Galois Theories of Fields and Covering Spaces

Gunjeet Singh (Mentee), Samuel Hsu (Mentor)
Twoples Project

Fall 2021

Contents

Abstract

In these notes, we will briefly introduce the classical Galois theory of fields and the Galois correspondence in covering space theory. We start with the basic field theory necessary to develop classical Galois theory. We will be mainly following Robaldo's thesis[1] for these notes. We refer to Herstein's *Topics in Algebra*[2] as primary text for field theory and some parts of classical Galois theory. The main reason to follow Robaldo's thesis is that he puts both Galois theories in a common framework of category theory, which will later help us to see better, the connections between these two and generalize them to Grothendieck's Galois theory, which is our aim for the next semester.

As for the prerequisites, We will assume familiarity with basic group and ring theory, and some categorical language when needed.

1 Field Theory

Fields are a special kind of rings. Apart from being an abelian group with respect to addition, $F \setminus \{0\}$ forms an *abelian* group under multiplication as well. Unlike in ring theory, here we will be primarily interested in subfields, or put in another way, *field extensions* and field automorphisms.

1.1 Field Extensions

Let F be a field. Then a field K is said to be an *extension* of F if F is a subfield of K. We will denote a typical field extension by K/F (*not to be confused with the quotient structure*).

Example 1.1. Some examples are - $\mathbb{C}/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $F(x)/F$ where $F(x)$ is the field of fractions of the ring of polynomials over F, that is, $F[x]$.

In the second example above, $\mathbb{Q}(\sqrt{2})$ represents the smallest field generated by $\mathbb{Q}$ and $\sqrt{2}$. In fact, we can see that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ but in general, $F(\alpha)$ is the field of rational functions in α where, α is some element in the extension K of F.

In general, if $S \subseteq K$, then $F(S)$ is the smallest subfield of K which contains F and S. In particular, if S is a singleton set, say a, then $F(a)$ is called a *simple extension* of F.

Now, we can consider K as a vector space over the field F where, K/F is some field extension (in fact, K has more structure than scalar multiplication, that is of multiplication). Then we define

Definition 1.2. *Degree* of K/F (denoted by $[K : F]$) is the dimension of K considered as vector space over F. When K is finite-dimensional vector space over F, we say that K is a *finite extension* of F.

Theorem 1.3. *If L is a finite extension of K and K is a finite extension of F then, L is a finite extension of F. Moreover,* $[L : F] = [L : K][K : F]$.

Proof. The main strategy of the proof is to explicitly find a basis for L over F. For this, let $[L : K] = n$ and $[K : F] = m$ with the basis elements $v_1, v_2, ..., v_n$ and $w_1, w_2, ..., w_m$ respectively. Then the elements $v_i w_j \in L$ with $i = 1, 2, .., n$ and $j = 1, 2, ..., m$ form a basis for L over F and this proves the theorem. □

Theorem 1.4. *An element $a \in K$ is algebraic over F if and only if $[F(a) : F]$ is finite.*

Proof. Let $a \in K$ be algebraic over F. Then we define a function

$$\begin{aligned} \varphi_a : F[x] &\to F(a) \\ \varphi_a(f(x)) &= f(a) \end{aligned}$$

Now, it is easy to see that φ_a is a ring homomorphism and $Ker\, \varphi_a = (p(x))$ $(= V$, say) where, $(p(x))$ is ideal generated by $p(x)-$ smallest degree irreducible polynomial in $F[x]$ such that $p(a) = 0$. Then $F[x]/V$ is a field isomorphic to $F(a)$ (because $F[x]/V$ contains F and a). Then the image of the basis set $1, x, x^2, ..., x^n$ where n is the degree of $p(x)$ forms a basis of $F(a)$ as a vector space over the field F. This proves one side of the theorem while the other direction is trivial. This proves the result. □

From this result, we can define that two elements of an algebraic extension K/F are conjugated, if they have the same minimal polynomial with coefficients in F. Some easy, yet important consequences of the above results are

Corollary 1.5. *If L/K and K/F are algebraic extensions, then L/F is algebraic.*

Corollary 1.6. *Any finite extension K/F is an algebraic extension.(Converse is not true in general)*

Theorem 1.7. *An element $a \in K$ is algebraic over F if and only if $[F(a) : F]$ is finite.*

Proof. Now, it is easy to see that φ_a is a ring homomorphism and $Ker\, \varphi_a = (p(x))$ $(= V$, say) where, $(p(x))$ is ideal generated by $p(x)-$ smallest degree irreducible polynomial in $F[x]$ such that $p(a) = 0$. Then $F[x]/V$ is a field isomorphic to $F(a)$ (because $F[x]/V$ contains F and a). Then the image of the basis set $1, x, x^2, ..., x^n$ where n is the degree of $p(x)$ forms a basis of $F(a)$ as a vector space over the field F. This proves one side of the theorem while the other direction is trivial. This proves the result. □

1.2 Splitting Fields

In the previous section, we considered elements in a given extension K/F which were algebraic over F. Now we turn our focus to polynomials $p(x)$ in $F(x)$ and wish to find an extension K of F over which $p(x)$ has a root.

