Fundamental Groups, Covering Spaces, and Connections to Galois Theory

Gabriel Hoag

March 2026

Contents

1 Abstract

The goal of this paper is to explore the relationship between field theory and topology via the Galois correspondence we see in both field extensions and covering spaces. In the end, we hope to prove an analogous version of the Fundamental Theorem of (Finite) Galois Theory for covering spaces. This will allow us to establish a deeper connection between the two areas. Furthermore, we can better understand the relationship between covering spaces and paths (specifically the fundamental group) through deck transformations. For readers who are new to algebraic topology but have backgrounds in algebra or topology, this paper can serve as a basic tool for understanding paths, the fundamental group, covering spaces and the Galois correspondence.

2 Introduction and Background

When reading about fundamental groups and covering spaces, there is an immediate, well-established connection that one can make to field extensions and towers of fields. This connection continues when we discuss deck transformations of a covering space, which has clear analogies to the Galois group of a field extension, with a similar notion of "fixing" the 'base' space/field while performing automorphisms on the upper one. Similar to in Galois Theory, we want to establish the relationship between the group of deck transformations and the intermediate spaces between the covering space and the base space.

To do this, we will begin by reviewing some basic topology centering around paths and homotopies. We will assume that the reader already has some knowledge of basic topology like open/closed sets, continuous functions, and product topologies. This will set us up to define and begin exploring the fundamental group of a space and what information we can glean from the fundamental group.

After this, we will similarly define and explore covering spaces, with the intent to connect them back to fundamental groups and understand the interplay between the two topics. It will also serve as the basis for the first notations of the connections to Galois Theory that we described above. To strengthen this connection, we will review basic Galois Theory, with the assumptions that the reader understands basic group theory and fields (definitions and basic theorems). This will help us in giving a proof for the Fundamental Theorem of Finite Galois Theory.

This will then culminate in us returning back to covering spaces and discussing the analogous concepts and theorems for covering spaces, hoping to see similar results and understand the differences.

3 Basic Topology

In order to begin our discussion of fundamental groups and covering spaces, we must first review some concepts from point-set topology. Throughout this paper, suppose that X is some topological space.

Definition: A path in X is any continuous mapping f from $I = [0, 1]$ to X. We will refer to $f(0)$ and $f(1)$ as the initial and terminal points of the path, respectively.

We can consider the 'product' of two paths f and g if $f(1) = g(0)$ by concatenating the two paths via

$$(f * g)(s) = \begin{cases} f(2s) & \text{if } s \leq \frac{1}{2} \\ g(2s-1) & \text{if } s > \frac{1}{2} \end{cases}$$

and see that $f * g$ is also a path (with continuity inherited from f and g) in X with initial point $f(0)$ and terminal point $g(1)$. Note that this is not the same as the composition of two functions.

Definition: Suppose that $f, g : Y \to X$. Then a *homotopy* of f and g will be a continuous map $H : I \times Y \to X$ such that $H(0, s) = f(s), H(1, s) = g(s)$. f and g will be considered "equivalent" or homotopic (notated $f \sim g$) if and only if there exists such a homotopy H, which we will refer to as the homotopy 'connecting f and g'.

For paths f, g in X, we will also require that f and g have the same initial and terminal points. Furthermore, all "intermediate paths" $f_t(s) = H(t, s)$ must also share those initial and terminal point.

An intuitive way to think about homotopies of pahts is by considering t as movement through "time" while s is movement through "space". Thus, as any "time" t, we have some intermediate path $f_t(s)$ that we can travel across in "space" s. As we move through time, these paths deform from f to g. The initial and terminal points represent fixed points of the path as we move through space.

This is like having our paths represented as a closed string or rubber band with fixed endpoints that we shift/stretch as we move through time. As we go from time 0 to time 1, this string gets moved from f to g.

Lemma 3.1: $\sim$ is an equivalence relation on the set of paths in X.

Proof. Let f, g, h be paths in X. Clearly any path f is equivalent to itself via the homotopy $H(t, s) = f(s)$ for all t, so $\sim$ is reflexive.

If $f \sim g$, then there exists homotopy H as described in Definition 1.2. Thus, consider $H'(t, s) = H(1 - t, s)$. H' will also be continuous, and $H'(0, s) = H(1, s) = g(s), H'(1, s) = H(0, s) = f(s)$. Furthermore, $H'(t, s) = H(1-t, s) = f_{1-t}(s)$ is a path in X for all t. So H' is a homotopy connecting g to f, therefore $g \sim f \Rightarrow \sim$ is symmetric.

If $f \sim g$ and $g \sim h$, then there exists homotopies H_1 and H_2 connecting f to g and g to h, respectively. Because $H_1(1, s) = g(s) = H_2(0, s)$, we can create a new homotopy

$$H(t, s) = \begin{cases} H_1(2t, s) & \text{if } t \leq \frac{1}{2} \\ H_2(2t-1, s) & \text{if } t > 1/2 \end{cases}$$

which is clearly our homotopy connecting f to h. Thus, $\sim$ is transitive. $\square$

This equivalence relation will allow us describe all paths in X (or any subset of paths) 'up to homotopy' and to disregard paths insignificant distinctions.

Example 3.2: Consider the unit circle S^1. For simplicity, we will consider S^1 to be in the complex plane, but could analogously work in the real plane. Let f be the trivial path $f(x) = 1$ for all $x \in I$ while path g does a counter-clockwise followed by a clockwise loop $g(x) = e^{4i\pi s}$ for $s \leq \frac{1}{2}$, $g(s) = e^{4i\pi - 4i\pi s} = e^{-4i\pi s}$ for $s > \frac{1}{2}$

We claim that $f \sim g$ via the homotopy

$$H(t,s) = \begin{cases} e^{4i\pi ts} & \text{if } s \leq \frac{1}{2} \\ e^{4i\pi t - 4i\pi ts} & \text{if } s > \frac{1}{2} \end{cases}$$

which can been seen to be continuous as there are no discontinuities around $x = \frac{1}{2}$. Furthermore, $H(0,s) = e^0 = 1 = f(s)$ and similarly $H(1,s) = g(s)$ for all s. Thus, $f \sim g$.

We will later consider the path $\alpha(s) = e^{2i\pi s}$ which performs a single counter-clockwise loop around the circle and see that it is not equivalent to f or g, i.e. $f \sim g \nsim h$, using covering space theory. These concepts will be important in understanding the fundamental group of S^1.

In order to describe the paths of X up to homotopy, we must make sure that our equivalence relation respects products of paths. This will ensure that taking the product of elements of the fundamental group will still make sense (as these elements are equivalence classes of paths of X).

Lemma 3.3: (Lemma II.3.1 in Massey) Let f_1, f_2, g_1, g_2 be paths in X. Suppose that $f_1 \sim f_2, g_1 \sim g_2$ and the products $f_1 * g_1, f_2 * g_2$ are well-defined. Then $f_1 * g_1 \sim f_2 * g_2$.

Proof. Because $f_1 \sim f_2$ and $g_1 \sim g_2$, then there exists homotopies H_1 and H_2 connecting f_1 to f_2 and g_1 to g_2, respectively. Thus, we will consider the new homotopy

$$H(t,s) = \begin{cases} H_1(t,2s) & \text{if } s \leq \frac{1}{2} \\ H_2(t,2s-1) & \text{if } s > \frac{1}{2} \end{cases}$$

$H_1(t,1) = f_1(1) = g_1(0) = H_2(t,0)$ for all t by definition (all intermediate paths of H_i have to share the same initial/terminal points). Thus, there are no issues with continuity around $x = \frac{1}{2}$. So continuity of H will then follow from H_1, H_2 being continuous. Furthermore,

$$H(0,s) = \begin{cases} H_1(0,2s) = f_1(2s) & \text{if } s \leq \frac{1}{2} \\ H_2(0,2s-1) = g_1(2s-1) & \text{if } s > \frac{1}{2} \end{cases} = (f_1 * g_1)(x)$$

Similarly, $H(1,s) = (f_2 * g_2)(s)$. It is also easily checked using the above property that the initial and terminal points of H will be the same as $f_1 * g_1$ and $f_2 * g_2$.

Therefore, H is the homotopy connecting $f_1 * g_1$ to $f_2 * g_2$, so $f_1 * g_1 \sim f_2 * g_2$ and $\sim$ respects *. □

Definition: We will consider a topological space X to be *path-connected* (or arc-connected) if for any two points $x_1, x_2 \in X$, there exists some path f in X such that x_1, x_2 are the initial and terminal points of f, respectively.

For the remainder of the paper, we will assume that all topological spaces are path-connected.

4 Fundamental Groups

4.1 Definitions and Terminology

The fundamental group will allow us to study the nature of paths within a given space by restricting to paths whose initial and terminal point are the same, called *closed* paths. Note that in any further discussion of paths, any path will actually represent its equivalency class of paths. By Lemma 3.3, this will yield no issues with the product *, which can now be naturally defined on the equivalence classes of paths.

Definition: For any $x \in X$, the *fundamental group* of X and x (notated $\pi(X, x)$), is the group of closed paths in X with initial point x with * as the binary operation.

Proposition 4.1: The fundamental group $\pi(X, x)$ is a group under *.

Proof. Once again, because all discussion of paths is up to homotopy, saying that any two paths f_1, f_2 are equal in the fundamental group is the same as saying $f_1 \sim f_2$.

Consider the trivial path $i(s) = x$ for all x. For any other path $f \in \pi(X, x)$, we want to show that $i*f = f*i = f$ which is equivalent to saying $i*f \sim f \sim f*i$. Consider the homotopy

$$H(t, s) = \begin{cases} f(\frac{2}{1+t}s) & \text{if } s \leq \frac{1}{2}(1+t) \\ x & \text{if } s > \frac{1}{2}(1+t) \end{cases}$$

in which we use the linear mapping of $[0, \frac{1}{2}(1+t)]$ onto I to "shrink" f into the proper interval. We can check that H is continuous as well as find that $H(0, s) = (f * i)(s), H(1, s) = f(s)$, and $H(t, 0) = H(t, 1) = x$ for all s, t. Thus, $f * i \sim f$. An analogous homotopy finds that $i * f \sim f$. So i is the identity element of $\pi(X, x)$.

