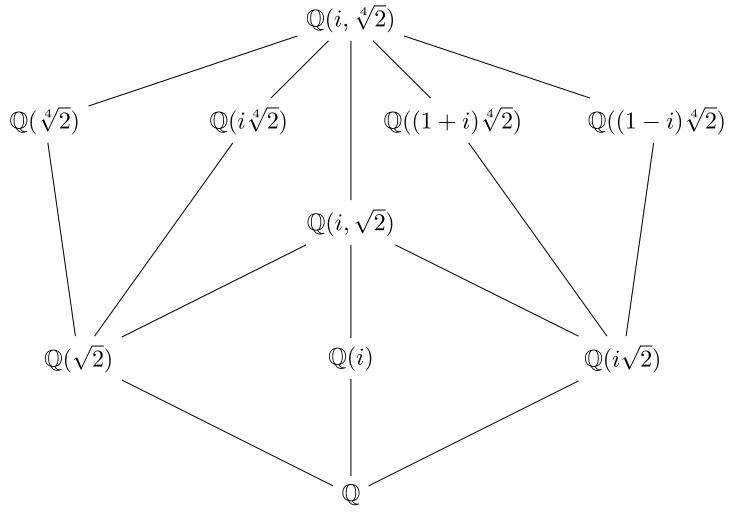


Figure 2: The subfields of the Galois extension $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt[4]{2})$.

Overall, Galois theory allows us to understand the structure of certain types of field extensions, namely Galois extensions, and assures us that their structure is the structure of the Galois group. Therefore, the problem of field structure boils down to a problem of group structure, whose structure is much easier to understand. As we will see, a similar thing happens in algebraic topology.

3 Algebraic Topology

This section will be a quick overview of the key concepts of algebraic topology needed for our main result.

3.1 Path Homotopy

Definition 3.1. Let $I = [0, 1]$. We say a continuous map $\alpha : I \to X$ is a **path** with **endpoints** $\alpha(0), \alpha(1)$ called the **initial** and **end/final** points, respectively. If $\alpha(0) = \alpha(1) = a$, then we say α is a **loop** with base point $a \in X$.

Given a topological space X and points $a, b \in X$, we denote the **space of paths** in X between a and b as $\Omega(X, a, b) := \{\alpha : I \to X \mid \alpha \text{ continuous}, \ \alpha(0) = a, \ \alpha(1) = b\}$. There are some simple operations we can define on the space of paths. We can define

a product of paths $* : \Omega(X, a, b) \times \Omega(X, b, c) \to \Omega(X, a, c)$ where

$$\alpha * \beta(t) = \begin{cases} \alpha(2t), & \text{if } 0 \leq t \leq 1/2 \\ \beta(2t), & \text{if } 1/2 \leq t \leq 1 \end{cases} .$$

We can also define an inversion $i : \Omega(X, a, b) \to \Omega(X, b, a)$ with $i(\alpha)(t) = \alpha(1 - t)$.

Definition 3.2. Let $\alpha, \beta \in \Omega(X, a, b)$. We say α, β are **path homotopic** if there is a continuous map $F : I \times I \to X$ such that $F(s, 0) = \alpha(t), F(s, 1) = \beta(t), \forall t \in I$, and $F(0, t) = a, F(1, t) = b, \forall s \in I$. We call such an F a **path homotopy** between a, b. Finally, "being path homotopic" is an equivalence relation, so we have symmetry, reflexivity, and transitivity on the path homotopy relation.

In other words, two paths that have the same initial and final points are path homotopic if one path can be continuously deformed into the other. In addition, for any fixed value $\overline{t} \in I$, $F(s, \overline{t}) \in \Omega(X, a, b)$ and is path homotopic to both α and β. These remarks can be made clearer by an example.

Example. Consider the continuous functions $f, g : I \to I$ with $f(s) = s^2$, $g(s) = \sqrt{s}$. So, $f, g \in \Omega(I, 0, 1)$. Define a continuous function $F : I \times I \to I$ by $F(s, t) = (1 - t)f(s) + tg(s)$. We have that $F(s, 0) = s^2$, $F(s, 1) = \sqrt{s}$, $F(0, t) = 0$, and $F(1, t) = 1$, so f and g are path homotopic.

In Figure 3, f (red) and g (blue) are plotted, with various s-time steps of F in green to show how f continuously transforms into g. As described before, each of the green curves are also continuous paths from $(0, 0)$ to $(1, 1)$ and are path homotopic to f and g.

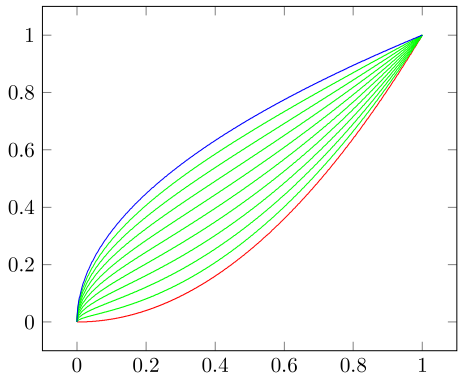


Figure 3: The graphs f, g plotted on $I \times I$, with various t-time steps of the path homotopy F.

Though, general path homotopy is not quite the notion we will use. Instead, we will restrict our focus to *loops* that are homotopic. It will turn out that homotopy classes of loops can be quite useful in describing topological spaces.

3.2 The Fundamental Group

Definition 3.3. The group $\pi_1(X, a) = \Omega(X, a, a)/\sim$, where $a \sim b$ if and only if a, b are path homotopic, is called the **fundamental group** of X with base point a.[3]

Although it was defined as such, it is important to verify that the fundamental group is actually a group.

Proposition 3.4. *The set $\pi_1(X, a)$ has a group structure under the equivalence class operation $[\alpha][\beta] = [\alpha * \beta]$.*

A full proof of this statement is rather explicit[4] since it involves coming up with specific path homotopies. That being said, we can briefly describe why this is true. If $\alpha, \beta \in \Omega(X, a, a)$, we know that $\alpha * \beta \in \Omega(X, a, a)$, so π_1 is closed under the given operation. Although $*$ is not associative generally, $*$ is associative up to path homotopy, which is exactly the condition we want. Finally, the constant loop $1_a \in \Omega(X, a, a)$, $1_a * \alpha \sim \alpha * 1_a \sim \alpha$, and $\alpha * i(\alpha) \sim 1_a$. Hence, π_1 is indeed a group.

Sometimes topological spaces admit a trivial fundamental group, which means that every loop is path homotopic to the constant loop at its basepoint. A space that is connected, or where the only sets that are open and closed are the empty set and the entire space, and admits a trivial fundamental group at any point is called *simply connected*. The following example is a good example of a simply connected space.

Example. Lets compute $\pi_1(\mathbb{R}, x)$, for any $x \in \mathbb{R}$. Visually, loops on the real line centered at a point $x \in \mathbb{R}$ look like segments based at x. Intuitively, it seems true that any two segments centered at the same point can be continuously transformed into one another. So the fundamental group should be trivial. Let's make this intuition explicit.

