Compact Riemann Surfaces
Prime Galois Coverings of $\mathbb{P}^1$

by

Michael Tsiang

B.A., University of California, Santa Cruz, 2004

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
Master of Science
in
The Faculty of Graduate Studies
(Mathematics)

The University of British Columbia
June, 2007
© Michael Tsiang 2007
Abstract

The uniqueness of the hyperelliptic involution is well known in the theory of Riemann surfaces. More precisely, we know that if $X$ is a hyperelliptic compact Riemann surface, there is a unique automorphism $\tau$ of order 2 such that $X/\langle \tau \rangle \cong \mathbb{P}^1$. We wish to generalize the situation slightly. We say $X$ is a prime Galois covering of $\mathbb{P}^1$ if there exists an automorphism $\tau$ of (odd) prime order $p$ such that $X/\langle \tau \rangle \cong \mathbb{P}^1$. This leads us to ask the question: When is this automorphism $\tau$ unique?

We begin by building the necessary background to understand prime Galois coverings of $\mathbb{P}^1$. We then prove a theorem due to González-Diez that answers our question about uniqueness. The proof given here follows his proof (given in [G-D]) quite closely, though we elaborate and modify certain details to make it more self contained.
# Table of Contents

Abstract ................................................. ii

Table of Contents ....................................... iii

Acknowledgements ....................................... iv

1 Background ........................................... 1
   1.1 Compact Riemann Surfaces .................... 1
      1.1.1 Meromorphic Functions ................. 3
      1.1.2 Meromorphic Differentials .......... 4
   1.2 Projective Curves ............................... 5
   1.3 Normalization .................................. 8
   1.4 Divisors ........................................ 9
      1.4.1 Special Divisors ...................... 12
   1.5 The Riemann-Hurwitz Formula ............. 13
   1.6 Group Actions ................................ 14
      1.6.1 Galois Coverings ...................... 15

2 Prime Galois Coverings of $\mathbb{P}^1$ ........... 17
   2.1 Examples ........................................ 17
   2.2 Preliminaries .................................. 19
      2.2.1 A Special Case ......................... 21

3 The Main Theorem .................................... 24
   3.1 Two Lemmas .................................... 24
   3.2 The Crucial Step ............................... 25
   3.3 Conclusion ..................................... 27

Bibliography ........................................... 28
Acknowledgements

I would like to thank my advisor Zinovy Reichstein for his guidance and patience throughout my time at UBC. I also acknowledge the help of all of the staff in the department office, especially Lee Yupitun for being all knowing.

I feel exceptionally fortunate and grateful to have the unending support of my parents, my brother David, and my sister Angela. Moreover, I thank my fellow graduate students for their friendship and help during my graduate career. In particular, I thank Christy Cameron, Warren Code, Chris Coulter, Alex Duncan, Florina Halasan, Patrick Ingram, Vishaal Kapoor, Simon Rose, Patrick Walls, Erick Wong, and Katya Yurasovskaya.

Lastly, I give a special thanks to Amy Goldlist. This paper, as well as most of my graduate work, would not have been possible without her friendship, support, and copy-editing skills.
Chapter 1

Background

Compact Riemann surfaces are of interest in different areas of mathematics. There are equivalences which connect the complex analytic objects to objects arising in pure algebra and in algebraic geometry.

The main purpose of this paper is to analyze the group actions of compact Riemann surfaces which admit a special type of automorphism. Namely, we will consider $p$-sheeted coverings of the Riemann sphere, where the covering map is induced by an automorphism of prime order $p$.

We will give references rather than proofs for most of the background results which are standard in the literature. The first two sections build the parallel languages of compact Riemann surfaces and projective curves. The third section then links the two together via a process called normalization. Given this link, we are able to apply techniques from either category to prove interesting results in both.

Using standard notation, we let $\mathbb{C}$ denote the complex plane, and let $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ denote the Riemann sphere.

1.1 Compact Riemann Surfaces

**Definition.** A **compact Riemann surface** is a compact connected Hausdorff topological space $X$ together with an open covering $\{U_i\}$ of $X$ and a family of mappings $z_i : U_i \rightarrow \mathbb{C}$ such that

(i) each $z_i : U_i \rightarrow \mathbb{C}$ is a homeomorphism of $U_i$ onto an open subset $z_i(U_i) \subset \mathbb{C}$; and

(ii) if $U_i \cap U_j \neq \emptyset$, then the function $z_j \circ z_i^{-1} : z_i(U_i \cap U_j) \rightarrow z_j(U_i \cap U_j)$
is biholomorphic.

We call such a \((U_i, z_i)\) a local (holomorphic) coordinate, and \(\{(U_i, z_i)\}\) a holomorphic coordinate covering.

By abuse of notation, we will often call \(z\) a local coordinate instead of the pair \((U, z)\) when it is unnecessary to specify the set \(U\).

From the classification of two-dimensional (real) manifolds, any compact orientable connected two-dimensional manifold is homeomorphic to a sphere with handles. The number of handles, \(g\), is called the genus, a topological invariant. Thus every compact Riemann surface, being a compact orientable connected one-dimensional complex manifold, has an associated genus.

**Definition.** Let \(X\) and \(Y\) be compact Riemann surfaces with \(\{(U_i, z_i)\}\) and \(\{(V_a, w_a)\}\) be their respective holomorphic coordinate coverings. A holomorphic mapping

\[ f : X \rightarrow Y \]

is a family of continuous mappings

\[ f_i : U_i \rightarrow Y, \]

such that

(i) \(f_i = f_j\) on \(U_i \cap U_j\) for \(U_i \cap U_j \neq \emptyset\); and

(ii) \(w_a \circ f_i \circ z^{-1}\) is a holomorphic function on \(f^{-1}(V_a) \cap U_i\) whenever \(f^{-1}(V_a) \cap U_i \neq \emptyset\).

The degree of \(f\), denoted \(\deg f\), is the number of points in the inverse image of any point in \(Y\), counting multiplicity.

A holomorphic mapping \(f : X \rightarrow Y\) of degree \(d\) is sometimes called a degree \(d\) covering map, and \(X\) is called a \(d\)-sheeted covering (or cover) of \(Y\). The following proposition makes clear why this terminology makes sense.

**Proposition 1.** [M] Let \(X\) and \(Y\) be compact Riemann surfaces. If \(f : X \rightarrow Y\) is a nonconstant holomorphic mapping, then \(f\) is surjective.

**Definition.** An isomorphism between compact Riemann surfaces \(X\) and \(Y\) is a holomorphic mapping \(f : X \rightarrow Y\) which is bijective and whose inverse \(f^{-1} : Y \rightarrow X\) is holomorphic. If there exists an isomorphism between \(X\)
Chapter 1. Background

and $Y$, we say that $X$ and $Y$ are isomorphic, and we write $X \cong Y$.

**Definition.** An isomorphism $f : X \to X$ is called an *automorphism* of $X$. The set of automorphisms of $X$ forms a group denoted by $\text{Aut}(X)$.

The general compact Riemann surface admits only the trivial automorphism. However, when $\text{Aut}(X)$ is nontrivial, we obtain a (nontrivial) group action on $X$; we will elaborate on group actions in later sections.

A result we will apply implicitly is that $\text{Aut}(X)$ is a finite group for every compact Riemann surface $X$ of genus $g \geq 2$. This can be proven by considering a finite set of special points on $X$ called *Weierstrass points* which every automorphism must permute. The famous bound $|\text{Aut}(X)| \leq 84(g-1)$ is Hurwitz's Theorem. A detailed proof can be found in [Fa].

1.1.1 Meromorphic Functions

**Definition.** A holomorphic mapping $f : X \to \mathbb{P}^1$ is called a *meromorphic function* on $X$, or simply a *function* on $X$. The field of meromorphic functions on $X$, also called the *function field* of $X$, is denoted by $\mathbb{C}(X)$.

