SEMI-TOPOLOGICAL GALOIS THEORY

HSUAN-YI LIAO, JYH-HAUR TEH

Abstract. We introduce splitting coverings to enhance the well known analogy between field extensions and covering spaces. Semi-topological Galois groups are defined for Weierstrass polynomials and a Galois correspondence is proved. Combining results from braid groups, we solve the topological inverse Galois problem. As an application, symmetric and cyclic groups are realized over $\mathbb{Q}$.

1. Introduction

It is well known that there is a Galois correspondence between subgroups of the fundamental group of a topological space X and covering spaces over it which is analogous to the Galois correspondence between field extensions and Galois groups. Since splitting fields play fundamental roles in Galois theory, it is natural to ask what kind of covering spaces correspond to splitting fields? This is the main motivation of our study in this paper. To answer this question, we study covering spaces defined by Weierstrass polynomials on X. A Weierstrass polynomial $f \in \mathcal{C}(X)[z]$ is a polynomial with coefficients in the ring of complex-valued continuous functions on X such that whenever we fix a point x in X, each root of $f_x(z)$ is simple. We introduce a new concept called splitting covering which plays the role similar to the one plays by splitting field in Galois theory. Another motivation of our study is related to the inverse Galois problem which asks if every finite group can be realized as a Galois group over the field of rational numbers. After a century since Hilbert used his famous irreducibility theorem ([9, Theorem 1.23]) to realize the symmetric group S_n over $\mathbb{Q}$, this problem is still open. Many partial results are known, for example, Shafarevich used tools from number theory to show that every solvable finite group can be realized over $\mathbb{Q}$. We refer the reader to the book ([5]) for more results. We define semi-topological Galois groups of Weierstrass polynomials and ask a what we call the topological inverse Galois problem(Question 4.1): Does every finite group appear as the semi-topological Galois group of some Weierstrass polynomial with coefficients of $\mathbb{Q}$-polynomials restricted to some subset of $\mathbb{C}$? We solve this problem in Theorem 4.2.

The paper is organized as follows: in section 2, we construct splitting coverings of Weierstrass polynomials f and show that such coverings are the smallest among covering spaces that f splits. We define semi-topological Galois groups of Weierstrass polynomials and study their properties. In section 3, we apply Chase-Harrison-Rosenberg Theorem to get a Galois correspondence between covering spaces and separable subrings. We use this result to prove one of the main results (Corollary 3.12) in this paper that the group of covering transformations of a splitting covering is isomorphic to semi-topological Galois group. In section 4, we solve the topological inverse Galois problem(Theorem 4.2) and obtain a criterion for realizing groups over $\mathbb{Q}$(Theorem 4.4). To exemplify the relation to the original inverse Galois problem, we apply our methods to realize symmetric and cyclic groups over $\mathbb{Q}$.

2000 *Mathematics Subject Classification.* Primary 13B05, 55R10; Secondary 12F12.

Key words and phrases. Semi-topological Galois theory, Weierstrass polynomial, splitting covering, inverse Galois problem.

Throughout this article, unless otherwise stated, X, Y, Z will denote topological spaces which are Hausdorff, path-connected, locally path-connected and semi-locally simply connected.

2. Splitting coverings

2.1. **Weierstrass polynomials.** Let $\mathcal{C}(X)$ be the ring of all continuous functions from X to $\mathbb{C}$ and $f_x(z) = a_n(x)z^n + a_{n-1}(x)z^{n-1} + \cdots + a_0(x)$ be an element in $\mathcal{C}(X)[z]$, the polynomial ring with coefficients in $\mathcal{C}(X)$. In general, there may not exist a continuous function $\alpha : X \to \mathbb{C}$ such that $f_x(\alpha(x)) = 0$ for all $x \in X$. For example, on the unit sphere S^1, there is no continuous function in $\mathcal{C}(S^1)$ which satisfies the equation $z^2 - x = 0$.

Definition 2.1. *A polynomial $f_x(z) = z^n + a_{n-1}(x)z^{n-1} + \cdots + a_0(x) \in \mathcal{C}(X)[z]$ is called a* ***Weierstrass polynomial*** *of degree n on X if for each $x \in X$, f_x has distinct n roots. For such f, the set $E = \{(x, z) \in X \times \mathbb{C} : f_x(z) = 0\}$ is called the* ***solution space*** *of f. A* ***root*** *(or* ***solution****) of f is a continuous function $\alpha : X \to \mathbb{C}$ such that $f_x(\alpha(x)) = 0$ for all $x \in X$.*

From [3, Theorem 4.2, pg 141], we know that the solution space of a Weierstrass polynomial under the first projection is a covering space over X, and the solution space of a Weierstrass polynomial is connected if and only if the Weierstrass polynomial is irreducible. Since a Weierstrass polynomial $f \in \mathcal{C}(X)[z]$ may no have solutions in X, it is natural to ask if we can find solutions of f in some covering spaces over X. This is analogous to finding roots of a polynomial in some field extensions in Galois theory. We will soon see that the universal cover of X plays the role of algebraic closure.

Definition 2.2. *Let $\lambda : Y \to X$ be a continuous map. The* ***pullback*** *$\lambda^* : \mathcal{C}(X) \to \mathcal{C}(Y)$ is defined by $\lambda^*(\gamma) := \gamma \circ \lambda$ which induces a ring homomorphism $\lambda^* : \mathcal{C}(X)[z] \to \mathcal{C}(Y)[z]$ by*

$$\lambda^*(a_n z^n + a_{n-1}z^{n-1} + \cdots + a_0) := (a_n \circ \lambda)z^n + (a_{n-1} \circ \lambda)z^{n-1} + \cdots + (a_0 \circ \lambda).$$

The following result is used throughout this paper, we quote here for the convenience of the reader.

Theorem 2.3. *(*[6, Lemma 79.1]*) Suppose that $p : (E, e_0) \to (X, x_0)$ is a covering map and $f : (Y, y_0) \to (X, x_0)$ is a continuous map. The map f can be lifted to a map $\widetilde{f} : (Y, y_0) \to (E, e_0)$ if and only if $f_*(\pi_1(Y, y_0)) \subset p_*(\pi_1(E, e_0))$. Furthermore, if such a lifting exists, it is unique.*

Proposition 2.4. *If f is a Weierstrass polynomial of degree n and $Y \xrightarrow{p} X$ is a connected covering space, then any two roots of p^*f are either equal everywhere or equal nowhere; in particular, p^*f has at most n roots.*

Proof. Suppose that α, β are roots of p^*f. Let $A = \{y \in Y \mid \alpha(y) = \beta(y)\}$ which is closed in Y. Let E be the solution space of f, and pr_1, pr_2 be the first and second projection respectively. For $y \in A$, there is a neighborhood U of $p(y)$ such that $pr_1^{-1}(U) = \coprod_{i=1}^n U_i$ is a trivial covering over U and for $x \in U$, each U_i contains a root of $f_x(z)$. We may take a smaller neighborhood if necessary such that $pr_2(U_1), \cdots, pr_2(U_n)$ lie in some disjoint open subsets $V_1, \cdots, V_n$ of $\mathbb{C}$ respectively. Assume that $\alpha(y) \in V_1$. Then the set $W := \alpha^{-1}(V_1) \cap \beta^{-1}(V_1) \cap p^{-1}(U)$ is an open neighborhood of y in Y and from the property of U, $W \subset A$. Hence A is open in Y. Consequently, A is empty or whole Y. In other words, two roots of p^*f are either equal everywhere or equal nowhere; thus, p^*f has at most n roots. □

Definition 2.5. *Let $f \in \mathcal{C}(X)[z]$ be a Weierstrass polynomial of degree n on X and $p : E \to X$ be a covering map. We say that f* ***splits*** *in E if p^*f has n distinct roots in E and a continuous function $\alpha \in \mathcal{C}(E)$ is a* ***root of f in*** *E if α is a root of p^*f. The Weierstrass polynomial f is said to be* ***irreducible*** *if it is irreducible as an element in the ring $\mathcal{C}(X)[z]$.*

Theorem 2.6. *(Algebraic closure) Let f be a Weierstrass polynomial on X of degree n. Then f splits in $\widetilde{X}$ where $p : (\widetilde{X}, \widetilde{x}_0) \to (X, x_0)$ is the universal covering of X.*

Proof. Let $E_1, \cdots, E_k$ be all path-connected components of the solution space $\pi : E \to X$ of f. Then for each i, $\pi_i := \pi|_{E_i} : E_i \to X$ is a covering space of X. Let $(\pi_i)^{-1}(x_0) = \{e_{i,1}, \cdots, e_{i,r_i}\}$. From Theorem 2.3, for each $e_{i,j}$, there exists a unique lifting, $\tilde{p}_{i,j} : (\tilde{X}, \tilde{x}_0) \to (E_i, e_{i,j})$ of p. Define $\alpha_{i,j} := q_i \circ \tilde{p}_{i,j}$ which are roots of p^*f where $q_i : E_i \to \mathbb{C}$ is the projection to the second factor. We have the following commutative diagram

$$\begin{tikzcd}
\tilde{X} \arrow[dr, "\tilde{p}_{i,j}"'] \arrow[drr, "\alpha_{i,j}"] \arrow[dd, "p"'] & & \\
& E_i \arrow[r, "q_i"] \arrow[dl, "\pi_i"] & \mathbb{C} \\
X & &
\end{tikzcd}$$

Note that if $(i,j) \neq (i^{'}, j^{'})$, then $q_i(e_{i,j}) \neq q_{i'}(e_{i^{'},j^{'}})$. Hence $\alpha_{i,j}(\tilde{x}_0) \neq \alpha_{i^{'},j^{'}}(\tilde{x}_0)$. Since $r_1 + r_2 + \cdots + r_k = n$, the maps $\alpha_{i,j}, j = 1, \cdots, r_i, i = 1, \cdots, k$ are all the roots of p^*f. □

2.2. **The existence and uniqueness of splitting coverings.** Let $Y \xrightarrow{p} X$ be a covering space of X. We denote the group of covering transformations by $A(Y/X)$, that is,

$$A(Y/X) = \{\Phi : Y \to Y \mid \Phi \text{ is a homeomorphism such that } p\Phi = p\}.$$

Definition 2.7. *We say that a covering $Y \xrightarrow{p} X$ is a* ***Galois covering*** *over X if $A(Y/X)$ acts on a fibre of X transitively (hence all fibres).*

The following result is a fundamental property of Galois coverings.

Theorem 2.8. *(*[6, Corollary 81.3]*) Let Y be a covering space over X. Then Y is a Galois covering over X if and only if $p_*\pi_1(Y, y_0) \lhd \pi_1(X, x_0)$. In particular, the universal covering of X is a Galois covering.*

Definition 2.9. *Let $Y \xrightarrow{p} X$ be a covering space and $x \in X$. The cardinality of $p^{-1}(x)$ is called the* ***degree*** *of Y over X, denoted by $[Y : X]$. If H is a subgroup of G, we denote $|G/H|$ by $[G : H]$.*

The following result is clear.

