GALOIS ORBITS OF PRINCIPAL CONGRUENCE HECKE CURVES

THOMAS A. SCHMIDT, KATHERINE M. SMITH

21 January 2002

ABSTRACT.

We show that the natural action of the absolute Galois group on the ideals defining principal congruence subgroups of certain *nonarithmetic* Fuchsian triangle groups is compatible with its action on the algebraic curves that these congruence groups uniformize.

0. INTRODUCTION

Grothendieck, see [Schn], sketched a program for the investigation of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by study of the action of this group on the set of algebraic curves defined by equations all of whose coefficients lie in $\bar{\mathbb{Q}}$. This program was strongly influenced by Belyi's [Bel] characterization of these *arithmetic* curves as being the algebraic curves which admit maps to the Riemann sphere ramified in at most three points. The program has been extremely fruitful, see say [Schn] or [JS2].

In particular, it has been recognized that any algebraic curve defined over $\bar{\mathbb{Q}}$ can be uniformized by some subgroup of the modular group $\mathrm{PSL}(2, \mathbb{Z})$. Here we use the closely related Hecke triangle groups, which have entries in rings of integers of certain algebraic extensions of the rationals, but which are in general nonarithmetic groups.

The entries of a Hecke group lie in the ring of integers of the maximal totally real subfield of a corresponding cyclotomic extension of the rational number field. Each ideal in this ring defines a principal congruence subgroup of the Hecke group. This subgroup uniformizes an algebraic curve, which we call a principal congruence Hecke curve. By way of an interpretation due to Wolfart [Wo3], the Belyi result implies that each principal congruence Hecke curve is defined over $\bar{\mathbb{Q}}$. We ask if the set map from ideals to algebraic curves is equivariant with respect to the action of the absolute Galois group. We prove, under certain restrictions, that the response is affirmative. This is our Theorem — we denote by G_m the Hecke group of index m, for this and further notation, see §1. A generalized version of this theorem is stated in §4.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Theorem. *Let p be an odd prime number and let n be an odd natural number which is relatively prime to p. Let $m = np^a$ for some nonnegative integer a. Let $\prod \mathcal{P}_i^{e_i}$ give the ideal factorization of (p) in the ring of integers of the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_m)$.*

Suppose that both p and n are greater than 5, and that the residue degree of the $\mathcal{P}_i$ is odd. Then the algebraic curves defined by $X_i := \overline{G_m(\mathcal{P}_i)\backslash\mathcal{H}}$ form a complete Galois orbit under the geometric action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the X_i is compatible with that on the set of the $\mathcal{P}_i$.

The theorem is applied in a special case in the following example.

Example.   Fix a prime m, greater than 5. Let p be any prime greater than 5 which is congruent to either 1 or -1 modulo m. Then the rational prime ideal (p) splits completely in $\mathbb{Z}(\zeta_m)$. The residue degree of each of the $\phi(m)/2$ corresponding ideals $\mathcal{P}_i$ is one. (Here, $\phi(n)$ denotes Euler's totient function.) Thus, m and p satisfy the hypotheses of the theorem. The absolute Galois group acts transitively on the $\mathcal{P}_i$; in particular, we find that the algebraic curves uniformized by the corresponding principal congruence groups form a single $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit of length $\phi(m)/2$.

In the case of $(m,p) = (7,13)$, there is thus a resulting Galois orbit of three curves. An application of Proposition 3 below shows these curves to be of genus $g = 37$. Proposition 4 shows that each of these curves is uniformized by a subgroup of a $(2,7,13)$ triangle group. An application of Proposition 5 shows that the curves are nonhyperelliptic, and each has automorphism group isomorphic to $\mathrm{PSL}(2,\mathbb{F}_{13})$. These automorphism groups have order fairly close to the Hurwitz bound — $84 \cdot 13$ out of the maximal $84 \cdot 36$ number of automorphisms for a curve of this genus. $\square$

A remark of MacBeath [Mac2] shows that curves such as our X_i cannot be uniformized by congruence subgroups of the modular group. The techniques of Streit [Str2] and of Streit and Wolfart [StrW] show that the X_i admit the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_m)$ as field of definition.

0.1 Brief History.

Our work is most directly inspired by that of Streit [Str1, Str2] and of Streit and Wolfart [StrW]. In particular, our key Proposition 1 is related to results of [Str2].

We work with the Hecke triangle Fuchsian groups, see §1.2. That triangle groups are directly related to the Grothendieck program is a result of Wolfart [Wo3]. To that date, the relationship of triangle groups to special curves seems to have been noticed most sharply by Macbeath [Mac1] , who showed that every Hurwitz curve — that is, every algebraic curve of genus g attaining the Hurwitz bound of $84(g-1)$ automorphisms — is uniformized by a subgroup of the $(2,3,7)$ triangle group. Building on Macbeath's work, Lehner and Newman [LN] found several families of Hurwitz curves. In particular, they used a specific principal congruence subgroup of a fixed Hecke group to determine one of these families.

The Hecke groups and their subgroups have been studied in various contexts. Recently, Cangül and Singerman [CS] considered low-index normal subgroups and regular maps. Chan et al, see say [CLLT], have studied congruence subgroups. For a brief survey of other related research see the introduction to [SS].

This work is an extension of parts of the second-named author's Oregon State University Ph.D. dissertation [Sm]. We thank Manfred Streit for comments on an early version of this paper. We thank both the referee and the reader for

suggestions for improvement of the text. We also thank Pierre Lochak for pointing out an ambiguity in a previous version.

In §1 we review material and fix notation. In §2 we give basic results about the curves we are studying. In §3 we show that the Galois orbits are as claimed in the Theorem. In §4 we give concluding remarks, and pose a closing question.

1. Background

1.1 Fuchsian Groups; Belyi's Theorem.

The Uniformization Theorem, see say [JS], states that every Riemann surface of sufficient topology (including all those of genus at least two) is biholomorphically equivalent to the quotient of the hyperbolic plane by a subgroup of its oriented isometry group. The upper half-plane model, $\mathcal{H} = \{\, z = x + iy \,|\, x, y \in \mathbb{R}, y > 0 \,\}$ of arc length ds with $ds^2 = (dx^2 + dy^2)/y^2$, has oriented isometry group $\mathrm{PSL}(2, \mathbb{R})$ where the action of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on $z \in \mathcal{H}$ is $Az = \frac{az+b}{cz+d}$. (Note that throughout we will choose representatives such as A for the class $\pm A$ in the appropriate projective group.) A discrete subgroup Γ of $\mathrm{PSL}(2, \mathbb{R})$ is called a *Fuchsian group*. It acts properly discontinuously, see [Bea], and hence $\Gamma \backslash \mathcal{H}$ is a reasonable quotient space, indeed it is a Riemann surface.

