J. Math. Sci. Univ. Tokyo
6 (1999), 559–574.

Fake Congruence Subgroups and the Hurwitz Monodromy Group

By Gabriel Berger

Abstract. Suppose G is a finite group, embedded as a transitive subgroup of S_n for some n. Suppose in addition that $(\mathcal{C}_1, \ldots, \mathcal{C}_4)$ is a quadruple of conjugacy classes of G. In earlier papers ([F], [D-F], [B-F]), it was shown that to these data one can canonically associate a finite index subgroup of $PSL_2(\mathbb{Z})$. For example, when N is an odd integer, G is the dihedral group D_N and the conjugacy classes all consist of involutions, the associated subgroup is $\Gamma_0(N)$. In this paper we investigate the case in which G is the semidirect product of the abelian group $\mathbb{Z}[\zeta_d]/\mathcal{N}$ (where ζ_d is a primitive d'th root of unity and $\mathcal{N}$ is an ideal of $\mathbb{Z}[\zeta_d]$ relatively prime to d) and the cyclic group $\langle\zeta_d\rangle$. We relate the corresponding subgroup of $PSL_2(\mathbb{Z})$ to the "fake congruence subgroups" described in [B2]. Specifically, if we let $\mathcal{C}$ denote the conjugacy class of ζ_d in the multiplicative subgroup $\langle\zeta_d\rangle$ and choose our conjugacy classes to be $(\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}^{-3})$, then the subgroup is in fact $\Gamma_0(\mathcal{N})$ (defined originally in [B2]; see section 2).

The author wishes to express his thanks to Takayuki Oda for introducing fake congruence subgroups and to Mike Fried for valuable discussions regarding Hurwitz spaces and connections with the modular group. We note that similar topics have been considered earlier by Helmut Voelklein, whose primary interest was the realization of certain finite groups of Lie type as Galois groups over $\mathbb{Q}$.

1. Introduction

In [F], [D-F] and [B-F], a new method of obtaining finite index subgroups of $PSL_2(\mathbb{Z})$ was introduced. This method allows us to interpret (possibly noncongruence) modular curves as reduced Hurwitz spaces of 4 branch point coverings of the Riemann sphere with specified ramification data. The prototypical example of this is the following early result of Fried ([F2]):

1991 *Mathematics Subject Classification.* Primary 11F06; Secondary 20F36.
Key words: Burau representation, fake congruence subgroup, Hurwitz space, modular tower.

Theorem 1. *Suppose N is an odd, positive integer. Let D_N by the dihedral group of order $2N$, and let $\mathcal{C}$ be the conjugacy class of involutions. Embed D_N in S_N by taking the permutation representation on the cosets of a subgroup of order 2. Then the reduced Hurwitz space of coverings of $\mathbb{P}^1$ with 4 branch points and ramification data $(D_N, \mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C})$ is $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{h}$. (See §2 for definitions and details).*

In this paper, we generalize Fried's result, giving the first known explicit infinite family of noncongruence modular curves with moduli space interpretations. We first replace $D_N = \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes \langle\zeta_d\rangle$, where ζ_d is a primitive d'th root of unity and $\mathcal{N}$ is an ideal of $\mathbb{Z}[\zeta_d]$ prime to d. (By $\mathbb{Z}[\zeta_d]/\mathcal{N}$, we are referring to the additive group of the ring.) We then show that for a suitable choice of ramification data, the corresponding reduced Hurwitz space is equal to $Y_0(\mathcal{N})$, the (noncompact) fake congruence modular curve of [B2]. As $\mathcal{N}$ varies over powers of a prime $\mathfrak{p}$, we obtain a modular tower (see [F2]).

The contents of the paper are as follows: in section 2, we review the definition of fake congruence subgroups (see [B2]). In section 3, we review the basic theory of Hurwitz spaces of four branched coverings of the projective line and their connection with finite-index subgroups of the modular group. In section 4, we describe the group and conjugacy classes to be used in connection with fake congruence subgroups. In section 5, we show how to identify reduced, absolute Nielson classes corresponding to the data of section 4 with $\mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$. In section 6, we show how the results of section 5 imply that $Y_0(\mathcal{N})$ is a reduced Hurwitz space, generalizing Fried's result. We also consider the case in which G is a centerless semi-direct product of two cyclic groups. Finally, in section 7, we show that letting $\mathcal{N}$ vary over powers of certain primes, we obtain a modular tower in the sense of Fried.

2. Construction of the $\Gamma(\mathcal{N})$

2.1. Fake congruence subgroups

To begin with, we fix natural numbers $d > 2$ and N, a primitive d'th root of unity ζ_d, and an ideal $\mathcal{N}$ of $\mathbb{Z}[\zeta_d]$ relatively prime to d.