Similar "stretching" as shown above can also be used to show that the product * is associative, as we can simply stretch the space over which we are traveling along a given path as we move through time.

We claim that the inverse element of any path f is the path $f^{-1}(s) = f(1-s)$ (note that this definitions can naturally be extended to all paths, not just closed paths). To show this, we must show that $f * f^{-1} = i = f^{-1} * f$. Consider homotopy

$$H'(t,s) = \begin{cases} f(2s) & \text{if } s < \frac{t}{2} \\ f(t) & \text{if } \frac{t}{2} \leq s \leq 1 - \frac{t}{2} \\ f(2s-2) & \text{if } 1 - \frac{t}{2} < s \end{cases}$$

from Massey's Lemma II.3.4, which shows that $i = f^* f^{-1}$. Switching f with it's inverse in the homotopy yields the other equality by symmetry.

$\pi(X, x)$ has an identity and inverse elements, and * is associative of equivalence classes of paths, so $\pi(X, x)$ is a group under *. □

Example 4.2: One of the most important examples for our work is the unit circle S^1. We claim that $\pi(S^1, 1) \cong \mathbb{Z}$ is the fundamental group. To see this, we must consider the path $\alpha(s) = e^{2i\pi s}$. As we mentioned earlier (but have yet to prove), α is not homotopic to the trivial path. Furthermore, any path in $\pi(S^1, 1)$ can be generated by α, as they are all characterized by the number of loops they make around the circle (and which direction). In this case, clockwise loops are inverses of counter-clockwise loops, i.e. $\alpha^{-1}(s) = e^{-2i\pi s}$. Therefore, because all non-zero powers of α are non-trivial, the homomorphism $\varphi : \mathbb{Z} \to \pi(S^1, 1), \varphi(n) = \alpha^n$ is injective. Because the fundamental group is generated by α, the map is also surjective and therefore an isomorphism, yielding our claim that $\pi(S^1, 1) \cong \mathbb{Z}$ and is therefore infinite cyclic.

Example 4.3: The fundamental group of torus $S^1 \times S^1$ at $(1, 1)$ will have two generators: a and b. a will represent a loop in the "first" component, while b is a loop in the second. Geometrically, a represents traveling in a loop through the center hole and b is a loop around the "tube", as we see in Figure 1. One can find that these two paths/generators commute with each other, i.e. $a * b = b * a$. Thus, all paths in the fundamental group (based around some arbitrary point) will be determined by the number of loops through the hole and around the tube. $a^m b^n = i$ if and only if $m = n = 0$. Thus, $\varphi : \mathbb{Z} \times \mathbb{Z} \to \pi(S^1 \times S^1, (1, 1)), \varphi(m, n) = a^m b^n$ is an isomorphism.

Interestingly, we note that this means $\pi(S^1 \times S^1, (1, 1)) \cong \pi(S^1, 1) \times \pi(S^1, 1)$, which we will try to generalize later.

4.2 Important Theorems

When further observing Examples 4.2 and 4.3, we see that the fundamental group is independent of our starting/base point. We look to generalize this.

Theorem 4.4: (Theorem II.3.5 in Massey) For path-connected space X, the fundamental group $\pi(X, x)$ is independent of the choice of x up to isomorphism.

Proof. Let $x_1, x_2 \in X$ and consider the fundamental groups $\pi(X, x_1$ and $\pi(X, x_2)$. Because X is path connected, there exists path γ connecting x_1 to x_2. This path induces the homomorphism $\Gamma : \pi(X, x_1) \to \pi(X, x_2), \Gamma(f) = \gamma^{-1} * f * \gamma$.

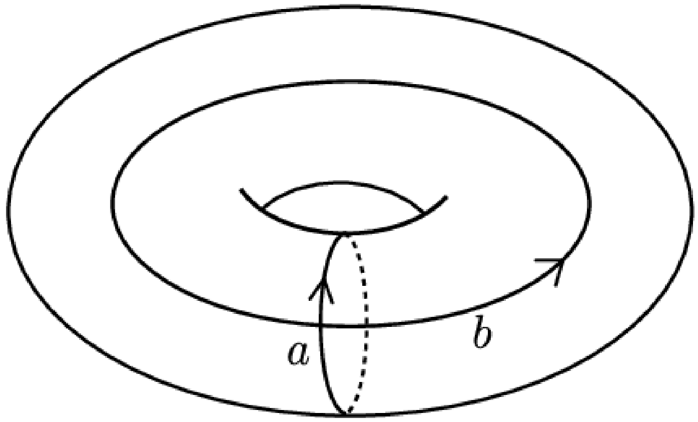


Figure 1: Fundamental Group of a Torus

This map is well defined as $\gamma^{-1} * f * \gamma$ take x_1 to x_2 to x_1 to x_1 back to x_2, so this is a path in $\pi(X, x_2)$. Furthermore, for any paths $f, g \in \pi(X, x_1)$,

$$\Gamma(g * f) = \gamma^{-1} * (f * g) * \gamma = (\gamma^{-1} * f * \gamma) * (\gamma^{-1} * g * \gamma) = \Gamma(f) * \Gamma(g)$$

so Γ is a homomorphism.

Next, consider the map $\Gamma^{-1} : \pi(X, x_2) \to \pi(X, x_1), \Gamma(f') = \gamma * f' * \gamma^{-1}$. By analogous work to above, this is also a homomorphism. Furthermore, for any $f \in \pi(X, x_1)$,

$$(\Gamma^{-1} \circ \Gamma)(f) = \Gamma^{-1}(\Gamma(f)) = \Gamma^{-1}(\gamma^{-1} * f * \gamma) = \gamma * \gamma^{-1} * f * \gamma * \gamma^{-1} = i * f * i = f$$

Therefore, $\Gamma^{-1} \circ \Gamma$ is the identity function on $\pi(X, x_1)$. Similar work finds that $\Gamma \circ \Gamma^{-1}$ is the identity function on $\pi(X, x_2)$. Therefore, Γ is an isomorphism and $\pi(X, x_1) \cong \pi(X, x_2)$. □

Because the fundamental group is independent of the point chosen for all relevant spaces in this paper, we will now denote $\pi(X, x)$ as $\pi(X)$ and disregard the base point. However, as Massey notes, the isomorphism described above is not unique, as there is not necessarily one unique γ mapping x_1 to x_2.

Definition: A path-connected space X will be called *simply connected* if its fundamental group $\pi(X, x)$ is trivial for some point $x \in X$.

Example 4.5: $\mathbb{R}^n$ is simply connected for any n. Similarly, any convex shape in $\mathbb{R}^n$ is simply connected. Although we have yet to prove α is non-trivial in S^1, doing so would show that S^1 is *not* simply connected. However, $S^n \subset \mathbb{R}^{n+1}$ is simply connected for $n \geq 2$.

There is some notation of a simply connected space having no significant "holes" in it that lead to non-trivial paths. However, determining what counts as 'significant' requires further observation. For example, $\mathbb{R}^2 - \{(0,0)\}$ is not simply connected, but $\mathbb{R}^2 - \{(0,0,0)\}$ is.

Lemma 4.6: For any continuous map $F : X \to Y$, if f is a (closed) path in X, then $F \circ f : I \to Y$ is a (closed) path in Y.

This follows immediately from continuity of F and f along with definition of paths. If any paths are closed, then the initial and terminal points are the same, so the image of those point (the initial and terminal points in the new path) will also be the same.

Corollary 4.7: For any (closed) path F in $X \times Y$, $\pi_1 \circ F$ is a (closed) path in X and $\pi_2 \circ F$ is a (closed) path in Y, where π_i is the projection map to the i-th coordinate.

Furthermore, it is clear that $F(s) = (f_1(s), f_2(s))$ for all s. So any path in $X \times Y$ can be described as (f_1, f_2) for some paths in X and Y.

Proposition 4.8: For all X, Y, $\pi(X \times Y) \cong \pi(X) \times \pi(Y)$.

Proof. From Corollary 4.7, we know that the map $\varphi : \pi(X \times Y) \to \pi(X) \times \pi(Y), \varphi(F) = (\pi_1 \circ F, \pi_2 \circ F)$ is well-defined. For all $s \in I, i \in \{1, 2\}$,

$$(\pi_i \circ (F * F'))(s) = \pi_i \circ \begin{cases} F(2s) & \text{if } s \leq \frac{1}{2} \\ F'(2s-1) & \text{if } s > \frac{1}{2} \end{cases}$$
$$= \begin{cases} (\pi_i \circ F(2s)) & \text{if } s \leq \frac{1}{2} \\ (\pi_i \circ F'(2s-1)) & \text{if } s > \frac{1}{2} \end{cases} = ((\pi_i \circ F) * (\pi_i \circ F'))(s)$$

$$\Rightarrow \pi_i \circ (F * F') = (\pi_i \circ F) * (\pi_i \circ F')$$
$$\begin{aligned} \Rightarrow \varphi(F * F') &= (\pi_1 \circ (F * F'), \pi_2 \circ (F * F')) \\ &= ((\pi_1 \circ F) * (\pi_1 \circ F'), (\pi_2 \circ F) * (\pi_2 \circ F')) \\ &= (\pi_1 \circ F, \pi_2 \circ F') * (\pi_1 \circ F, \pi_2 \circ F') = \varphi(F) * \varphi(F') \end{aligned}$$

so φ is a homomorphism.

Surjectivity also follows quickly as for any arbitrary $(f_1, f_2) \in \pi(X) \times \pi(Y)$, we can create (closed) path $F(s) = (f_1(s), f_2(s))$ in $X \times Y$. Then for all $s \in I$, $\pi_i(F(s)) = f_i(s)$, so $\pi_i \circ F = f_i$ and $\varphi(F) = (f_1, f_2)$.

