# Galois Groups and Fundamental Groups

**Rohan Gupta**

*A dissertation submitted for the partial fulfilment*
*of BS-MS dual degree in Science*


**Indian Institute of Science Education and Research Mohali**
**April 2017**

# Certificate of Examination

This is to certify that the dissertation titled **Galois groups and Fundamental groups** submitted by **Rohan Gupta** (Reg. No. MS12035) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Chetan Tukaram Balwe

Dr. Chandrakant S. Aribam

Dr. Varadharaj R. Srinivasan
(Supervisor)

Dated: April 20, 2017

# Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Varadharaj R. Srinivasan at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. This work is based on the book "Galois Groups and Fundamental Groups" authored by Tamás Szamuely([Sza]). Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of work done by me and all sources listed within have been detailed in the bibliography.

Rohan Gupta
(Candidate)

Dated: April 20, 2017

In my capacity as the supervisor of the candidates project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Varadharaj R. Srinivasan
(Supervisor)

## Acknowledgment

Firstly, I would like to express my sincere gratitude to my adviser Dr. Varadharaj R. Srinivasan for his support and motivation to carry out my MS thesis. His guidance has helped me throughout this project and I am extremely thankful to him for this opportunity and steering me in the right direction. I would also like to thank my committee members Dr. Chandrakant S. Aribam and Dr. Chetan Balwe for their insightful comments and questions.

I would also like to thank my batch mates who improved my understanding by helpful discussions.

Finally, I would like to thank my friends and family and most importantly my parents who continuously encouraged me and have guided me through life.

# Abstract

In this thesis, I will discuss the first three chapters of the "Galois Groups and Fundamental Groups" by Tamas Szamuely([Sza]).

Chapter 1 deals with basics of field theory, Galois theory and contains an introduction to Etale algebras. We will prove the categorical anti-equivalence of continuous left $Gal(k)$-sets with finite etale algebras over $k$. Chapter 2 deals with certain results from algebraic topology using which we obtain a categorical equivalence between category of left-$\pi_1(X, x)$ sets and category of covers of $X$. In Chapter 3 study Riemann surfaces and holomorphic map. The covers over Riemann surfaces create a link between field theory and theory of covers. We show that the category of finite covers of $X$ outside a finite discrete set of points is equivalent to the category of Riemann surfaces equipped with holomorphic maps onto $X$. Further, in this chapter, we establish that every finite group occurs as Galois group of some finite Galois extension of $\mathbb{C}(t)$.

# Contents

[section] [section]

# Chapter 1

# Field Theory and Galois Theory

There is a strong analogy between the Galois Group and the Fundamental Group. In Galois theory, we talk about the automorphisms of separable closures of the base field and for differential equations the analogous role is played by universal cover of the base domain. So to understand this analogy we start out with some basics of Galois Theory of fields, Infinite Galois theory and then introduce the notion of etale algebra to establish the Grothendieck Formulation of Galois Theory.

## 1.1 Algebraic Field Extensions

**Definition 1.1.1.** *Let $k$ be a field. An extension $L|k$ is called algebraic if every element of $k$ is a root of some polynomial in $k[x]$. This polynomial is said to be minimal if it is monic and irreducible. A field $\bar{k}$ is called algebraically closed if it has no algebraic extensions other than itself. An algebraic closure of a field $k$ is an algebraic extension which is algebraically closed.*

**Remark 1.1.** *A finite extension $L$ of $k$ is algebraic over $k$. If $L = k[\alpha]$, $\alpha \in L$ and $f$ is the minimal polynomial of $\alpha$, then $[L : k] = deg(f)$.*

**Theorem 1.1.1.** *Let $k$ be a field. Then there exists an algebraically closed field which contains $k$ as a sub field.*

*Proof.* We first construct a field $L_1|k$ such that every polynomial in $k[x]$ of degree$\geq 1$ has a root. Now, for every polynomial $f \in k[x]$, associate a set $X_f$ and let S be

the set of all such $X_f$(The set S and the set of polynomials in $k[x]$ are in bijection). Now form the polynomial ring $k[S]$. Claim that the ideal generated by $< f(X_f) >$ is proper. If not, then $1 \in < f(X_f) >$ and there exists function $g_i \in k[S]$ such that $\Sigma_{i=1}^{n} g_i f_i(X_{f_i}) = 1$, denote each $X_{f_i}$ by $X_i$ and $g_i$ is a polynomial in finite number of variables $X_1, ...X_N$ such that $N \geq n$. So we have $\Sigma_{i=1}^{n} g_i(X_1, ..., X_N) f_i(X_i) = 1$. Let F be the splitting field of polynomials $f_1, ...f_n$ and say $\alpha_i$ is a root of $f_i$ and let $\alpha_i = 0$ for $i > n$. So evaluating above equation at these points, we get

$\Sigma g_i(\alpha_1, ..\alpha_n, 0, ..., 0) f_i(\alpha_i) = 1$

$\implies 0 = 1$. Hence a contradiction. So the ideal $< f(X_f) >$ is proper and is contained in a maximal ideal say M. So we have the field $L_1 = k[S]/M$ containing $k$ by the embedding $\sigma : k \to k[S]/M$ given by $a \mapsto a + m$. Every polynomial $f \in k[x]$ has a root in $L_1$ which is $x_f$ because $f(x_f) \in < f(X_f) > \subseteq M$. Similarly we construct a field $L_2$ over $L_1$, such that every polynomial $f \in L_1[x]$ has a root in $L_2$ and so on. Then we get a tower of field extensions $k \subseteq L_1 \subseteq .....L_n \subseteq L_{n+1}...$ Let $L = \bigcup L_i$, $k \subset L$.. Coefficients of a polynomial $h(x) \in L[x]$ are coming from some $L_n$ for some large n. So $h(x)$ has a root in $L_{n+1}$ and hence a root in $L$. So $L$ is algebraically closed. □

**Corollary 1.1.1.** *Let k be a field. There exists an extension $\bar{k}$ which is algebraic over k and algebraically closed.*

*Proof.* Let E be an algebraically closed field containing $k$ as a sub field. Let $\overline{k}$ be the union of sub fields of E which are algebraic over $k$. So $\overline{k}$ is algebraic over $k$. Now we claim that if $\alpha \in E$ and $\alpha$ is algebraic over $\overline{k}$, then $\alpha$ is algebraic over $k$. To see this, consider a finite tower of field extensions $k \subset F \subset E$ such that $E|F$ is algebraic and $F|k$ is also algebraic. Let $\alpha \in E$ be a root of some polynomial $f(x) \in F[x]$, there exist $a_i's \in F$ such that $\Sigma_{i=0}^{n} a_i \alpha^i = 0$. Let $F_0 = k(a_0, ..., a_n)$ and $\alpha$ is algebraic over $F_0$. $\implies k \subset k(a_0, ...a_n) \subset F_0(\alpha)$ such that $[F_0(\alpha) : F_0] < \infty$ and $[F_0 : k] < \infty$. So $[F_0(\alpha) : k] < \infty$ i.e $\alpha$ is algebraic over $k$ and our claim follows.

Let $f \in \overline{k}[x] \subset E[x]$, then there exist $\alpha \in E$ which is a root of $f$ which implies that $\alpha$ is algebraic over $\overline{k}$ which further implies $\alpha$ is algebraic over k and hence $k(\alpha)$ is algebraic over k. Then $k(\alpha) \subseteq \overline{k}$, so $\alpha \in \overline{k}$. Hence $\overline{k}$ is algebraically closed and is algebraic closure of $k$. □

**Proposition 1.1.1.** *Let $\sigma : k \to L$ be an embedding of k into an algebraically closed field L. The number of extensions of $\sigma$ from k to $k(\alpha)$ is $\leq$ the number of roots of*

*minimal polynomial of $\alpha$ but is equal to number of distinct roots of minimal polynomial of $\alpha$.*

*Proof.* Let $k$ be the base field. $\sigma : k \to L$ be an embedding of of $k$ into an algebraically closed field $L$. We want to extend $\sigma$ to an embedding of an algebraic extension $E$ of $k$ into $L$. Lets consider the case when $E = k(\alpha)$, and $k(\alpha)$ is an algebraic extension.

Let $p(x)$ be the monic irreducible polynomial of $\alpha$. Let $\beta$ be the root of $\sigma p$ in $L$. We know that $k(\alpha) = k[\alpha]$, so every element of $k(\alpha)$ can be written in the form of $f(\alpha)$ for some $f \in k[x]$. Define an extension of $\sigma$ by $f(\alpha) \mapsto \sigma f(\beta)$. The map is well defined because for some $g(x) \in k[x]$ such that $g(\alpha) = f(\alpha)$ which implies $(g - f)(\alpha) = 0$ which means that $p(x)$ divides $g(x) - f(x)$ that further implies $\sigma p(x)$ divides $\sigma g(x) - \sigma f(x)$. So $\sigma g(\beta) = \sigma f(\beta)$. Hence the extension of $\sigma$ defined above is an extension to $k(\alpha)$. The number of such extensions depend on the degree of $p(x)$. □

**Theorem 1.1.2.** *Let $k$ be a field and $E$ be an algebraic extension of $k$, and $\sigma : k \to L$ be an embedding of $E$ in $L$. If $E$ is algebraically closed and $L$ is algebraic over $\sigma k$, then any such extension $\sigma$ is an isomorphism of $E$ onto $L$.*

*Proof.* Let S be the set of all pairs $(F, \tau)$ where $F \subset E$ containing $k$ and $\tau$ is an extension of $\sigma$ to an embedding of $F$ into $L$. Define ordering on S as follows: If $(F, \tau)$ and $(F', \tau') \in S$, then $(F, \tau) \leq (F', \tau')$ if $F \subset F'$ and $\tau'|_F = \tau$.

The set S is non-empty as $(k, \sigma) \in S$. Assume that $\{(F_i, \tau_i)\}$ is a totally ordered subset of S, let $F$ be the union of $F_i$'s and define $\tau|_{F_i}$ to be equal to $\tau_i$ for each $F_i$. Then the element $(F, \tau)$ is an upper bound of the totally ordered subset. It has a maximal element in S by Zorn's lemma. Say $(M, \lambda)$ where $\lambda$ is an extension of $\sigma$.

Now we show that $M = E$. Otherwise, there exists $\alpha \in E - M$ such that $\lambda$ has an extension to $M(\alpha)$ which contradicts the maximality of $(M, \lambda)$. This shows that there exists an extension of $\sigma$ to $E$ which is nothing but $\lambda$.

If $E$ is algebraically closed then so is $\sigma E$ because all the polynomials in $\sigma E[x]$ will have a root in $\sigma E$ which will come from the image under $\sigma$ of the root of polynomial in $E$. And if $L$ is algebraic over $\sigma k$, then $L$ is algebraic over $\sigma E$. This shows that $\sigma$ is an isomorphism of $E$ onto $L$ that is, $\sigma E = L$. □

## 1.2 Separable Extensions

Let E be an algebraic extension of a field F and $\sigma : F \to L$ be an embedding of F into an algebraically closed field L. We can extend $\sigma$ to an embedding of E into L. We assume that L is algebraic over $\sigma F$ and since it is algebraically closed it must be an algebraic closure of $\sigma F$. Let $S_\sigma$ denote the set of extensions of the embedding $\sigma$ to an embedding of E into L.

Assume $L^{'}$ be another algebraically closed field and let there be an embedding of F, $\tau : F \to L^{'}$ into $L'$. Just as done before, $L'$ is the algebraic closure of $\tau F$. We know there exists an isomorphism between two algebraically closed fields of k. Let $\lambda : L \to L'$ be an isomorphism. Let $S_\tau$ be the set of extensions of $\tau$ to an embedding of E into $L^{'}$. $\lambda : L \to L^{'}$ is an extension of $\tau \circ \sigma^{-1}$ applied to $\sigma F$.

Let $\sigma^{'} \in S_\sigma$, extending $\sigma$ to an embedding of E into L. Then $\lambda \circ \sigma^{'}$ is an extension of $\tau$ to an embedding of E into $L^{'}$ because the restriction of $\lambda \circ \sigma^{'}$ to $F$ is equal to $\tau \circ \sigma^{-1} \circ \sigma = \tau$. Hence, $\lambda \circ \sigma^{'}$ is an extension of $\tau$. $\lambda$ induces a map between $S_\sigma$ and $S_\tau$ given by $\sigma^{'} \mapsto \lambda \circ \sigma^{'}$ and an inverse map is given by $\lambda^{-1}$. Hence there is a bijection between the sets $S_\sigma$ and $S_\tau$ having the same cardinality. This cardinality is called as separable degree and we denote it be $[E : F]_s$.

**Theorem 1.2.1.** *For a tower $k \subset F \subset F$, $[E : k]_s = [E : F]_s[F : k]_s$. $[E : k]_s$ is finite and $[E : k]_s \leq [E : k]$ only when E is finite extension of k.*

*Proof.* Let $L$ be an algebraically closed field and $\sigma : k \to L$ be an embedding of $k$ into $L$. Let $\{\sigma_i\}_{i \in I}$ be the family of distinct extensions of $\sigma$ to an embedding of $F$ into $L$. We have seen that each $\sigma_i$ has only $[E : F]_s$ many extensions to an embedding of $E$ into $L$. By a simple counting argument, we can say that the number of elements of the set of embeddings $\tau_{ij}$ are $[E : F]_s[F : k]_s$ . So any embedding of $E$ into $L$ must be one of the $\tau_{ij}$. Hence we have the result $[E : k]_s = [E : F]_s[F : k]_s$. For the second part of the theorem, assume that $E|k$ is a finite extension generated by $\{\alpha_1, ...\alpha_r\}$. Then we have the tower: $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset ....k(\alpha_1, \alpha_2, ..., \alpha_r)$. Let $F_0 = k$ and $F_{t+1} = F_t(\alpha_{t+1})$. $[F_t(\alpha_{t+1}) : F_t]_s$ represents the number of extensions of $\sigma : F_t \to L(L$ is some algebraically closed field) to an embedding of $F_t(\alpha_{t+1})$ into $L$. By Proposition 1.1.1, $[F_t(\alpha_{t+1}) : F_t]_s \leq [F_t(\alpha_{t+1}) : F_t]$ and by multiplicativity of tower of field extensions, $[E : k]_s \leq [E : k]$. □

The following result follows immediately

**Corollary 1.2.1.** *Given a tower $k \subset M \subset L$ of finite field extensions , the extension $L|k$ is separable if and only if $L|M$ and $M|k$ are separable.*

**Corollary 1.2.2.** *A finite extension $L|k$ is separable if and only if $L = k(\alpha_1, \alpha_2....., \alpha_m)$ for some separable elements $\alpha_i \in L$.*

*Proof.* Let $L$ is separable over $k$ and $\alpha \in L$. Consider $k \subset k(\alpha) \subset L$. By previous result, we have $[k(\alpha) : k]_s = [k(\alpha) : k]$. By definition this means that $\alpha$ is separable over $k$. We have finite number of $\alpha_i$'s such that we have a tower, $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2), ....., \subset k(\alpha_1, ...\alpha_m)$. So each $\alpha_i$ is separable over $k$.

