## An Abstract of the Dissertation of

Katherine M. Smith for the degree Doctor of Philosophy in Mathematics presented on June 8, 2000. Title: Principal Subgroups of the Nonarithmetic Hecke Triangle Groups and Galois Orbits of Algebraic Curves.

Redacted for Privacy

Abstract approved: ______________________________

Thomas A. Schmidt

In 1998 Manfred Streit [12] found a class of non-biholomorphically equivalent algebraic curves that are $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ conjugate by using subgroups of the triangle group $\Delta(2,3,n)$. His work was an extension of work done by A. Macbeath [8] who proved that for $q = p \equiv \pm 1 \bmod 7$ there are three non-biholomorphically equivalent Riemann surfaces with $PSL_2(\mathbb{F}_q)$ acting as a Hurwitz group of conformal automorphisms.

In this dissertation, we use subgroups of the Hecke Groups to construct Reimann surfaces, which we then compactify. We show that the compactified surfaces are uniformized by a subgroup of a specific type of triangle group. Upon examination of the $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits of these surfaces when we view them as algebraic curves, we see that these non-biholomorphically equivalent surfaces are Galois conjugates.

Principal Subgroups of the Nonarithmetic Hecke Triangle Groups

and Galois Orbits of Algebraic Curves

by

Katherine M. Smith

A Dissertation

submitted to

Oregon State University

in partial fulfillment of

the requirements for the

degree of

Doctor of Philosophy

Presented June 8, 2000

Commencement June 2001

Doctor of Philosophy dissertation of Katherine M. Smith presented on June 8, 2000

APPROVED:

Redacted for Privacy

Major Professor, representing Mathematics

Redacted for Privacy

Chair of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

I understand that my dissertation will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my dissertation to any reader upon request.

Redacted for Privacy

Katherine Smith, Author

# Table Of Contents

## Table of Contents (Continued)

# PRINCIPAL SUBGROUPS OF THE NONARITHMETIC HECKE TRIANGLE GROUPS AND GALOIS ORBITS OF ALGEBRAIC CURVES

# 1 BACKGROUND

## 1.1 Introduction

> Unfortunately what is little recognized is that the most worthwhile scientific books are those in which the author clearly indicates what he does not know; for an author most hurts his readers by concealing difficulties. -Évariste Galois Quoted in N. Rose, Mathematical Maxims and Minims (Raleigh NC 1988)

Little is known about the absolute Galois group, $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. A fundamental problem concerning $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is the classification of its normal subgroups of finite index, i.e. determining which finite groups occur as Galois groups over $\mathbb{Q}$. Considering the Galois orbits of curves defined over $\overline{\mathbb{Q}}$ has been one way of examining this question. In 1984 Grothendieck's much more recently published manuscript *L'Equisse d'un Programme* [15] laid out a program aiming for a complete description of the absolute Galois group. He was inspired by the geometric methods used in 1979 by G. Belyi who proved the following theorem characterizing algebraic curves defined over $\overline{\mathbb{Q}}$, the algebraic closure of the rationals [3].

**Theorem 1.1** *(Belyi) Let $\mathcal{X}$ be an algebraic curve defined over $\mathbb{C}$. Then $\mathcal{X}$ is defined over $\overline{\mathbb{Q}}$ if and only if there exists a holomorphic function $f : \mathcal{X} \to \mathbb{P}^1\mathbb{C}$ such that all the critical values of $f$ lie in the set $\{0, 1, \infty\}$.*

In 1992 J. Wolfart proved the following variation of Belyi's theorem [5, 24]:

**Theorem 1.2** *(Wolfart) A smooth algebraic curve $\mathcal{X}$ is defined over $\overline{\mathbb{Q}}$ if and only if it is representable as the quotient space (compactified if necessary) $\overline{\mathcal{H}/\Gamma}$ of the complex upper half plane by a subgroup $\Gamma$ of finite index in a Fuchsian triangle group.*

This theorem implies that a Riemann surface that is uniformized by a subgroup of finite index in a triangle group can be defined by an equation with coefficients in $\overline{\mathbb{Q}}$. We define the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on a surface as the action on the coefficients of the defining equation.

In 1967 J. Lehner and M. Newman [12] used explicit representations of groups over algebraic number fields in order to determine certain Hurwitz surfaces, i.e. surfaces with maximal automorphism groups. In 1969 A. Macbeath [8] proved that for each $q = p \equiv \pm 1 \bmod(7)$ there are three non-biholomorphically equivalent Riemann surfaces with $PSL_2(\mathbb{F}_q)$ acting as a Hurwitz group of conformal automorphisms. We verify W. Harvey's [8] statement (presumably folklore) that compactification preserves uniformization by a subgroup of a triangle group. In 1998 M. Streit [19] found a class of non-biholomorphically equivalent algebraic curves that are $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ conjugate by using subgroups of the triangle group $\Delta(2, 3, n)$. In 1999 Streit and J. Wolfart [21] used similar methods to determine the $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits of certain Riemann surfaces.

There are only finitely many Riemann surfaces in the $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ orbit of a given Riemann surface defined over $\overline{\mathbb{Q}}$. Some invariants of the $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action are the orientation preserving automorphism group of the surface and the genus of the surface[10]. In addition, both the original Riemann surface and its image under a $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ element are surfaces that are uniformized by subgroups of the same index in the same overlying triangle group [24].

We shed some light on this subject by identifying specific classes of algebraic curves which form $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits. In particular, we prove that the algebraic curves determined by certain principal subgroups of nonarithmetic Hecke groups form a complete $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ orbit. To do this, we show that our surfaces have automorphism groups $PSL_2(\mathbb{F}_{p^n})$. This puts our work in a direct line going back at least to the work of L. Dickson [6]; we found ourselves particularly influenced by M. Streit's works [19, 20]. A particular set of Macbeath's generating triples for $PSL_2(\mathbb{F}_{p^n})$ affords a correspondence between the surfaces and homomorphisms from an appropriate triangle group to $PSL_2(\mathbb{F}_{p^n})$. This correspondence is our main tool for examining Galois orbits.

## 1.2 Definitions and Theorems

### 1.2.1 *Groups and Riemann Surfaces*

The theory of Fuchsian groups is crucial to the construction of our surfaces. Excellent references here are [2, 11]. A Fuchsian group is a discrete subgroup of

$PSL_2(\mathbb{R})$. Suppose $\mathcal{X}$ is a metric space and $G$ is a group of homeomorphisms of $\mathcal{X}$.

**Definition 1** *A family of subsets $\{A_\alpha\}$ of $\mathcal{X}$ is called* locally finite *if $A_\alpha \cap K \neq \emptyset$ for only finitely many $\alpha$, where $K$ is any compact subset of $\mathcal{X}$.*

**Definition 2** *A group $G$ acts* properly discontinuously *on $\mathcal{X}$ if the family of subsets $G_x = \{g(x) | g \in G\}$, for $x \in \mathcal{X}$, is locally finite.*

**Definition 3** *A closed region $F \subset \mathcal{X}$ is defined to be a* fundamental domain *for $G$ if*

**i)** $\bigcup_{g \in G} g(F) = \mathcal{X}$,

**ii)** $\mathring{F} \cap g(\mathring{F}) = \emptyset$ *for all* $g \in G \setminus \{Id\}$

Any Fuchsian group has a connected and convex fundamental domain. If $G$ and $H$ are Fuchsian groups with $H \leq G$ and $\{M_i\}$ a set of coset representatives for $G/H$ then a fundamental domain for $H$ can be obtained by taking the union of the regions obtained by applying each $M_i$ to a fundamental domain for $G$. The tiling of a fundamental domain of a Fuchsian group induces a tiling of the surface uniformized by the group. In particular, a fundamental domain for a subgroup of a triangle group with signature $(m_1, m_2, m_3)$ can be tiled with $(m_1, m_2, m_3)$ triangles. Thus, when considering surfaces uniformized by a subgroup of a triangle group with signature $(m_1, m_2, m_3)$ we get an induced triangulation of the surface by $(m_1, m_2, m_3)$ triangles.