The Riemann Existence Theorem, see say [JS2] for a discussion of a circle of ideas related to this, states that every compact nonsingular Riemann surface can be realized as an *algebraic curve*: thus as the common zero locus in some complex projective space $\mathbb{P}_{\mathbb{C}}^n$ to all homogeneous polynomials in a prime ideal I of $\mathbb{C}(x_0, \ldots, x_n)$ (such that the corresponding function field is of transcendence degree one over $\mathbb{C}$). A stunning result of Belyi [Bel] is that an algebraic curve can be defined with polynomials all of whose coefficients are algebraic over $\mathbb{Q}$ if and only if there is a (holomorphic) map from the curve to the Riemann sphere which is ramified over at most three points. We say that such an algebraic curve is *arithmetic*.

A *triangle Fuchsian group* is a subgroup of $\mathrm{PSL}(2, \mathbb{R})$ given by the words of even length in the reflections about the sides of a hyperbolic triangle. Wolfart [Wo3] has reinterpreted the Belyi theorem to say that an algebraic curve is arithmetic if and only if it is (the possible compactification of) a Riemann surface uniformized by a finite index subgroup of a triangle group.

The most celebrated Fuchsian triangle group is the *modular group*, $\Gamma = \mathrm{PSL}(2, \mathbb{Z})$, whose quotient surface is the moduli space for elliptic curves. The modular group is generated by $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; indeed, $\mathrm{PSL}(2, \mathbb{Z}) = \langle\, S, T \,|\, T^2 = (ST)^3 = I \,\rangle$. One can show that every arithmetic algebraic curve is the compactification of a Riemann surface uniformized by some finite index subgroup of the modular group [JS2].

There is a notion of arithmeticity for Fuchsian groups as well. Two Fuchsian groups are called *strictly commensurable* if they have a common subgroup of finite index in each. They are called *commensurable* if the first has a finite index subgroup which is $\mathrm{PSL}(2, \mathbb{R})$-conjugate to a finite index subgroup of the second. An element of $\mathrm{PSL}(2, \mathbb{R})$ is called *parabolic* if the square of its trace equals 4; it then fixes exactly one point on the boundary of $\mathcal{H}$. A Fuchsian group with parabolic elements is *arithmetic* if it is commensurable with the modular group $\mathrm{PSL}(2, \mathbb{Z})$. (A

general Fuchsian group is arithmetic if it is commensurable to a group arising from some quaternion algebra, see say [K].) Margulis [Mar] has shown that each strict commensurability class of nonarithmetic Fuchsian groups has a unique maximal element.

Takeuchi [T] addressed the question of exactly which Fuchsian triangle groups are arithmetic. Using the standard *signature* notation of (p, q, r) for the order of generating elements corresponding to rotation about vertices of a fundamental domain for the triangle group, we extract the following from his results.

Lemma A (Takeuchi [T]**).** *Let q and r be integers greater than 5 and such that r is a prime not dividing q. Then the Fuchsian triangle group of signature $(2, q, r)$ is nonarithmetic.*

A Fuchsian group is *finitely maximal* if it is contained as a finite index subgroup of no other Fuchsian group. Singerman [Si] has identified all finitely maximal Fuchsian groups. We extract the following from his results.

Lemma B (Singerman [Si]**).** *Let q and r be integers greater than 5 and such that r is a prime not dividing q. Then the Fuchsian triangle group of signature $(2, q, r)$ is finitely maximal.*

1.2 Hecke Groups.

A main role in the present work is played by the *Hecke (triangle Fuchsian) groups*:

$$G_m := \langle \begin{pmatrix} 1 & \lambda_m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle = \langle S_m, T \mid T^2 = (TS_m)^m = I \rangle,$$

where $\lambda_m = 2\cos(\pi/m)$ with $m \in \{3, 4, 5, \dots\}$. Note that G_3 is the modular group; G_3, G_4 and G_6 are the only arithmetic Hecke groups. Leutbecher [Leu] showed that the remaining G_m are pairwise incommensurable. Furthermore, see say [Bea], each G_m is a maximal Fuchsian group. Thus for $m \notin \{3, 4, 6\}$, G_m is the maximal element in its strict commensurability class.

Congruence subgroups of the modular group play a fundamental role in the theory of elliptic curves. We will use *principal congruence subgroups* of the Hecke groups. Fix an index m, and define $\mathcal{G} := \text{PSL}(2, \mathbb{Z}[\lambda_m])$; thus, $G_m \subset \mathcal{G}$. For I any ideal of $\mathbb{Z}[\lambda_m]$ we define

$$\mathcal{G}(I) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{G} \mid a \equiv d \equiv \pm 1 \mod (I), \ b, c \in I \}.$$

Recall that $\mathbb{Q}(\lambda_m)$ is the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{2m})$ and that $\mathbb{Z}[\lambda_m]$ is the full ring of integers of $\mathbb{Q}(\lambda_m)$, see say [Wa]. Leutbecher [Leu: Hilfssatz 2] showed that λ_m is a unit in this ring of integers as long as m is not the product of 2 with a prime power. If $m = np^a$ with n relatively prime to p, then the the primitive $(2m)^{\text{th}}$ roots of unity over $\mathbb{Q}$ reduce modulo p to give $(2n)^{\text{th}}$ roots of unity over the Galois field of p elements, see say [Wa].