Let B_n denote the Artin braid group

$$\langle\sigma_1, \ldots \sigma_{n-1} : \sigma_i\sigma_j = \sigma_i\sigma_j for \mid i-j \mid > 1 \text{ and } \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}\rangle.$$

The reduced Burau representation (see [Bi]) is a homomorphism $\pi_n : B_n \to GL_{n-1}(\mathbb{Z}[t, t^{-1}])$. It can be obtained, among other methods, via the Fox free calculus, or from the action of B_n on the homology of an infinite cyclic extension of $\mathbb{P}^1$ ramified over $n+1$ points. Its action on the generators of B_n is given as follows:

$$\sigma_1 \mapsto \begin{bmatrix} -t & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\sigma_r \mapsto \begin{bmatrix} 1_{r-2} & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & t & -t & 1 & 0 \\ \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 1_{n-r-2} \end{bmatrix} \quad (1 < r < n-1)$$

and

$$\sigma_{n-1} \mapsto \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & t & -t \end{bmatrix}.$$

Setting $t = \zeta_d$ and reducing modulo $\mathcal{N}$ gives us a map $\mathbb{Z}[t, t^{-1}] \to \mathbb{Z}[\zeta_d]/\mathcal{N}$, and hence a map $GL_{n-1}(\mathbb{Z}[t, t^{-1}]) \to GL_{n-1}(\mathbb{Z}[\zeta_d]/\mathcal{N})$. We then obtain a new map

$$\pi_{n,\mathcal{N}} : B_n \to GL_{n-1}(\mathbb{Z}[\zeta_d]/\mathcal{N})$$

by composing with the Burau representation.

Now suppose $n = 3$. In this case we can describe our map is as follows. First, notice that B_3 has presentation $\langle \sigma_1, \sigma_2 : \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \rangle$. Then $\pi_{3,\mathcal{N}}$ is given by

$$\sigma_1 \to \begin{pmatrix} -\zeta_d & 1 \\ 0 & 1 \end{pmatrix} \tag{1}$$

$$\sigma_2 \to \begin{pmatrix} 1 & 0 \\ \zeta_d & -\zeta_d \end{pmatrix}, \tag{2}$$

where we understand the matrix entries to be elements of $\mathbb{Z}[\zeta_d]/\mathcal{N}$.

Recall [Bi] that $Z(B_3)$ is generated by $(\sigma_1\sigma_2)^3$, and observe that

$$\pi_{3,\mathcal{N}}((\sigma_1\sigma_2)^3) = \begin{pmatrix} \zeta_d^3 & 0 \\ 0 & \zeta_d^3 \end{pmatrix}.$$

Thus $\pi_{3,\mathcal{N}}$ induces a map

$$\pi_{\mathcal{N}} : PSL_2(\mathbb{Z}) = B_3/Z(B_3) \to PGL_2(\mathbb{Z}[\zeta_d]/\mathcal{N}). \tag{3}$$

Definition 1. We have the following analogs of congruence groups and modular curves:

1. $\Gamma(\mathcal{N}) = \ker(\pi_{\mathcal{N}})$
2. $\Gamma_0(\mathcal{N}) = \{\gamma \in PSL_2(\mathbb{Z}) : \pi_{\mathcal{N}}(\gamma)\infty = \infty$ (where we take $\infty \in \mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$
3. $X(\mathcal{N}) = \mathfrak{h}^*/\Gamma(\mathcal{N})$
4. $X_0(\mathcal{N}) = \mathfrak{h}^*/\Gamma_0(\mathcal{N})$
5. $Y(\mathcal{N}) = \mathfrak{h}/\Gamma(\mathcal{N})$
6. $Y_0(\mathcal{N}) = \mathfrak{h}/\Gamma_0(\mathcal{N})$

Any subgroup of $PSL_2(\mathbb{Z})$ that contains $\Gamma(\mathcal{N})$ for some $\mathcal{N}$ with $d \neq 2$ will be called a **fake congrunce subgroup**.

If $d = 2$, we obtain the usual congruence objects with $\mathcal{N}$ replaced by N.

3. Hurwitz Spaces of Four-Branch Point Coverings and Fake Congruence Subgroups

3.1. Review of Hurwitz spaces

The references for this section are [F-V], [D-F] and [B-F]. Let G be a finite group embedded as a transitive subgroup of S_n for some positive integer n. Let $\mathbf{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_4)$ be a quadruple of conjugacy classes of G. We are interested in parametrizing coverings of $\mathbb{P}^1$ (over $\mathbb{C}$) ramified over four points with monodromy group G and ramification data $\mathbf{C}$. To do so, we introduce the following definitions.

DEFINITION 2. We set $U^4 = \{(z_1, \ldots, z_4) \in (\mathbb{P}^1)^4 : \ z_i \neq z_j \text{ for } i \neq j\}$, and let $U_4 = U^4/S_4$ denote the natural quotient. The **Nielsen class** $Ni(G, \mathbf{C})$ associated to the data $(G, \mathbf{C})$ is

$$\begin{aligned}(4)\quad \{(g_1, \ldots, g_4) \in G^4 : \langle g_1, \ldots, g_4\rangle = G,\ g_1 \cdots g_4 = 1 \\ \text{and there exists } \sigma \in S_4 \text{ such that } g_i \in \mathcal{C}_{i\sigma}\ (i = 1, 2, 3, 4)\}.\end{aligned}$$