Definition 1.8. An element $a \in K$ is a root of $p(x) \in F(x)$ of *multiplicity* m if $(x-a)^m | p(x)$, whereas $(x-a)^{m+1} \nmid p(x)$.

With this terminology at hand, we can prove using mathematical induction that

Lemma 1.9. *A polynomial of degree n over a field can have at most n roots in any extension field.*

Now we establish the existence of an extension, corresponding to some polynomial $p(x) \in F(x)$, where $p(x)$ has some root.

Theorem 1.10. *If $p(x) \in F(x)$ is a polynomial of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F, such that $[E : F] = n$, in which $p(x)$ has a root.*

Proof. Let $V = (p(x))$ be the ideal of $F(x)$ generated by $p(x)$. Then we know that $E = F[x]/V$ is a field. Identifying F with its image $\overline{F}$ in E via the quotient map, it is easy to see that E is the required extension of F. It is done by considering the natural basis of E. This proves the theorem. □

Using this result and Theorem 1.3, we can in fact prove that there is an extension E of F of degree at most $n!$ in which $f(x)$ has n roots.

Definition 1.11. If $f(x) \in F[x]$, a finite extension E of F is said to be a *splitting field* over F for $f(x)$ if over E, but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

Note that then the above paragraph establishes that for any given polynomial $p(x)$, we are guaranteed the existence of *a* splitting field. But an immediate question is, whether a given polynomial has a unique splitting field? If not, then what is the relation between the different splitting fields that it has?

To answer this, suppose we have two isomorphic fields F and F' with the isomorphism τ. For convenience sake, we denote the image of any $a \in F$ by a'. Then using τ, we can easily establish an isomporhism τ^* between $F[x]$ and $F'[t]$ by sending $f(x) = \sum_{k=1}^{n} a_k x^k$ to $\sum_{k=1}^{n} \tau(a_n) x^n$.
Now in a similar fashion, we can extend this analysis to establishing an isomorphism τ^{**} between $F[x]/(f(x))$ and $F'[t]/(f'(t))$ where, $f'(t) = \tau^*(f(x))$.

Theorem 1.12. *If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$; moreover, this isomoprhism σ sends v to w and preserves F.*

Proof. Refer to [2], theorem 5.3.3. □

Corollary 1.13. *If $p(x) \in F(x)$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takes a onto b and fixes F.*

Using this result, we can prove one of the most important theorems related to Galois theory.

Theorem 1.14. *Any splitting fields E and E′ of the polynomials $f(x) \in F(x)$ and $f'(t) \in F'[t]$, respectively, are isomorphic by an isomorphism ϕ with the property that it equals τ when restricted to F.*

Proof. Refer to [2], theorem 5.3.4. □

1.3 Algebraic Closure of Fields

A field L is called algebraically closed, if it has no algebraic extensions over itself. We can indeed prove the existence of an algebraically closed extension for any field F and the proof requires *Zorn's lemma*.
Further, we define the *algebraic closure of a field* F as the algebraically closed extension of F which also an *algebraic extension of* F. Its existence can be established using the result that the subset of algebraic elements of a field extension K/F is a subfield of K. Also by the definition, it is an algebraic extension of F.

To prove the existence, we consider the collection of all algebraic elements in an algebraically closed extension of F. These elements forming a subfield of the given extension is the required algebraic closure of F.

It can also be proved that all algebraic closures are isomorphic for a given field F (just like the splitting fields of a given polynomial are isomorphic). We denote the algebraic closure of a field F by $\overline{F}$.

1.4 Morphisms between Algebraic Extensions

To see the relation between classical Galois theory and covering space theory, we need a common framework in which we can formulate both of them and see their relationship. That framework is provided by category theory. So for classical Galois theory, we consider the collection of all field extensions of a particular field F. We want to take these as objects of certain category which we will denote by $\mathbf{E}(F)$.
Now to make $\mathbf{E}(F)$ into a category, we need to define morphisms between two extensions and prove that they satisfy all the properties of a category.

We define a morphism between K_1/F and K_2/F of a particular field F as a morphism $\sigma : K_1 \to K_2$ such that $\sigma(x) = x \ \forall x \in F$. Now since this means any such morphism is non-trivial, kernel of it will contain zero of F only and hence, *all such morphisms are injective.*

Proposition 1.15. *Every endomorphism of an algebraic extension is an automorphism.*

Proof. Let $\sigma : K/F \to K/F$ be an endomorphism. Since by above discussion, we know that σ is injective, we only need to show that it is surjective. So let $u \in K$ be some element. Since K is an algebraic extension, consider the minimal polynomial $f(x) \in F[x]$ of u. Note that $\sigma(f(x)) = f(\sigma(x))$ only since the coefficients are the base field F. So, $\sigma(f(u)) = 0 = f(\sigma(u))$ which implies, $\sigma(u)$ is also a root of $f(x)$. Hence, σ preserves the roots of $f(x)$. (This can be proved in general also using the same argument). Then restricting σ on the set of roots of $f(x)$ (call it S_g), we get a surjective map (because S_g is finite and σ is already injective) and hence a bijection. Therefore, there exists another root $v \ni \sigma(v) = u$. This proves the proposition. □

