

Algebra & Number Theory

Volume 9

2015

No. 9

**Congruence property in
conformal field theory**

Chongying Dong, Xingjun Lin and Siu-Hung Ng



Congruence property in conformal field theory

Chongying Dong, Xingjun Lin and Siu-Hung Ng

The congruence subgroup property is established for the modular representations associated to any modular tensor category. This result is used to prove that the kernel of the representation of the modular group on the conformal blocks of any rational, C_2 -cofinite vertex operator algebra is a congruence subgroup. In particular, the q -character of each irreducible module is a modular function on the same congruence subgroup. The Galois symmetry of the modular representations is obtained and the order of the anomaly for those modular categories satisfying some integrality conditions is determined.

Introduction

Modular invariance of characters of a rational conformal field theory (RCFT) has been known since the work of Cardy [1986], and it was proved by Zhu [1996] for rational and C_2 -cofinite vertex operator algebras (VOA), which constitute a mathematical formalization of RCFT. The associated matrix representation of $SL_2(\mathbb{Z})$ relative to the distinguished basis, formed by the trace functions of the irreducible modules or primary fields, is a powerful tool in the study of vertex operator algebras and conformal field theory. This matrix representation conceives many intriguing arithmetic properties, and the Verlinde formula [1988] is certainly a notable example. Moreover, it has been shown that these matrices representing the modular group are defined over a certain cyclotomic field [de Boer and Goeree 1991].

An important characteristic of the modular representation ρ associated with a RCFT is its kernel. It has been conjectured by many authors that the kernel is a congruence subgroup of a certain level n (see [Moore 1987; Eholzer 1995; Eholzer and Skoruppa 1995; Dong and Mason 1996; Bauer et al. 1997]). Eholzer further conjectured that this representation is defined over the n -th cyclotomic field \mathbb{Q}_n . In this case, the Galois group $\text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ acts on the representation ρ by

Dong and Ng were partially supported by NSF grants.

MSC2010: primary 17B69; secondary 18D10, 20H05, 81R05.

Keywords: Frobenius–Schur indicator, modular tensor category, modular group, vertex operator algebra.

its entrywise action. Coste and Gannon [1994] proved that ρ determines a signed permutation matrix G_σ for each automorphism σ of \mathbb{Q}_n . They also conjectured that the representation $\sigma^2\rho$ is equivalent to ρ under the intertwining operator G_σ . These conjectural properties were summarized as the congruence property of the modular data associated with RCFT in [Coste and Gannon 1999; Gannon 2006]. These remarkable properties of RCFT were established by Bantay [2003] under certain assumptions, and by Coste and Gannon [1994] under the condition that the order of the Dehn twist is odd. In the formalization of RCFT through conformal nets, the congruence property was proved by Xu [2006].

In this paper we give a positive answer to the conjecture on the congruence property for a rational and C_2 -cofinite vertex operator algebra V . Such a V has only finitely many irreducible modules [Dong et al. 1998a] M^0, \dots, M^p up to isomorphism and there exist $\lambda_i \in \mathbb{C}$ for $i = 0, \dots, p$ such that

$$M^i = \bigoplus_{n=0}^{\infty} M_{\lambda_i+n}^i$$

where $M_{\lambda_i}^i \neq 0$ and $L(0)|_{M_{\lambda_i+n}^i} = \lambda_i + n$ for any $n \in \mathbb{Z}$. Moreover, λ_i and the central charge c are rational numbers (see [Dong et al. 2000]).

The trace function for $v \in V_k$ on M^i is defined as

$$Z_i(v, q) = q^{\lambda_i - c/24} \sum_{n=0}^{\infty} (\text{tr}_{M_{\lambda_i+n}^i} o(v)) q^n$$

where $o(v) = v_{k-1}$ is the $(k-1)$ -st component operator of $Y(v, z) = \sum_{n \in \mathbb{Z}} v_n z^{-n-1}$ which maps each homogeneous subspace of M^i to itself. If $v = \mathbb{1}$ is the vacuum vector we get the q -character $\chi_i(q)$ of M^i . It is proved in [Zhu 1996] that if V is C_2 -cofinite then $Z_i(v, q)$ converges to a holomorphic function on the upper half-plane in variable τ where $q = e^{2\pi i \tau}$. By abusing the notation we also denote this holomorphic function by $Z_i(v, \tau)$. There is another vertex operator algebra structure on V [Zhu 1996] with grading $V = \bigoplus_{n \in \mathbb{Z}} V_{[n]}$. We will write $\text{wt}[v] = n$ if $v \in V_{[n]}$. Then there is a representation ρ_V of the modular group $\text{SL}_2(\mathbb{Z})$ on the space spanned by $\{Z_i(v, \tau) \mid i = 0, \dots, p\}$:

$$Z_i(v, \gamma \tau) = (c\tau + d)^{\text{wt}[v]} \sum_{j=0}^p \gamma_{ij} Z_j(v, \tau)$$

where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z})$ and $\rho_V(\gamma) = [\gamma_{ij}]$ [Zhu 1996].

Theorem I. *Let V be a rational, C_2 -cofinite, self-dual simple vertex operator algebra. Then each $Z_i(v, \tau)$ is a modular form of weight $\text{wt}[v]$ on a congruence subgroup of $\text{SL}_2(\mathbb{Z})$ of level n , which is the smallest positive integer such that*

$n(\lambda_i - c/24)$ is an integer for all i . In particular, each q -character χ_i is a modular function on the same congruence subgroup.

We should remark that the modularity of the q -characters of irreducible modules for some known vertex operator algebras such as those associated to the highest weight unitary representations for Kac–Moody algebras [Kac and Peterson 1984; Kac 1990] and the Virasoro algebra [Rocha-Caridi 1985] were previously known. The readers are referred to [Dong et al. 2001] for the modularity of $Z_i(v, \tau)$ when V is a vertex operator algebra associated to a positive definite even lattice.

According to [Huang 2008a; 2008b], the category \mathcal{C}_V of modules of a rational and C_2 -cofinite vertex operator algebra V under the tensor product defined in [Huang and Lepowsky 1995a; 1995b; 1995c; Huang 1995] is a modular tensor category over \mathbb{C} . To establish this theorem we have to turn our attention to general modular tensor categories.

Modular tensor categories, or simply called modular categories, play an integral role in the Reshetikhin–Turaev TQFT invariant of 3-manifolds [Turaev 2010] and topological quantum computation [Wang 2010]. They also constitute another formalization of RCFT [Moore and Seiberg 1990; Bakalov and Kirillov 2001].

Parallel to a rational conformal field theory, associated to a modular category \mathcal{A} are the invertible matrices \tilde{s} and \tilde{t} indexed by the set Π of isomorphism classes of simple objects of \mathcal{A} . These matrices define a projective representation $\bar{\rho}_{\mathcal{A}}$ of $SL_2(\mathbb{Z})$ by the assignment

$$\mathfrak{s} := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \mapsto \tilde{s} \quad \text{and} \quad \mathfrak{t} := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \mapsto \tilde{t},$$

and the well-known presentation $SL_2(\mathbb{Z}) = \langle \mathfrak{s}, \mathfrak{t} \mid \mathfrak{s}^4 = 1, (\mathfrak{st})^3 = \mathfrak{s}^2 \rangle$ of the modular group. It was proved by Ng and Schauenburg [2010] that the kernel of this projective representation of $SL_2(\mathbb{Z})$ is a congruence subgroup of level N , where N is the order of \tilde{t} . Moreover, both \tilde{s} and \tilde{t} are matrices over \mathbb{Q}_N . For factorizable semisimple Hopf algebras, the corresponding result was proved previously by Sommerhäuser and Zhu [2012].

The projective representation $\bar{\rho}_{\mathcal{A}}$ can be lifted to an ordinary representation of $SL_2(\mathbb{Z})$ which is called a *modular representation of \mathcal{A}* in [Ng and Schauenburg 2010]. There are only finitely many modular representations of \mathcal{A} but, in general, none of them is a canonical choice. However, if \mathcal{A} is the Drinfeld center of a spherical fusion category, then \mathcal{A} is modular (see [Müger 2003b]) and it admits a canonical modular representation defined over \mathbb{Q}_N whose kernel is a congruence subgroup of level N (see [Ng and Schauenburg 2010]). The canonical modular representation of the module category over the Drinfeld double of a semisimple Hopf algebra was shown to have a congruence kernel as well as Galois symmetry (see Theorem II (iii) and (iv)) in [Sommerhäuser and Zhu 2012].

The second main theorem of this paper is to prove that the congruence property and Galois symmetry holds for all modular representations of any modular category.

Theorem II. *Let \mathcal{A} be a modular category over any algebraically closed field \mathbb{k} of characteristic zero with the set of isomorphism classes of simple objects Π and Frobenius–Schur exponent N . Suppose $\rho : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{GL}_\Pi(\mathbb{k})$ is a modular representation of \mathcal{A} where $\mathrm{GL}_\Pi(\mathbb{k})$ denotes the group of invertible matrices over \mathbb{k} indexed by Π . Set $s = \rho(\mathfrak{s})$ and $t = \rho(\mathfrak{t})$. Then:*

- (i) $\ker \rho$ is a congruence subgroup of level n where $n = \mathrm{ord}(t)$ and, moreover, $N \mid n \mid 12N$.
- (ii) ρ is \mathbb{Q}_n -rational, i.e., $\mathrm{im} \rho \leq \mathrm{GL}_\Pi(\mathbb{Q}_n)$, where $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$ for some primitive n -th root of unity $\zeta_n \in \mathbb{k}$.
- (iii) For $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, the matrix $G_\sigma = \sigma(s)s^{-1}$ is a signed permutation matrix, and

$$\sigma^2(\rho(\gamma)) = G_\sigma \rho(\gamma) G_\sigma^{-1}$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. In particular, if $(G_\sigma)_{ij} = \epsilon_\sigma(i) \delta_{\hat{\sigma}(i)j}$ for some sign function ϵ_σ and permutation $\hat{\sigma}$ on Π , then $\sigma^2(t_{ii}) = t_{\hat{\sigma}(i)\hat{\sigma}(i)}$ for all $i \in \Pi$.

- (iv) Let a be an integer relatively prime to n with an inverse b modulo n . For the automorphism σ_a of \mathbb{Q}_n given by $\zeta_n \mapsto \zeta_n^a$,

$$G_{\sigma_a} = t^a s t^b s t^a s^{-1}.$$

We return to the modular tensor category \mathcal{C}_V associated to a rational, C_2 -cofinite and self-dual vertex operator algebra V . This yields a projective representation of $\mathrm{SL}_2(\mathbb{Z})$ on space spanned by the equivalence classes of irreducible V -modules. We show in Theorem 3.10 that the representation ρ_V of $\mathrm{SL}_2(\mathbb{Z})$ is a modular representation of \mathcal{C}_V . This implies that the kernel of ρ_V is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Although the congruence property proved in Theorem II is motivated by solving the congruence property conjecture on the trace functions of vertex operator algebras, the result has its own importance. We will discuss this in the rest of the introduction.

It was also shown in [Sommerhäuser and Zhu 2012] that the (unnormalized) T -matrix \tilde{t} of the module category over a factorizable Hopf algebra also enjoys the Galois symmetry $\sigma^2(\tilde{t}) = G_\sigma \tilde{t} G_\sigma^{-1}$ for any $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$. However, this extra symmetry does not hold for a general modular category \mathcal{A} (see Example 4.6). This condition is, in fact, related to the order of the quotient of the Gauss sums, called the *anomaly*, of \mathcal{A} . It is proved in Proposition 4.7 that Galois symmetry of the T -matrix is equivalent to the condition that the anomaly is a fourth root of unity. We will prove in Proposition 6.7 that the anomaly of any *integral* modular category is always a fourth root of unity. Therefore, the T -matrix of any integral modular

category enjoys the Galois symmetry. For a *weakly integral* modular category, such as the Ising model, the anomaly is always an eighth root of unity (Theorem 6.10).

Using Theorem II, we uncover some relations among the global dimension $\dim \mathcal{A}$, the Frobenius–Schur exponent N and the order of the anomaly α of a modular category \mathcal{A} . We define

$$J_{\mathcal{A}} = (-1)^{1+\text{ord } \alpha}$$

to record the parity of the order of the anomaly. If N is not a multiple of 4, then $J_{\mathcal{A}} \dim \mathcal{A}$ has a square root in \mathbb{Q}_N . If, in addition, $\dim \mathcal{A}$ is an odd integer, then $J_{\mathcal{A}}$ coincides with the Jacobi symbol $\left(\frac{-1}{\dim \mathcal{A}}\right)$. The consequence of this observation is a result closely related to the Cauchy theorem of integral fusion category.

The organization of this paper is as follows: Section 1 covers some basic definitions, conventions and preliminary results on spherical fusion categories and modular categories. In Section 2, we prove the congruence property, Theorem II (i) and (ii), by proving a lifting theorem of modular projective representations with congruence kernels. In Section 3, we prove the associated representation of modular invariance of trace functions of a rational, C_2 -cofinite vertex operator algebra V is a modular representation of its module category. Using Theorem II (i) and (ii), we prove Theorem I: the trace functions of V are modular forms. In Section 4, we assume the technical Lemma 4.2 to prove the Galois symmetry of modular categories as well as RCFTs, Theorem II (iii) and (iv). Section 5 is devoted to the proof of Lemma 4.2 by using generalized Frobenius–Schur indicators. In Section 6, we use the congruence property and Galois symmetry of modular categories (Theorem II) to uncover some arithmetic relations among the global dimension, the Frobenius–Schur exponent and the anomaly of a modular category. In particular, we determine the order of the anomaly of a modular category satisfying certain integrality conditions.

1. Basics of modular tensor categories

In this section, we will collect some conventions and preliminary results on spherical fusion categories and modular categories. Most of these results are quite well-known, and the readers are referred to [Turaev 2010; Bakalov and Kirillov 2001; Ng and Schauenburg 2007a; 2007b; 2008; 2010] and the references therein.

Throughout this paper, \mathbb{k} is always assumed to be an algebraically closed field of characteristic zero. The group of invertible matrices over a commutative ring K indexed by Π is denoted by $\text{GL}_{\Pi}(K)$, and we will write $\text{PGL}_{\Pi}(K)$ for its associated projective linear group. If $\Pi = \{1, \dots, r\}$ for some positive integer r , then $\text{GL}_{\Pi}(K)$ (resp. $\text{PGL}_{\Pi}(K)$) will be denoted by the standard notation $\text{GL}_r(K)$ (resp. $\text{PGL}_r(K)$) instead.

