J. Math. Soc. Japan
Vol. 55, No. 3, 2003

Nonexistence of modular fusion algebras whose kernels are certain noncongruence subgroups

By Makoto Tagami

(Received Jan. 15, 2002)

Abstract. A well-known conjecture states that the kernel of representation associated to a modular fusion algebra is always a congruence subgroup. Assuming this conjecture, Eholzer studied modular fusion algebras such that the kernel of representation associated to each of them is a congruence subgroup using the fact that all irreducible representaions of $SL(2, \boldsymbol{Z}/p^{\lambda}\boldsymbol{Z})$ are classified. He classified all strongly modular fusion algebras of dimension two, three, four and the nondegenerate ones with dimension ≤ 24. In this paper, we try to imitate Eholzer's work. We classify modular fusion algebras such that the kernel of representation associated to each of them is a noncongruence normal subgroup of $\Gamma := PSL(2, \boldsymbol{Z})$ containing an element $\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$. Among such normal subgroups, there exist infinitely many noncongruence subgroups. In a sense, they are the classes of near congruence subgroups. For such a normal subgroup G, we shall show that any irreducible representation of degree not equal to 1 of Γ/G is not associated to a modular fusion algebra.

1. Introduction.

In mathematical physics, it is known that for each conformal field theory (CFT) there is an associated fusion algebra which is an associative and commutative algebra over $\boldsymbol{C}$ of finite dimension and has a representation of $SL(2, \boldsymbol{Z})$ (ref. [**9**]). In order to investigate CFT, the classification problem of fusion algebras is a very important research. There are some partial results for this. For example, Eholzer classified all strongly modular fusion algebras of dimension two, three and four. He was able to classify all nondegenerate strongly modular fusion algebras of dimension less than 24. The term 'strongly' means the kernel of representation associated to fusion algebra is a congruence subgroup. The term 'nondegenerate' is defined in the next section. A representation $\rho : SL(2, \boldsymbol{Z}) \to GL(n, \boldsymbol{C})$ is called admissible if there exists a fusion algebra A such that (A, ρ) is a modular fusion algebra. These notions were introduced by Eholzer. Refer to [**8**] for strongly modular fusion algebras. In this classification, he used Nob's classification of irreducible representations of the finite group $SL(2, \boldsymbol{Z}_{p^{\lambda}})$ where p is a prime and λ is a positive integer (ref. [**16**], [**17**]). One reason of his classification is based on the following conjecture.

The Conjecture (ref. [**8**]). *The kernel of representation associated to a modular fusion algebra is always a congruence subgroup.*

2000 *Mathematics Subject Classification.* Primary 05E99; Secondary 11F06.
Key Words and Phrases. Fusion algebra, modular fusion algebra, non congruence subgroup, admissible, nondegenerate, little group method.

One purpose of this paper is to start attacking such conjecture. In this paper, we will imitate Eholzer's work in the following situation. This problem was suggested by professor Eiichi Bannai.

The Problem. Let $\Gamma := PSL(2, \boldsymbol{Z})$ and G be a normal subgroup with the finite index of Γ containing $\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$. Then,

(1) Decide all irreducible representations of Γ/G.

(2) Is the irreducible representation of Γ/G admissible?

We want to find a counter example for this conjecture, that is, an irreducible representation (of Γ) associated to a modular fusion algebra whose kernel is a non-congruence subgroup. It is our one wish to find a counter example in view of this problem since there exist infinitely many noncongruence subgroups among the normal subgroups of the problem and they are the classes like congruence subgroups in a sense. But the answer to this problem is negative. Namely, we prove the following theorem.

Theorem 1.1. *Let G be a normal subgroup with finite index of Γ containing $\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$. Then, all irreducible representations of degree not equal to* 1 *of Γ/G are not admissible.*

Remark. Though the representation associated to a modular fusion algebra is a representation of $SL(2, \boldsymbol{Z})$, we consider $PSL(2, \boldsymbol{Z})$ in this paper to make the proof easy. But the result does not change much even if we consider $SL(2, \boldsymbol{Z})$, since only the same representations appear. For the reducible representations, representations of degree ≤ 4 are classified in [**8**] since any of the kernels of the representations of degree 2 is a congruence subgroup. The reducible representations of degree ≥ 5 are too complicated to compute.

2. Fusion algebra and modular fusion algebra.

This section depends basically on [**8**]. We will adopt the following definition of fusion algebra in this paper (ref. [**8**], [**1**], [**9**]).

Definition 2.1 (Fusion algebra). Let A be an associative and commutative algebra over $\boldsymbol{C}$ (complex number field), and have a distinguished basis $\{x_0, x_1, \dots, x_n\}$ with multiplication defined by

$$x_i \cdot x_j := \sum_{k=0}^{n} N_{ij}^k x_k.$$

N_{ij}^k are called structure constants of A. Then, A is called fusion algebra if the following conditions are satisfied.

(i) $N_{i0}^j = \delta_{ij}$ (where δ is Kronecker's δ),

(ii) $N_{ij}^k \in \boldsymbol{Z}_{\geq 0}$,

(iii) There exists an involution $\hat{}$ of $\{0, 1, \dots, n\}$ such that $N_{ij}^0 = \delta_{i\hat{j}}$ and $N_{\hat{i}\hat{j}}^{\hat{k}} = N_{ij}^k$.

