DECK GROUPS, RIEMANN SURFACES, AND A DEEP DIVE INTO THE INVERSE GALOIS CONUNDRUM

Shaunak Bhandarkar, Sidhart Krishnan
Euler Circle
Palo Alto CA 94303, USA
shaunak@gmail.com
sidhartkrishnan@gmail.com

July 13, 2020

ABSTRACT

In this paper, we talk about the Inverse Galois problem, which as the title suggests, is essentially the "opposite" of Galois theory, though significantly harder. We start the paper by exploring a few examples of basic groups, such as $\mathbb{Z}/n\mathbb{Z}$, that can be realized as Galois groups. In particular, we will see that all abelian groups are Galois groups over $\mathbb{Q}$. The next section will explore Hilbertian fields, which allow us to realize Galois groups over $\mathbb{Q}$.

Then, we move on to the Inverse Galois problem over $\mathbb{C}(x)$, devoting a large part of the paper to studying the beautiful yet deep connection between fundamental groups, Deck groups, and Galois groups over fields of meromorphic functions on Riemann surfaces. As a culminating result, we show that any finite group can be realized as a Galois group over $\mathbb{C}(x)$! Finally, we also introduce Riemann's Existence Theorem along with some of the rigidity methods that are central to the study of the Inverse Galois Problem.

***K*eywords** Inverse Galois Theory · Hilbertian Fields · Fundamental Groups · Deck Groups · Riemann Surfaces

1 Introduction to the Inverse Galois Problem

In order to prove that there was no general solution for polynomials of degree 5, Evariste Galois first introduced the idea of the Galois group. If we consider a field extension E/F, then degree is the dimension of E as a vector space over F. We also can define the automorphism group to be the group of automorphisms of E that fix F. However, if F is to be the fixed field of all the automorphisms in $\mathrm{Aut}(E/F)$, then two properties must be satisfied. First, the field extension must be normal, meaning that if a polynomial $f(x) \in F[x]$ has a root in E then all of its roots are in E. Second it must be separable, meaning that every $x \in E$ has a separable minimal polynomial over F (i.e. with distinct roots). If E/F is a Galois extension then we denote $\mathrm{Aut}(E/F)$ by $\mathrm{Gal}(E/F)$. Evidently, we know how to determine whether a field extension is Galois, but we may naturally be inclined to ask ourselves the Inverse Galois Problem: what groups can be represented as a Galois group. Even more specifically, what groups can be realized as Galois groups over $\mathbb{Q}$. This question is much, much harder.

Throughout this paper, we assume knowledge of ordinary Galois theory, algebraic topology, as well as basic Riemann surface theory. The reader is encouraged to see the references at the end of the paper for further reading.

2 Some Motivating Examples

Recall that Galois theory first arose as a method to study the permuting action of field automorphisms that fixed a certain base field. Naturally, it's very interesting that the resulting set of automorphisms has a group structure. Let us investigate some basic examples of this:

1. Any quadratic extension of $\mathbb{Q}$ can be obtained by adjoining a square root to obtain a field extension of the form $\mathbb{Q}(\sqrt{n})$, for some squarefree integer n. Evidently, there are two automorphisms of $\mathbb{Q}(\sqrt{n})$ that remained fixed on $\mathbb{Q}$: the identity and $\sigma : \sqrt{n} \mapsto -\sqrt{n}$. Therefore, $\mathrm{Gal}(\mathbb{Q}(\sqrt{n})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.
2. In general, we may realize the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ by adjoining a primitive nth root of unity to $\mathbb{Q}$. In particular, for primes p, we see that we may realize the group $\mathbb{Z}/p\mathbb{Z}$.
3. Owing to the permuting action of a Galois group, it may naturally be embedded into the symmetric group S_n. However, one may wonder when S_n is actually realizable. As a simple example, one may verify that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$, where ω is a primitive cube root of unity; this follows from the fact that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field for the polynomial $x^3 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$. The Galois group has order 6 and is nonabelian - in other words, it's isomorphic to S_3.
4. In general, S_n is in fact realizable as a Galois group over the function field $\mathbb{C}(x)$ (as we will see, it turns out ALL groups are realizable as Galois groups over $\mathbb{C}(x)$!); the irreducible polynomial $f(x, y) = \frac{y^{n+1}-1}{y-1} - x = y^n + y^{n-1} + \cdots + 1 - x \in \mathbb{C}(x, y)$ produces a field extension with Galois group S_n. However, the reasoning - as we will see later - relies on the mysterious yet beautiful connection between Galois groups and fundamental groups in algebraic topology.

Now, we can prove a minor result pertaining to the Inverse Galois Problem: all finite abelian groups are realizable as some Galois group. To do this, we first establish the following lemma.

Lemma 2.1 (Special Case of Dirichlet's Theorem on Primes in an Arithmetic Progression)**.** *For any integer m there are an infinite number of primes p so that $p \equiv 1 \pmod{m}$.*

Proof. Suppose, for the sake of contradiction, that $p_1, p_2, \ldots, p_k$ are all such primes. Let $m = np_1p_2 \cdots p_k$. Since $\Phi_m(x) \in \mathbb{Z}[x]$ is monic, then $\lim_{x\to\infty} \Phi_m(mx)$ approaches infinity. Hence there exists an t so that $\Phi_m(mt) \geq 2$. Let p be a prime factor of $\Phi_m(mt)$. Then we can see that $p \mid \Phi_m(mk) \mid (mk)^m - 1$. Thus $(mk)^m \equiv 1 \pmod{p}$. We claim that the order of mk is m in the group $\mathbb{F}_p^\times$. Suppose that the order was $r < m$. Then

$$\begin{aligned} x^m - 1 = \prod_{d|m} \Phi_d(x) &= \Phi_m(x) \prod d < m\Phi_d(x) \\ &= \Phi_m(x) \left(\prod_{d|r} \Phi_d(x) \right) h(x) \\ &= \Phi_m(x)(x^r - 1)h(x) \end{aligned}$$

Since $p \mid (mk)^m - 1$, $p \nmid mk \implies \gcd(p, n) = 1$ and $p \neq p_i$ for $1 \leq i \leq k$. Moreover, $\Phi_m(mk) \equiv 0 \pmod{p}$ so $p \equiv 1 \pmod{n}$ which is a contradiction. Thus there are an infinite number of primes that are $1 \pmod{n}$. ■

Theorem 2.2 (Inverse Galois Problem for Finite Abelian Groups)**.** *If G is a finite abelian group, then there is a Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$*

Proof. We first consider $\mathbb{Q}[\zeta_n]$, where $\zeta_n = e^{2\pi i/n}$. We know that $\mathbb{Q}[\zeta_n]$ is Galois over $\mathbb{Q}$ with $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ being given by $\zeta_n \mapsto \zeta_n^a$ for $1 \leq a \leq n$ and $\gcd(a, n) = 1$. Since there are exactly n elements that follow the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$, we have that $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
Note that since $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ is abelian, any subgroup is automatically normal. By the Galois correspondence, any intermediate field K is also normal. If we write $K = \mathbb{Q}[\zeta_n]^H$, then $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})/H$.

Now, we have to use Lemma 2.1. We can write G as a direct product of cyclic groups $G \cong (\mathbb{Z}/a_1\mathbb{Z}) \times (\mathbb{Z}/a_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_r\mathbb{Z})$ where a_i are prime powers. We can find a prime $p_i \equiv 1 \pmod{a_i}$ fore each i. Thus $(\mathbb{Z}/p_i\mathbb{Z}) \cong \mathbb{Z}/(p_i - 1)\mathbb{Z}$ and so $\mathbb{Z}/a_i\mathbb{Z}$ is isomorphic to a quotient of $(\mathbb{Z}/p_i\mathbb{Z})$. This quotient corresponds to some field K_i as we established previously. This completes the proof as we may simply let $K = K_1K_2 \ldots K_r$ be the compositum of these fields, and this is our desired extension of $\mathbb{Q}$. ■

3 Hilbert's Irreducibility Theorem

Before we define Hilbertian Fields we first need to establish some background about regular fields.

Lemma 3.1. *Given a finite Galois extension (an FG-extension) k'/k and $x = (x_1, x_2, \dots x_m)$ then $k'[x]/k[x]$ is an FG-extension and* $\mathrm{Gal}(k'[x]/k[x]) \cong \mathrm{Gal}(k'/k)$.

Proof. Extend the action of G on k' to $k'[x]$ by $g \in G$ then $g(x_i) = x_i$ for $i = 1, 2, \dots, m$. It is clear that G fixes $k[x]$ and thus $k'[x]/k[x]$ is a FG-extension with Galois group G. ■

We can then use the Galois correspondence to conclude that for any intermediate field $k''[x]$, then $[k''[x] : k[x]] = [k'' : k]$.
Now we define the regular field extension as

Definition 3.2. L is said to be regular over k if k is algebraically closed in L. Say L/k is regular.