We also set $Ni(G, \mathbf{C})^{abs} = Ni(G, \mathbf{C})/N_{S_n}(\mathbf{C})$, where $N_{S_n}(\mathbf{C})$ is the normalizer of $\mathbf{C}$ in S_n, and the action of $N_{S_n}(\mathbf{C})$ is the diagonal conjugate action. Finally, the Hurwitz monodromy group H_4 is defined to be the fundamental group of U_4. It has the following presentation:

$$\begin{aligned}\langle Q_1, Q_2, Q_3 : Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}, \\ Q_1Q_3 = Q_3Q_1,\ Q_1Q_2Q_3Q_3Q_2Q_1 = 1\rangle.\end{aligned}$$

We have an action of H_4 on $Ni(G, \mathbf{C})^{abs}$ as follows: if $(g_1, \ldots, g_4) \in Ni(G, \mathbf{C})^{abs}$, then

$$(g_1, \ldots, g_4)\ Q_i = (g_1, \ldots, g_{i-1}, g_ig_{i+1}g_i^{-1}, g_i, g_{i+2}, \ldots, g_4).$$

(Thus Q_i sends g_i to $g_ig_{i+1}g_i^{-1}$, sends g_{i+1} to g_i, and fixes the other two elements of the quadruple.) It is easily verified that the action of H_4 on $Ni(G, \mathbf{C})^{abs}$ factors through to $H_4/Z(H_4)$.

Since H_4 is the fundamental group of U_4, each of its orbits on $Ni(G, \mathbf{C})^{abs}$ corresponds to a connected covering of U_4. Let $\mathcal{H}(G, \mathbf{C})$ denote the disjoint union of these coverings.

THEOREM 2 ([F-V]). *$\mathcal{H}(G, \mathbf{C})$ is a coarse moduli space for coverings of $\mathbb{P}^1$ with monodromy group G and ramification data $\mathbf{C}$.*

In fact, this theorem holds for coverings with an arbitrary number of branch points.

3.2. $PSL_2(\mathbb{C})$ action

We have canonical $PSL_2(\mathbb{C})$ actions on U^4, U_4, and $\mathcal{H} = \mathcal{H}(G, \mathbf{C})$ as above: if $\gamma \in PSL_2(\mathbb{C})$, then $\gamma(a, b, c, d) = (\gamma a, \gamma b, \gamma c, \gamma d)$. Also, γ acts on the set of coverings by attaching to $\phi : X \to \mathbb{P}^1$ the new covering $\gamma \circ \phi$. We denote the quotients of these actions by $U^{4\ red}$, ${U_4}^{red}$, and $\mathcal{H}^{red}$, respectively.

Lemma 1 ([K]). *$PSL_2(\mathbb{Z})$ is generated by*

$$S_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S_2 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

It is the free product of the cyclic groups of orders two and three (respectively) generated by

$$S_1 S_2 = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \text{ and } S_2 S_1 S_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

(respectively).

Proposition 1 ([F] Theorem 3.3, [D-F]). *There is a surjective homomorphism*

$$\phi : H_4 \to PSL_2(\mathbb{Z})$$

given by

$$\phi(Q_1) = S_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ \phi(Q_2) = S_2 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$
$$\phi(Q_3) = S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The kernel is the quaternion group Q_8 of order 8. Furthermore, $H_4/Z(H_4) \cong K_4 \rtimes PSL_2(\mathbb{Z})$, where K_4 is the Klein group of order 4 generated by $(Q_1 Q_2 Q_3)^2$ and $Q_1 Q_3^{-1}$.

Since $H_4/Z(H_4) \cong K_4 \rtimes PSL_2(\mathbb{Z})$ acts on $Ni(G, \mathbf{C})^{abs}$, we obtain a natural quotient action of $PSL_2(\mathbb{Z})$ on $Ni(G, \mathbf{C})^{abs}/K_4$.

THEOREM 3 ([B-F]). *Suppose $\mathcal{H}_O$ is a connected component of $\mathcal{H}$. Then there exists a subgroup Δ of finite index in $PSL_2(\mathbb{Z})$ such that we have the following commutative diagram:*

$$\begin{array}{ccc} \mathcal{H}_O^{red} & \longrightarrow & \mathfrak{h}/\Delta \\ \downarrow & & \downarrow \\ U_4{}^{red} & \longrightarrow & \mathfrak{h}/PSL_2(\mathbb{Z}) \end{array}$$

The horizontal maps are isomorphisms, and the bottom isomorphism is obtained by taking any $\{a,b,c,d\}$ to the unique (up to isomorphism) elliptic curve ramified over $\{a,b,c,d\}$. Furthermore, Δ arises as follows: by construction, $\mathcal{H}_O^{red}$ corresponds to the orbit of $x \in Ni(G,\mathbf{C})^{abs}$ under the action of $H_4/Z(H_4)$. Then Δ is the stabilizer of the image of x in $Ni(G,\mathbf{C})^{abs}/K_4$.

3.3. Motivating questions

The above results naturally lead to certain natural questions.