If $\varphi(F) = (i_X, i_Y)$ then $\pi_1 \circ F \sim i_X$ and $\pi_2 \circ F \sim i_Y$, so there exist homotopies H_1, H_2 connecting $\pi_1 \circ F$ to i_X and $\pi_2 \circ F$ to i_Y, respectively. Consider homotopy $H(t, s) = (H_1(t, s), H_2(t, s))$. $H(0, s) = (H_1(0, s), H_2(0, s)) = ((\pi_1 \circ F)(s), (\pi_2 \circ F)(s)) = F(s)$ and $H(1, s) = (H_1(1, s), H_2(1, s)) = (i_X(s), i_Y(s)) = i_{X \times Y}(s)$, so $F \sim i_{X \times Y}$. Thus, $Ker(\varphi) = i_{X \times Y} \Rightarrow \varphi$ injective.

φ isomorphism $\Rightarrow \pi(X \times Y) \cong \pi(X) \times \pi(Y)$. □

This yields a general result to what we discussed in Example 4.3 relating the torus to the unit circle. We could now extend this to say that the n-fold product $\times_{i=1}^{n} S^1$ has fundamental group isomorphic to $\mathbb{Z}^n$ under addition. This essentially corresponds to each "circle" we add creating another loop/generator. Within our work, we also saw that paths in $X \times Y$ could be uniquely defined by the projection paths they create in each space.

Corollary 4.9: For any space X, X is simply connected if and only if X^n is also simply connected.

Theorem 4.10: Any continuous map $f : X \to Y$ naturally induces a homomorphism $f_* : \pi(X) \to \pi(Y)$ by mapping each point within a given path. Furthermore, if $f \sim g$, then f and g induce the same homomorphism on the fundamental groups.

Proof. Well-definedness of f_* follows from Lemma 4.6. It is clear that f induces a homomorphism of the fundamental groups once one sees that for paths α, β in X,

$$f((\alpha * \beta)(s)) = \begin{cases} f(\alpha(s)) & \text{if } s \leq \frac{1}{2} \\ f(\beta(s)) & \text{if } s > \frac{1}{2} \end{cases}$$

and therefore $f_*(\alpha * \beta) = f_*(\alpha) * f_*(\beta)$.

If f, g are homotopic functions from X to Y, then consider some $\alpha \in \pi(X)$. Furthermore, if H is the homotopy connecting f and g, consider the induced homotopy $H_* : I \times \pi(X) \to \pi(Y), H_*(t, \alpha)(s) = H(t, \alpha(s))$ for all $s \in I$. We see that $H_*(0, \alpha) = f \circ \alpha$ and $H_*(1, \alpha) = g \circ \alpha$. Although we didn't require it, we will assume that both f, g map the base point of α to the same point in Y (as we proved in Theorem 4.4 that the choice of base point doesn't matter) as we see that this shows $f \circ \alpha \sim g \circ \alpha$, i.e. $f_*(\alpha) = g_*(\alpha)$. □

Theorem 4.10 will be helpful the following applications.

4.3 Applications of Fundamental Groups

4.3.1 Brouwer Fixed Point Theorem

Let E^2 represent the two-dimensional unit disk $\{x||x| \leq 1\}$. The Brouwer Fixed Point Theorem (Theorem 6.1 in Massey) states that any continuous map $f : E^2 \to E^2$ must have some fixed point $x_0 \in E^2$ such that $f(x_0) = x_0$.

To show this, we will first assume that there exists no such fixed point, so $f(x) \neq x, \forall x \in E^2$. This allows us to construct a ray for all x in the unit pointing from $f(x)$ to x. Now we can construct $r : E^2 \to S^1$, where $r(x)$ is the point on the unit circle that this ray intersects. One can check that this is a continuous mapping.

It is clear that for any $x \in S^1, r(x) = x$, as the ray intersects the unit circle at x itself. So if we consider the inclusion map $i : S^1 \to E^2, i(z) = z$, we have that ri is the identity map on S^1. Therefore, $(ri)_* = r_* i_*$ is the identity homomorphism on $\pi(S^1)$. However, from basic set theory this tells us that $i_* : \pi(S^1) \to \pi(E^2)$ is injective. This yields our contradiction, as we have discussed that $\pi(S^1)$ is infinite, but E^2 is simply connected and has a trivial fundamental group, so no such injection is possible.

4.3.2 Fundamental Theorem of Algebra

Suppose that $p(z) = z^n + a_{n-1}z^{n-1} + ... + a_1 z + a_0$ is some polynomial with coefficients $a_i \in \mathbb{C}$ and $n \geq 1$. The Fundamental Theorem of Algebra states that $p(z)$ with have a root/zero in $\mathbb{C}$.

Similar to our proof of Brouwer's, we will assume no such root exists. From analysis, we know that there exists some R such that $|z^n| > |a_{n-1}z^{n-1} + ... + a_1 z + a_0|$ for all $|z| > R$. Thus, consider the map $p(Rz)$, which clearly has no roots in $\mathbb{C}$ if and only if $p(z)$ also doesn't. So $q : S^1 \to S^1, q(z) = \frac{p(Rz)}{||p(Rz)||}$ is a well-defined map. As z travels around the unit circle, we see that $q(z)$ must also, as it must always be in the same half-plane as z^n. So q_* is a non-trivial homomorphism.

However, because $p(z)$ has no roots, q can be extended to a map $q(z) : E^2 \to S^1$ that is still continuous and well-defined. This yields a contradiction, as accoring to Ran's Lemma 7.2, a continuous mapping $f : S^1 \to S^1$ can be extended to E^2 if and only if f_* is the trivial homomorphism.

Thus, $p(z)$ must have some root in the complex numbers.

5 Covering Spaces

5.1 Definitions and Terminology

Covering spaces will allow us to create an overall structure relating different spaces to each other via covering maps. Similar to the structure and automorphisms of field extensions that we will see in next section, we will begin exploring how covering spaces can be viewed in an analogous matter.

Definition: A *covering space* of topological space X is a space $\tilde{X}$ with a continuous map $p : \tilde{X} \to X$ such that all $x \in X$ have some open neighborhood U where each path component of $p^{-1}(U)$ is mapped topologically onto U. This is the same as saying for any path component V or $p^{-1}(U)$, $p|_V : V \to U$ is a homeomorphism. We will notate the covering space as $(\tilde{X}, p)$. Our neighborhood U will be called an *elementary neighborhood of x*.

If $\tilde{X}$ is simply connected, then $(\tilde{X}, p)$ will be called a *universal covering space* for reasons we will see later.

We will assume that any covering space is mapped surjectively by p. To start building intuition for this, we will review a few examples.

Example 5.1: Consider the continuous map $p : \mathbb{R} \to S^1, p(x) = e^{2i\pi x}$. $(\mathbb{R}, p)$ is a (universal) covering space, as for any small open arc of the circle, its pre-image consists of disjoint open intervals that are homeomorphic to the arc under p.

However, if we consider the pair $([0,1], p)$, it is not a covering space as the preimage of any open neighborhood of $1 \in S^1$ (besides all of S^1) will consist of two half-open intervals that are not homeomorphic to the neighborhood. $p^{-1}(S^1) = [0,1]$ is also not homeomorphic to S^1, so 1 has no elementary neighborhood.

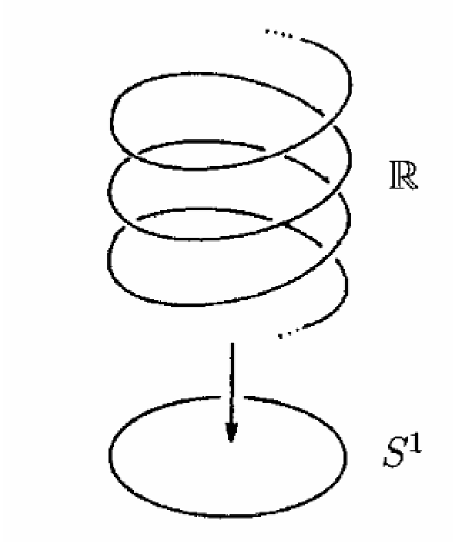


Figure 2: $\mathbb{R}$ covering S^1

We see that a covering space is a stronger version of a quotient mapping, requiring more "smoothness" in terms of local homeomorphisms. In Example 5.1, we see that we can essentially break up $\mathbb{R}$ into unit intervals which, when we identify the endpoints, will be homeomorphic S^1. This creates the idea of *sheets*, which will be the path-connected components of $p^{-1}(U)$ for any open $U \subseteq X$. Later, we will see that the number of such sheets are independent of U. We can describe the covering in Example 5.1 as an infinite-sheeted covering.

Example 5.2: The circle S^1 can also be use to cover itself via the map $p : S^1 \to S^1, p(z) = z^n, n \geq 1$. In this case, this map is an n-sheeted covering.

Proposition 5.3: If $(\tilde{X}, p_1)$ and $(\tilde{Y}, p_2)$ are covering spaces of X and Y, respectively, then $(\tilde{X} \times \tilde{Y}, P)$ is a covering space of $X \times Y$, where $P((\tilde{x}, \tilde{y})) = (p_1(\tilde{x}), p_2(\tilde{y}))$ for all $(\tilde{x}, \tilde{y}) \in \tilde{X} \times \tilde{Y}$.