For any primitive n -th root of unity $\zeta_n \in \mathbb{k}$, we let $\mathbb{Q}_n := \mathbb{Q}(\zeta_n)$ be the smallest subfield of \mathbb{k} containing all the n -th roots of unity in \mathbb{k} . Recall that $\text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is isomorphic to $U(\mathbb{Z}_n)$, the group of units of \mathbb{Z}_n . Let a be an integer relatively prime to n . The associated $\sigma_a \in \text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is defined by

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

Define $\mathbb{Q}_{\text{ab}} = \bigcup_{n \in \mathbb{N}} \mathbb{Q}_n$, the abelian closure of \mathbb{Q} in \mathbb{k} . Since \mathbb{Q}_n is Galois over \mathbb{Q} , we have $\sigma(\mathbb{Q}_n) = \mathbb{Q}_n$ for all automorphisms σ of \mathbb{Q}_{ab} . Moreover, the restriction map $\text{Aut}(\mathbb{Q}_{\text{ab}}) \xrightarrow{\text{res}} \text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is surjective for all positive integers n . Thus, for any integer a relatively prime to n , there exists a $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ such that $\sigma|_{\mathbb{Q}_n} = \sigma_a$.

1.1. Spherical fusion categories. In a left rigid monoidal category \mathcal{C} with tensor product \otimes and unit object $\mathbf{1}$, we denote a left dual V^\vee of $V \in \mathcal{C}$ with morphisms $\text{db}_V : \mathbf{1} \rightarrow V \otimes V^\vee$ and $\text{ev}_V : V^\vee \otimes V \rightarrow \mathbf{1}$ by the triple $(V^\vee, \text{db}_V, \text{ev}_V)$. The left duality can be extended to a monoidal functor $(-)^\vee : \mathcal{C} \rightarrow \mathcal{C}^{\text{op}}$, and so $(-)^{\vee\vee} : \mathcal{C} \rightarrow \mathcal{C}$ defines a monoidal equivalence. Moreover we can choose $\mathbf{1}^\vee = \mathbf{1}$. A *pivotal structure* of \mathcal{C} is an isomorphism $j : \text{Id}_{\mathcal{C}} \rightarrow (-)^{\vee\vee}$ of monoidal functors. One can respectively define the left and the right pivotal traces of an endomorphism $f : V \rightarrow V$ in \mathcal{C} as

$$\underline{\text{ptr}}^\ell(f) = \left(\mathbf{1} \xrightarrow{\text{db}_{V^\vee}} V^\vee \otimes V^{\vee\vee} \xrightarrow{\text{id} \otimes j_V^{-1}} V^\vee \otimes V \xrightarrow{\text{id} \otimes f} V^\vee \otimes V \xrightarrow{\text{ev}_V} \mathbf{1} \right)$$

and

$$\underline{\text{ptr}}^r(f) = \left(\mathbf{1} \xrightarrow{\text{db}_V} V \otimes V^\vee \xrightarrow{f \otimes \text{id}} V \otimes V^\vee \xrightarrow{j_V \otimes \text{id}} V^{\vee\vee} \otimes V^\vee \xrightarrow{\text{ev}_{V^\vee}} \mathbf{1} \right).$$

The pivotal structure is called *spherical* if the two pivotal traces coincide for all endomorphisms f in \mathcal{C} .

A *pivotal* (resp. *spherical*) *category* (\mathcal{C}, j) is a left rigid monoidal category \mathcal{C} equipped with a pivotal (resp. spherical) structure j . We will simply denote the pair (\mathcal{C}, j) by \mathcal{C} when there is no ambiguity. The left and the right pivotal dimensions of $V \in \mathcal{C}$ are defined as $d_\ell(V) = \underline{\text{ptr}}^\ell(\text{id}_V)$ and $d_r(V) = \underline{\text{ptr}}^r(\text{id}_V)$ respectively. In a spherical category, the pivotal traces and dimensions will be denoted by $\underline{\text{ptr}}(f)$ and $d(V)$ (or $\dim V$), respectively.

A *fusion category* \mathcal{C} over the field \mathbb{k} is an abelian \mathbb{k} -linear semisimple (left) rigid monoidal category with a simple unit object $\mathbf{1}$, finite-dimensional morphism spaces and finitely many isomorphism classes of simple objects (see [Etingof et al. 2005]). We will denote by $\Pi_{\mathcal{C}}$ the set of isomorphism classes of simple objects of \mathcal{C} , and by 0 the isomorphism class of $\mathbf{1}$, unless stated otherwise. If $i \in \Pi_{\mathcal{C}}$, we write i^* for the (left) dual of the isomorphism class i . Moreover, $i \mapsto i^*$ defines a permutation of order at most 2 on $\Pi_{\mathcal{C}}$.

In a spherical fusion category \mathcal{C} over \mathbb{k} , $d(V)$ can be identified with a scalar in \mathbb{k} for $V \in \mathcal{C}$. We use the abbreviation $d_i \in \mathbb{k}$ for the pivotal dimension of $i \in \Pi_{\mathcal{C}}$. By

[Müger 2003a, Lemma 2.8], $d_i = d_{i^*}$ for all $i \in \Pi_{\mathcal{C}}$. The global dimension $\dim \mathcal{C}$ of \mathcal{C} is defined by

$$\dim \mathcal{C} = \sum_{i \in \Pi_{\mathcal{C}}} d_i^2.$$

A pivotal category (\mathcal{C}, j) is said to be *strict* if \mathcal{C} is a strict monoidal category and if the pivotal structure j and the canonical isomorphism $(V \otimes W)^\vee(1/2) \rightarrow W^\vee \otimes V^\vee$ are identities. It has been proved in [Ng and Schauenburg 2007b, Theorem 2.2] that every pivotal category is *pivotaly equivalent* to a strict pivotal category.

1.2. Representations of the modular group. The modular group $SL_2(\mathbb{Z})$ is the group of 2×2 integral matrices with determinant 1. It is well-known that the modular group is generated by

$$s = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad t = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{with defining relations } (st)^3 = s^2, s^4 = \text{id}. \quad (1-1)$$

We denote by $\Gamma(n)$ the kernel of the reduction modulo n epimorphism $\pi_n : SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}_n)$. A subgroup L of $SL_2(\mathbb{Z})$ is called a *congruence subgroup of level n* if n is the least positive integer for which $\Gamma(n) \leq L$.

For any pair of matrices $A, B \in GL_r(\mathbb{k})$, with $r \in \mathbb{N}$, satisfying the conditions

$$A^4 = \text{id} \quad \text{and} \quad (AB)^3 = A^2,$$

one can define a representation $\rho : SL_2(\mathbb{Z}) \rightarrow GL_r(\mathbb{k})$ such that $\rho(s) = A$ and $\rho(t) = B$ via the presentation (1-1) of $SL_2(\mathbb{Z})$.

Suppose $\bar{\rho} : SL_2(\mathbb{Z}) \rightarrow PGL_r(\mathbb{k})$ is a projective representation of $SL_2(\mathbb{Z})$. A *lifting* of $\bar{\rho}$ is an *ordinary* representation $\rho : SL_2(\mathbb{Z}) \rightarrow GL_r(\mathbb{k})$ such that $\eta \circ \rho = \bar{\rho}$, where $\eta : GL_r(\mathbb{k}) \rightarrow PGL_r(\mathbb{k})$ is the natural surjection map. One can always lift $\bar{\rho}$ to a representation $\rho : SL_2(\mathbb{Z}) \rightarrow GL_r(\mathbb{k})$ as follows: let $\hat{A}, \hat{B} \in GL_r(\mathbb{k})$ such that $\bar{\rho}(s) = \eta(\hat{A})$ and $\bar{\rho}(t) = \eta(\hat{B})$. Then

$$\hat{A}^4 = \mu_s \text{id} \quad \text{and} \quad (\hat{A}\hat{B})^3 = \mu_t \hat{A}^2$$

for some scalars $\mu_s, \mu_t \in \mathbb{k}^\times$. Take $\lambda, \zeta \in \mathbb{k}$ such that $\lambda^4 = \mu_s$ and $\zeta^3 = \mu_t/\lambda$, and set $A = \hat{A}/\lambda$ and $B = \hat{B}/\zeta$. Then we have

$$A^4 = \text{id} \quad \text{and} \quad (AB)^3 = A^2.$$

Therefore, the assignment $\rho : s \mapsto A, t \mapsto B$ defines a lifting of $\bar{\rho}$.

Let ρ be a lifting of $\bar{\rho}$. Suppose $x \in \mathbb{k}$ is a 12-th root of unity. Then the assignment

$$\rho_x : s \mapsto \frac{1}{x^3} \rho(s), \quad t \mapsto x \rho(t) \quad (1-2)$$

also defines a lifting of $\bar{\rho}$. If $\rho' : \text{SL}_2(\mathbb{Z}) \rightarrow \text{GL}_r(\mathbb{k})$ is another lifting of $\bar{\rho}$, then

$$\rho'(\mathfrak{s}) = a\rho(\mathfrak{s}) \quad \text{and} \quad \rho'(\mathfrak{t}) = b\rho(\mathfrak{t})$$

for some $a, b \in \mathbb{k}^\times$. It follows immediately from (1-1) that $a^4 = 1$ and $(ab)^3 = a^2$. This implies $b^{12} = 1$ and $b^{-3} = a$. Therefore, we have $\rho' = \rho_b$ and so $\bar{\rho}$ has at most 12 liftings.

For any 12-th root of unity $x \in \mathbb{k}$, the assignment $\chi_x : \mathfrak{s} \mapsto x^{-3}, \mathfrak{t} \mapsto x$ defines a linear character of $\text{SL}_2(\mathbb{Z})$. It is straightforward to check that $\chi_x \otimes \rho$ is isomorphic to ρ_x as representations of $\text{SL}_2(\mathbb{Z})$. Therefore, the lifting of $\bar{\rho}$ is *unique* up to a linear character of $\text{SL}_2(\mathbb{Z})$.

1.3. Modular categories. Following [Kassel 1995], a *twist* (or *ribbon structure*) of a left rigid braided monoidal category \mathcal{C} with a braiding c is an automorphism θ of the identity functor $\text{Id}_{\mathcal{C}}$ satisfying

$$\theta_{V \otimes W} = (\theta_V \otimes \theta_W) \circ c_{W,V} \circ c_{V,W}, \quad \theta_V^\vee = \theta_{V^\vee}$$

for $V, W \in \mathcal{C}$. Associated to the braiding c is the Drinfeld isomorphism $u : \text{Id}_{\mathcal{C}} \rightarrow (-)^{\vee\vee}$. When \mathcal{C} is a braided fusion category over \mathbb{k} , there is a one-to-one correspondence between twists θ and spherical structures j of \mathcal{C} given by $\theta = u^{-1}j$ (see [Ng and Schauenburg 2007a, p. 38] for more details).

A *modular tensor category* over \mathbb{k} (see [Turaev 2010; Bakalov and Kirillov 2001]), also called a modular category, is a braided spherical fusion category \mathcal{A} over \mathbb{k} such that the S -matrix of \mathcal{A} defined by

$$\tilde{s}_{ij} = \underline{\text{ptr}}(c_{V_j, V_i^*} \circ c_{V_i^*, V_j})$$

is nonsingular, where V_j denotes an object in the class $j \in \Pi_{\mathcal{A}}$. In this case, the associated ribbon structure θ is of finite order N (see [Vafa 1988; Bakalov and Kirillov 2001]). Let $\theta_{V_i} = \theta_i \text{id}_{V_i}$ for some $\theta_i \in \mathbb{k}$. Since $\theta_{\mathbf{1}} = \text{id}_{\mathbf{1}}$, we have $\theta_0 = 1$. The T -matrix \tilde{t} of \mathcal{A} is defined by $\tilde{t}_{ij} = \delta_{ij}\theta_j$ for $i, j \in \Pi_{\mathcal{A}}$. It is immediate to see that $\text{ord}(\tilde{t}) = N$, which is called the *Frobenius–Schur exponent* of \mathcal{A} and denoted by $\text{FSexp}(\mathcal{A})$, is finite (see [Ng and Schauenburg 2007a, Theorem 7.7]).

The matrices \tilde{s}, \tilde{t} of a modular category \mathcal{A} satisfy the conditions

$$(\tilde{s}\tilde{t})^3 = p_{\mathcal{A}}^+ \tilde{s}^2, \quad \tilde{s}^2 = p_{\mathcal{A}}^+ p_{\mathcal{A}}^- C, \quad C\tilde{t} = \tilde{t}C, \quad C^2 = \text{id}, \quad (1-3)$$

where $p_{\mathcal{A}}^\pm = \sum_{i \in \Pi_{\mathcal{A}}} d_i^2 \theta_i^{\pm 1}$ are called the *Gauss sums*, and $C = [\delta_{ij^*}]_{i,j \in \Pi_{\mathcal{A}}}$ is called the *charge conjugation matrix* of \mathcal{A} . The quotient $p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ is a root of unity (see [Bakalov and Kirillov 2001, Theorem 3.1.19] or [Vafa 1988]), and

$$p_{\mathcal{A}}^+ p_{\mathcal{A}}^- = \dim \mathcal{A} \neq 0. \quad (1-4)$$

Moreover, \tilde{s} satisfies

$$\tilde{s}_{ij} = \tilde{s}_{ji} \quad \text{and} \quad \tilde{s}_{ij^*} = \tilde{s}_{i^*j} \tag{1-5}$$

for all $i, j \in \Pi_{\mathcal{A}}$.

The relations (1-3) imply that

$$\bar{\rho}_{\mathcal{A}} : \mathfrak{s} \mapsto \eta(\tilde{s}), \quad \mathfrak{t} \mapsto \eta(\tilde{t}) \tag{1-6}$$

defines a projective representation of $SL_2(\mathbb{Z})$, where $\eta : GL_{\Pi_{\mathcal{A}}}(\mathbb{k}) \rightarrow PGL_{\Pi_{\mathcal{A}}}(\mathbb{k})$ is the natural surjection. By [Ng and Schauenburg 2010, Theorem 6.8], $\ker \bar{\rho}_{\mathcal{A}}$ is a congruence subgroup of level N .

It is well-known that $\bar{\rho}_{\mathcal{A}}$ can be lifted to an ordinary representation (see [Bakalov and Kirillov 2001, Remark 3.1.9] or Section 1.2). Following [Ng and Schauenburg 2010], a lifting ρ of $\bar{\rho}_{\mathcal{A}}$ is called a *modular representation* of \mathcal{A} . By (1-4), for any 6-th root $\zeta \in \mathbb{k}$ of $p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$, we have that $(p_{\mathcal{A}}^+ / \zeta^3)^2 = \dim \mathcal{A}$. It follows from (1-3) that the assignment

$$\rho^{\zeta} : \mathfrak{s} \mapsto \frac{\zeta^3}{p_{\mathcal{A}}^+} \tilde{s}, \quad \mathfrak{t} \mapsto \frac{1}{\zeta} \tilde{t} \tag{1-7}$$

defines a modular representation of \mathcal{A} .

Thus, if ρ is a modular representation of \mathcal{A} , it follows from Section 1.2 that $\rho = \rho_x^{\zeta}$ for some 12-th root of unity $x \in \mathbb{k}$. Thus $\rho(\mathfrak{s})^2 = \pm C$. More precisely, $\rho(\mathfrak{s})^2 = x^6 C$.