This leads us into a lemma that allows us to simplify this definition.

Lemma 3.3. *Let $\bar{k}$ be an algebraic closure of k. If $f(x, y) \in k[x][y]$ is an irreducible polynomial over $k[x]$, and if $K = k[x][y]/(f)$ is the corresponding field extension of $k[x]$, then K is regular over k if and only if f is irreducible over $\bar{k}[x]$.*

Proof. Let L be the algebraic closure of k in K so K is regular over k if and only if $L = k$. Let f be an irreducible polynomial over $k[x]$ and let α be a root of f. Then we have a homomorphism $\varphi : k[x][y] \to k[x](\alpha)$ which sends $h(y) \mapsto h(\alpha)$ where $k[x](\alpha) \cong k[x][y]/\ker(\varphi) = k[x][y]/(f) = K$.
Then α satisfies a polynomial $F \in L[x][y]$ of degree $[K : L[x]]$ and $F \mid f$. Then by the tower law $[K : L[x]] = \frac{[K:k[x]]}{[L[x]:k[x]]} \leq [K : k[x]]$. Thus $\deg(F) \leq \deg(f)$.
Therefore if $L = k$ then f is not irreducible over $L[x][y]$ since it is divisible by F and thus it is not irreducible over $\bar{k}[x][y]$.

Now to prove the other direction, we assume that K is regular over k. Then $L = k$. Now let k' be an FG-extension of k and define K' to be the compositum of K and $k'[x]$ in an algebraic closure of $k[x]$. Then by Lemma 3.1, $k'[x]/k[x]$ is an FG-extension. Note that $K \cap k'[x]$ is of the form $k''[x]$ where k'' is an intermediate field.
Since $k'' \subset L = k$ then we get that $k'' = k$ so $K \cap k'[x] = k[x]$. Since $k'[x]/k[x]$ is Galois, it follows that $[K' : k'[x]] = [K : k[x]]$. Thus f is irreducible over $\bar{k}[x]$. ■

Now we can define a hilbertian field.

Definition 3.4. A field k is called hilbertian if for each irreducible polynomial $f(x, y) \in k[x, y]$ with $deg(f) \geq 1$ there are infinitely many $b \in k$ such that $f(b, y) \in k[y]$ is irreducible. The polynomial $f_b(y) = f(b, y)$ is called a specialization.

A key property of hilbertian fields that will not be proven in this paper is:

Proposition 3.5. *For any $p_1(x, y), \dots p_t(x, y) \in k[x][y]$ that are irreducible and of degree greater than 1 when viewed as a polynomial in y over $k[x]$, there are infinitely many $b \in k$ such that none of the specialized polynomials $p_1(b, y), \dots p_t(b, y)$ has a root in k.*

Another lemma we need before we establish Hilbert's Irreduciblity theorem is:

Lemma 3.6. *Let α be algebraic over a field K. If $f(x) = \sum_{i=0}^{n} a_i x^i$ is a polyomial over K of degree $n > 0$ with $f(\alpha) = 0$, then $g(y) = y^n + \sum_{i=0}^{n-1} a_i a_n^{n-i-1} y^i$ is a monic polynomial of degree n where $g(a_n\alpha) = 0$. This implies that $K[\alpha] = K[a_n\alpha]$.*

Proof. Just plug in $y = a_n\alpha$. Then

$$g(a_n\alpha) = a_n^{n-1} \left(\sum_{i=0}^{n} a_i \alpha^i \right) = 0$$

■

Thus we can conclude that if $f(x, y) \in K[x, y]$ is a separable polynomial in y over $K[y]$. Then we may assume that f is monic in y. Its discriminant is of the form $D(x) \in K[x]$ and is nonzero because f is separable in y. For each $b \in K$, the polynomial $f(b, y) \in K[y]$ has a discriminant $D(b)$. Thus $f(b, y)$ is separable for all $b \in L$ that do not make $D(b) = 0$.
Now we have to introduce the notion of a sparse set.

Definition 3.7. Let $M \subset \mathbb{N}$. We say M is sparse if there is a real number κ with $0 < \kappa < 1$ such that

$$|M \cap 1, 2, \dots, N| \leq N^{\kappa}$$

for all but finitely many N.

We can see that a finite set is sparse and all finite unions of sparse sets are still sparse. Now we can introduce a key theorem about these sparse sets.

Theorem 3.8. *Let $i_0 \in \mathbb{Z}$ and let $\phi(t) = \sum_{i=i_0}^{\infty} a_i t^i$ be a Laurent series with complex coefficients, converging for all $t \neq 0$ in a neighborhood of 0 in $\mathbb{C}$. Let $B(\phi)$ be the set of all $b \in \mathbb{N}$ for which $\phi(1/b)$ is an integer. Then $B(\phi)$ is a sparse set unless ϕ is a Laurent polynomial meaning that all but a finite number of the a_i's vanish.*

Before we jump into the proof of this theorem we have to establish a lemma concerning the Vandermonde determinant.

Lemma 3.9. *Let $s_0 < s_1 < \cdots < s_m$ be real numbers with $m \geq 1$. Let $\chi(s)$ be a real-valued function defined for $s_0 \leq s \leq s_m$. It is also m times continuously differentiable. Let V_m be the Vandermonde determinant defined as*

$$V_m = \begin{vmatrix} 1 & s_0 & s_0^2 & \cdots & s_0^m \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & s_m & s_m^2 & \cdots & s_m^m \end{vmatrix} = \prod_{i>j}(s_i - s_j)$$

Then there exists a number σ with $s_0 < \sigma < s_m$ such that

$$\frac{\chi^{(m)}(\sigma)}{m!} = \frac{1}{V_m} \begin{vmatrix} 1 & s_0 & \cdots & s_0^{m-1} & \chi(s_0) \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & s_m & \cdots & s_m^{m-1} & \chi(s_m) \end{vmatrix}$$

Proof. Let $F(s)$ be the function

$$F(s) = \begin{vmatrix} 1 & s_0 & \cdots & s_0^{m-1} & \chi(s_0) \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & s_{m-1} & \cdots s_{m-1}^{m-1} & \chi(s_{m-1}) & \\ 1 & s & \cdots & s^{m-1} & \chi(s) \end{vmatrix}$$

and set $c = \frac{F(s_m)}{(s_m - s_0)(s_m - s_1)\dots(s_m - s_{m-1})}$. Finally we can define $G(s) = F(s) - c(s - s_0)(s - s_1)\dots(s - s_{m-1})$. The function $G(s)$ vanishes at the points $s = s_0, s_1, \dots s_m$. Hence $G^{(m)}(s)$ vanishes at least at one point σ between s_0 and s_m. Since $G^{(m)}(s) = F^{(m)}(s) - m!c$ we get $F^{(m)}(\sigma) = m!c$.
Now if we expand $F(s)$ we get

$$\sum_{i=0}^{m-1} c_i s^i + V_{m-1}\chi(s)$$

where the c_i are constants that depend on $s_0, s_1, \dots s_m$ and V_{m-1} is the Vandermonde determinant of $s_0, s_1, \dots s_{m-1}$. Thus we get $F^{(m)}(\sigma) = V_{m-1}\chi^{(m)}(\sigma)$. Comparing the two expressions for $F^{(m)}(\sigma)$, we get:

$$\frac{\chi^{(m)}(\sigma)}{m!} = \frac{c}{V_{m-1}} = \frac{F(s_m)}{(s_m - s_0)\cdots(s_m - s_{m-1})V_{m-1}} = \frac{F(s_m)}{V_m}$$

This proves the lemma since σ satisfies the requirements in the lemma. ■

Now we can go on to the proof of Theorem 3.8

Proof. First we have to prove that all of the a_i's are real. To do this we must notice that the series $\bar{\phi} = \sum_{i=i_0}^{\infty} \bar{a}_i t^i$ has the same radius of convergence as ϕ. We also have that $\bar{\phi}(1/b) = \phi(1/b)$ for $b \in B(\phi)$. Since $B(\phi)$ is infinite, it follows that $\bar{\phi} = \phi$ which proves this claim.
From this claim we also see that the function $\chi(s) = \phi(1/s)$ is a real-valued function that is defined for large values of s. We claim that there is a $\lambda > 0$ and $m, S \in \mathbb{N}$ such that whenever $s_0, s_1, \dots s_m \in \mathbb{Z}$ with $\chi(s_0), \chi(s_1), \dots \chi(s_m) \in \mathbb{Z}$ and $S < s_0 < s_1, \cdots s_m$ then $s_m - s_0 \geq s_0^{\lambda}$. To prove this claim, we must note that for sufficiently large m, the series $\chi^{(m)}(s) = \sum_{i=\mu}^{\infty} d_i s^{-1}$ has only terms with negative powers of s. Here the d_i's are real numbers and since ϕ is not a