A Riemann surface is a connected 2-dimensional manifold $\mathcal{S}$ with a complex structure. A complex structure on $\mathcal{S}$ is a family of pairs $\{(U_\alpha, z_\alpha)\}$, where $U_\alpha$ is an open set of $\mathcal{S}$ and $z_\alpha$ is a map from $\mathcal{S}$ to $\mathbb{C}$, such that for any two pairs $(U_1, z_1)$, $(U_2, z_2)$, the map $z_2 \circ z_1^{-1} : z_1(U_1 \cap U_2) \to z_2(U_1 \cap U_2)$ is holomorphic and $\bigcup U_\alpha = \mathcal{S}$. The following theorem is called the uniformization theorem for nonsingular Riemann surfaces.

**Theorem 1.3** *(Koebe, Klein, Poincaré) Every Riemann surface $\mathcal{S}$ is conformally equivalent to $D/G$ with $D = \mathbb{C} \cup \infty$, $\mathbb{C}$, or the complex upper half plane, $\mathcal{H}$, and $G$ a freely acting discontinuous group of Möbius transformations that fixes $D$.*

*Proof:* See [7].

The Riemann surfaces that we examine are the compactifications of surfaces which are uniformized by certain subgroups of Hecke groups. Hecke groups are a direct generalization of $PSL_2(\mathbb{Z})$.

**Definition 4** *The Hecke group, $G_q$, is the group*

$$G_q = < S, T >$$

$$\textit{where } T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix}$$

$$\textit{with } \lambda_q = 2\cos(\frac{\pi}{q}), \; q \in \mathbb{Z}, \; q \geq 3.$$

In fact, $G_q$ is isomorphic to the abstract group with presentation $G_q = < S, T \,|\, T^2 = (ST)^q = I >$ . A fundamental domain for the Hecke group $G_q$ is given by two copies of the ideal triangle with vertices at $i$, $\zeta_{2q}$, and $\infty$, where $\zeta_{2q}$ is a primitive $2q$-th root of unity.

From the definition of the Hecke groups given above, we see that all the entries in the matrices of $G_q$ lie in the ring $\mathbb{Z}[\lambda_q]$. We know, from say [23], that $\mathbb{Z}[\lambda_q]$ is the ring of integers of $\mathbb{Q}(\lambda_q)$. Note that $\mathbb{Q}(\lambda_q) = \mathbb{Q}(\zeta_q + \zeta_q^{-1})$ since $\lambda_q = 2\cos(\frac{\pi}{q}) = \zeta_{2q} + {\zeta_{2q}}^{-1}$. Suppose that $\mathcal{I}$ is an ideal of $\mathbb{Z}[\lambda_q]$.

**Definition 5** *The subgroup $G_q(\mathcal{I})$ of $G_q$ defined by*

$$G_q(\mathcal{I}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_q | b, c \in \mathcal{I}, a \equiv d \equiv 1 \ mod(\mathcal{I}) \right\}$$

*is called a* <u>*principal congruence subgroup*</u> *of $G_q$.*

In fact, the aforementioned Lehner and Newman [12] used the congruence subgroup $G_3(17)$ to find a specific Hurwitz surface. A related class of groups that plays an important role for us are triangle groups. If $\tau$ is a hyperbolic triangle with angles $\frac{\pi}{m_1}$, $\frac{\pi}{m_2}$, and $\frac{\pi}{m_3}$, then the triangle group of signature $(m_1, m_2, m_3)$ is the group of words in even powers of the reflections in the sides of $\tau$. Since we are working in the hyperbolic plane, $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} < 1$. A presentation for the triangle group $T$ of signature $(m_1, m_2, m_3)$ is given by

$$T = < A, B \big| A^{m_1} = B^{m_2} = (AB)^{m_3} = I > .$$

The following results on triangle groups will be of use to us.

**Lemma 1.4** *The only Fuchsian groups which contain triangle groups are triangle groups.*

*Proof:* See [2].

This tells us that any triangle group is a subgroup of a triangle group if it is not maximal. The triangle groups we are most concerned with are maximal.

**Theorem 1.5** *(Singerman) If $p$ is an odd prime and $q > 3$ then the triangle group with signature $(2, q, p)$ is maximal.*

*Proof:* See [17].

**Definition 6** *Two groups $G$ and $H$ are called strictly commensurable if $G \cap H$ has finite index in both $G$ and $H$.*

**Definition 7** *Two Fuchsian groups $G$ and $H$ are called widely commensurable if $MGM^{-1}$ is strictly commensurable with $H$ for some $M \in PSL_2(\mathbb{R})$.*

**Definition 8** *If a Fuchsian group $G$ has a fundamental domain that is not compact then $G$ is arithmetic if it is widely commensurable with $PSL_2(\mathbb{Z})$.*

If the fundamental domain of a Fuchsian group is compact then arithmeticity is defined in terms of quaternion algebras [11].

The following is a special case of a result of K. Takeuchi [22].

**Theorem 1.6** *(Takeuchi) If* $p$ *and* $q$ *are finite primes with* $p \neq q$ *and* $p \geq 3,\ q > 3$ *then the triangle group with signature* $(2, q, p)$ *is non-arithmetic.*

*Proof:* See [22].

**Theorem 1.7** *(Margulis) The strict commensurability class of a non-arithmetic triangle group possesses a unique maximal element.*

*Proof:* See [14].

### 1.2.2 *Algebraic Background*

The group $PSL_2(\mathbb{F}_p)$ is the group of 2x2 matrices of determinant $\pm 1$ with entries in the field $\mathbb{F}_p$. It is well known that $PSL_2(\mathbb{F}_p)$ is a simple group for $p \geq 7$ (see, for instance, [1]).

**Lemma 1.8** *Let* $A, B \in PSL_2(\mathbb{F}_p)$. *If* $A$ *and* $B$ *are conjugate then they have the same trace up to sign. Furthermore, if* $A$ *and* $B$ *are non-parabolic and have the same trace up to sign then* $A$ *and* $B$ *are conjugates.*

*Proof:* We have $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $M = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$ with $ad - bc = eh - gf = \pm 1$ and $trace(A) = a + d$. Then

$$\begin{aligned} trace(MAM^{-1}) &= aeh - afg + hde - fdg \\ &= a(eh - fg) + d(he - fg) \\ &= \begin{cases} a + d & \text{if } eh - fg = 1, \\ -(a+d) & \text{if } eh - fg = -1. \end{cases} \end{aligned}$$

Now suppose that $A$ and $B$ are non-parabolic and have the same trace. The action of $PSL_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$ that of projective transformations. That is, if $[x, y] \in \mathbb{P}^1(\mathbb{F}_p)$ and $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in PSL_2(\mathbb{F}_p)$ then $M\Big([x, y]\Big) = [ax + by, cx + dy]$. Since $A$ is not parabolic it fixes 2 points in $\mathbb{P}^1(\mathbb{F}_p)$ and since the action of $PSL_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$ is doubly transitive [6], we can conjugate $A$ in $PSL_2(\mathbb{F}_p)$ so that $MAM^{-1}$ has fixed points 0 and $\infty$, which means $MAM^{-1}$ is of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$. Similarly, since $A$ and $B$ have the same trace, there is a matrix $N \in PSL_2(\mathbb{F}_p)$ so that $NBN^{-1} = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ or $NBN^{-1} = \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right)$. If $NBN^{-1} = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ then

$$MAM^{-1} = NBN^{-1}$$

$$N^{-1}MAM^{-1}N = B$$

$$N^{-1}MA(N^{-1}M)^{-1} = B.$$

Thus, $A$ and $B$ are conjugates. If $NBN^{-1} = \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right)$ then we can conjugate by the element $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ in $PSL_2(\mathbb{F}_p)$ to get $T(NBN^{-1})T^{-1} = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) = MAM^{-1}$ which gives us $(M^{-1}TN)B(M^{-1}TN)^{-1} = A$. So, in this case we also have that $A$ and $B$ are conjugates. $\square$

**Theorem 1.9** *(Kummer) Let $K$ be a number field of degree $n$ with ring of integers $\mathcal{O} = \mathbb{Z}[\lambda]$ generated by some $\lambda \in K$. Given a rational prime $p$, suppose the minimal polynomial $m(x)$ of $\lambda$ over $\mathbb{Q}$ has the following factorization into irreducibles over $\mathbb{Z}_p$:*

$$\bar{m}(x) = \prod_{i=1}^{r} \bar{m}_i(x)^{e_i}$$

*where the bar denotes reduction modulo $p$. Then the prime factorization of $< p >$ in $\mathcal{O}$ is*

$$< p > = \wp_1^{e_1} \dots \wp_r^{e_r}.$$

*where $\wp_i = < p, m_i(\lambda) >$ and $\mathcal{N}(\wp_i) = p^{deg\ m_i(x)}$, where $\mathcal{N}(\wp_i)$ is the norm of $\wp_i$.*

*Proof:* See, for example, [18].