Fix $x \in \mathbb{R}$. Define $f : I \times I \to \mathbb{R}$ by $f(s, t) = (1 - t)s + tx$. Define $F : I \times I \to \mathbb{R}$ taking $F(s, t) = f(\alpha(s), t)$, where $\alpha \in \Omega(\mathbb{R}, x, x)$. Then

$$F(s,0) = f(\alpha(s), 0) = \alpha(s) \quad F(s,1) = f(\alpha(s), 1) = x$$
$$F(0,t) = f(\alpha(0), t) = f(x,t) = x \quad F(1,t) = f(\alpha(1), t) = f(x,t) = x,$$

[3]The notation π_1 implies that there exists notions of π_2, π_3, etc. There are higher (and lower) notions of homotopy groups, but they will not be discussed as they are not needed for the discussion of the fundamental group.

[4]For the explicit proof, see Propositions 11.4, 11.6 in [2, pp. 183–184, 184–185].

so we have that F is a path homotopy between the constant loop at x and α. Hence, for every $\alpha \in \Omega(\mathbb{R}, x, x)$, $\alpha \sim x$ and thus, for all $x \in \mathbb{R}$, $\pi_1(\mathbb{R}, x)$ is trivial, as we suspected.

There are also more interesting fundamental groups. The next example is a widespread example that could be found in most algebraic topology textbooks.

Example. Another good computation is finding the fundamental group of a circle. For now, we will describe this fundamental group visually. It is possible to show what this fundamental group is given the previous discussion,[5] but we will discuss a much nicer way to prove this later.

Imagine a circle and choose any point on the circle. To make things easier, imagine a unit circle and choose the point to be $x = (1, 0)$. What are the possible loops based at x that lie on the unit circle? The constant loop at x is one, one loop around the circle is another, two loops around the circle is another, three loops around the circle is another, etc. We call the number of winds a path takes around S^1 to be called the loop's *winding number*. Are there any other types of loops? Since the loop must stay along the circumference of the circle, once the loop leaves x, it must trace around the rest of the circle, or trace back the way it left x. In the latter option, a curved continuous segment is path homotopic to a straight segment, which in turn is path homotopic to the segment's base point (as shown in the previous example). So, if a loop winds around the circle, goes past x and retraces back to x, we have that the loop is homotopic to a loop that only winds around the circle some integer number of times. We must deal with this type of loop.

Take $\alpha, \beta \in \Omega(S^1, x, x)$ such that their winding numbers are n and m respectively, with $n < m$. Is it possible to continuously deform β into α? To do so, we need to transform the extraneous $m - n$ winds of β into the point x. This either requires a transformation that tears one of the winds to deform each strand into a point or a transformation deforming the wind towards the interior of the circle. The first transformation would be a discontinuous function and therefore not a path homotopy. For the second transformation to work, the loop has to exit the topological space, so the second transformation would also not be a path homotopy. So α and β are not path homotopic. Thus, each path homotopy class of loops in S^1 is defined only by it's winding number, i.e., $\pi_1(S^1, x) \cong \mathbb{Z}$.

If (for now) this isomorphism is taken as fact, we can use it to find the fundamental group of another important spaces using the following lemma.

[5]For this proof given what we know, see [3, pp. 8–9].

Lemma 3.5. *Let X, Y be topological spaces and $(a, b) \in X \times Y$. Then*

$$\pi_1(X \times Y, (a, b)) \cong \pi_1(X, a) \times \pi_1(Y, b).$$

Proof. The result descends from the map $f : \pi_1(X \times Y, (a, b)) \to \pi_1(X, a) \times \pi_1(Y, b)$ taking $[\alpha] = [(\alpha_1, \alpha_2)]] \mapsto [\alpha_1] \times [\alpha_2]$. □

Example. With the previous proposition now proved, we can find the fundamental group of a torus $\mathbb{T}$. We identify with a torus with two copies of a circle, i.e., $\mathbb{T} \cong S^1 \times S^1$. For some point $x = (x_1, x_2) \in \mathbb{T}$, we have the following calculation:

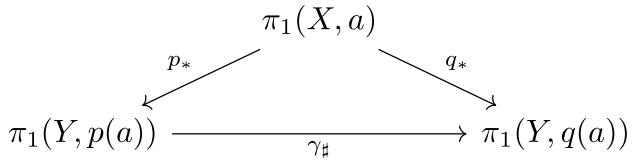
$$\pi_1(\mathbb{T}, x) \cong \pi_1(S^1 \times S^1, (x_1, x_2)) \cong \pi_1(S^1, x_1) \times \pi_1(S^1, x_2) \cong \mathbb{Z} \times \mathbb{Z}.$$

Thus, any loop homotopy class on a torus is uniquely defined by its winding number in two directions.

Finally, it is also useful to describe what maps between the fundamental groups of different spaces look like, as well as the fundamental groups at different base points of the same space.

If $f : X \to Y$ is a continuous mapping of topological spaces, then for every $x \in X$, we have a group homomorphism $\pi_1(f) : \pi_1(X, x) \to \pi_1(Y, f(x))$ which takes $\pi_1(f)([\alpha]) = [f\alpha]$. To keep notation simple, we write $f_* = \pi_1(f)$. In addition, if we have a path $\gamma \in \Omega(X, a, b)$, we have the group isomorphism $\gamma_\sharp : \pi_1(X, a) \to \pi_1(X, b)$ which takes $\gamma_\sharp[\alpha] = [i(\gamma) * \alpha * i(\gamma)]$. With these two mappings, we have the following important proposition:

Proposition 3.6. *Let $p, q : X \to Y$ be homotopic maps. The following diagram commutes:*



In this way, we can fully describe the relationship between the fundamental groups at different basepoints in the same space or in different spaces.

3.3 Covering Spaces

For this section and onwards, we will assume that the topological spaces we discuss are connected and locally path-connected. A space is *connected* if the only sets both

open and closed sets are the empty set and the entire space. A space is *locally path-connected* if every point has a path-connected neighborhood.

Definition 3.7. Let X be a topological space. We say a **covering space** of X is a **total space** E with a continuous **covering map** $p : E \to X$ such that for all $x \in X$, there is an open neighborhood $U \subset X$ such that $p^{-1}(U)$ is the disjoint union of open sets U_i and $p|_{U_i}$ is a homeomorphism for every U_i. We call such $U \subset X$ a **fundamental neighborhood**[6] of X.

In other words, given a space X, a covering space E is a space that is made of copies of the fundamental neighborhoods of X. It is also important to note that the covering map p is surjective. For notational sake, when we describe a covering space, which consists of a space and a map, we will just write the map. That is, we will say $p : E \to X$ is a cover or covering, understanding that E is the total space, X is the base space, and p is the covering map.