If $\mathcal{P}$ is a prime ideal of $\mathbb{Z}[\lambda_m]$ of absolute norm p^f, then by taking matrix entries modulo $\mathcal{P}$, one defines a homomorphism giving rise to the following short exact sequence of groups:

$$1 \to \mathcal{G}(\mathcal{P}) \to \mathcal{G} \to \mathrm{PSL}(2, \mathbb{F}_{p^f}) \to 1.$$

We define $G_m(\mathcal{P})$ to be $G_m \cap \mathcal{G}(\mathcal{P})$. Thus $G_m(\mathcal{P})$ is itself the kernel of a homomorphism and is in particular a normal subgroup of G_m. Our main work is the study of the arithmetic algebraic curves $X_i := \overline{G_m(\mathcal{P}_i)\backslash\mathcal{H}}$ for $p\mathbb{Z}[\lambda_m] = \prod \mathcal{P}_i^{e_i}$, with p a prime rational integer. We will show that the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the X_i, defined by the action on the coefficients of the defining polynomials, permutes the X_i exactly as $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ naturally permutes the prime ideals $\mathcal{P}_i$. In other terms, the map from ideals to algebraic curves is $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant.

1.3 $\mathbf{PSL}(2, \mathbb{F}_{p^f})$.

The modern treatment of $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ depends on the pioneering work of Dickson [D]. Based upon Dickson's classification of the subgroups of special projective groups, Borho [Bo] determined when certain pairs of elements can be generators.

Lemma C (Borho [Bo]**).** *Let n and p be as in the Theorem. Let f be the residue degree of any of the $\mathcal{P}_i$. Let $\bar{\lambda} = \bar{\zeta} + \bar{\zeta}^{-1}$ with $\bar{\zeta}$ a $(2n)^{\mathrm{th}}$ root of unity over $\mathbb{F}_p$ and suppose that $\mathbb{F}_{p^f} = \mathbb{F}_p(\bar{\lambda})$. The two elements $\begin{pmatrix} 1 & \bar{\lambda} \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generate all of $PSL(2, \mathbb{F}_{p^f})$ whenever $\bar{\lambda} \in \mathbb{F}_p(\bar{\lambda}^2)$.*

Slightly earlier than Borho's work, and also based upon Dickson's classification, Macbeath [Mac2] treated generating triples for $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ of the type (A, B, C) with $C = AB$. He defined an equivalence on these triples by letting $(A, B, C) \sim (A', B', C')$ if there is an isomorphism taking the first triple to the second. The study of the corresponding triples of traces (where to avoid ambiguity, one can work in $\mathrm{SL}(2, \mathbb{F}_{p^f})$ and thereafter descend to the projective group) was crucial to Macbeath's approach.

By way of fractional linear transformations, $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ acts on the projective line, $\mathbb{F}_{p^f} \cup \{\infty\}$. An element of $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ is called *parabolic* if it fixes exactly one point in the projective line. Dickson already noted that there are two conjugacy classes of parabolic elements, but any other pair of elements of the same trace are conjugate in $\mathrm{PSL}(2, \mathbb{F}_{p^f})$.

Recall that the automorphism group of $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ is the direct product of the conjugations induced by $\mathrm{PSL}(2, \mathbb{F}_{p^f}) \subset \mathrm{PGL}(2, \mathbb{F}_{p^f})$ and the automorphisms induced by the field automorphisms of $\mathbb{F}_{p^f}$ (a field automorphism induces an entry-wise action on a matrix), see say [Su; (8.8)]. Thus, the only possible differences in traces of two equivalent generating triples can be accounted for by field automorphisms taking one set of traces to the other (and, as always, signs being correctly treated).

1.4 Canonical Embedding, Action of the Absolute Galois Group.

Consider an arithmetic algebraic curve $\mathcal{C}$ of genus g. Let $\{\omega_1, \ldots, \omega_g\}$ be a basis over the complex numbers for $\Omega_{\mathcal{C}}$, the space of abelian differentials of $\mathcal{C}$. We obtain the *canonical map* to projective $g - 1$ space,

$$i : \mathcal{C} \to \mathbb{P}^{g-1}$$
$$P \mapsto [\omega_1(P) : \cdots : \omega_g(P)].$$

When $\mathcal{C}$ is nonhyperelliptic, this map is in fact an embedding. A different choice of basis for $\Omega_\mathcal{C}$ gives rise to a map which differs by an obvious projective change of coordinates; the image of $\mathcal{C}$ is thus isomorphic.

Fix $\omega \in \Omega_\mathcal{C}$, an automorphism α of $\mathcal{C}$, and a point P of $\mathcal{C}$. There are local coordinates at P such that $\omega = f(z)dz$ for some holomorphic $f(z)$. We find that $(\alpha^*\omega)(P) = (f \circ \alpha)(P)\, d(z \circ \alpha)$ defines locally at $Q = \alpha^{-1}(P)$ some element of $\Omega_\mathcal{C}$. If furthermore our α fixes P, then it will do so in such a way that $\alpha^*\omega(P) = \zeta\omega(P)$ for ζ an nth root of unity, where α is of order n. Note that then α does indeed fix P under the canonical map as given above.

The action of automorphisms such as α on $\Omega_\mathcal{C}$ is clearly linear. We thus obtain a representation of the automorphism group of $\mathcal{C}$ acting linearly upon the complex vector space $\Omega_\mathcal{C}$. Furthermore, the fixed points of automorphisms of $\mathcal{C}$ are given by the eigenvectors for the action of the automorphism group on $\Omega_\mathcal{C}$.

Now let $I(\mathcal{C})$ be the ideal of $\mathcal{C}$; that is, $\mathcal{C}$ is the subvariety of $\mathbb{P}^{g-1}$ of ideal $I(\mathcal{C})$. Thus $\mathcal{C}$ is the zero locus of all polynomials in $I(\mathcal{C})$. Since $\mathcal{C}$ is arithmetic, we may assume that this ideal is generated by polynomials whose coefficients are algebraic numbers.

Suppose now that $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. We extend the action of σ to an automorphism of $\mathbb{C}/\mathbb{Q}$. We then define $\sigma(\mathcal{C})$ to be the variety of the ideal $\sigma(I(\mathcal{C}))$. We have an induced set map, $f_\sigma : \mathcal{C} \to \sigma(\mathcal{C})$, sending in particular each $P = [x_0 : \cdots : x_{g-1}]$ with the $x_i \in \bar{\mathbb{Q}}$ to $\sigma(P) = [\sigma(x_0) : \cdots : \sigma(x_{g-1})]$.