Conversely, consider the tower $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2), ....., \subset k(\alpha_1, ...\alpha_m)$. Each $\alpha_i$ is separable over $k(\alpha_1, ..., \alpha_{i-1})$ because the minimal polynomial of each $\alpha_i$ has distinct roots over $k$. Which means that $[k(\alpha_1, .., \alpha_i) : k(\alpha_1, ..., \alpha_{i-1})]_s = [k(\alpha_1, .., \alpha_i) : k(\alpha_1, ..., \alpha_{i-1})]$ for all $1 \leq i \leq m + 1$. By multiplicativity of towers, $[L : k]_s = [L : k]$ and hence $L|k$ is a finite separable extension. □

**Definition 1.2.1.** *$E$ is a separable extension of the base field $k$ if and only if $[E : k]_s = [E : k]$. An algebraic element $a$ over $k$ is called separable over $k$ if $k(a)$ is a separable extension of $k$. Equivalently we can say that if the minimal polynomial of $\alpha$ has no multiple roots then $\alpha$ is separable. A polynomial $f \in k[x]$ is separable if it has no multiple roots. If $k \subset F \subset E$ and $\alpha \in E$ is separable over $k$, then $\alpha$ is separable over $F$.*

**Definition 1.2.2.** *Let E,F be field extensions of $k$ contained in some algebraic closure $\overline{k}$ of $k$. The smallest sub-field of the algebraic closure $\overline{k}$, which contains $E$ as well as $F$ is denoted by $EF$ and is called compositum of $E$ and $F$ in $\overline{k}$.*

**Corollary 1.2.3.** *If L,M are finite separable extensions of $k$, then their compositum is separable as well.*

*Proof.* Since $LM$ is the smallest sub field of $\overline{k}$ containing both $L$ and $M$, we have finitely many $\alpha$'s in $L$ such that $LM = M(\alpha_1, ...., \alpha_m)$. Each $\alpha_i$ is separable over $k$(because $L$ is separable over $k$), so each $\alpha_i$ is separable over $M$. So $LM|M$ is a separable extension. Also $M|k$ is separable, so $LM|k$ is a separable extension. □

**Definition 1.2.3.** *Compositum of all finite separable extensions of $k$ in $\overline{k}$ is called* ***separable closure*** *and is denoted by $k_s$.*

**Theorem 1.2.2.** ***Primitive Element Theorem*** *A finite separable extension can be generated by single element.*

*Proof.* [Lanon], Chapter 5, Theorem 4.6 □

## 1.3 Prerequisites on Galois Extensions

Let L be a finite field extension of k, the group of field automorphisms of L that fixes the elements of k is denoted by $Aut(L|k)$.

**Definition 1.3.1.** *Let L be an algebraic field extension of k. L is called a Galois extension of k if under the action of $Aut(L|k)$, the elements of L that remain fixed are exactly the elements of k. In this case, we denote $Aut(L|k)$ by $Gal(L|k)$ which is called the Galois group of $L|k$.*

**Lemma 1.3.1.** *$k_s|k$ is a Galois extension where $k_s$ denotes the separable closure of k.*

*Proof.* We need to verify that every element $\alpha \in k_s$ such that $\alpha \notin k$ is not fixed by all automorphisms $\sigma \in Aut(k_s|k)$(or alternatively we can say that it is moved by some automorphism). Let f be the minimal polynomial of $\alpha$ and $\alpha^{'}$ in $k_s$ be another root of f. There is an isomorphism of field extensions $k(\alpha)$ and $k(\alpha^{'})$, $k(\alpha) \xrightarrow{\sim} k(\alpha^{'})$ given by the map $\alpha \to \alpha^{'}$. By a previous result, we know that this isomorphism can be extended to an automorphism of algebraic closure $\overline{k}$ of k. Now we only have to check the fact that each element of $Aut(\overline{k}|k)$ maps the separable extension $k_s$ onto itself. This is indeed true because this automorphism sends an element $\gamma$ of $\overline{k}$ to another root $\gamma^{'}$ of its minimal polynomial, and if $\gamma$ is separable then its minimal polynomial is separable by definition which implies that $\gamma^{'}$ is separable. We call $Gal(k_s|k)$ the absolute Galois group of k. □

**Proposition 1.3.1.** *Let k be a field, $k_s$ a separable closure and $L \subset k_s$ a sub-field containing k. The following are equivalent:*

1. *The extension $L|k$ is Galois.*
2. *The minimal polynomial over k of each $\alpha \in L$ splits into linear factors in L.*
3. *Each automorphism $\sigma \in Gal(k_s|k)$ satisfies $\sigma(L) \subset L$.*

*Proof.* $1 \Rightarrow 2$

Let $p(x) \in k[x]$ be an irreducible polynomial of $\alpha \in L$ and let the distinct elements of the set $\sigma(\alpha) : \sigma \in Gal(L|k)$ be $\alpha_1, ..., \alpha_n$. Define $g(x) \in L[x]$ as $g(x) = \prod_{i=1}^{n}(x - \alpha_i)$.

Now each $\sigma \in G$ permutes $\alpha_i$, so each $\sigma$ fixes the coefficients of g(x). Hence, $g(x) \in k[x]$ with no repeated roots.

p(x) and g(x) have a common root in L i.e $\alpha$. So g(x) must divide p(x), but p(x) is irreducible. Hence p(x)=g(x). So $p(x)$ is separable as it has no repeated roots and hence it splits into linear factors in L.

$2 \Rightarrow 3$

Each $\sigma \in Gal(k_s|k)$ must map $\alpha \in L$ to a root of its minimal polynomial.$\Rightarrow$ $\sigma(L) \subset L$ because minimal polynomial of each $\alpha$ over k splits into linear factors in L.

$3 \Rightarrow 1$

Pick $\alpha \in L - k$. Since $k_s$ is Galois over k, Let $\sigma \in Gal(k_s|k)$ such that $\sigma(\alpha) \neq \alpha$. By (3), $\sigma(L) \subset L$ which means that $\sigma|_L \in Aut(L|k)$ such that $\sigma|_L(\alpha) \neq \alpha$. □

**Theorem 1.3.1.** ***Main theorem for finite extensions:***

*Let $L|k$ be a finite Galois extension with Galois group G. The maps $M \mapsto H := Aut(L|M)$ and $H \mapsto M := L^H$ yielding an inclusion reversing bijection between sub fields $L \supset M \supset k$ and subgroups $H \subset G$. The extension $L|M$ is always Galois. The extension $M|k$ is Galois iff H is normal subgroup of G, in this case we have $Gal(M|k) \cong G/H$.*

**Lemma 1.3.2.** *A finite extension $L|k$ is Galois if and only if it is the splitting field of an irreducible separable polynomial $f \in k[x]$.*

*Proof.* If L is the Splitting field of an irreducible separable polynomial then $L = k(\alpha_1, ..., \alpha_n)$ such that $f = \prod(x - \alpha_i)$ and without multiple roots. So, for $\sigma \in Gal(K_s|k)$, $\sigma(L) \subset L$. Hence by previous preposition, $L|k$ is Galois extension. Conversely, if $L|k$ is Galois, then part (2) of the previous proposition implies that L is the splitting field of a primitive element generating L over k. □

**Corollary 1.3.1.** *A finite extension $L|k$ is Galois with group $G = Aut(L|k)$ if and only if G has order [L:k].*

*Proof.* If $L|k$ is Galois, then L is the splitting field of an irreducible separable polynomial $f \in k[x]$. Then order of G is $|Aut(k(\alpha)|k)|$ where $\alpha$ is a primitive element and $L = k(\alpha)$. Since f is separable, $|G| = [L : k]$. Conversely, suppose $G = Aut(L|k)$, the extension $L|L^G$ is Galois by definition so G has order $[L : L^G] = [L : k]$. Hence $L^G = k$. □

## 1.4 Infinite Galois Extensions

The main problem that arises for infinite field extensions is that it is no longer true that all subgroups of Galois group arise as the subgroup fixing some sub extension $M|k$. Let $K|k$ be a infinite Galois extension, we first observe that K is a union of finite Galois extensions.

**Lemma 1.4.1.** *Each finite sub extension of $K|k$ can be embedded in a Galois sub extension.*

(This is because each finite separable sub extension is of the form $k(\alpha)$ with an appropriate element $\alpha$. We can embed $k(\alpha)$ in the splitting field of minimal polynomial of $\alpha$, which is finite Galois extension over k.)

**Construction 1.1.** *An inverse system of groups $(G_\alpha, \phi_{\alpha\beta})$ consists of: · a partially ordered set $(\Lambda, \leq)$ which is directed in the sense that for all $(\alpha, \beta) \in \Lambda$ with $\alpha \leq \gamma, \beta \leq \gamma$; · for each $\alpha \in \Lambda$, a group $G_\alpha$;*

*· for each $\alpha \leq \beta$ a homomorphism $\phi_{\alpha\beta} : G_\beta \to G_\alpha$ such that we have equalities $\phi_{\alpha\gamma} = \phi_{\alpha\beta} \circ \phi_{\beta\gamma}$ for $\alpha \leq \beta \leq \gamma$.*

*The inverse limit of the system is defined as the subgroup the direct product $\prod_{\alpha\in\lambda} G_\alpha$ consisting of sequences $(g_\alpha)$ such that $\phi_{\alpha\beta}(g_\beta) = g_\alpha$ for all $\alpha \leq \beta$. It is denoted by $\varprojlim G_\alpha$.*

**Definition 1.4.1.** *A profinite group is defined to be the inverse limit of a system of finite groups.*

**Example 1.1.** *A sequence of integers satisfying $x_n \equiv x_{n-1} mod p^n$ determines an object called p-adic integer. Consider the sequence $Z/pZ \xleftarrow{\lambda_1} Z/p^2Z \xleftarrow{\lambda_2} ..Z/p^nZ \xleftarrow{\lambda_n} ...$ such that $\lambda_n(\bar{s}_{n+1}) = \bar{s}_n$ The ring of p-adic integers is the projective limit $\varprojlim Z/p^nZ$ of $(A_n, \lambda_n)$ where $A_n = Z/p^nZ$.*

**Proposition 1.4.1.** *Let $K|k$ be an arbitrary Galois extension of fields. The Galois group of finite sub extensions of $K|k$ together with the homeomorphism $\phi_{ML}$ : $Gal(M|k) \to Gal(L|k)$ form an inverse system whose inverse limit is isomorphic to $Gal(K|k)$. In particular, $Gal(K|k)$ is a profinite group.*

*Proof.* Let $I = \{L \mid \text{k}\subseteq L \subseteq K, L|k \text{ is a finite Galois extension}\}$. Define partial ordering on I as: for $L_1, L_2 \in I$, $L_1 \leq L_2$ iff $L_1 \subseteq L_2$. Moreover, $\{Gal(L|k), \phi_{L_iL_j}\}_{L,L_i,L_j \in I}$ form an inverse system with homomorphism $\phi_{L_1L_2} : Gal(L_2|k) \to Gal(L_1|k)$ given by $\phi_{L_1L_2}(\sigma) = \sigma|_{L_1}$. The map is well defined: Take $\sigma \in Gal(L_2|k)$. Then since $L_2|L_1$ is a Galois extension, then $\sigma(L_1) \subset L_1$. Consider the homomorphism $\chi : Gal(K|k) \to \varprojlim Gal(L|k)$ given by $\sigma \mapsto \{\sigma|_L\}_{L\in I}$.

Injectivity: Let $\sigma \in ker(\chi)$ and $\chi(\sigma) = \{1_L\}_{L\in I} \implies \sigma|_L = 1_L, \forall L \in I$. Since $K = \bigcup_{L\in I} L$, we have $\sigma = 1_k$.

Surjectivity- Take $\{\sigma_L\}_{L\in I} \in \varprojlim Gal(L|k)$. Let $\alpha \in K$. Then $\exists L \in I$ such that $\alpha \in L$. Define $\sigma(\alpha) = \sigma_L(\alpha)$. This definition is well defined due to the fact that $\sigma_L$ forms a compatible system of automorphisms, i.e for $L_1, L_2 \in I$, $L_1 \subseteq L_2$, then $\sigma_{L_1}(\alpha) = \sigma_{L_2}(\alpha)$. So we have $\chi(\sigma) = \{\sigma_L\}_{L\in I}$. Hence surjectivity follows and $\chi$ is an isomorphism. So, $Gal(K|k)$ is a profinite group. □

Now we define Krull topology on profinite group. Let $G = \varprojlim G_\alpha$ be a profinite group. Each $G_\alpha$ is endowed with the discrete topology, $\prod_{\alpha\in\Lambda} G_\alpha$ is endowed with the product topology and finally $G \subseteq \prod_{\alpha\in\Lambda} G_\alpha$ is given the subspace topology. It follows from this construction that the natural projection maps $G \to G_\alpha$ are continuous. Under this topology, the profinite group becomes a topological group which is defined as follows

A group is called topological if the operations $p : G \times G \to G$ given by $p(g, h) = gh$ and $i : G \to G$ given by $i(g) = g^{-1}$ are continuous in the defined topology. Consider $\Pi_\alpha : \prod_{\alpha\in\Lambda} G_\alpha \to G_\alpha$. $\Pi_\alpha$ is continuous. $G \subseteq \prod_{\alpha\in\Lambda} G_\alpha$ where the subspace topology is generated by the open sets $\bigcup_{\alpha\in\Lambda}\{\pi_\alpha^{-1}(\{g_\alpha\})|g_\alpha \in G_\alpha\}$. It is enough to check that inverse images of one of these open sets under the above defined maps p and i are open.

$$\begin{aligned} p^{-1}(\Pi_\alpha^{-1}(\{g_\alpha\})) &= p^{-1}(\Pi_\alpha^{-1}(\{g_\alpha\}.h.h^{-1})) \\ &= p^{-1}(\Pi_\alpha^{-1}(\{g_\alpha.h\}) \circ \Pi_\alpha^{-1}(\{h^{-1}\})) \\ &= \bigcup_{h \in G_\alpha} (\Pi_\alpha^{-1}(\{g_\alpha.h\}) \times \Pi_\alpha^{-1}(\{h^{-1}\})) \end{aligned}$$

which is open. Continuity of p follows because the inverse image of a sub-basic open set is open under p. $i : G \to G$ is given by $i(g) = g^{-1}$. $i^{-1}(\Pi_\alpha^{-1}(\{g_\alpha\})) = (\Pi_\alpha^{-1}(\{g_\alpha\}))^{-1} = \Pi_\alpha^{-1}(\{g_\alpha^{-1}\})$ which is open. Hence i is open.