Proof. Because p_1, p_2 are both covering maps, then for any $x \in X, y \in Y$, there exist respective elementary neighborhoods U, V. Let U_i, V_j be the path-connected components of $p_1^{-1}(U)$ and $p_2^{-1}(V)$, respectively. One can check that the path-connected components of $P^{-1}(U \times V)$ will consist exactly of all $U_i \times V_j$. From there, it is clear that each of these path-components is mapped topologically onto $U \times V$ by P, as P inherits this from its component functions. Therefore, $U \times V$ in an elementary neighborhood of (x, y), so $(\tilde{X} \times \tilde{Y}, P)$ is a covering space of $X \times Y$ □

Example 5.4: By applying the above proposition to the Examples 5.1 and

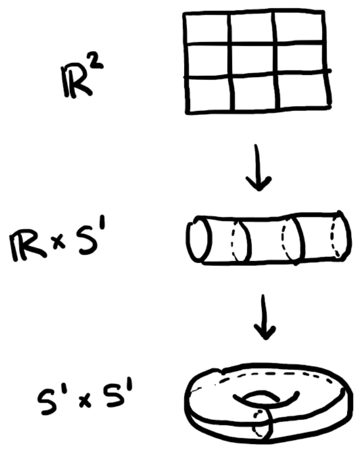


Figure 3: Coverings of Torus

5.2, we can find lots of covering spaces of the torus. By just using Example 5.1, we get the covering space $(\mathbb{R}^2, p)$ where $p((x_1, x_2)) = (e^{2i\pi x_1}, e^{2i\pi x_2})$. Combining both examples, we can find a covering space like $(\mathbb{R} \times S^1, p')$ with $p'(x, z) = (e^{2i\pi x}, z^n)$.

Interestingly, we note that if we consider the map $P : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times S^1, P((x, y)) = (x, e^{2i\pi y})$, then $(\mathbb{R} \times \mathbb{R}, P)$ is a covering space of $\mathbb{R} \times S^1$. Furthermore, $p \circ P = p'$ for $n = 1$, yielding the diagram in Figure 3. This leads us to the notation of a *sub-covering space*.

Definition: Suppose $(\tilde{X}, p)$ and (Y, p') are both covering spaces of X. Then (Y, p') will be called a *sub-covering space* of $(\tilde{X}, p)$ if there exists some map $\varphi : \tilde{X} \to Y$ such that $(\tilde{X}, \varphi)$ is a covering space of Y and the following diagram commutes:

$$\begin{array}{ccc} \tilde{X} & \xrightarrow{\varphi} & Y \\ & \searrow^{p} & \downarrow{p'} \\ & & X \end{array}$$

Furthermore, φ will be referred to as a *homomorphism* of the covering spaces. In particular, under our assumption of surjective covering spaces, this homomorphism will be surjective (although it does not have to be in a more general setting).

If two such homomorphism exists in both directions between $(\tilde{X}, p)$ and

(Y, p'), $\varphi_0 : \tilde{X} \to Y$ and $\varphi_1 : Y \to \tilde{X}$ such that φ_0, φ_1 are inverses of each other, then we call the two covering spaces *isomorphic*. In general, we will discuss covering spaces up to isomorphism.

An isomorphism of a covering space $(\tilde{X}, p)$ onto itself will be called an *automorphism* of the covering space, or a *deck transformation*, "over"/with respect to the base space. Deck transformations will form a group $Deck_p(\tilde{X}/X)$ under function composition, the study of which is our primary goal. There will also be strong relations and Galois correspondence with the fundamental group of the base space that is being covered.

In our example above, we could see that $(\mathbb{R} \times S^1, p')$ was a subcovering space of $(\mathbb{R} \times \mathbb{R}, p)$ with respect to the torus. Similarly, all covering spaces of S^1 seen in Example 5.2 are subcovering spaces of $(\mathbb{R}, p : x \to e^{2i\pi x})$ from Example 5.1.

Any shift of the real line in Exam 5.1 by integer multiples of 2π will be a deck transformation on $\mathbb{R}$, and we will later see that the group of deck transformations of $\mathbb{R}, p$ is isomorphic to $\mathbb{Z} \cong \pi(S^1)$. As we will show later, this is not a coincidence.

5.2 Fundamental Group of Covering Spaces

In order to discuss the relationship between covering spaces and the fundamental group, we must first consider how covering spaces affect paths. First, we want to show that any path in a space can be "lifted" to its covering space in a unique manner (by fixing an initial point in the pre-image). After this, we can then show that lifting preserves homotopy of paths.

Lemma 5.5: (Lemma V.3.1 in Massey) Let $(\tilde{X}, p)$ be a covering space of X. If f is a path in X with initial point $x \in X$, then for any point $x_0 \in p^{-1}(\{x\})$, there exists a unique path g in $\tilde{X}$ with initial point x_0 such that $p \circ g = f$.

By definition of a covering space, each $x \in X$ has some elementary neighborhood U_i. Because $f : I \to X$ and I is compact. Therefore, if we consider the collection of $\{f^{-1}(U_i)\}$, we can choose some finite subset that covers I. This allows us to "break up" our path into segments that are each contained within a given elementary neighborhood. Therefore, because we have an initial point for our path in $\tilde{X}$, we can use the associated path-component of $p^{-1}(U_0)$ and the fact that U_0 is homeomorphic with this component under p. This allows us to lift this segment and yields the appropriate initial point for when we life then next segment. Inductively continuing this process yields our path g in $\tilde{X}$.

Uniqueness of this paths follows from the fact that I is connected, as Massey shows in Lemma V.3.2.

Lemma 5.6: (Lemma V.3.3 in Massey) Let $(\tilde{X}, p)$ be a covering space of X. If f, g are paths in $\tilde{X}$, then $f \sim g$ if and only if $p \circ f \sim p \circ g$.

The forward direction of this proof is clear, as we can just compose the homotopy connecting f and g with the covering map (in the appropriate component) and we find the desired result.

The backwards direction follows from similar work to the proof above, defining a homotopy over small intervals/neighborhoods and combining them.

Example 5.7: (Continuation of Examples 4.2 and 5.1) With our new tools, we can finally show that the path α making a counter-clockwise loop around S^1 is non-trivial. We can do this by lifting α with base point $1 \in S^1$ to $\mathbb{R}$ with base point $0 \in p^{-1}(1)$ using the covering space described in 5.1. One can easily check that the resulting path will be $f(s) = s$ with terminal point $1 \in \mathbb{R}$.

This path is not homotopic to the trivial path in $\mathbb{R}$, as it is not even closed. Thus, α can not be homotopic to the trivial path in S^1 by Lemma 5.6. This verifies that the fundamental group of S^1 is not trivial and instead infinite cyclic.

In fact, lifting any path in the fundamental group of S^1 to $\mathbb{R}$ as we did above, we will see that lifting α^n yields terminal point n.

Theorem 5.8: If $(\tilde{X}, p)$ is a covering space of X, then p induces an injective homomorphism $p_* : \pi(\tilde{X}) \to \pi(X)$.

This follows immediately from Theorem 4.10 and Lemma 5.6 (which gives injectivity).

Essentially, this shows that the fundamental group of a covering space is isomorphic to a subgroup of the base space's fundamental group.

In the case of covering spaces of S^1, this injection is clear for $(\mathbb{R}, p)$ as the real numbers have a trivial fundamental group. For the n-sheeted covering of S^1 by itself, we see that $\pi(S^1) \cong \mathbb{Z}$ is mapped to $n\mathbb{Z} \subset \pi(S^1)$.

6 Basic Field and Galois Theory

6.1 Definitions

Galois Theory will explore automorphisms of fields that "fix" certain subfields and the relationship between field and group theory. To explore this, we must first understand basic field theory.

If a field F is contained in another field K, i.e. $F \subset K$ with the same addition and multiplication, then F is called a *subfield* of K while K is an *extension field* or just *extension* of F. The degree of K over F, $[K : F]$, is the dimension of K when considered as a vector space over F with the field's addition and multiplication. If $[K : F] < \infty$, then K is a *finite* extension of F.

Furthermore, any $\alpha \in K$ will be called *algebraic* over F if there exists some polynomial $f(x) \in F[x]$ such that α is a root of f. The monic polynomial of lowest degree in $F[x]$ satisfying this will be called the irredicible polynomial of α over F, denoted $irr(\alpha, F, x)$. The other roots of $irr(\alpha, F, x)$ will be called the *conjugates* of α over F. If all elements of K are algebraic over F, then K will be called an *algebraic* extension of F. The field containing all algebraic elements over F will be called the algebraic closure F^a.

Similarly, any $\alpha \in K$ that is algebraic over F will be called *separable* over F if $irr(\alpha, F, x)$ has no repeated roots. K will be a separable extension of F if all $\alpha \in K$ are separable over F.

We will notate extensions of F as $F(x_1, x_2, ...)$, which means the smallest field containing both F and all x_i.

Definition: We will give three equivalent definitions of a *normal* extension of a field F. K is called a normal extension of F if any of the three hold:

1. Any embedding of $K, \phi : K \to F^a$ that fixes F ($\phi(x) = x, \forall x \in F$) will map K onto itself, i.e. be an automorphism of K.

2. For all $y \in K$, any conjugates of y over F will also be in K, i.e. $irr(y, F, x)$ factors completely in $K[x]$.

3. K is a splitting field over F, meaning it is found by adding all the roots of a set of polynomials to F.

If K is both normal and separable over F, then it is a *Galois extension* of F. Furthermore, we can look at the group of automorphisms of K that fix F (equivalently the embeddings of K into F^a that fix F), which we will call the Galois Group of K over F: $Gal(K/F)$. These will be our primary area of interest in this section.

To allow further study of the Galois Group, we will state a few results from field theory without proof that will be useful to our work. Readers can refer to Lang's Chapter V if they want more details.

Proposition 6.1: Let k, F, K be fields and $k \subseteq F \subseteq K$. Then if K is a normal extension of k, it is also a normal extension of F.

This is most easily seen using the 1st definition of normal extensions.

Proposition 6.2: Let k, F, K be fields and $k \subseteq F \subseteq K$. Let "X" denote exactly one of the following: algebraic, finite, or separable. Then K is an X extension of k if and only if K is an X extension of F and F is an X extension of k.