1.5 Streit's Distinguished Eigenvalues.

Let H be a normal subgroup of a Fuchsian group G. As a set, the Riemann surface $H\backslash\mathcal{H}$ is simply $\{\, [z]_H \mid z \in \mathcal{H}\,\}$ where $[z]_H = \{\, hz \mid h \in H\,\}$. If $g \in G$, then the normality of H in G implies that $g \circ [z]_H = [gz]_H$ is well defined; furthermore, every element of Hg acts on $H\backslash\mathcal{H}$ as g does. We obtain a group homomorphism, say ϕ, from G to the automorphism group of $H\backslash\mathcal{H}$; the kernel of ϕ is H.

Now suppose that $G = \Delta = \Delta(p,q,r)$ is a triangle group of signature (p,q,r) with p, q and r relatively prime integers. Let $\gamma \in \Delta$ be of order r. If $[z]_H$ is a fixed point of $\phi(\gamma)$, then there exists $h \in H$ such that $(h\gamma)z = z$. But then by normality, there are $h_2, \ldots, h_r \in H$ such that $(h\gamma)^r = h h_2 \cdots h_r$ and $h h_2 \cdots h_r$ thus fixes $z \in \mathcal{H}$. If H is torsion-free, then we find $(h\gamma)^r = I$. But, any element of order r in Δ is conjugate to some power of γ. We conclude that there exists $\delta \in \Delta$ such that $h\gamma = \delta\gamma^j\delta^{-1}$ for some $j \in \{1, \ldots, r-1\}$. Thus $\phi(\gamma)$ and $\phi(\gamma)^j$ are conjugate.

Suppose further that $\text{Aut}(H\backslash\mathcal{H}) \subset \text{PSL}(2, \mathbb{F}_s)$ for some s and that $\phi(\gamma)$ is non-parabolic of order r there. Then $\phi(\gamma)$ is diagonalizable either over $\mathbb{F}_s$ or over its unique quadratic extension. The units of each of these fields being cyclic, in either case there is then a unique subgroup of diagonal (projective) matrices of order r. Considering traces, one now finds that j is congruent to either 1 or -1 modulo r.

We now state a proposition which mildly generalizes results in [Str2].

Proposition 1 (Streit). *Fix p, q and r pairwise relatively prime integers and let $\Delta = \Delta(p,q,r)$ be a triangle group of signature (p,q,r). Let H be a torsion-free and normal subgroup of Δ such that $H\backslash\mathcal{H}$ is nonhyperelliptic. Let $\mathcal{C}$ be the smooth canonical model of $H\backslash\mathcal{H}$ and let $\phi : \Delta \to \text{Aut}(\mathcal{C})$ be the natural homomorphism.*
Suppose that
(a) $\text{Aut}(\mathcal{C}) \subset \text{PSL}(2, \mathbb{F}_s)$ for some s; and,
(b) ϕ is surjective.

Then for any $\gamma \in \Delta$ of order r and such that $\phi(\gamma)$ is nonparabolic of order r there exists a primitive r^{th} root of unity ζ and an atlas of coordinates on $\mathcal{C}$ such that:

(1) The automorphism $\phi(\gamma)$ acts at each of its fixed points as either ζ or ζ^{-1};

(2) If $P \in \mathcal{C}$ is a fixed point of $\phi(\gamma)$, and A_γ is a matrix representation of $\phi(\gamma)$ acting on $\Omega_\mathcal{C}$, the complex vector space of abelian differentials on $\mathcal{C}$, then P is the projection to $\mathcal{C} \subset \mathbb{P}^{g-1} = \mathbb{P}(\Omega_\mathcal{C})$ of an eigenvector of A_γ of eigenvalue ζ or ζ^{-1};

(3) For P as above and $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, $\sigma(P) \in \sigma(\mathcal{C})$ is a fixed point of $\phi(\gamma)$ corresponding to an eigenvector of eigenvalue $\sigma(\zeta)$.

Proof(Sketch). We can choose local coordinates on $\mathcal{C}$ such that the action of $\phi(\gamma)$ is given in terms of the local coordinates of the hyperbolic setting. From the discussion of this section, this then implies the first statement. The second statement then follows from the discussion of the previous section. The third statement also follows from the previous section; note that the action of $\phi(\gamma)$ on $\sigma(\mathcal{C})$ is that of $f_\sigma \circ \phi(\gamma)$, with f_σ as in the previous section. $\square$

Remark. Under its hypotheses on γ, Proposition 1 establishes a one-to-one correspondence between eigenvalues $\pm\zeta^j$ and appropriate Galois images of $\mathcal{C}$. This is key to establishing that principal congruence curves do indeed lie in the same Galois orbit, see Proposition 9.

2. The Curves

Proposition 2. *Let m and p be as in the Theorem; let $\mathcal{P}$ be a prime ideal of $\mathbb{Z}[\lambda_m]$ lying above (p); and, let f be the residue degree of $\mathcal{P}$. Let Y be the noncompact Riemann surface $G_m(\mathcal{P})\backslash\mathcal{H}$. Then the (holomorphic) automorphism group of Y is isomorphic to $PSL(2, \mathbb{F}_{p^f})$.*

Proof. The Hecke group G_m is a maximal Fuchsian group and contains $G_m(\mathcal{P})$ as a normal subgroup. Therefore, the automorphism group of Y is isomorphic to $G_m/G_m(\mathcal{P})$, see say [JS].

From the definition of $G_m(\mathcal{P})$, it follows that $G_m/G_m(\mathcal{P}) \subset \mathrm{PSL}(2, \mathbb{F}_{p^f})$.

Since S_m and T generate all of G_m, their reductions modulo $G_m(\mathcal{P})$ generate the quotient group $G_m/G_m(\mathcal{P})$. The hypotheses on p and n ensure that we can apply Lemma C. We conclude that the reductions of S_m and T modulo $\mathcal{P}$ generate all of $\mathrm{PSL}(2, \mathbb{F}_{p^f})$. $\square$

Proposition 3. *Suppose that Y is as above. Let X be the compactification of Y; let X have its natural structure as a smooth projective curve. Then X is an arithmetic curve of genus*

$$g = 1 + \frac{p^f(p^{2f}-1)/2}{4pn}(pn - 2p - 2n).$$

Proof. Since Y is a ramified cover of $G_m\backslash\mathcal{H}$, we compute the genus with the Riemann-Hurwitz formula, see say [JS]. We compute using the corresponding ramified covering of compactified curves. These compatifications are given by adding points at the cusps – each cusp is a puncture which corresponds to a conjugacy class of primitive parabolic elements. The ramification degree at a point in the completed curve is computed by determining the order of the coset $gG_m(\mathcal{P})$ for $g \in G_m$ a (primitive) element fixing a lift of the point. Thus, ramification occurs

only above the cusps or above the projections of fixed points of elliptic elements of G_m to $G_m \backslash \mathcal{H}$.