We can also describe covering spaces to be *pointed* or *unpointed*. The definition given of a covering space is the definition of an unpointed cover. A covering space is pointed when we also identify fixed basepoints $x \in X$ and $y \in Y$ such that $p(y) = x$. A pointed cover is useful when discussing the fundamental group, since we can track how a covering space changes loops at a certain basepoint.

Example. Consider the unit circle S^1. It can be identified with the set of complex numbers with modulus 1, so any point on S^1 can be written in the form $e^{2i\pi t}$. We claim that a covering space of S^1 is $p : \mathbb{R} \to S^1$, where $p(t) = e^{2i\pi t}$.

Choose $x \in S^1$. Since p is surjective, we can say, for some $(a, b) \subset \mathbb{R}$, that $x \in U = p(a, b) \subset S^1$. Then $p^{-1}(U) = \bigcup\{(a + n, b + n) \subset \mathbb{R} \mid n \in \mathbb{Z}\}$. We can choose a and b to be as close as we like, so if we choose $b - a < 1$, then each open set $(a + n, b + n)$ is disjoint from one another. Also, $p|_{(a+n,b+n)}$ is a homeomorphism for every $n \in \mathbb{Z}$, so $p : \mathbb{R} \to S^1$ is a covering space of S^1.

Given the definition of a covering space, it is useful to ask what happens when a path in a base space is lifted into the total space. For a covering space $p : E \to X$ and continuous map $f : Y \to X$ between topological spaces, a *lift* is a continuous map $g : Y \to E$ such that $g \circ p = f$. The following theorem is given without proof, but is important in determining when any map can lift. A nice proof for this is given in Theorem 13.18 in [2, pp. 227–228].

[6]Other names for fundamental neighborhoods include *admissible sets* and *elementary neighborhoods*.

Theorem 3.8. *Let $p : E \to X$ be a covering and let $f : Y \to X$ be a continuous map. Fix $y \in Y$, let $x \in X$, and choose $\tilde{x} \in p^{-1}(x)$. There exists a map $g : Y \to E$ with $g(y) = \tilde{x}$ and $p \circ g = f$ if and only if $f_*(\pi_1(Y, y)) \subset p_*(\pi_1(E, \tilde{x}))$.*

This theorem tells us that there is an issue of well-definedness of g. For such a g to be defined, it must be the case that loops based at $y \in Y$ must map onto loops in X that are pushed forward from loops based at $\tilde{x} \in E$, which is exactly the condition given.

The type of lift we will like for our discussion are lifts of paths. As is it turns out, paths are lifted extremely nicely. A proof for the following theorem can be found in [3, p. 22].

Theorem 3.9 (Unique Path Lifting)**.** *Let $p : E \to X$ be a covering. Let $x \in X$ and $e \in p^{-1}(x)$. A path $\alpha : I \to X$ with $\alpha(0) = x$ lifts uniquely to a path $\alpha_e : I \to E$ such that $\alpha_e(0) = e$ and $p \circ \alpha_e = \alpha$. In addition, if $\alpha, \beta : I \to X$ are homotopic paths that start at x, then they lift to homotopic paths $\alpha_e, \beta_e : I \to E$ that start at e, and in particular, $\alpha_e(1) = \beta_e(1)$.*

Example. We saw that $p : \mathbb{R} \to S^1$ is a covering, where $p(t) = e^{2i\pi t}$. Consider the points $1, -1 \in S^1$ and a path $\alpha \in \Omega(S^1, 1, -1)$ where α traces around the top of the circle. Since $0 \in p^{-1}(1)$ and $1/2 \in p^{-1}(-1)$, we can lift α uniquely to α_0, in this case, where α_0 is the segment from 0 to 1/2. Additionally, if we take $\beta \in \Omega(S^1, 1, -1)$ where β traces around the bottom of the circle, then $\alpha \neq \beta$ and α is homotopic to β. Theorem 3.9 also says that α_0, β_0 are homotopic.

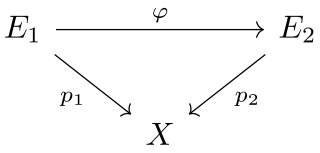
A notable corollary to unique path lifting is that $p_* : \pi_1(E, \tilde{x}) \to \pi_1(X, x)$ is injective. This is because if $p_*([\beta_1]) = p_*([\beta_2])$, then they must be lifted to the same equivalence class in $\pi_1(E, e)$ and so $[\beta_1] = [\beta_2]$. The injectivity of p_* tells us that we can identify $\pi_1(E, \tilde{x})$ with a subgroup of $\pi_1(X, x)$. This will be an important idea to hold on to, and from this we can motivate the following definition.

Definition 3.10. A covering $p : E \to X$ is **regular** if $p_*(\pi_1(E, e))$ is a normal subgroup of $\pi_1(X, x)$, for any $e \in p^{-1}(x)$. If a covering is simply connected, we say the covering is **universal**.

The term *universal* is a technical term in category theory. For our purposes, we say that a simply connected covering is universal because it covers all other coverings, so it universal in the sense of being the "largest." This notion of largeness will become clear soon. We can also describe the conditions for a universal cover to exist. To do this, we need to impose some constraints on a topological space and introduce one more definition. A space X is *semi-locally connected* if for all $x \in X$, there is a

path-connected neighborhood U such that $\pi_1(U, x) \to \pi_1(X, x)$ is trivial. With this definition, if X is connected and locally path-connected, X has a universal cover if and only if X is semi-locally connected. A proof for this is rather long, but can be found in [2, pp. 234–236]. The direction we desire is the backwards direction, and a proof of only the backwards direction is given in [3, p. 30].

Definition 3.11. Let X be a path-connected topological space. Denote $\mathbf{Cov}(X)$ by the category of (pointed) covering spaces of X with morphisms as **covering morphisms**, which are continuous maps $\varphi : E_1 \to E_2$ of covering spaces of X such that the following is commutative, with $p_1 : E_1 \to X$ and $p_2 : E_2 \to X$ the associated covering maps of E_1, E_2 respectively:



If such a $\varphi : E \to E$ is a homeomorphism, then we say φ is an **automorphism** of E. We will denote the group of automorphisms of E by $\mathrm{Aut}(E)$.

As in Galois theory, the covering morphisms we wish to look at are covering automorphisms since they have nice properties. Some of these include that given a regular cover $p : E \to X$, $\mathrm{Aut}(E) \cong \pi_1(X, x)/p_*(\pi_1(E, \tilde{x}))$, for $\tilde{x} \in p^{-1}(x)$ and if p is a universal cover, then $\mathrm{Aut}(E) \cong \pi_1(X, x)$. In addition, $\mathrm{Aut}(E)$ acts transitively on the fibers of x.

It will be important later to extract a lemma that is important in the well-definiteness of the morphisms of $\mathbf{Cov}(X)$. A proof can be found in [3, p. 29].

Lemma 3.12. *Any map $E' \to E''$ of covers of X is a covering.*

Given this, it is clear that the universal cover is a covering for any connected covering of X. With the following proposition, we can say more about the universal cover.