Laurent polynomial, $d_\mu \neq 0$. Thus $s^\mu \chi^{(m)}(s)$ tends towards d_μ as s goes to infinity. Thus there is an $S > 0$ so that $0 < |s^\mu \chi^{(m)}(s)| < |2d_\mu|$ for $s \geq S$. Now we can apply Lemma 3.9 to choose a σ. Then $\frac{V_m(\chi^{(m)}(\sigma)}{m!}$ is a nonzero integer and thus has an absolute value which is greater than or equal to 1. Thus. $V_m \geq \frac{1}{\chi^{(m)}(\sigma)}$ and so

$$(s_m - s_0)^{(m+1)(m+2)/2} \geq V_m \geq \frac{1}{\chi^{(m)}(\sigma)} \geq \frac{\sigma^\mu}{|2d_\mu|} \geq \frac{s_0^\mu}{|2d_\mu|}$$

This gives us $s_m - s_0 \geq \frac{\sigma^\mu}{|2d_\mu|}\Big)^{2/((m+1)(m+2))}$ so any $\lambda \geq 2\mu/((m+1)(m+2))$ satisfies this claim.
The third claim we need to complete this proof is that if $b_1 < b_2 < \cdots$ is an infinite sequence of positive integers with $b_{i+1} - b_i \geq b_i^\lambda$ for some $\lambda > 0$. Then the set $B = \{b_1, b_2, \dots\}$ is sparse. To see this we say that for each positive integer N, we let N' be the number of $b \in B$ with $\sqrt{N} < b \leq N$. Then $(N' - 1)(\sqrt{N})^\lambda \leq N$ and hence $N' - 1 \leq N^{1-\frac{\lambda}{2}}$. Thus $|B \cap 1, 2, \dots, N|$ is bounded by $\sqrt{N} + N' \leq \sqrt{N} + N^{1-\frac{\lambda}{2}}$ so B is sparse.
These claims help us prove the assertion that $B(\phi)$ is sparse. Since $B(\phi)$ consists of all integers b where $\chi(b) = \phi(1/b)$ is an integer, we can delete all integers less than or equal to S from $B(\phi)$ where S is defined in the same way as it in the second claim. Then the remaining set can be written as the union of m subsets of B each of which satisfies the condition for the third claim. Thus each of those sets are sparse and since a finite union of sparse sets is sparse, we are done. ■

Now we have to shift our focus to discuss the following theorem.

Theorem 3.10. *Let $f(x, y) \in \mathbb{C}[x, y]$ be of degree $n \geq 1$ in y. Let $c_0 \in \mathbb{C}$ be such that $f(c_0, y) \in \mathbb{C}[y]$ is separable of degree n. Then there exist holomorphic functions $\psi_1, \psi_2, \dots \psi_n$ defined in a neighborhood U of c_0 such that for each $c \in U$, the polynomial $f(c, y)$ has the distinct roots $\psi_1(c), \psi_2(c), \dots, \psi_n(c)$.*

While there are many proofs of this theorem, we will focus on an algebraic approach that requires less high-powered machinery.

Proof. It suffcies to show that for each root γ of $f(c_0, y)$ there is a holomorphic function ψ defined around c_0 with $\psi(c_0) = \gamma$ and $f(c, \psi(c)) = 0$ for all c close to c_0. As long as c is close enough to c_0, the values of these n ψ functions will be distinct and thus comprise of all roots of $f(c, y)$.
Replacing x by $x - c_0$ and y by $y - \gamma$ will result in the same problem so we may assume that $c_0 = \gamma = 0$. Thus we have to find a holomorphic function ψ with $\psi(0) = 0$ and $f(t, \psi(t)) = 0$ for all t sufficiently close to 0. If we consider the Taylor expansion of ψ we get $\psi(t) = \sum_{i=1}^\infty a_i t^i$ around 0. Since $f(0, 0) = 0$ we can say that $f(x, y) = ax + by +$ some higher order terms. Then $b = (\partial f/\partial y)(0, 0) \neq 0$. Since we can just divide by b, we may assume that $b = 1$. Then if we define $g(x, y) = y - f(x, y)$ so that g has no constant y term. Now the condition that $f(t, \psi(t)) = 0$ is equivalent to

$$\psi(t) = g(t, \psi(t)) \tag{3.1}$$

So now we can compute the coefficients a_i of ψ recursively, if we develop the right-hand side of 3.1 into a power series around 0. Indeed the t^i-th coefficient on the right hand side involves only a_j where $j < i$ and the coefficients of g. After completing the recursion a_i appears as a polynomial with non-negative integer coefficients comprised of coefficients of g. Note that only for the coefficients of g, only the $x^r y^s$ with $r + s \leq i$ occur. The coefficients a_i yield the unique power series $\psi(t) = \sum_{i=1}^\infty a_i t^i$ that solves Equation 3.1. It remains to see that this power series has a positive radius of convergence. Let C be a positive constant bounding the absolutely value of the coefficients of g. Consider the function

$$h(t, u) = C\left(-1 - u + \frac{1}{(1-t)(1-u)}\right)$$

Solving the quadratic equation $u = h(t, u)$ for u in terms of t, we get that

$$\Psi(t) = \frac{1}{2(C+1)}\left(1 - \frac{\sqrt{1 - t(1 + (1+2C)^2) + t^2(1 + (1+2C)^2)}}{1-t}\right)$$

is the unique holomorphic function defined around 0 with $\Psi(0) = 0$ and $\Psi(t) = h(t, \Psi(t))$. Here we say that $\sqrt{(}1) = 1$. The geometric series formula yields that

$$h(t, u) = C(t + t^2 + tu + u^2 + \cdots) = C\left(-1 - u + \sum_{r,s=0}^\infty t^r u^s\right)$$

for $|t| < 1, |u| < 1$. From this and the equation $\Psi(t) = h(t, \Psi(t))$, we see that the Taylor coefficients b_i of Ψ are obtained using the same polynomials as we did for the a_i's now applied to the coefficients of h which are all equal to C. Since C bounds the absolute value of the coefficients of g, it follows that $|a_i| \leq b_i$ for all i. But the Taylor series $\sum_{i=0}^{\infty} b_i t^i$ of Ψ has a positive radius of convergence and hence the same holds for $\psi(t) = \sum_{i=0}^{\infty} a_i t^i$ which proves the theorem. ■

The last lemma we need before we go into the proof of Hilbert's Irreducibility theorem is this one:

Lemma 3.11. *Let $p(x, y) \in \mathbb{Q}[x][y]$ be irreducible over $\mathbb{Q}[x]$ and of degree $r > 1$ in y. Then for $x_0 \in \mathbb{Z}$ we let $B(p, x_0)$ be the set of all $b \in \mathbb{N}$ such that $p(x_0 + \frac{1}{b}, c) = 0$ for some $c \in \mathbb{Q}$. Then for all but finitely many $x_0 \in \mathbb{Z}$, $B(p, x_0)$ is sparse.*

Proof. Note that since p is irreducible and thus separable over $\mathbb{Q}[x]$, $p(x_0, y)$ is separable for all but finitely many $x_0 \in \mathbb{Z}$ by Lemma 3.6. Thus we will only consider those x_0's to prove this lemma. We also may assume that $p(x, y) \in \mathbb{Z}[x, y]$. Write $p(x, y) = \sum_{i=0}^{r} p_i(x) y^i$ with $p_i(x) \in \mathbb{Z}[x]$. For suitably large R the expression

$$x^R p\left(x_0 + \frac{1}{x}, y\right) = \sum_{i=0}^{r} x^R p_i\left(x_0 + \frac{1}{x}\right) y^i$$

is an element of $\mathbb{Z}[x, y]$. Let $p_i'(x) = x^R p_i\left(x_0 + \frac{1}{x}\right)$. Then $p_r'(x)$ is a nonzero element of $\mathbb{Z}$. Using Lemma 3.6, we get that the polynomial

$$q(x, z) = z^r + \sum_{i=0}^{r-1} p_i'(x) p_r'(x)^{r-i-1} z^i$$

is an element of $\mathbb{Z}[x, z]$ and is monic. Suppose then that $p(x_0 + \frac{1}{b}, c) = 0$ for $c \in \mathbb{Q}, b \in ZZ$. Then $q(b, p_r'(b)c) = 0$ and since $q(b, z)$ is a monic polynomial in $\mathbb{Z}[z]$, it follows that $p_r'(b)c$ is integral over $\mathbb{Z}$. Thus $p_r'(b)c \in \mathbb{Z}$ since it lies in $\mathbb{Q}$.