Lemma 6.3: If K is a Galois extension of F with Galois group $Gal(K/F)$, then $|Gal(K/F)| = [K : F]$.

For any subgroup H of the Galois group $Gal(K/F)$, we can consider the largest subfield of K such that all automorphisms in H fix that subfield when acting on K. We will call this the "fixed field of H" or K^H.

When acting on K, the automorphisms in $Gal(K/F)$ will always map elements of K to their conjugates over F. In fact, if $\alpha \in K$ has some conjugate $\alpha' \in K$ over F, then there exists some automorphism $\sigma \in Gal(K/F)$ such that $\sigma(\alpha) = \alpha'$.

6.2 Fundamental Theorem of Finite Galois Theory

Before returning to covering spaces, we will prove the Fundamental Theorem of Finite Galois Theory (FToFGT) as a model for later proofs, following work from Lang and Jochnowitz. We will divide the FToFGT into two parts. For all parts, we will assume that K is a finite Galois extension of k with Galois group $Gal(K/k) \cong G$.

Part I of FToFGT: $K^G = k$, i.e. k is the only field fixed by all automorphisms in G. Furthermore, there exists a bijection between the intermediate fields F such that $k \subseteq F \subseteq K$ and the subgroups of G.

Proof. First, we can show that $K^G = k$. Because any $\sigma \in G = Gal(K/k)$ must fix k by definition, $k \subseteq K^G \subseteq K$. However, for any $\alpha \in K - k$, α must have some conjugate element over k, as $irr(\alpha, k, x)$ is of degree ≥ 2 with no repeated roots (by separability), and this conjugate must be in K by the 2nd definition of normal extensions. Thus, there must exist some $\sigma \in G$ that maps α to this conjugate, implying that $\alpha \notin K^G$. Therefore, $K^G \subseteq k \Rightarrow k = K^G$.

This allows us to develop a bijection from the intermediate fields between k, K and the subgroups of G. Since K is Galois over any intermediate field F by Propositions 6.1 and 6.2, then we can consider $Gal(K/F)$. Specifically, since any automorphism that fixes F must also fix $k \subseteq F$, we have that $Gal(K/F) \subseteq Gal(K/k)$. Thus, we can identify $H = Gal(K/F)$ as a subgroup of G. This allows for us to construct the map $\phi : F \to Gal(K/F) = H$. By our work above, we can similarly see that $K^H = F$, so $\phi(F_1) = \phi(F_2) = H \Rightarrow F_1 = K^H = F_2$. Thus, ϕ is injective.

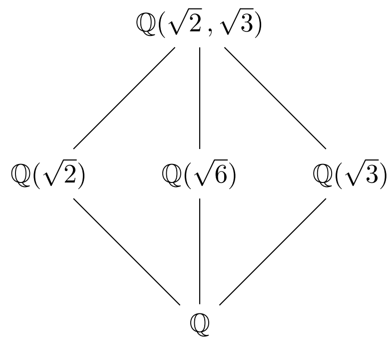
Next, we must show that ϕ is surjective, i.e. that every subgroup $H \subseteq G$ can be written as $Gal(K/F)$ for some intermediate field F. To do this, we will consider the intermediate field K^H and show that K is Galois over it and $Gal(K/K^H) = H$. Jochniwitz first shows that K is Galois over K^H by taking some arbitrary $\alpha \in K$, constructing a polynomial $f(x) \in K^H[x]$ such that α is a root of f, and showing that f has no repeated roots. So all α (and therefore K) is separable over K^H. K is also a splitting field over k, so it is clear it will also be a splitting field over K^H, as any irreducible polynomial $K^H[x]$ divides one in $k[x]$. Thus, K is normal over K^H by the 2nd definition of normal extensions, so K is Galois over K^H.

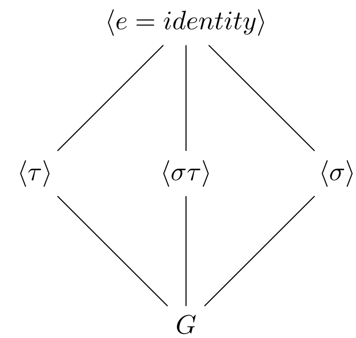
Next, we see that $H \subseteq Gal(K/K^H)$, as it fixes K^H by definition. Furthermore, because the above polynomial was constructed using elements of H, it is found that any minimal polynomial $irr(\alpha, K^H, x), \alpha \in K$ has degree $\leq |H|$. By Lang's Lemma VI.1.7, this implies that $[K : K^H] \leq |H|$. However, by the containment above, $|H| \leq |Gal(K/K^H)| = [K : K^H] \leq |H| \Rightarrow H = Gal(K/K^H)$ (as $|H|$ is finite by hypothesis), and we are done. $\square$

This bijection will be referred to as the "Galois correspondence" between the intermediate fields and subgroups. We can draw diagrams representing this correspondence as we see in the example below.

Example 6.4: Let $k = \mathbb{Q}, K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $[K : k] = 4$, and we see that there are 3 distinct intermediate fields strictly between k and K: $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$. Thus, by Part I of the FToFGT, the associated Galois group $G = Gal(K/k)$ will have 4 elements and 3 strict, non-trivial subgroups. This immediately tells us that $G = \mathbb{Z}^2 \times \mathbb{Z}^2$, the Klein-4 group. This group will be generated by automorphisms $\sigma : \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}$ and $\tau : \sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}$.

One can check that $\langle\sigma\rangle$ fixes $\mathbb{Q}(\sqrt{3})$, $\langle\tau\rangle$ fixes $\mathbb{Q}(\sqrt{2})$, and $\langle\sigma\tau\rangle$ fixes $\mathbb{Q}(\sqrt{6})$. This yields the two associated diagrams below:





We also notice that this correspondence is order-reversing in terms of containment: If $E_1 \subseteq E_2$, then every automorphism in $Gal(K/E_2)$ fixes E_2 and will therefore also fix E_1, implying that $Gal(K/E_2) \subseteq Gal(K/E_1)$.

Part II of FToFGT: Once again, we assume that K is a Galois extension of k and that F is an intermediate field. We claim that F is a normal extension of k if and only if $H = Gal(K/F)$ is a normal subgroup of $G = Gal(K/k)$. In this case, we will also show that $Gal(F/k) \cong Gal(K/k)/Gal(K/F) = G/H$.

Proof. For the first statement, we will abbreviate Jochnowitz's proof, recalling the 1st definition of a normal extension. Thus, we have that

$$
\begin{aligned}
F \text{ is a normal extension of } k &\Leftrightarrow \sigma(x) \in F, \forall x \in F, \forall \sigma \in G \\
&\Leftrightarrow H \text{ fixes } \sigma(x) \text{ (as } F = K^H) \\
&\Leftrightarrow \tau\sigma(x) = \sigma(x), \forall \tau \in H, x \in F, \sigma \in G \\
&\Leftrightarrow \sigma^{-1}\tau\sigma(x) = x, \forall \tau \in H, x \in F, \sigma \in G \\
&\Leftrightarrow \sigma^{-1}\tau\sigma \in H, \forall \tau \in H, \sigma \in G \text{ (as } \sigma^{-1}\tau\sigma \text{ fixes } F) \\
&\Leftrightarrow H \text{ is a normal subgroup of } G
\end{aligned}
$$

For the second statement, we will assume that F is a normal extension of k (and therefore Galois as $F \subseteq K$ separable over k) and construct a map $\varphi : G \to Gal(F/k)$. By finding that H is the kernel and surjectivity, the First Isomorphism Theorem of groups will yield our desired result. Let $\varphi(\sigma) = \sigma|_F$. Because we know that σ fixes k and F is normal over k, then $\sigma|_F$ will also fix k. Thus, $\sigma|_F$ is an automorphism of F by our 1st definition of normal extensions, so $\sigma|_F \in Gal(F/k)$ and our map is well-defined. Knowing this, it is also straight-forward to check that the map is a homomorphism.

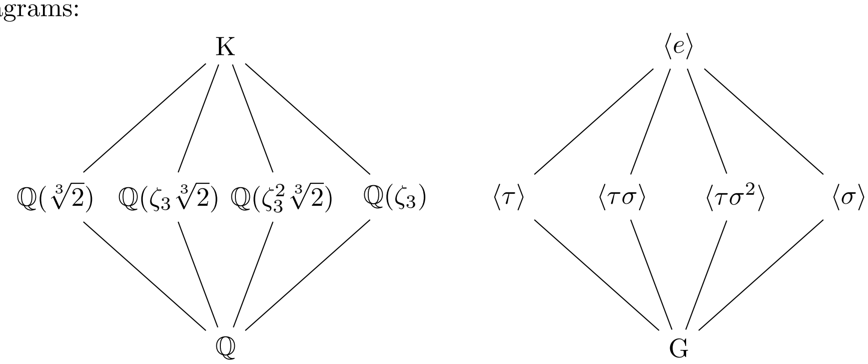
Because K is algebraic over F, $K = F(x_1, x_2, ...)$ for some x_i algebraic over K. Thus, if $\tau \in Gal(F/k)$, we can extend this map to an automorphism $\sigma \in Gal(K/k)$ by mapping these x_i to conjugates over k in an appropriate way. (In theory, we are actually extending an embedding of F into k^α over k to an embedding of K.) This finds a $\sigma \in G$ such that $\varphi(\sigma) = \sigma|_F = \tau$, so φ is surjective.

$$\begin{aligned} Ker(\varphi) &= \{\sigma \in G | \varphi(\sigma) = id \in Gal(F/k)\} \\ &= \{\sigma \in G | \sigma|_F = id\} \\ &= \{\sigma \in G | \sigma \text{ fixes F}\} \\ &= Gal(K/F) = H \end{aligned}$$

Therefore, we have that $Gal(F/k) \cong G/Ker(\varphi) = G/H$. □

Example 6.5: Let $k = \mathbb{Q}, K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, where ζ_3 is a primitive 3rd root of unity. One can verify that $[K : k] = 6$ ($[\mathbb{Q}(\sqrt[3]{2}), k] = 3$ and $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2})$). However, if we look at two of the elements of $Gal(K/k), \sigma : \sqrt[3]{2} \to \zeta_3\sqrt[3]{2}, \zeta_3 \to \zeta_3$ and $\tau : \sqrt[3]{2} \to \sqrt[3]{2}, \zeta_3 \to \zeta_3^2$, then we can see that these don't commute. For example, $\sigma\tau(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2} \neq \zeta_3^2\sqrt[3]{2} = \tau\sigma(\sqrt[3]{2})$. Thus, $Gal(K/k)$ must be a non-abelian group of order 6: $Gal(K/k) \cong S_3$. We also see that $|\langle\sigma\rangle| = 3, |\langle\tau\rangle| = 2$.