Example. Let G be any finite group and let $\{\chi_0 = 1_G$ (the principal character),

$\chi_1, \dots, \chi_n\}$ be the irreducible characters of G. Put $A := \{f : G \to \boldsymbol{C} \mid f(h^{-1}gh) = f(g)$ $\forall g, h \in G\}$. A is an associative and commutative algebra over $\boldsymbol{C}$ whose addition, multiplication and inner product are respectively defined as follows: for $\phi, \psi \in A$, $g \in G$,

$$(\phi + \psi)(g) := \phi(g) + \psi(g), \quad (\phi \cdot \psi)(g) := \phi(g) \cdot \psi(g), \quad (\phi, \psi)_G := \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)},$$

where $\bar{c}$ denotes the complex conjugate of c for any element c of $\boldsymbol{C}$. It is known that $\{\chi_0, \chi_1, \dots, \chi_n\}$ is an orthonormal basis of A. An involution $\hat{}$ is defined by $\hat{\phi}(g) := \overline{\phi(g)}$. Then A is a fusion algebra with a distinguished basis $\{\chi_0, \chi_1, \dots, \chi_n\}$.

Next, we shall define modular fusion algebra (ref. [**8**]). Let $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then we know that $SL(2, \boldsymbol{Z}) = \langle S, T \mid S^4 = I,\ S^2 = (ST)^3 \rangle$.

Definition 2.2 (Modular fusion algebra). Let A be a fusion algebra with structure constants N_{ij}^k and ρ be a unitary representation of $SL(2, \boldsymbol{Z})$. (A, ρ) is called modular fusion algebra if the following conditions are satisfied:

(i) $\rho(S)$ is symmetric and $\rho(T)$ is diagonal,

(ii) $N_{ij}^0 = \rho(S^2)_{ij}$,

(iii) (Verlinde's formula)

$$N_{ij}^k = \sum_{m=0}^{n} \frac{\rho(S)_{im}\rho(S)_{jm}\overline{\rho(S)_{km}}}{\rho(S)_{0m}}.$$

From this point onwards, we denote modular fusion algebra as MFA. MFA of dimension 1 is called a trivial MFA. Next, we introduce a very important example of MFA. This example is called finite group modular data (ref. [**9**], [**11**]).

Example. Let G be any finite group. We take the Grothendieck ring F of G-equivalent complex vector bundles over G (where we take conjugation as the action of G) as a fusion algebra and the modular data ρ of G as a representation of $SL(2, \boldsymbol{Z})$. Then (F, ρ) is a modular fusion algebra. It is known that the kernel of finite group modular data is a congruence subgroup (For this fact, refer to [**10**]).

The following nondegeneracy of MFA was introduced by Eholzer (ref. [**8**]).

Definition 2.3 (Nondegenerate). Let (A, ρ) be a MFA. When the characteristic polynomial of $\rho(T)$ does not have multiple root, (A, ρ) is called nondegenerate MFA and so is $\rho(T)$.

Let us introduce two lemmas to investigate nondegenerate MFA. These two lemmas are due to [**8**].

Lemma 2.1 (Eholzer). *Let (A, ρ) be a nondegenerate MFA. Then ρ is irreducible.*

Lemma 2.2 (Eholzer). *Let ρ and ρ' be equivalent, irreducible, and unitary representations of $SL(2, \boldsymbol{Z})$ such that $\rho(T) = \rho'(T)$ is diagonal and nondegenerate. Then, there exists a unitary diagonal matrix D such that $\rho = D^{-1}\rho' D$.*

REMARK. (i) Note that from Lemma 2.1, it is enough to find nondegenarate MFA in finding MFA from the irreducible representations of Γ.

(ii) Take an irreducible unitary representation ρ of Γ such that $\rho(T)$ is diagonal and nondegenerate. Let ρ' be any equivalent unitary representation of ρ such that $\rho(T) = \rho'(T)$. Then, by Lemma 2.2, there exists a unitary diagonal matrix $D = \begin{pmatrix} d_0 & & & & \\ & d_1 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & d_n \end{pmatrix}$ such that $\rho' = D^{-1}\rho D$. Thus $\rho'(S)_{ij} = \dfrac{d_j}{d_i}\rho(S)_{ij}$.

Apply Verlinde's formula for each representation ρ and ρ'.

$$\sum_{m=0}^{n} \frac{\rho(S)'_{im}\rho(S)'_{jm}\overline{\rho(S)'_{km}}}{\rho(S)'_{0m}} = \frac{d_k}{d_i d_j}\sum_{m=0}^{n} \frac{\rho(S)_{im}\rho(S)_{jm}\overline{\rho(S)_{km}}}{\rho(S)_{0m}}.$$

Since $|d_i| = 1$, if ρ' is associated to a MFA, for any i, j, k,

$$\left|\sum_{m=0}^{n} \frac{\rho(S)_{im}\rho(S)_{jm}\overline{\rho(S)_{km}}}{\rho(S)_{0m}}\right| \in \boldsymbol{Z} \text{ hold.}$$

There are many equivalent representations of ρ. But as soon as we find i, j, k such that $|\sum_{m=0}^{n} \rho(S)_{im}\rho(S)_{jm}\overline{\rho(S)_{km}}/(\rho(S)_{0m})| \notin \boldsymbol{Z}$, we do not need to investigate many other equivalent representations of ρ. From the above, we see that nondegeneracy simplifies the classification of MFA.