If, in the above, $e_i = 1$ for all $i$ and $r = [K : \mathbb{Q}]$ we say that $< p >$ splits completely in $\mathcal{O}$. The factorization of $< p >$ in $\mathcal{O}$ is given by

$$\begin{aligned} < p > &= \prod_{i=1}^{r} < p, m_i(\lambda_q) >^{e_i} \\ &= \prod_{i=1}^{r} \wp_i^{e_i} \\ &= \prod_{i=1}^{r} \wp_i. \end{aligned}$$

The last step is only true if there is no ramification. If we have a Galois extension of degree $n$, $\mathcal{N}(\wp_i) = p^{f_i} = p^f$, where $\mathcal{N}(\wp_i)$ is the norm of $\wp_i$ and $f$ is the degree of $m_i(x)$. Because we have a degree $n$ extension, $\mathcal{N}(p\mathcal{O}) = p^n$, which implies $\prod_{i=1}^{r} \mathcal{N}(\wp_i) = p^n$. But $\prod_{i=1}^{r} \mathcal{N}(\wp_i) = \sum_{i=1}^{r} p^f = p^{rf}$. Hence, $p^n = p^{rf}$ and so $|\mathcal{O}/\wp_i| = p^f$. Now, $\mathcal{O}/\wp_i$ is a finite integral domain and hence a field. Thus, $\mathcal{O}/\wp_i \approx \mathbb{F}_{p^f}$. If $p$ splits completely in $\mathcal{O}$ then $r = n$ and so $f = 1$. Note that we have shown the following:

**Lemma 1.10** *If $< p >= \wp_1 ... \wp_n$ for distinct primes $\wp_i$ of $\mathcal{O}_K$ then $\mathcal{N}(\wp_i) = p$ for all $i$.*

In the cyclotomic setting with $q$ a prime, we know $[\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q - 1$ where $\zeta_q$ is a primitive $q$th root of unity. Let $p \in \mathbb{Z}$ be such that $p$ splits completely in $\mathcal{O} := \mathbb{Z}[\zeta_q]$, the ring of integers of $\mathbb{Q}(\zeta_q)$.

**Lemma 1.11** *Let $p$ and $q$ be primes. The ideal $< p >$ splits completely in $\mathbb{Q}(\zeta_q)$ if and only if $\mathbb{F}_p$ contains all the $q$th roots of unity.*

*Proof:* Suppose $p$ splits completely in $\mathbb{Q}(\zeta_q)$. Let $\Phi(X)$ be the $q$th cyclotomic polynomial, which has degree $q-1$ as $q$ is prime. When we look at $\Phi(x)$ mod$(p)$ we see that as $q$ is prime,

$$\overline{\Phi(x)} = \overline{\left(\frac{x^q-1}{x-1}\right)} = \prod_{i=1}^{q-1}(x-\alpha_i) \bmod(p)$$

because $p$ splits completely in $\mathbb{Q}(\zeta_q)$. Thus, $x^q-1 = (x-1)\overline{\Phi(x)}$ splits completely in $\mathbb{F}_p[x]$ and hence all of the $q$th roots of unity are in $\mathbb{F}_p$.

Conversely, suppose $\mathbb{F}_p$ contains all the $q$th roots of unity. This means that $x^q-1 = (x-1)\overline{\Phi(x)}$ splits completely in $\mathbb{F}_p$. Thus, $\overline{\Phi(x)} = \prod_{i=1}^{q-1}(x-\alpha_i) \bmod(p)$. By Kummer's theorem we know that $<p>= \wp_1^{e1}...\wp_r^{e_r}$ in $\mathbb{Q}(\zeta_q)$ where $\wp_i =< p, m_i(\zeta_q) >$ with $\overline{\Phi(x)} = \prod_{i=1}^{r}\bar{m}_i(x)^{e_i}$. Combining this with the information above, we have

$$\prod_{i=1}^{r}\bar{m}_i(x)^{e_i} = \prod_{i=1}^{q-1}(x-\alpha_i)$$

and since all the roots on the right side of the equation are distinct, all the roots on the left side are also. Thus, $e_i = 1$ for all $i$ and $r = q-1$. Hence, $< p >$ splits completely in $\mathbb{Q}(\zeta_q)$. $\square$

If $< p >$ splits completely in $\mathbb{Q}(\zeta_q)$ then it also splits completely in $\mathbb{Q}(\lambda_q)$. This corresponds to the case where $p \equiv 1 \bmod(q)$. If $p$ splits to $\mathbb{Q}(\lambda_q)$ but not to $\mathbb{Q}(\zeta_q)$ then each prime $\wp_i$ of $\mathbb{Z}[\lambda_q]$ over $p$ has one prime of relative residue field degree 2 above it in $\mathbb{Z}[\zeta_q]$. This corresponds to the case where $p \equiv -1 \bmod(q)$. A similar argument to that of Lemma 1.11 shows that if $p$ splits in $\mathbb{Q}(\lambda_q)$ and not in $\mathbb{Q}(\zeta_q)$ then $\mathbb{F}_{p^2}$ contains all the $q$th roots of unity but $\mathbb{F}_p$ does not.

# 2 THE SURFACES

## 2.1 Statement of Main Theorem

We state our main result.

**Theorem 2.1** *Fix odd primes $p \neq q$, $q > 3$ such that $p$ splits completely in $\mathbb{Z}[\lambda_q]$. Let $\wp_i$ be the prime ideals dividing $p$ in $\mathbb{Z}[\lambda_q]$, and let $\mathcal{H}$ denote the complex upper half plane. Then the Riemann surfaces $\overline{\mathcal{H}/G_q(\wp_i)} = \mathcal{X}_i$ are algebraic curves which form a full $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ orbit.*

The proof is divided into three main parts: the construction of the $\mathcal{X}_i$, the characterization of the $\mathcal{X}_i$, and the examination of the $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ orbit.

## 2.2 Construction of the Surfaces

Consider the Hecke group $G_q$ and let $\{\wp_i\}$ be the prime ideals dividing $p$ in $\mathbb{Z}[\lambda_q]$. We assume $p$ splits completely in $\mathbb{Z}[\lambda_q]$, i.e. $< p >= \wp_1 \wp_2 \cdots \wp_n$. Consider the congruence subgroup $G_q(\wp_i)$ of $G_q$, where

$$G_q(\wp_i) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_q | b, c \in \wp_i, a \equiv d \equiv 1 \bmod(\wp_i) \right\}.$$

This is a normal subgroup of finite index in $G_q$ since it is the kernel of reduction $\bmod(\wp_i)$. Let $n = [G_q : G_q(\wp_i)]$. We can form the surface $\mathcal{H}/G_q(\wp_i)$ which is a Riemann surface with cusps. Recall that a fundamental domain $\mathcal{F}'$ for $G_q$ can be given by two triangles with angles $(\frac{\pi}{2}, \frac{\pi}{q}, 0)$. Since $G_q(\wp_i)$ is a subgroup of index $n$ in $G_q$, a fundamental domain $\mathcal{F}$ for $G_q(\wp_i)$ can be given as a union of $n$ copies of $\mathcal{F}'$. Thus the surface $\mathcal{S} = \mathcal{H}/G_q(\wp_i)$ can be triangulated by $(2, q, \infty)$ triangles.