Lemma 2.10. *If $Z \xrightarrow{q} Y$ and $Y \xrightarrow{p} X$ are two covering spaces with finite fibres, then $Z \xrightarrow{pq} X$ is a covering and $[Z : X] = [Z : Y][Y : X]$.*

Lemma 2.11. *If $Y \xrightarrow{p} X$ is a Galois covering, then $A(Y/X)$ has order $[Y : X]$.*

Proof. Let $G = A(Y/X)$. Since Y is Galois over X, the quotient space $\pi : Y \to Y/G$ is a covering equivalent to $Y \xrightarrow{p} X$. Hence the number of each fibre is $|G|$. □

Lemma 2.12. *Let $(Z, z_0) \xrightarrow{q} (Y, y_0)$ and $(Y, y_0) \xrightarrow{p} (X, x_0)$ be two covering spaces. If $Z \xrightarrow{pq} X$ is Galois, then $Z \xrightarrow{q} Y$ is Galois.*

Proof. Since Z is Galois over X, $(pq)_*\pi_1(Z, z_0) \lhd \pi_1(X, x_0)$. Also note that $(pq)_*\pi_1(Z, z_0) < p_*\pi_1(Y, y_0)$. Hence $(pq)_*\pi_1(Z, z_0) \lhd p_*\pi_1(Y, y_0)$ which implies $q_*\pi_1(Z, z_0) \lhd \pi_1(Y, y_0)$. Therefore, $Z \xrightarrow{q} Y$ is Galois. □

Definition 2.13. *Let f be a Weierstrass polynomial of degree n on X and $Y \xrightarrow{p} X$ be a covering space where Y is path-connected. We say that Y is a* ***splitting covering*** *of f if*

(1) *f splits in Y,*

(2) *Y is the smallest among such coverings, that is, if $Y' \overset{p'}{\to} X$ is a covering space that f splits, then there exists a covering map $\pi : Y' \to Y$ such that $p' = p \circ \pi$.*

Construction of a splitting covering of f: Let h_0 be an irreducible component of f in $\mathcal{C}(X)[z]$. Let $E_1 \overset{p_1}{\to} X$ be the solution space of h_0 and $\pi_1 : E_1 \to \mathbb{C}$ be the projection to the second component. Then $(p_1^* f)(z) = (z - \pi_1)g_1(z)$ in $(p_1^*\mathcal{C}(X))[z]$. Inductively, assume that for $i < n$, we have

$$(p_i^* f)(z) = (z - q_i^* \cdots q_2^* \pi_1) \cdots (z - q_i^* \pi_{i-1})(z - \pi_i)g_i(z)$$

in $(p_i^*\mathcal{C}(X))[z]$, where

$$\begin{tikzcd}
E_i \arrow[r, "q_i"] \arrow[rrrd, "p_i"] & E_{i-1} \arrow[r, "q_{i-1}"] & \cdots \arrow[r, "q_2"] & E_1 \arrow[d, "p_1"] \\
 & & & X
\end{tikzcd}$$

and $\pi_j : E_j \to \mathbb{C}$ is the projection to the last component for $j = 1, \cdots, i$. Note that g_i is a Weierstrass polynomial on E_i. For $i + 1$, let h_i be an irreducible component of g_i in $(p_i^*\mathcal{C}(X))[z]$, $E_{i+1} \overset{q_{i+1}}{\longrightarrow} E_i$ be the solution space of h_i, $p_{i+1} = p_1 q_2 \cdots q_{i+1}$ and $\pi_{i+1} : E_{i+1} \to \mathbb{C}$ be the projection to the last component. Hence

$$(p_{i+1}^* f)(z) = (z - q_{i+1}^* \cdots q_2^* \pi_1) \cdots (z - q_{i+1}^* \pi_i)(z - \pi_{i+1})g_{i+1}(z)$$

in $(p_{i+1}^*\mathcal{C}(X))[z]$. By induction, we have $E_f := E_n \overset{q:=p_n}{\longrightarrow} X$ and

$$(q^* f)(z) = (z - \alpha_1) \cdots (z - \alpha_{n-1})(z - \alpha_n)$$

in $(q^*\mathcal{C}(X))[z]$ where $\alpha_j := q_n^* \cdots q_{j+1}^* \pi_j$, $j = 1, \cdots, n$. Hence E_f is connected, and f splits in E_f. Note that an element in E_f is of the form $(\cdots(((x, z_1), z_2) \cdots, z_n)$. We identify it as $(x, z_1, \cdots, z_n)$. Then α_j is the projection to the $(j+1)$-th component, q is the projection to the first component and $E_f \subset S_f$ where

$$S_f := \{(x, z_1, \cdots, z_n) \in X \times \mathbb{C}^n : f_x(z_i) = 0,\ i = 1, \cdots, n, \text{ and } z_i \neq z_j \text{ if } i \neq j\}.$$

Theorem 2.14. *Let f be a Weierstrass polynomial of degree n on X. Then*

(1) *$E_f \overset{q}{\to} X$ is a splitting covering.*
(2) *Splitting covering is unique up to covering isomorphisms.*
(3) *$E_f \overset{q}{\to} X$ is a Galois covering.*

Proof. (1) Let $Y \overset{p}{\to} X$ be a covering space such that f splits in Y with roots $\beta_1, \cdots, \beta_n$. Let $x_0 \in X$, $(x_0, z_{0,1}, \cdots, z_{0,n}) \in E_f$ and y_0 be any element in $p^{-1}(x_0)$. After reordering $\beta_1, \cdots, \beta_n$ if necessary, we may assume that $\beta_1(y_0) = z_{0,1}, \cdots, \beta_n(y_0) = z_{0,n}$. Define $\pi : Y \to E_f$ by $\pi(y) = (p(y), \beta_1(y), \cdots, \beta_n(y))$. Then $p = q \circ \pi$. For any $e = (x, z_1, \cdots, z_n) \in E_f$ there exists a path-connected open neighborhood U of x in X such that $q^{-1}(U) = \coprod_i U_i$, $p^{-1}(U) = \coprod_j V_j$, all U_i and V_j are open in E_f and Y respectively, and $q|_{U_i}$ and $p|_{V_j}$ are homeomorphisms. Since V_j is path-connected and $p = q \circ \pi$, $\pi(V_j) \subset U_i$ for some i. Hence $\pi|_{V_j} = (q|_{U_i})^{-1} \circ (p|_{V_j})$ is a homeomorphism. Therefore, if $\pi(Y) \cap U_i \neq \emptyset$, then $\pi(V_j) \cap U_i \neq \emptyset$ for some j, and hence $U_i = \pi(V_j) \subset \pi(Y)$. In other words, either $U_i \subset \pi(Y)$ or $U_i \subset \pi(Y)^c$. Therefore, $\pi(Y)$ is open and closed in E_f. Since $(x_0, z_{0,1}, \cdots, z_{0,n}) \in \pi(Y)$ and E_f is connected, π is surjective. So $Y \overset{\pi}{\to} E_f$ is a covering space.

(2) Let $x_0 \in X$ and $e_0 \in q^{-1}(x_0)$. Suppose that $Y \xrightarrow{p} X$ is also a splitting covering. Then by the proof of part one, there exists a covering map $\pi : E_f \to Y$ and a covering map $\pi' : Y \to E_f$ such that the diagram

$$\begin{tikzcd}
E_f \arrow[rr, "\pi"] \arrow[dr, "q"'] & & Y \arrow[ll, bend left, "\pi'"] \arrow[dl, "p"] \\
& X &
\end{tikzcd}$$

commutes, and $\pi'(\pi(e_0)) = e_0$. By Theorem 2.3, $\pi \circ \pi^{'} = id_Y$, $\pi^{'} \circ \pi = id_{E_f}$. Hence the coverings $Y \xrightarrow{p} X$ and $E_f \xrightarrow{q} X$ are isomorphic.

(3) Let $x_0 \in X$ and $e_0, e_1 \in q^{-1}(x_0)$. By the argument in the first part, we have $\pi_0 : (E_f, e_0) \to (E_f, e_1)$ and $\pi_1 : (E_f, e_1) \to (E_f, e_0)$ such that $q = q \circ \pi_i$, $i = 0, 1$. By Theorem 2.3, $\pi_1 \circ \pi_0 = \pi_0 \circ \pi_1 = id_{E_f}$, and hence $\pi_0 \in A(E_f/X)$. Therefore, $A(E_f/X)$ acts transitively on $q^{-1}(x_0)$.

□

Recall that in Galois theory, the splitting field of a separable polynomial is Galois over the base field. The above result makes a parallel correspondence between splitting fields and splitting coverings.

Proposition 2.15. *Let f be an irreducible Weierstrass polynomial of degree n on X with solution space $E \xrightarrow{\pi} X$. Suppose that $p : Y \to E$ is a covering space and $q : Y \to X$ is a Galois covering of X where $q = \pi \circ p$. Then f splits in Y.*

Proof. Let $x_0 \in X$, $\pi^{-1}(x_0) = \{e_1, \cdots, e_n\}$ and $y_0 \in p^{-1}(e_1)$. Assume that γ_i is a path from e_1 to e_i in E. Since $q_*\pi_1(Y, y_0) = \pi_* p_* \pi_1(Y, y_0) \subset \pi_*\pi_1(E, e_1)$ and by Theorem 2.8, $q_*\pi_1(Y, y_0) \lhd \pi_1(X, x_0)$, we have

$$q_*\pi_1(Y, y_0) = [\pi_*\gamma_i] q_*\pi_1(Y, y_0) [\pi_*\gamma_i]^{-1} \subset [\pi_*\gamma_i] \pi_*\pi_1(E, e_1) [\pi_*\gamma_i]^{-1} = \pi_*\pi_1(E, e_i).$$

By Theorem 2.3, the map q can be lifted to a map $p_i : (Y, y_0) \to (E, e_i)$ such that the following diagram

$$\begin{tikzcd}
(Y, y_0) \arrow[dd, "q"'] \arrow[dr, "p_i"] \arrow[drr] & & \\
& (E, e_i) \arrow[r, "pr_2"'] \arrow[dl, "\pi"] & \mathbb{C} \\
(X, x_0) & &
\end{tikzcd}$$

is commutative. Therefore, $pr_2 \circ p_1, \cdots, pr_2 \circ p_n$, are all the roots of q^*f where $pr_2 : E \to \mathbb{C}$ is the projection to the second factor. □

Corollary 2.16. *Let f be an irreducible Weierstrass polynomial of degree n on X and $E \xrightarrow{\pi} X$ be its solution space. Suppose that $E \xrightarrow{\pi} X$ is a Galois covering. Then $E \xrightarrow{\pi} X$ is a splitting covering of f.*

Proof. From the above result, f splits in E. Let $Y \xrightarrow{p} X$ be a covering space such that f splits in Y. Let $\alpha_1, \cdots, \alpha_n$ be the n roots of p^*f. Define $q : Y \to E$ by $q(y) = (p(y), \alpha_1(y))$. Then $p = \pi \circ q$. For any $e \in E$, there is a neighborhood U of $\pi(e)$ such that U is evenly covered by p and q (see [6, pg 336]). Let V be the unique path-connected component of $\pi^{-1}(U)$ that contains e. Then V is clearly evenly covered by p and hence Y is a covering space over E. This shows that E is the splitting covering of f. □

2.3. **Another construction of splitting coverings.** Recall that any symmetric polynomial in n variables can be written as a unique polynomial in the elementary symmetric polynomials, $s_0, \cdots, s_{n-1}$ where

$$\prod_{i=1}^{n}(z-z_i) = z^n + \sum_{i=0}^{n-1}(-1)^{n-i}s_i(z_1,\cdots,z_n)z^i.$$

Hence there is a unique polynomial in n variables $\delta(a_0,\cdots,a_{n-1})$ such that

$$\delta(-s_{n-1}(z_1,\cdots,z_n),\cdots,(-1)^{n-i}s_i(z_1,\cdots,z_n),\cdots,(-1)^n s_0(z_1,\cdots,z_n)) = \prod_{1\leqslant i<j\leqslant n}(z_i-z_j).$$

The polynomial $\delta(a_0,\cdots,a_{n-1})$ is called the **discriminant polynomial**. Define $B^n := \mathbb{C}^n - Z(\delta)$ where $Z(\delta)$ is the set of zeros of δ.