A modular category \mathcal{A} is called *anomaly-free* if the quotient $p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ equals 1. The terminology addresses the associated anomaly-free TQFT with such a modular category [Turaev 2010]. In this spirit, we will simply call the quotient $\alpha_{\mathcal{A}} := p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ the *anomaly* of \mathcal{A} .

If \mathcal{A} is an anomaly-free modular category, then $p_{\mathcal{A}}^+$ is a *canonical* choice of square root of $\dim \mathcal{A}$, and hence a *canonical* modular representation of \mathcal{A} is determined by the assignment

$$\rho_{\mathcal{A}} : \mathfrak{s} \mapsto \frac{1}{p_{\mathcal{A}}^+} \tilde{s}, \quad \mathfrak{t} \mapsto \tilde{t}. \tag{1-8}$$

For any modular category \mathcal{A} over \mathbb{C} , we have that $\dim \mathcal{A} > 0$ (see [Etingof et al. 2005]). The *central charge* \mathfrak{c} of \mathcal{A} is a rational number modulo 8 defined by $\exp(\pi i \mathfrak{c} / 4) = p_{\mathcal{A}}^+ / \sqrt{\dim \mathcal{A}}$ where $\sqrt{\dim \mathcal{A}}$ denotes the positive square root of $\dim \mathcal{A}$, and so the anomaly α of \mathcal{A} is given by

$$\alpha = \exp\left(\frac{\pi i \mathfrak{c}}{2}\right). \tag{1-9}$$

We will show in Theorem 3.10 that the central charge \mathfrak{c} of the modular category \mathcal{C}_V is equal to central charge c of V modulo 4.

Remark. The S - and T -matrices of a modular category are preserved by equivalence of braided pivotal categories over \mathbb{k} , and so are the dimensions of simple objects, the global dimension, the Gauss sums and the anomaly. By the last paragraph of Section 1.1, without loss of generality, we may assume that the underlying pivotal category of a modular category over \mathbb{k} is *strict*.

1.4. Quantum doubles of spherical fusion categories. Let \mathcal{C} be a strict monoidal category. The left Drinfeld center $Z(\mathcal{C})$ of \mathcal{C} is a category whose objects are pairs of the form $\mathbf{X} = (X, \sigma_X)$, where X is an object of \mathcal{C} , and the *half-braiding* $\sigma_X(-) : X \otimes (-) \rightarrow (-) \otimes X$ is a natural isomorphism satisfying the properties $\sigma_X(\mathbf{1}) = \text{id}_X$ and

$$(\text{id}_V \otimes \sigma_X(W)) \circ (\sigma_X(V) \otimes \text{id}_W) = \sigma_X(V \otimes W)$$

for all $V, W \in \mathcal{C}$. It is well-known that $Z(\mathcal{C})$ is a braided strict monoidal category (see [Kassel 1995]) with unit object $(\mathbf{1}, \sigma_{\mathbf{1}})$ and tensor product $(X, \sigma_X) \otimes (Y, \sigma_Y) := (X \otimes Y, \sigma_{X \otimes Y})$, where

$$\sigma_{X \otimes Y}(V) = (\sigma_X(V) \otimes \text{id}_Y) \circ (\text{id}_X \otimes \sigma_Y(V)), \quad \sigma_{\mathbf{1}}(V) = \text{id}_V$$

for $V \in \mathcal{C}$. The forgetful functor $Z(\mathcal{C}) \rightarrow \mathcal{C}$, $\mathbf{X} = (X, \sigma_X) \mapsto X$, is a strict monoidal functor.

When \mathcal{C} is a (strict) spherical fusion category over \mathbb{k} , by Müger’s result [2003b], the center $Z(\mathcal{C})$ is a modular category over \mathbb{k} with the inherited spherical structure from \mathcal{C} . In addition,

$$p_{Z(\mathcal{C})}^+ = \dim \mathcal{C} = p_{Z(\mathcal{C})}^-.$$

Therefore, $Z(\mathcal{C})$ is anomaly-free and it admits a canonical modular representation $\rho_{Z(\mathcal{C})}$ described in (1-8). In particular,

$$\rho_{Z(\mathcal{C})}(\mathfrak{t}) = \tilde{t} \quad \text{and} \quad \rho_{Z(\mathcal{C})}(\mathfrak{s}) = \frac{1}{\dim \mathcal{C}} \tilde{s}, \tag{1-10}$$

which is called the *canonical normalization* of the S -matrix of $Z(\mathcal{C})$. By [Ng and Schauenburg 2010, Theorems 6.7 and 7.1], $\ker \rho_{Z(\mathcal{C})}$ is a congruence subgroup of level N , and $\text{im } \rho_{Z(\mathcal{C})} \leq \text{GL}_{\Pi_{Z(\mathcal{C})}}(\mathbb{Q}_N)$, where $N = \text{ord}(\tilde{t})$.

2. Rationality and kernels of modular representations

In this section, we prove the congruence property given in (i) and (ii) of Theorem II. Recall that a projective representation $\bar{\rho} : G \rightarrow \text{PGL}_r(\mathbb{k})$ of a group G determines a cohomology class $\kappa_{\bar{\rho}} \in H^2(G, \mathbb{k}^\times)$. For any section $\iota : \text{PGL}_r(\mathbb{k}) \rightarrow \text{GL}_r(\mathbb{k})$ of the natural surjection $\eta : \text{GL}_r(\mathbb{k}) \rightarrow \text{PGL}_r(\mathbb{k})$, the function $\gamma_\iota : G \times G \rightarrow \mathbb{k}^\times$ given by

$$\rho_\iota(ab) = \gamma_\iota(a, b) \rho_\iota(a) \rho_\iota(b)$$

determines a 2-cocycle in $\kappa_{\bar{\rho}}$, where $\rho_i = \iota \circ \bar{\rho}$. The cohomology class $\kappa_{\bar{\rho}}$ is trivial if and only if $\bar{\rho}$ can be *lifted* to a linear representation $\rho : G \rightarrow \text{GL}_r(\mathbb{k})$, i.e., $\eta \circ \rho = \bar{\rho}$ (see [Karpilovsky 1985, p. 72]).

Let $\pi : L \rightarrow G$ be a group homomorphism. For any 2-cocycle $\gamma \in Z^2(G, \mathbb{k}^\times)$, we have $\gamma \circ (\pi \times \pi) \in Z^2(L, \mathbb{k}^\times)$. The assignment $\gamma \mapsto \gamma \circ (\pi \times \pi)$ of 2-cocycles induces the group homomorphism $\pi^* : H^2(G, \mathbb{k}^\times) \rightarrow H^2(L, \mathbb{k}^\times)$, which is called the inflation map along π . In particular, $\pi^* \kappa_{\bar{\rho}} \in H^2(L, \mathbb{k}^\times)$ is associated with the projective representation $\bar{\rho} \circ \pi : L \rightarrow \text{PGL}_r(\mathbb{k})$.

The homology group $H_2(G, \mathbb{Z})$ is often called the *Schur multiplier* of G [Weibel 1994]. Since \mathbb{k}^\times is a divisible abelian group, $H^2(G, \mathbb{k}^\times)$ is naturally isomorphic to $\text{Hom}(H_2(G, \mathbb{Z}), \mathbb{k}^\times)$ for any group G . This natural isomorphism allows us to summarize the result of Beyl [1986, Theorem 3.9 and Corollary 3.10] on the Schur multiplier of $\text{SL}_2(\mathbb{Z}_m)$ as the following theorem. A proof of the statement is provided for the sake of completeness. The case for odd integers m was originally proved by Mennicke [1967].

Theorem 2.1. *Let \mathbb{k} be an algebraically closed field of characteristic zero and let m be an integer greater than 1. Then $H^2(\text{SL}_2(\mathbb{Z}_m), \mathbb{k}^\times)$ is isomorphic to \mathbb{Z}_2 when $4 \mid m$ and is trivial otherwise. Moreover, the image of the inflation map $\pi^* : H^2(\text{SL}_2(\mathbb{Z}_m), \mathbb{k}^\times) \rightarrow H^2(\text{SL}_2(\mathbb{Z}_{2m}), \mathbb{k}^\times)$ along the natural reduction map $\pi : \text{SL}_2(\mathbb{Z}_{2m}) \rightarrow \text{SL}_2(\mathbb{Z}_m)$ is always trivial.*

Proof. The first statement is a direct consequence of [Beyl 1986, Theorem 3.9]. For the second statement, it suffices to consider the case $m = 2^a q$ with $a \geq 2$ and q odd. Then, by the Chinese Remainder Theorem, there are split surjections $p : \text{SL}_2(\mathbb{Z}_m) \rightarrow \text{SL}_2(\mathbb{Z}_{2^a})$ and $p' : \text{SL}_2(\mathbb{Z}_{2m}) \rightarrow \text{SL}_2(\mathbb{Z}_{2^{a+1}})$ such that the following diagram of group homomorphisms commutes, where π' is the reduction map:

$$\begin{array}{ccc} \text{SL}_2(\mathbb{Z}_{2m}) & \xrightarrow{p'} & \text{SL}_2(\mathbb{Z}_{2^{a+1}}) \\ \pi \downarrow & & \downarrow \pi' \\ \text{SL}_2(\mathbb{Z}_m) & \xrightarrow{p} & \text{SL}_2(\mathbb{Z}_{2^a}) \end{array}$$

Applying the functor $H^2(-, \mathbb{k}^\times)$ to this commutative diagram, we obtain the following commutative diagram of abelian groups:

$$\begin{array}{ccc} H^2(\text{SL}_2(\mathbb{Z}_{2m}), \mathbb{k}^\times) & \xleftarrow{(p')^*} & H^2(\text{SL}_2(\mathbb{Z}_{2^{a+1}}), \mathbb{k}^\times) \\ \pi^* \uparrow & & \uparrow (\pi')^* \\ H^2(\text{SL}_2(\mathbb{Z}_m), \mathbb{k}^\times) & \xleftarrow{p^*} & H^2(\text{SL}_2(\mathbb{Z}_{2^a}), \mathbb{k}^\times) \end{array}$$

Since p and p' are split surjections, both p^* and $(p')^*$ are injective. Hence, by the first statement, they are isomorphisms. By [Beyl 1986, Corollary 3.10], $(\pi')^*$ is trivial, and so is π^* . \square

Theorem 2.1 is essential to the proof of the following lifting lemma for projective representations of $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.2. *Suppose $\bar{\rho} : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{PGL}_r(\mathbb{k})$ is a projective representation for some positive integer r such that $\ker \bar{\rho}$ is a congruence subgroup of level n . Let $\bar{\rho}_n : \mathrm{SL}_2(\mathbb{Z}_n) \rightarrow \mathrm{PGL}_r(\mathbb{k})$ be the projective representation which satisfies $\bar{\rho} = \bar{\rho}_n \circ \pi_n$, where $\pi_n : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}_n)$ is the reduction modulo n map and κ denotes the associated second cohomology class in $H^2(\mathrm{SL}_2(\mathbb{Z}_n), \mathbb{k}^\times)$. Then:*

- (i) *The class κ is trivial if and only if $\bar{\rho}$ admits a lifting whose kernel is a congruence subgroup of level n .*
- (ii) *If κ is not trivial, then $4 \mid n$ and $\bar{\rho}$ admits a lifting whose kernel is a congruence subgroup of level $2n$.*

In particular, there exists a lifting ρ of $\bar{\rho}$ such that $\ker \rho$ is a congruence subgroup containing $\Gamma(2n)$.

Proof. (i) If κ is trivial, there exists a linear representation $\rho_n : \mathrm{SL}_2(\mathbb{Z}_n) \rightarrow \mathrm{GL}_r(\mathbb{k})$ such that $\eta \circ \rho_n = \bar{\rho}_n$. Then $\rho := \rho_n \circ \pi_n$ is a lifting of $\bar{\rho}$ since

$$\eta \circ \rho = \eta \circ \rho_n \circ \pi_n = \bar{\rho}_n \circ \pi_n = \bar{\rho}.$$

In particular, $\ker \rho$ is a congruence subgroup of level at most n . Obviously, $\ker \rho \leq \ker \bar{\rho}$. Since $\ker \bar{\rho}$ is of level n , the level of $\ker \rho$ is at least n . Therefore, $\ker \rho$ is of level n .

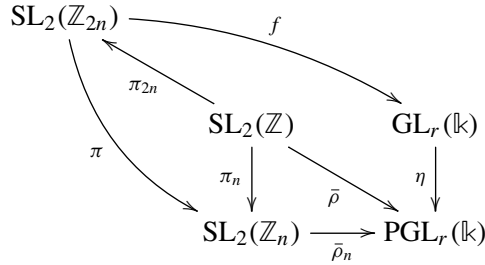
Conversely, assume $\rho : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{GL}_r(\mathbb{k})$ is a representation whose kernel is a congruence subgroup of level n and assume $\bar{\rho} = \eta \circ \rho$. Then ρ factors through $\mathrm{SL}_2(\mathbb{Z}_n)$ and so there exists a linear representation $\rho_n : \mathrm{SL}_2(\mathbb{Z}_n) \rightarrow \mathrm{GL}_r(\mathbb{k})$ such that $\rho = \rho_n \circ \pi_n$. Since

$$\eta \circ \rho_n \circ \pi_n = \eta \circ \rho = \bar{\rho} = \bar{\rho}_n \circ \pi_n,$$

we have $\eta \circ \rho_n = \bar{\rho}_n$. Therefore, ρ_n is a lifting of $\bar{\rho}_n$ and hence κ is trivial.

(ii) Now we consider the case when κ is not trivial. By Theorem 2.1, 4 divides n and $\pi^*(\kappa) \in H^2(\mathrm{SL}_2(\mathbb{Z}_{2n}), \mathbb{k}^\times)$ is trivial, where $\pi : \mathrm{SL}_2(\mathbb{Z}_{2n}) \rightarrow \mathrm{SL}_2(\mathbb{Z}_n)$ is the natural surjection (reduction) map. The composition $\bar{\rho}_n \circ \pi : \mathrm{SL}_2(\mathbb{Z}_{2n}) \rightarrow \mathrm{PGL}_r(\mathbb{k})$ defines a projective representation of $\mathrm{SL}_2(\mathbb{Z}_{2n})$, and its associated class in $H^2(\mathrm{SL}_2(\mathbb{Z}_{2n}), \mathbb{k}^\times)$ is $\pi^*(\kappa)$. Since $\pi^*(\kappa)$ is trivial, $\bar{\rho}_n \circ \pi$ can be lifted to a linear representation $f : \mathrm{SL}_2(\mathbb{Z}_{2n}) \rightarrow \mathrm{GL}_r(\mathbb{k})$, i.e., $\eta \circ f = \bar{\rho}_n \circ \pi$. Thus, we have the following

commutative diagram:



The commutativity of the upper quadrangle is given by

$$\eta \circ f \circ \pi_{2n} = \bar{\rho}_n \circ \pi \circ \pi_{2n} = \bar{\rho}_n \circ \pi_n = \bar{\rho}.$$

Set $\rho = f \circ \pi_{2n}$. Then $\eta \circ \rho = \bar{\rho}$ and so $\Gamma(2n) \leq \ker \rho$. Suppose $\Gamma(m) \leq \ker \rho$ for some positive integer $m < 2n$ and suppose $m \mid 2n$. Then $\Gamma(m) \leq \ker \rho \leq \ker \bar{\rho}$. Since $\ker \bar{\rho}$ is of level n , we have that $n \mid m$. Thus, $m = n$, and hence $\ker \rho$ is a congruence subgroup of level n . It follows from (i) that κ is trivial, a contradiction. Therefore, $\ker \rho$ is of level $2n$. \square

Now we can prove the following lifting theorem for projective representations of $\mathrm{SL}_2(\mathbb{Z})$ with congruence kernels.