**Lemma 1.4.2.** *$G = \varprojlim G_\alpha$ is a closed topological subgroup of $\prod_{\alpha \in \Lambda} G_\alpha$.*

*Proof.* Let $g = (g_\alpha) \in \prod_{\alpha \in \Lambda} G_\alpha$. If $g \notin \varprojlim G_\alpha$, we have to show that it has an open neighbourhood which does not meet $\varprojlim G_\alpha$. By assumption, for some $\beta, \gamma \in \Lambda$, $\phi_{\beta\gamma}(g_\gamma) \neq g_\beta$. Since $G_\alpha$ is Hausdorff, so is $\prod G_\alpha$. Choose open and disjoint neighbourhoods U and V of $\phi_{\beta\gamma}$ and $g_\beta$ in $G_\beta$ respectively. Let $U^{'}$ be the neighbourhood of $g_\gamma$ in $G_\gamma$ such that $\phi_{\beta\gamma}(U^{'}) \subseteq U$. Consider an open set $W = \prod_{\alpha \in \Lambda} V_\alpha$ of $\prod_{\alpha \in \Lambda} G_\alpha$, where $V_\gamma = U^{'}$, $V_\beta = V$ and $V_\alpha = G_\alpha$, $\alpha \neq \gamma, \beta$. Then W is the open neighbourhood of $(g_\alpha)$ disjoint from G. □

**Corollary 1.4.1.** *A profinite group is compact and totally disconnected(Only connected subsets are one-point subsets). Moreover, the open subgroups are precisely the closed subgroups of finite index.*

*Proof.* Each $G_\alpha$ is a finite group with discrete topology $\implies$ Each $G_\alpha$ is compact. By Tikhonov's theorem, $\prod_{\alpha \in \Lambda} G_\alpha$ is compact. Since closed subspaces of compact spaces are compact, $G = \varprojlim G_\alpha$ is compact. $G_\alpha$ is Hausdorff and totally disconnected, so $\prod_{\alpha \in \Lambda} G_\alpha$ is totally disconnected. G is compact and totally disconnected. Since G is a topological group, for any open subgroup U of G, $U \mapsto gU$ is a homeomorphism. So $G - U = \bigsqcup_{g \in G} gU$ is open, hence G U is closed. Since G is compact, these cosets must be finite in number. Conversely, a closed subgroup of finite index is open because if U is a closed subset of G, then $U = G - \bigsqcup_{g \in G} gU$, so U is open. □

**Theorem 1.4.1.** *Let L be a sub extension of the infinite Galois extension $K|k$. Then $Gal(K|L)$ is a closed subgroup of $Gal(K|k)$. Moreover, the following maps $L \mapsto H := Gal(K|L)$ and $H \mapsto L := K^H$, yield an inclusion reversing bijection between finite sub extension fields $K \supset L \supset k$ and closed subgroups $H \subset G$. We call a sub extension L*

*Galois over k if and only if $Gal(K|L)$ is normal subgroup of $Gal(K|k)$; and we obtain a natural isomorphism $Gal(L|k) \cong Gal(K|k)/Gal(K|L)$.*

## 1.5 Finite Etale Algebras

We have a base field $k$. Let $\bar{k}$ be its algebraic closure and $k_s \subset \bar{k}$ be its separable closure. Denote $Gal(k_s|k)$ by $Gal(k)$. Consider a finite separable extension L of k such that L is not necessarily a sub extension field of $k_s$. We have already seen that there are finitely many homomorphisms from L to $\bar{k}$(equal to [L:k]). Since L is separable, the images of these homomorphism will be contained in $k_s$. So, we may consider the finite set $Hom_k(L, k_s)$, which is endowed by a natural action of $Gal(k)$ given by $(g, \phi) \mapsto g \circ \phi$ for $g \in Gal(k), \phi \in Hom_k(L, k_s)$. The action of a topological group on a topological space is said to continuous if the map $m : G \times X \to X$ given by $(g, x) \mapsto gx$ is continuous. $Hom_k(L, k_s)$ is endowed with discrete topology. The continuity of the above defined action is equivalent to the openness of the stabilizer $G_x$ of each point $x \in X$. Stabilizer of $x \in X$=$G_x = \{g \in G | gx = x\}$. For $x \in X$, $m^{-1}(x) = U_x = \{(g, y) \in G \times X : gy = x\} = \bigsqcup\{(g, y) \in G \times \{y\} | gy = x\}$ for a fixed $y \in X$.Each of the above disjoint subsets are either empty or homeomorphic to $G_x$ via the map $g \mapsto (gh, y)$ for some $h \in G$ such that $hy = x$. Thus if $G_x$ is open, then $U_x$ is open and hence m is continuous.Conversely, $G_x$ is the preimage of x by the map $G \xrightarrow{i_x} G \times X \xrightarrow{m} X$, where $i_x(g) = (g, x)$. $i_x^{-1} \circ m^{-1}(x) = i_x^{-1}(U_x) = i_x^{-1}(\bigsqcup\{(g, y) \in G \times \{y\} | gy = x\}) \cong G_x$. So continuity of m implies openness of $G_x$.

**Lemma 1.5.1.** *The above left action of Gal(k) on $Hom_k(L, k_s)$ is continuous and transitive, hence $Hom_k(L, k_s)$ as a Gal(k)-set is isomorphic to the left coset space of some open subgroup in Gal(k). For L Galois over k this coset space is in fact a quotient by an open normal subgroup.*

*Proof.* The stabilizer U of an element $\phi \in Hom_k(L, k_s)$ consists of $g \in Gal(k)$ such that $g\phi = \phi$, it means g fixes $\phi(L)$. Hence U is open in Gal(k)(using main theorem of infinite Galois theory), so the action of Gal(k) is continuous. Since L is finite separable extension over k, it is generated by a primitive element $\alpha$ with minimal polynomial f. Each $\phi \in Hom_k(L, k_s)$ maps $\alpha$ to a root of f in $k_s$. $Gal(k)$ permutes these roots, so its action on $Hom_k(L, k_s)$ is transitive. The map $g \circ \phi \mapsto gU$ induces an isomorphism of $Hom_k(L, k_s)$ with left coset space $Gal(k)/U$. □

If M is another finite separable extension of k, each k-homomorphism $\phi : L \to M$ induces a map $Hom_k(M, k_s) \to Hom_k(L, k_s)$ by composition with $\phi$ i.e. $f \mapsto f \circ \phi$, $f \in Hom_k(M, k_s)$. This map is Gal(k)-equivariant. So, $Hom_k(,k_s)$ is a contravariant functor from category of finite separable extensions to category of finite sets with continuous transitive left Gal(k)-action.

**Theorem 1.5.1.** *Let $k$ be a field in a separable closure $k_s$. The contravariant functor defined above that maps a finite separable field extension $L|k$ to the finite set $Hom_k(L, k_s)$ equipped with left action of $Gal(k)$ gives an anti-equivalence between the category of finite separable extensions of k and the category of finite sets equipped with continuous and transitive left action of absolute Galois group $Gal(k)$. If we take Galois extensions instead of separable extensions, then we get the sets equipped with left $Gal(k)$ action isomorphic to some finite quotient of Gal(k).*

*Proof.* Recall two categories $C_1, C_2$ are called anti-equivalent iff there exists a contravariant functor $F : C_2 \to C_1$ which is fully faithful and essentially surjective.

Essentially surjective: We want to show that any continuous transitive Gal(k)-set S is isomorphic to some $Hom_k(L, k_s)$. Pick $s \in S$, we have seen that continuity of the Gal(k) action means that the stabilizer $U_s$ of s is open, hence it is closed and fixes some finite separable extension say L of k. Let $i : L \to k_s$ be the inclusion map. Stab. of $s = U_s = \{g \in Gal(k) | gs = s\}$ and Stab. of $i = \{g \in Gal(k) | g \circ i = g\}$. f $U_s \subset Gal(k)$ that fixes a fielf extension L of k, then $g \in U_s$ fixes $x \in L$ i.e $g \circ i(x) = i(x)$. So $Stabilizer(s) \subset Stabilizer(i)$. If $g \in Stabilizer(i)$, then $g \circ i(x) = i(x) = x$, which means $g \in U_s$, so $Stabilizer(s) \supset Stabilizer(i)$. Hence $Stabilizer(s) = Stabilizer(i)$. Now define a map $g \circ i \to gs$ from Gal$(k)-$sets $Hom_k(L, k_s) \to S$. The map is well-defined because stabilizer of i is same as stabilizer of G and it is clearly an isomorphism. Fully faithfulness: We need to show that given any two finite separable extensions L,M of k, the set of k-homomorphisms, $L \to M$ corresponds bijectively to the set of Gal(k)-maps $Hom_k(M, k_s) \mapsto Hom_k(L, k_s)$. Since both $Hom_k(M, k_s)$ and $Hom_k(L, k_s)$ are transitive Gal(k)-sets, so a map f between them is given by the image of a fixed $\phi \in Hom_{k(M,k_s)}$. We know that f is Gal(k)-equivariant, so if U is stabilizer of $\phi$ i.e for every $g \in U$, $g\phi = \phi$, then $g(f(\phi)) = f(g\phi) = f(\phi)$. So, $U \subset V$, where V is the stabilizer of $f(\phi)$. By taking the fixed sub fields of U and v, which are $\phi(M)$ and $f(\phi)(L)$ respectively, we get an inclusion $\phi(M) \supset f(\phi)(L)$. Let $\psi : \phi(M) \to M$ be the inverse , we can see that $\psi \circ f(\phi)$ is a unique element in $Hom_k(L, M)$. $\square$

Now we want extend this anti-equivalence to Gal(k)-sets which do not necessarily have transitive action. To do this we replace the category of finite separable extensions by finite dimensional etale k-algebra.

**Definition 1.5.1.** *A finite dimensional k-algebra A is called* ***etale****(over k) if it is isomorphic to a finite direct product of separable field extensions of k.*

**Theorem 1.5.2.** ***Main Theorem of Galois Theory- Grothendieck's version*** *The functor that maps a finite etale k-algebra A to finite set $Hom_k(A, k_s)$ gives an anti-equivalence between the category of finite etale k-algebras and the category of finite sets equipped with continuous left action of $Gal(k)$. Here separable field extensions give rise to sets with transitive Gal(k)-action and Galois extensions to sets isomorphic to finite quotients of Gal(k).*

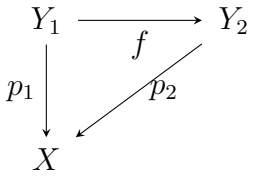
# Chapter 2

# Fundamental Groups in Topology

In this chapter we will study the topological analogue of Galois theory where the role of field extensions is played by covers and the role of absolute Galois group is played by the fundamental group. We will also study a version of Galois theorem that involves locally constant sheaves.

## 2.1 Covers

Fix a base space X. A space over X is a topological space Y such that we have a continuous map $p : Y \to X$.
We define a morphism between two spaces over X as a continuous map $f : Y_1 \to Y_2$ such that the following diagram commutes, here $p_1$ and $p_2$ are two different continuous maps of spaces over $X$




**Definition 2.1.1.** *Space $Y$ over $X$ is said to be a cover of $X$ if we have a continuous projection map $p : Y \to X$ with the following property that for every point $x \in X$ there is an open neighbourhood $V$ such that $p^{-1}(V)$ decomposes as the disjoint union of open subsets $U_i$ in $Y$ and $p|_{p^{-1}(V)}$ is a homeomorphism of $U_i$ onto $V$. The map $p$ is surjective.*

Take a non empty discrete topological space I and consider the product $X \times I$. The natural projection $p : X \times I \to X$ turns $X \times I$ into a cover of X. This is true because, for $x \in X$, V be an open neighbourhood of x such that $p^{-1}(V) = V \times I = \sqcup_{i \in I}(V \times i)$ and $V|_{p^{-1}(V)} : V \times i \to V$ is a homeomorphism.

**Proposition 2.1.1.** *A space Y over X is a cover if and only if each point of X has an open neighbourhood V such that the restriction of the projection $p : Y \to X$ to $p^{-1}(V)$ is isomorphic(as a space over V) to a trivial cover.*

*Proof.* If part is trivial. Let $x \in X$ and V be an open neighbourhood of x such that $p^{-1}(V) \cong V \times I = \sqcup_i(V \times i)$ and $p|_{(V \times i)} : (V \times i) \to V$ given by $(a, i) \mapsto a$ is a homeomorphism. So Y over X is a cover of X.

Only if: If Y over X is a cover, every $x \in X$ has an open neighbourhood V such that $p^{-1} = \sqcup_{i \in I} U_i$, where $U_i$ are disjoint open subsets of Y.

Define a map from $\sqcup_{i \in I} U_i \to V \times I$ by $u_i \mapsto (p(u_i), i)$, for $u_i \in U_i$. Injectivity is clear and surjectivity follows from the surjectivity of p and by the continuity of p and $p^{-1}$, the map is homeomorphism. So, $V \times I$ turns into a cover of V. □

Here the set I is called the fibres of p over the points of V.