Proposition 3.13 (Universal Property of Universal Coverings)**.** *Let $p : E \to X$ be a universal covering and let $p' : E' \to X$ be a covering where $p(\tilde{x}) = p'(\tilde{x}')$, for all $\tilde{x} \in E$ and $\tilde{x}' \in E'$. Then there exists a unique covering morphism $\varphi : E \to E'$ with $\varphi(\tilde{x}) = \tilde{x}'$.*

Proof. Since E is simply connected, $0 = p_*(\pi_1(E, \tilde{x})) \subset p'_*(\pi_1(E', \tilde{x}'))$, so by Proposition 3.8, φ exists. If $\varphi' : E \to E'$ was another covering morphism where $\varphi'(\tilde{x}) = \tilde{x}'$,

then by the uniqueness of path lifts, φ and φ' will lift every path at $\tilde{x}'$ the same way, so $\varphi = \varphi'$. $\square$

A quick corollary to Proposition 3.13 is that if a universal cover exists, then it is unique. Given a universal covering $p : E \to X$, $p : E \to X$ is also a covering that satisfies the equality condition. So E is unique up to isomorphism.

Universal covers, because they are simply connected, are as "basic" of a cover one can have. Any cover of a universal cover will be simply connected as well, so a universal cover is minimal in terms of the fundamental group. Universal coverings are also unique up to isomorphism and cover all other coverings, so there is a sense of "maximality" of covers with a "minimality" of the fundamental group. Given the intuition from Galois theory, it is worth asking, *do the covers between the universal cover and the base space have the same structure as the subgroups of the fundamental group of the base space?* Since the universal group is minimal in terms of its fundamental group but maximal in the sense of what it covers, the structure should not be the exact same. But motivated by our intuitions from Galois theory, it may be the case that the smaller a subgroup of the fundamental group is, the bigger the corresponding cover is. That is, there is a reverse-inclusion relationship between the covers of a space and the subgroups of the fundamental group.

The goal of the remainder of this paper is to show that this is true, and that there is a bijective correspondence between the fundamental group and covers of a space, as in Galois theory with the Galois group and Galois extensions. In fact, there is a strong analogy between the structure of Galois extensions and the covers of a space.

Example. A lingering question in this paper has been finding the fundamental group of a circle. Earlier, we noted that the fundamental group of a circle is $\mathbb{Z}$, but we have yet to prove it. To prove this, we will use the fact that for a universal covering $p : E \to X$, $\mathrm{Aut}(E) \cong \pi_1(X, x)$.

We know that $p : \mathbb{R} \to S^1$ taking $t \mapsto e^{2i\pi t}$ is a covering, and because $\mathbb{R}$ is simply connected, this covering is universal. We make this cover pointed by letting $t \in \mathbb{R}$ such that $p(t) = x \in S^1$, which was our chosen basepoint for the fundamental group. Any $\varphi \in \mathrm{Aut}(\mathbb{R})$ will satisfy $\varphi \circ p = p$. Since all automorphisms of $\mathbb{R}$ take $t \mapsto t + s$, for some $s \in \mathbb{R}$, we can re-write any $\varphi = \varphi_s : \mathbb{R} \to \mathbb{R}$.

Fix $s \in S$. Then

$$p \circ \varphi_s(t) = p(t + s) = e^{2i\pi(t+s)} = e^{2i\pi t} \cdot e^{2i\pi s} = p(t) \cdot p(s) = x \cdot p(s).$$

We need that t maps to x, so $p(s) = e^{2i\pi s} = 1$. This is only true if and only if $s \in \mathbb{Z}$, so we have that $\mathrm{Aut}(\mathbb{R}) = \{\varphi_s : \mathbb{R} \to \mathbb{R} \mid s \in \mathbb{Z}\}$. Hence $\mathrm{Aut}(\mathbb{R}) \cong \mathbb{Z}$, and thus

$\pi_1(X, x) \cong \mathbb{Z}$, for all $x \in S^1$.

4 The Galois Correspondence of Covering Spaces

As suggested at the end of the previous section, there is a strong analogy between Galois theory and covering spaces. In particular, the structure of Galois field extensions is related to the structure of the possible covering spaces of a topological space X. This section will prove that relationship holds at the categorical level via a functor to an orbit category, and describe the analogy.

4.1 Orbit Categories

Given a group G, a (left) action on a set S is a function mapping $G \times S \to S$ such that $es = s$ and $(g_1 g_2)s = g_1(g_2 s)$, for every $s \in S$ and $g_1, g_2 \in G$. We call a set S with a left group action by G a (left) G-set. The G-sets that will be of interest to our discussion will be the sets G/H consisting of left cosets gH, where H is a subgroup of G. In fact, these sets are transitive, meaning for any $h_1, h_2 \in H$, there exists a $g \in G$ such that $gh_1 = h_2$. Given two G-sets S, S', a G-map is a map $\varphi : S \to S'$ such that $f(gs) = gf(s)$, for every $s \in S$. From these notions, we can define a category.

Definition 4.1. Let $\mathcal{O}(G)$ be the **category of orbits**, which has objects as G-sets G/H and morphisms as G-maps $G/H \to G/K$.

From this definition, it would be nice to have a simpler way to characterize orbit categories. The sets G/H can be identified with all subgroups H of G, but what about the G-maps? If we define a G-map $\varphi : G/H \to G/K$ taking $H \mapsto \gamma K$ for some $\gamma \in G$, then $\gamma K = \varphi(H) = \varphi(hH) = h\varphi(H) = h\gamma K$, which implies that $\gamma^{-1} h \gamma \in K$, for every $h \in H$. Hence, G-maps in an orbit category take $gH \mapsto g\gamma K$, where $\gamma \in G$ such that $\gamma^{-1} H \gamma \subset K$. Thus, we can say that an orbit category for a group G is isomorphic to the category of the subgroups of G with morphisms as subconjugacy relations.

Additionally, we say that a *G-space* X is a space that is a G-set with continuous action $G \times X \to X$, and we define the *orbit space* $X/G := \{xG \mid x \in X\}$ with its topology as a quotient space topology on X. For example, given a subgroup H of a topological group G, G is an H-space with orbit space as the quotient space. Another example would be that S^1 is a G-map, where G is a group of rotations.

Galois theory has a very nice relationship with the category of orbits. By Theorem 2.7, $\mathbf{Gal}(L/K)$, the category of the intermediate extensions of L/K, is equivalent to

the category of subgroups of $\mathrm{Gal}(L/K)$, which is then equivalent to $\mathcal{O}(\mathrm{Gal}(L/K))$. We can say something similar about covering spaces.