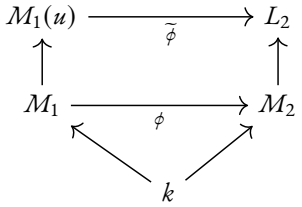
Proposition 1.16. *Every endomorphism of an algebraic extension is an automorphism.*

Proof. Let $\sigma : K/F \to K/F$ be an endomorphism. Since by above discussion, we know that σ is injective, we only need to show that it is surjective. So let $u \in K$ be some element. Since K is an algebraic extension, consider the minimal polynomial $f(x) \in F[x]$ of u. Note that $\sigma(f(x)) = f(\sigma(x))$ only since the coefficients are the base field F. So, $\sigma(f(u)) = 0 = f(\sigma(u)) \implies \sigma(u)$ is also a root of $f(x)$. Hence, σ preserves the roots of $f(x)$. (This can be proved in general also using the same argument). Then restricting σ on the set of roots of $f(x)$ (call it S_g), we get a surjective map (because S_g is finite and σ is already injective) and hence a bijection. Therefore, there exists another root $v \ni \sigma(v) = u$. This proves the proposition. □

1.4.1 Lifting Morphisms of Field Extensions

Let $L_1/M_1/F$ and $L_2/M_2/F$ be two sequences of field extensions of F. Given an *isomorphism* of extensions $\phi : M_1/F \to M_2/F$ we look for conditions to extend ϕ to a morphism $\widetilde{\phi} : L_1/F \to L_2/F$.

Lemma 1.17. *Let the setup be as above. Then if $u \in L_1$ is algebraic with the minimal polynomial $f(x) \in M_1[x]$, then $\widetilde{\phi}$ exists if and only if $\overline{f}(x) \in M_2[x]$ has at least one root in L_2. Moreover, the number of such extensions are equal to the number of roots of $\overline{f}(x)$ in L_2.*



Proof. If such extension $\widetilde{\phi}$ exists of ϕ, then it is clear that $\widetilde{\phi}(u) \in L_2$ is a root of $\overline{f}(x)$. Conversely, if $\overline{f}(x)$ has a root $\alpha \in L_2$, then we can construct a morphism $\widetilde{\phi}$ which sends $u \longrightarrow \alpha$ and is equal to ϕ on M_1. From this construction, the other part of the lemma is obvious. □

Now using this lemma and Zorn's lemma, we can prove a theorem which comes in handy in discussion on separable and normal extensions.

Theorem 1.18. *Let the setup be as of lemma 1.2 with the additional conditions that L_1/M_1 is algebraic and L_2/M_2 is algebraically closed, then there exists an inclusion morphism of extensions $\widetilde{\phi}$.*
Moreover if both L_1/M_1 and L_2/M_2 are algebraic closures, then $\widetilde{\phi}$ is an isomorphism.

Proof. The proof can be given by repeated application of the above lemma. We consider a chain of finite algebraic extensions (of the form $M(u_1)(u_2)...$ of M where, u_i are the elements of algebraic extension L_1. Then from the above lemma, we will get successive extensions of ϕ, each going into L_2 only since it is algebraically closed. Then we invoke Zorn's lemma and the fact that L_1 is algebraic, to conclude that the limit of all these extensions of ϕ is indeed our desired extensions of ϕ.
The other part can also be easily proved subsequently. □

An immediate corollary of this theorem is that every algebraic extension K/F is embedded as an intermediate extension of $\overline{F}/K/F$.

1.5 Some Special Types of Extensions

We will give only the definitions and then start our discussion on Galois extensions.
Since the splitting fields are algebraic (because they are finite extensions), they can be embedded in algebraic closure as well. Hence, a polynomial f in $F[x]$ splits completely into linear factors in $\overline{F}[x]$. We then say that f is a *separable polynomial* if it has no repeating roots. In other words, each root of f has multiplicity 1. We then define that an elements $u \in K$ of an extension K/F is separable, if its minimal polynomial is separable.

Definition 1.19. An extension K/F is said to be separable, if it is algebraic and all of its elements are separable. Furthermore, a field F is said to be *perfect* if all of its algebraic extensions are separable.

Now we turn our attention to exact extensions and then finally, we will define normal extensions.

We use the notation $Aut_{\mathbf{E}(F)}(K/F)$ to denote the group of automorphisms of an extension K/F, that is, all automorphisms of K which are constant of F.

So now let's see the relation between $Aut_{\mathbf{E}(K)}(L/K)$, $Aut_{\mathbf{E}(F)}(K/F)$, $Aut_{\mathbf{E}(F)}(L/F)$ for a sequence of *algebraic* extensions $L/K/F$.

1. $Aut_{\mathbf{E}(K)}(L/K) \subseteq Aut_{\mathbf{E}(F)}(L/F)$ clearly because F is a subfield of K.