1. *Given the data of a finite group and four conjugacy classes, how can one tell whether the resulting finite index subgroup of $PSL_2(\mathbb{Z})$ is congruence or not?* About this, very little is known, although one expects that in most cases, the subgroup will be noncongruence.
2. *Does every finite index subgroup of $PSL_2(\mathbb{Z})$ arise through the above procedure?* The only result on this to date is that of Diaz-Donagi-Harbater [D-D-H], which implies that every quotient curve $\mathfrak{h}^*/\Delta$ (where Δ has finite index in $PSL_2(\mathbb{Z})$ is a Hurwitz space. Since many Δ can give rise to the isomorphic quotient curves, however, our question remains unanswered.
3. *Is our original data (the group and four conjugacy classes) reflected in any way in the arithmetic associated to the resulting subgroup of $PSL_2(\mathbb{Z})$?* Traditional methods of studying congruence subgroups (basically, the theory of Hecke operators) fail completely in the noncongruence setting. Thus nothing so simple as examining the Fourier coefficients of a Hauptmodul or cusp form (these coefficients will in general have larger numerators and denominators) will suffice in this case. It seems, therefore, that more examples are needed.

4. The Group

Our general set up is as follows. Suppose $d \geq 1$ is an integer, and ζ_d is a primitive d'th root of unity. Let $\mathcal{N}$ be an ideal of $\mathbb{Z}[\zeta_d]$ coprime to d, and by abuse of notation, continue to denote the image of ζ_d in $\mathbb{Z}[\zeta_d]/\mathcal{N}$ by ζ_d. Subsequently, by $\mathbb{Z}[\zeta_d]/\mathcal{N}$ we will mean the additive group of $\mathbb{Z}[\zeta_d]/\mathcal{N}$ unless otherwise noted; $(\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ will denote the multiplicative group of (the ring) $\mathbb{Z}[\zeta_d]/\mathcal{N}$. We can embed $(\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ into the automorphism group of $\mathbb{Z}[\zeta_d]/\mathcal{N}$ by setting $\gamma(x) = \gamma x$ for $\gamma \in (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ and $x \in \mathbb{Z}[\zeta_d]/\mathcal{N}$. Thus we may form the semidirect product

$$\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*.$$

This group is generated by $\mathbb{Z}[\zeta_d]/\mathcal{N}$ and symbols $[\gamma]$ for $\gamma \in (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$, with the relations

$$[\gamma][\alpha] = [\gamma\alpha] \text{ for } \alpha \in (\mathbb{Z}[\zeta_d]/\mathcal{N})^* \text{ and } [\gamma]^{-1} t [\gamma] = \gamma t \text{ for } t \in \mathbb{Z}[\zeta_d]/\mathcal{N}.$$

(In the second equality, the left-hand multiplication is in $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$, and the right-hand multiplication is in the ring $\mathbb{Z}[\zeta_d]/\mathcal{N}$.) Let G be the subgroup $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes \langle \zeta_d \rangle$ of $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$.

Notice that $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ acts on $\mathbb{Z}[\zeta_d]/\mathcal{N}$ as a set: the additive group $\mathbb{Z}[\zeta_d]/\mathcal{N}$ acts upon itself by addition, and the multiplicative group $(\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ acts on $\mathbb{Z}[\zeta_d]/\mathcal{N}$ by multiplication. Thus if $\#\mathbb{Z}[\zeta_d]/\mathcal{N} = N$, we obtain an embedding of $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ and its subgroup G into S_N, given as follows: if $t \in \mathbb{Z}[\zeta_d]/\mathcal{N}$ and $x[\gamma] \in \mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$, then $x[\gamma]$ acts on t via

$$t(x[\gamma]) = (t + x)[\gamma].$$

Identify $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ and G with their images in S_N. Let $\mathcal{C}$ be the conjugacy class of $[\zeta_d]$. Set $\mathbf{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_4) = (\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}^{-3})$.

Proposition 2. $N_{S_N}(\mathbf{C}) = \{x \in S_N : xGx^{-1} = G,\ x\mathcal{C}x^{-1} = \mathcal{C}\} = \mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$.

Proof. Suppose $\sigma \in N_{S_N}(\mathbf{C})$. Then $\sigma^{-1}[\zeta_d]\sigma = (-t)[\zeta_d]t$ for some $t \in \mathbb{Z}[\zeta_d]/\mathcal{N}$. Furthermore, a calculation reveals that if $x \in \mathbb{Z}[\zeta_d]/\mathcal{N}$ and $[\zeta_d]^i \neq 1$, then

$$([\zeta_d]^i x)^n = [\zeta_d]^{ni}\left(\frac{\zeta_d^{ni} - 1}{\zeta_d^i - 1} x\right).$$

Thus the order of $[\zeta_d]^i x$ is equal to the order of $[\zeta_d]^i$, which is prime to the order of $\mathbb{Z}[\zeta_d]/\mathcal{N}$. Hence, since conjugation doesn't change the order of an element in $\mathbb{Z}[\zeta_d]/\mathcal{N}$, conjugation by σ restricts to an automorphism of $\mathbb{Z}[\zeta_d]/\mathcal{N}$. Thus $\sigma^{-1} \cdot 1 \cdot \sigma = a$ for some $a \in \mathbb{Z}[\zeta_d]/\mathcal{N}$. But then

$$\sigma^{-1} \cdot \zeta_d^i \cdot \sigma = \sigma^{-1} \cdot ([\zeta_d]^{-i} 1 [\zeta_d]^i) \cdot \sigma \tag{5}$$