Since $G_q(\wp_i)$ is a subgroup of finite index and its fundamental domain has finite hyperbolic area, there are only finitely many cusps, which correspond to non-congruent vertices of $\mathcal{F}$ at $\infty$. In terms of the fundamental domain for $G_q(\wp_i)$, the cusps are contained in $\mathbb{Q}(\lambda_q) \cup \{\infty\}$. Suppose $\{r_1, r_2, ..., r_s\}$ are orbit representatives of $H := G_q(\wp_i)$ on $\mathbb{Q}(\lambda_q) \cup \{\infty\}$. For each $r = r_i$, the stabilizer in $H$, $H_r$, is a parabolic subgroup of $H$. If $A \in G_q$ is such that $A(\infty) = r$ then $A^{-1}H_rA$ is a parabolic subgroup of $A^{-1}HA = H$ (since $H$ is normal) with fixed point $\infty = A^{-1}(r)$. This means that $A^{-1}H_rA$ is generated by some conjugate of a power of $S = \left(\begin{smallmatrix} 1 & \lambda_q \\ 0 & 1 \end{smallmatrix}\right)$. The order of the generating element of $A^{-1}H_rA$ is the cusp width of the cusp $r$. That is, the order of this element tells us how many triangles have sides coming into the cusp $r$. Since $\wp_i =< p, m_i(x) >$, $S^p \in H$ and since $p$ is prime and $\lambda_q \notin \wp_i$ [13], $S^t \notin H$ for $t < p$. Thus, $\infty$ has cusp width $p$ and as $G_q(\wp_i)$ is normal in $G_q$, all cusps have this same width. Having cusp width $p$ implies that $p$ (topological) triangles meet at the filled in cusp. The compactification does not affect the elliptic points of order 2 and $q$, so we know that we have triangles of the form $(2, q, p)$. Thus, $\overline{\mathcal{S}} = \overline{\mathcal{H}/G_q(\wp_i)}$ is a compact topological space that is triangulated by $(2, q, p)$ triangles.

## 2.3 Justifying the Structure of the Compactified Surface

The compactification of the surface $\mathcal{H}/G_q(\wp_i)$ is achieved by filling in the cusps. As there are only finitely many cusps, topologically the compactification amounts to repeated one-point compactifications until each cusp is filled. In terms of Riemann surfaces we can think of the cusps as punctured disks and the compactification as sewing in full disks to replace the punctured disks.

**Proposition 2.2** *The compactified surface* $\overline{\mathcal{H}/G_q(\wp_i)}$ *is a Riemann surface triangulated with* $(2, q, p)$ *triangles.*

*Proof:* We follow the arguments of [5] for a similar setting. Suppose $\overline{\mathcal{S}} = \overline{\mathcal{H}/G_q(\wp_i)}$ is triangulated (as a topological space) with $2n$ triangles of type $(2, q, p)$, where $n = [G_q : G_q(\wp_i)]$. Let $\mathcal{X}$ be the universal covering space of $\overline{\mathcal{S}}$. The triangulation of $\overline{\mathcal{S}}$ lifts to a triangulation of $\mathcal{X}$ by open triangles $\mathcal{T}^+$ and $\mathcal{T}^-$ of type $(2, q, p)$. Fix one $\mathcal{T}$ in $\mathcal{X}$ and let $\sigma_1, \sigma_2, \sigma_3$ be the reflections in the sides $e_1, e_2, e_3$ of $\mathcal{T}$. Note that the following properties hold:

**i)** the $\sigma_j$ are homeomorphisms of $\mathcal{X}$ preserving the triangulation of $\mathcal{X}$ by the $\mathcal{T}^+$ and $\mathcal{T}^-$ triangles;

**ii)** $\sigma_j$ maps $\mathcal{T}$ to the triangle sharing edge $e_j$ with $\mathcal{T}$ so that $\sigma|_{e_j} = 1$ and ${\sigma_j}^2 = 1$ for $j = 1, 2, 3$;

**iii)** the $\sigma_j$ action changes the orientation of the $\mathcal{T}^{\pm}$ triangles;

**iv)** for any $\tau \in < \sigma_1, \sigma_2, \sigma_3 > \leq \mathrm{Aut}(\mathcal{X})$, if $\tau\mathcal{T} = \mathcal{T}$ then $\tau = 1$.

Let $G_R =< \sigma_1, \sigma_2, \sigma_3 > \subseteq \mathrm{Aut}(\mathcal{X})$. Since $\mathcal{X}$ is connected, $G_R$ acts transitively on the set of triangles of $\mathcal{X}$. Now, $\mathcal{T}$ is one of the $(2, q, p)$ triangles. Since we have a finite triangulation, the set of (closed) triangles that intersect at the vertex $e_1 \cap e_2$ is

$$\{\sigma_1\overline{\mathcal{T}}, \sigma_2\sigma_1\overline{\mathcal{T}}, \sigma_1\sigma_2\sigma_1\overline{\mathcal{T}}, ..., (\sigma_1\sigma_2)^{p-1}\sigma_1\overline{\mathcal{T}} = \sigma_2\overline{\mathcal{T}}\}$$

where the angle between $e_1$ and $e_2$ is $\frac{\pi}{p}$. Note that since $\sigma_1\sigma_2$ is the product of two reflections that fix $e_1 \cap e_2$, it can be thought of as a hyperbolic rotation about $e_1 \cap e_2$ through an angle $\frac{2\pi}{p}$.

By (iii) above we know that $(\sigma_1\sigma_2)^{p-1}\mathcal{T} \neq \sigma_2\mathcal{T}$. So, $(\sigma_1\sigma_2)^p\mathcal{T} = \mathcal{T}$ and by (iv) above we get that $(\sigma_1\sigma_2)^p = 1$. By looking at the other vertices of $\mathcal{T}$ (i.e. $e_2 \cap e_3$ and $e_1 \cap e_3$) we similarly get that $(\sigma_2\sigma_3)^q = (\sigma_1\sigma_3)^2 = 1$.

Following Wolfart [24] we see that these local relations give the following presentation:

$$G_R =< \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = 1 = (\sigma_1\sigma_2)^p = (\sigma_2\sigma_3)^q = (\sigma_1\sigma_3)^2 > .$$

This is an index 2 extension of $\Delta(2, q, p)$, which is generated by $\sigma_1\sigma_2, \sigma_2\sigma_3, \sigma_1\sigma_3$.

Now we need to define a conformal structure on $\mathcal{T}$ and then extend it to all of $\mathcal{X}$. The covering map will then induce a complex structure on $\overline{\mathcal{S}}$. Let $\mathcal{D}$ be a hyperbolic triangle in $\mathcal{H}$ with angles $\frac{\pi}{2}, \frac{\pi}{q}$, and $\frac{\pi}{p}$. The hyperbolic reflections

$s_1, s_2, s_3$ in the sides of $\mathcal{D}$ fixing edges $\epsilon_1, \epsilon_2$, and $\epsilon_3$ of $\mathcal{D}$ respectively generate a group of hyperbolic motions, $G'$, that is isomorphic to $G_R$. Let $\alpha$ be one such isomorphism from $G_R$ to $G'$. We see that $\alpha$ takes any product $\tau$ of the $\sigma_j$'s and maps it to $\alpha(\tau)$, the corresponding product of the $s_i$. Now we define a homeomorphism $f : \mathcal{X} \to \mathcal{H}$ by taking any homeomorphism $\tilde{f} : \overline{\mathcal{T}} \to \overline{\mathcal{D}}$ that maps the edge $e_j$ fixed by $\sigma_j$ to the edge $\epsilon_j$ fixed by $s_j$ and extend $\tilde{f}$ to every $\tau\overline{\mathcal{T}}, \tau \in G_R$, by $f = \alpha(\tau) \circ \tilde{f} \circ \tau^{-1}$. Using (iv) above and the fact that $\mathcal{X}$ is tessellated by the $\tau T$, we see that each $\tau T$ uniquely determines $\tau$. Thus, our extension is well-defined.