2. If $\forall\, \sigma \in Aut_{\mathbf{E}(F)}(L/F)$, we have $\sigma(K) \subseteq K$, then there is a natural group homomorphism from $Aut_{\mathbf{E}(F)}(L/F)$ to $Aut_{\mathbf{E}(F)}(K/F)$ sending $\sigma \longrightarrow \sigma|_K$. The *kernel* of this map will be all automorphisms of L which preserve K and hence kernel is exactly $Aut_{\mathbf{E}(K)}(L/K)$. Thus we have a left-exact sequence of groups

$$1 \longrightarrow Aut_{\mathbf{E}(K)}(L/K) \longrightarrow Aut_{\mathbf{E}(F)}(L/F) \longrightarrow Aut_{\mathbf{E}(F)}(K/F)$$

Surjectivity of this map corresponds to the extensionability of endomorphisms on K/F to L/F. So if the map is surjective, then we have $Aut_{\mathbf{E}(F)}(K/F)$ isomorphic to quotient group $Aut_{\mathbf{E}(F)}(L/F)/Aut_{\mathbf{E}(K)}(L/K)$; we also have the following exact sequence of groups

$$1 \to Aut_{\mathbf{E}(K)}(L/K) \to Aut_{\mathbf{E}(F)}(L/F) \to Aut_{\mathbf{E}(F)}(K/F) \to 1$$

.

Definition 1.20. We say that a sequence of extensions $L/K/F$ is exact if the restriction operation $Aut_{\mathbf{E}(F)}(L/F) \to Aut_{\mathbf{E}(F)}(K/F)$ is a well-defined surjective group homomorphism, inducing a short exact sequence of groups, as above.

Now we define Normal Extensions.

Definition 1.21. K/F is a normal extension if it is algebraic and if all the irreducible polynomials having one root in K have all the other roots in K as well.

Clearly, any algebraically closed extension K/F is normal. Moreover, if $L/K/F$ is a tower of extensions, then L/F being normal implies L/K is normal.

We now state a useful proposition without proof. The proof can be found in [1], Section 3.1.7.

Proposition 1.22. *Let K/F be an algebraic extension. Then considered as subextension of $\overline{F}/F$, K/F is normal if and only if every automorphism σ of $\overline{F}/F$ is an automorphism of K/F when restricted to K, that is, $\sigma(K) = K$.*

2 Galois Theory

Let K/F be a field extension. Then we consider the action of a group G on it as a group homomorphism from G to $Aut_{\mathbf{E}(F)}(K/F)$.
We then define $Fix(G)$ as subset of K such that all elements in it are fixed by action of G. It is not hard to see that $Fix(G)$ is a *subfield of K*. Also, for a subgroup H of G, $Fix(G) \subseteq Fix(H)$.

Definition 1.5: We define an algebraic extension K/F as a Galois extension if $Fix(Aut_{\mathbf{E}(F)}(K/F)) = F$. In this case, we say that $Aut_{\mathbf{E}(F)}(K/F)$ is the *Galois Group of the extension*.

It is immediately clear that for a sequence $L/K/F$, if L/F is a Galois extension, then L/K is also a Galois extension. We now state two facts without proof.

1. Any Galois extension is normal and separable.
2. Any separable closure F_S/F is a Galois extension.

Definition 2.1. The absolute Galois Group of a field F is the group $Aut_{\mathbf{E}(F)}(F_S/F)$. We denote it by $Gal(F)$.

2.1 Classification of subextensions of a Finite Galois Extension

From lemma 1.17, it is clear that

$$|Hom_{\mathbf{E}(F)}(K/F, \overline{F}/F)| \leq [K : F]$$

Equality holds when K/F is a separable extension. Further if the extension is normal, then by proposition 1.22, every automorphism of $\overline{F}/F$ is a automorphism of K/F. Therefore, $|Hom_{\mathbf{E}(F)}(K/F, \overline{F}/F)| = |Aut_{\mathbf{E}(F)}(K/F)|$

Proposition 2.2. *If an extension K/F is finite and Galois (that is, separable and normal), then its Galois Group is finite and*

$$|Aut_{\mathbf{E}(F)}(K/F)| = [K : F]$$

Proposition 2.3 (*Artin's lemma*)**.** *Let G be a finite group acting on a field L by automorphisms. Then the extension $L/Fix(G)$ is finite and $[L : Fix(G)] \leq |G|$.*

Refer to [3] for its proof.

Now we come to the main theorem of classical Galois theory of fields.

Theorem 2.4. *Let L/F be a finite Galois extension with the Galois group G. Then there is a bijection between the set of intermediate extensions $L/K/F$ and the subgroups of G.*

Proof. From our discussion of exact extensions in section 1.5, we know that $Aut_{\mathbf{E}(K)}(L/K)$ is a subgroup of $G = Aut_{\mathbf{E}(F)}(L/F)$. Now since L/F is finite and Galois, L/K is also finite and Galois which gives $K = Fix(Aut_{\mathbf{E}(K)}(L/K))$ by the definition of Galois extensions (as all finite extensions are algebraic).