$$= (-t)[\zeta_d]^{-i}(t) \cdot a \cdot (-t)[\zeta_d]^i(t) \tag{6}$$

$$= (-t)[\zeta_d]^{-i}(a)[\zeta_d]^i(t) \tag{7}$$

$$= -t + \zeta_d^i a + t = \zeta_d^i a = a\zeta_d^i. \tag{8}$$

Since conjugation by σ is an automorphism of the additive group $\mathbb{Z}[\zeta_d]/\mathcal{N}$, we see that $\sigma^{-1} x \sigma = ax$ for any $x \in \mathbb{Z}[\zeta_d]/\mathcal{N}$. Furthermore, since conjugation by σ has an inverse, we see that a must be in $(\mathbb{Z}[\zeta_d]/\mathcal{N})^*$. We now claim that conjugation by σ has the same action on G as conjugation by $[a]t$. If suffices to verify this for $[\zeta_d]$ and for elements of $\mathbb{Z}[\zeta_d]/\mathcal{N}$ separately. First, $[\zeta_d]$:

$$(-t)[a]^{-1}[\zeta_d][a](t) = (-t)[\zeta_d]t = \sigma^{-1}[\zeta_d]\sigma.$$

Next, if $x \in \mathbb{Z}[\zeta_d]/\mathcal{N}$, then

$$(-t)[a]^{-1} x [a](t) = (-t) + ax + t = ax.$$

Thus $[a](t)\sigma^{-1}$ centralizes G. To conclude the proof, we need only the following:

LEMMA 2. *The centralizer of G in S_N is trivial.*

PROOF. We identify S_N with the permutations (as a set) of $\mathbb{Z}[\zeta_d]/\mathcal{N}$. Suppose $\gamma \in S_N$ centralizes G. Then $[\zeta_d]\gamma = \gamma[\zeta_d]$, and $x\gamma = \gamma x$ for all $x \in \mathbb{Z}[\zeta_d]/\mathcal{N}$. Thus if $y \in \mathbb{Z}[\zeta_d]/\mathcal{N}$, then letting the above elements act on y, we obtain

$$(y\zeta_d)\gamma = (y)\gamma\zeta_d, \text{ and } (x+y)\gamma = y\gamma + x.$$

So for all $y \in \mathbb{Z}[\zeta_d]/\mathcal{N}$,

$$(y\gamma)\zeta_d = (y\zeta_d)\gamma = (y(\zeta_d - 1) + y)\gamma = y\gamma + y(\zeta_d - 1).$$

Thus $(y\gamma)(\zeta_d - 1) = y(\zeta_d - 1)$. But since $\mathcal{N}$ and d are coprime, $\zeta_d - 1$ is a unit in (the ring) $\mathbb{Z}[\zeta_d]/\mathcal{N}$. So $y\gamma = y$, and so γ is the identity element. □ □

5. Identification with $\mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$

Lemma 3. *$Ni(G, \mathcal{C}_1, \ldots, \mathcal{C}_4)/K_4$ may be identified with the set*

$$T(\mathbb{Z}[\zeta_d]/\mathcal{N}) = \{(a,b,c) \in (\mathbb{Z}[\zeta_d]/\mathcal{N})^3 : \\ (b-a)\mathbb{Z}[\zeta_d]/\mathcal{N} + (c-b)\mathbb{Z}[\zeta_d]/\mathcal{N} = \mathbb{Z}[\zeta_d]/\mathcal{N}\}$$

The action of $\mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$ on $T(\mathbb{Z}[\zeta_d]/\mathcal{N})$ is as follows: if $t \in \mathbb{Z}[\zeta_d]/\mathcal{N}$, then $(a,b,c)t = (a+t, b+t, c+t)$. If $s \in (\mathbb{Z}[\zeta_d]/\mathcal{N})^*$, then $(a,b,c)s = (as, bs, cs)$.

Proof. Since there exists a unique element of K_4 such that the fourth coordinate is conjugate to $[\zeta_d]^{-3}$, any element of $Ni(G, \mathcal{C}_1, \ldots, \mathcal{C}_4)/K_4$ has a unique representative of the form

$$((-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e)$$

for some $a, b, c, e \in \mathbb{Z}[\zeta_d]/\mathcal{N}$. We identify this with the element (a,b,c), which we must show is in $T(\mathbb{Z}[\zeta_d]/\mathcal{N})$. Note that the group

$$\langle (-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e\rangle \cap \mathbb{Z}[\zeta_d]/\mathcal{N}$$

is generated by elements of the form

$$(-a)[\zeta_d]^i a \cdot (-b)[\zeta_d]^i b = (1-\zeta_d^{-i})(b-a)$$

and

$$(-b)[\zeta_d]^i b \cdot (-c)[\zeta_d]^i c = (1-\zeta_d^{-i})(c-b).$$

But recall that d is prime to $\mathcal{N}$. Thus

$$\langle (-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e\rangle \cap \mathbb{Z}[\zeta_d]/\mathcal{N}$$

is equal to

$$(b-a)\mathbb{Z}[\zeta_d]/\mathcal{N} + (c-b)\mathbb{Z}[\zeta_d]/\mathcal{N}.$$

But clearly

$$\langle (-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e\rangle = G$$

if and only if

$$\langle(-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e\rangle \cap \mathbb{Z}[\zeta_d]/\mathcal{N} = \mathbb{Z}[\zeta_d]/\mathcal{N}.$$