EXAMPLE. Let $\rho(S) := \dfrac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix}$, $\rho(T) := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then ρ is a unitary and irreducible representation of Γ.

$$\left|\sum_{m=0}^{1} \frac{\rho(S)_{1m}\rho(S)_{1m}\overline{\rho(S)_{1m}}}{\rho(S)_{0m}}\right| = \frac{2\sqrt{3}}{3} \notin \boldsymbol{Z}.$$

So, we can see that any equivalent unitary representation ρ' of ρ such that $\rho'(T) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is not admissible.

Next, we shall consider the normal subgroups of Γ containing $\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$.

3. Certain normal subgroups of Γ.

This section is based on [**13**]. Let $\Gamma := PSL(2, \boldsymbol{Z})$,

$$x := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad y := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad z := xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$a := [x, y] = xyxy^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad b := [x, y^2] = xy^2xy = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{in } \Gamma.$$

Let Γ' and Γ'' denote the first commutator subgroup and the second commutator subgroup, respectively. Then,

$$\Gamma = \langle x, y \mid x^2 = y^3 = 1 \rangle \quad \text{(the free group generated by two elements of order 2 and 3)},$$

$$\Gamma' = \langle a, b \rangle \quad \text{(the free group generated by } a \text{ and } b\text{)},$$

$$\Gamma = \sum_{r=0}^{5} z^r \Gamma',$$

and

$$\Gamma' = \sum_{i,j \in \mathbf{Z}} a^i b^j \Gamma'' \quad (\Gamma'/\Gamma'' \text{ is the free abelian group of rank 2}).$$

We also note that $[a, b^{-1}] = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} = z^6$.

Let $\triangle(m)$ denote the minimal normal subgroup containing z^m. Then, it is shown that $\triangle(m) = \Gamma(m)$ for $1 \le m \le 5$ by Brenner [**3**], and $\triangle(6) = \Gamma''$ for $m = 6$ by Newman [**14**] where $\Gamma(n) := \{A \in \Gamma \mid A \equiv I \pmod{n}\}$. So, the problem comes to consider normal subgroups which contain Γ''. Take any normal subgroup G containing z^6. Since $\triangle(2) = \Gamma(2)$ and $\triangle(3) = \Gamma(3)$,

$$z^2 \in G \Rightarrow G \supset \Gamma(2),$$

$$z^3 \in G \Rightarrow G \supset \Gamma(3).$$

In [**8**], it is shown that any irreducible representation (of degree not equal to 1) of $\Gamma/\Gamma(2) \simeq S_3$ (the symmetric group of degree 3) and $\Gamma/\Gamma(3) \simeq A_4$ (the alternating group of degree 4) is not admissible. Next, we shall assume that the order of z in Γ/G is equal to 6. In this case, we have the following lemma by Newman (ref. [**13**]).

Lemma 3.1 (Newman). *Let $\Gamma \triangleright G$. Assume that the order of z in Γ/G is equal to 6. Then, $\Gamma' \supset G \supset \Gamma''$.*

From now on, we consider only the normal subgroup G such that $\Gamma' \supset G \supset \Gamma''$. Such subgroups were classified by Newman.

Theorem 3.1 (ref. [**13**]). *There is a 1-1 corespondence between normal subgroups G such that $\Gamma' \supset G \supset \Gamma''$, $G \neq \Gamma''$ and the ordered triplets of integers (p, m, d) where*

$$p > 0, \quad 0 \le m \le d - 1, \quad m^2 + m + 1 \equiv 0 \pmod{d}.$$

(p, m, d) corresponds to the normal subgroup G such that

$$G = \sum_{i,j \in \mathbf{Z}} A^i B^j \Gamma'', \quad \text{where } A := a^p b^{mp}, B := b^{dp}.$$

Newman showed in [**15**] that the group (p, m, d) in Theorem 3.1 is a congruence subgroup if and only if $(p, m, d) = (1, 0, 1), (1, 1, 3), (2, 0, 1), (2, 1, 3)$. So, we obtain infinitely many noncongruence subgroups.

Let $G = \sum_{i,j \in \boldsymbol{Z}} A^i B^j \Gamma''$, where $A := a^p b^{mp}$, $B := b^{dp}$. Then,

$$\Gamma' = \sum_{\substack{i=0,\dots,p-1 \\ j=0,\dots,dp-1}} a^i b^j G$$

and so

$$\Gamma = \sum_{i=0,\dots,5} \sum_{\substack{j=0,\dots,p-1 \\ k=0,\dots,dp-1}} z^i a^j b^k G.$$

From this,

$$\Gamma/G \simeq \boldsymbol{Z}/6\boldsymbol{Z} \ltimes (\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}).$$

The action of $\boldsymbol{Z}/6\boldsymbol{Z}$ $(=\langle z \rangle)$ on $\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}$ is given as follows. For any $(i,j) \in \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}$,

$$\begin{aligned}
S^0(i,j) &:= (i,j), \\
S(i,j) &:= z^{-1}(i,j)z = (-mi - j, (m^2+m+1)i + (m+1)j), \\
S^2(i,j) &:= z^{-2}(i,j)z^2 = (-(m+1)i - j, (m^2+m+1)i + mj), \\
S^3(i,j) &:= z^{-3}(i,j)z^3 = (-i,-j), \\
S^4(i,j) &:= z^{-4}(i,j)z^4 = -S(i,j), \\
S^5(i,j) &:= z^{-5}(i,j)z^5 = -S^2(i,j).
\end{aligned}$$