The elliptic elements in G_m are the conjugates of T and of TS_m; the parabolic elements are the conjugates of S_m.

Since the conjugates of T all have trace zero, it is clear that none of these can be in $G_m(\mathcal{P}_i)$. But, T is of order 2. Hence, the ramification index at each point above the fixed point of T is two.

The reduction of ζ_{2m} modulo $\mathcal{P}$ is a $(2n)^{th}$ root of unity. Hence, TS_m induces an element which is of order n in $\mathrm{PSL}(2, \mathbb{F}_{p^f})$, see [Bo: Lemma 3.1]. The same holds for the G_m-conjugates of TS_m. Since $G_m/G_m(\mathcal{P})$ is isomorphic to $\mathrm{PSL}(2, \mathbb{F}_{p^f})$, we find that the ramification index at each point above the fixed point of TS_m is n.

In our setting λ_m is a unit, hence S_m^p is the lowest nontrivial power of S_m which is contained in $G_m(\mathcal{P})$. Therefore, the ramification at each point above the completed cusp of $G_m \backslash \mathcal{H}$ is of order p.

We thus know that X is a degree $d = p^f(p^{2f} - 1)/2 = \#\mathrm{PSL}(2, \mathbb{F}_{p^f})$ cover of the Riemann sphere, ramified over three points. In particular, Beyi's theorem implies that X is an arithmetic curve. The branching orders above the three points of ramificaqtion are $d - d/2$, $d - d/n$ and $d - d/p$. We find $g = 1 - d + \frac{1}{2}(d - d/2 + d - d/n + d - d/p) = 1 + \frac{n}{4pn}(pn - 2p - 2n)$. $\square$

Proposition 4. *Suppose that X is as above. Then X is uniformized by a normal subgroup of a triangle group of signature $(2, n, p)$.*

Proof. We argue topologically, using arguments similar to those of [Wo2]; see also [CIW]. A fundamental domain in $\mathcal{H}$ for G_m is made of two $(2, m, \infty)$ triangles. A fundamental domain for $G_m(\mathcal{P})$ contains $d = [G_m : G_m(\mathcal{P})] = \#\mathrm{PSL}(2, \mathbb{F}_{p^f})$ copies of the fundamental domain for G_m. Thus, the open Y of above is triangulated by $2d$ of the $(2, m, \infty)$ triangles.

Recall that $r = p$ is the smallest positive exponent such that S_m^r lies in $G_m(\mathcal{P})$. Thus the cusp width at ∞, see say [Leh], of Y is p; by the normality of $G_m(\mathcal{P})$ this is the cusp width of Y at every cusp. Therefore, there are $2p$ of the $(2, m, \infty)$ triangles which meet at each cusp of Y. Similarly, 4 such triangles meet at each image on Y of the fixed point of T and $2n$ meet at each image of the fixed point of TS_m. Let us call these images of fixed points *special points*.

Upon compactification, we find $2p$ topological triangles meeting at each of the former cusps, with the arrangements of the triangles at the special points unchanged. This topological data allows us to conclude that X is uniformized by a subgroup of a triangle group of signature $(2, n, p)$.

Let us denote by Δ the triangle group of signature $(2, n, p)$ whose subgroup K uniformizes X. Fix a generating triple (A, B, AB) of Δ such that A is of order 2, B of order n and AB of order p. Fix the homomorphism $\psi : G_m \to \Delta$ induced by mapping the generating triple (T, TS_m, S_m) to the generating triple (A, B, AB).

Now fix a fundamental domain in $\mathcal{H}$ for $G_m(\mathcal{P})$. This Fuchsian group is then generated by the side pairings of its domain. There are three basic types of pairings: parabolic — pairing across a cusp; elliptic; and hyperbolic. Each pairing can be expressed as a reduced word in T and TS. Here and for the remainder of the proof, for typographic simplicity we denote S_m by S. Let the pairings be given by the words: $P_i(T, TS)$ for parabolic pairings; $E_j(T, TS)$ for the elliptic pairings; and $W_k(T, TS)$, for the remaining generating words; respectively, and with appropriate indices.

Let $K \subset \Delta$ uniformize X. From the topological discussion above, there is a fundamental domain of K whose side pairings are the $W_k(A, B)$. Now, each parabolic $P_i(T, TS)$ is a conjugate of S^p and thus $P_i(A, B)$, its image under ψ, is the trivial word in Δ. Similarly, the elliptic words $E_j(T, TS)$ are conjugates of $(TS)^n$ and also have trivial images in Δ.

Since $G_m(\mathcal{P})$ is normal in G_m, the various conjugates $TW_k(T, TS)T^{-1}$ and $(TS)W_k(T, TS)(TS)^{-1}$ are contained in $G_m(\mathcal{P})$. That is, each of these can be expressed as some word in the various $P_i(T, TS)$, $E_j(T, TS)$ and $W_k(T, TS)$. We now apply ψ and find that the various $AW_k(A, B)A^{-1}$ and $BW_k(A, B)B^{-1}$ are expressible in terms of the $W_k(A, B)$. Since A and B generate Δ, we conclude that K is a normal subgroup of Δ. $\square$

We first read in [H] of the technique used in the preceding proof for passing from the signature of the noncocompact triangle group to that of the cocompact triangle group admitting a subgroup uniformizing the compactification of a Riemann surface. Having also proved that normality of subgroup is preserved under the compactification, we now easily determine the automorphism group of the algebraic curve defined by the compact Riemann surface.