We now check that $f$ agrees on the common edge, $\tau e_j$, of any two neighboring triangles, $\tau T$ and $\tau\sigma_j T$. First, on $\tau T$ we have

$$f|_{\tau\overline{T}}(\tau e_j) = \alpha(\tau) \circ \tilde{f} \circ \tau^{-1}(\tau e_j) = \alpha(\tau)(\epsilon_j);$$

Furthermore, on $\tau\sigma_j T$ we have

$$\begin{aligned}
f|_{\tau\sigma_j\overline{T}}(\tau e_j) &= \alpha(\tau\sigma_j) \circ \tilde{f} \circ (\tau\sigma_j)^{-1}(\tau e_j) \\
&= \alpha(\tau)\alpha(\sigma_j) \circ \tilde{f} \circ \sigma_j{}^{-1} \circ \tau^{-1}(\tau e_j) \\
&= \alpha(\tau)s_j \circ \tilde{f} \circ \sigma_j{}^{-1} \circ \tau^{-1}(\tau e_j) \\
&= \alpha(\tau)s_j(\epsilon_j) \\
&= \alpha(\tau)(\epsilon_j).
\end{aligned}$$

Hence, we see that $f$ agrees on the common edge, $\tau e_j$, of any two neighboring triangles, $\tau T$ and $\tau\sigma_j T$. Furthermore, on $e_j$ we have $f(e_j) = \epsilon_j$ and

$$\begin{aligned} s_j \circ f \circ \sigma_j^{-1}(e_j) &= s_j \circ f(e_j) \\ &= s_j(\epsilon_j) \\ &= \epsilon_j, \end{aligned}$$

and hence $f(e_j) = s_j \circ f \circ \sigma_j^{-1}(e_j)$. We also have $f \circ \sigma_j \circ f^{-1} = s_j$. The result of the above is that we can replace $\mathcal{X}$ with $\mathcal{H}$ and thereby induce a complex structure on $\mathcal{X}$ with the $\sigma_j$ antiholomorphic. On $\overline{\mathcal{S}}$, take the complex structure induced by the covering map $h : \mathcal{X} \to \overline{\mathcal{S}}$. The deck transformations of $\mathcal{X}$ completely determine $\overline{\mathcal{S}}$ up to biholomorphic equivalence. Now we see that $\overline{\mathcal{S}}$ is a Riemann surface tessellated with $(2, q, p)$ triangles and so $\overline{\mathcal{H}/G_q(\wp_i)} = \overline{\mathcal{S}} = \mathcal{H}/K_i$ with $K_i \leq \Delta(2, q, p)$ for each $i$. $\square$

# 3 PROPERTIES OF THE SURFACES

## 3.1 The Automorphism Group of the $\mathcal{X}_i$

**Proposition 3.1** *The automorphism group of each $\mathcal{X}_i$ is isomorphic to $PSL_2(\mathbb{F}_p)$.*

We prove the above proposition by first looking at the automorphism group of the noncompact surface and then proving that the automorphism group is preserved under the compactification.

### 3.1.1 *The Noncompact Case*

Let $\mathcal{O} = \mathbb{Z}[\lambda_q]$ and $N$ be any ideal of $\mathcal{O}$. Consider the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_q(N) & \longrightarrow & G_q & \longrightarrow & G_q/G_q(N) & \longrightarrow & 1 \\ \downarrow & & {\scriptstyle i}\downarrow & & {\scriptstyle j}\downarrow & & {\scriptstyle \alpha}\downarrow & & \downarrow \\ 1 & \longrightarrow & PSL_2(\mathcal{O})(N) & \xrightarrow{\text{incl}} & PSL_2(\mathcal{O}) & \xrightarrow{\psi} & PSL_2(\mathcal{O}/N\mathcal{O}) & \longrightarrow & 1 \end{array}$$

We know that $PSL_2(\mathcal{O}/N\mathcal{O}) \approx PSL_2(\mathbb{F}_{p^n})$ for some $n \in \mathbb{Z}$ (see, say, [16]) if and only if $N\mathcal{O}$ is a prime ideal. In our case, $N = \wp_i$ which is a prime ideal. Since $< p >$ splits completely, we have that $n = 1$. Thus, we know the automorphism group injects into $PSL_2(\mathbb{F}_p)$. Let $\bar{\lambda}_q$ denote a root of the minimal polynomial for $\lambda$ after reducing mod$(p)$. W. Borho [4] proves that $\overline{T}$ and $\overline{U}$ generate all of $PSL_2(\mathbb{F}_{p^n})$ provided that $\mathbb{F}_p(\bar{\lambda}_q^2) = \mathbb{F}_p(\bar{\lambda}_q)$ where $\overline{T} : z \mapsto \frac{-1}{z}$ and $\overline{U} : z \mapsto \bar{\lambda}_q - \frac{1}{z}$. Borho also treats the special cases $p \neq 2$ and for $q = 5, p^n \neq 9$, which we do not need. We have all of $PSL_2(\mathbb{F}_{p^n})$ provided that $\mathbb{F}_p(\bar{\lambda}_q^2) = \mathbb{F}_p(\bar{\lambda}_q)$. We have the following situation:

$$\begin{array}{ccc} \mathbb{F}_p(\bar{\lambda}_q) & & \mathbb{Q}(\lambda_q) \\ \Big\downarrow 2 & & \Big\downarrow 2 \\ \mathbb{F}_p(\bar{\lambda}_q^2) & & \mathbb{Q}(\lambda_q^2) \\ \Big\downarrow & & \Big\downarrow \frac{\varphi(2q)}{2} = \frac{q-1}{2} \\ \mathbb{F}_p & & \mathbb{Q} \end{array}$$

Note that $[\mathbb{F}_p(\bar{\lambda}_q^2) : \mathbb{F}_p(\bar{\lambda}_q)] = 1$ or $2$ and $[\mathbb{F}_p(\bar{\lambda}_q^2) : \mathbb{F}_p(\bar{\lambda}_q)]$ must divide $[\mathbb{F}_p(\bar{\lambda}_q) : \mathbb{F}_p]$. Thus, if $[\mathbb{F}_p(\bar{\lambda}_q) : \mathbb{F}_p]$ is odd, we know $[\mathbb{F}_p(\bar{\lambda}_q^2) : \mathbb{F}_p(\bar{\lambda}_q)] = 1$ and hence $\mathbb{F}_p(\bar{\lambda}_q^2) = \mathbb{F}_p(\bar{\lambda}_q)$.

**Lemma 3.2** *If $p$ splits completely in $\mathbb{Q}(\lambda_q)$ then $\mathbb{F}_p(\bar{\lambda}_q^2) = \mathbb{F}_p(\overline{\lambda_q}) \approx \mathbb{F}_p$.*

*Proof:* From the discussion following Theorem 1.9, we know that $\mathbb{F}_{p^f} \approx \mathcal{O}/\wp_i := \mathbb{Z}[\lambda_q]/\wp_i$. Let $m(x) = \prod m_i(x)$ be the minimal polynomial for $\lambda_q$ over $\mathbb{Q}$. Note that $\mathbb{F}_p[x]/\big(\bar{m}_i(x)\big) \approx \mathbb{F}_{p^f}$ where each $\bar{m}_i$ is irreducible of degree $f$. In general, the degree of $m_i(x)$ would be $f_i$ but we have a Galois extension and hence all $f_i$ are equal, say $f_i = f$. For some $j$, $\bar{m}_j(\bar{\lambda}_q) = 0$ and so $\mathbb{F}_p(\bar{\lambda}_q) \approx \mathbb{F}_p[x]/\big(\bar{m}_j(x)\big) \approx \mathbb{F}_{p^f}$. This means that $\mathbb{F}_p(\bar{\lambda}_q)$ is a degree $f$ extension of $\mathbb{F}_p$. But since $p$ splits into $< p > = \prod_{i=1}^{n} \wp_i$, taking norms gives $p^n = p^n f$ which implies $f = 1$. $\square$

Thus, $Aut(\mathcal{H}/G_q(\wp_i)) \approx PSL_2(\mathbb{F}_p)$ for each $i$. Note that we still have an infinite class of $p$ and $q$ because the only restrictions we have thus far imposed are for $p$ and $q$ to be odd primes with $p \neq q$, $q > 3$, and for $p$ to split completely in $\mathbb{Z}[\lambda_q]$ which means $p \equiv \pm 1 \bmod(q)$.

### 3.1.2 *The Compact Case*

In the previous section we saw that the automorphism group of the non-compact surfaces $\mathcal{H}/G_q(\wp_i)$ is $PSL_2(\mathbb{F}_p)$ for each $i$. We now show that the automorphism group of the compactified surface, $\mathcal{H}/K_i$ is also $PSL_2(\mathbb{F}_p)$. Fix an $i$ and let $K = K_i$. Consider the following diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & G_q(\wp_i) & \longrightarrow & G_q & \xrightarrow{\alpha} & G_q/G_q(\wp_i) \approx PSL_2(\mathbb{F}_p) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \phi\downarrow & & \nu\downarrow & & \downarrow \\
1 & \longrightarrow & K & \longrightarrow & \Delta & \xrightarrow{\beta} & \Delta(2,q,p)/K & \longrightarrow & 1
\end{array}$$

If we can show there exists a surjective homomorphism $\phi : G_q \to \Delta(2,q,p)$ which takes $H := G_q(\wp_i)$ onto $K$ then the following proposition proves that the automorphism group of the compactified surface $\mathcal{H}/K$ is $PSL_2(\mathbb{F}_p)$.