Theorem 2.3. *Suppose $\bar{\rho} : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{PGL}_r(\mathbb{k})$ is a projective representation for some positive integer r such that $\ker \bar{\rho}$ is a congruence subgroup of level n . Then the kernel of any lifting of $\bar{\rho}$ is a congruence subgroup of level m where $n \mid m \mid 12n$.*

Proof. By Lemma 2.2, $\bar{\rho}$ admits a lifting ξ such that $\ker \xi$ is congruence subgroup containing $\Gamma(2n)$. Let ρ be a lifting of $\bar{\rho}$. By Section 1.2, $\rho = \xi_x \cong \chi_x \otimes \xi$ for some 12-th root of unity $x \in \mathbb{k}$. Note that $\mathrm{SL}_2(\mathbb{Z}) / \mathrm{SL}_2(\mathbb{Z})' \cong \mathbb{Z}_{12}$ and $\Gamma(12) \leq \mathrm{SL}_2(\mathbb{Z})'$; see for example [Beyl 1986, Lemma 1.13]. Therefore, $\Gamma(12) \leq \ker \chi_x$ and hence

$$\ker(\chi_x \otimes \xi) \supseteq \mathrm{SL}_2(\mathbb{Z})' \cap \Gamma(2n) \supseteq \Gamma(12) \cap \Gamma(2n) \supseteq \Gamma(12n).$$

Therefore, ρ has a congruence kernel containing $\Gamma(12n)$ and so $m \mid 12n$. Since $\Gamma(m) \leq \ker \rho \leq \ker \bar{\rho}$ and $\ker \bar{\rho}$ is of level n , we have $n \mid m$. \square

A consequence of Theorem 2.3 is a proof for the statements (i) and (ii) of Theorem II.

Proof of Theorem II (i) and (ii). By [Ng and Schauenburg 2010, Theorem 6.8], the projective modular representation $\bar{\rho}_{\mathcal{A}}$ of a modular category \mathcal{A} over \mathbb{k} has a congruence kernel of level N where N is the order of the T -matrix of \mathcal{A} . It follows immediately from Theorem 2.3 that every modular representation ρ has a congruence kernel of level n where $N \mid n \mid 12N$. By Lemma A.1, $\mathrm{ord}(\rho(t)) = n$.

Now the statement Theorem II (ii) follows directly from [Ng and Schauenburg 2010, Theorem 7.1]. □

The congruence property, Theorem II (i) and (ii), is essential to the proof of Theorem I and to the Galois symmetry of modular categories in Sections 4 and 5.

Definition 2.4. Let \mathcal{A} be a modular category over \mathbb{k} with $\text{FSexp}(\mathcal{A}) = N$.

- (i) By virtue of Theorem II (i), a modular representation ρ of \mathcal{A} is said to be of level n if $\text{ord}(\rho(t)) = n$.
- (ii) The projective modular representation $\bar{\rho}_{\mathcal{A}}$ of \mathcal{A} factors through a projective representation $\bar{\rho}_{\mathcal{A},N}$ of $\text{SL}_2(\mathbb{Z}_N)$. We denote by $\kappa_{\mathcal{A}}$ the cohomology class in $H^2(\text{SL}_2(\mathbb{Z}_N), \mathbb{k}^\times)$ associated with $\bar{\rho}_{\mathcal{A},N}$.

By Theorem 2.1, the order of $\kappa_{\mathcal{A}}$ is at most 2. If $4 \nmid \text{FSexp}(\mathcal{A})$, then $\kappa_{\mathcal{A}}$ is trivial. However, if $4 \mid \text{FSexp}(\mathcal{A})$, Lemma 2.2 provides the following criterion to decide the order of $\kappa_{\mathcal{A}}$.

Corollary 2.5. *Let \mathcal{A} be a modular category over \mathbb{k} . Suppose $N = \text{FSexp}(\mathcal{A})$ and suppose $\zeta \in \mathbb{k}$ is a 6-th root of the anomaly of \mathcal{A} . Then $\kappa_{\mathcal{A}}$ is trivial if and only if $(x/\zeta)^N = 1$ for some 12-th root of unity $x \in \mathbb{k}$. In this case, $x^3 p_{\mathcal{A}}^+ / \zeta^3 \in \mathbb{Q}_N$. In particular, if $4 \nmid N$, then there exists a 12-th root of unity $x \in \mathbb{k}$ such that*

$$(x/\zeta)^N = 1 \quad \text{and} \quad x^3 p_{\mathcal{A}}^+ / \zeta^3 \in \mathbb{Q}_N.$$

Proof. By (1-7), ζ determines the modular representation ρ^ζ of \mathcal{A} given by

$$\rho^\zeta : \mathfrak{s} \mapsto \frac{\zeta^3}{p_{\mathcal{A}}^+} \tilde{\mathfrak{s}}, \quad \mathfrak{t} \mapsto \frac{1}{\zeta} \tilde{\mathfrak{t}}.$$

By Lemma 2.2 (i) and the last two paragraphs of Section 1.2, $\kappa_{\mathcal{A}}$ is trivial if and only if there exists a 12-th root of unity $x \in \mathbb{k}$ such that ρ_x^ζ is a level N modular representation of \mathcal{A} . By Theorem II (i), this is equivalent to $\text{id} = (x\tilde{\mathfrak{t}}/\zeta)^N$ or $(x/\zeta)^N = 1$. In this case, Theorem II (ii) implies $\zeta^3/(x^3 p_{\mathcal{A}}^+) \tilde{\mathfrak{s}} \in \text{GL}_{\Gamma_{\mathcal{A}}}(\mathbb{Q}_N)$ and hence $\zeta^3/(x^3 p_{\mathcal{A}}^+) \in \mathbb{Q}_N$. The last statement follows immediately from Theorem 2.1. □

The corollary implies some arithmetic relations among the Frobenius–Schur exponent, the global dimension and the anomaly of a modular category. These arithmetic consequences will be discussed in Section 6.

3. Modularity of trace functions for rational vertex operator algebras

In this section we prove that the trace functions of a rational, C_2 -cofinite vertex operator algebra V are modular forms on some congruence subgroup by showing that the representation ρ_V of $\text{SL}_2(\mathbb{Z})$, defined by modular transformation of the

trace functions of V , is a modular representation of \mathcal{C}_V . The congruence subgroup property obtained in Section 2 is then applied to ρ_V to conclude the modularity of the trace functions of V .

Preliminaries. In this subsection we briefly review some basics of vertex operator algebras following [Frenkel et al. 1988; Frenkel et al. 1993; Dong et al. 1997; 1998a; Lepowsky and Li 2004; Zhu 1996].

Let $V = (V, Y, \mathbb{1}, \omega)$ be a vertex operator algebra. Then V is C_2 -cofinite if the subspace $C_2(V)$ of V spanned by all elements of type $a_{-2}b$ for $a, b \in V$ has finite codimension in V . Recall from [Dong et al. 1998a] that V is rational if any admissible module is completely reducible. The component operator $L(n)$ of $Y(\omega, z) = \sum_{n \in \mathbb{Z}} L(n)z^{-n-2}$ will be used frequently. It is proved in [Dong et al. 1998a] that if V is rational then V has only finitely many irreducible admissible modules M^0, \dots, M^p up to isomorphism and there exist $\lambda_i \in \mathbb{C}$ for $i = 0, \dots, p$ such that

$$M^i = \bigoplus_{n=0}^{\infty} M_{\lambda_i+n}^i$$

where $M_{\lambda_i}^i \neq 0$ and $L(0)|_{M_{\lambda_i+n}^i} = \lambda_i + n$ for any $n \in \mathbb{Z}$. Moreover, if V is also assumed to be C_2 -cofinite, then λ_i and the central charge c of V are rational numbers (see [Dong et al. 2000]). In this paper we always assume that V is simple and we take M^0 to be V .

Another important concept is the contragredient module. Let $M = \bigoplus_{\lambda \in \mathbb{C}} M_{\lambda}$ be a V -module. Let $M' = \bigoplus_{\lambda \in \mathbb{C}} M_{\lambda}^*$ be the restricted dual of M . It is proved in [Frenkel et al. 1993] that $M' = (M', Y')$ is naturally a V -module such that

$$\langle Y'(a, z)u', v \rangle = \langle u', Y(e^{zL(1)}(-z^{-2})^{L(0)}a, z^{-1})v \rangle,$$

for $a \in V, u' \in M'$ and $v \in M$, and that $(M')' \simeq M$. Moreover, if M is irreducible, so is M' . A V -module M is said to be self-dual if M and M' are isomorphic. In this paper, we'll always assume that the vertex operator algebra V satisfies the following assumptions:

(V1) $V = \bigoplus_{n \geq 0} V_n$ with $\dim V_0 = 1$ is simple and self-dual.

(V2) V is C_2 -cofinite and rational.

The assumption (V2) is equivalent to the regularity [Dong et al. 1997]. That is, any weak module is completely reducible.

We now recall the notion of intertwining operators and fusion rules from [Frenkel et al. 1993]. Let $W^i = (W^i, Y_{W^i})$ for $i = 1, 2, 3$ be weak V -modules. Then an intertwining operator $\mathcal{Y}(\cdot, z)$ of type $\begin{pmatrix} W^3 \\ W^1 W^2 \end{pmatrix}$ is a linear map

$$\mathcal{Y}(\cdot, z) : W^1 \rightarrow \text{Hom}(W^2, W^3)\{z\}, \quad v^1 \mapsto \mathcal{Y}(v^1, z) = \sum_{n \in \mathbb{C}} v_n^1 z^{-n-1}$$

satisfying the following conditions:

- (i) For any $v^1 \in W^1$, $v^2 \in W^2$ and $\lambda \in \mathbb{C}$, we have $v^1_{n+\lambda} v^2 = 0$ for $n \in \mathbb{Z}$ sufficiently large.
- (ii) For any $a \in V$, $v^1 \in W^1$, we have

$$\begin{aligned} z_0^{-1} \delta\left(\frac{z_1 - z_2}{z_0}\right) Y_{W^3}(a, z_1) \mathcal{Y}(v^1, z_2) - z_0^{-1} \delta\left(\frac{z_1 - z_2}{-z_0}\right) \mathcal{Y}(v^1, z_2) Y_{W^2}(a, z_1) \\ = z_2^{-1} \delta\left(\frac{z_1 - z_0}{z_2}\right) \mathcal{Y}(Y_{W^1}(a, z_0) v^1, z_2). \end{aligned}$$

- (iii) For $v^1 \in W^1$, we have $\frac{d}{dz} \mathcal{Y}(v^1, z) = \mathcal{Y}(L(-1)v^1, z)$.

The sum in the definition of intertwining operator in [Frenkel et al. 1993] is over rational numbers. For a rational vertex operator algebra, this is true. In general, the sum should be over complex numbers. All of the intertwining operators of type $\binom{W^3}{W^1 W^2}$ form a vector space denoted by $I_V\binom{W^3}{W^1 W^2}$. The dimension of $I_V\binom{W^3}{W^1 W^2}$ is called the fusion rule of type $\binom{W^3}{W^1 W^2}$ for V , which is denoted by $N_{W^1, W^2}^{W^3}$.

The following properties of the fusion rule are well-known (see [Frenkel et al. 1993]).

Proposition 3.1. *Let V be a vertex operator algebra, and let M^i, M^j, M^k be three irreducible V -modules. Then:*

- (i) $N_{j,k}^i = N_{j,i^*}^{k^*}$, where we use W^{i^*} to denote $(W^i)'$ and where $N_{j,k}^i = N_{M^j, M^k}^{M^i}$.
- (ii) $N_{j,k}^i = N_{k,j}^i$.

Let M^1 and M^2 be two V -modules. A tensor product for the ordered pair (M^1, M^2) is a pair $(M, F(\cdot, z))$, which consists of a V -module M and an intertwining operator $F(\cdot, z)$ of type $\binom{M}{M^1 M^2}$, such that the following universal property holds: for any V -module X and any intertwining operator $I(\cdot, z)$ of type $\binom{X}{M^1 M^2}$, there exists a unique V -homomorphism ϕ from M to X such that $I(\cdot, z) = \phi \circ F(\cdot, z)$. Note that if there is a tensor product, then it is unique by the universal mapping property. In this case we will denote it by $M^1 \boxtimes M^2$.

In a series of papers [Huang and Lepowsky 1995a; 1995b; 1995c; Huang 1995; 2008a; 2008b], the tensor product \boxtimes of the modules for a vertex operator algebra V has been defined and studied extensively. We have the following result (see [Abe et al. 2004, Corollary 10] and [Huang and Lepowsky 1995a, Proposition 4.13]).

Theorem 3.2. *Let V be a rational and C_2 -cofinite vertex operator algebra, and let M^i, M^j, M^k be any three irreducible modules of V . Then:*

- (i) *The fusion rules $N_{i,j}^k$ are finite.*
- (ii) *The tensor product $M^i \boxtimes M^j$ of M^i and M^j exists and is equal to $\sum_k N_{i,j}^k M^k$.*

We finally review some facts about the modular transformation of trace functions of irreducible modules of a vertex operator algebra from [Zhu 1996]. Let V be a rational and C_2 -cofinite vertex operator algebra, and let M^0, \dots, M^p be the irreducible V -modules as before. There is another VOA structure on V , given by $(V, Y[\cdot, z], \mathbb{1}, \omega - c/24)$ and introduced in [Zhu 1996]. In particular,

$$V = \bigoplus_{n \geq 0} V_{[n]}.$$

We will write $wt[v] = n$ if $v \in V_{[n]}$. For each $v \in V_n$, we denote v_{n-1} by $o(v)$ and extend to V linearly. Recall that $M^i = \bigoplus_{n=0}^\infty M_{\lambda_i+n}^i$. For $v \in V$ we set

$$Z_i(v, q) = \text{tr}_{M^i} o(v)q^{L(0)-c/24} = \sum_{n \geq 0} (\text{tr}_{M_{\lambda_i+n}^i} o(v))q^{\lambda_i+n-c/24},$$

which is a formal power series in variable q . The constant c here is the central charge of V , and $Z_i(\mathbb{1}, q)$ is sometimes called the q -character of M^i . Then $Z_i(v, q)$ converges to a holomorphic function in $0 < |q| < 1$ [Zhu 1996]. As usual we let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid \text{im } \tau > 0\}$ and $q = e^{2\pi i \tau}$ with $\tau \in \mathfrak{h}$. We also denote the holomorphic function $Z_i(v, q)$ by $Z_i(v, \tau)$ when we discuss modular transformations of these functions.