Lemma 2.17. (1) *Let*

$$S := \{(a_0,\cdots,a_{n-1},z_1,\cdots,z_n) \in B^n\times\mathbb{C}^n : z^n + \sum_{i=0}^{n-1}a_iz^i = \prod_{i=1}^{n}(z-z_i)\}$$

and π be the projection to B^n. Then $\pi : S \to B^n$ is an $n!$-fold covering space.

(2) *Let $f_x(z) = z^n + \sum_{i=0}^{n-1}a_iz^i \in \mathcal{C}(X)[z]$ be a Weierstrass polynomial of degree n on X and let $S_f := \{(x,z_1,\cdots,z_n)\in X\times\mathbb{C}^n : f_x(z_i)=0,\ i=1,\cdots,n,$ and $z_i\neq z_j$ if $i\neq j\}$. Then $\widetilde{q} : S_f \to X$ is an $n!$-fold covering where $\widetilde{q}$ is the projection to X.*

Proof. (1) It is proved in [3, pg 88, Lemma 2.2] that the space

$$E^n = \{(a_0,\cdots,a_n,z)\in B^n\times\mathbb{C} | z^n + \sum_{i=0}^{n-1}a_iz^i = 0\}$$

is an n-fold covering over B^n under the natural projection. Since there are $n!$ permutations on coordinates of $(z_1,\cdots,z_n)$, similar argument shows that S is an $n!$-fold covering space over B^n.

(2) Let $f_x(z) = z^n + \sum_{i=0}^{n-1}a_iz^i$ and $a : X\to B^n$ be defined by $a(x) := (a_0(x),\cdots,a_{n-1}(x))$. Then we get the induced fibre bundle

$$\begin{tikzcd} a^*(S) \arrow[r, "a^*"] \arrow[d, "\pi^*"'] & S \arrow[d, "\pi"] \\ X \arrow[r, "a"] & B^n. \end{tikzcd}$$

Define $a' : S_f \to a^*(S)$ by $a'(x,z_1,\cdots,z_n) := (x,a(x),z_1,\cdots,z_n)$. Then a' is a homeomorphism and $\widetilde{q} = \pi^*\circ a'$. Hence $\widetilde{q} : S_f\to X$ is an $n!$-fold covering space.

□

Proposition 2.18. *Let E' be a connected component of S_f and $q := \widetilde{q}|_{E'}$. Then $E' \xrightarrow{q} X$ is a splitting covering of f.*

Proof. By the previous lemma, $E' \xrightarrow{q} X$ is a covering space. Moreover, f splits into $\alpha_1,\cdots,\alpha_n$ in E' where $\alpha_i : E'\to\mathbb{C}$ is the projection to the $(i+1)$-th component, $i=1,\cdots,n$. The result follows as in the proof of Theorem 2.14. □

Observe that $S \xrightarrow{\pi} B^n$ is a Galois covering since the map $(a,z_1,\cdots,z_n)\mapsto(a,z_{\sigma(1)},\cdots,z_{\sigma(n)})$ is a covering transformation for each $\sigma\in S_n$ where $a\in B^n$. Consequently, $S\xrightarrow{\pi} B^n$ becomes a locally trivial principal $A(S/B^n)$-bundle where we consider $A(S/B^n)$ with discrete topology.

The following result follows directly from [4, pg 51, Theorem 9.9].

Proposition 2.19. *Let $f_x(z) = z^n + \sum_{i=0}^{n-1} a_i(x)z^i$ and $g_x(z) = z^n + \sum_{i=0}^{n-1} b_i(x)z^i$ be two Weierstrass polynomials on a Hausdorff and paracompact space X and $a, b : X \to B^n$ be continuous functions defined by*

$$a(x) = (a_0(x), \cdots, a_{n-1}(x)),\ b(x) = (b_0(x), \cdots, b_{n-1}(x)).$$

Let $E_a \overset{q_a}{\to} X$ and $E_b \overset{q_b}{\to} X$ be the splitting covers of f and g respectively. If a and b are homotopic as maps from X to B^n, then $E_a \overset{q_a}{\to} X$ and $E_b \overset{q_b}{\to} X$ are equivalent covering spaces.

2.4. **Semi-topological Galois groups.** All rings are assumed to be commutative rings with identity if not mentioned explicitly.

Definition 2.20. *Let $\bar{T}$ be a ring and T be a subring of $\bar{T}$. We write $Aut_T(\bar{T})$ for the group of all ring automorphisms $\phi : \bar{T} \to \bar{T}$ such that $\phi(t) = t$ for all $t \in T$. Let f be a Weierstrass polynomial on X, and $p : E_f \to X$ be the splitting covering of f. Denote $R = q^*\mathcal{C}(X) = \{\gamma \circ q : \gamma \in \mathcal{C}(X)\}$ which is a subring of $\mathcal{C}(E_f)$. The **semi-topological Galois group** of f is defined to be the group $G_f := Aut_R(R[\alpha_1, \cdots, \alpha_n])$ where $\alpha_1, \cdots, \alpha_n : E_f \to \mathbb{C}$ are the roots of p^*f.*

The following result is an observation that the semi-topological Galois group of f is invariant under extensions over E_f.

Proposition 2.21. *Let $E_f \overset{q}{\to} X$ be the splitting covering of f and $\alpha_1, \cdots, \alpha_n : E_f \to \mathbb{C}$ be the roots of q^*f. If $Y \overset{p}{\to} X$ is a covering and f splits into $\alpha'_1, \cdots, \alpha'_n : Y \to \mathbb{C}$. Then there exists an isomorphism $\Phi : q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n] \to p^*\mathcal{C}(X)[\alpha'_1, \cdots, \alpha'_n]$ such that $\Phi(q^*\mathcal{C}(X)) = p^*\mathcal{C}(X)$, $\Phi(\{\alpha_1, \cdots, \alpha_n\}) = \{\alpha'_1, \cdots, \alpha'_n\}$, and hence, $G_f \cong Aut_{p^*\mathcal{C}(X)} p^*\mathcal{C}(X)[\alpha'_1, \cdots, \alpha'_n]$.*

Proof. By the definition of splitting coverings, there is a covering map $\pi : Y \to E_f$ such that $p = q \circ \pi$. Observe that $\pi^*\alpha_1, \cdots, \pi^*\alpha_n$ are all the roots of p^*f since $(p^*f)(\pi^*\alpha_i) = (\pi^*q^*f)(\pi^*\alpha_i) = \pi^*((q^*f)(\alpha_i)) = 0$ and $\pi^*\alpha_1, \cdots, \pi^*\alpha_n$ are distinct. Therefore, $\Phi := \pi^* : q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n] \to p^*\mathcal{C}(X)[\alpha'_1, \cdots, \alpha'_n]$ is an isomorphism which carries $q^*\mathcal{C}(X)$ onto $p^*\mathcal{C}(X)$ and $\{\alpha_1, \cdots, \alpha_n\}$ to $\{\alpha'_1, \cdots, \alpha'_n\}$. As a result, we obtain an isomorphism $\Psi : G_f \to Aut_{p^*\mathcal{C}(X)} p^*\mathcal{C}(X)[\alpha'_1, \cdots, \alpha'_n]$ which is defined by $\Psi(\phi)(g) = (\pi^*)\phi((\pi^*)^{-1}g)$. □

Example 2.22. *Let $f_x(z) = z^n - x$ for $x \in S^1 \subset \mathbb{C}$ where $n \in \mathbb{N}$. Then f is a Weierstrass polynomial, and its solution space E is an n-fold covering of S^1. Let $p : \mathbb{R} \to S^1$ be defined by $p(s) = e^{2\pi si}$ which is the universal covering space of S^1. $(p^*f)_s(z) = z^n - e^{2\pi si}$, where $s \in \mathbb{R}$. It is easy to see that roots of p^*f are $\alpha_j(s) = e^{\frac{2\pi i(s+j-1)}{n}}$, $j = 1, \cdots, n$. Note that for $j = 1, \cdots, n-1$, $e^{\frac{2\pi i}{n}}\alpha_j = \alpha_{j+1}$, and the constant function $e^{\frac{2\pi i}{n}}$ is an element in $R = p^*\mathcal{C}(S^1)$. Therefore, for $\phi \in G_f$, $e^{\frac{2\pi i}{n}}\phi(\alpha_j) = \phi(e^{\frac{2\pi i}{n}}\alpha_j) = \phi(\alpha_{j+1})$. Hence ϕ is uniquely determined by $\phi(\alpha_1)$. Let $\sigma : R[\alpha_1, \cdots, \alpha_n] \to R[\alpha_1, \cdots, \alpha_n]$ be defined by $\sigma(\tilde{\gamma})(s) := \tilde{\gamma}(s+1)$ where $s \in \mathbb{R}$ and $\tilde{\gamma} \in R[\alpha_1, \cdots, \alpha_n]$ is considered as a function on $\mathbb{R}$. Then for $p^*\gamma \in R$, $\sigma(p^*\gamma)(s) = \gamma(p(s+1)) = \gamma(p(s)) = (p^*\gamma)(s)$ Hence $\sigma|_R = id_R$. For $j = 1, \cdots, n-1$, $\sigma(\alpha_j) = \alpha_{j+1}, \sigma(\alpha_n) = \alpha_1$. Therefore $\sigma \in G_f$. Furthermore, for $j = 0, 1, \cdots, n-1$, $\sigma^j(\alpha_1) = \alpha_{1+j}$, and $\sigma^n = id$. From the above observations, we have $G_f \cong <\sigma> \cong \mathbb{Z}_n$.*

Proposition 2.23. *(Functoriality) Suppose that $\lambda : Y \to X$ is a covering map and f_1 is a Weierstrass polynomial of degree n on X. Let $f_2 = \lambda^* f_1$.*

(1) *There is a covering map $\widetilde{\lambda} : E_{f_2} \to E_{f_1}$ such that the following diagram commutes:*

$$\begin{tikzcd}
E_{f_2} \arrow[r, "\widetilde{\lambda}"] \arrow[d, "q"'] & E_{f_1} \arrow[d, "p"] \\
Y \arrow[r, "\lambda"] & X
\end{tikzcd}$$

where $p : E_{f_1} \to X, q : E_{f_2} \to Y$ are the splitting coverings of f_1 and f_2 respectively.