Further work and finding fixed fields yields the following (corresponding) diagrams:



From Part II of the FToFGT, we should have the normal extensions of k correspond with the normal subgroups of S_3. The only normal (strict, non-trivial) subgroup of S_3 is $\langle\sigma\rangle$, and indeed we see that $\mathbb{Q}(\zeta_3)$ is a normal extension of k using the 3rd definition (splitting field of $f(x) = x^3 - 1$), while the other intermediate fields contain one root of $x^3 - 2$ and not the others (and are therefore not normal extensions).

7 Galois Correspondence of Covering Spaces

As we've hinted towards earlier, deck transformations will act as our main point of focus in creating this Galois correspondence. Let $x \in X$ and $(\tilde{X}, p)$ be a covering space of X. Then because any deck transformation σ must preserve the covering space, it must map any $x_0 \in p^{-1}(x)$ to another $x_1 \in p^{-1}(x)$ (not necessarily distinct). For any $x \in X$, $p^{-1}(x)$ is called the *fiber* of x. Thus, we see that deck transformations act on a space by permuting these fibers and therefore permuting sheets within the covering space.

Proposition 7.1: The group of deck transformations of a universal covering space is isomorphic to the fundamental group of the base space.

Proof. Let (Y, p) be the universal covering space of X with $y \in Y$. Consider the mapping $\chi : Deck_p(Y/X) \to \pi(X)$, where if $\sigma \in Deck_p(Y/X) = G$ and $\sigma(y) = y_1$ and α is a path in Y from y to y_1, then $\chi(\sigma)$ is the path $p \circ \alpha$.

Because Y is simply-connected, then α is unique up to homotopy. By Lemma 5.6, $p \circ \alpha$ is unique up to homotopy. $p \circ \alpha \in \pi(X)$ as $\sigma(y) = y_1 \Rightarrow p(y) = p(y_1)$. Therefore, χ is well-defined. Suppose $\sigma, \tau \in G$ with $\tau(y_1) = y_2$ and σ as above. Thus, $\tau\sigma(y) = y_2$. Let α, β be the paths in Y from y to y_1 and y_1 to y_2, respectively. Then $\alpha * \beta$ is the unique path from y to y_2, so $\chi(\tau\sigma) = p \circ (\alpha * \beta)$. Clearly $\chi(\sigma) = p \circ \alpha$. However, because we know that α^{-1} is a path from $\sigma(y) = y_1$ to y, then $\tau \circ \alpha^{-1}$ is a path from $\tau(y_1) = y_2$ to $\tau(y)$. $\tau \in G$, so $p \circ (\tau \circ \alpha^{-1}) = p \circ \alpha^{-1}$. Note that this yields that $\alpha * \beta * (\tau \circ \alpha^{-1})$ is the path from y to $\tau(y)$. Therefore,

$$\begin{aligned} \chi(\tau) &= p \circ (\alpha * \beta * (\tau \circ \alpha^{-1})) \\ &= (p \circ (\alpha * \beta)) * (p \circ (\tau \circ \alpha^{-1})) \\ &= (p \circ (\alpha * \beta)) * (p \circ \alpha^{-1}) \\ &= p \circ (\alpha * \beta * \alpha^{-1}) \end{aligned}$$

Thus,

$$\begin{aligned} \chi(\tau) * \chi(\sigma) &= (p \circ (\alpha * \beta * \alpha^{-1})) * (p \circ \alpha) \\ &= p \circ (\alpha * \beta * \alpha^{-1} * \alpha) \\ &= p \circ (\alpha * \beta) = \chi(\tau\sigma) \end{aligned}$$

where we are using (without proof) the fact that continuous maps respect the products of paths. Thus, χ is a homomorphism.

By the uniqueness of lifting paths from the fundamental group given initial point y (Lemma 5.5) and the fact that the only automorphism that map y to itself in G is the identity (as we will see in Lemma 7.4), we find that χ is injective. Unique lifting and similar work to what we will see in Lemma 7.4 will also allow us to construct an automorphism $\sigma \in G$ such that $\sigma(y) = y_1$, for any $y_1 \in p^{-1}(p(y))$. Continuity and well-definedness of this automorphism will follow from the uniqueness of paths in the universal covering space and continuity of paths. Thus, we also find that χ is surjective as we can lift any path in the fundamental group, then create an automorphism whose action on y maps back to that path. This amounts to the universal covering space always being a *normal* covering space as we will define below.

So χ is an isomorphism, and $Deck_p(Y/X) \cong \pi(X)$. $\square$

Definition: A covering space (Y, p) will be called a *normal* covering space of X if the group of deck transformations acts transitively on the the fiber $p^{-1}(x)$ for $x \in X$. Informally, we will say that Y is *normal over* X (omitting the given covering map when there is no ambiguity).

In general, Y is normal covering space and we orient our homomorphism from above the other way $\pi(X) \to Deck_p(Y/X)$, then it will always be surjective. So the deck transformations will always be equal to a factor group of the base space's fundamental group (such as the deck transformations of $(S^1, p_n : z \to z^n)$ over S^1 being isomorphic to $\mathbb{Z}/n\mathbb{Z}$). Normal covering spaces will give us an analogy to normal field extensions, and we will later find a similar result to Part II of the FToFGT.

Proposition 7.2: Let (Y, p) be a covering space of X and (Y', p') be a subcovering with homomorphism $\varphi : Y \to Y'$. If (Y, p) is a normal covering space of X, then (Y, φ) is a normal covering space of Y'.

Proof. We already know that (Y, φ) is a covering space of Y'. Fix some $y' \in Y'$. We need to show that $Deck_\varphi(Y/Y')$ acts transitively on $\tilde{p}^{-1}(y)$. Equivalently we need that for all $y_1, y_2 \in \varphi^{-1}(y')$, there exists some path $\alpha \in \pi(Y', y')$ that when lifted to Y with initial point y_1, has terminal point y_2. Let $p'(y') = x \in X$. (Y', p') is a subcovering of (Y, p), so $p = p' \circ \varphi$ by our definition in Section 5. Therefore,

$$y_1, y_2 \in \varphi^{-1}(y') \subseteq \varphi^{-1}(p'^{-1}(x)) = (p' \circ \varphi)^{-1}(x) = p^{-1}(x)$$

Because Y is normal over X and $y_1, y_2 \in p^{-1}(x)$, there exists some path $\beta \in \pi(X, x)$ that satisfies this lifting property. Thus, there exists some lifted path γ in Y from y_1 to y_2 such that $p \circ \gamma = \beta$. Because $y_1, y_2 \in \varphi^{-1}(y')$, this means that $\varphi \circ \gamma \in \pi(Y', y')$. So we can take $\alpha = \varphi \circ \gamma$ and see that it satisfies our conditions. □

Furthermore, it is clear that the deck transformations of the top space over the subcovering space will be a subgroup of the deck transformations over the base space. This can be seen by considering the original definition of deck transformations, as any automorphism of Y that preserves $\varphi : Y \to Y'$ will also preserve $p' \circ \varphi = p : Y \to X$. This essentially amounts to these automorphisms "fixing" the lower spaces via the covering maps, very similarly to what we saw in Galois Theory. Thus, we intuitively will also later consider some "fixed space" Y^H for some subgroup H.

Another result of this work is that the deck transformations of a universal covering space over any subcovering will be isomorphic to a subgroup of the base space's fundamental group by Theorem 7.1.

Example 7.3: From Examples 5.1 and 5.2, we saw that $(S^1, p_n : z \to z^n)$ is a subcovering of $(\mathbb{R}, p : x \to e^{2i\pi x})$ over S^1. Specifically, this is a result of homomorphism $\tilde{p}_n : x \to e^{\frac{2i\pi x}{n}}$. We then have that $Deck_p(\mathbb{R}/S^1) \cong \mathbb{Z}$ and $Deck_{\tilde{p}_n}(\mathbb{R}/S^1) \cong n\mathbb{Z}$. Thus, we see that the deck transformation over the subcovering spaces are subgroups of the deck transformations over/fundamental group of S^1.

Definition: Let (Y, p) be a normal covering space of X and $G = Deck_p(Y/X)$. If H is a subgroup of G, consider the orbit of $y \in Y$ when H acts on it. Then the *fixed space* Y^H of H is the quotient space formed by mapping any such orbit to a single point (up to isomorphism).

Let $\bar{y}$ be the image of $y \in Y$ and $x = p(y) \in X$. Furthermore, let $\bar{p} : Y^H \to X, \bar{p}(\bar{y}) = p(y)$. We claim that $(Y^H, \bar{p})$ is a subcovering of (Y, p) with respect to X, with the quotient map q acting as our homomorphism. First note that $\bar{p}$ is well-defined, as if $\bar{y} = \bar{y_1}$, then y, y_1 are in the same orbit of $H \subseteq G$, so $y, y_1 \in p^{-1}(x) \Rightarrow \bar{p}(\bar{y}) = p(y) = x = p(y_1) = \bar{p}(\bar{y_1})$. We also see that, by construction, the homomorphism preserves the covering map, $p = \bar{p} \circ q$.

