International Electronic Journal of Algebra
Volume 28 (2020) 156-174
DOI: 10.24330/ieja.768210

MODULAR GROUP IMAGES ARISING FROM DRINFELD DOUBLES OF DIHEDRAL GROUPS

Deepak Naidu

Received: 28 October 2019; Revised: 30 May 2020; Accepted: 31 May 2020
Communicated by A. Çiğdem Özcan

Abstract. We show that the image of the representation of the modular group $\mathrm{SL}(2,\mathbb{Z})$ arising from the representation category $\mathrm{Rep}(D(G))$ of the Drinfeld double $D(G)$ is isomorphic to the group $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z}) \times S_3$, when G is either the dihedral group of order $2n$ or the dihedral group of order $4n$ for some odd integer $n \geq 3$.

Mathematics Subject Classification (2020): 18M20
Keywords: Drinfeld double, modular tensor category, modular group, congruence subgroup

1. Introduction

The modular group $\mathrm{SL}(2,\mathbb{Z})$ is the group of all 2×2 matrices of determinant 1 whose entries belong to the ring $\mathbb{Z}$ of integers. The modular group is known to play a significant role in conformal field theory [3]. Every two-dimensional rational conformal field theory gives rise to a finite-dimensional representation of the modular group, and the kernel of this representation has been of much interest. In particular, the question whether the kernel is a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ has been investigated by several authors. For example, A. Coste and T. Gannon in their paper [4] showed that under certain assumptions the kernel is indeed a congruence subgroup. In the present paper, we consider the kernel of the representation of the modular group arising from Drinfeld doubles of dihedral groups.

The group $\mathrm{SL}(2,\mathbb{Z})$ is generated by the matrices

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad Y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

and these matrices satisfy the relations

$$X^4 = I \qquad \text{and} \qquad (XY)^3 = X^2.$$

In fact, the relations above are defining relations for the modular group, that is, the modular group has the presentation

$$\langle X, Y \mid X^4 = 1, (XY)^3 = X^2 \rangle.$$

Let G be a finite group, let $D(G)$ denote the Drinfeld double of G, a quasi-triangular semisimple Hopf algebra, and let $\mathrm{Rep}(D(G))$ denote the category of finite-dimensional complex representations of $D(G)$. The category $\mathrm{Rep}(D(G))$ is a modular tensor category [1], and it comes equipped with a pair of invertible matrices S and T, called the S-matrix and T-matrix of $\mathrm{Rep}(D(G))$, and they satisfy the relations

$$S^4 = I \qquad \text{and} \qquad (ST)^3 = S^2. \tag{1}$$

Therefore, $\mathrm{Rep}(D(G))$ gives rise to a representation

$$\rho : \mathrm{SL}(2, \mathbb{Z}) \to \langle S, T \rangle$$

of the modular group such that $\rho(X) = S$ and $\rho(Y) = T$.

In their paper [9], Y. Sommerhäuser and Y. Zhu showed that the kernels of the representations of the modular group arising from factorizable semisimple Hopf algebras and from Drinfeld doubles of semisimple Hopf algebras are congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$. Later, S-H Ng and P. Schauenburg generalized the results of Y. Sommerhäuser and Y. Zhu to spherical fusion categories [8]. It follows from results in [9] that the kernel of ρ is a congruence subgroup. As a consequence, the image of ρ is finite. Our work gives a direct proof of this fact for dihedral groups of certain orders. Specifically, we show that if G is either the dihedral group of order $2n$ or the dihedral group of order $4n$ for some odd integer $n \geq 3$, then the image of ρ is isomorphic to the group $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z}) \times S_3$, where $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ denotes the projective special linear group, S_3 denotes the symmetric group on three letters, and $\mathbb{Z}/n\mathbb{Z}$ denotes the ring of integers modulo n.

Organization:

In Section 2, we recall basic facts about the modular tensor category $\mathrm{Rep}(D(G))$, and a description of the S-matrix and T-matrix for the dihedral groups.

In Section 3, we recall a presentation of the projective special linear group $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$, and a description of its normal subgroups.

Section 4 contains our main result in which we establish that when G is either the dihedral group of order $2n$ or the dihedral group of order $4n$ for some odd integer $n \geq 3$, the image of ρ is isomorphic to the group $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z}) \times S_3$.

Convention and notation:

Throughout this paper we work over the field $\mathbb{C}$ of complex numbers. The multiplicative group of nonzero complex numbers is denoted $\mathbb{C}^\times$. We will use the Kronecker symbol $\delta_{x,y}$, which is equal to 1 if $x = y$ and zero otherwise. For any character α of a group, $\deg \alpha$ denotes the degree of α, and $\overline{\alpha}$ denotes the complex conjugate of α. We denote by $[x]_n$ the image of the integer x in the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n; on occasions we will suppress the brackets as well as the subscript n.

2. Drinfeld doubles of finite groups

Let G be a finite group, let $D(G)$ denote the Drinfeld double of G, a quasi-triangular semisimple Hopf algebra, and let $\mathrm{Rep}(D(G))$ denote the category of finite-dimensional representations of $D(G)$. The category $\mathrm{Rep}(D(G))$ is a modular tensor category [1]. The simple objects of $\mathrm{Rep}(D(G))$ are in bijection with the set of pairs (x, α), where x is a representative of a conjugacy class of G, and α is an irreducible character of the centralizer $C_G(x)$ of x in G. The S-matrix and the T-matrix of $\mathrm{Rep}(D(G))$ are square matrices indexed by the simple objects of $\mathrm{Rep}(D(G))$, and are given by the following formulas [1,5].

$$\begin{aligned}
S_{(x,\alpha),(y,\beta)} &= \frac{1}{|C_G(x)||C_G(y)|} \sum_{g \in G(x,y)} \overline{\alpha}(gyg^{-1})\overline{\beta}(g^{-1}xg), \\
T_{(x,\alpha),(y,\beta)} &= \delta_{x,y}\delta_{\alpha,\beta}\frac{\alpha(x)}{\deg \alpha},
\end{aligned}$$

where $G(x, y)$ denotes the set $\{g \in G \mid xgyg^{-1} = gyg^{-1}x\}$. The function $G(x, y) \to G(y, x)$ that sends each element g to g^{-1} is a bijection, and as a consequence the matrix S is symmetric.