(2) *If $\alpha_1, \cdots, \alpha_n : E_{f_1} \to \mathbb{C}$ are all the roots of p^*f_1, then $\widetilde{\lambda}^*\alpha_1, \cdots, \widetilde{\lambda}^*\alpha_n$ are all the roots of q^*f_2.*

(3) *$\widetilde{\lambda}^* : p^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n] \to q^*\mathcal{C}(Y)[\widetilde{\lambda}^*\alpha_1, \cdots, \widetilde{\lambda}^*\alpha_n]$ is injective.*

(4) *The map $\widetilde{\lambda}$ induces a group monomorphism $\widehat{\lambda} : G_{f_2} \to G_{f_1}$ defined by $\widehat{\lambda}(\phi)(\alpha) = (\widetilde{\lambda}^*)^{-1}\phi(\alpha \circ \widetilde{\lambda})$.*

Proof. (1) Since f_2 splits in E_{f_2} and $q^*f_2 = q^*\lambda^*f_1 = (\lambda \circ q)^*f_1$, hence f_1 also splits in E_{f_2}. By the definition of splitting covering, there is a covering map $\widetilde{\lambda} : E_{f_2} \to E_{f_1}$ which makes the diagram commutes.

(2) This follows from a direct computation: $(q^*f_2)_y((\widetilde{\lambda}^*\alpha_j)(y)) = ((\lambda \circ q)^*f_1)_y(\alpha_j(\widetilde{\lambda}(y))) = ((p \circ \widetilde{\lambda})^*f_1)_y(\alpha_j(\widetilde{\lambda}(y))) = (p^*f_1)_{\widetilde{\lambda}(y)}(\alpha_j(\widetilde{\lambda}(y))) = 0$.

(3) Since $\widetilde{\lambda}$ is surjective, $\widetilde{\lambda}^* : \mathcal{C}(E_{f_1}) \to \mathcal{C}(E_{f_2})$ is injective. For $g \in \mathcal{C}(X)$, $\widetilde{\lambda}^*(p^*g) = (p \circ \widetilde{\lambda})^*g = (\lambda \circ q)^*g = q^*(\lambda^*g) \in q^*\mathcal{C}(Y)$. Thus the restriction of $\widetilde{\lambda}^*$ to $p^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$ is also injective.

(4) Observe that for $\phi \in G_{f_2}$, ϕ fixes $\widetilde{\lambda}^*p^*\mathcal{C}(X) \subset q^*\mathcal{C}(X)$; hence, $\phi(\widetilde{\lambda}^*(p^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n])) \subset \widetilde{\lambda}^*(p^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n])$. Therefore, $\widehat{\lambda}$ is well defined. It is a direct checking that $\widehat{\lambda}$ is a group monomorphism.

□

Proposition 2.24. *Let f be a Weierstrass polynomial of degree n on X and split in Y where $Y \xrightarrow{q} X$ is a covering. Let $\alpha_1, \cdots, \alpha_n$ be the roots of q^*f in Y. Suppose that T is a subring of $q^*\mathcal{C}(X)$ and $G = Aut_T T[\alpha_1, \cdots, \alpha_n]$. Then we have the following group homomorphism $\omega_{Y,T} : A(Y/X) \to G$ defined by*

$$\omega_{Y,T}(\Phi)(\beta)(y) := (\Phi^{-1})^*(\beta)(y) := \beta(\Phi^{-1}(y))$$

where $\Phi \in A(Y/X), \beta \in T[\alpha_1, \cdots, \alpha_n]$ and $y \in Y$. Furthermore, for the splitting covering $q : E_f \to X$ of f, the group homomorphism $\omega_f = \omega_{E_f, q^*\mathcal{C}(X)} : A(E_f/X) \to G$ is injective.

Proof. For $\Phi \in A(Y/X)$, it is easy to check that $(\Phi^{-1})^* : T[\alpha_1, \cdots, \alpha_n] \to T[\alpha_1, \cdots, \alpha_n]$ is a ring automorphism. From the fact that $(\Phi^{-1})^*|_T = id_T$, we have $(\Phi^{-1})^* \in Aut_T T[\alpha_1, \cdots, \alpha_n]$. Hence $\omega_{Y,T}$ is a group homomorphism. Let E_f be the splitting covering constructed in the section 2.3 and α_i be the projection to the $(i+1)$-th component, $i = 1, \cdots, n$. Suppose that $\Phi \in ker(\omega)$ and write $\Phi : E_f \to E_f$ as $\Phi(x, z_1, \cdots, z_n) = (\Phi_1(x, z_1, \cdots, z_n), \cdots, \Phi_{n+1}(x, z_1, \cdots, z_n))$. Since $(\Phi^{-1})^*(\alpha_i) = \alpha_i$, $\alpha_i \circ \Phi = \alpha_i$ for $i = 1, \cdots, n$. Therefore

$$\Phi_{i+1}(x, z_1, \cdots, z_n) = \alpha_i(\Phi(x, z_1, \cdots, z_n)) = \alpha_i(x, z_1, \cdots, z_n) = z_i,$$

and

$$\Phi_1(x, z_1, \cdots, z_n) = q(\Phi(x, z_1, \cdots, z_n)) = q(x, z_1, \cdots, z_n) = x.$$

Hence $\Phi = id_{E_f}$ and the result follows. □

3. Galois correspondence

3.1. **Correspondences between commutative rings and groups.** For a Weierstrass polynomial f in X, we have two groups associated to f, namely, $A(E_f/X)$ and G_f. We will show that these two groups are actually isomorphic. In order to do that, we use the Galois correspondence of commutative rings proved by Chase, Harrison and Rosenberg ([1]). All rings are supposed to be commutative rings with identity and connected, that is, have no idempotent other than 0 and 1 unless otherwise stated. For the convenience of the reader, we recall the following definition ([1], [2]).

Definition 3.1. (1) *A commutative R-algebra S is* ***separable*** *if S is a projective S^e-module where $S^e = S \otimes_R S^0$ is the enveloping algebra of S.*

(2) *Let R be a subring of S and G be a finite subgroup of $Aut_R(S)$. Then S is said to be* ***G-Galois*** *over R if $R = S^G := \{x \in S : \sigma(x) = x,\ \forall \sigma \in G\}$, and there exist elements $x_1, \cdots, x_n; y_1, \cdots, y_n$ of S such that*

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{e,\sigma},\ \forall \sigma \in G,$$

where e is the identity in G and

$$\delta_{e,\sigma} = \begin{cases} 1 & , \text{if } \sigma = e \\ 0 & , \text{if } \sigma \neq e. \end{cases}$$

Theorem 3.2. *(Chase-Harrison-Rosenberg)(*[1, Theorem 2.3]*) Let S be G-Galois over R. Then there is a one-to-one lattice-inverting correspondence between subgroups of G and separable R-subalgebras of S. If T is a separable R-subalgebra of S, then the corresponding subgroup is $H_T = \{\sigma \in G : \sigma(t) = t,\ \forall t \in T\}$. If H is a subgroup of G, then the corresponding separable R-subalgebra is $S^H = \{x \in S : \sigma(x) = x,\ \forall \sigma \in H\}$.*

The following notation will be used throughout this section.

Definition 3.3. *Let $A = \{(i_1, \cdots, i_{n-1}) \in \mathbb{N}^{n-1} : i_k = 0, \cdots, n-k,\ k = 1, \cdots, n-1\}$ be a set of $(n-1)$-tuples. We define a partial order on A by comparing entries from the back, more precisely, if $I = (i_1, \cdots, i_{n-1}), J = (j_1, \cdots, j_{n-1}) \in A$, we say that $I \prec J$ if there is a number ℓ such that $i_{n-k} = j_{n-k}$ for $k = 1, \cdots, \ell - 1$ but $i_{n-\ell} < j_{n-\ell}$. Let $\alpha_1, \cdots, \alpha_n$ be some symbols and $\sigma_i := (i\ i+1\ \cdots\ n) \in S_n$ (note that the order of σ_i is $n - i + 1$). We denote $\alpha^I := \alpha_1^{i_1}\alpha_2^{i_2} \cdots \alpha_{n-1}^{i_{n-1}}$ and $\sigma^I := \sigma_1^{i_1}\sigma_2^{i_2} \cdots \sigma_{n-1}^{i_{n-1}}$ where $I = (i_1, \cdots, i_{n-1}) \in A$. Let V_n be the following $n! \times n!$ matrix:*

$$V_n := (\sigma^{I_i}(\alpha^{I_j}))_{i,j=1,\cdots,n!}.$$

Example 3.4. *For $n = 3$, $\alpha^{I_0} = 1$, $\alpha^{I_1} = \alpha_1$, $\alpha^{I_2} = \alpha_1^2$, $\alpha^{I_3} = \alpha_2$, $\alpha^{I_4} = \alpha_1\alpha_2$, $\alpha^{I_5} = \alpha_1^2\alpha_2$, $\sigma^{I_0} = id$, $\sigma^{I_1} = (1\ 2\ 3)$, $\sigma^{I_2} = (1\ 3\ 2)$, $\sigma^{I_3} = (2\ 3)$, $\sigma^{I_4} = (1\ 2)$, $\sigma^{I_5} = (1\ 3)$, and*

$$V_3 = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_2 & \alpha_1\alpha_2 & \alpha_1^2\alpha_2 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_3 & \alpha_2\alpha_3 & \alpha_2^2\alpha_3 \\ 1 & \alpha_3 & \alpha_3^2 & \alpha_1 & \alpha_3\alpha_1 & \alpha_3^2\alpha_1 \\ 1 & \alpha_1 & \alpha_1^2 & \alpha_3 & \alpha_1\alpha_3 & \alpha_1^2\alpha_3 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_1 & \alpha_2\alpha_1 & \alpha_2^2\alpha_1 \\ 1 & \alpha_3 & \alpha_3^2 & \alpha_2 & \alpha_3\alpha_2 & \alpha_3^2\alpha_2 \end{pmatrix}$$

with $det(V_3) = -[(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)]^3$.