**Proposition 3.3** *There exists a map $\nu : G_q/G_q(\wp_i) \to \Delta(2,q,p)/K$ that is an isomorphism.*

*Proof:* For the moment, assume the surjective homomorphism $\phi$ as in the above diagram exists. (We prove the existence of $\phi$ below.) Define $\nu$ by $\nu \circ \alpha = \beta \circ \phi$.

**Claim 3.4** *The homomorphism* $\nu : G_q/G_q(\wp_i) \to \Delta(2,q,p)/K$ *is well defined.*

*Proof of Claim:* Suppose $g_1H = g_2H$. Then $g_2^{-1}g_1 \in H$. Now, $\nu \circ \alpha(g_2^{-1}g_1) = \beta \circ \phi(g_2^{-1}g_1) = \beta(k)$ for some $k \in K$ since $\phi$ takes $H$ to $K$. But then $\beta(k) = 1$ and so we have $\nu \circ \alpha(g_2^{-1}g_1) = 1$. Because both $\beta$ and $\phi$ are homomorphisms we have $1 = \nu \circ \alpha(g_2^{-1}g_1) = \beta(\phi(g_2))^{-1} \cdot \beta(\phi(g_1))$ and hence $\beta(\phi(g_2)) = \beta(\phi(g_1))$ which implies $\nu \circ \alpha(g_2) = \nu \circ \alpha(g_1)$ and thus $\nu(g_2H) = \nu(g_1H)$. ***End of Claim***

The surjectivity of $\nu$ follows from the fact that $\alpha$ and $\nu \circ \alpha$ are surjective. To see that $\nu$ is injective, let $g_1H$ be in the kernel of $\nu$. Then

$$\nu \circ \alpha(g_1) = 1 \Rightarrow \beta \circ \phi(g_1) = 1 \Rightarrow \phi(g_1) \in K \Rightarrow g_1 \in H.$$

Therefore, $\nu$ is an isomorphism. $\square$

This tells us that $\Delta(2,q,p)/K$, which is the automorphism group of $\mathcal{H}/K$, is isomorphic to $PSL_2(\mathbb{F}_p)$. It is left to show that there is a homomorphism $\phi : G_q \twoheadrightarrow \Delta = \Delta(2,q,p)$ that maps $H$ to $K$. First, we prove the following:

**Lemma 3.5** *Let* $h \in H \subseteq G_q$, $f$ *be the covering map* $f : \mathcal{H}/H \to \mathcal{H}/G_q$, *and* $M \subseteq S_d$ *be the monodromy group of* $f$, *which is a permutation representation of* $G_q$. *Referring to the following diagrams,* $H = ker\rho_G$.

$$\begin{tikzcd}
 & M \subseteq S_d & \\
H \subseteq G_q \arrow[ur, "\rho_G"] \arrow[rr, two heads, "\phi"] & & \Delta \supseteq K \arrow[ul, "\rho_\Delta"']
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathcal{H} \arrow[dl, "\pi_G"'] \arrow[dr, "\pi_H"] & \\
\mathcal{H}/H \arrow[rr, "f"] & & \mathcal{H}/G_q
\end{tikzcd}$$

*Proof:* We prove containment in both directions.

Let $h \in H \subseteq G$. Thinking in terms of the monodromy representation, $h$ corresponds to a loop based at $p \in \mathcal{H}/G_q$, say $[\alpha]$. Now, ${\pi_{\mathrm{G}}}^{-1}([\alpha])$ is a path in $\mathcal{H}$ from $z$ to $\overline{h}z$ for some $\overline{h} \in H$; we denote the path $[z, \overline{h}z]$. This implies that $\pi_{\mathrm{H}}([z, \overline{h}z])$ is a loop in $\mathcal{H}/H$ based at $q$ for some $q \in f^{-1}(p)$. Note that $\pi_{\mathrm{H}}(z) = \pi_{\mathrm{H}}(\overline{h}z)$ since $\overline{h} \in H$ and so even though $\pi_{\mathrm{H}}(z)$ can be any $q \in f^{-1}(p)$, $\pi_{\mathrm{H}}([z, \overline{h}z])$ is always a loop. Thus, each lift of $[\alpha]$ to $\mathcal{H}/H$ does not permute the sheets and so $\overline{h}$ corresponds to the identity element in $M$; that is to say, $\overline{h} \in ker\rho_{\mathrm{G}}$.

Conversely, suppose $g \in ker\rho_{\mathrm{G}}$. Since there is no permutation of the sheets, $g$ corresponds to a loop at $p$ in $\mathcal{H}/G_q$ which lifts to a loop at each of the $q \in f^{-1}(p)$ in $\mathcal{H}/H$. Thus, $g$ corresponds to an element in $\pi_1(\mathcal{H}/H, q) \approx H$ and so we must have $g \in H$. $\square$

Similarly, $K = ker\rho_{\Delta}$. We now need to show that $\phi(H) = K$.

**Lemma 3.6** *The following diagram commutes; that is,* $\rho_G = \rho_\Delta \circ \phi$.

$$\begin{tikzcd} & M \subseteq S_d & \\ H \subseteq G_q \arrow[ur, "\rho_G"] \arrow[rr, two heads, "\phi"] & & \Delta \supseteq K \arrow[ul, "\rho_\Delta"'] \end{tikzcd}$$

*Proof:* We have $G_q =< S, T \,|\, T^2 = (ST)^q = I >$ and

$\Delta =< \phi(T) = A, \phi(ST) = B, \phi(S) = C \,|\, A^2 = B^q = C^p = ABC = I >$, where $\phi$ is the canonical homomorphism from $G_q$ to $\Delta$ taking our distinguished order 2 and $q$ generators of $G_q$ to order 2 and $q$ generators of $\Delta$, respectively. Given $\mathcal{H}/K$ and $\mathcal{H}/\Delta$ are the compactifications of $\mathcal{H}/H$ and $\mathcal{H}/G_q$ respectively and that we know exactly the triangulations of these surfaces, we see that the monodromy permutation representation is the same for both $G_q$ and $\Delta$,

$$M =< \rho(\ell_2), \rho(\ell_q), \rho(\ell_\infty) >$$

$$\text{where } \rho(\ell_2) = (12)(34)\cdots(\{n-1\}n),$$

$$\rho(\ell_q) = (123...q)(\{q+1\}...2q)\cdots(\{n-q-1\}...\{n-1\}\{n\}),$$

$$\rho(\ell_\infty) = (12...p)(\{p+1\}...2p)\cdots(\{n-p-1\}...\{n-1\}\{n\})$$

of orders 2, $q$, and $p$ respectively. Since the monodromy representations are the same, $\rho_G(T) = \rho_\Delta \circ \phi(T),\ \rho_G(S) = \rho_\Delta \circ \phi(S)$ and since $\phi(T)$ and $\phi(S)$ generate $\Delta$ and all the maps are homomorphisms we see that $\rho_G(g) = \rho_\Delta \circ \phi(g)$ for all $g \in G_q$. □

Note that $\phi : ker\rho_G \to ker\rho_\Delta$ since

$$\rho_G(g) = 1 \Rightarrow \rho_\Delta \circ \phi(g) = 1 \Rightarrow \phi(g) \in ker\rho_\Delta.$$

Thus, $\phi$ is a homomorphism from $G_q$ to $\Delta$ taking $H$ onto $K$.

## 3.2 The $\mathcal{X}_i$ are Biholomorphically Distinct

In this section we prove that each of the $\mathcal{X}_i = \mathcal{H}/K_i$ are biholomorphically distinct Riemann surfaces.