Thus

$$\langle(-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e\rangle = G$$

if and only if

$$(b-a)\mathbb{Z}[\zeta_d]/\mathcal{N} + (c-b)\mathbb{Z}[\zeta_d]/\mathcal{N} = \mathbb{Z}[\zeta_d]/\mathcal{N}.$$

The rest of the lemma is clear. □

LEMMA 4. *The action of $PSL_2(\mathbb{Z})$ on $T(\mathbb{Z}[\zeta_d]/\mathcal{N})$ is given by*

$$(a,b,c)S_1 = (\zeta_d(b-a)+a, a, c)$$
$$(a,b,c)S_2 = (a, \zeta_d(c-b)+b, b)$$

PROOF.

$$\begin{aligned}&((-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e)S_1\\ =&(-a+\zeta_d^{-1}(a-b)\cdot[\zeta_d]\cdot[\zeta_d]\cdot[\zeta_d]^{-1}(\zeta_d^{-1}(b-a)+a),\\ &(-a)[\zeta_d]a, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e)\end{aligned}$$

and

$$\begin{aligned}&((-a)[\zeta_d]a, (-b)[\zeta_d]b, (-c)[\zeta_d]c, (-e)[\zeta_d]^{-3}e)S_1\\ =&((-a)[\zeta_d]a, -b+\zeta_d^{-1}(b-c)\cdot[\zeta_d]\cdot[\zeta_d]\cdot[\zeta_d]^{-1}\\ &(\zeta_d^{-1}(c-b)+b), (-b)[\zeta_d]b, (-e)[\zeta_d]^{-3}e).\end{aligned}$$

The result follows. □

Note that the above action factors through to $T(\mathbb{Z}[\zeta_d]/\mathcal{N})/N_{S_N}(\mathbf{C})$.

PROPOSITION 3. *The following are isomorphic as $PSL_2(\mathbb{Z})$-sets:*

1. $Ni(G, \mathcal{C}_1, \ldots, \mathcal{C}_4)^{abs}/K_4$
2. $T(\mathbb{Z}[\zeta_d]/\mathcal{N})/N_{S_N}(\mathbf{C})$
3. $\mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$, *with $PSL_2(\mathbb{Z})$ action given through the Burau representation $\pi_{\mathcal{N}} : PSL_2(\mathbb{Z}) \to PGL_2(\mathbb{Z}[\zeta_d]/\mathcal{N})$.*

Proof. The equivalence of 1 and 2 follows from lemmas 3 and 4 above. To show the equivalence of 2 and 3, first note that every element in $T(\mathbb{Z}[\zeta_d]/\mathcal{N})/N_{S_N}(\mathbf{C})$ has a representative of the form $(0,a,b)$. Define a map

$$\Psi : T(\mathbb{Z}[\zeta_d]/\mathcal{N})/N_{S_N}(\mathbf{C}) \to \mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$$

by

$$\Psi(0,a,b) = [b-a, -[\zeta_d]a].$$

This is clearly well-defined and injective. To show that it's surjective, note that $(x,y) \in (\mathbb{Z}[\zeta_d]/\mathcal{N})^2$ defines an element of $\mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$ if and only if

$$x(\mathbb{Z}[\zeta_d]/\mathcal{N}) + y(\mathbb{Z}[\zeta_d]/\mathcal{N}) = \mathbb{Z}[\zeta_d]/\mathcal{N}.$$

But this holds if and only if

$$(-1/[\zeta_d])y(\mathbb{Z}[\zeta_d]/\mathcal{N}) + (x - 1/[\zeta_d]\cdot y)(\mathbb{Z}[\zeta_d]/\mathcal{N}) = \mathbb{Z}[\zeta_d]/\mathcal{N},$$

and so by lemma 3, $(-1/[\zeta_d]\cdot y, x - 1/[\zeta_d]\cdot y)$ is a preimage of $[x,y] \in \mathbb{P}^1(\mathbb{Z}[\zeta_d]/\mathcal{N})$ in $T(\mathbb{Z}[\zeta_d]/\mathcal{N})/N_{S_N}(\mathbf{C})$.

We must now show that the group actions are compatible. Note that

$$\Psi((0,a,b)S_1) = \Psi(\zeta_d^{-1}a, 0, b) = \Psi(0, -\zeta_d^{-1}a, b - \zeta_d^{-1}a) = [b,a]$$

and

$$(\Psi(0,a,b))S_1 = [b-a, -\zeta_d a]S_1 = [-\zeta_d b, -\zeta_d a] = [b,a].$$

Similarly,

$$\Psi((0,a,b)S_2) = \Psi(0, \zeta_d^{-1}(b-a) + a, a) \tag{9}$$

$$= [\zeta_d^{-1}(a-b), (a-b) - \zeta_d a] = [b-a, \zeta_d(b-a) + \zeta_d^2 a] \tag{10}$$

and

$$(\Psi(0,a,b))S_2 = [b-a, -[\zeta_d]a]S_2 = [b-a, [\zeta_d](b-a) + [\zeta_d]^2 a].$$