Lemma 3.5. *The n-th symmetric group*

$$S_n = \{\sigma^I : I \in A\}.$$

Proof. Let $B_l = \{\sigma^{(0,\cdots,0,i_{n-l+1},\cdots,i_{n-1})} : 0 \leq i_k \leq n-k,\ \text{for } k = n-l+1, \cdots, n-1\}$ where $l = 2, \cdots, n$ and $\mathscr{P}\{n-l+1, \cdots, n\} := \{\sigma \in S_n : \sigma(j) = j,\ \forall j = 1, \cdots, n-l\}$. We claim that

$$B_l = \mathscr{P}\{n-l+1, \cdots, n\}$$

The cases $l = 1$ is obvious. Assume that $B_{l-1} = \mathscr{P}\{n-l+2, \cdots, n\}$. Then B_{l-1} is a subgroup of S_n. For $\tau, \rho \in S_n$, $\tau B_{l-1} = \rho B_{l-1}$ if and only if $\tau\rho^{-1} \in B_{l-1}$. Also note that if $0 \leqslant p, q \leqslant l-1$, $p \neq q$, then $(\sigma_{n-l+1}^p)(\sigma_{n-l+1}^q)^{-1} = \sigma_{n-l+1}^{p-q}$ is a cycle of length l, where σ_{n-l+1} is defined in Definition 3.3. But elements in B_{l-1} have length at most $l-1$, thus

$$(\sigma_{n-l+1}^p)(\sigma_{n-l+1}^q)^{-1} \in S_n - B_{l-1}.$$

Therefore $B_l = \coprod_{p=0}^{l-1} \sigma_{n-l+1}^p B_{l-1}$ and

$$|B_l| = l|B_{l-1}| = l|\mathscr{P}\{n-l+2, \cdots, n\}| = l!.$$

Moreover, from the definition, we have $B_l \subseteq \mathscr{P}\{n-l+1, \cdots, n\}$, and $|\mathscr{P}\{n-l+1, \cdots, n\}| = l! = |B_l|$. This implies that $B_l = \mathscr{P}\{n-l+1, \cdots, n\}$. Thus, by induction,

$$S_n = \mathscr{P}\{1, \cdots, n\} = B_n = \{\sigma^I | I \in A\}.$$

□

Lemma 3.6. *Let T be an integral domain. Suppose that $\alpha_1, \cdots, \alpha_n \in T$ are distinct. Then for each $n \in \mathbb{N}$, $det(V_n) \neq 0$.*

Proof. Let $C_k = (\sigma^{I_i}(\alpha^{I_j}))_{i,j=1,\cdots,\frac{n!}{(n-k)!}}$ for $k = 1, \cdots, n-1$. Then $V_n = C_{n-1}$ and $det(C_1) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i) \neq 0$. Our strategy is to get a recursive formula for $det(C_{k+1})$ in terms of $det(C_k)$.

Let $C_{k,l} = (\sigma^{I_i}(\alpha^{I_j}))_{i=1,\cdots,\frac{n!}{(n-k)!}, j=l\frac{n!}{(n-k)!}+1,\cdots,(l+1)\frac{n!}{(n-k)!}}$, for $l = 0, \cdots, (n-k-1)$. Moreover, for $\gamma \in S_n$, we define

$$C_{k,l}\gamma := (\sigma^{I_i}(\gamma(\alpha^{I_j})))_{i=1,\cdots,\frac{n!}{(n-k)!}, j=l\frac{n!}{(n-k)!}+1,\cdots,(l+1)\frac{n!}{(n-k)!}}.$$

Then for $i_{k+1} = 0, \cdots, n-k-1$, $I_i = (i_1, \cdots, i_k, 0, \cdots, 0)$,

$$\sigma^{I_i}(\sigma_{k+1}^{i_{k+1}}(\alpha^{I_j})) = (\sigma^{(i_1,\cdots,i_k,0,\cdots,0)} \circ \sigma_{k+1}^{i_{k+1}})(\alpha^{I_j}) = \sigma^{(i_1,\cdots,i_k,i_{k+1},0,\cdots,0)}(\alpha^{I_j})$$

which implies that

$$\begin{aligned} C_{k,l}\sigma_{k+1}^{i_{k+1}} &= (\sigma^{I_i}(\sigma_{k+1}^{i_{k+1}}(\alpha^{I_j})))_{i=1,\cdots,\frac{n!}{(n-k)!}, j=l\frac{n!}{(n-k)!}+1,\cdots,(l+1)\frac{n!}{(n-k)!}} \\ &= (\sigma^{I_i}(\alpha^{I_j}))_{i=(i_{k+1})\frac{n!}{(n-k)!}+1,\cdots,(i_{k+1}+1)\frac{n!}{(n-k)!}, j=l\frac{n!}{(n-k)!}+1,\cdots,(l+1)\frac{n!}{(n-k)!}}. \end{aligned}$$

Hence, by definition, we can divide C_{k+1} into blocks in the following way:

$$C_{k+1} = \begin{pmatrix} C_{k,0} & C_{k,1} & \cdots & C_{k,(n-k-1)} \\ C_{k,0}\sigma_{k+1} & C_{k,1}\sigma_{k+1} & \cdots & C_{k,(n-k-1)}\sigma_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ C_{k,0}\sigma_{k+1}^{n-k-1} & C_{k,1}\sigma_{k+1}^{n-k-1} & \cdots & C_{k,(n-k-1)}\sigma_{k+1}^{n-k-1} \end{pmatrix}.$$

For $j = l\frac{n!}{(n-k)!} + 1, \cdots, (l+1)\frac{n!}{(n-k)!}$,

$$\alpha^{I_j} = \alpha_1^{j_1} \cdots \alpha_k^{j_k} \alpha_{k+1}^l.$$

Therefore, for $p = 0, 1, \cdots, n-k-1$,

$$\sigma_{k+1}^p(\alpha^{I_j}) = \alpha_1^{j_1} \cdots \alpha_k^{j_k} \alpha_{k+p+1}^l.$$

Multiplying the first row of C_{k+1} by (-1) and added to each other row, we have

$$det(C_{k+1}) \quad = det \begin{pmatrix} C_{k,0} & C_{k,1} & \cdots & C_{k,(n-k-1)} \\ 0 & C_{k,1}\sigma_{k+1} - C_{k,1} & \cdots & C_{k,(n-k-1)}\sigma_{k+1} - C_{k,(n-k-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & C_{k,1}\sigma_{k+1}^{n-k-1} - C_{k,1} & \cdots & C_{k,(n-k-1)}\sigma_{k+1}^{n-k-1} - C_{k,(n-k-1)} \end{pmatrix}$$

If $l \neq 0$, for $i = 1, \cdots, \frac{n!}{(n-k)!}, j = l\frac{n!}{(n-k)!} + 1, \cdots, (l+1)\frac{n!}{(n-k)!}$,

$$C_{k,l}\sigma_{k+1}^p - C_{k,l} = (\sigma^{I_i}(\sigma_{k+1}^p(\alpha^{I_j}) - \alpha^{I_j}))_{i,j} = (\sigma^{I_i}(\alpha_1^{j_1}\cdots\alpha_k^{j_k})\sigma^{I_i}(\alpha_{k+p+1}^l - \alpha_{k+1}^l))_{i,j}$$
$$= (\sigma^{I_i}(\alpha^{I_j})\sigma^{I_i}(\sum_{q=0}^{l-1}\alpha_{k+1}^{l-1-q}\alpha_{k+p+1}^q)\sigma^{I_i}(\alpha_{k+p+1} - \alpha_{k+1}))_{i,j}.$$

If $l = 0$, $C_{k,0}\sigma_{k+1}^p - C_{k,0} = 0$.

Note that $\sigma^{I_i}(\alpha_{k+p+1} - \alpha_{k+1})$ is a common factor of entries of $(p+1)$-row for $p = 0, 1, \cdots, n-k-1$. We get a matrix D from dividing the common factor of the minor obtained by deleting the first row and first column, and we have

$$det(C_{k+1}) = det(C_k)det(D)(\prod_{p=1}^{n-k-1}\prod_{i=1}^{\frac{n!}{(n-k)!}}\sigma^{I_i}(\alpha_{k+p+1} - \alpha_{k+1})).$$

To calculate the determinant of D, we introduce the matrix

$$D_m = (E_{r,s}^m)_{r,s=1,\cdots,n-k-m}$$

where

$$E_{r,s}^m = (\sigma^{I_i}(\alpha^{I_j})\sigma^{I_i}(\sum_{q_0+\cdots+q_m=s-1}\alpha_{k+1}^{q_1}\alpha_{k+2}^{q_2}\cdots\alpha_{k+m}^{q_m}\alpha_{k+r+m}^{q_0}))_{i,j=1,\cdots,\frac{n!}{(n-k)!}}$$

Note that $D_1 = D$, $E_{r,1}^m = C_k$ for $r = 1, \cdots, n-k-m$, and $D_{n-k-1} = E_{1,1}^m = C_k$.

Then

$$det(D_m) = det\begin{pmatrix} E_{1,1}^m & E_{1,2}^m & \cdots & E_{1,n-k-m}^m \\ E_{2,1}^m & E_{2,2}^m & \cdots & E_{2,n-k-m}^m \\ \vdots & \vdots & \ddots & \vdots \\ E_{n-k-m,1}^m & E_{n-k-m,2}^m & \cdots & E_{n-k-m,n-k-m}^m \end{pmatrix}$$
$$= det\begin{pmatrix} C_k & E_{1,2}^m & \cdots & E_{1,n-k-m}^m \\ 0 & E_{2,2}^m - E_{1,2}^m & \cdots & E_{2,n-k-m}^m - E_{1,n-k-m}^m \\ \vdots & \vdots & \ddots & \vdots \\ 0 & E_{n-k-m,2}^m - E_{1,2}^m & \cdots & E_{n-k-m,n-k-m}^m - E_{1,n-k-m}^m \end{pmatrix}$$

and for $r, s \geq 2$, we have the matrix

$$E_{r,s}^m - E_{1,s}^m = (\sigma^{I_i}(\alpha^{I_j})\sigma^{I_i}(\sum_{q_0+\cdots+q_m=s-1}\alpha_{k+1}^{q_1}\alpha_{k+2}^{q_2}\cdots\alpha_{k+m}^{q_m}(\alpha_{k+r+m}^{q_0} - \alpha_{k+1+m}^{q_0}))$$
$$= (\sigma^{I_i}(\alpha^{I_j})\sigma^{I_i}(\sum_{q_0+\cdots+q_m=s-1}\alpha_{k+1}^{q_1}\alpha_{k+2}^{q_2}\cdots\alpha_{k+m}^{q_m}(\sum_{a+b=q_0-1}\alpha_{k+m+1}^a\alpha_{k+r+m}^b)\sigma^{I_i}(\alpha_{k+r+m} - \alpha_{k+1+m})))$$
$$= (\sigma^{I_i}(\alpha^{I_j})\sigma^{I_i}(\sum_{q_0+\cdots+q_{m+1}=s-2}\alpha_{k+1}^{q_1}\alpha_{k+2}^{q_2}\cdots\alpha_{k+m}^{q_m}\alpha_{k+m+1}^{q_{m+1}}\alpha_{k+(r-1)+(m+1)}^{q_0})\sigma^{I_i}(\alpha_{k+r+m} - \alpha_{k+1+m}))$$
$$= (E_{r-1,s-1}^{m+1}\sigma^{I_i}(\alpha_{k+r+m} - \alpha_{k+1+m})).$$