We have

$$T^{\exp(G)} = I, \tag{2}$$

where $\exp(G)$ denotes the exponent of G. In fact, the order of T is precisely $\exp(G)$ [5].

There is an involution $*$ on the set of simple objects of $\mathrm{Rep}(D(G))$ given by $(x, \alpha)^* = (g^{-1}x^{-1}g, \overline{\chi}^g)$, where g is an element of G such that $g^{-1}x^{-1}g$ is the element chosen to represent the conjugacy class of x^{-1}. The so-called *charge conjugation matrix* is the square matrix C indexed by the simple objects of $\mathrm{Rep}(D(G))$ defined by $C_{(x,\alpha),(y,\beta)} = \delta_{(x,\alpha)^*,(y,\beta)}$. We have $S^2 = C$ [1].

The S-matrix and T-matrix of $\mathrm{Rep}(D(G))$ when $G = G_1 \times G_2$ for finite groups G_1 and G_2 are given by the Kronecker products $S_1 \otimes S_2$ and $T_1 \otimes T_2$, where S_i and T_i denote the S-matrix and T-matrix of $\mathrm{Rep}(D(G_i))$, $i = 1, 2$.

Example 2.1. Let n be an integer with $n \geq 3$, and let Dih_n denote the Dihedral group of order $2n$ generated by the elements a and b subject to the relations $a^n = e$, $b^2 = e$, and $ba = a^{-1}b$.

(a) Suppose that n is even. Then there are $(n/2)+3$ conjugacy classes in Dih_n, and they are

$$\{e\},\ \{a^{n/2}\},\ \{a^k, a^{-k}\}\ (1 \leq k < n/2),\ \{a^{2k}b \mid 0 \leq k < n/2\},$$

$$\{a^{2k+1}b \mid 0 \leq k < n/2\}.$$

We choose the elements e, a^k $(1 \leq k \leq n/2)$, b, and ab as representatives of the conjugacy classes. The centralizers of these elements are

$$\begin{aligned} C(e) &= \mathrm{Dih}_n \\ C(a^{n/2}) &= \mathrm{Dih}_n \\ C(a^k) &= \langle a \rangle \qquad (1 \leq k < n/2) \\ C(b) &= \{e, b, a^{n/2}, a^{n/2}b\} \\ C(ab) &= \{e, ab, a^{n/2}, a^{1+n/2}b\}. \end{aligned}$$

The center of Dih_n is the subgroup $\{e, a^{n/2}\}$, and the character table of Dih_n is

	e	a^k	b	ab
χ_0	1	1	1	1
χ_1	1	$(-1)^k$	1	-1
χ_2	1	1	-1	-1
χ_3	1	$(-1)^k$	-1	1
ψ_i	2	$2\cos\left(\frac{2\pi ik}{n}\right)$	0	0

where $1 \leq i \leq (n/2) - 1$ and $1 \leq k \leq n/2$.

Let $\zeta = e^{\frac{2\pi i}{n}}$, a primitive nth root of unity. For each $1 \leq i \leq n$, let

$$\alpha_i : \langle a \rangle \to \mathbb{C}^\times$$

denote the group homomorphism that sends a to ζ^i. For $i, j \in \{0, 1\}$, let

$$\beta_{i,j} : \{e, b, a^{n/2}, a^{n/2}b\} \to \mathbb{C}^\times$$

denote the group homomorphism that sends b to $(-1)^i$ and sends $a^{n/2}$ to $(-1)^j$, and let

$$\gamma_{i,j} : \{e, ab, a^{n/2}, a^{1+n/2}b\} \to \mathbb{C}^\times$$

denote the group homomorphism that sends ab to $(-1)^i$ and sends $a^{n/2}$ to $(-1)^j$.

The simple objects of $\mathrm{Rep}(D(\mathrm{Dih}_n))$ are in bijection with the set consisting of the following pairs.

$$\begin{array}{rl}
(e, \chi_i) & 0 \leq i \leq 3 \\
(e, \psi_i) & 1 \leq i \leq (n/2) - 1 \\
(a^{n/2}, \chi_i) & 0 \leq i \leq 3 \\
(a^{n/2}, \psi_i) & 1 \leq i \leq (n/2) - 1 \\
(a^k, \alpha_i) & 1 \leq k < n/2, 1 \leq i \leq n \\
(b, \beta_{i,j}) & i, j \in \{0, 1\} \\
(ab, \gamma_{i,j}) & i, j \in \{0, 1\}
\end{array}$$

Set

$$\Delta_i = \begin{cases} 1 & \text{if } i = 0, 1 \\ -1 & \text{if } i = 2, 3 \end{cases} \qquad \text{and} \qquad \Delta'_i = \begin{cases} 1 & \text{if } i = 0, 3 \\ -1 & \text{if } i = 1, 2. \end{cases}$$

Then the S-matrix is given by the first three tables below, and the T-matrix is given by the fourth table below.

S	(e, χ_j)	(e, ψ_j)	$(a^{n/2}, \chi_j)$	$(a^{n/2}, \psi_j)$	(a^ℓ, α_j)
(e, χ_i)	$\frac{1}{2n}$	$\frac{1}{n}$	$\frac{1}{2n} \cdot (-1)^{ni/2}$	$\frac{1}{n} \cdot (-1)^{ni/2}$	$\frac{1}{n} \cdot (-1)^{\ell i}$
(e, ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{1}{n} \cdot (-1)^i$	$\frac{2}{n} \cdot (-1)^i$	$\frac{2}{n} \cdot \cos\left(\frac{2\pi\ell i}{n}\right)$
$(a^{n/2}, \chi_i)$	$\frac{1}{2n} \cdot (-1)^{nj/2}$	$\frac{1}{n} \cdot (-1)^j$	$\frac{1}{2n} \cdot (-1)^{n(i+j)/2}$	$\frac{1}{n} \cdot (-1)^{j+(ni/2)}$	$\frac{1}{n} \cdot (-1)^{j+\ell i}$
$(a^{n/2}, \psi_i)$	$\frac{1}{n} \cdot (-1)^{nj/2}$	$\frac{2}{n} \cdot (-1)^j$	$\frac{1}{n} \cdot (-1)^{i+(nj/2)}$	$\frac{2}{n} \cdot (-1)^{i+j}$	$\frac{2(-1)^j}{n} \cdot \cos\left(\frac{2\pi\ell i}{n}\right)$
(a^k, α_i)	$\frac{1}{n} \cdot (-1)^{kj}$	$\frac{2}{n} \cdot \cos\left(\frac{2\pi kj}{n}\right)$	$\frac{1}{n} \cdot (-1)^{i+kj}$	$\frac{2(-1)^i}{n} \cdot \cos\left(\frac{2\pi kj}{n}\right)$	$\frac{2}{n} \cdot \left(\frac{2\pi(\ell i+kj)}{n}\right)$