**Theorem 3.7** *The $\mathcal{X}_i$ are biholomorphically distinct.*

*Proof:* Let $K_j$ and $K_\ell$ be finite index subgroups of $\Delta = \Delta(2, q, p)$ such that $\mathcal{X}_j = \mathcal{H}/K_j$ and $\mathcal{X}_\ell = \mathcal{H}/K_\ell$ with $\mathcal{X}_j$ biholomorphically equivalent to $\mathcal{X}_\ell$. Suppose there exists an $M \in PSL_2(\mathbb{R})$ such that $MK_jM^{-1} = K_\ell$. Then $T = M\Delta M^{-1}$ is a triangle group commensurable with $\Delta$. But, we know that $\Delta(2, q, p)$ is maximal by Theorem 1.5 as long as $p$ is an odd prime and $q > 3$. Also, for our cases of $p$ and $q$, $\Delta(2, q, p)$ is non-arithmetic by Theorem 1.6 and so by Theorem 1.7 we see that $T = \Delta$. This allows us to conclude that $K_j = K_\ell$. Hence, for distinct subgroups $K_i$ of $\Delta(2, q, p)$ we have surfaces that are not biholomorphically equivalent. $\square$

## 3.3 Counting the $K_i$ and the Trace Triplets

The $K_i$ come from compactifying $\mathcal{X}_i = \mathcal{H}/G_q(\wp_i)$ and since $p$ splits completely in $\mathcal{O} = \mathbb{Z}[\lambda_q]$ there are $n$ distinct $\wp_i$ where $n = [\mathbb{Q} : \mathbb{Q}(\lambda_q)]$. Since $\lambda_q = \zeta_{2q} + {\zeta_{2q}}^{-1}$ we see that $n = \frac{\varphi(q)}{2}$ where $\varphi$ is the Euler $\varphi$-function, and so there are $\frac{\varphi(q)}{2}$ distinct $\mathcal{X}_i$. Since the $\mathcal{X}_i$ surfaces are uniformized by normal subgroups of $\Delta(2, q, p)$ which we called $K_i$, we see there are $\frac{\varphi(q)}{2}$ distinct subgroups $K_i$. We know that $\Delta(2, q, p)/K_i \approx PSL_2(\mathbb{F}_p)$. Thus, there is a homomorphism $\varphi_i : \Delta(2,q,p) \twoheadrightarrow PSL_2(\mathbb{F}_p)$ with $ker(\varphi_i) = K_i$. This surjective homomorphism identifies generators of $PSL_2(\mathbb{F}_p)$ of order 2, $q$, and $p$. In fact, as stated in section 3.1 we know that there are generators of the form $\overline{T}, \overline{U}$, and $\overline{S}$ mod$(\wp_i)$ where $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), U = \left(\begin{smallmatrix} \lambda_q & -1 \\ 1 & 0 \end{smallmatrix}\right), \quad S = \left(\begin{smallmatrix} 1 & \lambda_q \\ 0 & 1 \end{smallmatrix}\right)$. Now, $\lambda_q = 2\cos(\frac{\pi}{q}) = 2\cos(\frac{2\pi}{2q}) = \zeta_{2q} + {\zeta_{2q}}^{-1}$ where $\zeta_{2q}$ is a primitive $2q$-th root of unity. If we diagonalize $\overline{U}$ over $\overline{\mathbb{F}}_p$, we get $\overline{U}' = \begin{pmatrix} \bar{\zeta}_{2q} & 0 \\ 0 & \bar{\zeta}_{2q}^{-1} \end{pmatrix}$. Since $\overline{U}$ and $\overline{U}'$ are conjugate, trace$(\overline{U})$ = trace$(\overline{U}')$ $= \bar{\zeta}_{2q} + \bar{\zeta}_{2q}^{-1}$. We form a trace triplet by listing the traces of the generating triplet. As there are $\frac{\varphi(q)}{2}$ distinct sums $\bar{\zeta}_{2q} + \bar{\zeta}_{2q}^{-1}$ in $\mathbb{F}_p$, we see there are $\frac{\varphi(q)}{2}$ of the $(0, \bar{\zeta}_{2q} + \bar{\zeta}_{2q}^{-1}, 2)$ trace triplets for the generating triplets of $PSL_2(\mathbb{F}_p)$ corresponding to the homomorphisms from $\Delta(2,q,p)$ onto $PSL_2(\mathbb{F}_p)$ with kernels $K_i$. In section 4.1 we show that the homomorphism $\varphi : \Delta(2,q,p) \twoheadrightarrow PSL_2(\mathbb{F}_p)$ with $ker(\varphi) = K$ induces a one-to-one correspondence between the $K_i$ and the trace triplets.

## 3.4 The $\mathcal{X}_i$ are not Hyperelliptic

In order to show the $\mathcal{X}_i$ are not hyperelliptic we use the fact that $PSL_2(\mathbb{F}_p)$ is a simple group for $p \geq 7$ and the following result from [7].

**Proposition 3.8** *The hyperelliptic involution on a surface $M$ of genus $g \geq 2$ is in the center of $Aut(M)$.*

*Proof:* Since $Aut(\mathcal{X}_i) \approx PSL_2(\mathbb{F}_p)$, which is a simple group and hence has a trivial center, we see that the $\mathcal{X}_i$ cannot be hyperelliptic surfaces. □

## 3.5 The Genus of the $\mathcal{X}_i$ Surfaces

In order to compute the genus of the $\mathcal{X}_i$ we use the Riemann-Hurwitz formula.

**Theorem 3.9** *(Riemann-Hurwitz) If $S$ is the Riemann surface of an algebraic equation of degree $n$ and if the branch points have orders $n_1, n_2, ..., n_r$, then the genus $g$ of $S$ is given by*

$$g = 1 - n + \frac{1}{2}\sum_{i=1}^{r} n_i.$$

*Proof:* See, for instance, [9].

In our case, $n$ is given by the degree of the covering map of $\mathcal{H}/K$ over $\mathcal{H}/\Delta(2,q,p)$. This is equal to the index $[\Delta(2,q,p) : K]$ which is equal to the order of $\Delta(2,q,p)/K$. In section 3.1.2 we saw that $\Delta(2,q,p)/K \approx PSL_2(\mathbb{F}_p)$, which has order $\frac{p(p^2-1)}{2}$. Furthermore, we know from the geometry that the branch points are over $i, \zeta_{2q}$, and $\infty$. The order of branching over $i$ is $n - \frac{n}{2}$, over $\zeta_{2q}$ is $n - \frac{n}{q}$, and over $\infty$ is $n - \frac{n}{p}$. Using the Riemann-Hurwitz formula we now have

$$g = 1 - n + \frac{1}{2}(n - \frac{n}{2} + n - \frac{n}{q} + n - \frac{n}{p}).$$

Using our knowledge that $n = \frac{p(p^2-1)}{2}$, we get

$$
\begin{aligned}
g &= 1 - \frac{p(p^2-1)}{2} + \frac{p(p^2-1)}{4}\left(\frac{pq + 2p(q-1) + 2q(p-1)}{2pq}\right) \\
&= 1 - \frac{p(p^2-1)}{2}\left(\frac{2p + 2q - pq}{4pq}\right)
\end{aligned}
$$

# 4 GALOIS ORBITS

## 4.1 The Galois Orbit Consists of the $\mathcal{X}_i$ Surfaces.

The argument below follows a method due to M. Streit, who treats the case for triangle groups of the form $\Delta(2,3,q)$ [20]. Since the $\mathcal{X}_i$ are not hyperelliptic, we can take our surfaces $\mathcal{X}_i \approx \overline{\mathcal{H}/K_i}$ of genus $g$ and canonically embed them in $\mathbb{P}^{g-1}$ to get algebraic curves $\mathcal{C}_i$. We consider the ideal $\mathcal{I}_i$ of the variety $\mathcal{C}_i$, $\mathcal{I}_i =< p_{i1}, p_{i2}, ..., p_{ir_i} >$ where $p_{ij} = 0$ on $\mathcal{C}_i$. Let $\sigma$, a non-trivial element of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, act on $\mathcal{I}_i(\mathcal{C}_i)$ by extending the homomorphism $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ to $\mathbb{C}$. Now we have $\mathcal{C}^\sigma$ corresponding to $\mathcal{X}_i{}^\sigma \approx \mathcal{H}/L$ where $L \trianglelefteq \Delta(2,q,p)$, $[\Delta(2,q,p) : L] = [\Delta : K_i]$ and $\Delta(2,q,p)/L \approx \Delta(2,q,p)/K_i$. For a discussion of these facts, which can be proved using Belyi functions, see [24]. From this last, we see that $\Delta(2,q,p)/L \approx PSL_2(\mathbb{F}_p)$. Thus, there is a homomorphism $\varphi : \Delta(2,q,p) \twoheadrightarrow PSL_2(\mathbb{F}_p)$ with $ker(\varphi) = L$. This surjective homomorphism identifies generators of $PSL_2(\mathbb{F}_p)$ of order 2, $q$, and $p$. As discussed in Section 3.3, this means our generating triplet has trace triplet $(0, \bar{\zeta}_{2q} + \bar{\zeta}_{2q}^{-1}, 2)$ and so $L$ must be one of our $K_j$ since in Section 3.3 we saw that only trace triplets of this form correspond to homomorphisms from $\Delta(2,q,p)$ onto $PSL_2(\mathbb{F}_p)$ with kernels $K_i$.