So we get a recursive formula

$$det(D_m) = det(C_k)det(D_{m+1})(\prod_{r=2}^{n-k-m}\prod_{i=1}^{\frac{n!}{(n-k)!}}\sigma^{I_i}(\alpha_{k+r+m} - \alpha_{k+m+1})).$$

Since $D_{n-k-1} = C_k$, by this formula, we have $det(D_1) \neq 0$. Therefore from the formula relates C_{k+1} and C_k and the fact that $det(D) = det(D_1)$, we see that $det(C_{k+1}) \neq 0$. In particular, $det(V_n) = det(C_{n-1}) \neq 0$. □

Definition 3.7. *Suppose that f is a Weierstrass polynomial in X and $p : Y \to X$ is a covering where f splits with roots $\alpha_1, \cdots, \alpha_n$. Define $V : Y \to M_n(\mathbb{C})$, the set of all $n \times n$ complex matrices, by*

$$V(y) := (\sigma^{I_i}(\alpha^{I_j}(y)))_{i,j=1,\cdots,n!}$$

and $\Delta : Y \to \mathbb{C}$ by

$$\Delta(y) := det(V(y))$$

Lemma 3.8. *Let $Y \overset{p}{\to} X$ be a Galois covering. Suppose that $\lambda : Y \to \mathbb{C}$ is a continuous map satisfying $\lambda \circ \Phi = \lambda$, for all $\Phi \in A(Y/X)$. Then $\lambda \in p^*\mathcal{C}(X)$.*

Proof. Let $x_0 \in X$ and $y_1, y_2 \in p^{-1}(x_0)$. Since the group $A(Y/X)$ act transitively on $p^{-1}(x_0)$, there is $\Phi \in A(Y/X)$ such that $y_2 = \Phi(y_1)$. By the property of λ we have $\lambda(y_1) = \lambda \circ \Phi(y_1) = \lambda(y_2)$ which implies that λ takes constant value on each fibre. Since p is a quotient map, by [6, Theorem 22.2], $\lambda \in p^*\mathcal{C}(X)$. □

Lemma 3.9. *Let f be a Weierstrass polynomial on X with roots $\alpha_1, \cdots, \alpha_n$ in the splitting covering $q : E_f \to X$. Let $R = q^*\mathcal{C}(X)$ and T be a subring of R containing coefficients of q^*f and satisfies the following properties:*

(1) $T[\alpha_1, \cdots, \alpha_n] \cap R = T$,

(2) $\dfrac{1}{\Delta} \in T[\alpha_1, \cdots, \alpha_n]$.

Then

(1) *$T[\alpha_1, \cdots, \alpha_n]$ is G-Galois over T where $G = Aut_T T[\alpha_1, \cdots, \alpha_n]$.*

(2) *The group homomorphism $\omega_{Y,T} : A(Y/X) \to G = Aut_T T[\alpha_1, \cdots, \alpha_n]$ is surjective.*

Proof. (1) We have

$$T \subset T[\alpha_1, \cdots, \alpha_n]^G \subset T[\alpha_1, \cdots, \alpha_n]^{\omega_{Y,T}(A(Y/X))}.$$

Since E_f is Galois and by Lemma 3.8, we have $T \subset T[\alpha_1, \cdots, \alpha_n]^G \subset T[\alpha_1, \cdots, \alpha_n] \cap R = T$. This means that T is the subring fixed by G.

From $\dfrac{1}{\Delta} \in T[\alpha_1, \cdots, \alpha_n]$, we may define

$$\begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_{n!}(t) \end{pmatrix} := (V(t))^{-1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ for } t \in Y,$$

and then

$$V(t) \begin{pmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_{n!}(t) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

By Lemma 3.5,

$$\sum_{i=1}^{n!} \sigma(\alpha^{I_i}) y_i = \delta_{e,\sigma},\ \sigma \in S_n.$$

Since T contains all coefficients of q^*f, G merely permutes $\alpha_1, \cdots, \alpha_n$. Therefore,

$$\sum_{i=1}^{n!} \sigma(\alpha^{I_i}) y_i = \delta_{e,\sigma},\ \sigma \in G.$$

By definition, $T[\alpha_1, \cdots, \alpha_n]$ is G-Galois over T.

(2) Since Y is a Galois covering over X, from Lemma 3.8,

$$T \subset T[\alpha_1, \cdots, \alpha_n]^G \subset T[\alpha_1, \cdots, \alpha_n]^{\omega_{Y,T}(A(Y/X))} \subset R \cap T[\alpha_1, \cdots, \alpha_n] = T$$

which implies

$$T[\alpha_1, \cdots, \alpha_n]^G = T[\alpha_1, \cdots, \alpha_n]^{\omega_{Y,T}(A(Y/X))}.$$

Therefore, by part one and Chase-Harrison-Rosenberg Theorem, $\omega_{Y,T}(A(Y/X)) = G$.

□

Theorem 3.10. *Let f be a Weierstrass polynomial on X with roots $\alpha_1, \cdots, \alpha_n$ in the splitting covering $q : E_f \to X$ of f. Let $R = q^*\mathcal{C}(X)$. Then $R[\alpha_1, \cdots, \alpha_n]$ contains Δ^{-1}. Consequently, $R[\alpha_1, \cdots, \alpha_n]$ is G_f-Galois over R and the group homomorphisms $\omega_{E_f} : A(E_f/X) \to G_f$ is surjective.*

Proof. Since $\omega_{Y,R}(A(Y/X)) < G_f$, Lemma 3.8 implies

$$R \subset R[\alpha_1, \cdots, \alpha_n]^{G_f} \subset R[\alpha_1, \cdots, \alpha_n]^{\omega_{Y,R}(A(Y/X))} \subset R.$$

Hence $R[\alpha_1, \cdots, \alpha_n]^{G_f} = R$. By definition, $\Delta \in R[\alpha_1, \cdots, \alpha_n]$, and for each $\sigma \in G_f$,

$$\sigma(\Delta) = det((\sigma \circ \sigma^{I_i}(\alpha_{I_j}))_{i,j=1,\cdots,n!}) = sign(\sigma)\Delta.$$

Therefore, $\Delta^2 \in R[\alpha_1, \cdots, \alpha_n]^{G_f} = R$. By Lemma 3.6, $\Delta(t) \neq 0$ for all $t \in E_f$. Hence $\frac{1}{\Delta^2} \in R$, and $\frac{1}{\Delta} = \frac{\Delta}{\Delta^2} \in R[\alpha_1, \cdots, \alpha_n]$. By Lemma 3.9, $R[\alpha_1, \cdots, \alpha_n]$ is G_f-Galois over R. □

3.2. **The fundamental theorem of Galois theory.**

Theorem 3.11. *Let $f \in \mathcal{C}(X)[z]$ be a Weierstrass polynomial of degree n on X with roots $\alpha_1, \cdots, \alpha_n$ in the splitting covering $q : (E_f, e_0) \to (X, x_0)$ of f. Suppose that T is a subring of R containing the coefficients of q^*f where $R = q^*\mathcal{C}(X)$ and*

(1) $T[\alpha_1, \cdots, \alpha_n] \cap R = T$,

(2) $\dfrac{1}{\Delta} \in T[\alpha_1, \cdots, \alpha_n]$.

Then

(1) *$\omega = \omega_{E_f,T} : A(E_f/X) \to G = Aut_T T[\alpha_1, \cdots, \alpha_n]$ is an isomorphism.*

(2) *We have the following one-to-one correspondences between (based) covering spaces between $(E_f, e_0) \xrightarrow{q} (X, x_0)$, subgroups of $A(E_f/X)$, subgroups of G_f, and separable subrings of $T[\alpha_1, \cdots, \alpha_n]$ over T*

$$\begin{array}{ccccccc}
(E_f, e_0) & \longleftrightarrow & < e > & \longleftrightarrow & < e' > & \longleftrightarrow & T[\alpha_1, \cdots, \alpha_n] \\
\downarrow & & \wedge & & \wedge & & \cup \\
(L, l_0) & \longleftrightarrow & H & \longleftrightarrow & H' & \longleftrightarrow & L' \\
\downarrow & & \wedge & & \wedge & & \cup \\
(M, m_0) & \longleftrightarrow & J & \longleftrightarrow & J' & \longleftrightarrow & M' \\
\downarrow & & \wedge & & \wedge & & \cup \\
(X, x_0) & \longleftrightarrow & A(E_f/X) & \longleftrightarrow & G & \longleftrightarrow & T
\end{array}$$

which are given by the theory of covering spaces, ω, and Chase-Harrison-Rosenberg theorem, that is, $H = A(E_f/L)$, $H' = \omega(H)$, $L' = T[\alpha_1, \cdots, \alpha_n]^{H'}$, and $H' = G_{L'} = \{\phi \in G \mid \phi|_{L'} = id_{L'}\}$. Moreover, $[L : M] = [J : H] = [J' : H']$.

Proof. By Proposition 2.24, ω is injective and by Lemma 3.9, ω is surjective. Therefore, ω is an isomorphism.

For the second part, since E_f is Galois over X, it is also Galois over L by Lemma 2.12. Hence $[E_f : L] = |A(E_f/L)| = |H|$. Similarly, $[E_f : M] = |J|$. Therefore,

$$[L : M] = [E_f : M]/[E_f : L] = |J|/|H| = [J : H].$$

□

Corollary 3.12. *Let f be a Weierstrass polynomial of degree n on X with roots $\alpha_1, \cdots, \alpha_n$ in the splitting covering $E_f \xrightarrow{q} X$ of f. Then $\mathcal{C}(E_f) = q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$. In particular, the group homomorphism $\omega_{E_f} : A(E_f/X) \to G_f$ is an isomorphism.*

Proof. Clearly, $\mathcal{C}(E_f) \supset q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$. Conversely, let $H = A(E_f/X)$. Then H acts on $q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$ through the group monomorphism $\omega : A(E_f/X) \to Aut_{q^*\mathcal{C}(X)}q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$ defined in Proposition 2.24. By Lemma 3.8, $\mathcal{C}(E_f)^H = (q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n])^H = q^*\mathcal{C}(X)$. From the proof of Lemma 3.9, there are $x_1, \cdots, x_{n!}, y_1, \cdots, y_{n!} \in q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n] \subset \mathcal{C}(E_f)$ such that

$$\sum_{i=1}^{n!} \sigma(x_i)y_i = \delta_{e,\sigma}, \ \sigma \in H.$$

Therefore, $\mathcal{C}(E_f)$ and $q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$ are H-Galois over $q^*\mathcal{C}(X)$. In particular, $q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$ is a separable $q^*\mathcal{C}(X)$-subalgebra of $\mathcal{C}(E_f)$. Furthermore, $H_{q*\mathcal{C}(X)[\alpha_1,\cdots,\alpha_n]} = \{e\} = H_{\mathcal{C}(E_f)}$, so by the Galois correspondence from the Chase-Harrison-Rosenberg Theorem, $\mathcal{C}(E_f) = q^*\mathcal{C}(X)[\alpha_1, \cdots, \alpha_n]$. □

In general not all covering spaces are equivalent to polynomial covering spaces but it is true for spaces with free fundamental groups.