Let $f : X \to Y$ be a degree $d$ covering map. For $g \in \mathbb{C}(Y)$ we define $f^*(g) = g \circ f$ by the following commutative diagram:

$$
\begin{array}{ccc}
X & \xrightarrow{f} & Y \\
\downarrow{f^*(g)} & & \downarrow{g} \\
\mathbb{P}^1
\end{array}
$$

Since $g$ is a meromorphic function on $Y$, then the diagram shows that $g \circ f$ is a meromorphic function on $X$. We now have a map

$$
f^* : \mathbb{C}(Y) \to \mathbb{C}(X)
$$

$$
g \mapsto f^*(g) = g \circ f,
$$

and $f^*$ is called the *pullback* of $f$. We can easily check that $f^*$ is a ring homomorphism and is in fact a $\mathbb{C}$-algebra homomorphism.

Since $f$ is surjective, then $f$ induces an injective pullback $f^*$. This shows that $\mathbb{C}(X)$ is a finite algebraic field extension over $\mathbb{C}(Y)$ of degree $d$. 

3
Chapter 1. Background

The field of meromorphic functions on $\mathbb{P}^1$ is isomorphic to the function field in one variable $x$ over $\mathbb{C}$. In other words,

$$\mathbb{C}(\mathbb{P}^1) \cong \mathbb{C}(x).$$

Thus, if $f : X \to \mathbb{P}^1$ is a meromorphic function on $X$ of degree $d$, then $\mathbb{C}(X)$ is a finite algebraic field extension over $\mathbb{C}(x)$ of degree $d$. As every finite extension over a field of characteristic zero is separable, then there is an algebraic element $y$ such that $\mathbb{C}(X) = \mathbb{C}(x, y)$, and the minimal polynomial of $y$ over $\mathbb{C}(x)$ has degree $d$.

**Definition.** Let $X$ be a compact Riemann surface, $P \in X$, and $f$ a nonzero meromorphic function on $X$. By choosing a local coordinate $z$ in a neighbourhood of $P$ such that $z(P) = 0$, we have that in a neighbourhood of $P$,

$$f = z^\nu h(z), \quad \nu \in \mathbb{Z},$$

where $h(z)$ is a holomorphic function satisfying $h(0) \neq 0$. For any local coordinate $z$ such that $z(P) = 0$, the value of $\nu$ is the same and uniquely determined by $f$. This $\nu$ is called the *order* or *multiplicity* of $f$ at $P$, denoted $\nu_P(f)$.

When $\nu_P(f) > 0$, $P$ is called a zero of $f$ and $\nu_P(f)$ is the order of the zero $P$. When $\nu_P(f) < 0$, $P$ is called a pole of $f$ and $|\nu_P(f)|$ is the order of the pole $P$.

The ring $\mathcal{O}_{X,P} = \{f \in \mathbb{C}(X) : \nu_P(f) \geq 0\}$ is an example of a discrete valuation ring of $\mathbb{C}(X)$. Using discrete valuation rings, we can construct a categorical equivalence between finite extensions of fields of transcendence degree one over $\mathbb{C}$ and compact Riemann surfaces. We will not explicitly need this equivalence here, and so the reader is referred to [Fu].

### 1.1.2 Meromorphic Differentials

**Definition.** A meromorphic (respectively, holomorphic) differential on an open set $V \subset \mathbb{C}$ is an expression $\omega$ of the form

$$\omega = f(z)dz$$

where $f$ is a meromorphic (resp. holomorphic) function on $V$. We say that $\omega$ is a meromorphic (resp. holomorphic) differential in the coordinate $z$.

A meromorphic (resp. holomorphic) differential $\omega$ on a Riemann surface $X$ is a family of meromorphic (resp. holomorphic) differentials $\{\omega_i\}$ such that
Chapter 1. Background

(i) if \( \{(U_i, z_i)\} \) is a holomorphic coordinate covering of \( X \), then

\[
\omega_i = f_i(z_i)dz_i,
\]

where \( f_i \) is a meromorphic (resp. holomorphic) function on \( z_i(U_i) \subset \mathbb{C} \); and

(ii) if \( z_i = \varphi_{ij}(z_j) \) is the coordinate transformation on \( U_i \cap U_j \neq \emptyset \), then the local representation of the differential changes by

\[
f_i(\varphi_{ij}(z_j))d\varphi_{ij}(z_j) = f_j(z_j)dz_j,
\]

which is the chain rule.

The set of meromorphic differentials on \( X \) is denoted by \( \Omega^1(X) \).

**Definition.** Let \( X \) be a compact Riemann surface with \( \{(U_i, z_i)\} \) a holomorphic coordinate covering of \( X \) and \( \omega \) meromorphic differential on \( X \). If \( P \in U_i \cap U_j \), then

\[
\nu_P(f_i) = \nu_P \left( f_i(\varphi_{ij}(z_j)) \frac{d\varphi_{ij}(z_j)}{dz_j} \right) = \nu_P(f_j).
\]

This means we can define

\[
\nu_P(\omega) = \nu_P(f_i), \quad P \in U_i.
\]

If \( \nu_P(\omega) > 0 \), then \( P \) is called a zero of \( \omega \). If \( \nu_P(\omega) < 0 \), then \( P \) is called a pole of \( \omega \).

1.2 Projective Curves

**Definition.** Let \( V \) be a finite dimensional vector space over \( \mathbb{C} \). Consider the equivalence relation \( \sim \) on \( V \setminus \{0\} \): \( u \sim v \) if and only if there exists a \( \lambda \in \mathbb{C}^* \) with \( u = \lambda v \). The projective space associated to \( V \) is defined by

\[
\mathbb{P}(V) := V \setminus \{0\} / \sim.
\]

The dimension of \( \mathbb{P}(V) \) is defined by \( \dim \mathbb{P}(V) := \dim V - 1 \).

Geometrically, two vectors are equivalent (under \( \sim \)) if and only if they span the same line in \( V \). Thus the projective space associated to \( V \) is the set of all lines through the origin (one-dimensional subspaces) in \( V \).
Examples. (a) The projective line is defined to be $\mathbb{P}(\mathbb{C}^2)$, the projective space associated to $\mathbb{C}^2$. We denote the equivalence class map by

$$\pi : \mathbb{C}^2 \setminus \{(0,0)\} \to \mathbb{P}(\mathbb{C}^2).$$

We write

$$(x : y) := \pi((x, y)) \in \mathbb{P}(\mathbb{C}^2),$$

and call $(x : y)$ the homogeneous coordinates of the point $\pi((x, y))$.

By defining the map

$$\mathbb{P}(\mathbb{C}^2) \to \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$$

$$(x : y) \mapsto \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ \infty & \text{if } y = 0 \end{cases}$$

we see that $\mathbb{P}(\mathbb{C}^2)$ is equivalent to $\mathbb{C} \cup \{\infty\}$, which justifies the notation $\mathbb{P}^1$. The point $(1 : 0)$ is called the point at infinity.

(b) The projective plane $\mathbb{P}^2$ is defined to be the projective space associated to $\mathbb{C}^3$. That is,

$$\mathbb{P}^2 = \mathbb{P}(\mathbb{C}^3).$$

As in the previous example, $(x : y : z)$ are the homogeneous coordinates of the point $\pi((x, y, z)) \in \mathbb{P}^2$. The set

$$L_\infty = \{(x : y : z) \in \mathbb{P}^2 : z = 0\}$$

is called the line at infinity.

Definition. A projective plane curve $X \subset \mathbb{P}^2$ is defined as

$$X = \{(x : y : z) : F(x, y, z) = 0\},$$

for some nonconstant homogeneous polynomial $F$ in three variables over $\mathbb{C}$. The degree of $X$ is the degree of the defining homogeneous polynomial. If we restrict to $\mathbb{C}^2 = \mathbb{P}^2 \setminus L_\infty$, then $X$ satisfies the affine equation

$$f(x, y) = 0,$$

where

$$f(x, y) = F(x, y, 1).$$
Chapter 1. Background

A projective plane curve is irreducible if its defining homogeneous polynomial is irreducible.