Earlier, we discussed the group of automorphisms of a universal cover $p : E \to X$. Since it has a nice action on covers, we can ask if it is possible to find an object in the orbit category for a given cover of X. We know that for a connected pointed covering $p : E' \to X$ with $\tilde{x} \in p^{-1}(x)$, $p_*(\pi_1(E', \tilde{x})) \subset \pi_1(X, x)$. So covers correspond to subgroups of $\pi_1(X, x)$ which is exactly the object structure of $\mathcal{O}(\pi_1(X, x))$. Given a map $\phi : E' \to E''$ of covers of X, we know that the fundamental groups of E' and E'' correspond to subgroups of $\pi_1(X, x)$, so ϕ should correspond to a map between subgroups of $\pi_1(X, x)$. We would like to describe what these maps of covers looks like and we would very much like to say this correspondence is a bijection. We will do both of these things.

4.2 The Correspondence

We now have all the prerequisite knowledge to prove the main result of this paper.

Theorem 4.2 (Galois Correspondence of Covering Spaces)**.** *Let X be a connected, locally path connected, and semi-locally simply connected topological space*[7] *and fix $x \in X$. Choose $x \in X$. Then $\mathcal{O}(\pi_1(X, x))$ is equivalent to $\boldsymbol{Cov}(X)$.*

Proof. Let $G = \pi_1(X, x)$. Since X is connected, locally path connected, and semi-locally simply connected, a universal cover $p : E \to X$ exists. Consider the following functor $\mathcal{E}(-) : \mathcal{O}(G) \to \mathbf{Cov}(X)$. We need to make sure that $\mathcal{E}(-)$ is defined on objects and morphisms.

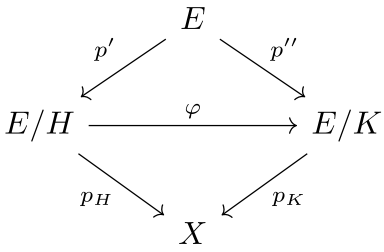
Since p is a universal cover, E is simply connected, so we have that $\mathrm{Aut}(E) \cong \pi_1(X, x)$. Hence, we can identify the subgroups H of G with the subgroups of $\mathrm{Aut}(E)$. For the rest of the proof, we will make the identification $\mathrm{Aut}(E) = G$ and any element $g \in G$ will be considered as an automorphism of E. Define $\mathcal{E}(G/H) := E/H$, the orbit space, and let $q : E \to E/H$ be the quotient map. If $U \subset X$ is a fundamental neighborhood of x for p and V is a component of $p^{-1}(U) \subset E$, then $p^{-1}(U) = \bigsqcup_{g \in \mathrm{Aut}(E)} gV$. Taking $q(p^{-1}(U))$, hV elements are identified, for $h \in H$, so by taking the quotient, $q(p^{-1}(U)) = \bigsqcup_{g \in G/H} g(q(V))$. Hence, $E/H \to X$ is a cover and $\mathcal{E}(-)$ is defined on objects. On morphisms, we know that a morphism $\phi_\gamma : G/H \to G/K$ takes $gK \mapsto g\gamma K$, for $\gamma \in G$ such that $\gamma^{-1} H \gamma \subset K$. We can send this morphism to $\mathcal{E}(\phi_\gamma) : E/H \to E/K$ where $Hg \mapsto K\gamma g$. Thus, $\mathcal{E}(-)$ is also defined on morphisms.

[7] These definitions are given in Section 3.3 but can be confusing to understand. If the definitions are confusing, think of X as a manifold, e.g., a torus.

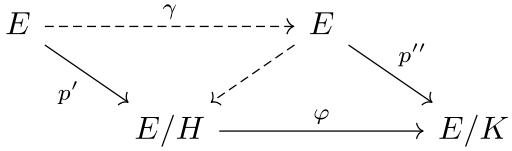
From the specification of where objects and morphisms go, functoriality on $\mathcal{O}(G)$ follows.

Now we need to show that $\mathcal{E}(-)$ is an equivalence of categories, that is, that it is essentially surjective, full, and faithful. Let E' be a connected cover of X. By Lemma 3.12, $E \to E'$ is a cover, and since E is simply connected, $E \to E'$ is universal. If $\mathrm{Aut}_{E'}(E) = \{\phi \in \mathrm{Aut}(E) \mid \phi(E') = E'\}$ is a subgroup of $\mathrm{Aut}(E)$, then because $\mathrm{Aut}(E) \cong G$, $E' \cong E/\mathrm{Aut}_{E'}(E) \cong E/H = \mathcal{E}(G/H)$. Hence $\mathcal{E}(-)$ is essentially surjective.

Consider the following diagram:



Since E/H and E/K are covers, with a morphism of covers φ, the bottom half of the diagram commutes. Since $p'' : E \to E/K$ is a covering and by Lemma 3.12, $\varphi : E/H \to E/K$ is a map of coverings, by the universal property of universal coverings, $p' : E \to E/H$ is a covering where $\varphi \circ p' = p''$. Since $p'' = \varphi \circ p' : E \to E/K$, we have that $\varphi \circ p'$ is a cover. Because $p'' : E \to E/K$ is a universal covering, then by the universal property of universal covers and unique lifting, there exists a unique map $\gamma : E \to E$ where $\varphi \circ p' = p'' \circ \gamma$. Since γ is a covering of a universal covering and universal coverings are unique up to isomorphism, γ is an isomorphism and so γ is invertible. So, the following diagram commutes:



Using these observations, we can prove that $\mathcal{E}(-)$ is full and faithful. We begin with fullness. By the commutativity of the diagram, $\varphi : E/H \to E/K$ taking $He \mapsto H\gamma e$. For ϕ_γ as defined before and $e \in E$,

$$\mathcal{E}(\phi_\gamma)(e) = K\gamma e = p'' \circ \gamma(e) = p'' \circ \gamma \circ (p')^{-1}(He) = \varphi(He),$$

so $\mathcal{E}(-)$ is full. Let $\phi_{\gamma_1}, \phi_{\gamma_2} : G/H \to G/K$ be maps such that $\mathcal{E}(\phi_{\gamma_1}) = \mathcal{E}(\phi_{\gamma_2})$. Take $e \in p^{-1}(x)$, where $x \in X$ is our chosen point. Since $\mathcal{E}(\phi_{\gamma_1})$ is a map of covers, $\mathcal{E}(\phi_{\gamma_1})$ sends fibers of x in E/H to fibers of x in E/K. Since any element in $(p')^{-1}(x) = g(He)$, for $g \in G/H$, then $\mathcal{E}(\phi_{\gamma_1})$ takes $g(He)$ to $g'(Ke)$, for $g' \in G/K$. So, $\mathcal{E}(\phi_{\gamma_1})$ sends $g(He)$ to $g'(Ke)$, which is exactly what ϕ_{γ_1} does. The same argument can be made for $\mathcal{E}(\phi_{\gamma_2})$. Since $\mathcal{E}(\phi_{\gamma_1}) = \mathcal{E}(\phi_{\gamma_2})$, we have that $\phi_{\gamma_1} = \phi_{\gamma_2}$, and thus $\mathcal{E}(-)$ is faithful. □

With this result, we can specify the exact relationship between coverings of a space X and subgroups of the fundamental group.