Now if additionally, $|1/b| = \epsilon$, then $c = \psi_i(1/b)$ for $i = 1, 2, \dots, r$ which we know exist by Theorem 3.10. Thus $h(b)\psi_i(1/b) = h(b)c \in \mathbb{Z}$. Set $\phi_i(t) = h(t^{-1})\psi_i(t)$ for $0 < |t| < \epsilon, i = 1, 2, \dots, r$. The above shows that if $b \in B(p, x_0)$ and $1/b < \epsilon$ then $\phi_i(1/b) = h(b)\psi_i(1/b) \in \mathbb{Z}$ for some $i = 1, \dots, r$. Thus, up to a finite set, $B(p, x_0)$ lies in the union of the sets $B(\phi_i)$. By Theorem 3.8, the set $B(\phi_i)$ is sparse if ϕ_i is not a rational function.

However, if ϕ_i is rational then, then we can show that $B(\phi_i)$ is finite. Then $p(x_0 + t, \phi_i(t))$ is identically zero. Thus $p(x_0 + x, \phi_i(x)) = 0$ in $\mathbb{C}[x]$ if x is a transcendental element over $\mathbb{C}$. Then $\phi_i(x)$ is algebraic over $\mathbb{Q}[x]$ and hence it is also algebraic over $\bar{\mathbb{Q}}[x]$. But we also note that since $\bar{\mathbb{Q}}[x]$ is algebraically closed over $\mathbb{C}[x]$ (which we can show by Lemma 3.3), it follows that $\phi_i(x) \in \bar{\mathbb{Q}}[x]$. For each $\beta \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we can consider the rational function ϕ^β obtained by applying β to all of the coefficients of ϕ_i. Then $\phi^\beta(q) = \phi_i(q)$ for all $q \in \mathbb{Q}$ with $\phi_i(q) \in \mathbb{Q}$. If there are infinitely many such q, it follows that $\phi^\beta = \phi_i$ for all β and hence ϕ has rational coefficients. Then $\phi(x - x_0) \in \mathbb{Q}[x]$ is a zero of $p(x, y)$ over $\mathbb{Q}[x]$. This contradicts the fact that p is irreducible over $\mathbb{Q}[x]$ and thus $B(\phi_i)$ is finite.

Finally, since $B(p, x_0)$ is a union of $B(\phi_i)$ which are all sparse, then $B(p, x_0)$ is also sparse which proves the lemma. ■

Thus now we have all of the tools we need to prove Hilbert's Irreducibility Theorem.

Theorem 3.12. *The field $\mathbb{Q}$ is hilbertian.*

Proof. Given polynomials $p_i(x, y) \in \mathbb{Q}[x][y]$ as in the hypothesis of proposition 3.5, we can choose $x_0 \in \mathbb{Z}$ that satisfies Lemma 3.11 for all p_i. Let C be the set of $b \in \mathbb{N}$ such that none of the specialized polynomials $p_i(x_0 + \frac{1}{b}, y)$ has a root in $\mathbb{Q}$. Set $B = \mathbb{N}\ C$. Then B is the union of $B(p_i, x_0)$ which are all sparse by Lemma 3.11. Thus B is sparse meaning that its complement C is infinite which gives us the infinite b's to satisfy the defintion of a hilbertian field. Thus $\mathbb{Q}$ is hilbertian. ■

This theorem, alongside Riemann's existence theorem, is critical to establishing the concept of rigidity and its application to the Inverse Galois Problem. Specifically, we will use Hilbert's Irreducibility Theorem to establish the General Rigidity Criterion.

We finish this section by using Hilbert's Irreducibility Theorem to prove that the symmetric group S_n is realizable over $\mathbb{Q}$.

To do this we will prove that S_n is realizable over any hilbertian field k. Consider the polynomial $f(y) \in k[x_1, x_2, \dots x_n][y]$ defined by $f(y) = y^n + x_1 y^{n-1} + \cdots + x_n$ and let $a_1, a_2, \dots a_n$ be the roots of

$f(y)$. Then S_n acts naturally on the roots where if $\sigma \in S_n$, then $\sigma : (a_1, a_2, \ldots a_n) \mapsto (a_{\sigma(1)}, \ldots, a_{\sigma(n)}$. This actions extends to an automorphism $\tau : k[a_1, a_2, \ldots a_n] \to k[a_1, a_2, \ldots a_n]$. In this way we have constructed an action on $k[a_1, a_2, \ldots a_n]$. Consider a fixed field F of this action in $k[a_1, a_2, \ldots a_n]$. Then F contains $k[x_1, x_2, \ldots x_n]$ and further , $k(a_1, a_2, \ldots a_n) : F] = |S_n| = n!$. But since $a_1, a_2, \ldots a_n$ are the roots of a polynomial of degree n over $k[x_1, x_2, \ldots x_n]$ it follows that $[k[a_1, a_2, \ldots a_n] : k[x_1, x_2, \ldots x_n]] \leq n!$. Thus, $F = k[x_1, x_2, \ldots x_n]$ so we can apply Artin's Thoerem which states that if G is a finite group of automorphisms on a field E and the fixed field of E is K then E/K is a finite Galois extension with $\mathrm{Gal}(E/K) = G$. This tells us that

$$\mathrm{Gal}(k[a_1, a_2, \ldots a_n]/k[x_1, x_2, \ldots x_n]) = S_n$$

which shows that S_n occurs regularly over k. Thus if k is Hilbertian then S_n is realizable as a Galois group over k and hence over $\mathbb{Q}$.

4 A Beautiful Connection to Algebraic Topology

When first confronted with the Inverse Galois Problem, one may consider trying to analyze certain groups and how they can be realized as Galois groups. Perhaps, we could look at some naturally occurring groups, and then see if we can somehow establish a connection with Galois theory...

That's exactly what happens in algebraic topology! Recall that for a path-connected space X, the fundamental group $\pi_1(X, x)$ with respect to a base point $x \in X$ is the set of all homotopy classes of loops in X originating at x. It turns out that fundamental groups bear a strong resemblance to Galois groups.

Before we do that, we first briefly review covering spaces. For our purposes, we'll assume that all topological spaces that we introduce are path-connected and omit certain proofs in this section.

Definition 4.1. Let X' and X be two topological spaces. We say that X' is a covering space of X if there exists a map $f : X' \to X$ such that f is a continuous surjective map, and for any open neighborhood $U \subset X$, $f^{-1}(U)$ is a union of (finitely or countably many) disjoint neighborhoods $U_1, U_2, \cdots$ such that for each U_i, $f|_{U_i}$ is a homeomorphism onto U.

Suppose for a given point $x \in X$, its preimage under the covering map is $\{y_1, y_2, ...\}$. Evidently, we may project any curve in X' down to a curve in X. However, given any curve C in X that originates at $x \in X$, we may lift C to a unique curve C' in X' that originates at some y_i. Indeed, for the part of C within some neighborhood of x, we have an isomorphic copy of this curve within the corresponding neighborhood of y_i. Then, we can construct a neighborhood around some x_1 which encompasses the next part of the curve, and see that this uniquely determines the next part of the curve C' in the preimage. Continuing in this manner, we may just "glue" all these open neighborhoods together to obtain a unique curve C' in X' starting at y_i and that is a lift of C. Moreover, we can say the following:

Proposition 4.2. *If two curves C_1 and C_2 in X are homotopic, then any lifts of C_1 and C_2 in X' beginning at the same point are also homotopic.*

Corollary 4.3. *The covering map $f : X' \to X$ induces the inclusion homomorphism*

$$f_* : \pi_1(X', y) \to \pi_1(X, x)$$

where y is any one of the points in the preimage of x under f.

Proof. Indeed, if some curve $f_*(\gamma') = 1$ (where 1 represents the identity loop), then for any representative C' of the class γ', $f(C') = C$ is null-homotopic. Thus, by our proposition, any lift of C is also null-homotopic, i.e., $\gamma' = 1$. Since kernel of f_* is trivial, the map is injective. ■

Now, something interesting is going on here. Suppose we have a point $x \in X$ and $y_1, y_2, ...$ in X'. Then, clearly $x = f(y_1) = f(y_2) = ...$ and each curve originating at x has unique lifts originating at the y_i's. We call such lifts conjugate.

Definition 4.4. Let C' be a curve in X'. Then the number of curves conjugate to C' in X', if finite, is called the degree of the covering, $\deg(f)$. Moreover, the covering $f : X' \to X$ is called a Galois covering if every conjugate of a loop in X' is again a loop.