**Corollary 2.1.1.** *For a connected space X, all the fibres of the covering map p are homeomorphic to the discrete space I.*

By previous proof we can see that the points of X over which the fibres of p equal some I form an open subset of X. If for some point $x' \in X$, the fibres of p equal equals $J \neq I$, they will form an open subset of X disjoint from V. So, by varying I, we can decompose X as disjoint union of open subsets. But if X is connected, this is not possible. Hence the fibres of p over the points of X must be homeomorphic to same discrete space I.

**Definition 2.1.2.** *Assume a continuous left action of a group G on a space Y, this action is said to be even if every point y of Y has an open neighbourhood V such that for all $g \in G$, the sets $gV$ are pairwise disjoint.*

Define an equivalence relation on Y as $y \sim g.y, g \in G$. Write G/Y for Y/∼. Define a topology in the following way so that the projection $p_G : Y \to G/Y$ is continuous,

$\tau_{G/Y}$=$\{U \subseteq G/Y | p_G^{-1}(U)$ is open in Y $\}$. Now we have a quotient space G/Y whose underlying set is the set of orbits of G.

**Lemma 2.1.1.** *If G is group acting evenly on a connected space Y, the projection $p_G : Y \to G/Y$ turns Y into a cover of G/Y.*

*Proof.* For $\forall g \in G$, $p_G : Y \to G/Y$ given by $y \mapsto \bar{y}$ is clearly surjective.
Let $\bar{y} \in G/Y$ such that y is its representative element in Y. Let $U_y$ be an open neighbourhood of of $y \in Y$ such that $\{gU_y\}$ are pairwise disjoint. Set $U_{\bar{y}} = p_G(U_y)$.
So, $p_G^{-1}(U_{\bar{y}}) = \bigcup_{g\in G}(gU_y) = \bigsqcup_{g\in G}(gU_y)$.
We know that an action of a group on a space Y gives homeomorphism for every $g \in G$, $\tau_g : Y \to Y$ given by $y \mapsto g.y$. So each $gU_y$ are open and so is their disjoint union. Hence $p_G^{-1}(U_{\bar{y}})$ is open and by continuity of $p_G$, $U_{\bar{y}}$ is open. So, $p_G$ is an open map. Now we just need to show that $p_G$ restricted to $p_G^{-1}$ is a bijection from $gU_y$ to $U_{\bar{y}}$ . Consider the map $\phi : U_y \to U_{\bar{y}} = p(U_y)$. $\phi$ is clearly surjective. Now if $\phi(x) = \phi(y)$, it means $Gx = Gy$ or equivalently $gx = y$. So if we take an open neighbourhood U of X such that gU are pairwise disjoint for $g \in G$, $gU = V$ such that $y \in V$ is an open neighbourhood of y. If $g \neq id$, $U \cap gU = \phi$, so U and V are disjoint neighbourhoods of x and y respectively. So, for every point in Y we can find such neighbourhoods, which are disjoint from each other. This would contradict the connectedness of Y. Hence g=id or x=y. Hence $\phi$ is a homeomorphism. Composing $\phi$ with $\tau_g$, we get the required homeomorphism from $gU_y$ to $U_{\bar{y}}$. □

## 2.2 Galois Covers

Assume the base space X is locally connected i.e. each point in X admits a neighbourhood basis consisting of open connected subsets. Given a cover $p : Y \to X$, its automorphisms are precisely the topological automorphisms of the space Y over X compatible with p, i.e if $\phi \in Aut(Y|X)$, then $p \circ \phi = p$. $Aut(Y|X)$ forms a group under composition.

Also note that for each point $x \in X$, $Aut(Y|X)$ maps the fibres $p^{-1}(x)$ onto itself. So, $p^{-1}(x)$ is equipped with natural action of $Aut(Y|X)$.

**Lemma 2.2.1.** *For a connected cover $p : Y \to X$, if an automorphism $\phi$ has a fixed point i.e $\phi(y) = y$, then $\phi$ must be identity.*

We prove a more general proposition to establish above lemma.

**Proposition 2.2.1.** *Let $p : Y \to X$ be a cover, $Z$ a connected topological space. $f, g : Z \to Y$ two continuous maps satisfying $p \circ f = p \circ g$. If there is a point $z \in Z$ with $f(z) = g(z)$, then $f = g$.*

*Proof.* Let $M = \{z \in Z | f(z) = g(z)\}$. For $z \in Z$, let $f(z) = g(z) = y$. Let V be an open neighbourhood around p(y) such that $p^{-1}(V) = \bigsqcup_i U_i$, where $U_i$ are open subsets of Y such that restriction of p to $p^{-1}(V)$ is homeomorphism of $U_i$ and V. Let $y \in U_i$ for a fixed i. By the continuity of f and g, f and g must map an open neighbourhood W of z into $U_i$.

Now we know p maps $U_i$ homeomorphically to V. So by $p \circ f = p \circ g$, f and g must agree on W. So, M is open.

Now consider $z^{'} \in Z$ such that $f(z^{'}) \neq g(z^{'})$. So, $f(z^{'})$ maps some open neighbourhood of $z^{'}$ into $U_i$ and $g(z^{'})$ maps some open neighbourhood of $z^{'}$ into $U_j$, $i \neq j$. Consider the intersection of these two neighbourhoods, f,g maps this new neighbourhood into $U_i$ and $_j$ respectively. Again by previous argument, $Z - M$ is open or M is closed. So, by connectedness of Z, a non-empty clopen subset must be the whole of the space. So $f = g$ on $Z$. □

Substituting Z=Y, f=id and $g = \phi$, the previous lemma follows.

**Proposition 2.2.2.** *If $p : Y \to X$ is a connected cover, the action of $Aut(Y|X)$ is even.*

*Proof.* Let $y \in Y$ and set $x = p(y)$. Let V be an open connected neighbourhood of x such that $p^{-1}(V) = \bigsqcup_i U_i$ where $U_i$ are open subsets of Y and p restricted to $p^{-1}(V)$ is a homeomorphisms of $U_i$ and V. Assume $y \in U_i$ for a fixed i. We claim that $U_i$ is an open neighborhood of y and $\phi \in Aut(Y|X)$ such that $\{\phi U_i\}$ are pairwise disjoint. Let $\phi \neq id \in Aut(Y|X)$, then we know it maps fibres of p onto itself.

We can see that, $\phi(U_i) = U_j$, $i \neq j$ by following argument:

$p \circ \phi(U_i) = p(U_i) = V$

$\phi(U_i) = p^{-1}(V) = \bigsqcup_j U_j$, since $U_i$ is connected and $\phi$ is a homeomorphism, hence, $\phi(U_i)$ is connected. So, $\phi(U_i) = U_j$.If $i = j$, then we have a fixed point y, so by previous lemma, $\phi$ must be identity which is not the case. Hence $i \neq j$. So $\{\phi U_i\}$ are pairwise disjoint for $\phi \in Aut(Y|X)$. □

**Proposition 2.2.3.** *If G is a group acting evenly on a connected space Y, the automorphism group of the cover $p_G : Y \to G/Y$ is precisely G.*

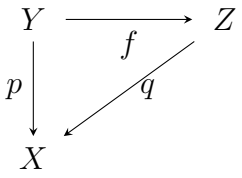
*Proof.* We can trivially see that G is a subgroup of $Aut(Y|(G/Y)$. Take $y \in G/Y$ and let V be its open neighbourhood such that $p_G^{-1}(V) = \bigsqcup_{h\in G} hU$, hU are open subsets in Y. So the action of G will take the fibres of p over V to itself. So $G \subset Aut(Y|G/Y)$. We have seen that fibres of $p_G$ over a point of G/Y are precisely the orbits of G. So if we take $\phi \in Aut(Y|(G/Y))$ and $y \in Y$, then $\exists g \in G$ such that $\phi(y) = gy$. Also $g^{-1} \in Aut(Y|(G/Y))$, so $\phi \circ g^{-1} \in Aut(Y|(G/Y))$
$\phi \circ g^{-1}(y) = \phi(g^{-1}.y) = g.g^{-1}.y = y$
So $\phi \circ g^{-1} = id$ or $\phi = g$.
Hence $\phi \in G \implies Aut(Y|(G/Y)) \subset G$.
$Aut(Y|(G/Y)) = G$. □

If we have a connected cover $p : Y \to X$, we can form the quotient of Y by the action of $Aut(Y|X)$ . It can be seen that the projection p is the composition of continuous maps $Y \to Aut(Y|X)/Y \xrightarrow{\bar{p}} X$.

**Definition 2.2.1.** *A cover $p : Y \to X$ is called Galois if it is connected and the induced map $\bar{p}$ defined above is a homeomorphism. It is equivalent to saying that a connected cover $p : Y \to X$ is Galois if and only if the action of $Aut(Y|X)$ on the fibres of p is transitive for every point in X.*

**Theorem 2.2.1.** ***Main Theorem on Galois Covers*** *Let $p : Y \to X$ be a Galois cover. For each subgroup H of $G = Aut(Y|X)$ the projection p induces a natural map $p_{\bar{H}} : H/Y \to X$ which turns $H/Y$ into a cover of X.*

*Conversely, if $Z \to X$ is a connected cover fitting into a commutative diagram*




*Then $f : Y \to Z$ is a galois cover and actually $Z \cong H/Y$ for the subgroup $H = Aut(Y|Z)$ of G. The maps $H \mapsto H/Y, Z \mapsto Aut(Y|Z)$ induce a bijection between the subgroups of G and the intermediate covers Z as above. The cover $q : Z \to X$ is Galois if and only if H is a normal subgroup of G, in which case $Aut(Z|X) \cong G/H$.*

## 2.3 The Monodromy Action

**Definition 2.3.1.** *Suppose we have a topological space X. A path in X is a continuous map $f : [0,1] \to X$, where [0,1] is the closed unit interval. This path is called a loop or a closed path if its endpoints coincide that is $f(0) = f(1)$.*
*Two paths $f, g : [0,1] \to X$ are called homotopic if $f(0) = g(0)$, $f(1) = g(1)$ and there is continuous map(also called a homotopy) $h : [0,1] \times [0,1] \to X$ such that $h(0,y) = f(y)$ and $h(1,y) = g(y)$ $\forall y \in [0,1]$.*

#### Homotopy of paths is an equivalence relation

Reflexivity: $f \sim f$ and the homotopy $h : [0,1] \times [0,1] \to X$ is given by $h(x,y) = f(y)$

Symmetric:$f \sim g \implies g \sim f$

Let $h : [0,1] \times [0,1] \to X$ is a homotopy between f and g such that $h(0,y) = f(y)$, $h(1,y) = g(y)$, $f(0) = g(0)$ and $f(1) = g(1)$. Then define $h' : [0,1] \times [0,1] \to X$ by $h'(x,y) = h(1-x,y)$.
$h'(0,y) = g(y)$ and $h'(1,y) = f(y)$. So $h'$ is a continuous map such that g is homotopic to f.

Transitivity:$f \sim g$, $g \sim h \implies f \sim h$.

Let $h_1 : [0,1] \times [0,1] \to X$ be a homotopy between f and g such that $h_1(0,y) = f(y)$ and $h_1(1,y) = g(y)$ and let $h_2 : [0,1] \times [0,1] \to X$ be a homotopy between g and h such that $h_2(0,y) = g(y)$ and $h_2(1,y) = h(y)$. Define $h_3 : [0,1] \times [0,1] \to X$ by $h_3(x,y) = h_1(2x,y)$ if $0 \leq x \leq \frac{1}{2}$ and $h_3(x,y) = h_2(2x-1,y)$ if $\frac{1}{2} \leq x \leq 1$. $h_3(0,y) = h_1(0,y) = f(y)$, $h_3(1,y) = h_2(1,y) = h(y)$, $h_3(\frac{1}{2},y) = h_1(1,y) = h_2(0,y) = g(y)$, so $h_3$ is continuous and hence f and h are homotopic.

Given two paths $f, g : [0,1] \times [0,1] \to X$ with $f(0) = g(1)$, we define their product or composition as following:

$f \circ g : [0,1] \to X$ by $(f \circ g)(x) = g(2x)$ for $0 \leq x \leq \frac{1}{2}$ and $(f \circ g)(x) = f(2x-1)$ for $\frac{1}{2} \leq x \leq 1$.

**Lemma 2.3.1.** *The above defined operation passes to quotient modulo homotopy equivalence. It means that if $f_1$, $f_2$ are two homotopic paths such that $f_1(1) = f_2(1) = g(0)$, then $f_1 \cdot g$ and $f_2 \circ g$ are also homotopic.*

*Proof.* $f_1 \sim f_2$ which means that $f_1(1) = f_2(1)$ and $f_1(0) = f_2(0)$ and also $\exists h$ : $[0,1] \times [0,1] \to X$ such that $h(0,y) = f_1(y)$ and $h(1,y) = f_2(y)$, $y \in [0,1]$.

Define $H : [0,1] \times [0,1] \to X$ by $H(x,y) = h(x, g(y))$, $H(0,y) = h(0, g(y)) = f_1 \circ g(y)$, $H(1,y) = h(1, g(y)) = f_2 \circ g(y)$.

Therefore H is a homotopy between $f_1 \circ g(y)$ and $f_2 \circ g(y)$. □

Composition of paths induces a multiplication on the set of homotopy classes of closed paths with endpoint equal to fixed $x \in X$. We denote this set by $\pi_1(X,x)$. $\pi_1(X,x)$ equipped with the multiplication described above forms a group. If $f$ is homotopic to $f^{'}$ and $g$ is homotopic to $g^{'}$, we can a find a homotopy between $f \circ g$ and $f^{'} \circ g^{'}$ by composition of two homotopies. Constant path $[0,1] \to \{x\}$ constitutes the identity element of the group. Inverse of a path $f : [0,1] \to X$ is given by $f^{-1}(x) = f(1-x)$.

**Lemma 2.3.2.** *For a path-connected topological space X, there is a isomorphism between $\pi_1(X,x)$ and $\pi_1(X,y)$ .*

*Proof.* f is a path from x to y and $f^{-1}$ is a path from y to x. Define a map, $\beta_f$ : $\pi_1(X,x) \to \pi_1(X,y)$ by $y \mapsto f \circ g \circ f^{-1}$.

$\beta_f(g) = f \circ g \circ f^{-1}$. $\beta_f$ is a homeomorphism.