S	$(b, \beta_{i',j'})$
(e, χ_i)	$\frac{1}{4} \cdot \Delta_i$
(e, ψ_i)	0
$(a^{n/2}, \chi_i)$	$\frac{1}{4} \cdot \Delta_i \cdot (-1)^{j'}$
$(a^{n/2}, \psi_i)$	0
(a^k, α_i)	0
$(b, \beta_{i,j})$	$\frac{1}{4} \cdot \begin{cases} (-1)^{i+i'} + (-1)^{i+j+i'+j'} & \text{if } 4 \mid n \\ (-1)^{i+i'} & \text{if } 4 \nmid n \end{cases}$
$(ab, \gamma_{i,j})$	$\begin{cases} 0 & \text{if } 4 \mid n \\ \frac{1}{4} \cdot (-1)^{i+j+i'+j'} & \text{if } 4 \nmid n \end{cases}$

S	$(ab, \gamma_{i',j'})$
(e, χ_i)	$\frac{1}{4} \cdot \Delta'_i$
(e, ψ_i)	0
$(a^{n/2}, \chi_i)$	$\frac{1}{4} \cdot \Delta'_i \cdot (-1)^{j'}$
$(a^{n/2}, \psi_i)$	0
(a^k, α_i)	0
$(b, \beta_{i,j})$	$\begin{cases} 0 & \text{if } 4 \mid n \\ \frac{1}{4} \cdot (-1)^{i+j+i'+j'} & \text{if } 4 \nmid n \end{cases}$
$(ab, \gamma_{i,j})$	$\frac{1}{4} \cdot \begin{cases} (-1)^{i+i'} + (-1)^{i+j+i'+j'} & \text{if } 4 \mid n \\ (-1)^{i+i'} & \text{if } 4 \nmid n \end{cases}$

T	(e, χ_i)	(e, ψ_i)	$(a^{n/2}, \chi_i)$	$(a^{n/2}, \psi_i)$	(a^k, α_i)	$(b, \beta_{i,j})$	$(ab, \gamma_{i,j})$
	1	1	$(-1)^{ni/2}$	$(-1)^i$	ζ^{ki}	$(-1)^i$	$(-1)^i$

(b) Suppose that n is odd. Then there are $(n+3)/2$ conjugacy classes in Dih_n, and they are

$$\{e\}, \quad \{a^k, a^{-k}\} \quad (1 \le k \le (n-1)/2), \quad \{a^k b \mid 0 \le k < n\}.$$

We choose the elements e, a^k $(1 \le k \le (n-1)/2)$, and b as representatives of the conjugacy classes. The centralizers of these elements are

$$\begin{aligned} C(e) &= \mathrm{Dih}_n \\ C(a^k) &= \langle a \rangle \qquad (1 \le k \le (n-1)/2) \\ C(b) &= \{e, b\}. \end{aligned}$$

The center of Dih_n is trivial in this case, and the character table of Dih_n is

	e	a^k	b
χ_0	1	1	1
χ_1	1	1	-1
ψ_i	2	$2\cos\left(\frac{2\pi ik}{n}\right)$	0

where $1 \le i \le (n-1)/2$ and $1 \le k \le (n-1)/2$.

Let $\zeta = e^{\frac{2\pi i}{n}}$, a primitive nth root of unity. For each $1 \le i \le n$, let

$$\alpha_i : \langle a \rangle \to \mathbb{C}^\times$$

denote the group homomorphism that sends a to ζ^i. For $i \in \{0, 1\}$, let

$$\beta_i : \{e, b\} \to \mathbb{C}^\times$$

denote the group homomorphism that sends b to $(-1)^i$.

The simple objects of $\mathrm{Rep}(D(\mathrm{Dih}_n))$ are in bijection with the set consisting of the pairs

$$\begin{aligned} &(e, \chi_i) && i \in \{0, 1\} \\ &(e, \psi_i) && 1 \le i \le (n-1)/2 \\ &(a^k, \alpha_i) && 1 \le k \le (n-1)/2, 1 \le i \le n \\ &(b, \beta_i) && i \in \{0, 1\}, \end{aligned}$$

and the S-matrix and the T-matrix are given by the following tables.

S	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2n}$	$\frac{1}{n}$	$\frac{1}{n}$	$\frac{1}{2}\cdot(-1)^i$
(e,ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi\ell i}{n}\right)$	0
(a^k,α_i)	$\frac{1}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi kj}{n}\right)$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi(kj+\ell i)}{n}\right)$	0
(b,β_i)	$\frac{1}{2}\cdot(-1)^j$	0	0	$\frac{1}{2}\cdot(-1)^{i+j}$

T	(e,χ_i)	(e,ψ_i)	(a^k,α_i)	(b,β_i)
	1	1	ζ^{ki}	$(-1)^i$

3. Projective special linear groups

For any commutative ring R, the special linear group $\mathrm{SL}(2,R)$ is the group consisting of all 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ with $a,b,c,d\in R$ such that $ad-bc=1$. Let n be a positive integer. Of particular interest is the special linear group $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$, where $\mathbb{Z}/n\mathbb{Z}$ is the ring of integers modulo n. The order of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ for $n\geq 2$ is given by the following formula [6].

$$|\,\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})| = n^3\prod_{p|n}\left(1-\frac{1}{p^2}\right),$$

where p runs over all primes that divide n.