Corollary 4.3. *Let X be a connected, locally path connected, and semi-locally simply connected topological space, and choose $x \in X$. Then for every subgroup H of $\pi_1(X, x)$, there is a covering $p : E \to X$ with a basepoint $\tilde{x} \in p^{-1}(x)$ such that $p_*(\pi_1(E, \tilde{x})) = H$.*

Proof. The functor defined in the proof of Theorem 4.2 is essentially surjective, so the result follows directly. □

Although we can see similarities to Galois theory, it is important to note that these results are only *analogous* to Galois theory. There is not much more we can determine about coverings from fields. Nevertheless, the power of this result lies in the fact that it is allows us to algebraically determine the pointed covering spaces of X. It can be very difficult to determine all covering spaces of X, since some may not be obvious at all. This is much like field extensions, where it is easy to find $\mathbb{Q}(i)$ as an intermediate field of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$, but not easy to find $\mathbb{Q}((1+i)\sqrt[4]{2})$. Working with groups is much easier, and because the structure of covering spaces can be determined in terms of subgroups of the fundamental group, it is significantly easier to compute all covering spaces and know that there are none missing. To strengthen the anaology even further, we can choose to introduce new terminology. We can call regular covers *Galois covers* or *normal covers*. Recall that regular covers correspond to normal subgroups of the fundamental group, so, like normal extensions, normal covers are indeed *normal*. Both terms may be found in some texts on the subject.

We highlight the power of the Galois correspondence and its analogy to Galois theory with a few examples.

Example. A common result is finding the coverings of real projective spaces $\mathbb{RP}^n$. We construct a real projective space $\mathbb{RP}^n$ by taking an n-sphere S^n and identifying each point on the n-sphere to its antipodal point. From this contruction, the map $p_n : S^n \to \mathbb{RP}^n$ taking a point on the n-sphere to its antipodal class in $\mathbb{RP}^n$ is

surjective. Since a real projective space is Hausdorff, for $[x] \in \mathbb{RP}^n$, we can choose an open neighborhood $U \subset \mathbb{RP}^n$ of $[x]$ that is small enough such that $p_n^{-1}(U)$ is disjoint from its antipodal neighborhood. Then $p_n^{-1}(U)$ is the disjoint union of two open sets that are each homeomorphic to U. So $p_n : S^n \to \mathbb{RP}^n$ is a covering.

Consider $n \geq 2$. The automorphisms of S^n that preserve the covering p_n are the identity map and the map that takes points on the n-sphere to their antipode. Hence, there are only two possible automorphisms, so $\mathbb{Z}/2\mathbb{Z} \cong \mathrm{Aut}(S^n) \cong \pi_1(\mathbb{RP}^n, x)$. Since the only subgroups of $\mathbb{Z}/2\mathbb{Z}$ are trivial, and because S^n is not homeomorphic to $\mathbb{RP}^n$, by the Galois correspondence of covering spaces, we have that $p : S^n \to \mathbb{RP}^n$ is a universal covering, and there no other distinct coverings. In addition, S^n must be simply connected, and in particular has a trivial fundamental group.

Keep in mind that this result is for $n \geq 2$. Although $p_1 : S^1 \to \mathbb{RP}^1$ is a covering, the final part of the argument above fails for $n = 1$ because S^1 is homeomorphic to $\mathbb{RP}^1$ and there are infinitely many automorphisms of S^1 that preserve the covering to $\mathbb{RP}^1$.

Example. We know, that for $x \in S^1$, $\pi_1(S^1, x) \cong \mathbb{Z}$. Additionally, we know that $p : \mathbb{R} \to S^1$ is a universal cover of S^1, where $t \mapsto e^{2i\pi t}$. Knowing this, we can determine all the possible coverings of S^1.

From the Galois correspondence of covering spaces, we know that for every subgroup H of $\mathbb{Z}$, there exists a covering $p_H : \mathbb{R}/H \to S^1$. Since every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, then we can re-write any covering as $p_H = p_n : \mathbb{R}/n\mathbb{Z} \to S^1$, which takes $t + n\mathbb{Z} \to e^{2i\pi t}$. Since $n\mathbb{Z} = -n\mathbb{Z}$, we have that $n = 0$ is the smallest integer we can pick, which yields the covering space $\mathbb{R}/0\mathbb{Z} \cong \mathbb{R}$, our universal covering. If we take $n \geq 1$, we have $p_n : \mathbb{R}/n\mathbb{Z} \to S^1$, taking $t + n\mathbb{Z} \to e^{2i\pi t}$. Under p_n, we have that 0 and n map to the same point, which in this case is the $x \in S^1$ that we chose. We can visualize what each of these total spaces look like and how they cover S^1. Since $\mathbb{R}/n\mathbb{Z}$ is isomorphic to the interval $[0, n) \subset \mathbb{R}$, we can think of the covering spaces as wrapping $\mathbb{R}$ over S^1 in increments of $[0, n)$. In essence, these covering spaces are helixes with larger and larger coils, as illustrated in Figure 4.

Now that we know the structure of the fundamental group, can we find an analogous Galois extension with Galois group $\mathbb{Z}$? The problem is that finite Galois theory where new fields are constructed by algebraic extensions does not allow for infite Galois groups, so it is not possible to find a Galois group that is $\mathbb{Z}$. Though, with a nice construction, we can get close.

Consider a topological group X and a collection of topological groups X_i indexed by a partially-ordered set I. An *inverse limit* is the group X with continuous homomorphisms $\varphi_i : X \to X_i$ such that for any topological group Y and continuous homomorphisms $\psi_i : Y \to X_i$, there exists a unique continuous homomorphism

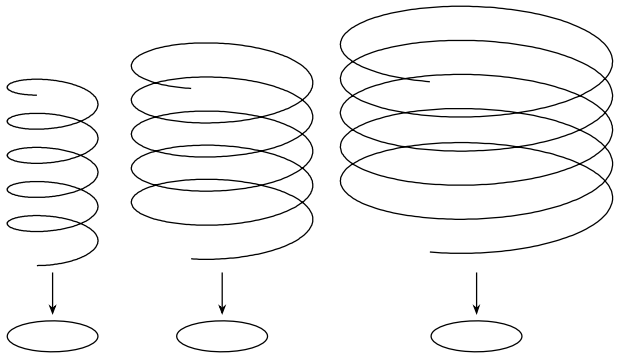


Figure 4: From left to right, visual representations of covers of S^1 for $1 \leq n \leq 3$.

$\psi : Y \to X$ such that $\psi_i = \varphi_i \circ \psi$. The inverse limit is denoted by $\varprojlim_{i \in I} X_i$. We say that a topological group X is *profinite* if it is an inverse limit of finite groups equipped with the discrete topology, i.e., that every subset of X is an open set.

As it turns out, we can define a topology on any Galois group. This topology takes open sets as a fundamental system of neighborhoods of the identity automorphism of the Galois group. We call this topology the *Krull topology*, and if the Galois group is finite, the Krull topology is the discrete topology. From this, for a finite Galois extension $K \subseteq L$, $\mathrm{Gal}(L/K)$ is profinite. A proof for this can be found in [4, pp. 68–69].