The full modular group $SL_2(\mathbb{Z})$ acts on \mathfrak{h} by

$$\gamma : \tau \mapsto \frac{a\tau + b}{c\tau + d}, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}).$$

The following theorem was established in [Zhu 1996].

Theorem 3.3. *Let V be a rational and C_2 -cofinite vertex operator algebra, and let M^0, \dots, M^p be the irreducible V -modules. Then for any $\gamma \in SL_2(\mathbb{Z})$ there exists a $\rho_V(\gamma) = [\gamma_{ij}]_{i,j=0,\dots,p} \in GL_{p+1}(\mathbb{C})$ such that, for any $0 \leq i \leq p$ and $v \in V_{[n]}$,*

$$Z_i(v, \gamma\tau) = (c\tau + d)^n \sum_{j=0}^p \gamma_{ij} Z_j(v, \tau).$$

Theorem 3.3, in fact, gives a group homomorphism $\rho_V : SL_2(\mathbb{Z}) \rightarrow GL_{p+1}(\mathbb{C})$. We call $\rho_V(\gamma)$ the genus one modular matrices. In particular,

$$S = \rho_V \left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \quad \text{and} \quad T = \rho_V \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right).$$

are respectively called the *genus one* S - and T -matrices of V . It is immediate to see that $T_{jk} = \delta_{jk} e^{2\pi i(\lambda_j - c/24)}$.

One of our main goals is to show that the kernel of ρ_V is a congruence subgroup.

We need the following results on the Verlinde formula [1988] from [Huang 2008a; 2008b] (also see [Moore and Seiberg 1990]).

Theorem 3.4. *Let V be a vertex operator algebra satisfying (V1) and (V2). Then the genus one S -matrix of V defined above has the following properties:*

- (i) S is symmetric and $S^2 = C$, where $C_{ij} = \delta_{ij^*}$. In particular, C has order at most 2 and is also symmetric.
- (ii) $S_{ij}^{-1} = S_{i^*j} = S_{ij^*}$.
- (iii) (Verlinde formula) For any $i, j, k \in \{0, \dots, p\}$,

$$N_{i,j}^k = \sum_{q=0}^p \frac{S_{iq} S_{jq} S_{k^*q}}{S_{0q}}$$

Unitarity of S . In this subsection, we will prove that the genus one S -matrix of V defined on page 2137 is unitary and consequences of this fact. Our approach is slightly different from that given in [Etingof et al. 2005] for the unitarity of a normalized S -matrix of a modular category. Recall that $S^2 = C$. In fact, this equality holds for any symmetric matrix satisfying the Verlinde formula as follows:

Lemma 3.5. *Let \mathcal{C} be a fusion category over \mathbb{C} with commutative Grothendieck ring. Suppose A is a complex symmetric matrix indexed by $\Pi_{\mathcal{C}}$ such that $A_{0r} \neq 0$ for all $r \in \Pi_{\mathcal{C}}$ and suppose A satisfies the Verlinde formula in the sense that*

$$N_{ij}^k = \sum_{r \in \Pi_{\mathcal{C}}} \frac{A_{ir} A_{jr} A_{k^*r}}{A_{0r}} \tag{3-1}$$

for all $i, j, k \in \Pi_{\mathcal{C}}$, where N_{ij}^k is the fusion rule of \mathcal{C} . Then we have $A_{0r} \in \mathbb{R}$ and $A^2 = C$, and we have that A is unitary, where $C_{ij} = \delta_{ij^*}$ for $i, j \in \Pi_{\mathcal{C}}$.

Proof. By the Verlinde formula (3-1), $\sum_{r \in \Pi_{\mathcal{C}}} A_{ir} A_{jr} = N_{ij}^0 = \delta_{ij^*}$ for any $i, j \in \Pi_{\mathcal{C}}$. This implies A is invertible and $(A^{-1})_{ij} = A_{ij^*} = A_{i^*j}$ for $i, j \in \Pi_{\mathcal{C}}$. Hence, we have $A_{i^*j^*} = A_{ij}$ and $A_{0j} = A_{0j^*}$ for all $i, j \in \Pi_{\mathcal{C}}$. Let $\mathcal{K}_0(\mathcal{C})$ be the Grothendieck ring of \mathcal{C} and let $\mathcal{K}_{\mathbb{C}}(\mathcal{C}) = \mathcal{K}_0(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$. Note that $\mathcal{K}_{\mathbb{C}}(\mathcal{C})$ is commutative \mathbb{C} -algebra. For $b \in \Pi_{\mathcal{C}}$, let

$$e_b = A_{0b} \sum_{a \in \Pi_{\mathcal{C}}} A_{ab} a \in \mathcal{K}_{\mathbb{C}}(\mathcal{C}),$$

and $E = \{e_b \mid b \in \Pi_{\mathcal{C}}\}$. Then

$$\begin{aligned} e_a e_b &= A_{0a} A_{0b} \sum_{c,d} A_{ac} A_{bd} c d = A_{0a} A_{0b} \sum_{c,d,r} A_{ac} A_{bd} N_{cd}^r r \\ &= A_{0a} A_{0b} \sum_{c,d,r,z} A_{ac} A_{bd} \frac{A_{cz} A_{dz} A_{r^*z}}{A_{0z}} r = A_{0a} A_{0b} \sum_{r,z} \frac{\delta_{az^*} \delta_{bz^*} A_{r^*z}}{A_{0z}} r \\ &= \delta_{ab} A_{0a}^2 \sum_r \frac{A_{r^*a^*}}{A_{0a^*}} r = \delta_{ab} A_{0a} \sum_r A_{ra} r = \delta_{ab} e_a. \end{aligned}$$

Hence, E is the set of all primitive idempotents of $\mathcal{K}_{\mathbb{C}}(\mathcal{C})$.

The duality permutation defined on $\Pi_{\mathcal{C}}$ can be extended to a sesquilinear linear map \dagger on $\mathcal{K}_{\mathbb{C}}(\mathcal{C})$, i.e.,

$$\left(\sum_{x \in \Pi_{\mathcal{C}}} \alpha_x x\right)^{\dagger} = \sum_{x \in \Pi_{\mathcal{C}}} \bar{\alpha}_x x^*$$

for $\alpha_x \in \mathbb{C}$. Moreover, \dagger is an \mathbb{R} -algebra automorphism of $\mathcal{K}_{\mathbb{C}}(\mathcal{C})$, but \dagger is not \mathbb{C} -linear. In particular, e_b^{\dagger} is in E and hence \dagger defines a permutation on E .

For $x \in \mathcal{K}_{\mathbb{C}}(\mathcal{C})$, denote by $\epsilon(x)$ the coefficient of the unit object 0 in x . Then

$$\epsilon(ab) = N_{ab}^0 = \delta_{ab^*} \quad \text{for } a, b \in \Pi_{\mathcal{C}}.$$

We now define the sesquilinear form (\cdot, \cdot) on $\mathcal{K}_{\mathbb{C}}(\mathcal{C})$ by

$$(x, y) = \epsilon(xy^{\dagger}).$$

Note that $(x, x) > 0$ for $x \neq 0$. Thus

$$0 < (e_b, e_b) = \epsilon(e_b e_b^{\dagger}).$$

Therefore, $e_b^{\dagger} = e_b$ and so $(e_b, e_b) = A_{0b}^2 > 0$ and $A_{0b} A_{ab} = \overline{A_{0b} A_{a^*b}}$ for all $a, b \in \Pi_{\mathcal{C}}$. The former implies $A_{0b} \in \mathbb{R}$ and hence $A_{ab} = A_{a^*b}$ for all $a, b \in \Pi_{\mathcal{C}}$. Therefore, A is unitary. □

The following corollary is an immediate consequence of Lemma 3.5 and the modularity of \mathcal{C}_V presented in Theorem 3.9.

Corollary 3.6. *Let V be a vertex operator algebra satisfying (V1) and (V2). Then the genus one S -matrix of V defined on page 2137 is unitary and satisfies $\bar{S} = SC$.*

The following result can be proved easily by using Corollary 3.6.

Corollary 3.7. *Let V be a vertex operator algebra satisfying (V1) and (V2). For any $u \in V_{[m]}$, $v \in V_{[n]}$, $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z})$ and $\tau_1, \tau_2 \in \mathfrak{h}$ we have*

$$\sum_i Z_i(u, \gamma \tau_1) \overline{Z_i(v, \gamma \tau_2)} = (c\tau_1 + d)^m (c\tau_2 + d)^n \sum_i Z_i(u, \tau_1) \overline{Z_i(v, \tau_2)}.$$

In particular, $\sum_{0 \leq i \leq p} |\chi_i(\tau)|^2$ is invariant under the action of $\text{SL}_2(\mathbb{Z})$.

Proof. Note that T is a diagonal matrix with diagonal entries $e^{2\pi i(\lambda_j - c/24)}$ for $j = 0, \dots, p$ which is clearly a unitary matrix, as λ_j and c are rational numbers. It follows from Corollary 3.6 that the representation ρ is unitary. Set

$$f(\tau_1, \tau_2) = \sum_i Z_i(u, \tau_1) \overline{Z_i(v, \tau_2)}.$$

Then

$$\begin{aligned}
 f(\gamma\tau_1, \gamma\tau_2) &= \sum_i Z_i(u, \gamma\tau_1) \overline{Z_i(v, \gamma\tau_2)} \\
 &= (c\tau_1 + d)^m \overline{(c\tau_2 + d)^n} \sum_{i,j,k} \gamma_{ij} Z_j(u, \tau_1) \overline{\gamma_{ik} Z_k(v, \tau_2)} \\
 &= (c\tau_1 + d)^m \overline{(c\tau_2 + d)^n} \sum_i Z_i(u, \tau_1) \overline{Z_i(v, \tau_2)}. \quad \square
 \end{aligned}$$

Here we use Corollary 3.7 to study the extensions of vertex operator algebras. As before we assume that V is a vertex operator algebra satisfying (V1) and (V2). We also assume that U is an extension of V satisfying (V1) and (V2). Then $U = \sum_i n_i M^i$ as a V -module, where n_i is nonnegative and $n_0 = 1$, as the vacuum vector is unique. The main goal is to determine the possible values of n_i . There have been a lot of discussions on this in the literature using the modular invariance of the characters (see, for example, [Cappelli et al. 1987a; 1987b; Gannon 2005]). It seems that using the characters of irreducible modules is not good enough, as the characters of irreducible modules are not linearly independent in general. In this section we use the conformal blocks instead of the characters to approach the problem.

For $u, v \in V$, we set

$$f_V(u, v, \tau_1, \tau_2) = \sum_{i=0}^p Z_i(u, \tau_1) \overline{Z_i(v, \tau_2)}$$

(see Corollary 3.7). Similarly we can define

$$f_U(u, v, \tau_1, \tau_2) = \sum_M Z_M(u, \tau_1) \overline{Z_M(v, \tau_2)}$$

for $u, v \in U$ where M ranges through the equivalent classes of irreducible U -modules. Since each irreducible U -module M is a direct sum of irreducible V -modules, we see that, for $u, v \in V$,

$$f_U(u, v, \tau_1, \tau_2) = \sum_{i,j=0}^p X_{ij} Z_i(u, \tau_1) \overline{Z_j(v, \tau_2)}$$

for some $X_{ij} \in \mathbb{Z}_+$ and all i, j . If $u = v = \mathbb{1}$ and $\tau_1 = \tau_2 = \tau$, then $f_U(\mathbb{1}, \mathbb{1}, \tau, \tau)$, which is the sum of square norms of the irreducible characters of U , is $SL_2(\mathbb{Z})$ -invariant. We now determine the matrix $X = [X_{ij}]$. It will be clear from our proof below that the $SL_2(\mathbb{Z})$ -invariance of $f_U(\mathbb{1}, \mathbb{1}, \tau, \tau)$ is not good enough to determine the matrix X .

Proposition 3.8. *The matrix X satisfies $X_{00} = 1$ and $X\gamma = \gamma X$, where $\gamma \in SL_2(\mathbb{Z})$, and is identified with the modular transformation matrix $\rho_V(\gamma)$.*

Proof. For any $u \in V_{[m]}$, let

$$\mathbf{Z}(u, \tau) = \begin{bmatrix} Z_0(u, \tau) \\ \vdots \\ Z_p(u, \tau) \end{bmatrix}.$$

Then

$$\mathbf{Z}(u, \gamma\tau) = (c\tau + d)^m \gamma \mathbf{Z}(u, \tau) \quad \text{and} \quad f_U(u, v, \tau_1, \tau_2) = \mathbf{Z}(u, \tau_1)^T X \overline{\mathbf{Z}(v, \tau_2)}.$$

By Corollary 3.7,

$$\begin{aligned} (c\tau_1 + d)^m \overline{(c\tau_2 + d)^n} \mathbf{Z}(u, \tau_1)^T X \overline{\mathbf{Z}(v, \tau_2)} \\ = f_U(u, v, \gamma\tau_1, \gamma\tau_2) = \mathbf{Z}(u, \gamma\tau_1)^T X \overline{\mathbf{Z}(v, \gamma\tau_2)} \\ = (c\tau_1 + d)^m \overline{(c\tau_2 + d)^n} \mathbf{Z}(u, \tau_1)^T \gamma^T X \overline{\gamma \mathbf{Z}(v, \tau_2)}. \end{aligned}$$

This implies that

$$\mathbf{Z}(u, \tau_1)^T X \overline{\mathbf{Z}(v, \tau_2)} = \mathbf{Z}(u, \tau_1)^T \gamma^T X \overline{\gamma \mathbf{Z}(v, \tau_2)}$$

for all u, v . Since γ is unitary, it is enough to show that if $\mathbf{Z}(u, \tau_1)^T A \overline{\mathbf{Z}(v, \tau_2)} = 0$ for all $u, v \in V$ where $A = [a_{ij}]$ is a fixed matrix, then $A = 0$.