4. Review of the little group method.

In this section, we review the little group method (ref. [**6**]). It enables us to compute the irreducible representations of a group with the form $H \ltimes A$ where A is an abelian group. In this paper we denote $\mathrm{Irr}(G)$ as the set of all irreducible representations of G. Consider $G := H \ltimes A$ where A is abelian. H acts on $\mathrm{Irr}(A)$ as follows. For $h \in H$, $\rho \in \mathrm{Irr}(A)$, $a \in A$,

$$(h\rho)(a) := \rho(a^h),$$

where a^h denotes the action of H on A. Then,

$$\mathrm{Irr}(A) = \bigcup_{i=1}^{n} \hat{A}_i \quad \text{(the orbit decomposition by the action of } H\text{)}.$$

Fix $\rho_i \in \hat{A}_i$.

$$H_i := \{h \in H \mid h\rho_i = \rho_i\}, \quad G_i := H_i \cdot A.$$

For any $\chi \in \mathrm{Irr}(H_i)$, we extend χ to an element of $\mathrm{Irr}(G_i)$ as follows.

For $(h \in H_i,\ a \in A,\ \chi(ha) := \chi(h))$.

Put

$$\rho_i(ha) := \rho_i(a).$$

Then, we can regard ρ_i as $\rho_i \in \mathrm{Irr}(G_i)$.

$$\theta_{\chi i} := (\chi \otimes \rho_i)^G$$

where $(\chi \otimes \rho_i)^G$ denotes the induced representation of $\chi \otimes \rho_i$. Then $\theta_{\chi i} \in \mathrm{Irr}(G)$ and

$$\mathrm{Irr}(G) = \{\theta_{\chi i} \mid 1 \le i \le n, \chi \in H_i\}.$$

5. The irreducible representations of the quotient group of degree 2 and 3.

We now compute the irreducible representations of $\boldsymbol{Z}/6\boldsymbol{Z} \ltimes (\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z})$ using the little group method. Let

$$G := \boldsymbol{Z}/6\boldsymbol{Z} \ltimes (\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}), \quad H := \boldsymbol{Z}/6\boldsymbol{Z}, \quad A := \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}.$$

For $(i,j),(k,l) \in \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}$, $\phi_{ij}(k,l) := \xi_{dp}^{ikd+jl}$ where ξ_n is a primitive n-th root of 1. Then,

$$\mathrm{Irr}(A) = \{\phi_{ij} \mid (i,j) \in \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z}\}.$$

Fix $\phi_{ij} \in \mathrm{Irr}(A)$. H acts on $\mathrm{Irr}(A)$ as follows:
For $(l,m) \in A$,

$$(z^k\phi_{ij})(l,m) := \phi_{ij}(S^k(l,m)).$$

Let $H_{ij} := \{h \in H \mid (h\phi_{ij}) = \phi_{ij}\}$, $G_{ij} := H_{ij} \cdot A$. Then we obtain the following lemma using some elementary computations.

Lemma 5.1. $z \in H_{ij} \Leftrightarrow i = j = 0$,
$z^2 \in H_{ij} \Leftrightarrow 3j \equiv 0,\ id \equiv (m-1)j \pmod{dp}$,
$z^3 \in H_{ij} \Leftrightarrow 2i \equiv 0 \pmod{p},\ 2j \equiv 0 \pmod{dp}$.

Take $\psi \in \mathrm{Irr}(H_{ij})$. $\theta_{\psi ij} := (\psi \otimes \phi_{ij})^G$ is an irreducible representation by the little group method. Since H_{ij} is an abelian, $\deg \psi = 1$. So,

$$\deg \theta_{\psi ij} = |G : G_{ij}| = |H : H_{ij}|.$$

From this, we see that the degrees of the irreducible representations are 1, 2, 3, or 6. We investigate if each of the irreducible representations of degrees 2 and 3 is admissible. Note that $x = z^3 S^4(0,1)$ in G.

(i) **Degree 2.**

The irreducible representations of degree 2 appear in the case of $|H : H_{ij}| = 2$, i.e. $H_{ij} = \langle z^2 \rangle$. Then,

$$G_{ij} = \langle z^2 \rangle \cdot A, \quad G = G_{ij} + zG_{ij}.$$

For $0 \le k, l \le 2$, let $\psi_k(z^{2l}) := \omega^{kl}$ where $\omega := \xi_3$, and $\theta_{kij} := (\psi_k \otimes \phi_{ij})^G$. Then,

$$\theta_{kij}(z) = \begin{pmatrix} 0 & \omega^k \\ 1 & 0 \end{pmatrix}, \quad \theta_{kij}(x) = \begin{pmatrix} 0 & \omega^{2k}\xi_{dp}^{id-mj} \\ \omega^k \xi_{dp}^{id-(m+1)j} & 0 \end{pmatrix}.$$

By Lemma 5.1, $z^2 \in H_{ij} \Leftrightarrow 3j \equiv 0,\ id \equiv (m-1)j \pmod{dp}$. So,

$$\theta_{kij}(x) = \begin{pmatrix} 0 & \omega^{2k}\xi_{dp}^{-j} \\ \omega^k \xi_{dp}^{-2j} & 0 \end{pmatrix}.$$