$\beta_f[h \circ g] = [f \circ h \circ g \circ f{-}1] = [f \circ h \circ f^{-1} \circ f \circ g \circ h^{-1}] = [f \circ h \circ f^{-1}][f \circ g \circ h^{-1}] = \beta_f(h)\beta_f(g)$.

$\beta_f$ is an isomorphism. $\beta_f \circ \beta_{f^{-1}}[g] = \beta_f[f^{-1} \circ g \circ f] = f \circ f^{-1} \circ g \circ f \circ f^{-1} = [g]$ and similarly $\beta_{f^{-1}} \circ \beta_f[g] = [g]$. □

**Lemma 2.3.3.** ***Path Lifting lemma***
*Let $p : Y \to X$ be a cover, $y$ a point of $Y$ and $x = p(y)$. Given a path $f : [0,1] \to X$ with $f(0) = x$, there is a unique path $\tilde{f} : [0,1] \to Y$ with $\tilde{f}(0) = y$ and $p \circ \tilde{f} = f$.*

*Proof.* Let $\theta$ be an open cover of X. $f^{-1}(\theta) = \{f^{-1}(G) | G \in \theta\}$ where G are open sets in $\theta$ whose union X. So $f^{-1}(\theta)$ cover [0,1]. By Lebesgue covering lemma, we have a number $\eta$ such that for a natural number n, $\eta > \frac{1}{n}$. Consider the partition of [0,1] as $\{0, \frac{1}{n}, \frac{2}{n}, ...\frac{n-1}{n}\}$ such that for j=1,2...,n.

$f([\frac{j-1}{n}, \frac{j}{n}]) \subset G$, for some $G \subset X$. Let $f_o$ denote the restriction of $f|_{[0,\frac{1}{n}]}$, then $f([o, \frac{1}{n}]) \subset G_o \implies f(0) = x \in G_o$. Since $G_o$ is an open set in X, we have a sheet $\tilde{G_o} \in Y$ such that p(y)=x.

$p|_{\tilde{G_o}} = p_o$. Since $p_o$ is a homeomorphism between $\tilde{G_o}$ and $G_o$. Let $q_o^{-1}$ be its inverse. On sub interval $[0, \frac{1}{n}]$, we define $\tilde{f_o} = q_o \circ f_o$.

We have the initial piece of $\tilde{f}$. Now let $f_j$ be the restriction of f to $[\frac{j}{n}, \frac{j+1}{n}]$. Assume inductively for $j^{th}$ step that $\tilde{f_j} : [\frac{j}{n}, \frac{j+1}{n}] \to Y$ is defined such that $p \circ \tilde{f_j} = f_j$ and $\tilde{f_j}(\frac{j}{n}) = \tilde{f}_{j-1}(\frac{j}{n})$ and $\tilde{f_o}(0) = y$.

Call $f_j(\frac{j+1}{n}) = x_{j+1}$, $\tilde{f_j}(\frac{j+1}{n}) = \tilde{x}_{j+1}$ and $p(\tilde{x}_{j+1}) = x_{j+1}$ .

Now let $G_{j+1} \in \theta$ be an evenly covered neighbourhood of $x_{j+1}$ such that $f([\frac{j+i}{n}, \frac{j+2}{n}]) \subset G_{j+i}$. Let $\tilde{G}_{j+1}$ be a sheet in Y containing $_{j+1}$ with $p(\tilde{x}_{j+1}) = x_{j+1}$. Call $p|_{\tilde{G}_{j+1}} = p_{j+1}$. $p_{j+1}$ is a homeomorphism of $\tilde{G}_{j+1}$ onto $G_{j+1}$ . Let $q_{j+1}$ be its inverse such that $q_{j+1}(x_{j+1} = \tilde{x}_{j+1})$.

Set $\tilde{f}_{j+1} = q_{j+1} \circ f_{j+1} \implies p \circ \tilde{f}_{j+1} = f_{j+1}$ such that $\tilde{f}_{j+1}(\frac{j+1}{n}) = q_{j+1}(x_{j+1}) = \tilde{x}_{j+1} = \tilde{f_j}(\frac{j+1}{n})$.
Now glue the pieces of $\tilde{f_j}$ to yield $\tilde{f} : [0,1] \to Y$ such that $p \circ \tilde{f} = f$ and $\tilde{f}(0) = y$. Uniqueness follows from a previous proposition with X, Y and Z=[0,1]. □

**Lemma 2.3.4.** ***Homotopy lifting lemma***

*Assume moreover given a second path $g : [0,1] \to X$ homotopic to f. Then the unique $\tilde{g} : [0,1] \to Y$ with $\tilde{g}(0) = y$ and $p \circ \tilde{g} = g$ has the same end point as $\tilde{f}$ i.e. $\tilde{f}(1) = \tilde{g}(1)$.*

*Proof.* We have to show that given a homotopy $F : [0,1] \times [0,1] \to X$ with $F(0,t) = f(t)$ and $F(1,t) = g(t)$, there is a lifting $\tilde{F} : [0,1] \times [0,1] \to Y$ of F such that $p \circ \tilde{F} = F$, $\tilde{F}(0,t) = \tilde{f}(t)$ and $\tilde{F}(1,t) = \tilde{g}(t)$. The construction is same as the previous one. Consider the covering $\theta$ of X by evenly covered open neighbourhoods. Let $\epsilon$ be a Lebesgue number for the covering $\{F^{-1}(U) | U \in \theta\}$. We can choose n large enough such that any square in $[0,1] \times [0,1]$ is contained in $f^{-1}(U)$.

Now since $[0,1] \times [0,1]$ is compact. We can have a partition with grid points $\{(\frac{j}{n}, \frac{k}{n}) | 0 \le j \le n, 0 \le k \le n\}$. $S_{jk}$ is a square with vertices $\{(\frac{j}{n}, \frac{k}{n}), (\frac{j+1}{n}, \frac{k}{n}), (\frac{j+1}{n}, \frac{k+1}{n}), (\frac{j}{n}, \frac{k+1}{n})\}$. And the proof goes same as that of previous lemma. □

Now we construct the left action of $\pi_1(X,x)$ on the fibre $p^{-1}(x)$. We need $\pi_1(X,x)\times p^{-1}(x) \to p^{-1}(x)$ given by $([\alpha],y) \mapsto [\alpha].y$

If $\tilde{\alpha}$ is the unique lift of $\alpha$, so the endpoint of $\tilde{\alpha}$ must be lying over x i.e. $\tilde{\alpha} \in p^{-1}(x)$. So define $[\alpha].y = \tilde{\alpha}(1)$. This action is well defined: Replace $\alpha$ by $\alpha^{'}$ such that $\alpha$ is homotopic to $\alpha^{'}$. So, $\tilde{\alpha}$ and $\tilde{\alpha}^{'}$ will be homotopic by homotopy lifting property and so they will have the same endpoint.

Claim: The above defined action is left action. Consider $\mu_{[\alpha]} : p^{-1}(x) \to p^{-1}(x)$ given by $y \mapsto \tilde{\alpha}(1)$. To verify that its a left action, we need to show that each $\mu_{[\alpha]}$ is a bijective map.

Surjectivity: Let $y_1 \in p^{-1}(x)$. Take $\alpha^{-1}$, based at x. Take its unique lift $\tilde{\alpha^{-1}}$ such that $\tilde{\alpha^{-1}}(0) = y_1$. Let $y_2$ be the end point of the $\tilde{\alpha^{-1}}$. Then $\mu_{[\alpha]}(y_2) = y_1$

Injectivity: If $\mu_{[\alpha]}(y_1) = \mu_{[\alpha]}(y_2)$, $\tilde{\alpha_1}\circ(\tilde{\alpha_2})^{-1}$ is a lifting of $\alpha\circ\alpha^{-1}$ which is homotopic $e_{y_1}$ to and has to be equal to unique lift $e_{y_1}$. So, $y_1 = y_2$. The above defined left action is called **the monodromy action** on the fibre $p^{-1}(x)$.

We first define a functor $Fib_x$ from the category of covers to the category of sets equipped with left $\pi_1(X,x) - action$ by sending the cover $p : Y \to X$ to the fibres $p^{-1}(x)$ . $Fib_x$ is a functor:

Suppose $f : Y \to Z$ is a morphism of covers such that $p_1 : Y \to X$ and $p_2 : Z \to X$ and $p_1 = p_2 \circ f$ are the two covering maps. Fix $y \in Y$ such that $p(y) = x$. Take a path $\alpha$ in X whose unique lift in Y is $\tilde{\alpha}_1$ and in Z is $\tilde{\alpha}_2$. So $p_1 \circ \tilde{\alpha}_1 = p_2 \circ \tilde{\alpha}_2 = \alpha$. This implies $p_2 \circ f \circ \tilde{\alpha}_1 = p_2 \circ \tilde{\alpha}_2 \implies f \circ \tilde{\alpha}_1 = \tilde{\alpha}_2$ such that $z = f(y)$.

**Theorem 2.3.1.** *Let $X$ be a connected as well as locally simply connected topological space with a base point $x \in X$ . The functor $Fib_x$ defined above gives an equivalence of category of covers of $X$ and the category of sets equipped with left action of group $\pi_1(X,x)$. Connected covers come from sets with transitive left action of $\pi_1(X,x)$ and Galois covers come from coset spaces of normal subgroups.*

The above theorem is proved with the help of following two theorems:

**Theorem 2.3.2.** *For a connected and locally simply connected topological space $X$ and a base point $x \in X$, the functor $Fib_x$ is representable by a cover $\tilde{X}_x \to X$.*

The cover $\tilde{X}_x$ depends on the choice of x. By definition, the cover maps from $\pi : \tilde{X}_x \to X$ to $p : Y \to X$ correspond bijectively to the points in fibres $p^{-1}(x)$. In

particular, $Fib_x(\tilde{X}_x) \cong Hom_x(\tilde{X}_x, \tilde{X}_x)$ and the identity map of $\tilde{X}_x$ corresponds to the an element $\tilde{x}$ in the fibre $\pi^{-1}(x)$, this is called the universal element. That is, we have $\pi^{-1}(x) \cong Hom_X(\tilde{X}_x, \tilde{X}_x)$.

If $p : Y \to X$ is an arbitrary cover of X, an element $y \in pi^{-1}(x)$ corresponds to the cover map $\pi_y : \tilde{X}_x \to Y$ by the isomorphism $Fib_x(Y) \cong Hom_x(\tilde{X}_x, Y)$.

**Theorem 2.3.3.** *The cover $\tilde{X}_x$ is a connected Galois cover of X, with automorphism group isomorphic to $\pi_1(X, x)$. Moreover, for each cover $Y \to X$ the left action of $Aut(\tilde{X}_x|X)^{op}$ on $Fib_x(Y)$ given by previous construction is exactly the monodromy action of $\pi_1(X, x)$.*

*Proof.* Proof of Theorem 2.3.1

We need to check $Fib_x$ satisfies the condition of fully-faithfulness and essential surjectivity.

Fully-faithfulness: Given two connected covers $p : Y \to X$ and $q : Z \to X$, we have to prove that each map $\phi : Fib_x(Y) \to Fib_x(Z)$ of $\pi_1(X, x)$-sets come from a unique map $Y \to Z$ of covers. Consider a morphism of covers $\pi_y : \tilde{X}_x \to Y$ compatible over X. By the main theorem on Galois covers, $\pi_y$ realizes Y as a quotient of $\tilde{X}_x$ by the stabilizer $U_y = Aut(\tilde{X}_x|Y)$ of $y$ which means that for the galois cover $\pi_y : \tilde{X}_x \to Y$ and a subgroup $U_y = Aut(\tilde{X}_x|Y)$, $\pi_y$ induces a map : $U_y/\tilde{X}_x \to Y$ and let $\psi_y : Y \to U_y/\tilde{X}_x$ be the inverse map. Since $U_y \subset stab(\phi(y))$ because for $g \in U_y$, we have $g(\phi(y)) = \phi(y) = \phi(g(y))$. So $\pi_{\phi(y)=z} : \tilde{X}_x \to Z$ corresponding to $\phi(y)$ induces a map $U_y/\tilde{X}_x \to Z$. Composing above map with $\psi_y$, we get a unique map from $Y \to Z$.

For essential surjectivity, we have to show that each left $\pi_1(X, x)$ set S is isomorphic to the fibre of some cover of $X$. Lets say S is transitive, pick a point $y$ in some cover $Y$ of $X$. Take the the quotient of $\tilde{X}_x$ by the stabilizer of point $s \in S$. If S is not transitive, then decompose it into $\pi_1(X, x)$ orbits and take disjoint union covers obtained from each orbit. We get the bijection from $\sqcup S_i \to \sqcup H_i/\tilde{X}_x$. □

## 2.4 Locally constant sheaves and their classification

**Definition 2.4.1.** *Let $X$ be a topological space. A presheaf of sets $\mathcal{F}$ on $X$ is a rule that associates each non-empty open subset $U \subset X$ a set $\mathcal{F}(U)$ and each inclusion $V \subset U$ a map $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$. Here $\rho_{UU}$ are the identity maps. If we have a tower of inclusions $W \subset V \subset U$, the the identity $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$ holds. Elements of $\mathcal{F}(U)$ are called sections of $\mathcal{F}$ over $U$.*

*We can similarly define presheaf of groups, abelian groups or rings where $\mathcal{F}(U)$ are groups, abelian groups or rings respectively and $\rho_{UV}$ are the homomorphisms.*

With this definition, we see that presheaf of sets on a space X forms a category where the morphism of presheafs $\Phi : \mathcal{F} \to \mathcal{G}$ is collection of the maps $\Phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ such that for every inclusion $V \subset U$, we have the following commutative diagram.

$$\begin{array}{ccc} \mathcal{F}(V) & \xrightarrow{\Phi_V} & \mathcal{G}(V) \\ {\scriptstyle \rho^{\mathcal{F}}_{UV}}\downarrow & & \downarrow{\scriptstyle \rho^{\mathcal{G}}_{UV}} \\ \mathcal{F}(U) & \xrightarrow{\Phi_U} & \mathcal{G}(U) \end{array}$$

We can think of continuous real valued functions defined locally on the open sets of X. For each inclusion $V \subset U$ we have an inclusion map $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ such that for $f \in \mathcal{F}(U)$, $\rho_{UV}(f) = f|_V$. Given two open sets $U_1$ and $U_2$ and continuous functions $f_i : U_i \to R$, $i = 1, 2$ such that $\forall x \in U_1 \cap U_2$ we have $f_1(x) = f_2(x)$, we can define a continuous function $f : U_1 \cup U_2 \to R$ by setting $f(x) = f_i(x)$ if $x \in U_i$. This is the patching property of continuous functions.