The only other thing we need is that $(Y^H, \bar{p})$ is, in fact, a covering space of X. Let U be some elementary neighborhood of x for the covering space (Y, p). Then because all path-connected components of $p^{-1}(U)$ are mapped topologically onto U by p, any element of $Deck_p(Y/X)$ must homeomorphically permute these components in order to preserve the covering space. Thus, the quotient map q will map disjoint subcollections of these components to path-connected components of $\bar{p}^{-1}(U)$, which will therefore also be mapped topologically onto U by $\bar{p}$. Thus, $(Y^H, \bar{p})$ is a subcovering of (Y, p).

The only remaining fact we need before proving our final theorem is the uniqueness of a deck transformation given an action on one element of the covering space.

Lemma 7.4: Let (Y, p) be a (path-connected) covering space of X and $y \in Y$. Suppose that $\sigma, \sigma_1 \in Deck_p(Y/X)$. If $\sigma(y) = \sigma_1(y)$, then $\sigma = \sigma_1$.

Proof. Let $\sigma(y) = y_1 \Rightarrow p(y) = p(y_1)$. We want to show that this uniquely determines the deck transformation. Because Y is path-connected, then for any $z \in Y$, there exists some path α in Y from y to z. Therefore, $\beta = p \circ \alpha$ is a path in X from $p(y)$ to $p(z)$. $\sigma \in Deck_p(Y/X)$, so $p \circ (\sigma \circ \alpha) = \beta$ as for any $t \in I$, $\sigma \circ \alpha(t)$ and $\alpha(t)$ must map to the same points in X. Thus, because $\sigma \circ \alpha$ is a path in Y from $\sigma(y) = y_1$ to $\sigma(z)$, we know that it is the unique path found from lifting β to a path starting at y_1. So this path must have a unique terminal point, i.e. $\sigma(z)$ is unique. □

A few important results follow from this Lemma. For examples, we know know that the only deck transformation that has any fixed points is the identity. Also, we know that deck transformations act *discontinuously* on the space, i.e. that for any $y \in Y$ there exists a neighborhood V of y such that $\sigma \neq \sigma_1 \Rightarrow \sigma(V) \cap \sigma_1(V) = \emptyset$. This is found be considering the elementary neighborhood U of $p(y)$ and recalling that σ, σ_1 permute the path-connected components of $p^{-1}(U)$ and because y gets mapped to different elements by the two automorphisms, then the path-connected component it lives in also will.

7.1 Fundamental Theorem of Galois Correspondence of Covering Spaces

Now, we can use the FToFGT as a model for proving similar relations surrounding covering spaces and deck transformations. Thus, we will also break up the Fundamental Theorem of Galois Correspondence of Covering Spaces (FTGCCS) into two parts. For all parts, we will assume that (Y, p) is a normal covering space of X with automorphism group $G = Deck_p(Y/X)$.

Part I of FTGCCS: $Y^G = X$, i.e. X is the only space fixed by all automorphisms in G. Furthermore, there exists a bijection between the (path-connected) subcoverings of (Y, p) up to isomorphism and the subgroups of G.

Proof. Following out work from before, we will first prove that $Y^G = X$ by considering X to be a covering of itself via the identity map. Let $x \in X$. Because Y is a normal covering of X, we know that for any $y_1, y_2 \in p^{-1}(x)$, there exists some automorphism $\sigma \in Deck_p(Y/X)$ such that $\sigma(y_1) = y_2$. Thus, the orbit of any $y \in p^{-1}(x)$ under this group action is all of $p^{-1}(x)$. Therefore, the quotient map $q : Y \to Y^G$ will identify all elements of $p^{-1}(x)$ to a single point and $\bar{p}$ is the identity map. This is exactly the same as the quotient map induced by $p : Y \to X$, therefore $(Y^G, \bar{p}) = (X, i_X)$.

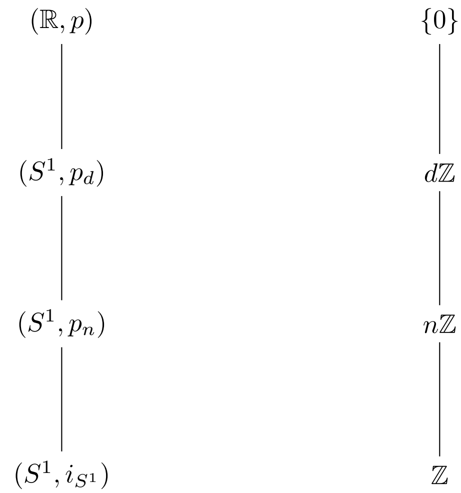
From this, we can develop a bijection between the subcoverings of (Y, p) and the subgroups of G, as Y is normal over any subcovering by Proposition 7.2. Thus, by our earlier work, we have that we can map any subcovering (Y', p') with homomorphism φ to $H = Deck_\varphi(Y/Y') \subseteq G$. Let $\Phi : (Y', p') \to Deck_\varphi(Y/Y')$. By our work above, we know that if $H = Deck_\varphi(Y/Y')$, the $Y^H = Y'$. So $\Phi((Y', p')) = H = \Phi((Y'', p'')) \Rightarrow (Y', p') \cong (Y^H, \bar{p}) \cong (Y'', p'')$. Thus, Φ is injective.

To show that Φ is surjective, we need to consider some subgroup $H \subseteq G$ and show that there is some subcover (Y', p') of (Y, p) such that $\phi((Y', p')) = H$. Naturally, we will consider $(Y', p') = (Y^H, \bar{p})$. As we showed earlier in this section, we already know that the $(Y^H, \bar{p})$ is a subcovering of (Y, p) with homomorphism from the quotient map q. Furthermore, Proposition 7.2 yields that (Y, q) is a normal covering of Y^H. Thus, we just need to show that $Deck_q(Y/Y^H) = H$.

By the way we defined the fixed space, we know that any automorphism in H fixes all points in Y^H under the quotient mapping, so $H \subseteq Deck_q(Y/Y^H)$. So let $\sigma \in Deck_q(Y/Y^H)$ and suppose that $\sigma(y) = y_1$ for some $y, y_1 \in Y$. From Lemma 7.4, if we can find some element of H that has the same action on y, then we will know that these automorphisms are equal and $\sigma \in H$. However, $\sigma \in Deck_q(Y/Y_H) \Rightarrow q(y) = q(y_1)$. By definition, two points in Y only get mapped to the same point in Y^H if they are in the same orbit of H, i.e. if there exists some $\tau \in H$ such that $\tau(y) = y_1$. Thus, by Lemma 7.4, $\sigma = \tau \in H$, so $H = Deck_q(Y/Y^H)$ and Φ is surjective. □

We see that this result is stronger that the one in Galois theory, as our result don't require finiteness. Working with the infinite case in Galois Theory requires that one give the Galois group a topology and focus on the closed subgroups. This actually allows us to use the results from covering spaces over to Galois theory as opposed to our current direction, although we won't be focusing on that.

Example 7.5: Using our work from Examples 5.1 and 5.2, we know that $(\mathbb{Z}, p : x \to e^2 i\pi x)$ is a covering space of S^1 and $(S^1, p_n : z \to z^n)$ is a subcovering for all $n \in \mathbb{Z}^+$ associated with the subgroup $n\mathbb{Z}$. In fact, for all $d|n$, (S^1, p_n) is a subcovering of (S^1, p_d) via the quotient homomorphism $z \to z^{\frac{n}{d}}$ Therefore, we get the below associated diagrams:



Before proving Part II of our Theorem, we must first give an intermediate Lemma similar to one that Jochnowitz uses in her proof of Part II of FToFGT. She claims that a field extension F/k is normal if and only if every $\sigma \in Gal(K/k)$ maps F to itself. This allows her to state that $\sigma(x) \in F, \forall x \in F$. Lemma 7.6 will serve a similar purpose:

Lemma 7.6: Let (Y, p) be a normal cover of X with subcover (Y', p') via homomorphism φ. Suppose that $x \in X$. Then (Y', p') is a normal cover of X if and only if $\varphi \circ \sigma(y_1) = \varphi \circ \sigma(y_2)$, $\forall \sigma \in Deck_p(Y/X), \forall y' \in p'^{-1}(x)$, and $\forall y_1, y_2 \in \varphi^{-1}(y') = f$. Essentially, σ maps the fiber f of y' to the fiber of another element of Y'.

Proof. ($\Leftarrow$) Let $y_1', y_2' \in p'^{-1}(x)$ and $y_1, y_2 \in Y | \varphi(y_1) = y_1', \varphi(y_2) = y_2' \Rightarrow p(y_1) = p(y_2) = x$. (Y, p) is a normal cover of X, so there exists some $\sigma \in Deck_p(Y/X)$ such that $\sigma(y_1) = y_2$. So consider the map $\lambda : Y' \to Y', \lambda = \varphi \circ \sigma \circ \varphi^{-1}$. Note that this mapping is well defined, as φ^{-1} will map any $y' \in Y'$ to its fiber in Y. σ will then send this fiber to another fiber of some $y'' \in Y$ by hypothesis, all elements of which will be mapped to y'' by φ. One can quickly check that λ is continuous by focusing on a specific in Y over Y' and recognizing that all the functions above are homeomorphims within the sheets. Furthermore, λ has continuous inverse $\lambda^{-1} = \varphi \circ \sigma^{-1} \circ \varphi^{-1}$, so it is an automorphism of Y'. λ also fixes X under p' by construction, as any elements getting permuted by σ must map to the same $x \in X$ by p and therefore their images in Y' must also map to that x by p'. Thus, $\lambda \in Deck_{p'}(Y'/X)$ and $\lambda(y'_1) = y'_2$, so (Y', p') is a normal covering of X.