Corollary. *Suppose that X is as above. Let Δ be the triangle group of signature $(2, n, p)$ and $K \triangleleft \Delta$ the corresponding uniformizing group. Then the automorphism group of X is isomorphic to Δ/K.*

Proof. The automorphism group of X is isomorphic to the quotient by K of the normalizer in $\mathrm{PSL}(2, \mathbb{R})$ of K. Since K is normal in Δ, this normalizer contains Δ. But, by our conditions on n and p, Δ is finitely maximal. Therefore, Δ is the normalizer and the claim follows. $\square$

Proposition 5. *Suppose that X is as above. Then X is nonhyperelliptic and has automorphism group isomorphic to $PSL(2, \mathbb{F}_{p^f})$.*

Proof. A hyperelliptic Riemann surface has a normal subgroup of order 2. But, it is well known that $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ is a simple group for $p > 3$ and any f. Thus, it suffices to show that $\mathrm{Aut}(X)$ is indeed $\mathrm{PSL}(2, \mathbb{F}_{p^f})$. By Proposition 2, it suffices to prove that each automorphism of $X = \overline{Y}$ restricts to an automorphism of Y.

Consider the tiling of X by $(2, n, p)$-triangles as discussed in the proof of Proposition 4. By the Corollary to Proposition 4, each automorphism of X is induced by some $\delta \in \Delta$. The effect on the tiling of such an automorphism is hence a permutation of the tiling. In particular, the automorphism restricts to give a permutation on the set of points of valency p. Therefore, the automorphism restricts to an automorphism of the complement of these points. However, the cusps of Y are completed to the points of valency p. We have thus proved that every nontrivial automorphism of X restricts to a nontrivial automorphism of Y. $\square$

3. The Galois Orbits

Proposition 6. *Let $\mathcal{P}_i$ be as in the Theorem. Let X_i be the corresponding projective curves. The X_i are pairwise nonisomorphic.*

Proof. Suppose that X_i and X_j are isomorphic for some i and j; let $K_i, K_j \subset \Delta$ be the corresponding uniformizing groups. Then there exists $M \in \mathrm{PSL}(2, \mathbb{R})$ such that

$MK_jM^{-1} = K_i$. But, then $M\Delta M^{-1}$ contains K_i. Since Δ is a finitely maximal nonarithmetic group, K_i is contained in no other finitely maximal Fuchsian group. We conclude that $M\Delta M^{-1} = \Delta$. But, the PSL$(2,\mathbb{R})$ normalizer of a finitely maximal Fuchsian group is the group itself. Hence, $M \in \Delta$. Since K_j is a normal subgroup of Δ, we conclude that K_i and K_j are equal. $\square$

Proposition 7. *Fix some $X = X_i$. Let Z be in the Galois orbit of the arithmetic curve X. Then Z is one of the X_j.*

Proof. Since X is not hyperelliptic, the canonical map gives a nonsingular embedding of X into $\mathbb{P}^{g-1}$, which for simplicity we call X as well. The ideal of X can then be taken to be generated by polynomials with algebraic coefficients, and if $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then $\sigma(X)$ is the algebraic curve whose ideal is generated by the polynomials arising from applying σ coefficient-wise to the generators of the ideal of X. Since X is uniformized by a normal subgroup of the triangle group Δ and has automorphism group isomorphic to PSL$(2,\mathbb{F}_{p^f})$, the same is true for its image under σ; see [Wo2] or [JStr].

Thus, there is a surjective homomorphism $\phi_\sigma : \Delta \to \mathrm{PSL}(2,\mathbb{F}_{p^f})$ whose kernel uniformizes the algebraic curve $\sigma(X)$. Now, see say [Mac2], any element of order two in PSL$(2,\mathbb{F}_{p^f})$ has zero trace, any element of order $n \neq p$ has trace $\bar{\zeta} + \bar{\zeta}^{-1}$ with $\bar{\zeta}$ a $(2n)^{\mathrm{th}}$ root of unity, and any element of order p has trace 2 (all up to signs). Hence, ϕ_σ sends the fixed generating triple (A, B, C) of Δ to a generating triple of trace triple $(0, \bar{\zeta} + \bar{\zeta}^{-1}, 2)$.

For each j, let $\phi_j : \Delta \to \mathrm{PSL}(2,\mathbb{F}_{p^f})$ be the surjective homomorphism corresponding to X_j. Fix $\bar{\zeta}_{2n}$ a primitive $(2n)^{\mathrm{th}}$ root of unity over $\mathbb{F}_p$. We claim that for each trace triple of the form $(0, \bar{\zeta}_{2n}^r + \bar{\zeta}_{2n}^{-r}, 2)$ there is some j and some field automorphism α of $\mathbb{F}_{p^f}$ such that the given trace triple is the image of the trace triple of ϕ_j under α. Indeed, by Kummer's Theorem see say [Wa: Prop. 2.14], the ideals $\mathcal{P}_j$ are in one-to-one correspondence with the irreducible factors modulo p of the minimal polynomial for $\lambda_m = \zeta_{2m} + \zeta_{2m}^{-1}$ over $\mathbb{Q}$. As stated in §1.2, ζ_{2m} reduces to some $\bar{\zeta}_{2n}$. But then, each $\bar{\zeta}_{2n}^r + \bar{\zeta}_{2n}^{-r}$ is the root of some irreducible factor. Any two roots of the same irreducible factor are Galois conjugates, that is are paired by some field automorphism of $\mathbb{F}_{p^f}$. Therefore, given a trace triple $(0, \bar{\zeta}_{2n}^r + \bar{\zeta}_{2n}^{-r}, 2)$, we do indeed have that there is some j and some field automorphism α which takes the trace triple of ϕ_j to this given trace triple.

Having proved the claim of the previous paragraph, we conclude that there is some j such that the trace triple of ϕ_σ is mapped to the trace triple of ϕ_j by some field automorphism α. But, the kernel of ϕ_σ is the kernel of the composition of ϕ_σ with the the automorphism of PSL$(2,\mathbb{F}_{p^f})$ induced by α. In particular, the kernel of ϕ_σ must then be K_j. That is, $\sigma(X)$ is biholomorphically equivalent to X_j. $\square$

The following proposition is unnecessary for the proof of our theorem, but may be of independent interest. Although the various Hecke groups G_{np^a} are incommensurable, we point out that their principal congruence subgroups uniformize algebraic curves which have the same compactification. It might be interesting to investigate the relations amongst the corresponding automorphic forms. Compare this with Wolfart's [Wo1] proof that the coefficients of automorphic forms for the nonarithmetic triangle groups are essentially transcendental.