If n is odd, then

$$\left\langle X,Y\,\middle|\,X^4=1,(XY)^3=X^2,Y^n=1,\left(XY^{\frac{n+1}{2}}XY^2\right)^3=1\right\rangle$$

is a presentation of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ [2], and if n is a power of 2, then

$$\left\langle X,Y\,\middle|\,X^4=1,(XY)^3=X^2,Y^n=1,W(k)XW(k)=X,W(k)Y=Y^{k^2}W(k)\right\rangle$$

is a presentation of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ [9,4], where k runs over all odd integers between 1 and n, $W(k)=XY^\ell X^{-1}Y^kXY^\ell$, and ℓ is an integer such that $k\ell\equiv 1 \pmod n$. The matrices

$$X=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\qquad\text{and}\qquad Y=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},$$

where the entries of the matrices are identified with their images in the ring $\mathbb{Z}/n\mathbb{Z}$, satisfy the relations in both the cases above.

The projective special linear group $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ is defined by

$$\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})/\pm I,$$

where I is the identity matrix. If n is odd, then

$$\left\langle X, Y \,\middle|\, X^2 = 1, (XY)^3 = 1, Y^n = 1, \left(XY^{\frac{n+1}{2}}XY^2\right)^3 = 1 \right\rangle$$

is a presentation of $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ [2]. The cosets

$$X = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad Y = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

satisfy the relations given above.

The group homomorphism $\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ induced by the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is surjective [6]. It follows that for each positive divisor r of n, the group homomorphism

$$\phi^n_r : \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/r\mathbb{Z})$$

induced by the ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ is surjective.

Let r be a positive divisor of n. A subgroup H of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ is said to be of **level** r if there exists a subgroup K of $\mathrm{SL}(2,\mathbb{Z}/r\mathbb{Z})$ such that $H = \left(\phi^r_n\right)^{-1}(K)$ and r is minimal with this property. We record the following result for later use.

Lemma 3.1. *Let n be a positive integer.*

(a) *If r_1 and r_2 are positive divisors of n such that r_2 divides r_1, then* $\mathrm{Ker}\,\phi^n_{r_1} \leq \mathrm{Ker}\,\phi^n_{r_2}$.

(b) *If H is a subgroup of* $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ *of level r such that $r \neq n$, then H contains* $\mathrm{Ker}\,\phi^n_{n/p}$ *for some prime p that divides n.*

Let $n = n_1 n_2 \cdots n_t$ denote the decomposition of n into a product of powers of distinct primes. Choose integers $u_1, u_2, \ldots, u_t$ such that

$$\frac{n}{n_i} \cdot u_i \equiv 1 \pmod{n_i}$$

for $i = 1, 2, \ldots, t$. The function

$$\prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z} \xrightarrow{\ \sim\ } \mathbb{Z}/n\mathbb{Z} : ([a_1]_{n_1}, [a_2]_{n_2}, \ldots, [a_t]_{n_t}) \mapsto \left[\sum_{i=1}^{t} \frac{n}{n_i} \cdot u_i \cdot a_i\right]_n$$

is a ring isomorphism, and it induces a group isomorphism

$$\mathrm{SL}\left(2, \prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z}\right) \xrightarrow{\ \sim\ } \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z}).$$

Using the natural group isomorphism

$$\prod_{i=1}^{t} \mathrm{SL}\left(2, \mathbb{Z}/n_i\mathbb{Z}\right) \xrightarrow{\sim} \mathrm{SL}\left(2, \prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z}\right)$$

we obtain the group isomorphism

$$\prod_{i=1}^{t} \mathrm{SL}\left(2, \mathbb{Z}/n_i\mathbb{Z}\right) \xrightarrow{\sim} \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$$

that sends the tuple

$$\left(\begin{pmatrix} [a_1]_{n_1} & [b_1]_{n_1} \\ [c_1]_{n_1} & [d_1]_{n_1} \end{pmatrix}, \begin{pmatrix} [a_2]_{n_2} & [b_2]_{n_2} \\ [c_2]_{n_2} & [d_2]_{n_2} \end{pmatrix}, \dots, \begin{pmatrix} [a_t]_{n_t} & [b_t]_{n_t} \\ [c_t]_{n_t} & [d_t]_{n_t} \end{pmatrix} \right)$$

of matrices to the matrix

$$\begin{pmatrix} \left[\sum_{i=1}^{t} \frac{n}{n_i} \cdot u_i \cdot a_i\right]_n & \left[\sum_{i=1}^{t} \frac{n}{n_i} \cdot u_i \cdot b_i\right]_n \\ \left[\sum_{i=1}^{t} \frac{n}{n_i} \cdot u_i \cdot c_i\right]_n & \left[\sum_{i=1}^{t} \frac{n}{n_i} \cdot u_i \cdot d_i\right]_n \end{pmatrix}.$$

We will use this isomorphism in the next section.

The following result was proved by D. L. McQuillan in the paper [7].

Theorem 3.2. *Let n be an odd positive integer. The normal subgroups of level n of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ are precisely the subgroups of the center of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$, with the exception that if $3 \mid n$ and $3^2 \nmid n$, then in addition there are normal subgroups KC, where K is the image in $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ of the unique Sylow 2-subgroup of $\mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z})$ and C is a subgroup of the center of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$.*

Let $\pi : \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ denote the natural projection. We deduce immediately the following from Theorem 3.2.

Corollary 3.3. *Let n be an odd positive integer. The subgroups*

$$\begin{array}{ll} C & \\ \pi(H) & \\ \pi(K)C & \quad (\textit{if } 3 \mid n \textit{ and } 3^2 \nmid n) \end{array}$$

exhaust all the normal subgroups of $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$, where C is a subgroup of the center of $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$, H is a subgroup of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ of level less than n, and K is the image in $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ of the unique Sylow 2-subgroup of $\mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z})$.

We note that the center of $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ consists of all cosets of the form $\pm \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ with $a^2 \equiv 1 \pmod{n}$ [7], and the unique Sylow 2-subgroup of $\mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z})$ is the subgroup $\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & -1 \\ -1 & 1 \end{smallmatrix}\right) \rangle$.

4. Main result

Let n be an odd integer with $n \geq 3$, and let Dih_n denote the Dihedral group of order $2n$ generated by the elements a and b subject to the relations $a^n = e$, $b^2 = e$, and $ba = a^{-1}b$. In this section, we determine the group structure of the image of the representation of the modular group $\mathrm{SL}(2,\mathbb{Z})$ arising from the modular tensor category $\mathrm{Rep}(D(\mathrm{Dih}_n))$. For a description of the simple objects of $\mathrm{Rep}(D(\mathrm{Dih}_n))$ and the corresponding S-matrix and T-matrix we refer the reader to Example 2.1.