This completes the proof. □

6. Relations with Fake Congruence Groups

6.1. The main theorems

Suppose d and N are relatively prime natural numbers and that there exists an integer b of (multiplicative) order d mod N. We may then form the semi-direct product

$$\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/d\mathbb{Z} = \{\gamma, t : \gamma^d = t^N = 1, \gamma^{-1}t\gamma = t^b\}.$$

LEMMA 5. *$\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/d\mathbb{Z}$ has trivial center if and only if $b-1$ and N are coprime.*

PROOF. Suppose $t^j\gamma^i$ is an element of the center of $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/d\mathbb{Z}$ for some nonnegative integers $j < N$ and $i < d$. We first show that $t^j\gamma^i \in \mathbb{Z}/N\mathbb{Z}$, i.e., that $i = 0$. Since $t^j\gamma^i \in \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/d\mathbb{Z}$, we must have

$$t^{-1} \cdot t^j\gamma^i \cdot t = t^j\gamma^i.$$

But

$$t^{-1} \cdot t^j\gamma^i \cdot t = t^j \cdot t^{-1}\gamma^i \cdot t = t^j\gamma^i t^{-b^i+1}.$$

Thus $t^{-b^i+1} = 1$, or $b^i \equiv 1 \bmod N$. Since b has order d, d must divide i, so i must equal 0.

So the only elements in the center of $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/d\mathbb{Z}$ are powers of t. But for $j < N$, t^j is central if and only if $\gamma^{-1}t^j\gamma = t^j$, or equivalently, $t^{j(b-1)} = 1$. But this occurs precisely when N divides $j(b-1)$. Finally, such a j exists if and only if $j = 0$ or $\gcd(N, b-1) > 1$. □

THEOREM 4. *A) Suppose $d \geq 2$ is a positive integer, ζ_d is a primitive d'th root of unity, and $\mathcal{N}$ is an ideal of $\mathbb{Z}[\zeta_d]$ relatively prime to d. Let $G = \mathbb{Z}[\zeta_d]/\mathcal{N} \rtimes \langle\zeta_d\rangle$ and suppose $\mathcal{C}$ is the conjugacy class of $[\zeta_d]$ in G. Then $Y_0(\mathcal{N})$ (see §2 for the definition of $Y_0(\mathcal{N})$ is a reduced Hurwitz space for coverings of $\mathbb{P}^1$ ramified over 4 points with monodromy group G and ramification data $(\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}^{-3})$.*

B) Suppose $d \geq 2$ is a positive integer, and N is a positive integer relatively prime to d. Suppose b is an integer with multiplicative order d mod N. Let

$$G = \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/d\mathbb{Z} = \{\gamma, t : \gamma^d = t^N = 1, \gamma^{-1}t\gamma = t^b\},$$

and suppose G has trivial center. Let $\mathcal{C}$ be the conjugacy class of γ. Suppose ζ_d is a primitive root of unity and that $\mathcal{N}$ is the ideal $(N, \zeta_d - b)$. Then $Y_0(\mathcal{N})$ is a reduced Hurwitz space for coverings of $\mathbb{P}^1$ ramified over 4 points with monodromy group G and ramification data $(\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}^{-3})$.

Proof. A) follows directly from theorem 3 and proposition 3.
Since $\mathbb{Z}[\zeta_d]/\mathcal{N} \cong \mathbb{Z}/M\mathbb{Z}$, where

$$M = \frac{N}{gcd(N, 1-b)},$$

we have $\mathbb{Z}[\zeta_d]/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$ under the conditions of the theorem. Thus B) follows from A). □

6.2. Geometric interpretation

Recall that that $Y_0(N)$ parametrizes elliptic curves together with an isogeny of degree N. Equivalently (by Fried's theorem), for N odd, $Y_0(N)$ parametrizes equivalence classes of diagrams of the form

$$\begin{array}{ccc} E' & \xrightarrow{\alpha} & E \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow{\beta} & \mathbb{P}^1 \end{array},$$

where E' and E are elliptic curves, the vertical maps are of degree 2 and are ramified over four points, and α is an isogeny of degree N. We require the map β to be non-Galois of degree N, with Galois closure E' and monodromy group D_N. This then implies that β has ramification data as in theorem 1. Finally, we consider two diagrams to be equivalent if and only if the lower horizontal maps are equivalent mod $PSL_2(\mathbb{C})$.

Theorem 4A then states that $Y_0(\mathcal{N})$ parametrizes equivalence classes of diagrams of the following form:

$$\begin{array}{ccc} Y & \xrightarrow{\alpha} & X \\ \downarrow & & \downarrow \gamma \\ W & \xrightarrow{\beta} & \mathbb{P}^1 \end{array}.$$

We require all maps to be ramified over 4 points, and the vertical maps to be Galois, with monodromy group $\mathbb{Z}/d\mathbb{Z} = \langle \zeta_d \rangle$. In addition, the map

γ should have ramification data of the form $(\zeta_d, \zeta_d, \zeta_d, \zeta_d^{-3})$ (here, ζ_d is its own conjugacy class in $\mathbb{Z}/d\mathbb{Z} = \langle\zeta_d\rangle$). Furthermore, α must be Galois with group $\mathbb{Z}[\zeta_d]/\mathcal{N}$. Finally, in the notation of theorem 4A, we require β to have monodromy group G and ramification data $(\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}^{-3})$.