**Definition 2.4.2.** *A presheaf $\mathcal{F}$ is a sheaf if it satisfies the following two axioms:*

*1. Given a non-empty open set $U$ and a covering $\{U_i : i \in I\}$ of $U$ by non-empty open sets, if two sections $s, t \in \mathcal{F}(U)$ satisfy $s|_{U_i} = t|_{U_i} \forall i \in I$, then $s = t$.*

*2.For any open covering $\{U_i : i \in I\}$ of $U$ as above, given a system of sections $s_i \in \mathcal{F}(U)_i : i \in I$ with the property $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$, $\exists s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i \forall i \in I$.*

**Definition 2.4.3.** *Let $S$ be a topological space and $X$ be another topological space. Define a sheaf $\mathcal{F}_S$ on $X$ where the elements of $\mathcal{F}_S(U)$ are the continuous functions $U \to S$ for a non-empty open subset $U \subset X$.*

*If the space $S$ is discrete, then the sheaf $\mathcal{F}_S$ is called the* ***constant sheaf*** *on $X$ with value $S$.*

**Definition 2.4.4.** *A sheaf $\mathcal{F}$ on topological space $X$ is called locally constant if every point in $X$ has an open neighbourhood $U$ such that $\mathcal{F}|_U$ is isomorphic to a constant sheaf.*

**Definition 2.4.5.** *Let $p : Y \to X$ be a space over $X$, $U \subset X$ be an open set in $X$. A section of $p$ over $U$ is a continuous map $s : U \to Y$ such that $p \circ s = id_U$. So we can define a presheaf $\mathcal{F}_Y$ such that for an open set $U \subset X$, the elements of $\mathcal{F}_Y(U)$ are the sections of $p$ over $U$.*

**Proposition 2.4.1.** *The presheaf $\mathcal{F}_Y$ just defined is a sheaf. If $p : Y \to X$ is a cover, the $\mathcal{F}_Y$ is locally constant. It is constant if and only if the cover is trivial.*

*Proof.* The sections of the presheaf are nothing but continuous functions $U \to Y$ which satisfy the sheaf axioms or the patching property. So $\mathcal{F}_Y$ is a sheaf.
If Y is cover over X, take a point $x \in X$ and an open connected neighbourhood V of $x$. By an earlier result in covers, we know that the cover over V is trivial i.e. it is isomorphic to $V \times p^{-1}(x)$. Let s be a section of p over V. $s(V)$ is a connected open subset of Y such that $p(s(V)) = V$. So $s(V)$ must be one of the components of $p^{-1}(V)$. Hence the sections of p over V are in bijection with the points in the fibre $p^{-1}(x)$ and $\mathcal{F}_Y|_V$ is isomorphic to constant sheaf defined by the fibres over $x$. □

A morphism $\phi : Y \to Z$ of covers over X induces a natural morphism $\mathcal{F}_Y \to \mathcal{F}_Z$ of locally constant sheaves by the map $s \mapsto \phi \circ s$ where $s : U \to Y$ is a section of $p : Y \to X$ over $U$. So we have a functor $Y \to \mathcal{F}_Y$.

**Definition 2.4.6.** *Let $\mathcal{F}$ be a presheaf of sets on space $X$. Take a point $x \in X$. The* ***Stalk*** *$\mathcal{F}_x$ of $\mathcal{F}$ at $x$ is defined as disjoint union of open neighbourhoods $U$ of $x$ modulo $\sim$, where the equivalence relation $\sim$ is as: $s \in \mathcal{F}(U)$ and $t \in \mathcal{F}(V)$ are equivalent if $\exists$ open neighbourhood $W \subset U \cap V$ of $x$ such that $s|_W = t|_W$.*

*The sets $\mathcal{F}(U)$ form a direct system indexed by an indexing set whose direct limit is $\mathcal{F}_x$.*

**Construction 2.1.** *Construction of space $X_{\mathcal{F}}$*

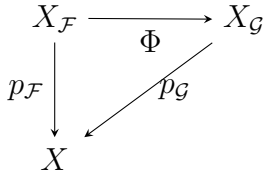
*Now we construct a space $p_{\mathcal{F}} : X_{\mathcal{F}} \to X$ over $X$. $X_{\mathcal{F}}$ is a disjoint union of the stalks $\mathcal{F}_x$. Define $p_{\mathcal{F}}^{-1}(x) = \mathcal{F}_x \ \forall x \in X$. $p_{\mathcal{F}}$ is the projection map defined by $\mathcal{F}_x \to \{x\}$. Now we give a topology to the space $X_{\mathcal{F}}$. Given an open set $U \subset X$ and a section $s \in \mathcal{F}(U)$, define a map $i_s : U \to X_{\mathcal{F}}$ by $x \mapsto s_x$ where $s_x$ is the image of $s$ in the stalk $\mathcal{F}_x$. The sets $i_s(U)$ are the open sets in $X_{\mathcal{F}}$ for all $U$ and $s$. This definition turns the maps $i_s$ and $p_{\mathcal{F}}$ into continuous maps. Moreover we have $p_{\mathcal{F}}^{-1}(U) = \bigcup_{s \in \mathcal{F}(U)} i_s(U)$.*

*If $\mathcal{F}$ is locally constant, then $X_{\mathcal{F}}$ is a cover of $X$. For a connected open set $U \subset X$, $\mathcal{F}|_U \cong F$, where $F$ is a constant sheaf and has discreet topology. Then the fibres of $p_{\mathcal{F}}$ over $x \in U$ is equal to $F$, so $p_{\mathcal{F}}^{-1}(U) \cong U \times F$.*

**Theorem 2.4.1.** *The above defined functor induces an equivalence between the categories of covers of $X$ and that of locally constant sheaves on $X$.*

A morphism $\phi : \mathcal{F} \to \mathcal{G}$ of presheaves induces the maps $\mathcal{F}_x \to \mathcal{G}_x$ for each $x \in X$ which induces a map $\Phi : X_{\mathcal{F}} \to X_{\mathcal{G}}$(as sets) compatible with projections onto $X$.

This map $\Phi$ is a morphism of spaces over X. We just need to see that the map $\Phi$ is continuous. Consider the following commutative diagram




Let $U \subset X$ be an open set and $t \in \mathcal{G}(U)$ where $i_t : U \to X_{\mathcal{G}}$ is a continuous map such that $p_{\mathcal{G}} \circ i_t = id_U$. By the commutativity of the diagram, we have $p_{\mathcal{G}} \circ \Phi = p_{\mathcal{F}}$ or $p_{\mathcal{G}} = p_{\mathcal{F}} \circ \Phi^{-1}$. So we have $p_{\mathcal{G}}(i_t(U)) = U = p_{\mathcal{F}}(\Phi^{-1}(i_t(U)))$. It means that $\Phi^{-1}(i_t(U))$ is open and hence the map $\Phi$ is continuous.

So the rule $\mathcal{F} \to X_{\mathcal{F}}$ is a functor from the category of sheaves on X to the category of spaces over X. If the sheaf $\mathcal{F}$ is locally constant, then the spaces over X become the covers of X and the fibres of $X_{\mathcal{F}}$ over $x$ is the stalk $\mathcal{F}_x$.

*Proof.* Proof of Theorem 2.4.1

We need to show $\mathcal{F}_{X_{\mathcal{F}}} \cong \mathcal{F}$ functorially given a locally constant sheaf $\mathcal{F}$ on $X$ and conversely, given a cover $Y \to X$, $X_{\mathcal{F}_Y} \cong Y$. We have a natural morphism of sheaves

$\mathcal{F} \to \mathcal{F}_{X_\mathcal{F}}$ given by $s \mapsto i_s$ where $s \in \mathcal{F}(U)$ and $i_s : U \to X_\mathcal{F}$ is a local section. Similarly we have a morphism of covers $Y \to X_{\mathcal{F}_Y}$ where $y$ maps to corresponding point in the fibre $\mathcal{F}_{Y,x}$ over $x$ where $y \in Y$ is a point in the fibres over the point $x$. To show that these morphisms are isomorphisms, we consider an open covering $\{U_i : i \in I\}$ of X. $\mathcal{F}|_{U_i}$ is constant sheaf $\forall i \in I$. By replacing each $U_i$ by $X$, $\mathcal{F}$ becomes constant on $X$ and so we can assume $\mathcal{F}$ to be a constant sheaf with values in a discrete set F. We have $X_F \cong X \times F$, so $\mathcal{F}_{X_\mathcal{F}} \cong \mathcal{F}$ holds true. Conversely, the local sections of the trivial cover $X \times F \to X$ is the constant sheaf defined by F. □

Combining it with Theorem 2.3.1 we obtain the following result:

**Theorem 2.4.2.** *Let $X$ be a connected and locally simply connected topological space, and let $x$ be a point in $X$. The category of locally constant sheaves of sets on $X$ is equivalent to the category of sets endowed with a left action of $\pi_1(X, x)$.*

$\mathcal{F}_x$ is equipped with left action by $\pi_1(X, x)$. $\pi_1(X, x) \times \mathcal{F}_x \to \mathcal{F}_x$ defined by $\alpha.y = \tilde{f}(1)$, where $f$ is a representative of the class $\alpha$ such that $f(0) = x = f(1)$, $\tilde{f}$ is a unique lift of $f$.

**Theorem 2.4.3.** *Let $X$ and $x$ be as above and $R$ be a commutative ring. The category of locally constant sheaves of $R$-modules on $X$ is equivalent to category of left modules over the group ring $R[\pi_1(X, x)]$.*

*Proof.* The stalk $\mathcal{F}_x$ is an R module and is equipped with left action by $\pi_1(X, x)$. We need to show that $\mathcal{F}_x$ is $R[\pi_1(X, x)]$ module that is the action of $\pi_1(X, x)$ is compatible with the R-module structure. Define the direct product of sheaves $\mathcal{F} \times \mathcal{F}$ by $(\mathcal{F} \times \mathcal{F})(U) = \mathcal{F}(U) \times \mathcal{F}(U)$ where $U \subset X$ is an open set. Its stalk over a point $x$ is $\mathcal{F}_x \times \mathcal{F}_x$. Addition on $\mathcal{F}$ over an open set $U$ is simple defined by $(s_1, s_2) \mapsto s_1 + s_2$ and similarly we can induce this map to the level of stalk $\mathcal{F}_x$. And since $\mathcal{F}_x$ is equipped with left action of $\pi_1(X, x)$, we have $\sigma(s_1 + s_2) = \sigma s_1 + \sigma s_2$ for $\sigma \in \pi_1(X, x)$ and $s_1, s_2 \in \mathcal{F}_x$ and $\sigma(\alpha s_1) = \alpha\sigma(s_1)$ for $\alpha \in R$. □

## 2.5 Local systems

**Definition 2.5.1.** *A complex local system on $X$ is a locally constant sheaf of finite dimensional complex vector space. If the space $X$ is connected, then the stalks have the same dimension which is called the dimension of the complex system.*

The following corollary follows from the previous theorem and definition:

**Corollary 2.5.1.** *Let $X$ be a connected and simply connected topological space. Category of complex local systems on $X$ is equivalent to the category of finite dimensional left representations of $\pi_1(X, x)$.*

This means that for given a complex system on X, we have a homomorphism $\pi_1(X, x) \to GL(n.C)$. This called the monodromy representation of local system.

**Example 2.1.** *Let $D \subset C$ be a connected open subset. Consider $n^{th}$ order linear differential equation $y^n + a_1 y^{n-1} + a_2 y^{n-2} ..... + a_{n-1} y' + a_n y = 0$ where $a_i$ are the holomorphic functions on $D$. For every open set $U \subset D$, consider the local holomorphic solutions of the equation on $U$. A C-linear combination of the local solutions over $U$ is also a solution of the differential equation. So the solutions over $U$ form a complex vector space, denote it by $S(U)$. By a theorem of Cauchy([For81], Theorem 11.2) we know that each point of $D$ has an open neighbourhood $U$ such that $S(U)$ has a finite basis $x_1, x_2 .... x_n$. So the local solution form a subsheaf of $\mathcal{O}^n$. $S$ is a complex local system of dimension $n$.*

*The local system $S$ of the above example is uniquely determined $n$-dimensional left representation of $\pi_1(X, x)$. Take a point $x \in D$, a closed path $f : [0, 1] \to D$ such that $f(0) = x = f(1)$ representing $\gamma \in \pi_1(X, x)$. Take $s \in S_x$ which is germ of the holomorphic function satisfying the differential equation. Since $S$ is a complex local system or a locally constant sheaf, we have a cover $p_S : D_S \to D$. We have $s \in S_x = p_S^{-1}(x)$. Action of $\gamma$ on $s$ is given by $[\gamma].s = \tilde{f}(1)$, such that $\tilde{f}(0) = s$ and $\tilde{f}$ is the unique lift of $f$ to the space $D_S$.More explicitly, we can look into the proof of homotopy lifting lemma, we have open sets $U_1, ....U_k$ of $D$ such that $f^{-1}(U_1), ....f^{-1}(U_k)$ form an open covering of $[0, 1]$. $S$ being a locally constant sheaf is constant over each $U_i$. There are section $s_i \in S_i$ such that $s_i|_{U_i \cap U_{i+1}} = s_{i+1}|_{U_i \cap Ui+1}$ for all $1 \leq i \leq k-1$, such that $s_1$ maps to $s$, $s_k$ maps to $\gamma s$ in $S_x$. $\gamma s$ is the analytic continuation of the germ $s$ along the path $f$.*

# Chapter 3

# Riemann surfaces

The main aim of this chapter is to draw a link between the Galois theory and the theory of covers which can be done by studying covers of Riemann surfaces. We will use some results from the theory of Riemann surfaces to study the absolute Galois group of $\mathbb{C}(t)$.