Definition 4.5. A homeomorphism σ from X' to itself is said to be a covering transformation if $f(\sigma(y)) = f(y)$ for all $y \in X'$. One can see that the set of all covering transformations of X' over X form a group, which is called the covering transformation group (or the Deck group), denoted by $\Gamma(X' \xrightarrow{f} X)$.

Proposition 4.6. *The action of a covering transformation $\sigma \in \Gamma(X' \xrightarrow{f} X)$ is completely determined by its action on a single point of X'.*

Proof. Indeed, suppose $\sigma(P_1) = P_2$ for some $P_1, P_2 \in X'$. Then, take an arbitrary point $Q \in X'$. Then, let C_1 be a curve from P_1 to Q. This implies that under σ, C_1 is taken to a unique curve C_2 that originates at P_2. This means the endpoint of C_2 is uniquely determined, and since Q was arbitrary, we see that the action of σ on P_1 completely determines the covering transformation. ■

This allows us to formulate the following result:

Theorem 4.7. *Suppose $f : X' \to X$ is Galois. Let P_1 be a point in X' and let $\{P_1, P_2, ...\}$ be the set of points conjugate to P_1. Then,*

$$\Gamma(X' \xrightarrow{f} X) = \{\sigma(P_1 \mapsto P_1), \sigma(P_1 \mapsto P_2), ...\}$$

where $\sigma(P_1 \mapsto P_i)$ denotes the unique covering transformation that sends P_1 to P_i.

In particular, a Galois covering is transitive. Also, if P_1 has finitely many conjugates, then the order of the Deck group is just $\deg(f)$. Now, we come to the crucial theorem connecting the fundamental group with the Deck group:

Theorem 4.8. *If $f : X' \to X$ is a Galois covering, then $f_*(\pi_1(X', x'))$ is a normal subgroup of $\pi_1(X, x)$, which gives us the group isomorphism*

$$\pi_1(X, x)/f_*(\pi_1(X', x')) \cong \Gamma(X' \xrightarrow{f} X).$$

In particular, if we take the universal covering space $\tilde{X}$ of X (which is simply connected), we see that

$$\pi_1(X, x) \cong \Gamma(\tilde{X} \xrightarrow{f} X).$$

Now, it is possible for different coverings of X to correspond to the same subgroup of $\pi_1(X, x)$. However, in this case, it is left to the reader to show that we may construct a homeomorphism between these two spaces that commutes with their covering operation on X. Namely, if f_1 is a covering $X_1 \to X$ and f_2 is a covering $X_2 \to X$, then there exists a homeomorphism $g : X_1 \to X_2$ such that $f_1 = f_2 \circ g$ and that sends the base point of X_1 to that of X_2. Such coverings X_1 and X_2 are said to belong to the same covering class, denoted by (X', x'), where X' is a representative of the class and $x' \in X'$ is a base point.

This brings us to the elegant Galois correspondence of covering spaces:

Theorem 4.9. *There is a one-to-one correspondence between all covering classes of (X, x) (lying between (X, x) and the universal covering class $(\tilde{X}, \tilde{x})$) and all subgroups of $\pi_1(X, x)$ given by*

$$[(X', x') \xrightarrow{f} (X, x)] \Longleftrightarrow \Gamma' = f_*(\pi_1(X', x')).$$

In particular, the universal covering space $\tilde{X}$ corresponds to $\Gamma' = 1$.

Moreover, suppose Γ' is a subgroup of $\pi_1(X, x)$; clearly, $\Gamma = f_*(\pi_1(X', x'))$ for some covering space X' of X. Then, Γ' is a normal subgroup of $\pi_1(X, x)$ if and only if $(X', x') \xrightarrow{f} (X, x)$ is a Galois covering. In this case, we have the isomorphism

$$\pi_1(X, x)/\Gamma' \cong \Gamma(D' \xrightarrow{f} D).$$

5 Some Riemann Surfaces Added to the Mix

Okay, so at this point, it seems like we can make some Galois groups out of fundamental groups. In particular, if we look at the Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, and remove some finite set of points $\{p_1, p_2, ..., p_n\}$, the fundamental group of the resulting topological space $\hat{\mathbb{C}}$
$\{p_1, p_2, ..., p_n\}$ with respect to any given base point is the free group on $n - 1$ generators, $F_{n-1} = \underbrace{\mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}}_{n-1 \text{ times}}$.

What's so special about this group is that any finite group G on $n - 1$ generators $\{g_1, g_2, ..., g_{n-1}\}$ can be written as a quotient of F_{n-1} via the canonical homomorphism

$$\phi : F_{n-1} \to G$$

that sends each generator of F_{n-1} to a corresponding generator of G.

Therefore, if we could express fundamental groups as Galois groups somehow, then via the Galois correspondence, we'd be able to realize any quotient of the fundamental group of the Riemann sphere with n punctures for any $n \in \mathbb{Z}_+$, and thus any finite group!

Our remaining link arises from the study of Riemann surfaces - complex topological spaces with additional structure.

Definition 5.1. Recall that a Riemann surface is a Hausdorff topological space with complex an equivalence class of complex atlases, i.e., a class of open coverings $U = \bigcup_i U_i$ together with maps $f_i : U_i \to \mathbb{C}$ such that for any i, j, $f_j \circ f_i^{-1} : f_i(U_i \cap U_j) \to \mathbb{C}$ is holomorphic.

Definition 5.2. For two Riemann surfaces, X and Y, a holomorphic map $\phi : Y \to X$ is a continuous map with the additional structure that for any open subsets $U \subset X$, $V \subset Y$ with $\phi(U) \subset V$ and complex charts $f : U \to \mathbb{C}$, $g : V \to \mathbb{C}$, the function $f \circ \phi \circ g^{-1} : g(V) \to \mathbb{C}$ is holomorphic.

It turns out that, locally, a map between Riemann surfaces resembles an nth power map:

Proposition 5.3. *For any map of Riemann surfaces $\phi : Y \to X$, let $x = \phi(y)$ be the image of some point $y \in Y$. There exist open sets U_x around x and V_y around y with complex charts $f : U_x \to \mathbb{C}$ and $g : V_y \to \mathbb{C}$ such that the local coordinate map $h := f^{-1} \circ \phi \circ g : V_y \to U_x$ is given by either $h(z) = 0$ or $h(z) = z^e$ for some positive integer e that does not depend on the choice of the complex charts.*

We omit this proof, but remark that e is special because it's known as the ramification index (or branching order) of ϕ at y; y is known as a branch point. Moreover, from this proposition, it follows that any holomorphic map between Riemann surfaces is open since a map of the form $z \mapsto z^e$ is clearly open. Essentially, we have characterized what maps between Riemann surfaces look like at a local level.

Corollary 5.4. *The preimage of a point $x \in X$ under ϕ (from the previous proposition) forms a discrete set. Furthermore, if we let S_ϕ be the set of branch points of the map from the previous proposition, then S_ϕ is a discrete set. In particular, if Y is compact, then S_ϕ is finite.*

Proof. Consider a point $q \in \phi^{-1}(x)$. By our proposition, we may choose a neighborhood small enough around q so that the map locally resembles $z \mapsto z^e$, for some $e \in \mathbb{Z}_+$. Such an open map is indeed discrete. The same idea can be applied to show that S_ϕ is a discrete set. Moreover, if Y is compact, then $S_\phi \subset Y$ is a closed subset of a compact set, and hence compact as well. Any compact discrete set is clearly finite, so we're done. ■

We now restrict our attention to proper maps, namely maps between Riemann surfaces for which the preimage of every compact set is also compact. Observe that for proper maps between locally compact surfaces (such as Riemann surfaces), these maps are also closed.

Theorem 5.5. *If X is a connected Riemann surface and $\phi : Y \to X$ is a proper holomorphic map between Riemann surfaces, then the map is surjective with finite fibres. Additionally, the restriction*

$$Y \setminus \phi^{-1}(\phi(S_\phi)) \to X \setminus \phi(S_\phi)$$

is a finite topological cover.