Theorem 3.13. *(*[3, Theorem 6.3, pg 110]*) Suppose that $\pi_1(X)$ is a free group. Then every finite covering map onto X is equivalent to a polynomial covering map.*

It is natural to ask whether any connected Galois covering of finite degree is equivalent to the splitting covering of a Weierstrass polynomial. The following result is an enhancement of theorem above.

Proposition 3.14. *Suppose that $\pi_1(X)$ is free. Then any finite connected Galois covering of X is equivalent to the splitting covering of some Weierstrass polynomial on X.*

Proof. Let $Y \xrightarrow{p} X$ be a finite connected Galois covering of X. Theorem 3.13 demonstrates that there is a Weierstrass polynomial f on X such that its solution space is equivalent to $Y \xrightarrow{p} X$. Moreover, by Corollary 2.16, the splitting covering $E_f \xrightarrow{q} X$ is equivalent to $Y \xrightarrow{p} X$. □

Corollary 3.15. *Suppose that $\pi_1(X)$ is free and $Y \xrightarrow{p} X$ is a finite connected Galois covering of X. Then $A(Y/X) \cong Aut_{p^*\mathcal{C}(X)}\mathcal{C}(Y)$ and $\mathcal{C}(Y)$ is $A(Y/X)$-Galois over $p^*\mathcal{C}(X)$.*

Proof. By Proposition 3.14, there exists a Weierstrass polynomial f on X with splitting covering $E_f \xrightarrow{q} X$ equivalent to $Y \xrightarrow{p} X$, that is, there is a covering equivalence $\Phi : Y \to E_f$. Therefore, Φ^* gives an isomorphism from $\mathcal{C}(E_f)$ to $\mathcal{C}(Y)$ mapping $q^*\mathcal{C}(X)$ onto $p^*\mathcal{C}(X)$. As a result of Proposition 3.12, $A(Y/X) \cong A(E_f/X) \cong Aut_{p^*\mathcal{C}(X)}\mathcal{C}(Y)$ and $\mathcal{C}(Y)$ is $A(Y/X)$-Galois over $p^*\mathcal{C}(X)$. □

4. Groups as Galois groups

4.1. **Realization of groups as semi-topological Galois groups.** It is natural in our setting to ask the following inverse Galois problem:

Question (Topological inverse Galois problem) Does every finite group appear as the semi-topological group of some Weierstrass polynomial with coefficients of $\mathbb{Q}$-polynomials restricted to some subset of $\mathbb{C}$?

In this section we will solve this problem and relate it to the original inverse Galois problem. Let $\mathbb{C}^+$ be the set of complex numbers with real part greater than zero, and let

$$F_n = \{(x_1, x_2, \cdots, x_n) \in (\mathbb{C}^+)^n : x_i \neq x_j, \ \forall i \neq j\}.$$

Then the n-th symmetric group S_n acts on F_n by permuting x_i's. Let C_n be the quotient space F_n/S_n which is homeomorphic to the space $B^n = \mathbb{C}^n - Z(\delta)$ where $Z(\delta)$ is the zero set of the discriminant polynomial δ (see Section 2.3).

For a continuous function $\alpha : X \to C_n$, represent the class $\alpha(x)$ by $[(\alpha_1(x), \cdots, \alpha_n(x))]$ where α_i's may not be continuous functions but the elementary symmetric polynomials formed by $\alpha_1, \cdots, \alpha_n$ are continuous functions on X. So we have a Weierstrass polynomial $f_x(z) = \prod_{i=1}^n (z - \alpha_i(x))$. The solution space E of f is an n-fold covering over X. We denote the set of all equivalence classes of n-fold covering spaces obtained from such f by $\mathcal{PC}_n^+(X)$.

It is clear that two homotopic maps from X to C_n give the equivalent covering spaces ([3, pg 92, Corollary 3.3]) and it is know that C_n is an Eilenberg-Mac-Lane space of type $(B(n), 1)$([3, pg 98]), where $B(n)$ is the Artin braid group which is the fundamental group of C_n. By [8, pg 428, Theorem 11], there is a bijective correspondence

$$[X, C_n] \to Hom(\pi_1(X), B(n))^{conj}$$

defined by mapping the free homotopy class of a map $\alpha : X \to C_n$ to the conjugacy class of the induced homomorphism $\alpha_* : \pi_1(X) \to B(n)$. Therefore, we have a map,

$$Hom(\pi_1(X), B(n))^{conj} \cong [X, C_n] \to \mathcal{PC}_n^+.$$

The last arrow maps α to the solution space of f_α which by definition is a surjection. Moreover, if we denote $\pi_1(F_n)$ by $H(n)$, then we have the braid group sequence ([3, pg 17])

$$1 \to H(n) \overset{\rho_n}{\to} B(n) \overset{\tau_n}{\to} S_n \to 1,$$

and the following commutative diagrams(a similar diagram is in [3, pg 108])

$$\begin{tikzcd}
Hom(\pi_1(X), H(n))^{conj} \arrow[d, "\rho_n \circ -"'] & \\
Hom(\pi_1(X), B(n))^{conj} \arrow[r] \arrow[d, "\tau_n \circ -"'] & \mathcal{PC}_n^+(X) \arrow[d, "inclusion"'] \\
Hom(\pi_1(X), S_n)^{conj} \arrow[r] & \mathcal{C}_n(X)
\end{tikzcd}$$

where $\mathcal{C}_n(X)$ denotes the set of equivalence classes of n-fold covering spaces on X, $Hom(\pi_1(X), S_n)^{conj} \to \mathcal{C}_n(X)$ is given by the characteristic maps of covering spaces, and the horizonal maps are always surjective (see [3, pg 99]). In particular, if the fundamental group of the base space X is a free group, then the homomorphism $\tau\circ$ is surjective, so each n-fold covering space of X is equivalent to the solution space of a Weierstrass polynomial of this type. The argument is similar to the one in the proof of [3, pg 110, Theorem 6.3].

Lemma 4.1. *Suppose that $\pi_1(X)$ is free. Then $\mathcal{C}_n(X) = \mathcal{PC}_n^+$.*

The above result is used to prove the following main result of this paper.

Theorem 4.2. *Let G be any finite group. Then there is a Weierstrass polynomial on a compact subset of the complex plane with rational polynomials as coefficients such that G is isomorphic to its semi-topological Galois group.*

Proof. Since G is finite, there exists a finitely generated free group F and a normal subgroup N of F such that $G = F/N$. If F is generated by m elements, then we take m disjoint open discs $D_1, \cdots, D_m$ in a compact disk D in $\mathbb{C}$ such that $\pi_1(X) \cong F$ where $X = D - \cup_{j=1}^m D_j$. By the Galois correspondence of covering spaces, there is a connected covering space $E' \xrightarrow{q} X$ such that $N \cong q_*\pi_1(E')$ and $A(E'/X) \cong F/N \cong G$. Since $q_*\pi_1(E')$ is normal in $\pi_1(X)$, by Theorem 2.8, $E' \xrightarrow{q} X$ is Galois. By Lemma 4.1, E' is equivalent to the solution space E of some irreducible Weierstrass polynomial f defined on X and for each $x \in X$, roots of $f_x(z)$ have images in $\mathbb{C}^+$. Then $E \xrightarrow{p} X$ is Galois, and by Corollary 2.16, E is the splitting covering of f. Let $\alpha_1, \cdots, \alpha_n$ be the roots of f in E. Define

$$g_x(z) = \prod_{i=1}^{n}(z - \alpha_i(x))(z - \overline{\alpha_i(x)}) = z^{2n} + \sum_{j=0}^{2n-1} a_j(x)z^j,$$

where "$-$" is the complex conjugation. Then the function g is a Weierstrass polynomial of degree $2n$ on X and all a_i's are real-valued functions. Since E is the splitting covering of f, it is also the splitting covering of g.

Let $a : X \to B^{2n}$ be the continuous function defined by $a(x) = (a_0(x), \cdots, a_{2n-1}(x))$. Then $a(X) \subset B^{2n}$ is compact where $B^{2n} = \mathbb{C}^{2n} - Z(\delta)$ and δ is the discriminant polynomial. Since $Z(\delta)$ is closed in $\mathbb{C}^{2n}$, the distance between $a(X)$ and $Z(\delta)$ is a positive number $\varepsilon = d(a(X), V(\delta))$. Then by the Stone-Weierstrass theorem([7, Theorem 7.32]), there are $\tilde{a}_0, \cdots, \tilde{a}_{2n-1} \in \mathbb{Q}[x]$ such that $\|\tilde{a}_j - a_j\| < \varepsilon/4n$, $j = 0, \cdots, 2n-1$ where $||\tilde{a}_j - a_j|| = max_{x\in X}|\tilde{a}_j(x) - a_j(x)|$. Hence $||\tilde{a} - a|| \leq \sum_{i=1}^{2n} ||\tilde{a}_j - a_j|| < \varepsilon/2$.

Then for any $x \in X$,

$$d(\tilde{a}(x), V(\delta)) \geq d(a(x), V(\delta)) - d(a(x), \tilde{a}(x)) > \varepsilon - \varepsilon/2 = \varepsilon/2.$$

Therefore we have a map $\tilde{a} = (\tilde{a}_0, \cdots, \tilde{a}_{2n-1}) : X \to B^{2n}$ and a Weierstrass polynomial $\widetilde{g}_x(z) = z^{2n} + \sum_{j=0}^{2n-1} \tilde{a}_j(x)z^j$. Let $H(x,t) := (1-t)a(x) + t\tilde{a}(x)$ for $t \in [0,1], x \in X$. Then $|a(x) - H(x,t)| = t|a(x) - \widetilde{a}(x)| < t\varepsilon/2 \leq \varepsilon/2$, so $H : X \times I \to B^{2n}$ is a homotopy between a and $\widetilde{a}$. Hence Proposition 2.19 and Theorem 3.11 imply that $G_{\tilde{g}} \cong G_g \cong G$. □

4.2. **Relation to inverse Galois problem.** In the following, we fix X a path-connected subset of $\mathbb{C}$. Let $E_f \xrightarrow{q} X$ be the splitting covering of a Weierstrass polynomial f on X, and let $\alpha_1, \cdots, \alpha_n : E_f \to \mathbb{C}$ be all roots of f in E_f. We define

$$T := \{\frac{q^*g}{q^*h} \mid g, h \in \mathbb{Q}[x],\ h(x) \neq 0,\ \forall x \in X\}$$

and

$$W := \{\frac{q^*g}{q^*h} \mid g, h \in \mathbb{Q}[x],\ h \neq 0\} \cong \mathbb{Q}(x).$$

Lemma 4.3.

$$Aut_T T[\alpha_1, \cdots, \alpha_n] \cong Aut_W W[\alpha_1, \cdots, \alpha_n].$$

Proof. Since T is a subring of W, we have a restriction map $r : Aut_W W[\alpha_1, \cdots, \alpha_n] \to Aut_T T[\alpha_1, \cdots, \alpha_n]$ by sending φ to $\varphi|_{T[\alpha_1, \cdots, \alpha_n]}$. We use that notation $\alpha^I := \alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}$ where $I = (i_1, i_2, \cdots, i_n)$.