## 3.1 Basics

X-topological space which is Hausdorff. We define a **Complex atlas** on $X$ as an open cover $\mathcal{U} = \{U_i : i \in I\}$ with the associated maps $f_i : U_i \to C^n$ that map $U$ homeomorphically onto some open subset of $C^n$, and for each pair $(i, j) \in I \times I$, with a additional condition that the maps $f_i \circ f_j^{-1} : f_j(U_i \cap U_j) \to C^n$ become holomorphic. We call these $f_i$'s as complex charts.

Equivalence of complex atlases: Two complex atlases $\mathcal{U}$ and $\mathcal{U}'$ are said to be equivalent if their union is also a complex atlas and the map $f_i' \circ f_j^{-1} : f_j(U_i' \cap U_j) \to \mathbb{C}^n$ are holomorphic.

The space defined above is called n-dimensional complex manifold. For n=1, the space is called Riemann surface.

**Example 3.1.** *In 2-sphere $S^2$, fix two antipodal points $0, \infty \in S^2$. Now define the following two complex charts: $z : S^2 - \infty \to C$ mapping it homeomorphically onto $C$ by stereographic projection defined below:*

*$z(p,q,r) = \frac{p}{1-r} + i\frac{q}{1-r}$ where $(p,q,r)$ is a point in $S^2$. And the other complex chart which is a homeomorphism from $S^2 - 0 \to C$ defined by the maps $\infty \mapsto 0$ and $z \mapsto \frac{1}{z}$. The two maps defined above are holomorphic and the Riemann surface is called complex projective line $P_1(C)$.*

**Definition 3.1.1.** *Holomorphic map between two Riemann surfaces $Y$ and $X$ is a continuous map $\phi : Y \to X$ such that every pair of open sets $U \subset X$ and $V \subset Y$ fulfilling the condition $\phi(V) \subset U$ and also for the complex charts $f : U \to C$ and $g : V \to C$, $f \circ \phi \circ g^{-1} : g(V) \to C$ are holomorphic functions.*

## 3.2 Important facts about Riemann surfaces and Holomorphic maps

**Proposition 3.2.1.** *Let $\phi : Y \to X$ be a holomorphic map between two Riemann surfaces and $x$, $y$ be points in $X$ and $Y$ resp. such that $\phi(y) = x$. Then open neighbourhoods $U_y$ of $y$ and $V_x$ of $x$ such that $\phi(U_y) \subset V_x$ and the complex charts $g_y : U_y \to C$ and $f_x : V_x \to C$ that satisfy $f_x(x) = g_y(y) = 0$ and the following diagram commutes for a positive integer $e_y$.*

$$\begin{array}{ccc} U_y & \xrightarrow{\phi} & V_x \\ {\scriptstyle g_y}\downarrow & & \downarrow{\scriptstyle f_x} \\ C & \xrightarrow{z \mapsto z^{e_y}} & C \end{array}$$

**Definition 3.2.1.** *The integer $e_y$ defined above is called the ramification index or branching order of $\phi$ at the point $y$. The points in the surface $Y$ with $e_y > 1$ are called branch points of $\phi$ and their set is called $S_\phi$.*

**Corollary 3.2.1.** *A holomorphic map between two Riemann surfaces is open.*

*Proof.* Since the complex charts $f_x$ and $g_x$ are open and continuous and the map $z \mapsto z^e$ is open, the map $\phi$ is open. □

**Corollary 3.2.2.** *The fibres of $\phi$ and set $S_\phi$ are discrete closed subsets of $Y$.*

**Definition 3.2.2.** *A map between two locally compact topological spaces is called **Proper** if it is continuous and the pre-image of every compact subset is compact. Additionally, for Hausdorff spaces, a proper map is closed as well.*

**Proposition 3.2.2.** *Let $\phi : Y \to X$ be a proper holomorphic map between two Riemann surfaces and $X$ be connected. This map $\phi$ is surjective having finite fibres. Also, when restricted to $Y - \phi^{-1}(\phi(S_\phi))$, $\phi$ turns into a cover of $X - \phi(S_\phi)$.*

*Proof.* The fibres of $\phi$ form a discrete closed subset of Y and discrete closed subsets of compact space are finite.

Surjectivity of $\phi$: $\phi$ is an open map, so by the openness of $Y$, $\phi(Y)$ becomes open in $X$. Also, $\phi$ is proper hence it is closed, so $\phi(Y)$ is also closed in $X$. But since $X$ is connected, $\phi(Y) = X$, hence $\phi$ is surjective. Since the fibres of $\phi$ are finite, consider finitely many pre-images of a point $x \in X - \phi(S_\phi)$. By a previous result, each of these has an open neighbourhood $V_y$ mapping homoemorphically onto an open neighbourhood of $x$. Take the intersection over these finite open neighbourhoods of $x$ which is open and we have an open neighbourhood around each point $x$ satisfying the definition of covers. So $Y - \phi^{-1}(\phi(S_\phi))$ turns into a cover of $X - \phi(S_\phi)$. □

**Definition 3.2.3.** *A proper surjective map of locally compact Riemann surfaces is called* ***finite branched cover*** *if outside a discrete closed subset, it restricts to a cover.*

**Notation** Let $X$ be a connected Riemann surface and $S \subset X$ be a discrete closed subset of $X$. The category of Riemann surfaces equipped with proper holomorphic maps $Y \to X$ such that all its branched points lie above $S$ is denoted by $Hol_{X,S}$.

**Theorem 3.2.1.** *There is an equivalence between the category of Riemann surfaces and the topological covers of $X - S$ obtained by sending a Riemann surface $\phi : Y \to X$ to the topological cover $Y - \phi^{-1}(S) \to X - S$ via restricting the map $\phi$.*

The following helping lemma proves theorem for $S = \emptyset$:

**Lemma 3.2.1.** *Let $p : Y \to X$ be a connected topological cover of a Riemann surface $X$. A unique complex structure can be given to space $Y$ such that $p$ is a holomorphic map.*

*Proof.* Since $Y$ is a cover of $X$, every $y \in Y$ has an open neighbourhood $V$ such that it is mapped homeomorphically onto an open neighbourhood $U$ of the point $p(y)$. Take an open subset $U'$ of $U$ containing the point $p(y)$ and a complex chart $f : U' \to C$, then $f \circ p$ defines a complex chart in the neighbourhood of point $y \in Y$ since $p$ and

$f$ are local homeomorphisms. And open neighbourhood around $y \in Y$ belongs to complex atlas on $Y$. The complex structure is unique because $p|_V : V \to U$ is a homeomorphism. □

**Proposition 3.2.3.** *Let $X$ be a connected Riemann surface and $S \subset X$ be a discrete closed set, $X' = X - S$ and $\phi' : Y' \to X'$ be a finite connected cover of $X'$. Then there exists a Riemann surface $Y \supset Y'$ as an open set and there is a proper holomorphic map $\phi : Y \to X$ such that $\phi|_{Y'} = \phi'$ and $Y' = Y - \phi^{-1}(S)$.*

**Definition 3.2.4.** *$Y$ is a finite Galois Branched cover of $X$ in above proposition, if $Y'$ is Galois over $X'$.*

Facts about Galois branched covers: If $\phi : Y \to X$ is a proper holomorphic map between connected Riemann surfaces and $Y$ is Galois branched cover of $X$, then:

1. $Aut(Y|X)$ acts transitively on the fibres of $\phi$.

2. All the points in $\phi^{-1}(\phi(y))$ are branch points if $y \in Y$ is a branch point with the same branching order.

## 3.3 Relation with field Theory

**Definition 3.3.1.** *A function $f$ on Riemann surface $X$ is called meromorphic if for some closed discrete space $S \subset X$, $f$ is holomorphic on $X - S$ and for all complex charts $\phi : U \to C$, the function $f \circ \phi^{-1} : \phi(U) \to C$ is holomorphic.*

The ring of meromorphic functions on $X$ is denoted by $\mathcal{M}(X)$.

**Lemma 3.3.1.** *$\mathcal{M}(X)$ is a field if $X$ is connected.*

*Proof.* Take $f \in \mathcal{M}(X)$ and if the zeroes of $f$ form a discrete closed space, then $\frac{1}{f} \in \mathcal{M}(X)$. Assume that the solution set $S$ isn't discrete or we can say that it is an infinite subset of X, $S$ must have a limit point. Indeed, assume that there is no limit point of the infinite subset $S$, so every point $x \in X$ has an open neighbourhood $U_x$ such that $S \cap U_x$ contains at most one point which is $x$, only when $x \in S$. Hence $S$ cannot be covered by finite collection of open neighbourhoods. Similarly we can argue $X$ cannot be covered by finite collection of open subsets, which means $X$ is not compact, which is a contradiction. Hence $S$ has a limit point say $x$.

By composing $f$ with complex chart $U \to C$ such that $x \in U$, we get a holomorphic function on complex domain whose set of zeros has a limit point. By a theorem on complex analysis ([1],Theorem 10.18), $f$ is zero on the complex domain and hence $f$ is zero in some neighbourhood of $x$. Now form a set of those points in $X$, such that the function $f$ vanishes on the neighbourhood of those points. This set is open and also it is closed because it contains all of its limit points. Now since $X$ is connected, then $f = 0$ on X, which is a contradiction. So set of zeros of $f$ is discrete and hence $\frac{1}{f} \in \mathcal{M}(X)$. □

**Theorem 3.3.1.** ***Riemann's Existence Theorem*** *Let $x_1, x_2, ...x_n$ be finite number of points in compact Riemann surface $X$ and assume $a_1, a_2....a_n$ be a sequence of complex numbers. Then there exists a meromorphic function $f$ contained in $\mathcal{M}(X)$ with the property that $f$ is holomorphic at all the $x_i$ with $f(x_i) = a_i$, $1 \leq i \leq n$.*

A holomorphic map $\phi : Y \to X$ between two Riemann surfaces induces a ring homomorphism $\phi^* : \mathcal{M}(X) \to \mathcal{M}(Y)$ by the map $\phi^*(f) = f \circ \phi$. Under the assumptions that $X$ is connected, $X$ and $Y$ are compact, $\phi$ is proper surjective map with finite fibres, $\mathcal{M}(Y)$ becomes a finite etale algebra over $\mathcal{M}(X)$. $Y$ is the disjoint union of connected and compact Riemann surfaces $Y_i$ if not, then there are infinitely many connected components covering $Y$ which contradicts compactness of $Y$. So we have $\mathcal{M}(Y) = \Pi\mathcal{M}(Y_i)$.

**Proposition 3.3.1.** *Let $\phi : Y \to X$ be a non-constant holomorphic map of compact and connected Riemann surfaces, which has a degree $d$ as a branched cover. The induced field extension $\mathcal{M}(Y)|\phi^*\mathcal{M}(X)$ is finite of degree $d$.*

The above proposition follows from the following lemma

**Lemma 3.3.2.** *Let $\phi : Y \to X$ be a proper holomorphic map of connected Riemann surfaces which has a degree $d$ as a branched cover. Every meromorphic function $f \in \mathcal{M}(Y)$ satisfies a polynomial equation of degree $d$ over $\mathcal{M}(X)$.*

*Proof.* Take $S$ to be the set of branch points of $\phi : Y \to X$. Take a point $x \in X - \phi(S)$. Since $Y - \phi^{-1}(\phi(S_\phi))$ is a topological cover of $X - S(\phi)$, there exists an open neighbourhood $U \subset X$ containing $x$ such that $\phi^{-1}(U) \cong \bigsqcup V_i$, where $V_i$'s are open neighbourhoods in $Y$. The restriction of $\phi$ to $V_i$ is an homeomorphism of $V_i$ onto $U$. Denote the holomorphic section of $\phi$ mapping $U$ onto $V_i$ homeomorphically by $s_i$. Let $f_i = f \circ s_i$, $f_i$ meromorphic on $U$. Substitute $A = \Pi(t - f_i) = t^d + a_{d-1}t^{d-1} + ...a_0$,

where $a_i$'s are symmetric polynomials of $f_i$ and hence are meromorphic. Now take another point $x^{'} \in X - \phi(S)$ and let $U^{'}$ be the neighbourhood around $x^{'}$. Construct a polynomial $A^{'}$ as done for the previous point on open set $U \cap U^{'}$. The roots of $A^{'}$ and $A$ are same meromorphic functions so the coefficients of $A^{'}$ coincide with those of $A$. So $a_i$'s extend to meromorphic functions in $X - \phi(S)$. Now we show that they extend to meromorphic function in $X$. Take $x \in \phi(S)$, pick a coordinate chart $f_x : U_x \to \mathbb{C}$ where $U_x \subset U$ is a neighbourhood around $x$ with $f_x(x) = 0$. The function $f_x \circ \phi$ defines a holomorphic function in some open neighbourhood of each of the points $y \in \phi^{-1}(x)$ such that $(f_x \circ \phi)(x) = f_x(x) = 0$. $f$ is meromorphic for all $y \in Y$, we find a positive $k$ such that $(f_x \circ \phi)^k f$ is holomorphic for $y \in \phi^{-1}(x)$.

Compose the above functions with $s_i$ to get function in $U_x - \{x\}$. The function $f_x^k f_i$ are bounded on $U_x - \{x\}$. By Riemann removable singularity Theorem([1], Theorem 10.20), $a_i$'s extend to holomorphic functions on $U_x$. $A \in \mathcal{M}(X)[t]$. Now we see that over $U$, $(\phi^* A \circ s_i)(f \circ s_i) = A(f_i) = 0$. □

*Proof.* Proof of Proposition 3.3.1

Take $x \in X - \phi(S)$. Let $y_1, ...y_k \in \phi^{-1}(x)$. We can find an $f \in \mathcal{M}(Y)$ such that $f$ is holomorphic at each of $y_i$ and $f(y_i)$ are distinct. Also by previous lemma such $f$ satisfies a polynomial $(\phi^* a_n) f^n + .... + \phi^* a_0 = 0$ where $a_i \in \mathcal{M}(X)$. Assuming that all $a_i$ are holomorphic at $x$, the polynomial $a_n(x) f(y_i)^n + ....a_0(x)$ has d roots which are the distinct $f(y_i)$.