The charge conjugation matrix associated to $\mathrm{Rep}(D(\mathrm{Dih}_n))$ is the identity, and so $S^2 = I$ Therefore, the relations in (1) reduce to the following.

$$S^2 = I \qquad \text{and} \qquad (ST)^3 = I. \tag{3}$$

Since the group Dih_n has exponent $2n$, the relation in (2) gives $T^{2n} = I$. We note that, in fact, the order of T is precisely $2n$.

We will need the matrices ST^nS, $ST^{n+1}S$, and $ST^{n-1}S$, described below.

ST^nS	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2}$	0	0	$\frac{1}{2}\cdot(-1)^{i+j}$
(e,ψ_i)	0	$\delta_{i,j}$	0	0
(a^k,α_i)	0	0	$\delta_{i,j}\delta_{k,\ell}$	0
(b,β_i)	$\frac{1}{2}\cdot(-1)^{i+j}$	0	0	$\frac{1}{2}$

$ST^{n+1}S$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2n}+\frac{1}{2}\cdot(-1)^{i+j}$	$\frac{1}{n}$	$\frac{1}{n}\cdot\zeta^{-\ell j}$	0
(e,ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi\ell i}{n}\right)\cdot\zeta^{-\ell j}$	0
(a^k,α_i)	$\frac{1}{n}\cdot\zeta^{-ki}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi kj}{n}\right)\cdot\zeta^{-ki}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi(kj+\ell i)}{n}\right)\cdot\zeta^{-(ki+\ell j)}$	0
(b,β_i)	0	0	0	$\delta_{i,j}$

$ST^{n-1}S$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2n}+\frac{1}{2}\cdot(-1)^{i+j}$	$\frac{1}{n}$	$\frac{1}{n}\cdot\zeta^{\ell j}$	0
(e,ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi\ell i}{n}\right)\cdot\zeta^{\ell j}$	0
(a^k,α_i)	$\frac{1}{n}\cdot\zeta^{ki}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi kj}{n}\right)\cdot\zeta^{ki}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi(kj+\ell i)}{n}\right)\cdot\zeta^{ki+\ell j}$	0
(b,β_i)	0	0	0	$\delta_{i,j}$

The computations involved in determining the matrices above are routine, albeit tedious. As a sample, we show the computation of one entry. The entry of the matrix $ST^{n+1}S$ corresponding to the pair $((a^k,\alpha_i),(a^\ell,\alpha_j))$ can be computed as follows.

$$\sum_{r=0,1} ST^{n+1}_{(a^k,\alpha_i),(e,\chi_r)} S_{(e,\chi_r),(a^\ell,\alpha_j)} + \sum_{r=1}^{(n-1)/2} ST^{n+1}_{(a^k,\alpha_i),(e,\psi_r)} S_{(e,\psi_r),(a^\ell,\alpha_j)}$$
$$+ \sum_{r=1}^{(n-1)/2}\sum_{s=1}^{n} ST^{n+1}_{(a^k,\alpha_i),(a^r,\alpha_s)} S_{(a^r,\alpha_s),(a^\ell,\alpha_j)}$$
$$= \sum_{r=0,1}\frac{1}{n^2} + \sum_{r=1}^{n}\frac{4}{n^2}\cdot\cos\left(\frac{2\pi kr}{n}\right)\cdot\cos\left(\frac{2\pi\ell r}{n}\right)$$
$$+ \sum_{r=1}^{(n-1)/2}\sum_{s=1}^{n}\frac{4}{n^2}\cdot\cos\left(\frac{2\pi(ks+ri)}{n}\right)\cdot\cos\left(\frac{2\pi(rj+\ell s)}{n}\right)\cdot\zeta^{rs}$$

Applying a trigonometric identity, we get the following expression.

$$= \frac{2}{n^2} + \frac{2}{n^2}\sum_{r=1}^{n}\left[\cos\left(\frac{2\pi r(k+\ell)}{n}\right) + \cos\left(\frac{2\pi r(k-\ell)}{n}\right)\right]$$
$$+ \frac{2}{n^2}\sum_{r=1}^{(n-1)/2}\sum_{s=1}^{n}\left[\cos\left(\frac{2\pi(ks+ri+rj+\ell s)}{n}\right)\right.$$
$$\left. + \cos\left(\frac{2\pi(ks+ri-rj-\ell s)}{n}\right)\right]\cdot\zeta^{rs}$$

$$= \frac{2}{n^2} + \frac{1}{n^2}(-2 + n\delta_{k,\ell}) + \frac{1}{n^2} \sum_{r=1}^{(n-1)/2} \sum_{s=1}^{n} \Big[\zeta^{r(i+j)} \cdot \zeta^{(k+\ell+r)s} + \zeta^{-r(i+j)} \cdot \zeta^{(-k-\ell+r)s}$$
$$+\zeta^{r(i-j)} \cdot \zeta^{(k-\ell+r)s} + \zeta^{-r(i-j)} \cdot \zeta^{(-k+\ell+r)s}\Big]$$
$$= \frac{1}{n} \cdot \left(\zeta^{-(k+\ell)(i+j)} + \zeta^{(\ell-k)(i-j)}\right)$$
$$= \frac{2}{n} \cdot \cos\left(\frac{2\pi(kj+\ell i)}{n}\right) \cdot \zeta^{-(ki+\ell j)},$$

where we used the formulas

$$\sum_{i=1}^{(n-1)/2} 2\cos\left(\frac{2\pi ki}{n}\right) = \begin{cases} n-1 & \text{if } n \mid k \\ -1 & \text{if } n \nmid k \end{cases}$$

and

$$\sum_{i=1}^{n} \zeta^{ki} = \begin{cases} n & \text{if } n \mid k \\ 0 & \text{if } n \nmid k. \end{cases}$$

Lemma 4.1. *Let n be an odd integer with $n \geq 3$, let S and T denote the matrices associated to the modular tensor category* $\mathrm{Rep}(D(\mathrm{Dih}_n))$*, and let $A = ST^nST^n$ and $B = T^n$. The matrices A and B have orders 3 and 2, respectively, and satisfy the relation $BA = A^{-1}B$, and therefore the group $\langle A, B\rangle$ generated by A and B is isomorphic to S_3.*

Proof. The matrix A is described below.