Proof. Since $\phi(Y)$ is open in X (because ϕ is an open map) and is also closed (since ϕ is proper), we see that $\phi(Y) = X$ since X is connected. Next, finiteness of fibres follows from the fact that any $x \in X$ forms a compact set (namely the singleton set), and so its preimage is compact and discrete, hence finite. Thus, we see that

$$\phi' : Y \setminus \phi^{-1}(\phi(S_\phi)) \to X \setminus \phi(S_\phi)$$

is a covering map because we have removed all the branched points; therefore, each neighborhood of some (unbranched) point in the preimage of some $x \in X \setminus \phi(S_\phi)$ maps homeomorphically to a neighborhood of x in $X \setminus \phi(S_\phi)$. In fact, for any $x_1, x_2 \in X \setminus \phi(S_\phi)$, $\phi'^{-1}(x_1)$ and $\phi'^{-1}(x_2)$ have the same cardinality, since each path from x_1 to x_2 uniquely lifts to a path that begins at some point of $\phi'^{-1}(x_1)$ and ends at a unique point of $\phi'^{-1}(x_2)$. Thus, ϕ' is a finite-sheeted covering. ■

Now, we can extend this idea a bit further:

Proposition 5.6. *Given a proper (nonconstant) holomorphic map $\phi : Y \to X$, there exists some positive integer n such that ϕ attains each value $y \in Y$ exactly n times, counting multiplicity due to branch points.*

Proof. Let n be the number of sheets in the unbranched covering

$$\phi' : Y \setminus \phi^{-1}(\phi(S_\phi)) \to X \setminus \phi(S_\phi).$$

If we have $s \in \phi(S_\phi)$, then suppose $\phi^{-1}(s) = \{r_1, r_2, ..., r_m\}$. Also, let e_i denote the branching order of r_i under f. Then, there is some neighborhood U_i of r_i and V_i of s so that every $t \in V_i \setminus s$ has e_i preimage points in U_i. Thus, we may take some neighborhood $V \subset V_1 \cap \cdots \cap V_m$ of s for which $\phi^{-1}(V) \in U_1 \cup \cdots \cup U_m$, meaning that for each $t \in V \setminus s$ (which must be unbranched), $\phi^{-1}(t)$ consists of $e_1 + ... + e_m$ distinct points. Therefore, ϕ attains each point in X $n = e_1 + ... + e_m$ times, which is the sum of all the branching orders. ■

Corollary 5.7. *On any compact Riemann surface Y, a meromorphic function $f : Y \to \hat{\mathbb{C}}$ has the same number of zeroes as poles, counting multiplicity.*

6 Return of the Galois Group

Now, we connect Riemann surfaces with field theory.

Definition 6.1. Let X be a Riemann surface. A function f is said to be a meromorphic function on X if it's a holomorphic function on $X \setminus S$, for some discrete closed subset $S \subset X$, with the additional condition that for any complex chart $g : U \to \mathbb{C}$, the complex function $f \circ g^{-1} : g(U) \to \mathbb{C}$ is meromorphic (in the usual sense).

In fact, the set of all meromorphic functions on X form a field, denoted by $\mathcal{M}(X)$. Clearly, any sum or product of meromorphic functions on X is also meromorphic. Showing that the multiplicative inverse of any $f \in \mathcal{M}(X)$ is also in $\mathcal{M}(X)$ is slightly harder, but it amounts to showing that the poles of $\frac{1}{f}$ form a discrete closed set, or equivalently that the zeroes of f form a discrete closed set (this follows readily using the Identity Principle of Complex Analysis).

Now, we introduce the elementary symmetric functions on Riemann surfaces. Suppose we have an unbranched holomorphic n-sheeted covering of Riemann surfaces $\psi : Y' \to X'$, and let f be a meromorphic function on Y'. For any $x \in X'$, there is a neighborhood U of x for which $\psi^{-1}(U) = V_1 \cup ... \cup V_n$ is a disjoint union of homeomorphic neighborhoods in Y'. Now, let $\tau_i : U \to V_i$ be the inverse mapping of U homeomorphically to V_i. Then, we may define a function $f_i := \tau_i^* f = f \circ \tau_i$. Then, if we let t be an indeterminate variable, and consider the polynomial

$$\prod_{i=1}^{n}(t - f_i) = t^n + c_1 t^{n-1} + ... + c_n$$

we see that $c_i = (-1)^i s_i(f_1, f_2, ..., f_n)$, where s_i denotes the ith elementary symmetric function in n variables. Since the construction of the c_i is the same across any neighborhood U in X', we may "glue" each local c_i to obtain global meromorphic functions $c_1, ..., c_n$ on $\mathcal{M}(X)$.

Definition 6.2. The c_i above are called the elementary symmetric functions with respect to the covering $\psi : Y' \to X'$.

Now, we aim to find a connection between the fields of meromorphic functions on our Riemann surfaces:

Proposition 6.3. *Let $\phi : Y \to X$ be an n-sheeted branched holomorphic covering map. Suppose $A \subset X$ is a discrete closed subset that contains the image of S_ϕ, and let $B = \phi^{-1}(A) \subset Y$. If f is a meromorphic function on $Y \setminus B$, then f can be meromorphically continued to Y if and only if each of $c_1, ..., c_n \in \mathcal{M}(X \setminus A)$ can be meromorphically continued to X.*

Now, observe that a nonconstant holomorphic map $\phi : Y \to X$ between Riemann surfaces induces a map $\phi_* : \mathcal{M}(X) \to \mathcal{M}(Y)$ given by $\phi_*(f) = f \circ \phi$ (in the language of category theory, we have a contravariant functor going from the category of Riemann surfaces and holomorphic maps between them to the category of fields of meromorphic functions on Riemann surfaces and homomorphisms between them). Now, given that ϕ is surjective, as in the case of a branched (or unbranched) cover, ϕ_* is injective. Indeed, if $\phi_*(f) = \phi_*(g)$ for some $f, g \in \mathcal{M}(X)$, then since for any $x \in X$, $x = \phi(y)$ for some $y \in Y$, we see that $f(x) = f \circ \phi(y) = g \circ \phi(y) = g(x)$, implying that $f = g$ in $\mathcal{M}(X)$.

Now, with Proposition 6.3 in mind, we state the following important theorem:

Theorem 6.4. *As usual, let $\phi : Y \to X$ be a branched holomorphic n-sheeted covering map of Riemann surfaces. If $f \in \mathcal{M}(Y)$ and $c_1, ..., c_n \in \mathcal{M}(X)$ are the elementary symmetric functions of f, then*

$$f^n + (\phi_* c_1) f^{n-1} + \cdots + (\phi_* c_n) = 0.$$

Moreover, the injection $\mathcal{M}(X) \to \mathcal{M}(Y)$ defines an algebraic field extension of degree at most n. Finally, if there exists an $f \in \mathcal{M}(Y)$ and some $x \in X$ with preimages $y_1, y_2, ..., y_n \in Y$ such that the $f(y_i)$ (with $1 \leq i \leq n$) are all distinct, then this field extension has degree n.

Proof. The first part of the theorem follows immediately from the definition of elementary symmetric functions: clearly, for any $1 \leq i \leq n$, f_i is a root of the polynomial

$$\prod_{i=1}^{n}(t - f_i) = t^n + c_1 t^{n-1} + \cdots + c_n$$

and since $f_i = f \circ \tau_i$, we have $f = f \circ \tau_i \circ \phi = f_i \circ \phi = \phi_*(f_i)$, so we may apply ϕ_* to the equation

$$(f_i)^n + c_1(f_i)^{n-1} + \cdots + c_n = 0$$

to obtain

$$f^n + (\phi_* c_1) f^{n-1} + \cdots + (\phi_* c_n) = 0.$$

Next, from the above equation, we see that the minimal polynomial of any $f \in \mathcal{M}(Y)$ has degree at most n. Now, if $L = \mathcal{M}(Y)$ and $K = \phi_*\mathcal{M}(X)$. Suppose $g \in L$ has a minimal polynomial with the maximal degree N across all meromorphic functions in L. We claim that g is a primitive element, i.e., $L = K(g)$. If not, then take any $f \in L$ and consider $K(f, g)$; by the Primitive Element Theorem, there exists some other $h \in L$ such that $K(f, g) = K(h)$. However, $[K(h) : K] \leq n_0$ but

$$[K(f, g) : K] \geq [K(g) : K] = n_0$$

meaning that $K(g) = K(f, g)$ and $f \in K(g)$. Therefore, L is a finite extension of K of degree $n_0 \leq n$.

In particular, if the minimal polynomial of any $f \in L$ must have m distinct roots, for some $m \leq n$. Thus, if $m = n$, we immediately see that L has degree n over K. ■

As a matter of fact, the last statement of the theorem is always satisfied, and it's a deep result known as Riemann's Existence Theorem (analytic version).