Now given any subgroup H of G, we can have an intermediate extension $L/Fix(H)/Fix(L)$ where $Fix(L) = F$ by definition. So now we want to prove that $Aut_{\mathbf{E}(Fix(H))}(L/Fix(H)$ is exactly equal to H so that we can have our required bijective correspondence. Note that by Artin's lemma, we already have $[L : Fix(H)] \leq |H|$ (considering action of H on L). Now since L/K is Galois, $L/Fix(H)$ is also Galois and therefore, $|Aut_{\mathbf{E}(Fix(H))}(L/Fix(H)| = [L : Fix(H)]$. For the other side of inequality, note that H is already a subset of $Aut_{\mathbf{E}(Fix(H))}(L/Fix(H)$ and hence, we have $|Aut_{\mathbf{E}(Fix(H))}(L/Fix(H)| \geq |H|$. Since these groups are finite, they are equal. Hence the theorem is proved. □

3 Covering space theory

We now switch to a classic topic in topology. Here, instead of Galois groups given by automorphisms of a field fixing a certain subfield, we want to look at automorphisms of a cover which act transitively on the fibers of a covering $p : Y \twoheadrightarrow X$. In this analogy, instead of Galois groups acting on the finite set consisting of some roots of a polynomial we have a group $Aut(Y, p)$ acting on the fibers of p. Here we are primarily following chapter 4 of [**?**].

One may object that usually the analogy invokes the *fundamental group* acting on the set consisting of the fiber $F \to Y \twoheadrightarrow X$ via path lifting. This isn't a major issue though since for locally path-connected, semi-locally simply connected spaces X we have the structure theorem which states the category $\mathbf{Cov}(\mathbf{X})$ of covers of X is equivalent to $\mathrm{Fun}(\Pi_1(X), \mathrm{Set})$, the category of functors from the fundamental groupoid of X to the category of sets. We will have a few more words to say about this in Section 4.

3.1 Fundamental Group of a Topological space

Let X be a topological space. Then a *path* on X is a continuous function $p : I = [0, 1] \to X$ with $p(0)$ as initial point and $p(1)$ as end point. A loop is a path with same end points.

Definition 3.1. Let f and g be two continuous functions from space X to Y. Then they are **homotopic relative to** A, $A \subset X$, if there exists a continuous map H called homotopy, such that

$$\begin{aligned} &H : X \times I \to Y \\ &H(x, 0) = f(x),\ H(x, 1) = g(x) \\ &H(x, t) = x\ \forall x \in A,\ t \in I \end{aligned}$$

A special case for this is *path homotopy*, defined between two paths p and p' on X starting and ending at the same points. Thus we have there $X = I$ and $A = \{p(0),\ p(1)\}$.

It is easy to see that homotopy defines an equivalence relation on the set of all paths on a space X. We denote $[p]$ to be the path-equivalence class of all paths on X.

Given two paths p_1 and p_2 such that $p_1(1) = p_2(0)$, we can define a third path p by concatenating the two paths as follows:

$$p(t) = p_1 \circ p_2(t) = \begin{cases} p_1(t), & t \in [0, 1/2] \\ p_2(t), & t \in [1/2, 1] \end{cases}$$

Using this operation of concatenation, we can in fact, define a well-defined operation on the set of all path-homotopy classes of X as $[p]*[q] = [p \circ q]$. It is not so difficult to show that this operation is associative (whenever defined), and has left and right identities (path homotopy classes of constant paths at initial and final endpoints of a path, respectively). Moreover, we can define the inverse of a $[p]$ as $[p^{-1}] \ni p^{-1}(t) = p(1-t)$.

We can somehow make a category with this operation. The process is to take objects as all the points in our topological space X. We also assume that *it is path-connected* so that there is atleast one path between two arbitrary points in the space. Now we define the $Hom(x, y)$ as the set of all path-homotopy classes between x and y. With the above concatenation operation defined on the set of path-homotopy classes, we actually have a category. Since every path-homotopy class has an inverse and the collection of objects is actually a *set*, this category is a *groupoid* and we denote it by $\Pi_1(X)$. We call it the *Fundamental Groupoid of X*.

For each point $x \in X$, we have its automorphism group $Aut_{\Pi_1(X)}(x)$. It is called the *Fundamental Group of X based at x* (denoted by $\Pi_1(X, x)$).

3.2 Covering Spaces

Definition 3.2. A covering space over x, is a topological space Y which admits a *surjective* continuous map $p : Y \to X$ with the property that for each $x \in X$, there is an open neighborhood V_x such that $p^{-1}(V_x)$ is a disjoint union of open sets U_i (where i belongs to some indexing set I) and each U_i is homeomorphic to V_x via the map p.

It is not hard to see that covering maps are local homeomorphisms, and thus, are *open*. We now define a morphism between two such covers, (Y, p) and (Z, p'), as a continuous map $\phi : Y \to Z$ satisfying $p' \circ \phi = p$. With these morphisms, covering spaces over X form a category called **Cov(X)**.

These maps also preserve the fibers structure. We say that y is a "point over x" if y belongs to the fiber of x. The fiber of any point in the base space is a *discrete subset of the covering space*. if the base space X is connected, then the cardinality of fibers is constant and that number is known as the *degree of cover*.