Next note the equality $\mathbf{Z}(u, \tau_1)^T A \overline{\mathbf{Z}(v, \tau_2)} = \sum_{ij} a_{ij} Z_i(u, \tau_1) \overline{Z_j(v, \tau_2)}$. For simplicity, set $q_j = e^{2\pi i \tau_j}$ for $j = 1, 2$. Then

$$\begin{aligned} 0 &= \mathbf{Z}(u, \tau_1)^T A \overline{\mathbf{Z}(v, \tau_2)} \\ &= \sum_{i,j} \sum_{m_i, n_j \geq 0} a_{ij} (\text{tr}_{M_{\lambda_i+m_i}^i} o(u) \overline{\text{tr}_{M_{\lambda_j+n_j}^j} o(v)}) q_1^{\lambda_i+m_i-c/24} \overline{q_2^{\lambda_j+n_j-c/24}}. \end{aligned}$$

This implies that each coefficient of $q_1^m \overline{q_2^n}$ for any rational numbers m, n must be zero. We now prove that $a_{ij} = 0$ for all i, j . Fix i and j . Then the coefficient of $q_1^{\lambda_i-c/24} \overline{q_2^{-\lambda_j-c/24}}$ in $\mathbf{Z}(u, \tau_1)^T A \overline{\mathbf{Z}(v, \tau_2)}$ is

$$\sum_{k,l} a_{kl} \text{tr}_{M_{\lambda_k+m_k}^k} o(u) \overline{\text{tr}_{M_{\lambda_l+n_l}^l} o(v)}$$

where $k, l \in \{0, \dots, p\}$ satisfy $m_k + \lambda_k = \lambda_i$, $n_l + \lambda_l = \lambda_j$. Fix $n \geq 0$ such that $n \geq m_k$ and $n \geq n_l$ for all k, l occurring in the summation above. Recall from [Dong et al. 1998b] that there is a finite dimensional semisimple associative algebra $A_n(V)$ such that $M_{m_k+\lambda_k}^k, M_{n_l+\lambda_l}^l$ are the inequivalent simple modules of $A_n(V)$. As a result we can choose $u, v \in V$ such that $o(u) = 1$ on $M_{\lambda_i}^i$ and $o(u) = 0$ on all other $M_{\lambda_k+m_k}^k$, and such that $o(v) = 1$ on $M_{\lambda_j}^j$ and $o(v) = 0$ on all other $M_{\lambda_l+n_l}^l$. Therefore, for this u and v , we have that the coefficient of $q_1^{\lambda_i-c/24} \overline{q_2^{-\lambda_j-c/24}}$ in $\mathbf{Z}(u, \tau_1)^T A \overline{\mathbf{Z}(v, \tau_2)}$ is a nonzero multiple of a_{ij} . This forces $a_{ij} = 0$, completing the proof. \square

The congruence property theorem. Now we come back to the theories of vertex operator algebras. Let V be a rational and C_2 -cofinite vertex operator algebra. For any V -module M , set $\theta_M = e^{2\pi i L(0)}$. The following result from [Huang 2008a, Theorem 4.1] is important in this paper.

Theorem 3.9. *Let V be a vertex operator algebra satisfying (V1) and (V2). Then the V -module category \mathcal{C}_V with the dual M^i (M a V -module), braiding σ which is denoted by \mathcal{C} in [Huang 2008a, p. 877] and twist θ is a modular tensor category over \mathbb{C} .*

Note that $\text{End}_V(M^i) = \mathbb{C}$, $0 \leq i \leq p$. Recall from discussions in Sections 1.1 and 1.3 that the pivotal dimension d_i of the simple V -module is a nonzero real number and the global dimension $\dim \mathcal{C}_V = \sum_{i=0}^p d_i^2$ is at least 1. Let \tilde{s} and \tilde{t} be the S - and T -matrices of \mathcal{C}_V , and $D = \sqrt{\dim \mathcal{C}_V}$ the positive square root of $\dim \mathcal{C}_V$, and c the central charge of \mathcal{C}_V . We fix the normalization $s = \tilde{s}/D$, and simply call s the *normalized S -matrix* of \mathcal{C}_V . We will prove in Theorem 3.10 that s is identical to the genus one S -matrix of V up to a sign.

Theorem 3.10. *Let V be a vertex operator algebra satisfying (V1) and (V2). Then:*

- (i) *The normalized S -matrix s of \mathcal{C}_V and the genus one S -matrix of V are identical up to a sign.*
- (ii) *The representation ρ_V defined by modular transformation of trace functions is a modular representation of \mathcal{C}_V . In particular, $\ker \rho_V$ is a congruence subgroup of level n where n is the order of the genus one T -matrix of V , and ρ_V is \mathbb{Q}_n -rational.*
- (iii) *The central charge c of \mathcal{C}_V is equal to the central charge c of V modulo 4.*

Proof. Let

$$\sigma_{M^i M^j} : M^i \boxtimes M^j \rightarrow M^j \boxtimes M^i$$

be the braiding of \mathcal{C}_V . It is proved in [Huang 2008a] that the pivotal trace of $\sigma_{M^{i^*} M^j} \sigma_{M^j M^{i^*}}$ on $M^j \boxtimes M^{i^*}$ equals S_{ij}/S_{00} . This implies that $S = \lambda s$ where $\lambda = S_{00}/s_{00}$. Using the unitarity of s and S , we conclude that λ is a complex number of norm 1. This forces $\lambda = \pm 1$, which proves the first statement.

It follows from Theorem 3.9 that the T -matrix of \mathcal{C}_V is given by $\tilde{t} = [\delta_{ij} \theta_i]_{i,j=0,\dots,p}$ and $\theta_j = e^{2\pi i \lambda_j}$. Therefore, that genus one T -matrix of V is given by $T = \tilde{t} e^{-2\pi i c/24}$, where c is the central charge of V . In particular, ρ_V is a modular representation of \mathcal{C}_V . The second part of the second statement is an immediate consequence of Theorem II (i) and (ii).

By (i), (1-3) and Theorem 3.4 we see that

$$C = (ST)^3 = \pm (s\tilde{t} e^{-2\pi i c/24})^3 = \pm \frac{p^+}{D} e^{-6\pi i c/24} C,$$

where p^+ is the Gauss sum of \mathcal{C}_V . This implies that $\pm 1 = (p^+/D)e^{-\pi ic/4}$ or $p^+/D = \pm e^{\pi ic/4}$. In particular, $c = c \pmod 4$. □

Theorem I now follows from Theorem 3.10 immediately.

We next discuss two different definitions of dimension of modules of rational and C_2 -cofinite vertex operator algebras given in [Dong et al. 2013; Bakalov and Kirillov 2001]. As before we assume that V is a vertex operator algebra satisfying (V1) and (V2). Recall the following definition of quantum dimension from [Dong et al. 2013]. Let M be a V -module. Set $Z_M(\tau) = \text{ch}_q M = Z_M(\mathbb{1}, \tau)$. The quantum dimension of M over V is defined as

$$\text{qdim}_V M = \lim_{y \rightarrow 0} \frac{Z_M(iy)}{Z_V(iy)}$$

where y is real and positive. It is shown in [Dong et al. 2013] that if V is a vertex operator algebra satisfying (V1) and (V2) with the irreducibles M^i for $i = 0, \dots, p$ such that $\lambda_i > 0$ for $i \neq 0$, then

$$\text{qdim}_V M^i = \frac{S_{i0}}{S_{00}}. \tag{3-2}$$

On the other hand, because V is a vertex operator algebra satisfying (V1) and (V2), the tensor category \mathcal{C}_V of V -modules is modular by Theorem 3.9. The pivotal dimension $d_i = \dim M^i$ of M^i is also defined in the modular tensor category \mathcal{C}_V . We now prove that these two dimensions coincide.

Proposition 3.11. *Let V be a vertex operator algebra satisfying (V1) and (V2), and suppose $\lambda_i > 0$ for $i \neq 0$. Then for any irreducible V -module M^i , we have $\dim M^i = \text{qdim}_V M^i$.*

Proof. Since $\dim M^i = d_i = s_{0i}/s_{00}$, the result follows from Theorem 3.10 and (3-2) immediately. □

The modular transformation property on the conformal blocks has been used extensively in the study of rational vertex operator algebras. The modular transformation property gives an estimation of the growth conditions on the dimensions of homogeneous subspaces as the q -character of an irreducible module is a component of a vector-valued modular function [Knopp and Mason 2003]. The growth condition helps us to show that a rational and C_2 -cofinite vertex operator algebra with central charge less than one is an extension of the Virasoro vertex operator algebra associated to the discrete series [Dong and Zhang 2008], and to characterize vertex operator algebra $L(1/2, 0) \otimes L(1/2, 0)$ [Zhang and Dong 2009; Dong and Jiang 2010]. The congruence subgroup property of the action of the modular group on the conformal block is expected to play an important role in the classification of rational vertex operator algebras. Since the q -character of an irreducible module is a modular function on a congruence subgroup and the sum of the square norms of

the q -characters of the irreducible modules is invariant under $SL_2(\mathbb{Z})$, this gives a lot of information on the dimensions of homogeneous subspaces of vertex operator algebras. For example, one can use these properties to determine the possible characters of the rational vertex operator algebras of central charge 1 [Kiritsis 1989]. This will avoid some difficult work in [Dong and Jiang 2011; 2013] of determining the dimensions of homogenous subspaces of small weights when characterizing certain classes of rational vertex operator algebras of central charge one.

4. Galois symmetry of modular representations

It was conjectured by Coste and Gannon that the representation of $SL_2(\mathbb{Z})$ associated with a RCFT admits a Galois symmetry (see [Coste and Gannon 1999, Conjecture 3; Gannon 2006, Conjecture 6.1.7]). Under certain assumptions, the Galois symmetry of these representations of $SL_2(\mathbb{Z})$ was established by Coste and Gannon [1999] and by Bantay [2003].

In this section, we will prove that such Galois symmetry holds for all modular representations of a modular category as stated in Theorem II (iii) and (iv). It will follow from Theorem 3.10 that this Galois symmetry holds for the representation ρ_V defined by modular transformation of the trace functions of any VOA V satisfying (V1) and (V2).

The Galois symmetry for the canonical modular representation of the Drinfeld center of a spherical fusion category (Lemma 4.2) plays a crucial for the general case, and we will provide its proof in the next section.

Galois action on a normalized S -matrix. Let \mathcal{A} be a modular category over \mathbb{k} with Frobenius–Schur exponent N , and let ρ be a level n modular representation of \mathcal{A} . By virtue of Theorem II (i) and (ii), $N | n | 12N$ and $\rho(SL_2(\mathbb{Z})) \leq GL_\Pi(\mathbb{Q}_n)$, where $\Pi_{\mathcal{A}}$ is simply abbreviated as Π .

A fixed 6-th root ζ of the anomaly of \mathcal{A} determines the modular representation ρ^ζ of \mathcal{A} (see (1-7)). It follows from Section 1.2 that $\rho = \rho_x^\zeta$ for some 12-th root of unity $x \in \mathbb{k}$. Let

$$s = \rho(\mathfrak{s}) \quad \text{and} \quad t = \rho(\mathfrak{t}).$$

Then

$$s = \frac{\zeta^3}{x^3 p_{\mathcal{A}}^+} \tilde{s}, \quad t = \frac{x}{\zeta} \tilde{t} \in GL_\Pi(\mathbb{Q}_n). \tag{4-1}$$

Thus $s^2 = x^6 C = \pm C$, where C is the charge conjugation matrix $[\delta_{ij^*}]_{i,j \in \Pi}$. Set $\text{sgn}(s) = x^6$.

Following [de Boer and Goeree 1991, Appendix B], [Coste and Gannon 1994] or [Etingof et al. 2005, Appendix], for each $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$, there exists a unique

permutation, denoted by $\hat{\sigma}$, on Π such that

$$\sigma\left(\frac{s_{ij}}{s_{0j}}\right) = \frac{s_{i\hat{\sigma}(j)}}{s_{0\hat{\sigma}(j)}} \quad \text{for all } i, j \in \Pi. \tag{4-2}$$

Moreover, there exists a function $\epsilon_\sigma : \Pi \rightarrow \{\pm 1\}$ such that

$$\sigma(s_{ij}) = \epsilon_\sigma(i)s_{\hat{\sigma}(i)j} = \epsilon_\sigma(j)s_{i\hat{\sigma}(j)} \quad \text{for all } i, j \in \Pi. \tag{4-3}$$

Define $G_\sigma \in \text{GL}_\Pi(\mathbb{Z})$ by $(G_\sigma)_{ij} = \epsilon_\sigma(i)\delta_{\hat{\sigma}(i)j}$. Then (4-3) can be rewritten as

$$\sigma(s) = G_\sigma s = s G_\sigma^{-1} \tag{4-4}$$

where $(\sigma(y))_{ij} = \sigma(y_{ij})$ for $y \in \text{GL}_\Pi(\mathbb{Q}_n)$. Since $G_\sigma \in \text{GL}_\Pi(\mathbb{Z})$, this equation implies that the assignment,

$$\text{Aut}(\mathbb{Q}_{ab}) \rightarrow \text{GL}_\Pi(\mathbb{Z}), \quad \sigma \mapsto G_\sigma$$

defines a representation of the group $\text{Aut}(\mathbb{Q}_{ab})$ (see [Coste and Gannon 1994]). Moreover,

$$\sigma^2(s) = G_\sigma s G_\sigma^{-1}, \tag{4-5}$$

$$G_\sigma = \sigma(s)s^{-1} = \sigma(s^{-1})s. \tag{4-6}$$

Note that the permutation $\hat{\sigma}$ on Π depends only on the modular category \mathcal{A} , as $s_{ij}/s_{0j} = \tilde{s}_{ij}/\tilde{s}_{0j}$ in (4-2). However, the matrix G_σ does depend on s , and hence the representation ρ .

Suppose $\tilde{t} = [\delta_{ij}\theta_j]_{i,j \in \Pi}$. Then $t = x\tilde{t}/\zeta$ is a diagonal matrix of order n . If $\sigma|_{\mathbb{Q}_n} = \sigma_a$ for some integer a relatively prime to n , then

$$\sigma(t) = \sigma_a(t) = t^a.$$

By virtue of (4-5), to prove Theorem II (iii), it suffices to show that

$$\sigma^2(t) = G_\sigma t G_\sigma^{-1}. \tag{4-7}$$

We first establish the following simple observation.

Lemma 4.1. *For any integers a, b such that $ab \equiv 1 \pmod{n}$, we have*

$$s^2 = (t^a s t^b s t^a)^2.$$

Proof. It follows from direct computation that

$$s^2 \equiv \begin{bmatrix} 0 & -a \\ b & 0 \end{bmatrix}^2 \equiv (t^a s t^b s t^a)^2 \pmod{n}.$$

By Theorem II (i), ρ factors through $\text{SL}_2(\mathbb{Z}_n)$ and so we obtain the equality. \square

Galois symmetry of Drinfeld doubles. Before we return to prove the Galois symmetry for general modular categories, we need to settle the special case, stated in the following lemma, when \mathcal{A} is the Drinfeld center of a spherical fusion category over \mathbb{k} , and ρ is the canonical modular representation of \mathcal{A} .