**Definition.** Let $X$ be a projective plane curve. A rational function $f : X \to \mathbb{P}^1$ on $X$ is a quotient of homogeneous polynomials of the same degree:

$$f(x, y, z) = \frac{g(x, y, z)}{h(x, y, z)}$$

with $\deg g = \deg h$, and $h$ is not identically zero on $X$. The field of rational functions, also called the function field of $X$, is denoted by $\mathbb{C}(X)$.

As the notation suggests, it transpires that the function field of a projective plane curve and that of a compact Riemann surface are identical.

**Definition.** Let $X$ be a projective plane curve defined by the homogeneous polynomial $F(x, y, z)$. We say a point $P \in X$ is singular (or $P$ is a singularity of $X$) if

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

A smooth point on $X$ is one that is not singular. If every point on $X$ is smooth, then $X$ is a smooth or nonsingular curve.

Any projective curve has at most finitely many singular points (see [Hu]).

**Definition.** Let $X$ be a projective plane curve defined by the homogeneous polynomial $F(x, y, z)$. We call a point $P \in X$ a double point of $X$ if all of the first partials of $F$ vanish at $P$ but not all of the second partials. At these points, $X$ has two tangent lines at $P$, either intersecting or one tangent counted with multiplicity. If the tangent lines are distinct, then $P$ is called an ordinary double point of $X$.

We can similarly define triple points and, even more generally, $k$-tuple points, but we will not need them for our purposes. Ordinary double points are the simplest and most "well behaved" singularities.

Let $X$ and $Y$ be projective plane curves of degrees $d$ and $e$, respectively. The intersection number of $X$ and $Y$, denoted $X \cdot Y$, is the number of points in $X \cap Y$, counting multiplicity. If $X$ and $Y$ do not share a common component – that is the defining homogeneous polynomials of $X$ and $Y$ do not
have a common irreducible factor — then $X \cdot Y = de$. This is known as Bézout’s Theorem (see [Hu]).

For a more general definition of intersection number, see [Ha, Chapter V].

### 1.3 Normalization

There is a startling and beautiful connection between projective plane curves and Riemann surfaces. An important result is that every smooth projective plane curve is a compact Riemann surface. In this section, we will see that every irreducible projective plane curve has a compact Riemann surface associated to it, and thus we establish a categorical equivalence. An extensive treatment of normalization can be found in [Gr].

**Definition.** Suppose $X$ is an irreducible projective plane curve, and $S$ its set of singular points. If there exists a compact Riemann surface $X'$ and a holomorphic mapping

$$\sigma : X' \to \mathbb{P}^2,$$

such that

(i) $\sigma(X') = X$;

(ii) $\sigma^{-1}(S)$ is a finite set; and

(iii) $\sigma : X' \setminus \sigma^{-1}(S) \to X \setminus S$ is injective,

then we call $(X', \sigma)$ the *normalization* of $X$.

Note that if $X$ is a smooth projective plane curve, then $X$ itself along with the identity mapping is a normalization of $X$.

If $(X', \sigma)$ is a normalization of $X$, we often (by abuse of terminology) say that $X'$ is a normalization of $X$, leaving the map $\sigma$ implicit.

**Theorem 1.** [Gr] *For any irreducible projective plane curve $X \subset \mathbb{P}^2$, there exists a normalization of $X$. Moreover, the normalization is unique: if $(X', \sigma)$ and $(\tilde{X}, \tilde{\sigma})$ are normalizations of $X$, then there exists an isomorphism*

$$\tau : X' \to \tilde{X}$$
such that the diagram

\[
\begin{array}{c}
X' \\
\sigma
\end{array}
\xrightarrow{\gamma}
\begin{array}{c}
\tilde{X} \\
\tilde{\sigma}
\end{array}
\xrightarrow{\sigma}
\begin{array}{c}
X
\end{array}
\]

commutes.

**Theorem 2.** [Gr] Any compact Riemann surface $X'$ can be obtained through the normalization of a certain projective plane curve $X$ with at most ordinary double points. That is, there exists a holomorphic mapping $\sigma : X' \to \mathbb{P}^2$ such that $\sigma(X')$ is a projective curve possessing at most ordinary double points.

With these two theorems working in the background, we will let $X$ be a compact Riemann surface or, equivalently, a smooth projective curve for the remainder of the paper. Given this we can always use a homogeneous polynomial to define our compact Riemann surfaces. Nevertheless, for ease of computation and notation, we often write the algebraic equation in affine coordinates, even if the curve defined this way is singular. The curve we are actually interested in is often the normalization of the curve we actually write down! We simply verify (when necessary) that the singular points in the affine model do not affect our computations after we normalize the curve.

Two projective plane curves $X$ and $Y$ are *birationally isomorphic* if their respective normalizations $X'$ and $Y'$ are isomorphic. This implies that birationally isomorphic curves have isomorphic function fields ($\mathbb{C}(X) \cong \mathbb{C}(Y)$), and there is a unique nonsingular curve (in the sense that normalizations are unique), with an isomorphic function field. It is this nonsingular model with which we work.

### 1.4 Divisors

Divisors are a way of encoding information about zeros and poles of functions and differentials. The beautiful and powerful Riemann-Roch Theorem is a statement which allows us to determine how many linearly independent functions (or differentials) there are on a compact Riemann surface with prescribed zeros and poles.
Chapter 1. Background

Definition. A divisor $D$ of $X$ is a formal finite sum

$$D = m_1P_1 + \cdots + m_nP_n = \sum_{i=1}^{n} m_iP_i,$$

where $m_i \in \mathbb{Z}$ and $P_i \in X$, $i = 1, \ldots, n$. The degree of $D$ is defined as

$$\deg D = \sum_{i=1}^{n} m_i.$$

The support of $D$ is the set $\text{Supp}(D)$ of points in $X$ which have nonzero coefficients in $D$.

The set of all divisors of $X$ forms an abelian group $\text{Div}(X)$ under the obvious addition of divisors.

There is a partial ordering on $\text{Div}(X)$. For divisors $D_1 = \sum n_P P$ and $D_2 = \sum m_P P$, we write

$$D_1 \geq D_2 \text{ if and only if } n_P \geq m_P \text{ for all } P \in X.$$

A divisor $D$ is effective if $D \geq 0$.

Definition. Let $f$ be a nonzero meromorphic function on $X$. The divisor of $f$, denoted $(f)$, is the divisor of the form

$$(f) = \sum_{P \in X} \nu_P(f)P.$$

Divisors of this form are called principal divisors.

Definition. Two divisors $A$ and $D$ are said to be linearly equivalent if their difference is a principal divisor, that is,

$$A - D = (f) \text{ for some } f \in \mathcal{C}(X).$$

This equivalence relation is denoted by $A \sim D$.

Since every nonzero meromorphic function has the same number of zeros as poles, we have that every principal divisor has degree 0.

If two divisors are linearly equivalent, then they have the same degree. On $\mathbb{P}^1$, the converse is also true. That is, every divisor on $\mathbb{P}^1$ of degree 0 is a principal divisor.
Chapter 1. Background

**Definition.** Let \( \omega \) be a nonzero meromorphic differential on \( X \). The *divisor of \( \omega \), denoted \( (\omega) \), is the divisor of the form

\[
(\omega) = \sum_{P \in X} \nu_P(\omega)P.
\]

Divisors of this form are called *canonical divisors.*

All canonical divisors on a compact Riemann surface \( X \) are linearly equivalent, so we are often able to consider the canonical divisor class

\[
K := (\omega) \in \text{Div}(X)/\sim
\]

without specifying the differential \( \omega \). Abusing notation, we often say \( K \) is a canonical divisor, though it is in fact an equivalence class.

**Definition.** For a divisor \( D \) on \( X \), define

\[
L(D) = \{0 \neq f \in \mathbb{C}(X) : (f) \geq -D\} \cup \{0\}.
\]

This is a vector space over \( \mathbb{C} \). We denote the dimension by

\[
\ell(D) := \dim L(D).
\]

**Definition.** The *complete linear series of \( D \) is defined as

\[
|D| = \{E \in \text{Div}(X) : E \sim D \text{ and } E \geq 0\}.
\]

It is not difficult to see that there is a natural bijection between the complete linear series \( |D| \) and the projective space \( \mathbb{P}(L(D)) \).