Put $\alpha := \xi_6$, and $\beta := \xi_{dp}$. Take a conjugate of θ_{kij} with $P := (1/\sqrt{2})\begin{pmatrix} \alpha^k & -\alpha^k \\ 1 & 1 \end{pmatrix}$,

$$P^{-1}\theta_{kij}(z)P = \begin{pmatrix} \alpha^k & 0 \\ 0 & -\alpha^k \end{pmatrix}, \quad P^{-1}\theta_{kij}(x)P = \frac{\alpha^{3k}}{2}\begin{pmatrix} \beta^{-j}+\beta^{-2j} & \beta^{-j}-\beta^{-2j} \\ \beta^{-2j}-\beta^{-j} & -(\beta^{-j}+\beta^{-2j}) \end{pmatrix}.$$

Since $3j \equiv 0 \pmod{dp}$, we have $\beta^{-j} = \omega^l$ for $l = 1$ or 2. (If $l = 0$, $j = 0$. Since $id \equiv (m-1)j \pmod{dp}$, we have $i = 0$. This contradicts $z \notin H_{ij}$.) So, the possibilities of $P^{-1}\theta_{kij}(x)P$ are only

$$\frac{\alpha^{3k}}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix}, \quad \frac{\alpha^{3k}}{2}\begin{pmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}.$$

The above two representations are isomorphic to $N_1(\chi_1) \otimes \rho_k$ and $N_1(\chi_1) \otimes \rho_{k+3}$, respectively where $\rho_k(x) := (-1)^k$ and $\rho_k(z) := \alpha^k$. We can refer to [**17**] for $N_1(\chi_1)$. The kernel of $N_1(\chi_1)$ is a congruence subgroup. So, this is not what we are looking for. Also, it is shown in [**8**] that any of these representations is not admissible.

(ii) **Degree 3.**

The irreducible representations of degree 3 appear in the case of $|H : H_{ij}| = 3$, i.e. $H_{ij} = \langle z^3 \rangle$. Then,

$$G_{ij} = \langle z^3 \rangle \cdot A, \quad G = G_{ij} + zG_{ij} + z^2 G_{ij}.$$

For $0 \le k, l \le 1$, let $\psi_k(z^{3l}) := (-1)^{kl}$, $\theta_{kij} := (\psi_k \otimes \phi_{ij})^G$. Then,

$$\theta_{kij}(z) = \begin{pmatrix} 0 & 0 & (-1)^k \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \theta_{kij}(x) = \begin{pmatrix} \beta^{id-(m+1)j} & 0 & 0 \\ 0 & \beta^{id-mj} & 0 \\ 0 & 0 & \beta^j \end{pmatrix}.$$

By Lemma 5.1, $z^3 \in H_{ij} \Leftrightarrow 2i \equiv 0 \pmod{p}$, $2j \equiv 0 \pmod{dp}$. Moreover, using the fact that $\theta_{kij}(x)$ is not a scalar matrix and $(xz)^3 = 1$, we see that the possibilities of $\theta_{kij}(x)$ are only

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{for } k = 0$$

and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{for } k = 1.$$

Each of these representations is isomorphic to each of the representations $N_1(1, \chi_1) \otimes \rho$ with $\deg \rho = 1$. We can refer to [**17**] for $N_1(1, \chi_1)$. Since the kernel of $N_1(1, \chi_1)$ is a congruence subgroup, this is not what we are looking for, too. Also, it is shown in [**8**] that any of these representations is not admissible.

Lastly, we shall consider the irreducible representations of degree 6.

6. The irreducible representations of degree 6.

Take $(i,j) \in (\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/dp\boldsymbol{Z})$ such that the congruence equations in Lemma 5.1 do not hold. Then $H_{ij} = 1$. So, ϕ_{ij}^G becomes an irreducible representation by the little group method.

$$\phi_{ij}^G(z) = \begin{pmatrix} & & & & & 1 \\ 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \end{pmatrix}$$

Take a conjugate of ϕ_{ij}^G with $P := (1/\sqrt{6})(\alpha^{cd})$ where α^{cd} denotes (c,d) entry.

$$P^{-1}\phi_{ij}^G(z)P = \begin{pmatrix} 1 & & & \\ & \alpha^{-1} & & \\ & & \ddots & \\ & & & \alpha^{-5} \end{pmatrix}$$

We note that $\phi_{ij}^G(z)$ is nondegenerate. Therefore, by a remark in section 2, the investigation becomes simpler. Furthermore, these representations are simpler than usual. We shall talk on this fact in details, later.

$$\begin{aligned} P^{-1}\phi_{ij}^G(x)P &= P^{-1}\phi_{ij}^G(z^3S^4(0,1))P = (P^{-1}\phi_{ij}^G(z)P)^3P^{-1}\phi_{ij}^G(S^4(0,1))P \\ &= \frac{1}{6}\begin{pmatrix} 1 & & & & & \\ & -1 & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & 1 & \\ & & & & & -1 \end{pmatrix}\left(\sum_{l=0}^{5}\alpha^{(-c+d)l}\phi_{ij}^G(S^{4+l}(0,1)\right), \end{aligned}$$

where $\sum_{l=0}^{5}\alpha^{(-c+d)l}\phi_{ij}^G(S^{4+l}(0,1))$ denotes (c,d) entry. The index of S is computed with mod 6. We define k_i and x_i as follows:

$$S^0(0,1) = (0,1) \quad k_0 := j,$$

$$S^1(0,1) = (-1, m+1) \quad k_1 := -id + (m+1)j,$$

$$S^2(0,1) = (0,1) \quad k_2 := -id + mj,$$

$$S^3(0,1) = (0,-1) \quad k_3 := -j,$$

$$S^4(0,1) = -S^1(0,1) \quad k_4 := -k_1,$$

$$S^5(0,1) = S^2(0,1) \quad k_5 := -k_2,$$

$x_i := \sum_{l=0}^{5} \alpha^{il} \beta^{k_{l+4}}$ where the index of k is computed with modulo 6. Then

$$P^{-1}\phi_{ij}^{G}(x)P = \frac{1}{6}\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 \\ -x_5 & -x_0 & -x_1 & -x_2 & -x_3 & -x_4 \\ x_4 & x_5 & x_0 & x_1 & x_2 & x_3 \\ -x_3 & -x_4 & -x_5 & -x_0 & -x_1 & -x_2 \\ x_2 & x_3 & x_4 & x_5 & x_0 & x_1 \\ -x_1 & -x_2 & -x_3 & -x_4 & -x_5 & -x_0 \end{pmatrix}.$$