$A = ST^nST^n$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2}$	0	0	$\frac{1}{2}\cdot(-1)^i$
(e,ψ_i)	0	$\delta_{i,j}$	0	0
(a^k,α_i)	0	0	$\delta_{i,j}\delta_{k,\ell}$	0
(b,β_i)	$\frac{1}{2}\cdot(-1)^{i+j}$	0	0	$\frac{1}{2}\cdot(-1)^j$

Since S and T have orders 2 and $2n$, respectively, the inverse of A is T^nST^nS, which is described below.

$A^{-1} = T^nST^nS$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2}$	0	0	$\frac{1}{2}\cdot(-1)^{i+j}$
(e,ψ_i)	0	$\delta_{i,j}$	0	0
(a^k,α_i)	0	0	$\delta_{i,j}\delta_{k,\ell}$	0
(b,β_i)	$\frac{1}{2}\cdot(-1)^j$	0	0	$\frac{1}{2}\cdot(-1)^i$

A routine calculation shows that $A^2 = A^{-1}$, and so A has order 3. The matrix B has order 2, since T has order $2n$. We have $BA = T^nST^nST^n = A^{-1}B$, and it follows that the group $\langle A,B\rangle$ is isomorphic to S_3. □

Lemma 4.2. *Let n be an odd integer with $n \geq 3$, let S and T denote the matrices associated to the modular tensor category* Rep$(D(\mathrm{Dih}_n))$*, and let $P = TST^{n+1}ST$ and $Q = T^{n+1}$. The matrices P and Q have orders 2 and n, respectively, and they satisfy the relations*

$$(PQ)^3 = I \qquad \textit{and} \qquad \left(PQ^{\frac{n+1}{2}}PQ^2\right)^3 = I.$$

Proof. The matrices P and Q are described below.

$P = TST^{n+1}ST$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2n}+\frac{1}{2}\cdot(-1)^{i+j}$	$\frac{1}{n}$	$\frac{1}{n}$	0
(e,ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi\ell i}{n}\right)$	0
(a^k,α_i)	$\frac{1}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi kj}{n}\right)$	$\frac{2}{n}\cdot\cos\left(\frac{2\pi(kj+\ell i)}{n}\right)$	0
(b,β_i)	0	0	0	$\delta_{i,j}$

$Q = T^{n+1}$	(e,χ_i)	(e,ψ_i)	(a^k,α_i)	(b,β_i)
	1	1	ζ^{ki}	1

We have $P^{-1} = T^{-1}ST^{n-1}ST^{-1}$, whose description is easily obtained from the descriptions of $ST^{n-1}S$ and T given earlier. We find that $P^{-1} = P$, and so P has order 2. The order of Q is $2n/\gcd(2n, n+1) = 2n/\gcd(2, n+1) = n$.

A calculation shows that $PQP = ST^{n+1}S$. Using the descriptions of $ST^{n+1}S$ and T given earlier, we immediately see that the matrices $ST^{n+1}S$ and T^n commute. Then

$$Q^{-1}PQ^{-1} = T^{n-1}(TST^{n+1}ST)T^{n-1} = T^n(ST^{n+1}S)T^n = ST^{n+1}S = PQP,$$

and it follows that $(PQ)^3 = I$.

The matrix $PQ^{\frac{n+1}{2}}PQ$ and its square are described below.

$PQ^{\frac{n+1}{2}}PQ^2$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2n} + \frac{1}{2}\cdot(-1)^{i+j}$	$\frac{1}{n}$	$\frac{1}{n}$	0
(e,ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{4\pi\ell i}{n}\right)$	0
(a^k,α_i)	$\frac{1}{n}\cdot\zeta^{-2ki}$	$\frac{2}{n}\cdot\cos\left(\frac{4\pi kj}{n}\right)\cdot\zeta^{-2ki}$	$\frac{2}{n}\cdot\cos\left(\frac{4\pi(kj+\ell i)}{n}\right)\cdot\zeta^{-2ki}$	0
(b,β_i)	0	0	0	$\delta_{i,j}$

$(PQ^{\frac{n+1}{2}}PQ^2)^2$	(e,χ_j)	(e,ψ_j)	(a^ℓ,α_j)	(b,β_j)
(e,χ_i)	$\frac{1}{2n} + \frac{1}{2}\cdot(-1)^{i+j}$	$\frac{1}{n}$	$\frac{1}{n}\cdot\zeta^{2\ell j}$	0
(e,ψ_i)	$\frac{1}{n}$	$\frac{2}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{4\pi\ell i}{n}\right)\cdot\zeta^{2\ell j}$	0
(a^k,α_i)	$\frac{1}{n}$	$\frac{2}{n}\cdot\cos\left(\frac{4\pi kj}{n}\right)$	$\frac{2}{n}\cdot\cos\left(\frac{4\pi(kj+\ell i)}{n}\right)\cdot\zeta^{2\ell j}$	0
(b,β_i)	0	0	0	$\delta_{i,j}$

A routine calculation shows that the product of the two matrices above is the identity. $\square$

Lemma 4.3. *Let n be an odd integer with $n \geq 3$, let S and T denote the matrices associated to the modular tensor category* $\mathrm{Rep}(D(\mathrm{Dih}_n))$*, and let $P = TST^{n+1}ST$ and $Q = T^{n+1}$. The group $\langle P, Q\rangle$ generated by P and Q is isomorphic to the group* $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$.

Proof. As stated earlier,

$$\left\langle X, Y \,\middle|\, X^2 = 1, (XY)^3 = 1, Y^n = 1, \left(XY^{\frac{n+1}{2}}XY^2\right)^3 = 1 \right\rangle$$

is a presentation of $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ [2], and the cosets

$$X = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad Y = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

satisfy the relations above.

By Lemma 4.2, the matrices P and Q satisfy the defining relations of the gorup $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ with P substituted for X, and Q substituted for Y. Therefore, there is a surjective group homomorphism $\varphi : \mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z}) \to \langle P, Q\rangle$ such that $\varphi(X) = P$ and $\varphi(Y) = Q$.