**Definition.** For a divisor \( D \) on \( X \), define

\[
\Omega(D) = \{\omega \in \Omega^1(X) : (\omega) \geq D\} \cup \{0\}.
\]

This is also a vector space over \( \mathbb{C} \), and we denote the dimension by

\[
i(D) := \dim \Omega(D).
\]

**Proposition 2.** [Fu] Let \( K \) be a canonical divisor on \( X \). Then for any divisor \( D \) on \( X \),

\[
i(D) = \ell(K - D).
\]
Theorem (Riemann-Roch). [Fu] If $X$ is a compact Riemann surface of genus $g$ and $D$ is a divisor of degree $d$ on $X$, then

$$\ell(D) - \ell(K - D) = d + 1 - g.$$ 

Corollary 1. If $X$ is a compact Riemann surface of genus $g$, then there are $g$ linearly independent holomorphic differentials on $X$. That is, if $K$ is a canonical divisor, then

$$\ell(K) = g.$$ 

Corollary 2. Let $K$ be any canonical divisor on a compact Riemann surface of genus $g$. Then $\deg K = 2g - 2$.

1.4.1 Special Divisors

As an application of the Riemann-Roch Theorem, we consider special divisors and prove Clifford’s Theorem.

Definition. An effective divisor $D$ on $X$ is a special divisor if

$$\ell(D) > 1 \quad \text{and} \quad \ell(K - D) > 1.$$ 

Remark 1. Note that if $D$ is an effective divisor of degree $d < g - 1$, then the Riemann-Roch Theorem gives

$$\ell(D) - \ell(K - D) = d + 1 - g < 0,$$

so $1 < \ell(D) \leq \ell(K - D)$. This shows that any effective divisor of degree $d \leq g - 1$ is a special divisor. In particular, when $d = g - 1$, we have $\ell(D) = \ell(K - D)$.

Proposition 3. An effective divisor $D$ on $X$ is a special divisor if and only if there exists an effective divisor $E$ such that $D + E$ is a canonical divisor on $X$. The divisor $E$ is called a complementary divisor of $D$.

Proof. Let $D$ be a special divisor on $X$. Consider the complete linear series $|K - D| = \{E \in \text{Div}(X) : E \sim K - D \text{ and } E \geq 0\}$. Since $|K - D|$ is in one-to-one correspondence with $\mathbb{P}(L(K - D))$, then

$$\dim |K - D| = \ell(K - D) - 1 \geq 0.$$ 

In particular, $|K - D|$ is nonempty, and hence there exists $E \in \text{Div}(X)$ with $E \geq 0$ such that $E \sim K - D$ or, equivalently, $D + E \sim K$.

Conversely, if there exists an effective divisor $E$ such that $D + E = K$ is canonical, then $\ell(K - D) = \ell(E) \geq 1$. \qed
Chapter 1. Background

Theorem (Clifford). If $D$ is a special divisor on a curve of genus $g \geq 2$, then

$$\ell(D) \leq \frac{1}{2} \deg D + 1.$$ 

Proof. Let $K$ be a canonical divisor, which we can choose to be effective (since $g \geq 2$). We may assume $\ell(D - P) \neq \ell(D)$ for every $P \in X$, since otherwise we can work with $D - P$ and get a better estimate. By Proposition 3, there is an effective divisor $E$ such that $D + E = K$, so in particular $E = K - D \geq 0$. Since $D$ and $K - D$ are effective, then $L(0)$ is a subspace of $L(K - D)$, and $L(D)$ is a subspace of $L(K)$. Choose $h \in L(D)$ such that $h \notin L(D - P)$ for any $P \in \text{Supp}(K - D)$. Consider the linear transformation

$$T : L(K - D)/L(0) = L(K)/L(D) \quad \tilde{f} = \tilde{f}h.$$ 

By our choice of $h$, we see that $T$ is injective, so

$$\dim(L(K - D)/L(0)) \leq \dim(L(K)/L(D)),$$

or equivalently, $\ell(K - D) - 1 \leq g - \ell(D)$. Thus

$$\ell(D) + \ell(K - D) \leq g + 1.$$ 

By the Riemann-Roch Theorem,

$$\ell(D) - \ell(K - D) = \deg D + 1 - g.$$ 

Adding the two expressions gives

$$2 \ell(D) \leq \deg D + 2,$$

which yields the result. \qed

1.5 The Riemann-Hurwitz Formula

The main tool from the background is the Riemann-Hurwitz Formula. We will apply this repeatedly in our proofs.

Definition. Let $f : X \to Y$ be a nonconstant holomorphic mapping with $P \in X$. If $z$ is a local coordinate in a neighbourhood of $f(P)$ such that
Chapter 1. Background

\[ z(f(P)) = 0, \text{ then } g := z \circ f : X \to \mathbb{P}^1 \text{ is a meromorphic function on } X. \] We define the \textit{multiplicity} of \( f \) at \( P \), denoted \( \nu_P(f) \), as

\[ \nu_P(f) := \nu_P(g). \]

This is independent of the choice of local coordinate.

When \( Y = \mathbb{P}^1 \), this is equivalent to the notation defined earlier for meromorphic functions.

**Definition.** Let \( f : X \to Y \) be a nonconstant holomorphic mapping. A point \( P \in X \) is called a \textit{ramification point} of \( f \) if \( \nu_P(f) > 1 \). A point \( Q \in Y \) is called a \textit{branch point} of \( f \) if it is the image of a ramification point of \( f \). We say \( f \) is \textit{unramified} if \( f \) has no ramification points.

For any nonconstant holomorphic mapping \( f \), the set of ramification points is finite. Consider

\[ R = \sum_{P \in X} (\nu_P(f) - 1)P. \]

Note that for \( P \in X \) such that \( \nu_P(f) = 1 \), the coefficient of \( P \) in \( R \) is zero. Thus we can consider \( R \) as a sum over only the ramification points of \( f \), which implies that \( R \) is a finite sum. Hence \( R \in \text{Div}(X) \). We call \( R \) the \textit{ramification divisor} of \( f \).

**Theorem (Riemann-Hurwitz Formula).** [Gr] Let \( X \) be a compact Riemann surface of genus \( g_X \), and \( Y \) be a compact Riemann surface of genus \( g_Y \). Let \( f : X \to Y \) be a nonconstant holomorphic mapping with \( \deg f = n \), and let \( R \) denote the ramification divisor of \( f \). Then

\[ 2g_X - 2 = (2g_Y - 2)n + \deg R. \]

1.6 Group Actions

**Definition.** Let \( H \) be a finite group and \( X \) a compact Riemann surface. An \textit{action} of \( H \) on \( X \) is a map \( H \times X \to X \), which we write as \( (h, P) \mapsto hP \), such that

(i) \( (h_1h_2)P = h_1(h_2P) \) for \( h_1, h_2 \in H \) and \( P \in X \), and

(ii) \( 1P = P \) for \( P \in X \), where \( 1 \in H \) is the identity element.
The *orbit* of a point $P \in X$ is the set

$$\text{Orb}(P) = \{hP : h \in H\}.$$ 

The *stabilizer* of $P$ is the subgroup

$$\text{Stab}(P) = \{h \in H : hP = P\}.$$ 

The *kernel* of the action of $H$ on $X$ is the subgroup

$$K = \{h \in H : hP = P \text{ for all } P \in X\}.$$ 

If $K$ is trivial, then the action is called *faithful*.

By fixing $h \in H$, the map which sends $P$ to $hP$ is a bijection. If for every $h \in H$, this bijection is a holomorphic mapping from $X$ to itself, then $H$ is a group of automorphisms acting on $X$.

The *quotient space* $X/H$ is the set of orbits. We have nice structure when $H$ is a group of automorphisms of $X$, as the following results show.