This can be proved by noting that cardinality of $p^{-1}(x)$ is a locally constant map. Then if we partition the space X by the equivalence relation: $x \sim y$ iff the fibers of both have the same cardinality; then each partition is an open set of X and since in our case, X is connected, we have a trivial partition, that is, cardinality of all fibers is same. The cover is called finite if its degree is finite. **We will restrict ourselves to covers of locally path-connected, connected spaces only.**

We say that a cover $q : Z \to X$ is an intermediate cover of $p : Y \to X$ if there is a covering morphism $f : (Y; p) \to (Z; q)$. Then we might be tempted to assume that Y is then a covering space of Z. But it is not always the case and let's see when it actually holds.

Proposition 3.3. *For $p : Y \to X$ any covering space and $q : Z \to X$ a connected cover, any covering morphism from Y to Z given by a map $f : Y \to Z$ is a covering map of Z.*

Proof. For a point $z \in Z$, we may take a connected neighborhood V of point $q(z)$ in X, which satisfies the covering property for both p and q. Hence, $p^{-1}(V) = \bigcup(U_i)$ in Y and $p^{-1}(V) = \bigcup(V_i)$ in Z. Since, each U_i is homeomorphic to V, it is connected and its image $f(U_i)$ is also connected. Further, the commutation relation $q \circ f = p$ implies that it is equal to one of V_j's. Now since morphisms of covers preserve fibers, the open set V_k in which z lies, is the desired neighborhood which satisfies the covering property w.r.t. f (because we now have $f^{-1}(V_k) = \bigcup(U_i)$).

For surjectiveness, we can apply the above reasoning to any point $y \in Y$ (by putting $z = f(y)$). Hence, $f(Y)$ is the union of all such open sets in Z and hence is open in Z. So if we now prove that $f(Y)$ is closed in Z, we are done by connectedness of Z. For this, take any point $z \in (f(Y))^c \subseteq Z$ and a neighborhood W of $q(z)$ which satisfies the covering property w.r.t. both p and q. Then z is in one of the stacks W_k. This is clearly disjoint with $f(Y)$. Hence, $f(Y)$ is closed. □

3.2.1 New Covering Spaces from Old

Consider an action of group G on a topological space Y. Then we can construct a natural quotient space Y/G by sending each point $y \in Y$ to its equivalence class $[y]$ via the quotient map π. We can equip Y/G with a quotient topology using the map π and this will satisfy the universal property of quotient maps as well.
We are interested in a special type of group action.

Definition 3.4. Let a group G acting on a topological space Y. Then the action is called an *even action* if for every point $y \in Y$, there is an open neighborhood U of it such that $g(U) \bigcap g'(U) = \emptyset$ for every $g \neq g'$.

Such actions produce covering spaces.

Proposition 3.5. *If G acts evenly on Y, then the quotient map $\pi : Y \to Y/G$ is a covering map of Y/G.*

Proof. For each $y \in Y$, pick neighborhoods U_y which satisfy the condition of even group action. Then each $g(U_y)$ is a disjoint subset for different $g \in G$ and is open, since it is just a homeomorphic image of open set U_y. By the definition of quotient map π, U_y is mapped to $\pi(U_y)$. Further, each member of $g(U_y)$ is in the equivalence class of its corresponding element in U. Hence, we can identify each $g(U_y)$ with $\pi(U_y)$ via the map π. Therefore, union of $g(U_y)$ for all $g \in G$, forms the inverse image of the $\pi(U_y)$ and therefore, $\pi(U_y)$ is open in Y/G (by the definition of quotient topology); it is also then a neighborhood of $\pi(y)$. Hence the result. □

3.3 Action of $Aut_{\mathbf{Cov(X)}}(Y, p)$ on Y

First we will discuss automorphisms of coverings and then consider their natural action on the corresponding covering space.

Automorphisms of a covering $p : Y \to X$ such that the homeomorphisms $Y \to Y$ commute with p, that is, given a homeomorphism ψ of Y, $p \circ \psi = p$.

Lemma 3.6. *Let $p : Y \to X$ be a covering map. Let Z be a connected topological space and consider maps $f, g : Z \to Y$ with $p \circ f = p \circ g$. If f and g are equal at one point they have to be the same map.*

Proof. The idea is to show that the subset of Z where f and g coincide (name it A), is both, open and closed in Z which by the connectedness of Z, will equal to whole Z then. Suppose that for $z \in Z$, $f(z) = g(z) = y$ (say). Then consider the neighborhood U of $p(y)$ which satisfies the covering map conditions. Hence, there is a disjoint collection U_i of open subsets in Y each of which, is homeomorphic to U via the map p. Now since $f(z)$ and $g(z)$ are equal, they lie in the same such open set U_k for some k. Then the neighborhood $W = f^{-1}(U_k) \bigcap g^{-1}(U_k)$ is a subset of Z where f and g agree. Because if they don't, then for any such $w \in W$, it will have two distinct images in U_k, and thus two distinct images in U which contradicts the fact that $p(f(w)) = p(g(w))$.