Lemma 4.2. *Let \mathcal{C} be a spherical fusion category over \mathbb{k} , and take $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$. Suppose G_σ is the signed permutation matrix determined by the canonical normalization $s = \tilde{s}/\dim \mathcal{C}$ of the S -matrix of the center $Z(\mathcal{C})$, i.e., $G_\sigma = \sigma(s)s^{-1}$. Then the T -matrix \tilde{t} of $Z(\mathcal{C})$ satisfies*

$$\sigma^2(\tilde{t}) = G_\sigma \tilde{t} G_\sigma^{-1}. \tag{4-8}$$

In particular, if $(G_\sigma)_{ij} = \epsilon_\sigma(i)\delta_{\hat{\sigma}(i)j}$ for some sign function ϵ_σ and permutation $\hat{\sigma}$ on $\Pi_{Z(\mathcal{C})}$, then $\sigma^2(\tilde{t}_{ii}) = \tilde{t}_{\hat{\sigma}(i)\hat{\sigma}(i)}$ for all $i \in \Pi_{Z(\mathcal{C})}$. Moreover, for any integers a, b relatively prime to $N = \text{ord}(\tilde{t})$ such that $\sigma|_{\mathbb{Q}_N} = \sigma_a$ and $ab \equiv 1 \pmod{N}$,

$$G_\sigma = \tilde{t}^a s \tilde{t}^b s \tilde{t}^a s^{-1}.$$

The proof of this lemma, which requires the machinery of generalized Frobenius–Schur indicators, will be developed independently in Section 5.

Galois symmetry of general modular categories. Let c be the braiding of the modular category \mathcal{A} . Without loss of generality, we further assume the underlying pivotal category of \mathcal{A} is *strict*. We set

$$\sigma_{X \otimes Y}(V) = (c_{X,V} \otimes Y) \circ (X \otimes c_{V,Y}^{-1})$$

for any $X, Y, V \in \mathcal{A}$. Then $(X \otimes Y, \sigma_{X \otimes Y})$ is a simple object of $Z(\mathcal{A})$ if X, Y are simple objects of \mathcal{A} . Moreover, if V_i denotes a representative of $i \in \Pi$, then

$$\{(V_i \otimes V_j, \sigma_{V_i \otimes V_j}) \mid i, j \in \Pi\}$$

forms a complete set of representatives of simple objects in $Z(\mathcal{A})$ (see [Müger 2003b, Section 7]). Let $(i, j) \in \Pi \times \Pi$ denote the isomorphism class of $(V_i \otimes V_j, \sigma_{V_i \otimes V_j})$ in $Z(\mathcal{A})$. Then we have $\Pi_{Z(\mathcal{A})} = \Pi \times \Pi$ and the isomorphism class of the unit object of $Z(\mathcal{A})$ is $(0, 0) \in \Pi_{Z(\mathcal{A})}$.

Let \tilde{s} and $\tilde{t} = [\delta_{ij}\theta_i]_{i,j \in \Pi}$ be the S - and T -matrices of \mathcal{A} respectively. Then the S - and T -matrices of the center $Z(\mathcal{A})$, denoted by \tilde{s} and \tilde{t} respectively, are indexed by $\Pi \times \Pi$. By [Ng and Schauenburg 2010, Section 6],

$$\tilde{s}_{ij,kl} = \tilde{s}_{ik}\tilde{s}_{jl}^*, \quad \tilde{t}_{ij,kl} = \delta_{ik}\delta_{jl} \frac{\theta_i}{\theta_j}.$$

Thus $\text{FSexp}(\mathcal{A}) = \text{ord}(\tilde{t}) = \text{ord}(\tilde{t}) = N$.

Proof of Theorem II (iii) and (iv). The canonical normalization s of \tilde{s} is

$$s_{ij,kl} = \frac{1}{\dim \mathcal{A}} \tilde{s}_{ik} \tilde{s}_{jl}^* = \text{sgn}(s) s_{ik} s_{jl}^*,$$

where $\text{sgn}(s) = \pm 1$ is given by $s^2 = \text{sgn}(s)C$ (see (4-1)). Moreover, $s \in \text{GL}_{\Pi \times \Pi}(\mathbb{Q}_N)$.

For $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$, we have

$$\sigma(s_{ij,kl}) = \text{sgn}(s) \epsilon_\sigma(i) \epsilon_\sigma(j) s_{\hat{\sigma}(i)k} s_{\hat{\sigma}(j)l}^* = \epsilon_\sigma(i) \epsilon_\sigma(j) s_{\hat{\sigma}(i)\hat{\sigma}(j),kl} = \epsilon_\sigma(i, j) s_{\hat{\sigma}(i,j),kl},$$

where ϵ_σ and $\hat{\sigma}$ are respectively the associated sign function and permutation on $\Pi \times \Pi$. Thus,

$$\epsilon_\sigma(i, j) = \epsilon_\sigma(i) \epsilon_\sigma(j), \quad \hat{\sigma}(i, j) = (\hat{\sigma}(i), \hat{\sigma}(j))$$

and so

$$(G_\sigma)_{ij,kl} = \epsilon_\sigma(i) \epsilon_\sigma(j) \delta_{\hat{\sigma}(i)k} \delta_{\hat{\sigma}(j)l}$$

where G_σ is the associated signed permutation matrix of σ on s . By Lemma 4.2, we find

$$\sigma^2 \left(\frac{\theta_i}{\theta_j} \right) = \sigma^2(\tilde{t}_{ij,ij}) = \tilde{t}_{\hat{\sigma}(i,j),\hat{\sigma}(i,j)} = \tilde{t}_{\hat{\sigma}(i)\hat{\sigma}(j),\hat{\sigma}(i)\hat{\sigma}(j)} = \frac{\theta_{\hat{\sigma}(i)}}{\theta_{\hat{\sigma}(j)}}$$

for all $i, j \in \Pi$. Since $\theta_0 = 1$,

$$\frac{\theta_{\hat{\sigma}(i)}}{\sigma^2(\theta_i)} = \frac{\theta_{\hat{\sigma}(0)}}{\sigma^2(\theta_0)} = \theta_{\hat{\sigma}(0)}$$

for all $i \in \Pi$. By (4-1), $t = \tilde{\zeta}^{-1} \tilde{t}$ where $\tilde{\zeta} = \zeta/x$. Then

$$t_{\hat{\sigma}(i)\hat{\sigma}(i)} = \frac{\theta_{\hat{\sigma}(i)}}{\tilde{\zeta}} = \frac{\sigma^2(\theta_i) \theta_{\hat{\sigma}(0)}}{\tilde{\zeta}} = \sigma^2(t_{ii}) \beta \tag{4-9}$$

for all $i \in \Pi$, where $\beta = t_{\hat{\sigma}(0)\hat{\sigma}(0)} \cdot \sigma^2(\tilde{\zeta}) \in \mathbb{k}^\times$. Suppose $\sigma|_{\mathbb{Q}_n} = \sigma_a$ for some integer a relatively prime to n . Then (4-9) is equivalent to the equalities

$$G_\sigma t G_\sigma^{-1} = \beta t^{a^2} \quad \text{or} \quad G_\sigma^{-1} t^{a^2} G_\sigma = \beta^{-1} t. \tag{4-10}$$

Now it suffices to show that $\beta = 1$.

Apply σ^2 to the equation $(s^{-1}t)^3 = \text{id}$. It follows from (4-10) that

$$\text{id} = G_\sigma s^{-1} G_\sigma^{-1} t^{a^2} G_\sigma s^{-1} G_\sigma^{-1} t^{a^2} G_\sigma s^{-1} G_\sigma^{-1} t^{a^2} = \beta^{-2} (G_\sigma s^{-1} t s^{-1} t s^{-1} G_\sigma^{-1} t^{a^2}).$$

This implies

$$\text{id} = \beta^{-2} (s^{-1} t s^{-1} t s^{-1} G_\sigma^{-1} t^{a^2} G_\sigma) = \beta^{-3} (s^{-1} t s^{-1} t s^{-1} t) = \beta^{-3} \text{id}.$$

Therefore, $\beta^3 = 1$.

Apply σ^{-1} to the equality $sts = t^{-1}st^{-1}$. Since $\sigma^{-1}|_{\mathbb{Q}_n} = \sigma_b$ where b is an inverse of a modulo n , we have

$$G_\sigma^{-1}st^b s G_\sigma = t^{-b} s G_\sigma t^{-b} \quad \text{or} \quad st^b s = G_\sigma t^{-b} s G_\sigma t^{-b} G_\sigma^{-1}.$$

This implies

$$\begin{aligned} G_\sigma^{-1}t^a st^b st^a G_\sigma &= G_\sigma^{-1}t^a G_\sigma t^{-b} s G_\sigma t^{-b} G_\sigma^{-1}t^a G_\sigma \\ &= \sigma^{-1}(G_\sigma^{-1}t^{a^2} G_\sigma)t^{-b} s G_\sigma t^{-b} \sigma^{-1}(G_\sigma^{-1}t^{a^2} G_\sigma) \\ &= \sigma^{-1}(\beta^{-1})t^b t^{-b} s G_\sigma t^{-b} \sigma^{-1}(\beta^{-1})t^b \\ &= \sigma^{-1}(\beta^{-2})s G_\sigma. \end{aligned}$$

Therefore,

$$t^a st^b st^a = \sigma^{-1}(\beta^{-2})G_\sigma s. \quad (4-11)$$

Note that

$$(G_\sigma s)^2 = G_\sigma s G_\sigma s = s G_\sigma^{-1} G_\sigma s = s^2.$$

Square both sides of (4-11) and apply Lemma 4.1. We obtain

$$s^2 = \sigma^{-1}(\beta^{-4})s^2.$$

Consequently, $\sigma^{-1}(\beta^{-4}) = 1$ and this is equivalent to $\beta^4 = 1$. Now we can conclude that $\beta = 1$ and so

$$G_\sigma t G_\sigma^{-1} = t^{a^2}.$$

By (4-11), we also have $G_\sigma = t^a st^b st^a s^{-1}$. □

Remark 4.3. For the case $\mathcal{A} = \text{Rep}(D(H))$, where H is a semisimple Hopf algebra, the T -matrix \tilde{t} of \mathcal{A} was proven to satisfy $\sigma^2(\tilde{t}_{ii}) = \tilde{t}_{\hat{\sigma}(i)\hat{\sigma}(i)}$ in [Sommerhäuser and Zhu 2012, Proposition 12.1]. The underlying modular representation of \mathcal{A} , in the context of Theorem II (iii) and (iv), is the canonical modular representation of \mathcal{A} described in Section 1.4.

We can now establish the Galois symmetry of RCFT as a corollary.

Corollary 4.4. *Let V be a vertex operator algebra satisfying (V1) and (V2) with simple V -modules M^0, \dots, M^p . Then the genus one S - and T -matrices of V admit the Galois symmetry: for $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$, there exists a signed permutation matrix $G_\sigma \in \text{GL}_{p+1}(\mathbb{C})$ such that*

$$\sigma(S) = G_\sigma S = S G_\sigma \quad \text{and} \quad \sigma^2(T) = G_\sigma T G_\sigma^{-1}$$

where the associated permutation $\hat{\sigma} \in S_{p+1}$ of G_σ is determined by

$$\sigma\left(\frac{S_{ij}}{S_{0j}}\right) = \frac{S_{i\hat{\sigma}(j)}}{S_{0\hat{\sigma}(j)}} \quad \text{for all } i, j = 0, \dots, p.$$

In particular, $\sigma^2(T_{ii}) = T_{\hat{\sigma}(i)\hat{\sigma}(i)}$. If $n = \text{ord}(T)$ and $\sigma|_{\mathbb{Q}_n} = \sigma_a$ for some integer a relatively prime to n , then

$$G_\sigma = T^a S T^b S T^a S^{-1}$$

where b is an inverse of a modulo n .

Proof. The result is an immediate consequence of Theorem 3.10 and Theorem II (iii) and (iv). □

Remark 4.5. The modular representation ρ factors through a representation given by $\rho_n : \text{SL}_2(\mathbb{Z}_n) \rightarrow \text{GL}_\Pi(\mathbb{k})$. For any integers a, b such that $ab \equiv 1 \pmod{n}$, the matrix

$$\mathfrak{d}_a = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \equiv \mathfrak{t}^a \mathfrak{s} \mathfrak{t}^b \mathfrak{s} \mathfrak{t}^a \mathfrak{s}^{-1} \pmod{n}$$

is uniquely determined in $\text{SL}_2(\mathbb{Z}_n)$ by the coset $a + n\mathbb{Z}$ of \mathbb{Z} . Moreover, the assignment $u : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \text{SL}_2(\mathbb{Z}_n)$, $\sigma_a \mapsto \mathfrak{d}_a$, defines a group monomorphism. Theorem II (iv) implies that the representation $\phi_\rho : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \text{GL}_\Pi(\mathbb{Z})$, $\sigma \mapsto G_\sigma$, associated with ρ , also factors through ρ_n , satisfying the following commutative diagram:

$$\begin{array}{ccc} \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) & \xrightarrow{\phi_\rho} & \text{GL}_\Pi(\mathbb{k}) \\ u \downarrow & \nearrow \rho_n & \uparrow \rho \\ \text{SL}_2(\mathbb{Z}_n) & \xleftarrow{\pi_n} & \text{SL}_2(\mathbb{Z}) \end{array}$$

The Galois symmetry enjoyed by the T -matrix of the Drinfeld center of a spherical fusion category (Lemma 4.2) does not hold for a general modular category, as demonstrated in the following example.

Example 4.6. Consider the Fibonacci modular category \mathcal{A} over \mathbb{C} which has only one isomorphism class of non-unit simple objects. We abbreviate this non-unit class by 1 (see [Rowell et al. 2009, Section 5.3.2]). Thus, $\Pi_{\mathcal{A}} = \{0, 1\}$. The S - and T -matrices are given by

$$\tilde{s} = \begin{bmatrix} 1 & \varphi \\ \varphi & -1 \end{bmatrix}, \quad \tilde{t} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{4\pi i}{5}} \end{bmatrix}.$$

where $\varphi = (1 + \sqrt{5})/2$. The central charge is $\mathfrak{c} = 14/5$ and the global dimension is $\dim \mathcal{A} = 2 + \varphi$. Therefore, $\alpha = e^{7\pi i/5}$ is the anomaly of \mathcal{A} and $\zeta = e^{7\pi i/30}$ is a 6-th root of α (see (1-9)). Thus

$$s = \rho^\zeta(\mathfrak{s}) = \frac{1}{\sqrt{2 + \varphi}} \tilde{s}, \quad t = \rho^\zeta(\mathfrak{t}) = \begin{bmatrix} e^{-\frac{7\pi i}{30}} & 0 \\ 0 & e^{\frac{17\pi i}{30}} \end{bmatrix}$$

and ρ^ζ is a level 60 modular representation of \mathcal{A} by Theorem II. In $\text{Gal}(\mathbb{Q}_{60}/\mathbb{Q})$, the unique nontrivial square is σ_{49} . Since $\sigma_7(\sqrt{5}) = -\sqrt{5}$, we have $\sigma_7(\tilde{s}_{i0}/\tilde{s}_{00}) = \tilde{s}_{i1}/\tilde{s}_{01}$. Therefore, $\hat{\sigma}_7$ is the transposition $(0, 1)$ on $\Pi_{\mathcal{A}}$, and

$$\sigma_7^2(t) = \sigma_{49}(t) = \begin{bmatrix} e^{\frac{17\pi i}{30}} & 0 \\ 0 & e^{-\frac{7\pi i}{30}} \end{bmatrix} = \begin{bmatrix} t_{11} & 0 \\ 0 & t_{00} \end{bmatrix}.$$

However, the Galois symmetry does not hold for \tilde{t} , as

$$\sigma_7^2(\tilde{t}) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{6\pi i}{5}} \end{bmatrix} \neq \begin{bmatrix} \tilde{t}_{11} & 0 \\ 0 & \tilde{t}_{00} \end{bmatrix}.$$

We close this section with the following proposition which provides a necessary and sufficient condition for such Galois symmetry of the T -matrix \tilde{t} of a modular category.