**Theorem 3.** [M] Let a finite group $H \leq \text{Aut}(X)$ act faithfully on a compact Riemann surface $X$. Then $X/H$ is a compact Riemann surface. In addition, the map $\pi$ which sends $P \to \text{Orb}(P)$ is a holomorphic mapping from $X \to X/H$ of degree $|H|$, and $\nu_P(\pi) = |\text{Stab}(P)|$ for any point $P \in X$.

**Proposition 4.** [M] Let a finite group $H \leq \text{Aut}(X)$ act faithfully on $X$. Then $\text{Stab}(P)$ is cyclic for every $P \in X$.

### 1.6.1 Galois Coverings

We finally arrive at defining our main objects of study, prime Galois coverings. Though we define the coverings over general compact Riemann surfaces, we will restrict to the case where $X$ is a prime Galois covering of $\mathbb{P}^1$ throughout the rest of the paper.

**Definition.** A compact Riemann surface $X$ is a *Galois covering* of $Y$ if there exists an automorphism $\tau \in \text{Aut}(X)$ such that $X/\langle \tau \rangle \cong Y$. If $\tau$ has order $d$ in $\text{Aut}(X)$, then the Galois covering is *$d$-sheeted*.

When $d$ is prime, then we say $X$ is a *prime Galois covering* of $Y$ (and we use $p$ instead of $d$ to denote prime).
Chapter 1. Background

The terminology "d-sheeted Galois covering" makes sense. Indeed, the natural projection \( \pi : X \to X/\langle \tau \rangle \) is a holomorphic mapping of degree \( d \). Furthermore, if \( X \) is a Galois covering of \( Y \), then the function field \( \mathbb{C}(X) \) is a Galois extension of \( \mathbb{C}(Y) \).

We see immediately that the ramification points of \( \pi \) are precisely the fixed points of \( \tau \).

A natural question which arises when studying Galois coverings is whether the automorphism \( \tau \) unique. That is, if there exists \( \sigma \in \text{Aut}(X) \) with \( |\sigma| = |\tau| \) such that \( X/\langle \sigma \rangle \cong X/\langle \tau \rangle \), is \( \sigma = \tau \)? In this section, we will see that when \( |\tau| = 2 \) and \( X/\langle \tau \rangle \cong \mathbb{P}^1 \), then our question is answered in the affirmative for every such \( X \). It is this special case that we use as motivation for studying prime Galois coverings of \( \mathbb{P}^1 \) for general (odd) primes.

**Definition.** A compact Riemann surface \( X \) of genus \( g \geq 2 \) is hyperelliptic if it is a 2-sheeted Galois covering of \( \mathbb{P}^1 \). Thus there exists an automorphism \( \tau \in \text{Aut}(X) \) of order 2 such that \( X/\langle \tau \rangle \cong \mathbb{P}^1 \). The automorphism \( \tau \) is called the hyperelliptic involution.

A quick application of the Riemann-Hurwitz Formula shows that the hyperelliptic involution has \( 2g + 2 \) fixed points. Moreover, the Riemann-Hurwitz Formula also implies that any involution on \( X \) which has \( 2g + 2 \) fixed points must yield a quotient of \( \mathbb{P}^1 \). The following theorem says there actually are no other such involutions.

**Theorem 4.** [Fa] The hyperelliptic involution \( \tau \) on a (hyperelliptic) compact Riemann surface \( X \) of genus \( g \geq 2 \) is the unique involution on \( X \) with \( 2g + 2 \) fixed points.

Through suitable change of coordinates, any hyperelliptic compact Riemann surface can be described by (the normalization of) the affine equation

\[
y^2 = f(x),
\]

where the hyperelliptic involution sends the point \((x, y)\) to \((x, -y)\).

More generally, a prime Galois covering of \( \mathbb{P}^1 \) admits the affine equation

\[
y^p = f(x),
\]

and the automorphism \( \tau \in \text{Aut}(X) \) of prime order \( p \) sends \((x, y)\) to \((x, \zeta_p y)\) for a primitive \( p \)-th root of unity \( \zeta_p \). The natural projection \( X \to X/\langle \tau \rangle \) sends \((x, y)\) to \( x \).
Chapter 2

Prime Galois Coverings of $\mathbb{P}^1$

The appeal of hyperelliptic compact Riemann surfaces is that the groups of automorphisms are (in theory) easy to compute for these surfaces. Indeed, if $X$ is a hyperelliptic compact Riemann surface and $\tau$ is the hyperelliptic involution, then we have a central extension

$$1 \rightarrow \langle \tau \rangle \rightarrow \text{Aut}(X) \rightarrow H \rightarrow 1,$$

where $H = \text{Aut}(X)/\langle \tau \rangle$ is a finite group of automorphisms acting on $\mathbb{P}^1$. The finite automorphism groups which act on $\mathbb{P}^1$ have been completely classified (see [Sh]): they are cyclic, dihedral, $A_4$, $S_4$, and $A_5$.

In a similar way, we wish to classify all groups which act as automorphisms on prime Galois coverings of $\mathbb{P}^1$. Ideally, we hope for a unique automorphism $\tau$ of order $p$ such that $X/\langle \tau \rangle \cong \mathbb{P}^1$. However, we will see examples of curves which have two distinct automorphisms of prime order which quotient to yield $\mathbb{P}^1$. Fortunately our automorphism $\tau$ is unique once the genus of $X$ is sufficiently large. Moreover, when two distinct automorphisms exist, we can classify the curve up to isomorphism.

2.1 Examples

Example 1. Let $C_p$ be the Fermat curve defined by the equation

$$y^p = x^p - 1.$$  

The groups generated by $\tau_1(x, y) = (x, \zeta_p y)$ and $\tau_2(x, y) = (\zeta_p x, y)$ are distinct, but we see that $\tau_1$ and $\tau_2$ are conjugate via the automorphism $\sigma(x, y) = (y, x)$.

Note there is another automorphism of order $p$ given by $\tau(x, y) = (\zeta_p x, \zeta_p y)$. The group $\langle \tau \rangle$ is also conjugate to $\langle \tau_1 \rangle$ and $\langle \tau_2 \rangle$, since $\phi \circ \tau \circ \phi^{-1} = \tau_2^{-p}$, where $\phi(x, y) = (1/x, -y/x)$.

Example 2. Define the curves $D_p$ by the equation

$$y^p = (x^p - 1)(x^p - \lambda^p)^{p-1},$$
Chapter 2. Prime Galois Coverings of $\mathbb{P}^1$

where $\lambda \in \mathbb{C}$, $\lambda^p \neq 1$. As in the previous example, let $\tau_1(x, y) = (x, \zeta_p y)$ and $\tau_2(x, y) = (\zeta_p x, y)$. The automorphism

$$\sigma(x, y) = \left( \frac{x^p - \lambda^p}{y}, \frac{x^{p-1}(1 - \lambda^p)}{x^p - 1} \right)$$

conjugates $\langle \tau_1 \rangle$ and $\langle \tau_2 \rangle$ since $\sigma \circ \tau_1 \circ \sigma^{-1} = \tau_2^{p-1}$.

**Example 3.** Let $X$ be the curve defined by the equation

$$y^p = (x^p - 1)(x^p - \lambda^p)^k,$$

for $\lambda^p \neq 1, k < p - 1$. In this case, $\tau_1(x, y) = (x, \zeta_p y)$ has $2p$ fixed points, which are given by $(\zeta_p^i, 0), (\zeta_p^i \lambda, 0), i = 1, \ldots, p$. Meanwhile, $\tau_2(x, y) = (\zeta_p x, y)$ has $p$ fixed points, given by $(0, \zeta_p^i \lambda), i = 1, \ldots, p$, which implies $\tau_1$ and $\tau_2$ are not conjugate.