We note that once we specify the map β, Y and X will be uniquely determined. Two diagrams are considered to be equivalent if and only if the lower horizontal maps are equivalent mod $PSL_2(\mathbb{C})$.

7. Modular Towers

We now interpret our results in terms of Fried's concept of modular tower ([F2], [F-K]). Suppose G is a finite group and that p is a prime dividing the order of G. We follow the notation of [F2]: ${}_p\widetilde{G}$ denotes the universal p-Frattini cover of G, and ${}_p^n\widetilde{G}$ denotes the n'th characteristic quotient of ${}_p\widetilde{G}$. Fix an integer $d \geq 2$, and a prime $\mathfrak{p}$ in $\mathbb{Z}[\zeta_d]$ lying over a rational prime integer p. For any natural number n, let $G(\mathfrak{p}^n)$ denote the semi-direct product $\mathbb{Z}[\zeta_d]/\mathfrak{p}^n \rtimes \langle\zeta_d\rangle$.

PROPOSITION 4. *For all natural numbers n, ${}_p\widetilde{G(\mathfrak{p}^n)} = \mathbb{Z}[\zeta_d]_{\mathfrak{p}} \rtimes \langle\zeta_d\rangle$. If $p\mathbb{Z}[\zeta_d] = \mathfrak{p}$, then ${}_p^n\widetilde{G(\mathfrak{p}^1)} = G(\mathfrak{p}^{n+1})$.*

PROOF. The first statement follows from the fact (see [F2]) that ${}_p\widetilde{G}$ is the smallest Frattini cover of G with a projective p- Sylow subgroup. The second follows from the fact that ${}_p^n\widetilde{G(\mathfrak{p}^1)} = {}_p\widetilde{G(\mathfrak{p}^1)}/p^n\mathfrak{p} = {}_p\widetilde{G(\mathfrak{p}^1)}/\mathfrak{p}^{n+1}$. □

Thus if $p\mathbb{Z}[\zeta_d] = \mathfrak{p}$, we obtain a modular tower

$$\cdots \to X_0(\mathfrak{p}^{n+1}) \to X_0(\mathfrak{p}^n) \to \dots$$

of reduced Hurwitz spaces.

References

[A-Sw] Atkin, O. and H. P. F. Swinnerton-Dyer, Modular Forms on Noncongruence Subgroups, Proc. Symp. Pure Math. AMS **XIX** (1971), 1–25.

[Be] Belyi, G. V., On Extensions of the Maximal Cyclotomic Field Having a Given Galois Group, J. Reine. Angew. Math. **341** (1983), 1–25.

[B] Berger, G., Hecke Operators on Non-congruence Subgroups, t 319, Series 1 C.R. Acad. Sci. Paris (1994), 915–919.

[B2] Berger, G., Fake Congruence Subgroups and the Hurwitz Monodromy Group, to appear in the Journal of Algebra (1999).

[B-F] Berger, G. and M. Fried, The Hurwitz Monodromy Group H_4, in preparation (1997).

[C] Cohen, H., A Course in Computational Algebraic Number Theory, GTM 138, Springer-Verlag, 1993.

[Bi] Birman, J., Braids, Links, and Mapping Class Groups, Princeton, 1973.

[D-F] Debes, P. and M. Fried, Integral Specialization of Families of Rational Functions, to appear.

[F] Fried, M., Arithmetic of 3 and 4 Branch Point Covers: A Bridge Provided by Noncongruence Subgroups of SL(2,Z), Sem. de Theorie des Nombres, Paris 1987–88, 77–117, Prog. Math. 81, Birkhauser, 1990.

[F-K] Fried, M. and Y. Kopeliovich, Applying Modular Towers to the Inverse Galois Problem, to appear.

[F-V] Fried, M. and H. Volklein, The Inverse Galois Problem and Rational Points on Moduli Spaces, Math. Ann. **290** no. 4 (1991), 771–800.

[F2] Fried, M., Introduction to Modular Towers: Generalizing Dihedral Group-Modular Curve Connections, Recent Developments in the Inverse Galois Problem, pp. 111–173, Contemporary Mathematics, no. 186, 1995.

[F-H] Fulton, W. and J. Harris,Representation Theory: A First Course, Springer-Verlag, New York, 1991.

[K] Koblitz, N., Introduction To Elliptic Curves and Modular Forms, Springer-Verlag, New York, 1984.

[M] Macbeath, A. M., Generators of the Linear Fractional Groups, Proc. Symp. Pure Math. **12** (1968), 14–32.

[O-T] Oda, T. and T. Terasoma, Surjectivity of Reductions of the Burau Representation of Artin Braid Groups, draft (1995).

[Sch] Scholl, A. J., Modular Forms and de Rham Cohomology; Atkin-Swinnerton-Dyer congruences, Invent. Math. **79** (1985), 49–77.

[V] Volklein, H., Braid Group Action via $GL(n,q)$ and $U(n,q)$, and Galois Realizations, Israel J. Math. **82** (1993), 405–427.

[W] Wolfahrt, K., An Extension of F Klein's Level Concept, IJM **8**, 529–535.

(Received August 8, 1998)

Department of Mathematics
The University of California at Irvine
Irvine, CA 92697-3875
U.S.A.
E-mail: gberger@math.uci.edu