To show that A is closed in Z, we show that its complement A^c is open. So choose any point $z \in A^c$. Then $f(z) \neq g(z)$, but $p(f(z)) = p(g(z))$. Then using the same argument as above, we have that $f(z)$ and $g(z)$ lie in distinct open subsets U_i and U_j. Then W as defined above, is the required neighborhood of z where f and g are distinct. This proves the lemma. □

In particular, *if a covering automorphism of a connected cover has a fixed point, that is, if it is equal to the identity map at some point, then it has to be the identity map.*

Now, given a covering space Y over X, there is a natural action of the group $Aut_{\mathbf{Cov(X)}}(Y, p)$ on Y where each automorphism $\psi : Y \to Y$ sends $y \in Y$ to $\psi(y)$, preserving the fiber structure. If we consider group action as a group homomorphism, then this group action corresponds to the identity homomorphism on $Aut_{\mathbf{Cov(X)}}(Y, p)$, which is a subgroup of automorphism group of Y - $Aut(Y)$ (the group of *all* homeomorphisms on Y).

Proposition 3.7. *For a connected cover $p : Y \to X$, the above action is even.*

Proof. Let $y \in Y$ be any element. Then for $p(y) = x$, we have by the definition of covering map, an open neighborhood V of x such that $p^{-1}(V)$ is a union of disjoint open sets V_i in Y. Then $y \in V_k$ for some k. Since any automorphism of covering space preserves fiber structure, every automorphism ψ takes V_k to some other V_i.

Now we know that Y is connected and also that for any two automorphisms ψ_a and ψ_b for $a, b \in Y$, $p \circ \psi_a = p \circ \psi_b$ because, $p \circ \psi_a = p \circ \psi_b = p$ by definition of automorphisms of covering spaces. Hence by lemma 3.6, if $\psi \neq id_Y$, then $i \neq k$. Thus, V_k is the required neighborhood of y whose image under each element of $Aut_{\mathbf{Cov(X}}(Y, p)$ is distinct. Therefore, the action is even. □

Therefore by Proposition 3.5, Y is a covering space of $Y/Aut_{\mathbf{Cov(X)}}(Y, p)$ via the quotient map. Also by the definition of automorphisms of coverings, the automorphism group of this covering is precisely, $Aut_{\mathbf{Cov(X)}}(Y, p)$. In general,

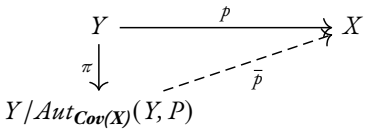
Proposition 3.8. *If a group G acts evenly on a space Y, then the group of automorphisms of the covering $Y \to Y/G$ is G itself.*

3.4 Galois Coverings and Classification of their subcoverings

Definition 3.9. A cover $p : Y \to X$ is a *Galois cover* if the action of $Aut_{\mathbf{Cov(X)}}(Y, p)$ on each of its fibers is transitive. In other words, for any given $x \in x$ and two points y and y' in its fiber, there is a covering automorphism on Y which takes y to y'. In this case, we call $Aut_{\mathbf{Cov(X)}}(Y, p)$ the *Galois group of the covering*.

Requiring the action of $Aut_{\mathbf{Cov(X)}}(Y, p)$ to be transitive is analogous to studying the Galois groups of irreducible polynomials: for reducible polynomials we normally study the Galois groups of each irreducible factor since for irreducible polynomials the Galois group acts transitively on the set of roots. Note that in general, for the natural group action of $Aut_{\mathbf{Cov(X)}}(Y, p)$ on Y takes $y \in Y$ to its equivalence class $[y]$. But since automorphisms preserve fiber structure, each element of $[y]$ lies in the fiber of $p(y)$, that is, $[y]$ is a subset of fiber of $p(y)$. But for Galois covers, there is equality here meaning $[y]$ is *equal to* fiber of $p(y)$. In this way, Galois covers are very special, "nice" covers and so we can expect certain nice properties of them which we will see now. Now let's see another characterization of Galois coverings:

Proposition 3.10. *A covering $p : Y \to X$ is Galois if and only if $\overline{p}$ is a homeomorphism.*



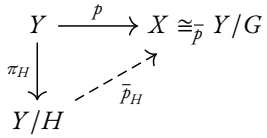
Proof. From the universal property of quotient spaces, we know that $\overline{p}$ is continuous. It is also surjective and an open map because p is both, surjective and open. So now if Y is a Galois cover, then the action of $Aut_{\mathbf{Cov(X)}}(Y, p)$ is transitive on fibers and therefore the equivalence class of each $y \in Y$ is the whole fiber of $p(y)$. Hence if $\overline{p}(y) = \overline{p}(y')$, then this implies $p(y) = p(y')$. Therefore, both y and y' are in the same fiber and hence have the same equivalence class.