Note that the affine equation for $X$ has a singularity at $\infty$. To show that $\infty$ is not fixed by $\tau_2$, we consider the natural projection $X \to X/\langle \tau \rangle \cong \mathbb{P}^1$ that sends $(x, y)$ to $x$. By taking the parameter $x = \frac{t}{1}$, where $t$ is a local parameter near 0, we see that $X$ has $p$ points $\infty_i, i = 1, \ldots, p$, above $\infty \in \mathbb{P}^1$ explicitly given by the $p$ roots

$$y = \zeta_p^i \sqrt{(1 - t)^p(1 - \lambda^p)^p} t^{1+k},$$

$i = 1, \ldots, p$. These points are not fixed by the action of $\tau_2$. Thus we are able to work with the normalization of $X$ and our analysis remains the same.

By construction $X/\langle \tau_1 \rangle \cong \mathbb{P}^1$, so the Riemann-Hurwitz Formula tells us that $X/\langle \tau_2 \rangle \not\cong \mathbb{P}^1$ since the number of fixed points of $\tau_2$ is different from that of $\tau_1$.

**Remark 2.** Suppose $X$ has an algebraic equation

$$y^p = (x - a_1)^{d_1} (x - a_2)^{d_2} \cdots (x - a_n)^{d_n},$$

where $1 \leq d_i \leq p - 1$. Consider the parameter

$$z = y^s (x - a_1)^{t_1} (x - a_2)^{t_2} \cdots (x - a_n)^{t_n},$$

for some choice of $s, t_i \neq 0 \pmod{p}$, $i = 1, \ldots, n$. One easily checks that $C(x, z) = C(x, y)$ and so $z$ is a valid change of variables. Then

$$z^p = y^{sp}(x - a_1)^{pt_1} (x - a_2)^{pt_2} \cdots (x - a_n)^{pt_n} = (x - a_1)^{sdt_1} \cdots (x - a_n)^{sdt_n} = (x - a_1)^{sdt_1 + pt_1} \cdots (x - a_n)^{sdt_n + pt_n}.$$
Chapter 2. Prime Galois Coverings of \( \mathbb{P}^1 \)

In particular, since \( \gcd(d_i, p) = 1 \), we can choose \( s \) and \( t \) such that

\[
sd_1 + pt_1 = 1.
\]

Once we fix \( s \), we then choose the \( t_i \) such that \( 1 \leq sd_i + pt_i \leq p - 1 \), for \( i = 2, \ldots, n \). This computation shows that we can always assume one branch point has multiplicity 1.

Moreover, we see that if \( \sum_{i=1}^n d_i \equiv 0 \pmod{p} \), then

\[
\sum_{i=1}^n sd_i + pt_i \equiv \sum_{i=1}^n sd_i \equiv s \sum_{i=1}^n d_i \equiv 0 \pmod{p}.
\]

2.2 Preliminaries

The argument used to prove the following lemma is a slight generalization of the proof of [P, Lemma 5].

**Lemma 1.** Let \( X, X_1, X_2 \) be smooth curves of genus \( g, g_1, g_2 \) respectively. If \( \sigma_1: X \to X_1 \) and \( \sigma_2: X \to X_2 \) are (possibly ramified) covers of the same prime degree \( p \) and \( g \geq p^2 + (g_1 + g_2 - 2)p + 2 \) then there is an isomorphism \( \alpha: X_1 \to X_2 \) such that the diagram

\[
\begin{array}{c}
\xymatrix{ X \ar[rr]^\sigma_1 \urddr_{\sigma_2} & & \ar[d] X_2 \\
X_1 & & X_2 \\
} \\
\end{array}
\]

commutes.

Note that here the covers \( \sigma_1 \) and \( \sigma_2 \) are not assumed to be Galois.

**Proof.** Let \( Y \) be the image of the map

\[ X \xrightarrow{(\sigma_1, \sigma_2)} X_1 \times X_2. \]

Denote the degree of \( X \to Y \) by \( s \) and the degree of the projection \( Y \to X_i \) by \( r_i \). Then \( sr_1 = sr_2 = p \), so either

(i) \( s = p \) and \( r_1 = r_2 = 1 \)

or

(ii) \( s = 1 \) and \( r_1 = r_2 = p \).
If (i) holds then $Y$ is the graph of an isomorphism $\alpha$ between $X_1$ and $X_2$, which yields the desired result.

It thus remains to rule out (ii), that is, to show that $s \neq 1$. Assume the contrary. Then $Y$ is birationally isomorphic to $X$ (but possibly singular).

Let $H = X_1 \times \{pt\}$ and $V = \{pt\} \times X_2$. (Here $H$ stands for "horizontal" and $V$ for "vertical"). Then

$$Y \cdot H = r_2 = p, \quad Y \cdot V = r_1 = p.$$ 

An inequality of Castelnuovo and Severi now tells us that

$$X \cdot X \leq 2r_1r_2 = 2p^2;$$ 

see [Ha, Exercise V.1.9]. By the adjunction formula [Ha] we now see that

$$2g-2 \leq X \cdot (X + K) = X \cdot (X + (2g_1 - 2)V + (2g_2 - 2)H) \leq 2p^2 + (2g_1 + 2g_2 - 2)p$$ 

contradicting our assumption on $g$. \hfill $\Box$

**Theorem 5.** Let $X$ be a curve of genus $g$ and $H_1, H_2$ be subgroups of $\text{Aut}(X)$ of prime order $p$. Denote the genus of $X/H_i$ by $g_i$. If

$$g \geq p^2 + (g_1 + g_2 - 2)p + 2$$

then $H_1 = H_2$.

**Proof.** Take $X_i = X/H_i$ and $\sigma_i : X \to X_i$ to be the natural projection. By Lemma 1 there is an isomorphism $\alpha$ between $X_1$ and $X_2$ such that $\alpha \sigma_1 = \sigma_2$.

Let $x \in X$ in general position and $x_i = \sigma_i(x) \in X_i$ for $i = 1, 2$. Then

$$\alpha(x_1) = x_2$$

and

$$\sigma_2^{-1}(x_2) = \sigma_1^{-1}(\alpha^{-1}x_2) = \sigma_1^{-1}(x_1).$$

But in our situation, $\sigma_1^{-1}(x_1)$ is precisely $H_1 \cdot x_1$. In other words, we have $H_1 \cdot x = H_2 \cdot x$ for every $x \in X$. Equivalently, $H_1 = H_2$, as claimed. \hfill $\Box$

**Corollary 3.** Let $X$ be a curve of genus $g \geq p^2 - 2p + 2$. Then there is at most one subgroup $H$ of order $p$ in $\text{Aut}(X)$ such that $X/H \cong \mathbb{P}^1$. In particular, if such a subgroup $H$ exists, it is normal in $\text{Aut}(X)$. 

20
Chapter 2. Prime Galois Coverings of $\mathbb{P}^1$

2.2.1 A Special Case

We briefly consider the specific case where $X$ is a compact Riemann surface of genus 4 that is a 3-sheeted covering of $\mathbb{P}^1$.

**Proposition 5.** Let $X$ be a compact Riemann surface of genus 4. Suppose there exist functions on $X$ of degree 3. Then one of the following conditions holds. Either

(i) There exists a function $f$ of degree 3 on $X$ such that $(f) = A - D$, where $A, D$ are effective and $D + D \sim K$, and any other function of degree 3 on $X$ is a Möbius transformation of $f$; or

(ii) There is no such function, and there are exactly two functions of degree 3 on $X$ which are not Möbius transformations of each other.