If one of the $a_i$ is not holomorphic at $x$, the consider an small neighbourhood around $x$. $f$ is holomorphic on that neighbourhood and and the neighbourhood doesn't contain images of branch points. So take one of the points in that neighbourhood where all $a_i$ are holomorphic. We have $\mathcal{M}(Y) \cong \mathcal{M}(X)(f)$. □

Now, the functor $Y \to \mathcal{M}(Y)$ is from the category of compact Riemann surfaces mapping onto a compact Riemann surface $X$ via a holomorphic map to the category of finite etale algebra's over $\mathcal{M}(X)$.

**Theorem 3.3.2.** *The above defined functor induces an anti-equivalence between the category of finite Galois extension of the field $\mathcal{M}(X)$ and finite Galois branched covers of $X$ having the same degree.*

Above theorem follows from the following result:

**Proposition 3.3.2.** *Let $A$ be a finite etale algebra over $\mathcal{M}(X)$ where $X$ is compact and connected Riemann surface. Then there exists a compact Riemann surface $Y$ (that maps holomorphically onto $X$) such that there is an isomorphism between $\mathcal{M}(Y)$ and $A$ as an $\mathcal{M}(X)$-algebra.*

*Proof.* Consider a finite field extension $L|\mathcal{M}(X)$. Let $\alpha$ be the primitive element in $L$, generating $L$ over $\mathcal{M}(X)$ and $F$ be the minimal separable polynomial of $\alpha$ with degree $d$. Since $F$ is separable, the ideal $< F, F^{'} >$ generates the whole ring $\mathcal{M}[t]$([DFon], Proposition 33, Chapter13). So there exists functions $P, Q \in \mathcal{M}(X)$ such that $PF+PF^{'} = 1$. The coefficients of $F$ are in $\mathcal{M}(x)$, evaluate these coefficients at some point $x \in X$ and call the resulting polynomial $F_x$. $F_x$ and $F_x^{'}$ can have a common zero only at the points in $X$ where either A or B. Let $S$ be a discrete closed set of the points in $X$ that are the poles of the function $F$ ,$A$ and $B$ and $X^{'} = X - S$. If $F_x(a) = 0$ then $F_x^{'}(a) \neq 0$. So, for $x \in X^{'}$, the polynomial $F_x \in C[t]$ has d distinct roots.

For an open set $U \subset X^{'}$, let $\mathcal{F}(U)$ be the set of holomorphic functions $f$ on $U$ such that $F(f) = 0$. We claim that $\mathcal{F}$ is a locally constant sheaf with stalks of cardinality d. By implicit function theorem([PG78], pg.19), for a point $x \in X^{'}$ and a root $a_i$ of polynomial $F_x \in C[t]$, $F_x^{'}(a_i) \neq 0$ implies that there exists functions $f_i$in a neighbourhood of $x$ such that $f_i(x) = a_i$ and $F(f_i) = 0$. So we have d such functions $f_i$, each corresponding to d roots of $F_x$. The polynomial $F$ of degree d is a product of polynomials $(t - f_i)$, so the sheaf $\mathcal{F}$ cannot have more than d sections. So over a connected open subset $V \subset X^i$, $\mathcal{F}$ is isomorphic to finite set of functions $f_1, ...f_d$.

We know that category of locally constant sheaves over $X$ is equivalent to the category of covers over $X$. So there exists a cover $p_{\mathcal{F}} : X_{\mathcal{F}}^{'} \to X^{'}$ of $X^{'}$. By a previous proposition 3.2.9 , for each connected component of the cover $X_{\mathcal{F}}^{'}$ we get a compact Riemann surface $Y_j$. Now we have to show that $X_{\mathcal{F}}^{'}$ is connected which means that we get only one Riemann surface. To see that, define a function $f$ on $X_{\mathcal{F}}^{'}$ by $f(f_i) = f_i(p_{\mathcal{F}}(f_i))$. We have seen in a proof of previous proposition that $f$ extends to a meromorphic function on each $Y_j$ and moreover $f \in \mathcal{M}(Y_j)$ has a minimal polynomial $H$ over $\mathcal{M}(X)$ of degree $d_j$, where degree $d_j$ is the cardinality of the fibres of cover of one of the connected components. Now as assumed in the beginning $F(f) = 0$, so $G$ must divide $F$, but since $F$ is irreducible, $F = G$ and hence $d_j = d$. So there is only one connected compact Riemann surface, denote it by $Y$. By the map $f \mapsto \alpha$ and the equality of degrees of the two field extension of $\mathcal{M}(X)$, we have $L = \mathcal{M}(Y)$. □

The above theorem along with a previous theorem gives the following corollary:

**Corollary 3.3.1.** *For a compact and connected Riemann surface $X$, the category of compact Riemann surfaces mapping holomorphically onto $X$ is equivalent to the category of finite sets quipped with continuous left action of $Gal(\overline{\mathcal{M}(X)}|\mathcal{M}(X))$.*

Now we consider the case when $X = \mathbb{C}P^1$ in Theorem 3.3.2:

**Proposition 3.3.3.** *There exists a holomorphic map $Y \mapsto \mathbb{C}P^1$ which is not constant, where $Y$ is compact and connected Riemann surface. As a result, $\mathcal{M}(Y)$ becomes a finite field extension of $\mathbb{C}(t)$.*

*Proof.* $\mathcal{M}(Y)$ contains a non-constant meromorphic function f by Theorem 3.3.1. Define a function $\rho_f : Y \to \mathbb{C}P^1$ by

$$\rho_f(y) = \begin{cases} \text{f(y)} & \text{y is not a pole of f} \\ \infty & \text{y is a pole of f} \end{cases}$$

We need to show that $\rho_f$ is holomorphic. Consider complex charts in a neighbourhood of point $y \in Y$ given by $g : U \to C$ such that $f$ is holomorphic on $U - \{y\}$ and two complex charts given on $\mathbb{C}P^1$ are $z$ and $\frac{1}{z}$ as defined in the beginning of the chapter.

Now if $f$ does not have a pole at $y$, then the function $z \circ \rho_f \circ g^{-1}$ is holomorphic on $g(U)$. If $f$ has a pole at $y$, then the function $\frac{1}{z} \circ \rho_f \circ g^{-1}$ maps $g(U - \{y\})$ onto an open subset around 0 of C and by Riemann's removable singularity theorem([[Rudon], Theorem 10.20), the function extends to holomorphic function on $g(U)$. So $\rho_f$ is holomorphic.

From the result [Gar], Claim[3.0.1], it follows that $\mathcal{M}(\mathbb{C}P^1) \cong C(t)$. And from Proposition 3.3.1, it follows that $\mathcal{M}(Y)$ is a finite extension of $C(t)$. □

## 3.4 The absolute Galois group of $\mathbb{C}(t)$

**Theorem 3.4.1.** *Consider a connected and compact Riemann surface $X$ and denote the complement of finite set of points by $X'$. Fix an algebraic closure $\overline{\mathcal{M}(X)}$ of $\mathcal{M}(X)$ and take the compositum of all finite sub extension fields in this closure that are*

*coming from holomorphic maps $Y \to X$ of compact and connected Riemann surfaces restricting to a cover over $X^{'}$. Call this composite as $K_{X'}$. $K_{X'}|\mathcal{M}(X)$ is Galois field extension and there is an isomorphism $Gal(K_{X'}|\mathcal{M}(X)) \cong \widehat{\pi_1(X', x)}$, for some $x \in X^{'}$.*

The above theorem uses the following result.

**Lemma 3.4.1.** *A compact and connected Riemann surface which restricts to a cover over $X^{'}$ as above gives rise to a finite sub extension of $K_{X'}|\mathcal{M}(X)$.*

*Proof.* Proof of Theorem 3.4.1

Every finite field extension $L|\mathcal{M}(X)$ comes from a Riemann surface that restricts to a cover over $X^{'}$ and is Galois over $\mathcal{M}(X)$. Similarly it holds for all the Galois conjugates of $L$ and since the composite of Galois extensions is Galois, then $K_{X'}|\mathcal{M}(X)$ is Galois.

By a result([Sza], corollary 2.3.9) coset spaces of normal subgroups of $\widehat{\pi_1(X', x)}$ correspond to finite Galois covers of $X^{'}$. By Proposition 3.2.3, the finite Galois covers over $X^{'}$ correspond to finite Galois branched covers over $X$ and by Theorem 3.3.2 these finite Galois branched covers correspond to finite Galois extensions of $\mathcal{M}(X)$ which are the sub extension of $K_{X'}|\mathcal{M}(X)$. This gives a bijection between finite quotients of $\widehat{\pi_1(X', x)}$ and $Gal(K_{X'}|\mathcal{M}(X))$. □

**Remark 3.1.** *The Galois group $Gal(\overline{\mathcal{M}(X)}|\mathcal{M}(X))$ is isomorphic to the inverse limit of system of groups $Gal(K_{X'}|\mathcal{M}(X))$ such that for $X^{'} \subset X^{"}$, we have the inclusion $K_{X'} \supset K_{X^{"}}$. This is because finite sub extension fields of closure of $\mathcal{M}(X)$ are precisely $K_{X'}$.*

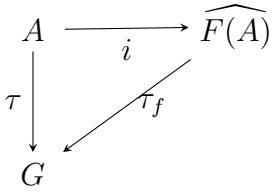
Consider the the complex projective line, $X = \mathbb{C}P^1$ and a finite set of points $x_1, ..., x_n$ in $\mathbb{C}P^1$. The fundamental group of complement of these finite set of points in $\mathbb{C}P^1$ can be presented as follows

$\pi_1(\mathbb{C}P^1 - \{x_1, ...x_n\}, x) =< \gamma_1, \gamma_2....\gamma_n | \gamma_1\gamma_2....\gamma_n = 1 >$ where each $\gamma_i$ is a generator which is a closed path through the point $x$ and is around the points $x_i$. The maps $\gamma_i \mapsto f_i \in F_{n-1}$ and $\gamma_n \mapsto (f_1 f_2 .. f_{n-1})^{-1}$ gives an isomorphism between the above group and the free group $F_{n-1}$ having n-1 generators, here $f_i$ are free generators of the group $F_{n-1}$. So we conclude that every finite group has a finite presentation and it arises as finite quotient of $\pi_1(\mathbb{C}P^1 - \{x_1, ...x_n\}, x)$ and we know that $\mathcal{M}(\mathbb{C}P^1) \cong \mathbb{C}(t)$, we have the following result coming from above theorem:

**Corollary 3.4.1.** *Every finite group arises in correspondence to Galois group of some finite extension $L|\mathbb{C}(t)$*

**Definition 3.4.1.** *Take a set $A$ and let $F(A)$ be the free group having basis $A$. Form the quotients of the free group $F(A)/U$ by the normal subgroups $U$ of the free group having finite index which contains all points of $X$ except some finite points. The inverse limit of this system is called the free profinite group and is denoted by $\widehat{F}(A)$*

We define the inclusion $i : X \to \widehat{F(A)}$ with a universal property that suppose we have a profinite group $G$ and and a mapping $\tau : A \to G$, such that all normal subgroups having a finite index in G and they contain all the points of $\lambda(A)$ except some finite points, then there exists a unique mapping $\tau_F : \widehat{F(A)} \to G$ between profinite groups such that the following diagram commutes




**Theorem 3.4.2.** *There is an isomorphism of profinite groups $Gal(\overline{\mathbb{C}(t)}|\mathbb{C}(t)) \cong \widehat{F(\mathbb{C})}$.*

The proof of the theorem uses the following group-theoretic result:

**Proposition 3.4.1.** *Let $X$ be a set and consider a system of finite subsets denoted by $\mathcal{S}$ where $S \subset X$ and it is given a partial ordering by inclusion. Consider an inverse system of profinite groups $(G_S, \tau_{SR})$ where $\mathcal{S}$ is the indexing set which satisfies:*

*1. The homomorphisms $\tau_{SR}$ are surjective for subsets $S$ of $R$.*

*2.Each profinite group $G_S$ consists of system $z_x : x \in S$ of elements such that the map $\widehat{F(S)} \to G_S$ coming from $x \to z_x$ gives an isomorphism between $\widehat{F(S)}$ and $G_S$ , and also for all subsets $S \subset R$ we have $\lambda_{SR}(z_x) = 1$ for $x \in R - S$.*

*There is an isomorphism between $\varprojlim G_S$ and $\widehat{F}(X)$.*

*Proof.* Let $S$ be a set of points in $C$ which is finite. Denote $\mathbb{C}P^1 - (S \cup \infty)$ by $X_S$. $Gal(K_{X_S}|\mathbb{C}(t))$ is a quotient of the absolute Galois group $Gal(\overline{\mathbb{C}(t)}|\mathbb{C}(t))$ and it is isomorphic to free profinite group generated by $|S|$ generators $\gamma_a$ for each $a \in S$. Now

if we have subset $R$ of $\mathbb{C}$ such that S is subset of R, then we get an inclusion of Galois extensions $K_{X_S} \subset K_{X_R}$ where $X_R = P^1 - (R \cup \infty)$. We have seen in infinite Galois theory that there is a surjection $\tau_{SR} : Gal(K_{X_R}|\mathbb{C}(t)) \to Gal(K_{X_S}|\mathbb{C}(t))$. By Theorem given in the starting of this section, this map is induced by the map of fundamental groups $\pi_1(X_R, x) \to \pi_1(X_S, x)$ for some point $x$. For each $a \in R - S$, $\tau_{SR}(\gamma_a) = 1$. So we get an inverse system where indexing set consists of finite subsets of $\mathbb{C}$. We have seen that every finite sub extension of $\overline{\mathbb{C}(t)}$ lies in $K_{X_S}$ for some suitable subset $S$, so the inverse limit is of above system is $Gal(\overline{\mathbb{C}(t)}|\mathbb{C}(t))$. The theorem follows from above proposition. □

# Bibliography


[DFon] Dummit and Foote, *Abstract algebra*, Third edition.

[For81] Otto Forster, *Lectures on riemann surface*.

[Gar] Paul Garrett, *Notes on riemann sphere*, `www-users.math.umn.edu/~garrett/m/complex/notes_2014.../06_Riemann_sphere.pdf`.

[Lanon] Serge Lang, *Algebra*, Third edition.

[PG78] Joseph Harris Phillip Griffiths, *Principles of algebraic geometry*, 1978.

[Rudon] Walter Rudin, *Real and complex analysis*, Third edition.

[Sza] Tamas Szamuely, *Galois groups and fundamental groups*.