For $\psi \in Aut_T T[\alpha_1, \cdots, \alpha_n]$, define $\widetilde{\psi} : W[\alpha_1, \cdots, \alpha_n] \to W[\alpha_1, \cdots, \alpha_n]$ by

$$\widetilde{\psi}(\sum_I \frac{a_I}{b_I}\alpha^I) = \frac{1}{B}\psi(\sum_I a_I B_I \alpha^I)$$

where $B = \prod_I b_I$, $B_I = \frac{B}{b_I}$ and $a_I, b_I \in \mathbb{Q}[x]$. Then it straightforward to show that $\widetilde{\psi} \in Aut_W W[\alpha_1, \cdots, \alpha_n]$. In consequence, we obtain a map $\Phi : Aut_T T[\alpha_1, \cdots, \alpha_n] \to Aut_W W[\alpha_1, \cdots, \alpha_n]$ defined by $\Phi(\psi) = \widetilde{\psi}$ which is a group isomorphism. □

Theorem 4.4. *Suppose that $T[\alpha_1, \cdots, \alpha_n] \cap R = T$ where $R = q^*\mathcal{C}(X)$. Then G_f occurs as a Galois group of a Galois extension of $\mathbb{Q}$.*

Proof. Since $\Delta^2 \in R$ and $\Delta \in T[\alpha_1, \cdots, \alpha_n]$, $\Delta^2 \in T$ by assumption. So $\Delta^2 = \frac{q^*g}{q^*h}$ for some $g, h \in \mathbb{Q}[x]$ and $h(x) \neq 0$ for $x \in X$. By Lemma 3.6, $\frac{1}{\Delta^2} = \frac{q^*h}{q^*g} \in R$, so $g(x) \neq 0$ for all $x \in X$. This implies $\frac{1}{\Delta^2} \in T$. Then $\frac{1}{\Delta} = \frac{\Delta}{\Delta^2} \in T[\alpha_1, \cdots, \alpha_n]$. By Theorem 3.11, $Aut_T(T[\alpha_1, \cdots, \alpha_n]) \cong G_f$ Lemma 4.3 implies that $Aut_W(W[\alpha_1, \cdots, \alpha_n]) \cong G_f$. Moreover, $W[\alpha_1, \cdots, \alpha_n]$ is the splitting field of $f \in W[z]$, and hence, $W[\alpha_1, \cdots, \alpha_n]$ is a Galois extension of W. Since $W \cong \mathbb{Q}(x)$ and $\mathbb{Q}$ is Hilbertian([9, pg 18, Theorem 1.23]), G_f occurs as a Galois group of certain Galois extension L of $\mathbb{Q}$ as wished. □

Corollary 4.5. *If $T[\alpha_1, \cdots, \alpha_n] = T[\alpha]$ where $\alpha \in T[\alpha_1, \cdots, \alpha_n]$ is a root of a polynomial $h \in T[z]$ of degree n, then G_f can be realized as a Galois group over $\mathbb{Q}$.*

Proof. For $\varphi \in T[\alpha] \cap R$, $\varphi = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ for some $a_0, \cdots, a_{n-1} \in T$. Let $x \in X$ and $\pi^{-1}(x) = \{e_1, \cdots, e_n\}$. Then $\varphi(x) = a_0(x) + a_1(x)\alpha(e_j) + \cdots + a_{n-1}(x)\alpha(e_j)^{n-1}$ for all $j = 1, \cdots, n$. Since E_f over X is Galois, for each e_j, there is a unique $g_j \in G_f$ such that $g_j(e_1) = e_j$. Applying all g_j to φ, their sum is $n\varphi(x) = na_0(x) + a_1(x)\sum_{j=1}^n (g_j \cdot \alpha)(e_1) + \cdots + a_{n-1}(x)(\sum_{j=1}^n g_j \cdot \alpha^{n-1})(e_1)$. Since $\sum_{j=1}^n (g_j \cdot \alpha^k)(e_1) = \sum_{j=1}^n \alpha^k(e_j)$ and it is well known that $\sum_{j=1}^n \alpha^k(e_j)$ can be expressed as a polynomial of coefficients of h, so $\sum_{j=1}^n (g_j \cdot \alpha^k) \in T$ which implies that $\varphi \in T$. Hence by the result above, we have our claim. □

In the following, we apply our method to realize symmetric groups and cyclic groups over $\mathbb{Q}$.

Corollary 4.6. *The n-th symmetric group S_n can be realized as a Galois group over $\mathbb{Q}$.*

Proof. By Theorem 4.2, there is a space $X \subset \mathbb{C}$ and a Weierstrass polynomial $f \in \mathcal{C}(X)[z]$ such that $G_f = S_n$. Suppose that $p : E_f \to X$ is the splitting covering of f and f splits into $\alpha_1, \cdots, \alpha_n$ in E_f. Let $\varphi \in T[\alpha_1, \cdots, \alpha_n] \cap R$. Then $\varphi = \sum_I a_I \alpha^I$ where $I = (i_1, \cdots, i_n)$, $\alpha^I = \alpha_1^{i_1}\alpha_2^{i_2} \cdots \alpha_n^{i_n}$. Since for any $\sigma \in G_f$, $\sigma\varphi = \varphi$, we have $(n!)\varphi = \sum_{\sigma \in S_n} \sigma\varphi = \sum_I a_I \sum_{\sigma \in S_n} \sigma(\alpha^I)$. Note that the sum $\sum_{\sigma \in S_n} \sigma(\alpha^I) = \sum_{\sigma \in S_n} \alpha_{\sigma(1)}^{i_1}\alpha_{\sigma(2)}^{i_2} \cdots \alpha_{\sigma(n)}^{i_n}$ which is a symmetric polynomial in $\alpha_1, \cdots, \alpha_n$. So by the fundamental theorem of symmetric polynomials, the sum can be expressed as a polynomial with rational coefficients of elementary symmetric polynomials in $\alpha_1, \cdots, \alpha_n$, which are just the coefficients of p^*f, and hence $\sum_{\sigma \in S_n} \sigma(\alpha^I) \in T$. This implies that $\varphi \in T$. So by Theorem 4.4, S_n can be realized as a Galois group over $\mathbb{Q}$. □

Corollary 4.7. *Any cyclic group $\mathbb{Z}_n$ can be realized as a Galois group over $\mathbb{Q}$.*

Proof. Let $f_x(z) = z^n - x \in \mathcal{C}(S^1)[z]$ which is clearly an irreducible Weierstrass polynomial on S^1. By Example 2.22, $G_f = \mathbb{Z}_n$. Let $p : E_f \to S^1$ be the splitting covering of f and $\alpha_1, \cdots, \alpha_n$ be the roots of f. Since $\alpha_1(s) \neq 0$ for all $s \in E_f$, the function $\beta_i := \frac{\alpha_i}{\alpha_1}$ is a continuous function on E_f. From $\alpha_j(s)^n = (p^*x)(s) = p(s)$ for any $j = 1, \cdots, n$, we have $\beta_i^n(s) = 1$ for all $s \in E_f$. Since E_f is connected, β_i is a constant function. By renumbering the roots if necessary, we may assume that $\beta_j = e^{\frac{2\pi i}{n}(j-1)} = \beta_2^{j-1}$ for $j = 2, \cdots, n$. Let $\varphi \in T[\alpha_1, \cdots, \alpha_n] \cap R$ where $R = p^*\mathcal{C}(S^1)$ and write $\varphi = \sum_I a_I \alpha^I$. We have $\alpha^I = \alpha_1^{i_1}(\beta_2\alpha_1)^{i_2}(\beta_2^2\alpha_1)^{i_3} \cdots (\beta_2^{n-1}\alpha_1)^{i_n} = \beta_2^{i_2+2i_3+\cdots+(n_1)i_n}\alpha_1^{i_1+i_2+\cdots+i_n} = \beta_2^{c_I}\alpha_1^{\sum I}$ where $c_I = \sum_{j=2}^n (j-1)i_j$, $\sum I = i_1 + i_2 + \cdots + i_n$ for $I = (i_1, i_2, \cdots, i_n)$. Since G_f has n elements, for a point $x \in S^1$, $p^{-1}(x) = \{y_1, \cdots, y_n\}$. From $\varphi \in R$, $n\varphi(y_1) = \sum_{j=1}^n \varphi(y_j) =$

$\sum_I b_I(x)(\sum_{j=1}^n \alpha^I(y_j))$ where $b_I = p \circ a_I$. By a property of covering transformations, there is a unique $\sigma_j \in G_f$ such that $\sigma_j(y_1) = y_j$. Then $n\varphi(y_1) = \sum_I b_I(x)(\sum_{j=1}^n \beta_2^{c_I}\alpha_1^{\sum I}(\sigma_j(y_1))) = \sum_I b_I(x)\beta_2^{c_I}(\sum_{j=1}^n \alpha_j^{\sum I}(y_1)) = \sum_I b_I(x)\beta_2^{c_I}((\sum_{j=1}^n \beta_j^{\sum I})\alpha_1^{\sum I}(y_1)) = \sum_I b_I(x)\beta_2^{c_I}(\frac{\beta_2^{n\sum I}-1}{\beta_2-1})\alpha_1^{\sum I}(y_1) = b_0(x) \in T$ where $b_0 = b_{(0,\cdots,0)}$. This implies that $\varphi \in T$ and hence $T[\alpha_1, \cdots, \alpha_n] \cap R = T$. By Theorem 4.4, $\mathbb{Z}_n$ can be realized as a Galois group over $\mathbb{Q}$. □

Acknowledgements The authors thank the referee for his\her detailed comments which largely improve this paper, and the National Center of Theoretical Sciences of Taiwan (Hsinchu) for providing a wonderful working environment.

References

1. S. U. Chase, D. K. Harrison, and A. Rosenberg, Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. No. 52 (1965).
2. C. Greither, Cyclic Galois Extensions of Commutative Rings, Lecture notes in mathematics, 1534, Springer-Verlag (1992).
3. V. L. Hansen, Braids and Coverings, Selected topics. London Mathematical Society Texts 18, Cambridge University Press (1989).
4. D. Husemoller, Fibre Bundles, Graduate Texts in Mathematics 20, Springer-Verlag (1966).
5. G. Malle and H. Matzat, Inverse Galois Theory, Springer-Verlag (1999).
6. J. R. Munkres, Topology: A First Course, Prentice-Hall (1975).
7. W. Rudin, Principles of mathematical analysis, 3rd edition, McGraw-Hill(1985).
8. E.H. Spanier, Algebraic topology, McGraw-Hill, (1966).
9. H. Völkiein, Groups as Galois Groups: An Introduction, Cambridge Studies in Advanced Mathematics 53, Cambridge University Press (1996).

Department of Mathematics, National Tsing Hua University of Taiwan, No. 101, Kuang Fu Road, Hsinchu, 30043, Taiwan.
E-mail address: s9821502@m98.nthu.edu.tw, jyhhaur@math.nthu.edu.tw