**Proof.** [Fa] We first note that $3 = g - 1$, so Remark 3 implies that every divisor $D$ of degree 3 is a special divisor. By Clifford’s Theorem,

$$\ell(D) \leq \frac{5}{2} < 3.$$  

(i): Suppose there exists a function $f$ of degree 3 such that $(f) = A - D$ with $A, D$ effective and $D + D \sim K$. By definition, $f \in L(D)$, so $\ell(D) > 1$. From the preceding comment, we have $1 < \ell(D) < 3$, so $\ell(D) = 2$. Assume there is an effective divisor $D_1 \neq D$ with $\deg D_1 = 3$ and $\ell(D_1) = 2$. (If no such divisor exists, then the only functions of degree 3 on $X$ are constant multiplies of $f$ and (i) is proved.) Let $f_1 \in L(D_1) \setminus \mathbb{C}$. If $D_1$ is linearly equivalent to $D$, then there exists $h \in \mathcal{C}(X)$ such that $(h) + D_1 = D$. Then $L(D) = \langle 1, f \rangle$ and $L(D_1) = \langle h, fh \rangle = \langle 1, f_1 \rangle$. Thus there are constants $a, b, c, d \in \mathbb{C}$ such that

$$1 = afh + bh$$

$$f_1 = cfh + dh$$

so that

$$f_1 = \frac{af + b}{cf + d}.$$  

Now assume $f_1$ is not a Möbius transformation of $f$, which means $D_1$ is not linearly equivalent to $D$. This implies $1, f, f_1, ff_1$ are four linearly independent functions in $L(D + D_1)$. So $\ell(D + D_1) \geq 4$, and by the Riemann-Roch Theorem,

$$\ell(K - D - D_1) = \ell(D + D_1) - \deg(D + D_1) - 1 + g = \ell(D + D_1) - 6 - 1 + 4 \geq 1.$$  

21
Since \( \deg(D + D_1) = 6 \), then \( D + D_1 \) is a canonical divisor. But \( D + D \) is also a canonical divisor, which implies \( D_1 \) is linearly equivalent to \( D \), which contradicts our assumption.

(ii): We now assume that there is no function of degree 3 such that twice the polar divisor of \( f \) is canonical. Let \( f \) be a function of degree 3 so that \( (f) = A - D \). By Remark 1, \( D \) is a special divisor, so Proposition 3 allows us to choose an effective divisor \( D_1 \) of degree 3 such that \( D + D_1 \sim K \). Note that \( D \) and \( D_1 \) are not linearly equivalent. As before, Clifford's Theorem gives \( \ell(D) = 2 \), so Remark 1 and Proposition 2 yield \( \ell(K - D) = i(D) = 2 \). This implies there is a divisor \( D_2 \) of degree 3 such that \( D_2 \neq D_1 \) and \( D + D_2 \sim K \). Choose holomorphic differentials \( \omega_i \) such that \( (\omega_i) = D + D_1 \), \( i = 1, 2 \), and define \( f_1 = \omega_2/\omega_1 \). Since the polar divisor \( D_1 \) of \( f_1 \) is not linearly equivalent to \( D \), then we have constructed a function of degree 3 which is not a Möbius transformation of \( f \).

Let \( E \) denote the polar divisor of a function \( h \) of degree 3, where \( h \) is not a Möbius transformation of \( f \). Then \( 1, f, h, fh \) are four linearly independent functions in \( L(D + E) \). Using the same argument as in Case (i), we have that \( D + E \) is a canonical divisor. If \( \omega \) is a differential such that \( (\omega) = D + E \), then \( \omega \) is a divisor of degree 3 such that \( D_2 \neq D_1 \) and \( D + D_2 \sim K \). Choose holomorphic differentials \( \omega_i \) such that \( (\omega_i) = D + D_1 \), \( i = 1, 2 \), and define \( f_1 = \omega_2/\omega_1 \). Since the polar divisor \( D_1 \) of \( f_1 \) is not linearly equivalent to \( D \), then we have constructed a function of degree 3 which is not a Möbius transformation of \( f_1 \).

Arguing as before, \( h \) is thus a Möbius transformation of \( f_1 \).

Remark 3. We revisit Example 3 and consider the case where \( p = 3 \) and \( k = 1 \). Let \( x : X \rightarrow \mathbb{P}^1 \) denote the projection onto the \( x \)-coordinate. The divisor of this function is given by

\[
(\omega) = (0, \lambda) + (0, \zeta_3 \lambda) + (0, \zeta_5 \lambda) - \infty_1 - \infty_2 - \infty_3 = A - D.
\]

The divisor of the differential \((1/y^2)dx\) is

\[
K = 2 \left( \sum_{i=1}^{3} 2\infty_i - \sum_{i=1}^{3} ((\zeta_3^i, 0) + (\zeta_5^i \lambda, 0)) \right) + \left( 2 \sum_{i=1}^{3} ((\zeta_3^i, 0) + (\zeta_5^i \lambda, 0)) - \sum_{i=1}^{3} 2\infty_i \right)
= \sum_{i=1}^{3} 2\infty_i = 2D = D + D.
\]
Chapter 2. Prime Galois Coverings of $\mathbb{P}^1$

We see that since the canonical divisor $K$ has degree 6, then the genus of $X$ is 4. Since $D$ is the polar divisor of a function of degree 3 on $X$ with $D + D = K$, then by Proposition 5, every function of degree 3 on $X$ is a Möbius transformation of the projection $x$, and hence the covering of $X$ over $\mathbb{P}^1$ is unique.

Remark 4. Proposition 5 also shows that for the curves $D_3$ (Example 2 with $p = 3$), $\langle \tau_1 \rangle$ and $\langle \tau_2 \rangle$ are the only subgroups of order 3 which quotient to $\mathbb{P}^1$. 

23
Chapter 3

The Main Theorem

We prove the following theorem.

**Theorem 6.** [G-D] Let $X$ be a compact Riemann surface of genus $g$. If $\text{Aut}(X)$ has two distinct subgroups $H_1, H_2$ of prime order $p$ such that the quotient $X/H_i$ is isomorphic to $\mathbb{P}^1$, then $H_1$ and $H_2$ are conjugate in $\text{Aut}(X)$. Moreover, $g$ is either $(p - 1)^2$ or $(p - 1)(p - 2)/2$.

3.1 Two Lemmas

**Lemma 2.** Let $\sigma, \tau \in \text{Aut}(X)$ have prime order $p$. Assume that $\sigma$ and $\tau$ commute and $\langle \sigma \rangle \neq \langle \tau \rangle$. Then $\sigma$ permutes the fixed point set of $\tau$, $\text{Fix}(\tau)$, dividing it into a number of orbits of length $p$. In particular, the number of points fixed by $\tau$ is a multiple of $p$.

**Proof.** If $P \in \text{Fix}(\tau)$, then $\sigma \tau(P) = \tau \sigma(P)$ implies

$$\sigma(P), \sigma^2(P), \ldots, \sigma^{p-1}(P) \in \text{Fix}(\tau).$$

Since the stabilizer of any point is cyclic (Proposition 4), then if $P$ is fixed by both $\tau$ and $\sigma$, we have $\langle \sigma \rangle = \langle \tau \rangle$, contradicting our assumption. So $\sigma^i(P) \neq \sigma^j(P) \in \text{Fix}(\tau)$ for $0 \leq i \neq j \leq p - 1$. Thus $P, \sigma(P), \sigma^2(P), \ldots, \sigma^{p-1}(P)$ is an orbit of length $p$, and hence $|\text{Fix}(\tau)|$ is a multiple of $p$. \qed

**Lemma 3.** Let $X$ be of arbitrary genus with commuting automorphisms $\tau, \sigma$ of same prime order $p$ such that $X/\langle \tau \rangle \cong \mathbb{P}^1$ and $\langle \sigma \rangle \neq \langle \tau \rangle$. Then $X$ is isomorphic to the compact Riemann surface defined by an algebraic equation of the form

$$y^p = (x^p - 1)(x^p - \lambda_2^p)^{m_2} \cdots (x^p - \lambda_r^p)^{m_r}$$

where $1, \lambda_r^p, \ldots, \lambda_r^p \in \mathbb{C}$ are all distinct and $1 \leq m_i < p$, for $i = 1, \ldots, r$.

**Proof.** Since $X$ is a $p$-sheeted Galois covering of $\mathbb{P}^1$, $X$ admits an algebraic model of the form

$$y^p = (x - a_1)^{d_1}(x - a_2)^{d_2} \cdots (x - a_n)^{d_n}, \ 1 \leq d_i < p,$$
Chapter 3. The Main Theorem

in which \( r \) is expressed as \( r(x, y) = (x, \zeta_p y) \) and \((a_i, 0), i = 1, \ldots, n\) are the fixed points of \( r \).