Given a finite field $\mathbb{F}_p$, for some prime p, it is a known result that for every $n \in \mathbb{N}$, there exists a unique Galois extension $\mathbb{F}_p \subseteq L_n$ that has degree n. If we consider the Galois extension $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, for $\overline{\mathbb{F}}_p$ the algebraic closure of $\mathbb{F}_p$, endowed with the Krull topology, we see that each $\mathrm{Gal}(L_n/\mathbb{F}_p)$ is a subgroup with the discrete topology. In addition, each $\mathrm{Gal}(L_n/\mathbb{F}_p)$ is generated by the Frobenius automorphism taking $x \mapsto x^p$, so each $\mathrm{Gal}(L_n/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ and we can construct the following inverse limit:

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{n \in \mathbb{N}} \mathrm{Gal}(L_n/\mathbb{F}_p) \cong \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

This construction of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is analogous to the construction of covering spaces of S^1. An inverse limit is a sequence of topological groups with morphisms between them that relate elements of one topological group to the next. Taking the inverse limit of each $\mathbb{Z}/n\mathbb{Z}$ is like what we did for the coverings of S^1, where each covering was determined by $\mathbb{Z}/n\mathbb{Z}$ and sequentially sending elements of one covering to another in such a way that preserved a specific basepoint. In this way, we draw a nice analogy between the Galois group of $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ and the universal covering of S^1.

It should be noted that in general we do not want to discuss the algebraic closure

of a field to be analogous to the universal covering of a space. The algebraic closure is, in general, not Galois because it does not have to be separable. The *separable closure* of a field is always Galois, so it is the correct analogy to the universal covering. That being said, the algebraic closure was used in the previous example because for fields of characteristic 0 and perfect fields, the algebraic closure of the field is the separable closure of the field. Since $\mathbb{F}_p$ is perfect, the algebraic closure can be used instead of the separable closure.

In addition, we call the Galois group of a separable closure the *absolute Galois group*. Again, a separable closure is Galois so this makes sense to say, and since separable closures are unique up to isomorphism, the absolute Galois group is indeed unique.

Example. We have shown that given a base space, we can construct its universal covering, and we can use the universal covering to determine the fundamental group of the base space. It is also possible to construct a universal covering given a finite group. To do this, we can utilize a construction called a *Cayley complex*.

In general, given a group G with n generators and m relations, we take the *wedge sum* of n circles and attach m *2-cells* to form a space with fundamental group G. A wedge sum connects the circles at a single point, and, for our purposes, attaching a 2-cell consists of overlaying the boundary of a disc over the circles. Every finite group is a quotient of a free group, so any finite group can be described with finitely-many generators and relations, and this construction is always possible. Next, we create a *Cayley graph* of G, with each node being an element of G and each edge an action by a generator. We make it a *Cayley complex* by attaching 2-cells at each node corresponding to each relation. This Cayley complex is simply connected and is a covering of the previously-constructed space, so it is a universal covering. For more information on this construction, see [5, p. 77].

In the first section, we found the subfields of $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$, whose Galois group was $D_4 = \{s, r \mid s^2 = r^4 = e\}$. Using the procedure above, lets construct a corresponding space and universal covering for D_4. To construct the space, we first take the wedge sum of two circles, one corresponding to s and the other to r. This looks like two circles connected at a single point, call it x. Next, we attach two 2-cells, one for each relation. In this case, for the r-circle, we attach a 2-cell corresponding to the r^4-relation, which means the boundary of a disc is split into four equal parts with each quarter corresponding to the entire r-circle. In this way, it takes four applications of r to get back to where you started on the attached 2-cell. For the s-circle, we attach a boundary of a disc corresponding to the s^2-relation that is split into two equal parts with each part corresponding to the entire s-circle. In this way, it takes two applications of s to get back to where you started on the attached 2-cell. The

resulting connected space, call it X, has fundamental group $\pi_1(X, x) \cong D_4$, which is visualized in Figure 5. It is easy to see that any element of D_4 can be visualized as a loop winding around some combination of the two circles.

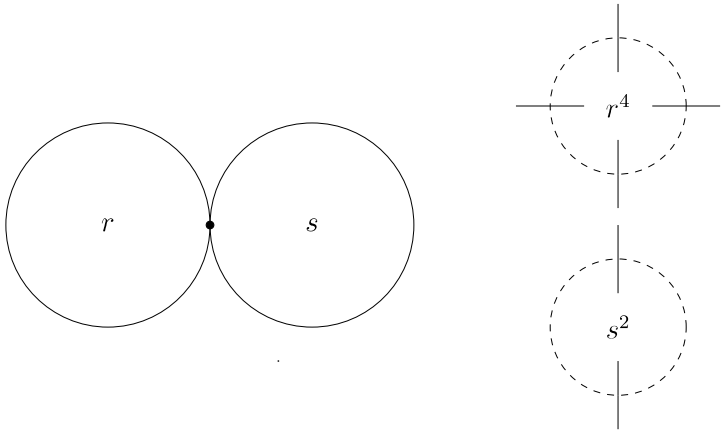


Figure 5: The space X which has fundamental group $\pi_1(X, x) = D_4$, where x is the intersection of the circles.

Next, we need to construct the universal covering space. To do this, create a graph by taking nodes as the elements of D_4, and at each node, multiplying the corresponding element of D_4 by each generator to connect two nodes with a directed edge. For example, multiplying r^2 by r creates an edge from r^2 to r^3 and multiplying r^2 by s creates an edge from r^2 to $r^2 s$. The resulting graph is called a Cayley graph, and the full one for D_4 is given in Figure 6. Then, we will attach 2-cells for each

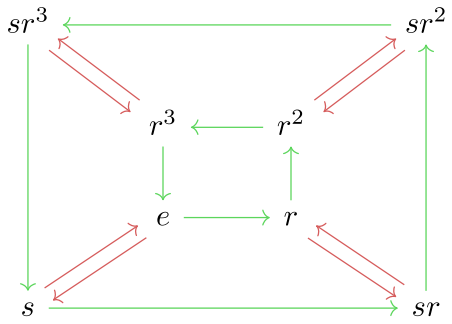


Figure 6: Cayley Graph for D_4, with green edges being multiplication by r and red edges being multiplication by s.

relation over the loops at each node on the Cayley graph. For example, at r^2, a 2-cell will be attached corresponding to the green loop and another corresponding to the

red loop at r^2. In total, there are 8 r^4-relations attached and 8 s^2-relations attached. The resulting space E is called a Cayley complex, and it is simply connected. To make it a covering of X, we need a covering map. Let $p : E \to X$ where every node it taken to the intersection point x, each r^4-relation 2-cell in E is taken to the r^4-relation 2-cell in X, each s^2-relation 2-cell in E is taken to the s^2-relation 2-cell in X, each green arrow is taken to the r-circle, and each red arrow is taken to the s-circle. This map is surjective, and the other covering map conditions are met. So, $p : E \to X$ is a universal covering of X.