Let $\pi : \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ denote the natural projection. Consider the kernel of φ. By Corollary 3.3, either $\operatorname{Ker}\varphi$ is a subgroup of the center of $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$, or $\operatorname{Ker}\varphi = \pi(H)$ for some subgroup H of $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ of level less than n, or if $3 \mid n$ and $3^2 \nmid n$, then $\operatorname{Ker}\varphi$ is possibly equal to $\pi(K)C$, where C is a subgroup of the center of $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ and K is the image in $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ of the unique Sylow 2-subgroup of $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$.

A central element of $\mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z})$ is necessarily of the form $\pm \left(\begin{smallmatrix} u & 0 \\ 0 & u \end{smallmatrix}\right)$ with $u^2 \equiv 1 \pmod n$, and it is easily verified that it corresponds to $(XY^u)^3$. Suppose that for some integer u with $u^2 \equiv 1 \pmod n$, the element $(XY^u)^3$ is in the kernel of φ. Then $(PQ^u)^3 = I$, equivalently, $PQ^{-u}P = Q^uPQ^u$. A routine calculation shows that

$$\left(PQ^{-u}P\right)_{(e,\psi_1),(a,\alpha_1)} = \frac{2}{n} \cdot \cos\left(\frac{2\pi u}{n}\right) \cdot \zeta^u$$

and

$$\left(Q^uPQ^u\right)_{(e,\psi_1),(a,\alpha_1)} = \frac{2}{n} \cdot \cos\left(\frac{2\pi}{n}\right) \cdot \zeta^u,$$

where $\zeta = e^{2\pi i/n}$. Therefore, we must have $\cos\left(\frac{2\pi u}{n}\right) = \cos\left(\frac{2\pi}{n}\right)$. Then $\sin\left(\frac{2\pi u}{n}\right) = \pm\sin\left(\frac{2\pi}{n}\right)$, and therefore $\cos\left(\frac{2\pi u}{n}\right) + i\sin\left(\frac{2\pi u}{n}\right) = \cos\left(\frac{2\pi}{n}\right) \pm i\sin\left(\frac{2\pi}{n}\right)$, equivalently, $\zeta^u = \zeta^{\pm 1}$. It follows that $u \equiv \pm 1 \pmod n$. We conclude that $\operatorname{Ker}\varphi$ can not be a nontrivial central subgroup.

Let H be a subgroup of $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ of level less than n. By Lemma 3.1, the subgroup H contains $\operatorname{Ker}\phi^n_{n/p}$ for some prime p that divides n, where $\phi^n_{n/p} : \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/(n/p)\mathbb{Z})$ is the reduction homomorphism. Observe that $\operatorname{Ker}\phi^n_{n/p}$ contains the matrix $\left(\begin{smallmatrix} 1 & n/p \\ 0 & 1 \end{smallmatrix}\right)$, and therefore the coset $\pm\left(\begin{smallmatrix} 1 & n/p \\ 0 & 1 \end{smallmatrix}\right)$, which corresponds to $Y^{n/p}$, lies in $\pi(H)$. The image of $Y^{n/p}$ under φ is the matrix $Q^{n/p}$.

By Lemma 4.2, Q has order n, and so $Q^{n/p} \neq I$. It follows that $\operatorname{Ker}\varphi$ can not be of the form $\pi(H)$ for some subgroup H of $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ of level less than n.

The group $\mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z})$ contains a unique Sylow 2-subgroup, generated by the matrices $\begin{pmatrix} [0]_3 & [-1]_3 \\ [1]_3 & [0]_3 \end{pmatrix}$ and $\begin{pmatrix} [-1]_3 & [-1]_3 \\ [-1]_3 & [1]_3 \end{pmatrix}$. Suppose that $3 \mid n$ and $3^2 \nmid n$. Then there is an injection $\mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z}) \hookrightarrow \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$. Choose an integer u such that $\frac{n}{3} \cdot u \equiv 1 \pmod 3$. The image of the matrix $\begin{pmatrix} [0]_3 & [-1]_3 \\ [1]_3 & [0]_3 \end{pmatrix}$ in $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ is $\pm\begin{pmatrix} \left[1-\frac{n}{3}\cdot u\right]_n & \left[-\frac{n}{3}\cdot u\right]_n \\ \left[\frac{n}{3}\cdot u\right]_n & \left[1-\frac{n}{3}\cdot u\right]_n \end{pmatrix}$, and it is easily verified that it corresponds to

$$XY^{-1}XY^{-\frac{n}{3}u}XY^{1+\frac{n}{3}u}X;$$

suppose that this element lies in $\operatorname{Ker}\varphi$. Then $PQ^{-1}PQ^{-\frac{n}{3}u}PQ^{1+\frac{n}{3}u}P = I$, equivalently, $Q^{-\frac{n}{3}u}PQ^{1+\frac{n}{3}u} = PQ$. A routine calculation shows that

$$\left(Q^{-\frac{n}{3}u}PQ^{1+\frac{n}{3}u}\right)_{(e,\chi_0),(a,\alpha_1)} = \frac{1}{n}\cdot\zeta^{1+\frac{n}{3}u}$$

and

$$(PQ)_{(e,\chi_0),(a,\alpha_1)} = \frac{1}{n}\cdot\zeta,$$

where $\zeta = e^{2\pi i/n}$. Therefore, we must have $\zeta^{1+\frac{n}{3}u} = \zeta$, equivalently, $\frac{n}{3}\cdot u \equiv 0 \pmod n$, a contradiction. It follows that $\operatorname{Ker}\varphi$ can not be of the form $\pi(K)C$ where C is a subgroup of the center of $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})$ and K is the image in $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})$ of the unique Sylow 2-subgroup of $\mathrm{SL}(2,\mathbb{Z}/3\mathbb{Z})$.