Theorem 6.5 (Analytic Riemann's Existence Theorem)**.** *Let X be a compact Riemann surface, $\{x_1, ..., x_n\}$ be a finite set of points on X, and $a_1, ..., a_n$ a sequence of complex numbers. There exists some $f \in \mathcal{M}(X)$ such that $f(x_i) = a_i$ for $1 \leq i \leq n$.*

Therefore, it follows that $\mathcal{M}(Y)$ is an algebraic extension of $\mathcal{M}(X)$ of degree n. Now, we relate branched coverings to unbranched coverings:

Proposition 6.6. *Suppose $A \subset X$ is a discrete closed subset of a Riemann surface X, and let $X' = X \setminus A$. Also, suppose $\psi : Y' \to X'$ is a proper unbranched holomorphic covering. Then ψ extends to a proper holomorphic branched covering $\phi : Y \to X$ such that $Y' = Y \setminus \phi^{-1}(A)$ is an open subset of Y.*

Proof. Consider some $x \in A$; we may take some open neighborhood U_x of x such that it contains no other points of A and there is a chart going from U_x to the unit disc $D \subset \mathbb{C}$ (by performing some suitable linear transformation in the complex plane). Clearly, the restriction of ψ to $\psi^{-1}(U_x \setminus \{x\})$ is a finite cover, so suppose it's a disjoint union of d open neighborhoods $V_x^1 \cup \cdots \cup V_x^d$, with each V_x^i being homeomorphic to a finite connected cover of $U_x \setminus \{x\}$, which is homeomorphic to the punctured unit disc $\dot{D} = D \setminus \{0\}$.

Now, if we let E be the universal cover of $\dot{D}$, we have the isomorphism

$$\Gamma(E \to \dot{D}) \cong \pi_1(\dot{D}, b) \cong \mathbb{Z}$$

where $b \in \dot{D}$ is some base point. Therefore, the deck transformation group is infinite cyclic, meaning that any finite cover of $\dot{D}$ corresponds to a quotient group of $\mathbb{Z}$, namely $\mathbb{Z}/k\mathbb{Z}$, for some $k \in \mathbb{Z}_{\geq 2}$. It follows that each cover V_x^i of $\dot{D}$ is given by $z \mapsto z^k$ for some $k > 1$. Since there exists a cover of this form going from $\dot{D} \to \dot{D}$, we also see that V_x^i is homeomorphic to $\dot{D}$ since they are in the same covering class.

Next, choose "abstract" points y_x^i, and define $Y = Y' \cup \bigcup_{i=1}^{d} y_x^i$ as the disjoint union of Y' and these new points. We then define an extension ϕ of ψ by mapping each y_x^i to x. Thus, we may extend the holomorphic isomorphism $V_x^i \to \dot{D}$ to a map $V_x^i \cup \{y_x^i\} \to D$ which sends $y_x^i \mapsto 0$. Moreover, we may define the topology on Y so that this map becomes a homeomorphism as well. Along with the complex structure on Y', this forms well-defined complex charts on neighborhoods in Y, and the map ϕ is clearly holomorphic, since its restriction ψ to Y' is holomorphic and it looks like $z \mapsto z^k$ (for some $k \in \mathbb{Z}_{\geq 2}$) on any y_x^i for any given $x \in A$. Finally, ϕ is proper since ψ is proper (why?), ϕ has finitely many fibres, and the compact subsets of X' differ from those of X by finitely many points (namely, the points in A). ■

Now that we know an unbranched cover can be extended to a branched covering map of Riemann surfaces, we observe its effect on the Deck group.

Proposition 6.7. *Suppose X, Y, and Z are Riemann surfaces, and let $\phi_1 : Y \to X$ and $\phi_2 : Z \to X$ be proper holomorphic covering maps. For a closed discrete subset $A \subset X$, let $X' = X \setminus A$, $Y' = \phi_1^{-1}(X')$, and $Z = \phi_2^{-1}(X')$. Then, every biholomorphic mapping $\sigma' : Y' \to X'$ that preserves the fibers can be extended to a fiber-preserving biholomorphic map $\sigma : Y \to X$.*

Proof. This proof uses a lot of the same ideas as those of Proposition 6.6. As before, take some $x \in A$ and let U_x be a sufficiently small neighborhood (so that no other points in A are in U_x) with a chart going to the unit disc with $x \mapsto 0$. Let $V_x^1, ..., V_x^p \in Y$ be the disjoint connected components of $\phi_1^{-1}(U)$, and similarly, let $W_x^1, ..., W_x^q \in Z$ be disjoint connected components of ϕ_2^{-1}. Then, the $V_x^i \setminus \phi_1^{-1}(x)$ and the $W_x^j \setminus \phi_2^{-1}(x)$ are the connected components of $\phi_1^{-1}(U_x \setminus \{x\})$ and $\phi_2^{-1}(U_x \setminus \{x\})$, respectively.

Now, given that $\sigma' : Y' \to Z'$ is a fiber-preserving holomorphic mapping, it's restriction

$$\sigma'|\phi_1^{-1}(U_x \setminus \{x\}) \to \phi_2^{-1}(U_x \setminus \{x\})$$

is biholomorphic. This means that $p = q$, and we may renumber the indices, so that $\sigma'(V_x^i \setminus \phi_1^{-1}(x)) = W_x^i \setminus \phi_2^{-1}(x)$. Because $\phi_1|V_x^i \setminus \phi_1^{-1}(x) \to U_x \setminus \{x\}$ is a finite-sheeted unbranched cover, $V_x^i \cap \phi_1^{-1}(x)$ consists of exactly one point b_i; we can do the same procedure for W_x^i to obtain one such point c_i. Hence we can extend the map

$$\sigma'|\phi_1^{-1}(U_x \setminus \{x\}) \to \phi_2^{-1}(U_x \setminus \{x\})$$

to a bijective mapping

$$\phi_1^{-1}(U_x) \to \phi_2^{-1}(U_x).$$

Now, just as we did in Proposition 6.6, we may verify that this map is biholomorphic and a homeomorphism. Applying this procedure to all points $x \in A$ gives us an extended biholomorphic map $\sigma : Y \to Z$, as desired. ■

Why did we prove the convoluted-sounding theorem above? Precisely so that we'd have the following corollary under our belts:

Corollary 6.8. *Every covering transformation $\sigma' \in \Gamma(Y' \to X')$ can be extended to a covering transformation $\sigma \in \Gamma(Y \to X)$.*

Therefore, the Deck groups $\Gamma(Y' \to X')$ and $\Gamma(Y \to X)$ are essentially the same and it makes sense to call Y a finite Galois cover of X if Y' is Galois over X'.

Proposition 6.9. *Suppose $\phi : Y \to X$ is a proper holomorphic map of Riemann surfaces that is topologically a Galois branched cover. Then, the following hold:*

1. *The Deck group $\Gamma(Y \to X)$ acts transitively on all fibers.*
2. *If $y \in Y$ is a branch point with ramification index e, then so are all points in $\phi^{-1}(\phi(y))$. The stabilizers of these points in $\Gamma(Y \to X)$ are conjugate cyclic subgroups of order e.*

Proof. Because the Deck group $\Gamma(Y' \to X')$ acts transitively on all fibers, so does $\Gamma(Y \to X)$ by the continuity of automorphisms. The first part of the second statement follows from Proposition 6.7 given that y maps to the other points in $\phi^{-1}(\phi(y))$ under certain Deck transformations.

The last assertion follows from the fact that in order to stabilize a branch point y, a sufficiently small neighborhood over which ϕ resembles the map $z \mapsto z^e$ must also be stabilized, which can only be done by the action of a cyclic (rotation) group of order e. ■

In particular, we revisit the second statement when we get to the notion of rigidity.

Theorem 6.10. *Suppose X is a Riemann surface and*

$$P(T) = T^n + c_1 T^{n-1} + \cdots + c_n \in \mathcal{M}(X)$$

is an irreducible polynomial of degree n. Then, there exists a Riemann surface Y, a branched holomorphic n-sheeted covering $\phi : Y \to X$, and a meromorphic function $f \in \mathcal{M}(Y)$ such that $(\phi_* P)(f) = 0$. The triple (Y, ϕ, f) is "uniquely determined" in that if (Z, τ, g) is another triple with the same properties, then there is a fiber-preserving biholomorphic map $\sigma : Y \to Z$ such that $g = \sigma_*(f)$.