Using Figure 1 and Theorem 4.2, we can find all of the covering spaces of X. We know that the covering spaces will take the form E/H, where H is a subgroup of D_4, so we will construct covers by identifying nodes of Figure 6. We won't consider all of the covers, just some.

- If $H = D_4$, then $E/H \cong X$. This is because all nodes are identified with x, all green arrows are identified with the r-circle, all red arrows are identified with the s-circle, all r^4-relation 2-cells in E are identified with the r^4-relation in X, and all s^2-relation 2-cells in E are identified with the s^2-relation in X.

- If $H = \langle r^2 \rangle$, then E/H will identify nodes of E that differ by multiples of r^2, as well as their edges and corresponding r^4-relation and s^2-relation 2-cells. For example, in Figure 6, the sr^3 and sr nodes are identified, along with their green and red edges, and r^4-relation and s^2-relation 2-cells. We identify E/H with $D_4/H = \langle s, r \mid s^2 = r^2 = 1 \rangle$, so E/H is a wedge sum of two circles, with 4 r^4-relations and 4 s^2-relations. Note that the r^4-relations are attached like 2 r^2-relation 2-cells due to the identifications by H. In addition, since $\langle r^2 \rangle$ is a normal subgroup of D_4, E/H is a regular covering of X.

- If $H = \langle s, r^2 \rangle$, then E/H will identify nodes of E that differ by multiples of either r^2 or s, as well as their edges and attached 2-cells. For example, in Figure 6, the sr^3 and r nodes are identified, along with their green and red edges, and r^4-relation and s^2-relation 2-cells. We identify E/H with $D_4/H = \langle s, r^2 \mid s = r^2 = 1 \rangle$, so E/H is a wedge sum of two circles, with 4 r^4-relations from E and 4 s^2-relations. Note that the r^4-relations are attached like 2 r^2-relations and the s^2-relations are attached like 2 identity relations due to the identifications by H. Since $\langle s, r^2 \rangle$ is a normal subgroup of D_4, E/H is a regular covering of X.

- If $H = \{e\}$, then $E/H \cong E$. This is because there are no additional identifications from H.

From these examples, we see that the relationship between the two theories are not exact. Although $\mathbb{RP}^n$ admitted a finite fundamental group, S^1 did not, which

made it more difficult to compare the field and topology sides. Though, once we include infinite Galois extensions, and in particular the absolute Galois group, this analogy is much more apparent.

5 Concluding Remarks

As has been discussed throughout this paper, we can draw a strong analogy between the Galois correspondences of fields and covering spaces. The heart of this analogy comes from how Theorems 2.7 and 4.2 specify similar relationships between maximal objects and subobjects, which turn questions of non-obvious structure into questions of well-known group structure. In Galois theory, this is a bijective correspondence between the subgroup structure of Galois groups and the subfield structure of Galois extensions. In algebraic topology, this is a bijective correspondence between the subgroup structure of fundamental groups and the connected pointed covers of a connected, locally path-connected, and semi-locally simply connected topological space.

We can briefly recap each idea in the analogy. A fixed base field in Galois theory is analogous to a fixed base space. A separable extension is analogous to a covering of the base space, with the separable closure being analogous to the universal covering. The separable closure is the correct analogy over the algebraic closure because the separable closure is the separable closure of all separable extensions of a base field, and the universal covering is the universal covering of all coverings of a base space. So like the universal covering, the separable closure is indeed *universal*. In addition, all possible separable extensions of the base field are the intermediate extensions of the separable closure, and all possible coverings of a base space are the intermediate coverings of the base space. They are also both unique up to isomorphism. Fixing a separable closure is analogous to fixing a basepoint for the coverings, which makes the coverings pointed. For the conclusion of Theorem 4.2 about the structure of the coverings of the base space to hold, all coverings must be pointed, and by fixing a separable closure we can also find a specific structure of intermediate fields. Since the Galois group of a fixed separable closure of a field is the absolute Galois group of the field, the absolute Galois group is analogous to the fundamental group. Finally, although normal extensions are analogous to regular coverings, because all normal intermediate fields of a separable closure are also separable, we have that Galois extensions are analogous to the regular coverings of a base space. The points of the analogy are summarized in the table below:

In field theory	In algebraic topology
base field	base space
separable extension	covering
separable closure	universal covering
fixed separable closure	fixed basepoint
absolute Galois group	fundamental group
Galois extension	regular covering

This analogy is also by no means an end. The analogy stretches far beyond coverings, comparing ideas in algebraic number theory, like class field theory, to ideas in topology. These ideas can be put under one topic called *arithmetic topology*. The theory draws analogies between 3-manifolds and number rings, knots and prime ideals, and curves over finite fields and surface-bundles over S^1. Part of this was explored in the relationship between S^1 and $\mathbb{Z}$, that is, $\pi_1(S^1, x) \cong \mathbb{Z}$, which can be compared to the relationship between a finite field $\mathbb{F}_p$ and its absolute Galois group $\hat{\mathbb{Z}}$. To explore these ideas further, a good text is [6], which discusses the Galois correspondence of covering spaces on [6, p. 18].

Natural things to consider next involve extending the discussion in this article into an expository piece on the fundamentals of arithmetic topology. In particular, providing exposition on topics and notions in class field theory like number fields, quadratic reciprocity, prime ramification, and scheme theory, to set up a discussion of the extended analogy.

References

[1] Emil Artin. *Galois theory. Edited and with a supplemental chapter by Arthur N. Milgram.* Ed. by Arthur N. Milgram. Reprint of the 1944 second edition. Mineola, NY: Dover Publications, 1998. ISBN: 0-486-62342-4.

[2] Marco Manetti. *Topology. Translated from the Italian by Simon G. Chiossi.* Vol. 91. Unitext. Cham: Springer, 2015. ISBN: 978-3-319-16957-6; 978-3-319-16958-3.

[3] J. P. May. *A concise course in algebraic topology.* Chicago, IL: University of Chicago Press, 1999. ISBN: 0-226-51182-0; 0-226-51183-9. URL: `https://www.math.uchicago.edu/~may/CONCISE/ConciseRevised.pdf`.

[4] Luis Ribes and Pavel Zalesskii. *Profinite groups.* 2nd ed. Vol. 40. Ergeb. Math. Grenzgeb., 3. Folge. Berlin: Springer, 2010. ISBN: 978-3-642-01641-7; 978-3-642-01642-4.

[5] Allen Hatcher. *Algebraic topology.* Cambridge: Cambridge University Press, 2002. ISBN: 0-521-79540-0. URL: `https://pi.math.cornell.edu/~hatcher/AT/AT.pdf`.

[6] Masanori Morishita. *Knots and primes. An introduction to arithmetic topology. Based on the Japanese original (Springer, 2009).* Universitext. Berlin: Springer, 2012. ISBN: 978-1-4471-2157-2; 978-1-4471-2158-9.