By Lemma 2.2, when ρ moves to any equivalent unitary representation ρ' such that $\rho'(z) = \rho(z)$, there exists some unitary diagonal matrix $D = \begin{pmatrix} d_0 & & & \\ & d_1 & & \\ & & \ddots & \\ & & & d_5 \end{pmatrix}$ such that $\rho' = D^{-1}\rho D$. So if some ρ' is associated to a MFA, $x_i \neq 0$ must hold for all i. (If some x_i is 0, it contradicts to Verlinde's formula.) So, from now on we assume that $x_i \neq 0$ for all i.

Lemma 6.1. *$(PD)^{-1}\phi_{ij}^{G}(x)PD$ is symmetric.*

$$\Leftrightarrow d_1^2 = -\frac{x_5}{x_1}, \quad d_2^2 = \frac{x_4}{x_2}, \quad d_3^2 = -1, \quad d_4^2 = \frac{x_2}{x_4}, \quad d_5^2 = -\frac{x_1}{x_5}, \quad x_1x_2 = x_4x_5, \quad x_2^3 = x_4^3$$

Proof. This follows from comparing the entries of $(PD)^{-1}\phi_{ij}^{G}(x)PD$. □

We note from Lemma 6.1 that there are only two choices of d_i respectively such that $(PD)^{-1}\phi_{ij}^{G}(x)PD$ is symmetric.

Lemma 6.2. *There exist some diagonal unitary matrix D such that $(PD)^{-1}\phi_{ij}^{G}(x)PD$ is symmetric if and only if there exists i such that $\omega^i x_1 = x_5$ and $x_2 = \omega^i x_4$.*

Proof. This is a consequence of Lemma 6.1. □

Lemma 6.3. (i) $x_1 = x_5,\ x_2 = x_4 \Leftrightarrow id \equiv (m-1)j \pmod{dp}$.
(ii) $\omega x_1 = x_5,\ x_2 = \omega x_4 \Leftrightarrow 2id \equiv (2m+1)j \pmod{dp}$.
(iii) $\omega^2 x_1 = x_5,\ x_2 = \omega^2 x_4 \Leftrightarrow id \equiv (m+2)j \pmod{dp}$.

Proof. We will prove only (i). Proofs of (ii) and (iii) are similar to that of (i). Note that $x_i := \sum_{l=0}^{5} \alpha^{il}\beta^{k_{l+4}}$. From $x_1 = x_5$, we obtain

$$\sin\frac{2\pi}{dp}(id - mj) + \sin\frac{2\pi}{dp}j = 0.$$

Also, from $x_2 = x_4$, we obtain

$$\cos\frac{2\pi}{dp}(id - mj) - \cos\frac{2\pi}{dp}j = 0.$$

These equations are equivalent to $id \equiv (m-1)j \pmod{dp}$. □

Let $I = \xi_4$.

LEMMA 6.4. (i) *If* $x_1 = x_5$ *and* $x_2 = x_4$ *hold. Let* $d_0 = 1,\ d_1 = I,\ d_2 = 1,\ d_3 = I,\ d_4 = 1,\ d_5 = I$. *Then,*

$$(PD)^{-1}\phi_{ij}^{G}(x)PD = \frac{1}{6}\begin{pmatrix} x_0 & Ix_1 & x_2 & Ix_3 & x_2 & Ix_1 \\ Ix_1 & -x_0 & Ix_1 & -x_2 & Ix_3 & -x_2 \\ x_2 & Ix_1 & x_0 & Ix_1 & x_2 & Ix_3 \\ Ix_3 & -x_2 & Ix_1 & -x_0 & Ix_1 & -x_2 \\ x_2 & Ix_3 & x_2 & Ix_1 & x_0 & Ix_1 \\ Ix_1 & -x_2 & Ix_3 & -x_2 & Ix_1 & -x_0 \end{pmatrix}.$$

(ii) *If* $\omega x_1 = x_5$ *and* $x_2 = \omega x_4$ *hold. Let* $d_0 = 1,\ d_1 = \beta^5,\ d_2 = \beta^{10},\ d_3 = \beta^3,\ d_4 = \beta^4,\ d_5 = \beta^{11}$. *Then,*

$$(PD)^{-1}\phi_{ij}^{G}(x)PD = \frac{1}{6}\begin{pmatrix} x_0 & \beta^5x_1 & \beta^{10}x_2 & \beta^3x_3 & \beta^4x_2 & \beta^{11}x_1 \\ \beta^5x_1 & -x_0 & \beta^{11}x_1 & \beta^4x_2 & \beta^9x_3 & \beta^4x_2 \\ \beta^{10}x_2 & \beta^{11}x_1 & x_0 & \beta^5x_1 & \beta^{10}x_2 & \beta^9x_3 \\ \beta^3x_3 & \beta^4x_2 & \beta^5x_1 & -x_0 & \beta^{11}x_1 & \beta^{10}x_2 \\ \beta^4x_2 & \beta^9x_3 & \beta^{10}x_2 & \beta^{11}x_1 & x_0 & \beta^{11}x_1 \\ \beta^{11}x_1 & \beta^4x_2 & \beta^9x_3 & \beta^{10}x_2 & \beta^{11}x_1 & -x_0 \end{pmatrix}.$$