Conversely, if $\overline{p}$ is injective, suppose y and y' be two points in Y in the same fiber. Then by the commutation diagram above, $\overline{p}(y) = \overline{p}(y')$ which implies $y \sim y'$. This means that the action is transitive on the fibers and hence the cover Y is Galois. □

Corollary 3.11. *In particular, by Proposition 3.8, the $Y \to Y/G$ is also a Galois covering as here, $\overline{p}$ will correspond to the identity map which is indeed, a homeomorphism.*

Now we want to bring out a correspondence between the subgroups of G, which in our case will be $Aut_{\mathbf{Cov(X)}}(Y, p)$, and the subcovers of $Y \to X$.

So consider a cover $Y \to X$ with its automorphism group G, that is, $Aut_{\mathbf{Cov(X)}}(Y, p)$. Then for any subgroup H of G, the action of H on Y will also be even (because G acts evenly on Y). Therefore, the group of automorphisms of $Y \to Y/H$ will be H itself by Proposition 3.8 and $Y \to Y/H$ will be a covering by Proposition 3.5. It is in fact, a Galois cover by the above corollary.



Now we consider the inverse problem that given $Y \to X$ a Galois cover with an intermediate connected cover $Z \to X$, we want to find a subgroup H of G for which $Z \cong Y/H$.

We can assume Z is connected by restricting Z to a single path-component, and in turn Y to a single component of Z since continuous maps must preserve path-connected components. Each restriction of $Y \to X$ remains Galois, because by definition $Aut_{\mathbf{Aut(X)}}(Y, p)$ acts transitively and evenly on Y.

Note that given any connected subcover $q : Z \to X$ of the cover $p : Y \to X$, the covering transformation $f : Y \to Z$ is a covering of Z by Proposition 3.3. Now for an automorphism ϕ of Y over Z, $f \circ \phi = f$ implies $p \circ \phi = p$ (by composing with q) and thus, ϕ is also an automorphism of Y over X. Now define $H := Aut_{\mathbf{Cov(Z)}}(Y, f)$; then $H \subseteq G$. We now prove that $f : Y \to Z$ is Galois. For that, let z_1, z_2 be two points in the fiber of $z \in Z$. Then both these points also lie in the fiber $p^{-1}(q(z))$. Since $p : Y \to X$ is already a Galois cover, there exists an automorphism $\psi \in G$ for which, $\psi(z_1) = z_2$. This means $f(z_1) = f(z_2) = f \circ \psi(z_1)$. We look at copies of z_1 and z_2 which lie in the same connected component of Y. For these, because Z was assumed to be connected, z_1 and z_2

Then by lemma 3.6, f and $f \circ \psi$ are equal and hence, ψ belongs to H as well. It is also easy to see now that $Z \cong Y/H$. Therefore we have the following correspondence:

Theorem 3.12. *Let $p : Y \to X$ be a Galois cover. Then there is a bijective correspondence between the subgroups of G and the intermediate covers of $Y \to X$ such that, each subgroup H of G corresponds to the subcover $\bar{p}_H : Y/H \to X$ and, any intermediate cover $Y \to Z \to X$ corresponds to the subgroup $Aut_{\mathbf{Cov(Z)}}(Y, f)$ of G.*

4 Towards both in a common context

Here is what we plan to do next semester:

We have remarked before that the two results – Theorems 2.4 and 3.12 – appear to be dual to each other, in that Galois theory is about a contravariant correspondence between *extensions* $A \rightarrowtail B$ and symmetry groups, while covering space theory is about a contravariant correspondence between *coverings* $E \twoheadrightarrow B$ and symmetry groups. One might wonder if we could make a formal analogy between the two. Taking a hint from algebraic geometry, we might try to recast Galois theory for fields using affine varieties and attempt covering space theory here. However we immediately run into an issue: covering theory as typically stated works poorly for schemes. For example, we cannot assume locally connected for schemes. Furthermore and perhaps more fundamentally, there is still the issue of defining an appropriate notion of fundamental group in the algebraic setting.

Next semester we will see that Grothendieck's Galois theory, which resolves the above issues, invokes several fundamental themes on duality, the most important one being a variant of Tannakian reconstruction. This theme realizes the intuition that Galois theory and covering space theory are about representations of the symmetry group(oids) present in the aforementioned contravariant correspondences. For example, for Galois theory we will eventually recover the statement that intermediate extensions of Galois extensions are equivalent to (finite) sets equipped with a (transitive) action of the Galois group; this will be dual to how in covering space theory the (connected) coverings of a nice enough[1] space are equivalent to sets equipped with a (transitive) $\pi_1(X)$ action. The main goal for next semester then is to define Galois categories and focus on the two Galois theories we saw this semester as the primary examples.

[1] Path connected, locally path connected, and semi-locally simply connected, as we saw above.

References

[1] Marco António Delgado Robalo, *Galois Theory towards Dessins d'Enfants*, Master's Thesis, IST-Lisbon, 2009, Available at https://fenix.tecnico.ulisboa.pt/downloadFile/395139415315/dissertacao.pdf.

[2] I.N. Herstein, *Topics In Algebra*, Second Edition, Wiley Student Edition, 2019

[3] Noam Elkies, *Math 250 Course Notes*, Retrieved from https://people.math.harvard.edu/~elkies/M250.04/artinlemma.html Fall 2021.