($\Rightarrow$) This follows from our definition of $Y' = Y^H$, where $H = Deck_\varphi(Y/Y')$. Thus, any action by a deck transformation on Y' is actually the transformation acting on the orbits of H in Y. Thus, this action will only be defined if it acts consistently on an orbit and maps it to another orbit, yielding another element of Y'. Let $y'_1, y'_2 \in p'^{-1}(x)$. Then by hypothesis, there exists some $\lambda \in Deck_{p'}(Y'/X)$ such that $\lambda(y'_1) = y'_2$. By our description above, this is the same as there being some $\sigma_1 \in Deck_p(Y/X)$ that maps the orbit $\varphi^{-1}(y'_1)$ to the orbit $\varphi^{-1}(y'_2)$, i.e. maps the fibers of the first elements to the second. Thus, $\forall y_2 \in \varphi^{-1}(y'_2), \exists y_1 \in \varphi^{-1}(y'_1)$ such that $\sigma_1(y_1) = y_2$.

Thus, suppose that there exists some $\sigma \in Deck_p(Y/X)$ such that $\sigma(y) = y_2$ for some $y \in \varphi^{-1}(y_1)$. Then Y normal over Y' implies that there exists some $\tau \in Deck_\varphi(Y/Y')$ such that $\tau(y) = y_1$. So $\sigma_1\tau(y) = \sigma_1(y_1) = y_2$. Thus, by Lemma 7.4, $\sigma_1\tau = \sigma$, so σ permutes the elements of $\varphi^{-1}(y'_1)$ then sends them all to $\varphi^{-1}(y'_2)$. Because our choices of y'_1, y'_2 were arbitrary, we can do this with any such transformation and fiber, so we are done. ☐

Let $F = \{\varphi^{-1}(y') | y' \in p'^{-1}(x)\}$ be the set of these fibers over Y'. So σ simply permutes elements of F, while $\tau \in H = Deck_\varphi(Y/Y')$ will fix every element of F, as that's the same as fixing Y'. This has also shown that we can extend or quotient our deck transformations between Y and Y', similar to results in Galois theory.

Part II of FTGCCS: Suppose that (Y, p) is a covering space of X with subcovering space (Y', p') and homomorphism φ. Then (Y', p') is a normal covering space of X if and only if $H = Deck_\varphi(Y/Y')$ is a normal subgroup of $G = Deck_p(Y/X)$. In this case, we will also show that $Deck_{p'}(Y'/X) \cong Deck_p(Y/X)/Deck_\varphi(Y/Y') = G/H$. Let $x \in X$ be arbitrary and $f = \varphi^{-1}(p') \in F$

Proof. For both parts, we will imitate the proof we saw in Galois theory.

$$
\begin{aligned}
Y' \text{ is a normal covering of } X &\Leftrightarrow \sigma(f) \in F, \forall \sigma \in G, f \in F \text{ (by Lemma 7.6)} \\
&\Leftrightarrow H \text{ fixes } \sigma(f), \forall \sigma \in G, f \in F \text{ (equal to fixing } Y' = Y^H) \\
&\Leftrightarrow \tau\sigma(f) = \sigma(f), \forall \tau \in H, f \in F, \sigma \in G \\
&\Leftrightarrow \sigma^{-1}\tau\sigma(f) = f, \forall \tau \in H, f \in F, \sigma \in G \\
&\Leftrightarrow \sigma^{-1}\tau\sigma \text{ acts as the identity on elements of F}, \forall \tau \in H, \sigma \in G \\
&\Leftrightarrow \varphi \circ (\sigma^{-1}\tau\sigma) = \varphi, \forall \tau \in H, \sigma \in G \\
&\Leftrightarrow \sigma^{-1}\tau\sigma \in H, \forall \tau \in H, \sigma \in G \text{ (as it preserves the covering } \varphi) \\
&\Leftrightarrow H \text{ is a normal subgroup of } G
\end{aligned}
$$

In this case, we will consider the map $\phi : G \to Deck_{p'}(Y'/X), \phi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$ similar to what we saw in Lemma 7.6. As we saw, $\phi(\sigma)$ is a deck transformation of Y' over X, so this map is well-defined. Furthermore, $\forall \sigma, \gamma \in G$,

$$\begin{aligned}\phi(\sigma\gamma) &= \varphi \circ \sigma\gamma \circ \varphi^{-1} \\ &= (\varphi \circ \sigma \circ \varphi^{-1})(\varphi \circ \gamma \circ \varphi^{-1}) \\ &= \phi(\sigma)\phi(\gamma)\end{aligned}$$

so ϕ is a homomorphism. The kernel will be all $\tau \in G$ such that $\phi(\tau) = \varphi \circ \tau \circ \varphi^{-1}$ is the identity transformation on Y'. Therefore it will be the τ such that for any $y \in Y$,

$$\phi(\tau)(\varphi(y)) = \varphi(y) \Rightarrow \varphi \circ \tau(y) = \varphi(y) \Rightarrow \tau \in H$$

Finally, because we can extend any deck transformation of Y' over X to one of Y by Lemma 7.6, this map will be surjective as it will simply return us to the initial transformation. By the First Isomorphism Theorem, we have that

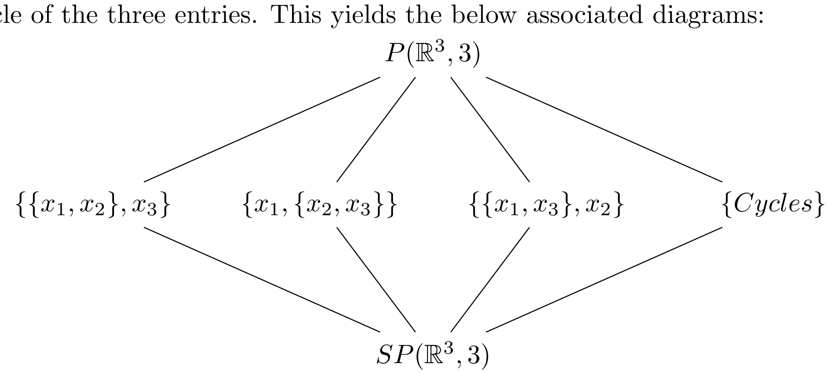
$$Deck_{p'}(Y'/X) = G/Ker(\phi) = G/H = Deck_p(Y/X)/Deck_\varphi(Y/Y')$$

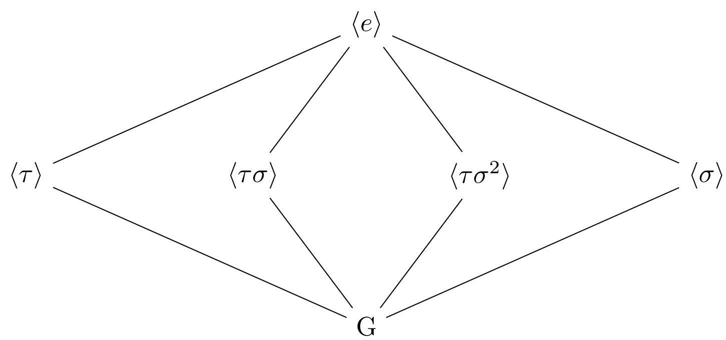
□

Corollary 7.7: If (Y, p) is a universal covering space of X, then there is a bijection between the (normal) subcoverings of Y and the (normal) subgroups of $\pi(X)$.

This follows immediately from applying the FTGCCS to Proposition 7.1.

Example 7.8: Let $x_1, x_2, x_3 \in \mathbb{R}^3$ be distinct. Then consider the permutation space $P(\mathbb{R}^3, 3) = \{(x_1, x_2, x_3)\}$ of order triples. This is a universal covering space of the space $SP(\mathbb{R}^3, 3) = \{\{x_1, x_2, x_3\}\}$ of unordered triples. The symmetric group S_3 acts on this spaces by permuting the entries. Thus, the fixed spaces of any subgroup will be one that is unaffected by the swaps within the subgroup. Suppose that τ is a swap of the first and second entry while σ is a cycle of the three entries. This yields the below associated diagrams:





Here we know that none of the subgroups generated by $\tau, \tau\sigma, \tau\sigma^2$ are normal. One can then see that the associated spaces are not normal, as the elements of S_3 do not act consistently on the fibers of the intermediate space. Thus, these spaces will not be normal coverings of $SP(\mathbb{R}^3, 3)$. However, the subgroup $\langle\sigma\rangle$ is a normal subgroup. The associated covering $\{Cycle\}$ (which quotients all cycles of (x_1, x_2, x_3) is a single point) is also normal, as all elements of S_3 will either fix a cycle or swap the fibers of (x_1, x_2, x_3) with (x_1, x_3, x_2), acting consistently.

8 References

1. Brock, E. (2024). The correspondence of Galois groups and covering spaces (thesis).

2. Collins, C. (2018, May). *Covering Spaces, Graphs, and Groups*. math.uchicago.edu. https://math.uchicago.edu/m̃ay/REU2018/REUPapers/Collins.pdf

3. Dhanwani, N. K., Nair, A. K., & Rajeevsarathy, K. (2020, October). WRITING PERIODIC MAPS AS WORDS IN DEHN TWISTS (thesis). ResearchGate.net. Retrieved April 2, 2026, from https://www.researchgate.net/publication/344802296_Writing_periodic_maps_as_words_in_Dehn_twists.

4. Jochnowitz, N. (2025, February). Lecture 10. Math 437. Rochester.

5. Jochnowitz, N. (2025, February). Lecture 11. Math 437. Rochester.

6. Jänich, K. (1984). Topologie (S. Levy, Trans.). Springer.

7. Lang, S. (2012). Algebra (3rd ed., Vol. 1). Springer Nature.

8. Massey, W. S. (2014). A basic course in algebraic topology. Springer.

9. Ran, D. (2015). AN INTRODUCTION TO THE FUNDAMENTAL GROUP. math.uchicago.edu. https://math.uchicago.edu/ may/REU2015/REUPapers/Ran.pdf

10. Sullivan, J. (2022, August). Covering Spaces. partiallyordered.com. April 1, 2026, https://www.partiallyordered.com/posts/covering-spaces