Remark 2 allows us to assume \( d_1 = 1 \), and Lemma 2 implies \( n = rp \) for some integer \( r \). Since \( X/\langle \tau \rangle \cong \mathbb{P}^1 \) (the projection \( x \) is the quotient map), then \( \sigma \) induces an automorphism \( \tilde{\sigma} : \mathbb{P}^1 \to \mathbb{P}^1 \) of order \( p \). By normalizing \( x \) so \( 0 \) and \( \infty \) are the fixed points of \( \tilde{\sigma} \) and \( a_1 = 1 \), we can assume that \( \tilde{\sigma} \) is the rotation \( \tilde{\sigma}(x) = \zeta_p \cdot x \) for some \( p \)-th root of unity \( \zeta_p \).

We can number the fixed points of \( \tau \) so that

\[
\{(a_{(k-1)p+1}, 0), \ldots, (a_{kp}, 0)\}, \quad k = 1, \ldots, r
\]

are the \( \sigma \)-orbits given in Lemma 2. Then \( d_{(k-1)p+1} = \cdots = d_{kp} \) and

\[
a_{(k-1)p+2} = \tilde{\sigma}(a_{(k-1)p+1}) = \zeta_p \cdot a_{(k-1)p+1}.
\]

Thus the algebraic model of \( X \) is

\[
y^p = \prod_{i=1}^{p} (x - \zeta_p^i) \prod_{i=1}^{p} (x - \zeta_p^i \lambda_2)^{m_2} \cdots \prod_{i=1}^{p} (x - \zeta_p^i \lambda_r)^{m_r},
\]

as desired.

We also note that \( \sigma \) is necessarily of the form \( \sigma(x, y) = (\zeta_p^s x, \zeta_p^d y) \) for some integer \( 1 \leq j < p \).

3.2 The Crucial Step

**Proposition 6.** Let \( X \) be of arbitrary genus and \( p > 2 \) a prime. Then \( \text{Aut}(X) \) contains a \( p \)-group \( H \) of order \( \geq p^2 \) generated by automorphisms \( \tau_1, \tau_2 \) of prime order \( p \) with \( X/\langle \tau_1 \rangle \cong \mathbb{P}^1 \) if and only if \( X \) is isomorphic to one of the following curves:

\( C_p : y^p = x^p - 1 \),

\( D_p : y^p = (x^p - 1)(x^p - \lambda^p)^{p-1}, \) for some \( \lambda \in \mathbb{C}, \lambda^p \neq 1. \)

Moreover, in both cases, \( H \) is the group of order \( p^2 \) consisting of automorphisms of the form

\[
\tau(x, y) = (\zeta_p^s x, \zeta_p^d y) \quad \text{with} \quad 1 \leq s, d \leq p.
\]

**Proof.** Since \( p \)-groups have nontrivial centre, there exists \( \sigma \in H \) of order \( p \) commuting with \( \tau_1 \) and \( \tau_2 \). By Lemma 3, \( X \) has the form

\[
y^p = (x^p - 1)(x^p - \lambda_2^p)^{m_2} \cdots (x^p - \lambda_r^p)^{m_r}
\]
with $\tau_1(x, y) = (x, \zeta_p y)$ and $\sigma(x, y) = (\zeta_p^* x, \zeta_p^* y)$.

We want to show that $\tau_2$ has at most $2p$ fixed points. Suppose otherwise. Then $\tau_2$ has more than $2p$ fixed points. Consider $x \circ \tau_2 : X \to \mathbb{P}^1$, where $x : X \to X/\langle \tau_1 \rangle \cong \mathbb{P}^1$ is the projection map. Since $x$ has degree $p$, then the Riemann-Hurwitz Formula gives

$$g > (p - 1)(2p - 2)/2 = p^2 - 2p + 1.$$ 

By Corollary 3, this means that there is at most one subgroup of $\text{Aut}(X)$ of order $p$ such that the quotient space is $\mathbb{P}^1$. This is a contradiction since $\langle \tau_1 \rangle \neq \langle \tau_2 \rangle$. Thus $\tau_2$ has at most $2p$ fixed points.

The Riemann-Hurwitz Formula is the same for $\tau_1$ and $\tau_2$, so both have the same number of fixed points. By Lemma 2, $\tau_1$ has either $p$ or $2p$ fixed points, so $X$ is of one of the following forms:

- $C_p : y^p = x^p - 1$,
- $D^k_p : y^p = (x^p - 1)(x^p - \lambda)^k$.

At this point, we split into two cases, the case where $p = 3$ and the case where $p > 3$. We first assume $p > 3$. We claim that $H = \langle \tau_1, \sigma \rangle$, meaning $\tau_2 \in \langle \tau_1, \sigma \rangle$. Suppose the contrary. Then $\tau_1$ and $\tau_2$ induce on $\tilde{X} = X/\langle \sigma \rangle$ automorphisms $\tilde{\tau}_1$ and $\tilde{\tau}_2$ which again satisfy our hypotheses. Since the genus $\tilde{g}$ of $\tilde{X}$ is strictly less than the genus $g$ of $X$, this forces $\tilde{X} = C_p$ and $X = D^k_p$ for some $k \in \mathbb{Z}$ and $\lambda \in \mathbb{C}$. For the projection $X \to X/\langle \sigma \rangle = \tilde{X}$, the Riemann-Hurwitz Formula states

$$2g - 2 = p(2\tilde{g} - 2) + (p - 1) \cdot (\#\text{Fix}(\sigma)).$$

Since $p > 3$, this contradicts the Riemann-Hurwitz Formulas for $D^k_p \to D^k_p/\langle \tau_1 \rangle$ and $C_p \to C_p/\langle \tau_1 \rangle$ given respectively by

$$2g - 2 = p(-2) + (p - 1)2p$$
$$2\tilde{g} - 2 = p(-2) + (p - 1)p.$$ 

Thus the group $H = \langle \tau_1, \tau_2 \rangle$ consists of the elements

$$\tau(x, y) = (\zeta_p^i x, \zeta_p^j y),$$

with $1 \leq i, j \leq p$. Example 3 illustrates that in order for $H$ to contain two distinct proper subgroups with quotient $\mathbb{P}^1$, we must have $k = p - 1$, so $D^k_p = D_p$.

The case $p = 3$ follows from Remarks 3 and 4. \qed
Chapter 3. The Main Theorem

Proof of Theorem 6. By the uniqueness of the hyperelliptic involution, we assume \( p \geq 3 \). Let \( \tau_1, \tau_2 \in \text{Aut}(X) \) be as given. Then each \( \langle \tau_i \rangle \) is contained in some Sylow \( p \)-subgroup \( H_i \) \((i = 1, 2)\). Since Sylow groups are conjugate, there is \( \varphi \in \text{Aut}(X) \) such that \( \tau_1' = \varphi \circ \tau_1 \circ \varphi^{-1} \in H_2 \). Now if \( \langle \tau_1' \rangle \neq \langle \tau_2 \rangle \), Proposition 6 implies \( X \) is either \( C_p \) or \( D_p \) and \( H = \langle \tau_1', \tau_2 \rangle \) is the group given there. From Examples 1 and 2, we have that \( \tau_1' \) and \( \tau_2 \) are conjugate, which implies that \( \tau_1 \) and \( \tau_2 \) are also conjugate. \( \square \)

3.3 Conclusion

In proving Theorem 6, we now know exactly when the automorphism \( \tau \) is not unique. The curves we examined in Examples 1 and 2 turn out to be the only counterexamples in our quest for uniqueness. Moreover, the automorphisms in the counterexamples are conjugate, which is the next best thing to being unique.

Much of the beauty in these results comes from the lack of use of high powered techniques. The classical tools we used here, such as the Riemann-Roch Theorem and the Riemann-Hurwitz Formula, allow for interesting results without losing much of the intuition and geometry inherent in the subject.
Bibliography