(iii) *If* $\omega^2 x_1 = x_5$ *and* $x_2 = \omega^2 x_4$ *hold. Let* $d_0 = 1,\ d_1 = \beta,\ d_2 = \beta^2,\ d_3 = \beta^3,\ d_4 = \beta^4,\ d_5 = \beta^{11}$. *Then,*

$$(PD)^{-1}\phi_{ij}^{G}(x)PD = \frac{1}{6}\begin{pmatrix} x_0 & \beta x_1 & \beta^2x_2 & \beta^3x_3 & \beta^8x_2 & \beta^7x_1 \\ \beta x_1 & -x_0 & \beta^7x_1 & \beta^8x_2 & \beta^9x_3 & \beta^8x_2 \\ \beta^2x_2 & \beta^7x_1 & x_0 & \beta x_1 & \beta^2x_2 & \beta^9x_3 \\ \beta^3x_3 & \beta^8x_2 & \beta x_1 & -x_0 & \beta^7x_1 & \beta^2x_2 \\ \beta^8x_2 & \beta^9x_3 & \beta^2x_2 & \beta^7x_1 & x_0 & \beta^7x_1 \\ \beta^7x_1 & \beta^8x_2 & \beta^9x_3 & \beta^2x_2 & \beta^7x_1 & -x_0 \end{pmatrix}.$$

REMARK.

(i) By Lemma 6.1, we know that there are only two choices of $d_0, d_1, \dots, d_5$, i.e., the choices of ± 1. So, when ρ' moves to any equivalent representation of ρ, Verlinde's formula of ρ' is different from that of ρ only by ± 1. From now on, let N_{ij}^k denote Verlinde's formula of the matrix of Lemma 6.4 where index i corresponds to row $i+1$.

(ii) We now prove Theorem 1.1. The matrices of representation are indexed by $\{0, 1, \dots, n\}$. There are $n!$ ways to index the matrices of representation. We have to consider all the cases. But, when we look at the matrices of Lemma 6.4 carefully, we see that how the values of N_{ij}^k (up to ± 1) appear are the same regardless of indexing, since the matrices look like a circulant. So, we only have to investigate the integral condition of N_{ij}^k by indexing the remark (i).

We shall show that the integral condition for each case in Lemma 6.4 does not hold.

(i) The case of $x_1 = x_5$ and $x_2 = x_4$.

Explicitly, put $c := \cos(2\pi j/dp)$, $s := \sin(2\pi j/dp)$. Then, we can write

$$x_0 = 2(2c^2 + 2c - 1), \quad x_1 = -2sI(1 + 2c), \quad x_2 = 2(2c + 1)(c - 1), \quad x_3 = 4sI(1 - c).$$

By the above remark, $-N_{12}^3 + N_{13}^4 = 2c$ must be an integer. Since $-1 \le c \le 1$, we have $c = -1, -1/2, 0, 1/2, 1$. Also, since

$$N_{11}^1 = -s\frac{16c^5 - 24c^4 - 82c^3 + 5c^2 + 36c - 5}{6(1+2c)(c-1)(2c^2+2c-1)(c+1)},$$

we have $c \neq 1/2, 1, 0, 1$.

Furthermore, since $N_{11}^4 = (c-1)/(2(2c^2+2c-1))$, we have $c \neq 1/2$.

Thus, these representations are not admissible.

(ii) The case of $\omega x_1 = x_5$ and $x_2 = \omega x_4$.

We consider two cases i.e., when p is odd and p is even.

Here, we note that d is not even. (If d is even, it contradicts to $m^2 + m + 1 \equiv 0 \pmod{d}$.)

(1) p:odd.

Put $c := \cos(2\pi/dp)(2^{-1}j)$, $s := \sin(2\pi/dp)(2^{-1}j)$. (Where 2^{-1} denotes the inverse element of 2 in $\boldsymbol{Z}/dp\boldsymbol{Z}$.) Then, we can write

$$x_0 = 2(2c^2+2c-1), \quad x_1 = -2s\alpha(1+2c), \quad x_2 = -2\alpha^2(2c+1)(c-1), \quad x_3 = -4sI(1-c).$$

By the above remark, $-N_{12}^3 + N_{13}^4 = -2c$ must be an integer. So, $c = -1, -1/2, 0, 1/2, 1$. Also, since

$$N_{11}^1 = -s\frac{16c^5 - 24c^4 - 82c^3 + 5c^2 + 36c - 5}{6(1+2c)(c-1)(2c^2+2c-1)(c+1)},$$

we have $c \neq -1/2, -1, 0, 1$.

Furthermore, since $N_{11}^4 = (c-1)/(2(2c^2+2c-1))$, we have $c \neq 1/2$.

Therefore, these representations are not admissible.

(2) p:even.

In this case, from $2id \equiv (2m+1)j \pmod{dp}$, $id \equiv mj + j/2 + k\,dp/2 \pmod{dp}$, $k = 0, 1$. $k = 0$ is similar to the case when p is odd.