## 4.2 Each $\mathcal{X}_i$ is an Element of the Galois Orbit.

Fix an $\mathcal{X}_i$, call it $\mathcal{X}$, and let $\mathcal{G}$ be the Galois orbit of $\mathcal{X}$ under the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

**Proposition 4.1** *Each $\mathcal{X}_i$ is an element of the Galois orbit $\mathcal{G}$.*

*Proof:* (Following Streit [19]) Let $Q$ be a fixed point of $\gamma_q$, an order $q$ generator of $PSL_2(\mathbb{F}_p) \approx Aut(\mathcal{X}_i)$. Using the canonical model of $\mathcal{X}_i$ discussed above, let $(U_\alpha, z)$ be a chart at $Q$ that describes the $\gamma_q$ action as multiplication by $\zeta_q$. This allows us to write $\omega = f(z)dz$ for $\omega \in \Omega(\mathcal{X})$ where $\Omega(\mathcal{X})$ is the vector space of holomorphic 1-forms on $\mathcal{X}_i$. It follows that $f(z \circ \gamma_q)d(z \circ \gamma_q)$ locally defines a 1-form at $R = \gamma_q^{-1}(Q)$, call it $\omega^{\gamma_q} \in \Omega(\mathcal{X})$. If $\omega_1, \omega_2, ..., \omega_g$ is a basis for $\Omega(\mathcal{X})$ then $\omega^{\gamma_q} = \sum_{i=1}^{g} a_{ij}^{\gamma_q} \omega_j$. The matrix $\left(a_{ij}^{\gamma_q}\right) := A_{\gamma_q}$ gives a representation of $Aut(\mathcal{X}_i)$ acting on $\Omega(\mathcal{X})$ where

$$
\begin{aligned}
[\omega_1(Q), ..., \omega_g(Q)] &= [\omega_1 \circ \gamma_q(R), ..., \omega_g \circ \gamma_q(R)] \\
&= A_{\gamma_q}[\omega_1(R), ..., \omega_g(R)].
\end{aligned}
$$

In affine coordinates on our curve in $\mathbb{P}^{g-1}$ we have

$$
\begin{aligned}
(\omega_1^{\gamma_q}(Q), ..., \omega_g^{\gamma_q}(Q)) &= (\zeta_q \omega_1(Q), ..., \zeta_q \omega_g(Q)) \\
&= A_{\gamma_q}(\omega_1(Q), ..., \omega_g(Q)) \\
&= \zeta_q(\omega_1(Q), ..., \omega_g(Q)).
\end{aligned}
$$

So, each fixed point of $\gamma_q$ on $\mathcal{X}_i$ corresponds to a vector in $\Omega(\mathcal{X})$ which is an eigenvector of $A_{\gamma_q}$ with eigenvalue $\zeta_q$. It turns out that we can "see" the action of the order $q$ automorphism on $\mathcal{X}^\sigma$ at $Q^\sigma$ by looking at the Galois action on the elements of $\overline{\mathbb{Q}}$. Let $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. In $\mathcal{X}_i^\sigma$ the point $Q^\sigma$ is a fixed point of $\gamma_q$ and thus corresponds to an eigenvector of the eigenvalue $\zeta_q^\sigma$. Of course, $\zeta_q^\sigma$ is some other primitive $q$-th root of unity, say $\zeta_q^m$.

We know by Lemma 1.11 that we have a corresponding primitive $q$-th root of unity in $\overline{\mathbb{F}}_p$ and hence the automorphism of $\mathcal{X}^\sigma$ that fixes $Q^\sigma$ has trace $\bar{\zeta}_q^m + \bar{\zeta}_q^{-m}$. By considering the diagram below we see that the corresponding trace triplet relating to generators of $Aut(\mathcal{X}^\sigma)$ has the form $(0, \bar{\zeta}_q^m + \bar{\zeta}_q^{-m}, 2)$.

$$\begin{tikzcd} & \Delta \arrow[dl, "\varphi"'] \arrow[dr, "\varphi_i"] & \\ Aut(\mathcal{X}) \arrow[rr, "isom"] & & Aut(\mathcal{X}^\sigma) \end{tikzcd}$$

A trace triplet of this form corresponds to a homomorphism from $\Delta(2, q, p)$ to $PSL_2(\mathbb{F}_p) = Aut(\mathcal{X}^\sigma)$ which has kernel one of our $K_j$. From Section 4.1 we know that we have one of our $\mathcal{X}_i$ surfaces. With the full $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action we see that we get each primitive $q$-th root of unity and so we get each of our $\mathcal{X}_i$ surfaces. $\square$

# Bibliography

[1] M. Artin. *Algebra.* Prentice Hall, Englewood, NJ, 1991.

[2] A. Beardon. *The Geometry of Discrete Groups.* Springer-Verlag, New York, 1983.

[3] G. Belyi. On Galois Extensions of a Maximal Cyclotomic Field. *Math. USSR Izvestiya*, 14:247–256, 1979.

[4] W. Borho. Kettenbrüche im Galoisfeld. *Abh. Math. Sem. Univ. Hamburg*, 39:76–82, 1973.

[5] P.B. Cohen, C. Itzykson, and J. Wolfart. Fuchsian Triangle Groups and Grothendieck Dessins: Variations on a Theme of Belyi. *Commun. Math. Phys.*, 163:605–627, 1994.

[6] L.E. Dickson. *Linear Groups with an Exposition of the Galois Field Theory.* Dover, New York, 1958.

[7] H. Farkas and I. Kra. *Riemann Surfaces.* Springer-Verlag, New York, 1980.

[8] W. Harvey. Drawings, Triangle Groups and Algebraic Curves. *Preprint - King's College, London*, 1997.

[9] G. Jones and D. Singerman. *Complex Functions.* Cambridge University Press, Cambridge, 1987.

[10] G. Jones and M. Streit. Galois Groups, Monodromy Groups and Cartographic Groups. In *Geometric Galois Actions, 2*, London Math Soc. Lecture Notes Ser. 243, pages 25–65. Cambridge University Press, 1997.

[11] S. Katok. *Fuchsian Groups.* University of Chicago Press, Chicago, 1992.

[12] J. Lehner and M. Newman. On Riemann Surfaces with Maximal Automorphism Groups. *Glasgow Math. J.*, 8:102–112, 1967.

[13] A. Leutbecher. Über die Heckeschen Gruppen $\mathcal{G}(\lambda)$. *Abh. Math. Sem. Hambg.*, 31:199–205, 1967.

[14] G.A. Margulis. *Discrete Subgroups of Semisimple Lie Groups.* Springer-Verlag, 1991.

[15] L. Schneps and P. Lochak, editors. *Geometric Galois Actions, 1*, pages 5–20. London Math Soc. Lecture Notes Ser. 242. Cambridge University Press, 1997.

[16] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton Univrsity Press, 1971.

[17] D. Singerman. Finitely Maximal Fuchsian Groups. *J. London Math. Soc. (2)*, 6:29–38, 1972.

[18] I. Stewart and D. Tall. *Algebraic Number Theory.* Chapman and Hall, 1979.

[19] M. Streit. Homology, Belyi Functions and Canonical Models. *Manuscr. Math.*, 90:489–509, 1996.

[20] M. Streit. Field of Definition and Galois Orbits for the Macbeath-Hurwitz Curves. *Preprint of the Dept. Math. Joh. Wolf. Goethe-Univers. Frank./Main*, 1998.

[21] M. Streit and J. Wolfart. Galois Actions on Some Series of Riemann Surfaces With Many Automorphisms. *Preprint of the Dept. Math. Joh. Wolf. Goethe-Univers. Frank./Main*, 1999.

[22] K. Takeuchi. Arithmetic Triangle Groups. *J. Math. Soc. Japan*, 29(1):91–106, 1977.

[23] L. Washington. *Introduction to Cyclotomic Feilds.* Springer-Verlag, New York, 2 edition, 1997.

[24] J. Wolfart. Mirror-invariant Triangulations of Riemann Surfaces, Triangle Groups, and Grothendieck Dessins: Variations on a Theme of Belyi. *Preprint of the Dept. Math. Joh. Wolf. Goethe-Univers. Frank./Main*, 1992.