Proposition 8. *Let n be an odd positive integer and p a rational prime which does not divide n, and suppose both p and n are greater than 5. Fix a nonnegative integer a, and let $m = np^a$. Then for each prime ideal $\mathcal{Q}$ in the factorization of (p) in $\mathbb{Z}[\lambda_m]$, there is a prime ideal $\mathcal{P}$ in the factorization of (p) in $\mathbb{Z}[\lambda_n]$, such that $\overline{G_m(\mathcal{Q})\backslash\mathcal{H}}$ and $\overline{G_n(\mathcal{P})\backslash\mathcal{H}}$ are isomorphic as algebraic curves.*

Proof. Recall that (p) ramifies completely in $\mathbb{Q}(\zeta_{p^a})$ and that $\mathbb{Q}(\zeta_{np^a})$ is the composition of $\mathbb{Q}(\zeta_{p^a})$ with $\mathbb{Q}(\zeta_n)$. Thus, the residue degree f of $\mathcal{Q}$ equals the residue degree of $\mathcal{P}_i$, for $\mathcal{P}_i$ any of the prime ideal divisors in $\mathbb{Z}[\lambda_n]$ of (p).

By Proposition 4, both $\overline{G_m(\mathcal{Q})\backslash\mathcal{H}}$ and the $\overline{G_n(\mathcal{P}_i)\backslash\mathcal{H}}$ are uniformized by normal subgroups of the triangle group of signature $(2, n, p)$. Indeed, by Proposition 5 and the remarks of the previous paragraph, these normal groups all share a common index in this triangle group.

Consider the generating triple of $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ induced by our chosen generators of G_m under the identification of $G_m/G_m(\mathcal{Q})$ with this projective group. By the arguments of the proof of Proposition 7, there is some $\mathcal{P}_i$ such that this generating triple arises in the analogous manner from the isomorphism of $G_n/G_n(\mathcal{P}_i)$ with the projective group. With $\mathcal{P}$ equal to this $\mathcal{P}_i$, our result follows. $\square$

Proposition 9. *The arithmetic curves X_i form a single Galois orbit.*

Proof. Given i and j, we will show that there is some $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which takes X_i to X_j.

Fix a primitive root of unity $\bar{\zeta}_{2n} \in \bar{\mathbb{F}}_p$ such that the algebraic curve X_i is determined by the homomorphism ϕ_i which takes our preferred generators of Δ to generators of $\mathrm{PSL}(2, \mathbb{F}_{p^f})$ of trace triple $(0, \bar{\zeta}_{2n} + \bar{\zeta}_{2n}^{-1}, 2)$. Suppose that in a similar manner X_j corresponds to the trace triple $(0, \bar{\zeta}_{2n}^r + \bar{\zeta}_{2n}^{-r}, 2)$, with r relatively prime to $2n$.

Consider the automorphism of order n of X_i, $\alpha = \phi_i(TS_m)$. Let P be a fixed point of α. Let ζ_{2n} be a primitive root of unity in $\bar{\mathbb{Q}}$ which reduces modulo $\mathcal{P}_i$ to $\bar{\zeta}_{2n}$. There are appropriate local (affine) coordinates on X_i, such that α acts locally by multiplication by the primitive n^{th} root of unity ζ_{2n}^2.

There exists $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(\zeta_{2n}) = \zeta_{2n}^r$. Now, define the algebraic curve $\sigma(X_i)$ and the set map f_σ as in §1.4. Then $\alpha \circ f_{\sigma^{-1}}$ is an automorphism of $\sigma(X_i)$ of order m which fixes $\sigma(P)$. Indeed, pulling back our local coordinates, $\alpha \circ \sigma^{-1}$ acts locally at $\sigma(P)$ by multiplication by ζ_{2n}^r. By Proposition 1, $\sigma(X_i)$ corresponds to the trace triple $(0, \bar{\zeta}_{2n}^r + \bar{\zeta}_{2n}^{-r}, 2)$ and is thus biholomorphically equivalent to X_j. $\square$

4. CONCLUDING REMARKS

Since every arithmetic algebraic curve is uniformized by a subgroup of a triangle group, there is great possibility for generalization of our work. Indeed, up to $\mathrm{PSL}(2, \mathbb{R})$-conjugation, each triangle group can be taken to lie in some $\mathrm{PSL}(2, \mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of a number field. Thus the study of congruence subgroups is very natural. Again, most of the corresponding curves will be uniformized by noncongruence subgroups of the modular group.

The reader may well have noticed that our proof of the main theorem implies the following general result.

Theorem. *Let $\mathcal{O}_K$ be the ring of algebraic integers of a Galois extension field K of $\mathbb{Q}$. Let $\mathcal{G} = PSL(\mathcal{O}_K)$ and let $G \subset \mathcal{G}$ be a noncocompact triangle Fuchsian group. Suppose p is an odd rational prime whose $\mathcal{O}_K$ ideal factorization is $(p) = \prod \mathcal{P}_i^{e_i}$; let f be the residue degree of the $\mathcal{P}_i$. For each i, let $G(\mathcal{P}_i) = G \cap \mathcal{G}(\mathcal{P}_i)$ and let $X_i := \overline{G_m(\mathcal{P}_i)\backslash\mathcal{H}}$ be the corresponding algebraic projective curve.*

Suppose that $Aut(X_i)$ is isomorphic to $PSL(2, \mathbb{F}_{p^f})$; that the natural homomorphism from G to $Aut(X_i)$ is surjective; and that this homomorphism from G factors through a nonarithmetic finitely maximal triangle group of signature $(2, m, p)$ for some odd m relatively prime to p. Then the set map sending $\mathcal{P}_i$ to X_i is $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ equivariant.

Our main technique is the use of Macbeath's generating triples for $PSL(2, \mathbb{F}_{p^f})$. We learned of this approach from Streit [Str2], who uses the $(2, 3, 7)$ triangle group to study aspects of the so-called Macbeath-Hurwitz curves. Streit also treats certain subgroups of signatures $(2, 3, n)$ and suggests that one should be able to continue in this vein to more general signatures. We do this, in particular by using a different set of the trace triples (see §1.3) of Macbeath.