Having exhausted all cases, we conclude that $\operatorname{Ker}\varphi$ must be trivial, and hence φ is an isomorphism. □

Theorem 4.4. *Let n be an odd integer with $n \geq 3$. The image of the representation of the modular group $\mathrm{SL}(2,\mathbb{Z})$ arising from the modular tensor category $\mathrm{Rep}(D(\mathrm{Dih}_n))$ is isomorphic to the group $\mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z}) \times S_3$.*

Proof. Let S and T be the matrices associated to the modular tensor category $\mathrm{Rep}(D(\mathrm{Dih}_n))$, and as before let $P = TST^{n+1}ST$, $Q = T^{n+1}$, $A = ST^nST^n$, and $B = T^n$. Then $T = QB$ and

$$T(AT^n)(T^{-1}P) = T(ST^nS)(ST^{n+1}S) = TST^{2n+1}ST = TSTST = S, \tag{4}$$

where we used (3); it follows that

$$\langle S,T\rangle = \langle P,Q\rangle\langle A,B\rangle.$$

Using the descriptions of the matrices involved, we immediately see that P and B commute, and Q and A commute. We have

$$SPS = S(TST^{n+1}ST)S = (ST)^2T^{n-1}(TS)^2 = T^{-1}ST^{n-1}ST^{-1} = P^{-1} = P,$$

showing that the matrices P and S commute, where we used Lemma 4.2 and (3). It follows that the subgroups $\langle P, Q\rangle$ and $\langle A, B\rangle$ of $\langle S, T\rangle$ commute element-wise. Therefore, the intersection of these subgroups must be contained in the center of $\langle A, B\rangle$. By Lemma 4.1, the group $\langle A, B\rangle$ is isomorphic to S_3, which has trivial center, and so the intersection in question must be trivial. Therefore,

$$\langle P, Q\rangle\langle A, B\rangle \cong \langle P, Q\rangle \times \langle A, B\rangle \cong \mathrm{PSL}(2, \mathbb{Z}/n\mathbb{Z}) \times S_3,$$

where we used Lemma 4.1 and Lemma 4.3. □

Theorem 4.5. *Let n be an odd integer with $n \geq 3$. The images of the representations of the modular group* $\mathrm{SL}(2, \mathbb{Z})$ *arising from the modular tensor categories* $\mathrm{Rep}(D(\mathrm{Dih}_{2n}))$ *and* $\mathrm{Rep}(D(\mathrm{Dih}_n))$ *are isomorphic.*

Proof. Let S and T denote the matrices associated to $\mathrm{Rep}(D(\mathrm{Dih}_n))$, and let S' and T' denote the matrices associated to $\mathrm{Rep}(D(\mathbb{Z}/2\mathbb{Z}))$. Then the image of the representation of $\mathrm{SL}(2, \mathbb{Z})$ arising from $\mathrm{Rep}(D(\mathrm{Dih}_{2n}))$ is isomorphic to the group $\langle S \otimes S', T \otimes T'\rangle$, since Dih_{2n} is isomorphic to $\mathrm{Dih}_n \times \mathbb{Z}/2\mathbb{Z}$. We have

$$S' = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad \text{and} \qquad T' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Let $A' = T'S'$ and $B' = T'$. The matrices A' and B' have orders 3 and 2, respectively, and they satisfy the relation $B'A' = (A')^{-1}B$. As before, let $P = TST^{n+1}ST$, $Q = T^{n+1}$, $A = ST^nST^n$, and $B = T^n$. It is easily verified that $T'S'(T')^{n+1}S'T' = I, (T')^{n+1} = I, S'(T')^nS'(T')^n = A', (T')^n = B'$, and from this it follows that the matrices $P \otimes I, Q \otimes I, A \otimes A'$, and $B \otimes B'$ lie in $\langle S \otimes S', T \otimes T'\rangle$.

We have $T \otimes T' = (B \otimes B')(Q \otimes I)$, and

$$(T \otimes T')(A \otimes A')(T \otimes T')^{n-1}(P \otimes I) = TAT^{n-1}P \otimes T'A'(T')^{n-1} = S \otimes S',$$

where we used (4); it follows that

$$\langle S \otimes S', T \otimes T'\rangle = \langle P \otimes I, Q \otimes I, A \otimes A', B \otimes B'\rangle = \langle P \otimes I, Q \otimes I\rangle\langle A \otimes A', B \otimes B'\rangle.$$

As seen in the proof of Theorem 4.4, the subgroups $\langle P, Q\rangle$ and $\langle A, B\rangle$ commute element-wise, and so the subgroups $\langle P \otimes I, Q \otimes I\rangle$ and $\langle A \otimes A', B \otimes B'\rangle$ commute element-wise too. The group $\langle A \otimes A', B \otimes B'\rangle$ is isomorphic to S_3, which has trivial center, and so the subgroups $\langle P \otimes I, Q \otimes I\rangle$ and $\langle A \otimes A', B \otimes B'\rangle$ intersect trivially.

Then

$$\begin{aligned}\langle P\otimes I, Q\otimes I\rangle\langle A\otimes A', B\otimes B'\rangle &\cong \langle P\otimes I, Q\otimes I\rangle \times \langle A\otimes A', B\otimes B'\rangle\\ &\cong \mathrm{PSL}(2,\mathbb{Z}/n\mathbb{Z})\times S_3,\end{aligned}$$

where we used Lemma 4.3. □

References

[1] B. Bakalov and A. Kirillov, Jr., Lectures on Tensor Categories and Modular Functors, University Lecture Series, 21, Amer. Math. Soc., 2001.

[2] H. Behr and J. Mennicke, *A presentation of the groups* $\mathrm{PSL}(2,p)$, Canadian J. Math., 20 (1968), 1432-1438.

[3] J. L. Cardy, *Operator content of two-dimensional conformally invariant theories*, Nuclear Phys. B, 270(2) (1986), 186-204.

[4] A. Coste and T. Gannon, *Congruence subgroups and rational conformal field theory*, preprint, arXiv:math/9909080 [math.QA], (1999).

[5] A. Coste, T. Gannon and P. Ruelle, *Finite group modular data*, Nucl. Phys. B, 581(3) (2000), 679-717.

[6] R. C. Gunning, Lectures on Modular Forms, Notes by Armand Brumer, Annals of Mathematics Studies, 48, Princeton University Press, Princeton, N.J., 1962.

[7] D. L. McQuillan, *Classification of normal congruence subgroups of the modular group*, Amer. J. Math., 87(2) (1965), 285-296.

[8] S.-H. Ng and P. Schauenburg, *Congruence subgroups and generalized Frobenius-Schur indicators*, Comm. Math. Phys., 300(1) (2010), 1-46.

[9] Y. Sommerhäuser and Y. Zhu, Hopf Algebras and Congruence Subgroups, Mem. Amer. Math. Soc., 219(1028), 2012.

Deepak Naidu
Department of Mathematical Sciences
Northern Illinois University
DeKalb, Illinois 60115, USA
email: dnaidu@math.niu.edu