Let $k = 1$. Put $c := \cos(2\pi/dp)(2^{-1}j)$, $s := \sin(2\pi/dp)(2^{-1}j)$. Then, we can write

$$x_0 = 2(2c^2+2c-1), \quad x_1 = 2s\beta^4(-1+2c), \quad x_2 = -2\beta^2(2c-1)(c+1), \quad x_3 = 4sI(1+c).$$

By the above remark, $-N_{12}^3 + N_{13}^4 = 2c$ must be an integer. So $c = -1, -1/2, 0, 1/2, 1$. Also, since

$$N_{11}^1 = s\frac{16c^5 + 24c^4 - 82c^3 - 5c^2 + 36c + 5}{6(-1+2c)(c-1)(2c^2-2c-1)(c+1)},$$

we have $c \neq 1/2, -1, 0, 1$.

Furthermore, since $N_{11}^4 = (c-1)/(2(2c^2+2c-1))$, we have $c \neq -1/2$.

Thus, these representations are not admissible.

(iii) The case of $\omega^2 x_1 = x_5$ and $x_2 = \omega^2 x_4$.

Put $c := \cos(2\pi/dp)j$, $s := \sin(2\pi/dp)j$. Then, we can write $x_0 = 2(2c^2+2c-1)$,

$x_1 = 2s\beta^5(1+2c)$, $x_2 = 2\beta^4(2c+1)(c-1)$, $x_3 = 4sI(1-c)$. By the above remark, $N_{12}^3 + N_{13}^4 = -2c$ must be an integer. So, $c = -1, -1/2, 0, 1/2, 1$. Also, since

$$N_{11}^1 = s\frac{16c^5 - 24c^4 - 82c^3 + 5c^2 + 36c - 5}{6(1+2c)(c-1)(2c^2+2c-1)(c+1)},$$

we have $c \neq -1/2, -1, 0, 1$.

Moreover since $N_{11}^4 = (c-1)/(2(2c^2+2c-1))$, we have $c \neq 1/2$.

Therefore, these representations are not admissible. This completes the proof of Theorem 1.1. □

Acknowledgement. The author would like to thank Professor Eiichi Bannai for suggesting this problem and for his untiring advices. The author would also like to thank Ms. Rowena Baylon for editing the grammar in this paper.

References

[1] Eiichi Bannai, Association schemes and fusion algebras (an introduction), J. Algebraic Combin., **2** (1993), no. 4, 327–344.

[2] Eiichi Bannai, E. Bannai, O. Shimabukuro and M. Tagami, Modular invariants of the modular data of finite groups, Preprint, April 2001.

[3] J. L. Brenner, The linear homogeneous group. III, Ann. of Math. (2), **71** (1960), 210–223.

[4] A. Coste and T. Gannon, Congruence subgroups and conformal field theory, in preparation, 2000.

[5] A. Coste, T. Gannon and P. Ruelle, Finite group modular data, Nuclear Phys. B, **581** (2000), no. 3, 679–717.

[6] C. W. Curtis and I. Reiner, Methods of representation theory with applications to finite groups and orders, Wiley Classics Library Edition Publishes, vol. 1 (1994).

[7] R. Dijkgraaf, C. Vafa, E. Verlinde and H. Verlinde, The operator algebra of orbifold models, Comm. Math. Phys., **123** (1989), no. 3, 485–526.

[8] W. Eholzer, On the classification of modular fusion algebras, Comm. Math. Phys., **172** (1995), no. 3, 623–659.

[9] T. Gannon, Modular data: the algebraic combinatorics of conformal field theory, Preprint, Feb. 2001.

[10] T. H. Koornwinder, B. J. Schroers, J. K. Slinkerland and F. A. Bais, Fourier transform and the Verlinde formula for the quantum-double of a finite group, J. Phys. A: Math. Gen., **32** (1999), 8539–8549.

[11] G. Lusztig, Leading coefficients of character values of Hecke algebras, The Arcata Conference on Representaions of Finite Groups (Arcata, Calif., 1986), 235–262, Proc. Sympos. Pure Math., **47**, Part 2, Amer. Math. Soc., Providence, RI, 1987.

[12] G. Lusztig, Exotic Fourier transform, Duke Math. J., **73** (1994), no. 1, 227–241, 243–248.

[13] M. Newman, A complete description of the normal subgroups of genus one of the modular group, Amer. J. Math., **86** (1964), 17–24.

[14] M. Newman, A note on modular groups, Proc. Amer. Math. Soc., vol. 14 (1963), 124–125.

[15] M. Newman, Normal subgroups of the modular group which are not congruence subgroups, Proc. Amer. Math. Soc., vol. 16 (1965), 831–832.

[16] A. Nobs, Die irreduziblen darstellungen der gruppen $SL_2(\boldsymbol{Z}_p)$ insbesondere $SL_2(\boldsymbol{Z}_2)$, Teil I, Comment. Math. Helv., **51** (1976), 465–489.

[17] A. Nobs and J. Wolfart, Die irreduziblen darstellungen der gruppen $SL_2(\boldsymbol{Z}_p)$ insbesondere $SL_2(\boldsymbol{Z}_2)$, Teil II, Comment. Math. Helv., **51** (1976), 491–526.

Makoto Tagami
Graduate School of Mathematics
Kyushu University
Ropponmatsu, Fukuoka, 810-8560
Japan