The set of values for (p, m) excluded in the hypothesis of our main theorem is determined by: (1) the desire to have the resulting cocompact triangle group be nonarithmetic and maximal; and (2) the desire to have the automorphism group of the X_i be all of the corresponding special projective group. The latter condition is the more severe, and our hypotheses were not even sharp with respect to the use of the Borho result, Lemma C, to ensure this (our demanding that the residue degree f be odd is overly restrictive). The use of the nonarithmetic and maximal cocompact groups is to exclude "extra" automorphisms. More careful accounting might well keep track of such automorphisms.

The possibilities for the automorphism group of the Y of Proposition 2 which are excluded by our hypotheses are explicitly listed in the full Borho [Bo] result. When p is odd, the proper subgroups of $PSL(2, \mathbb{F}_{p^f})$ that elements T and S_m can generate are an icosahedral group or a conjugate of $PSL(2, \mathbb{F}(\bar{\lambda}^2))$. In the very special case $(p^f, m) = (9, 5)$ of the *simple* icosahedral group, our results hold *mutatis mutandis*. In the remaining cases, one could hope to get good control of the generating triples and thus be able to weaken the hypotheses of our Theorem.

We have only treated the case of nonhyperelliptic X here. However, as Manfred Streit reminded us, results of B. Schindler [Schi] show that there are few hyperelliptic curves uniformized by normal subgroups of triangle groups.

In summary, we are led to the following question.

Question. *Fix a triangle group Δ all of whose entries are in some number field and consider the primes of the number field lying over some fixed rational prime. Do the corresponding principal congruence subgroups of Δ always uniformize a complete Galois orbit of nonisomorphic algebraic curves?*

Added in Proof: Results similar to that of [Bo] have recently been given by Lang et al [LLT]; they apply these results to find the indices of principal congruence subgroups of Hecke groups .

[LLT] M.-L. Lang, C.-H. Lim and S.-P. Tan, *Principal congruence subgroups of the Hecke groups*, J. Number Th. **85** (2000), 220–230.

References

[Bea]   A. Beardon, *The Geometry of discrete groups*, Grad. Text Math. 91, Springer-Verlag, Berlin, 1984.

[Bel]   G. V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk. SSSR **43** (1979), 269–279; English transl. in Math. USSR–Izv. **14** (1980), 247–256.

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

[CS]   .I. N. Cangül and D. Singerman, *Normal subgroups of Hecke groups and regular maps*, Math. Proc. Cambridge Philos. Soc. **123** (1998), 59–74.

[CLLT]   S.-P. Chan, M.-L. Lang, C.-H. Lim and S.-P. Tan, *The invariants of the congruence subgroups $G_0(\mathfrak{P})$ of the Hecke group G_5*, Ill. J. Math. **38** (1994), 636–652.

[CIW]   P.B. Cohen, C. Itzykson and J. Wolfart, *Fuchsian triangle groups and Grothendieck dessins: Variations on a Theme of Belyi*, Commun. Math. Phys. **163** (1994), 605–627.

[D]   L.E. Dickson, *Linear groups with an exposition of the Galois field theory*, (republished), Dover, New York, 1958.

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

[H]   W. Harvey, *Drawings, triangle groups and algebraic curves*, Preprint - King's College, London (1997).

[K]   S. Katok, *Fuchsian groups*, University of Chicago Press, Chicago, 1992.

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

[JS2]   _____, *Belyi functions, hypermaps and Galois groups*, Bull. London Math. Soc. **28** (1996), 561–590.

[JSt]   G. Jones and M. Streit, *Galois groups, monodromy groups and cartographic groups*, Geometric Galois Actions, 2 (L. Schneps and P. Lochak, eds.), London Math Soc. Lecture Notes Ser. 243, Cambridge University Press, Cambridge, 1997.

[Leh]   J. Lehner, *Discontinuous groups and automorphic functions*, American Mathematical Society, Providence, R.I., 1964.

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

[LN]   J. Lehner and M. Newman, *On Riemann surfaces with maximal automorphism groups*, Glasgow Math. J. **8** (1967), 102–112.

[Mac1]   A. M. Macbeath, *On a theorem of Hurwitz*, Proc. Glasgow Math. Assoc. **5** (1961), 90–96.

[Mac2]   _____, *Generators of linear fractional groups*, Number Theory (W.J. Leveque, E.G. Straus, eds.), Proc. Symp. in Pure Math. 12, Amer. Math. Soc., Providence, 1969.

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

[SS]   T. Schmidt and M. Sheingorn, *Length spectra of the Hecke triangle groups*, Math. Z. **220** (1995), 369–397.

[Schi]   B. Schindler, *Period matrices of hyperelliptic curves*, Manuscipta Math. **78** (1993), 369–380.

[Schn]   L. Schneps, *Geometric Galois Actions, 1*, London Math Soc. Lecture Notes Ser. 242 (L. Schneps, eds.), Cambridge University Press, Cambridge, 1997.

[Si]   D. Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38.

[Sm]   K. M. Smith, *Principal subgroups of the nonarithmetic Hecke triangle groups and Galois Orbits of algebraic curves*, Ph.D. Dissertation, Oregon State University (2000).

[Str1]   M. Streit, *Homology, Belyi functions and canonical models*, Manuscr. Math. **90** (1996), 489–509.

[Str2]   _____, *Field of definition and Galois orbits for the Macbeath-Hurwitz curves*, Arch. Math. (2000).

[StrW]   _____, *Galois actions on some series of Riemann surfaces with many automorphisms*, Preprint of the Dept. Math. Joh. Wolf. Goethe-Univers. Frank./Main (1999).

[Su]   M. Suzuki, *Group Theory II*, Grundlehren der mathematischen Wissenschaften, 247, Springer-Verlag, Berlin, 1982.

[T]   K. Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), 91–106.

[Wa]   L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, Berlin, 1997.

[Wo1]   J. Wolfart, *Eine arithmetische Eigenschaft automorpher Formen zu gewissen nicht-arithmetischen Gruppen*, Math. Ann **262** (1983), 1–21.

[Wo2]   _____ , *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).

[Wo3]   _____ , *The 'obvious' part of Belyi's theorem and Riemann surfaces with many automorphisms*, Geometric Galois Actions, 1 (L. Schneps, ed.), London Math Soc. Lecture Notes Ser. 242, Cambridge University Press, Cambridge, 1997.

Oregon State University, Corvallis, OR 97331 USA