And now, we begin our final descent into Galois territory! Observe that if $\phi : Y \to X$ is a holomorphic branched cover of Riemann surfaces, then $\Gamma(Y \to X)$ has a representation into the automorphism group $\mathrm{Aut}(\mathcal{M}(Y)/\phi_*\mathcal{M}(X))$. Indeed, for any $f \in \mathcal{M}(Y)$ and $\sigma \in \Gamma(Y \to X)$, we may define $\sigma f = f \circ \sigma^{-1}$. Clearly, $f \mapsto \sigma f$ is an automorphism of $\mathcal{M}(Y)$. Moreover, if $\sigma, \tau \in \Gamma(Y \to X)$, then

$$(\sigma\tau)f = f \circ (\sigma\tau)^{-1} = f \circ \tau^{-1}\sigma^{-1} = \sigma(f \circ \tau^{-1}) = \sigma(\tau f)$$

so we have a group homomorphism

$$\Gamma(Y \to X) \to \mathrm{Aut}(\mathcal{M}(Y)).$$

In fact, every such automorphism $f \mapsto \sigma f$ trivially fixes the elements of the subfield $\phi_*\mathcal{M}(X)$, so our group homomorphism is in fact

$$\Gamma(Y \to X) \to \mathrm{Aut}(\mathcal{M}(Y)/\phi_*\mathcal{M}(X)).$$

Now, we come to the big theorem at last:

Theorem 6.11. *Suppose X is a Riemann surface, $K := \mathcal{M}(X)$, and $P(T) \in K(T)$ is an irreducible monic polynomial of degree n. Let (Y, ϕ, f) be the triple from Theorem 6.10 and let $L = \mathcal{M}(Y)$. Then, L is a field extension of K (technically, ϕ_*K) of degree n and $L \cong K(T)/(P(T))$. Each covering transformation $\sigma \in \Gamma(Y \to X)$ induces an automorphism $g \mapsto \sigma g = g \circ \sigma^{-1}$ of L leaving K fixed. The corresponding group homomorphism*

$$\theta : \Gamma(Y \to X) \to \mathrm{Aut}(L/K)$$

is in fact a group isomorphism. Finally, the covering Y is Galois over X if and only if L is Galois over K.

Proof. We have already proven parts of this culminating result earlier in the section. First, we already know L is a degree n field extension of K using the last statement of Theorem 6.4. Because $P(f) = 0$, we have the field isomorphism $K(T)/(P(T)) \cong L$ using basic field theory.

The homomorphism $\theta : \Gamma(Y \to X) \to \mathrm{Aut}(L/K)$ is injective because $\sigma f \neq f$ for any $\sigma \in \Gamma(Y \to X)$ that is not the identity. Furthermore, for any $\alpha \in \mathrm{Aut}(L/K)$, we have that $(Y, \phi, \alpha f)$ is another valid triple, according to Theorem 6.10. Thus, by the uniqueness statement of this theorem, there is some $\tau \in \Gamma(Y \to X)$ for which $\tau_* f = \alpha f$. If $\sigma = \tau^{-1}$, then $\sigma f = f \circ \sigma^{-1} = f \circ \tau = \tau_* f = \alpha f$, so $\alpha \in \mathrm{Aut}(L/K)$ corresponds to $\sigma \in \Gamma(Y \to X)$, showing that θ is surjective, thus establishing the isomorphism.

Finally, either Y being Galois over X or $\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$ means that both the Deck group and the automorphism group have n elements, meaning that the Deck group acts transitively on Y over X and that the automorphism group is in fact Galois. ■

At last, we see that fundamental groups are Deck groups, and Deck groups are Galois groups! This correspondence highlights a beautiful connection spanning algebra, topology, and complex analysis.

By corollary to this theorem, we can finally realize all Galois groups over the function field $\mathbb{C}(x)$:

Corollary 6.12. *All finite groups can be realized as Galois groups over the base field $\mathbb{C}(x)$.*

Proof. Consider the Riemann sphere with n punctures, i.e. $X' = \hat{\mathbb{C}} \setminus \{x_1, ..., x_n\}$ for some $x_i \in \hat{\mathbb{C}}$. Then, letting U be the universal cover of this space, we have that

$$\Gamma(U \to X') \cong \pi_1(X', x') \cong F_{n-1}$$

where F_{n-1} is the free group on $n-1$ generators. In particular, for any group G with $n-1$ generators, we may write it as some quotient of F_{n-1}, which by the Galois correspondence of covering spaces (Theorem 4.9) corresponds is the Deck group of some Galois cover U' of X'. By Proposition 6.6, this unbranched cover extends to a branched Galois cover $\phi : Y \to X$, where $X = \hat{\mathbb{C}}$ (observe that $\{x_1, ..., x_n\}$ is a discrete closed set) and Y is some Riemann surface. Therefore, since $\Gamma(Y \to X)$ is Galois, it follows from our main theorem above that $\mathcal{M}(Y)$ is Galois over $\mathcal{M}(X)$ and

$$G \cong \Gamma(Y \to X) \cong \mathrm{Gal}(\mathcal{M}(Y)/\mathcal{M}(X)) = \mathrm{Gal}(\mathcal{M}(Y)/\mathbb{C}(x))$$

where we use the fact that $\mathcal{M}(X) = \mathcal{M}(\hat{\mathbb{C}}) = \mathbb{C}(x)$. Since n was arbitrary, we see that any finite group G is realizable as a Galois group over $\mathbb{C}(x)$! ■

7 The Rigidity Method and Beyond

At last, we come to the rigidity method, which is incredibly an powerful technique in realizing groups as Galois groups. This method first starts out by realizing groups as Galois groups over $\mathbb{C}(x)$ (which we have done using Riemann surface theory) and subsequently using a method of descent to realize groups over "lower" fields like $\mathbb{Q}$. It turns out that Riemann's Existence Theorem is central to unlocking this method. In Section 6, we saw the analytic version as Theorem 6.5.

First, we introduce two complementary definitions:

Definition 7.1 (Algebraic Definition)**.** Consider triples (G, P, C), where G is a finite group, P is a finite subset of $\hat{\mathbb{C}}$, and $C = (C_p)_{p \in P}$ is a family of nontrivial conjugacy classes in G. We define two triples (G, P, C) and (G', P', C') to be equivalent if $P = P'$ and there is an isomorphism $G \to G'$ that maps C_p to C'_p for each $p \in P$. Denote the equivalence class of these triples by $\mathcal{T} = [G, P, C]$. We call such a $\mathcal{T}$ a ramification type.

Definition 7.2 (Topological Definition)**.** Let $f : R \to \hat{\mathbb{C}} \setminus \{p_1, ..., p_n\}$ be a finite Galois covering, and call the Deck group H. For each p_i, let C_{p_i} be the associated conjugacy class in H (recall the second statement of Proposition 6.9).

Now, we state the other two versions of Riemann's Existence Theorem.

Theorem 7.3 (Algebraic Riemann's Existence Theorem)**.** *Let $\mathcal{T} = [G, P, (C_p)_{p \in P}]$ be a ramification type. Label the elements of P as $p_1, ..., p_{|P|}$. Then, there exists a finite Galois extension of type $\mathcal{T}$ if and only if there exist generators $g_1, ..., g_{|P|}$ of G with $g_1 g_2 ... g_{|P|} = 1$ and each $g_i \in C_{p_i}$.*

Theorem 7.4 (Topological Riemann's Existence Theorem)**.** *Let $\mathcal{T} = [G, P, (K_p)_{p \in P}]$ be a ramification type. Label the elements of P by $p_1, ..., P_{|P|}$. Then, there exists a finite Galois covering of the punctured Riemann sphere $\hat{\mathbb{C}} \setminus P$ with type $\mathcal{T}$ if and only if there exist generators $g_1, ..., g_{|P|}$ of G with $g_1 ... g_{|P|} = 1$ and each $g_i \in K_{p_i}$.*

While we omit the the proofs of the above theorems, we remark that they are very similar and can be used to show (again) that all finite groups are realizable over $\mathbb{C}(x)$ as a quotient of a free group F_{n-1} for some n, since a free group actually can be presented in the form

$$F_{n-1} = <\gamma_1, ..., \gamma_n | \gamma_1 \gamma_2 ... \gamma_n = 1>$$

indicating that Riemann's Existence Theorem is applicable.

Lastly, we remark that rigidity can be used to show that both symmetric groups and most of the simple groups can be realized as Galois groups. Moreover, it allows us to descend from a field like $\mathbb{C}(x)$ to our field of interest, $\mathbb{Q}$. The Inverse Galois Problem still remains open over $\mathbb{Q}$, but we hope the reader has learned something interesting about Deck groups, Riemann surfaces, and the Inverse Galois problem! At last, we rest our case.

References

[1] Forster O.: Lectures on Riemann Surfaces. 1st edn. Springer Graduate Texts in Mathematics (1981)

[2] Malle B., Matzat H.: Inverse Galois Theory. 2nd edn. Springer Monographs in Mathematics (2018)

[3] Volklein H.: Groups as Galois Groups. 1st edn. Cambridge University Press (1996)

[4] Szamuely T.: Galois Groups and Fundamental Groups. 1st edn. Cambridge University Press (2009)

[5] Kuga M., Addington S., Mulase M.: Galois' Dream: Group Theory and Differential Equations. 1st edn. Springer Publishing (2005)

[6] Serre J.P.: Topics in Galois Theory. 2nd edn. Research Notes in Mathematics (2008)

[7] Landesman, Aaron. Riemann Surfaces. Retrieved from https://web.stanford.edu/ aaronlan/assets/riemann-surfaces.pdf.