Proposition 4.7. *Suppose \mathcal{A} is a modular category over \mathbb{k} with Frobenius–Schur exponent N and T -matrix $\tilde{t} = [\delta_{ij}\theta_i]_{i,j \in \Pi_{\mathcal{A}}}$. Let $\zeta \in \mathbb{k}$ be a 6-th root of the anomaly $\alpha = p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ of \mathcal{A} . Then, for any $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ and $i \in \Pi_{\mathcal{A}}$,*

$$\frac{\theta_{\hat{\sigma}(i)}}{\sigma^2(\theta_i)} = \theta_{\hat{\sigma}(0)} = \frac{\zeta}{\sigma^2(\zeta)}. \tag{4-12}$$

Moreover, the following statements are equivalent:

- (i) $\theta_{\hat{\sigma}(0)} = 1$ for all $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$.
- (ii) $\sigma^2(\theta_i) = \theta_{\hat{\sigma}(i)}$ for all $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$.
- (iii) $(p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-)^4 = 1$.

Proof. By (1-7), the assignment

$$\rho^\zeta(s) = s = \lambda^{-1}\tilde{s}, \quad \rho^\zeta(t) = t = \zeta^{-1}\tilde{t}$$

defines a modular representation of \mathcal{A} where $\lambda = p_{\mathcal{A}}^+ / \zeta^3$. For $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ and $i \in \Pi_{\mathcal{A}}$, Theorem II (iii) implies that

$$\sigma^2\left(\frac{\theta_i}{\zeta}\right) = \sigma^2(t_{ii}) = t_{\hat{\sigma}(i)\hat{\sigma}(i)} = \frac{\theta_{\hat{\sigma}(i)}}{\zeta}.$$

Thus (4-12) follows, as $\theta_0 = 1$.

By (4-12), the equivalence of (i) and (ii) is obvious. Statement (i) is equivalent to

$$\sigma^2(\zeta) = \zeta \quad \text{for all } \sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}}). \tag{4-13}$$

Since the anomaly α is a root of unity, so is ζ . By Lemma A.2, (4-13) holds if and only if $\zeta^{24} = 1$ or $\alpha^4 = 1$. □

Remark 4.8. For a modular category \mathcal{A} over \mathbb{C} , it follows from (1-9) that the anomaly of \mathcal{A} is a fourth root of unity if and only if its central charge c is an integer modulo 8.

5. Galois symmetry of quantum doubles

In this section, we provide a proof for Lemma 4.2 which is a special case of Theorem II (iii) and (iv), but which is also crucial to the proof of the theorem. We will invoke the machinery of *generalized Frobenius–Schur indicators* for spherical fusion categories introduced in [Ng and Schauenburg 2010].

Generalized Frobenius–Schur indicators. Frobenius–Schur indicators for group representations have been recently generalized to the representations of Hopf algebras [Linchenko and Montgomery 2000] and quasi-Hopf algebras [Mason and Ng 2005; Schauenburg 2004; Ng and Schauenburg 2008]. A version of the second Frobenius–Schur indicator was introduced in conformal field theory [Bantay 1997], and some categorical versions were studied in [Fuchs et al. 1999; Fuchs and Schweigert 2003]. All these different contexts of indicators are specializations of the Frobenius–Schur indicators for pivotal categories introduced in [Ng and Schauenburg 2007b].

The most recent introduction of the equivariant Frobenius–Schur indicators for semisimple Hopf algebras by [Sommerhäuser and Zhu 2012] has motivated the discovery of generalized Frobenius–Schur indicators for pivotal categories [Ng and Schauenburg 2010]. The specialization of these generalized Frobenius–Schur indicators to spherical fusion categories carries a natural action of $SL_2(\mathbb{Z})$. This modular group action has played a crucial role for the congruence subgroup theorem [Ng and Schauenburg 2010, Theorem 6.8] of the projective representation of $SL_2(\mathbb{Z})$ associated with a modular category. These indicators also admit a natural action of $Aut(\mathbb{Q}_{ab})$ which will be employed to prove the Galois symmetry of quantum doubles in this section. For the purpose of this paper, we will only provide relevant details of generalized Frobenius–Schur indicators for our proof to be presented here. The readers are referred to [Ng and Schauenburg 2010] for more details.

Suppose \mathcal{C} is a strict spherical fusion category over \mathbb{k} with Frobenius–Schur exponent N . For any pair (m, l) of integers, $V \in \mathcal{C}$ and $X = (X, \sigma_X) \in Z(\mathcal{C})$, there is a naturally defined \mathbb{k} -linear operator $E_{X,V}^{(m,l)}$ on the finite-dimensional \mathbb{k} -space $\mathcal{C}(X, V^m)$ (see [Ng and Schauenburg 2010, Section 2]). Here, $V^0 = \mathbf{1}$; $V^m = (V^\vee)^{-m}$ if $m < 0$; and V^m is the m -fold tensor product of V if $m > 0$. The (m, l) -th *generalized Frobenius–Schur indicator* for $X \in Z(\mathcal{C})$ and $V \in \mathcal{C}$ is

$$v_{m,l}^X(V) := \text{tr}(E_{X,V}^{(m,l)}) \tag{5-1}$$

where tr denotes the ordinary trace map. In particular, for $m > 0$ and $f \in \mathcal{C}(X, V^m)$, the operator $E_{X,V}^{(m,1)}(f)$ is the following composition:

$$X \xrightarrow{X \otimes \text{db}_{V^\vee}} X \otimes V^\vee \otimes V \xrightarrow{\sigma_X(V^\vee) \otimes V} V^\vee \otimes X \otimes V \xrightarrow{V^\vee \otimes f \otimes V} V^\vee \otimes V^m \otimes V \xrightarrow{\text{ev}_V \otimes V^m} V^m.$$

It can be shown by graphical calculus that, for $m, l \in \mathbb{Z}$ with $m \neq 0$,

$$E_{X,V}^{(m,l)} = (E_{X,V}^{(m,1)})^l \quad \text{and} \quad (E_{X,V}^{(m,1)})^{mN} = \text{id} \tag{5-2}$$

(see [Ng and Schauenburg 2010, Lemmas 2.5 and 2.7]). Hence, for $m \neq 0$, we have

$$\nu_{m,l}^X(V) = \text{tr}((E_{X,V}^{(m,1)})^l). \tag{5-3}$$

Note that $\nu_{m,1}^1(V)$ coincides with the Frobenius–Schur indicator $\nu_m(V)$ of $V \in \mathcal{C}$ introduced in [Ng and Schauenburg 2007b].

Galois group action on generalized Frobenius–Schur indicators. Let $\mathcal{K}(Z(\mathcal{C}))$ denote the Grothendieck ring of $Z(\mathcal{C})$ and let $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C})) = \mathcal{K}(Z(\mathcal{C})) \otimes_{\mathbb{Z}} \mathbb{k}$. For any matrix $y \in \text{GL}_{\Pi}(\mathbb{k})$, we define the linear operator $F(y)$ on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$ by

$$F(y)(j) = \sum_{i \in \Pi} y_{ij} i \quad \text{for all } j \in \Pi,$$

where $\Pi = \Pi_{Z(\mathcal{C})}$. Then $F : \text{GL}_{\Pi}(\mathbb{k}) \rightarrow \text{Aut}_{\mathbb{k}}(\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C})))$ is a group isomorphism. In particular, every representation $\rho : G \rightarrow \text{GL}_{\Pi}(\mathbb{k})$ of a group G can be considered as a G -action on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$ through F . More precisely, for $g \in G$, we define

$$gj = F(\rho(g))(j) \quad \text{for all } j \in \Pi.$$

Let \tilde{s} and \tilde{t} be the S - and T -matrices of $Z(\mathcal{C})$. The $\text{SL}_2(\mathbb{Z})$ -action on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$ associated with the canonical modular representation $\rho_{Z(\mathcal{C})}$ of $Z(\mathcal{C})$ is then given by

$$\mathfrak{s}j = \sum_{i \in \Pi} s_{ij} i \quad \text{and} \quad \mathfrak{t}j = \theta_j j, \tag{5-4}$$

where $\tilde{t} = [\delta_{ij} \theta_j]_{i,j \in \Pi}$ and $s = \tilde{s} / \dim \mathcal{C}$ (see (1-10)). Note that $s \in \text{GL}_{\Pi}(\mathbb{Q}_N)$ by Theorem II (ii), since $N = \text{ord}(\tilde{t})$.

Now we extend the generalized indicator $\nu_{m,l}^X(V)$ linearly via the basis Π to a functional $I_V((m, l), -)$ on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$. Let $V \in \mathcal{C}$ and $(m, l) \in \mathbb{Z}^2$, and let $z = \sum_{i \in \Pi} \alpha_i i \in \mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$ for some $\alpha_i \in \mathbb{k}$. Then we define

$$I_V((m, l), z) = \sum_{i \in \Pi} \alpha_i \nu_{m,l}^{X_i}(V)$$

where X_i denotes an arbitrary object in the isomorphism class i . The $\text{SL}_2(\mathbb{Z})$ -actions on \mathbb{Z}^2 and on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$ are related by these functionals on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$. In

the following theorem, we summarize some results on these generalized indicators relevant to the proof of Lemma 4.2 (see Section 5 of [Ng and Schauenburg 2010]).

Theorem 5.1. *Let \mathcal{C} be a spherical fusion category \mathcal{C} over \mathbb{k} with Frobenius–Schur exponent N . Suppose $z \in \mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$, $\mathbf{X} = (X, \sigma_X) \in Z(\mathcal{C})$, $V \in \mathcal{C}$, $(m, l) \in \mathbb{Z}^2$ and $J = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Then:*

- (i) $v_{m,l}^{\mathbf{X}}(V) \in \mathbb{Q}_N$.
- (ii) $v_{1,0}^{\mathbf{X}}(V) = \dim_{\mathbb{k}} \mathcal{C}(X, V)$.
- (iii) $I_V((m, l)\gamma, z) = I_V((m, l), \gamma^J z)$ for $\gamma \in \text{SL}_2(\mathbb{Z})$, where $\gamma^J = J\gamma J$.

In particular, $\text{Aut}(\mathbb{Q}_{\text{ab}})$ acts on the generalized Frobenius–Schur indicators $v_{m,l}^{\mathbf{X}}(V)$. □

For $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$, the matrix $G_\sigma = \sigma(s)s^{-1}$ is also given by

$$(G_\sigma)_{ij} = \epsilon_\sigma(i)\delta_{\hat{\sigma}(i)j}$$

for some sign function ϵ_σ and permutation $\hat{\sigma}$ on Π (see (4-2), (4-3) and (4-4)). Define $\mathfrak{f}_\sigma = F(G_\sigma)$. Then

$$\mathfrak{f}_\sigma j = \epsilon_\sigma(\hat{\sigma}^{-1}(j))\hat{\sigma}^{-1}(j) \quad \text{for } j \in \Pi. \tag{5-5}$$

Since the assignment $\text{Aut}(\mathbb{Q}_{\text{ab}}) \rightarrow \text{GL}_\Pi(\mathbb{Z})$, $\sigma \mapsto G_\sigma$ is a representation of $\text{Aut}(\mathbb{Q}_{\text{ab}})$,

$$\mathfrak{f}_\sigma \mathfrak{f}_\tau = \mathfrak{f}_{\sigma\tau} \quad \text{for all } \sigma, \tau \in \text{Gal}(\mathbb{Q}_N/\mathbb{Q}).$$

Therefore, by direct computation,

$$\mathfrak{f}_{\sigma^{-1}} j = \mathfrak{f}_\sigma^{-1} j = \epsilon_\sigma(j)\hat{\sigma}(j) \quad \text{for } j \in \Pi.$$

Remark 5.2. Since $s \in \text{GL}_\Pi(\mathbb{Q}_N)$, if $\sigma, \sigma' \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ such that $\sigma|_{\mathbb{Q}_N} = \sigma'|_{\mathbb{Q}_N}$, then

$$G_\sigma = G_{\sigma'} \quad \text{and so} \quad \mathfrak{f}_\sigma = \mathfrak{f}_{\sigma'}.$$

Now we can establish the following lemma which describes a relation between the $\text{Aut}(\mathbb{Q}_{\text{ab}})$ -action on $\mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$ and the $\text{SL}_2(\mathbb{Z})$ -action in terms of the functionals $I_V((m, l), -)$.

Lemma 5.3. *Take $V \in \mathcal{C}$ and let a, l be nonzero integers such that a is relatively prime to lN . Suppose $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ satisfies $\sigma|_{\mathbb{Q}_N} = \sigma_a$. Then, for all $z \in \mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$,*

$$I_V((a, l), z) = I_V((1, 0), \mathfrak{t}^{-al}\mathfrak{f}_\sigma z).$$

Proof. Let X_j be a representative of $j \in \Pi$. By (5-2), (5-3) and Theorem 5.1 (i), for any nonzero integer m , there is a linear operator $E_m = E_{X_j, V}^{(m,1)}$ on a finite-dimensional space such that $(E_m)^{mN} = \text{id}$ and

$$v_{m,k}^{X_j}(V) = \text{tr}(E_m^k) \in \mathbb{Q}_N$$

for all integers k . In particular, the eigenvalues of E_m are $|mN|$ -th roots of unity.

Suppose $\tau \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ such that $\tau|_{\mathbb{Q}_{|mN|}} = \sigma_a$. Then $\tau|_{\mathbb{Q}_N} = \sigma_a = \sigma|_{\mathbb{Q}_N}$. Therefore,

$$\sigma(v_{l,-1}^{X_j}(V)) = \tau(\text{tr}(E_l^{-1})) = \text{tr}(E_l^{-a}) = v_{l,-a}^{X_j}(V) = I_V((l, -a), j) \tag{5-6}$$

and

$$\begin{aligned} \sigma(v_{1,l}^{X_j}(V)) &= \sigma_a(\text{tr}(E_1^l)) = \text{tr}(E_1^{la}) = v_{1,la}^{X_j}(V) \\ &= I_V((1, la), j) = I_V((1, 0)t^{la}, j) = I_V((1, 0), t^{-la}j). \end{aligned} \tag{5-7}$$

Here, the last equality follows from Theorem 5.1 (iii).

On the other hand, by Theorem 5.1 (iii), we have

$$v_{1,l}^{X_j}(V) = I_V((1, l), j) = I_V((l, -1)s^{-1}, j) = I_V((l, -1), sj) = \sum_{i \in \Pi} s_{ij} v_{l,-1}^{X_i}(V).$$

Therefore, (5-6) and Theorem 5.1 (iii) imply

$$\begin{aligned} \sigma(v_{1,l}^{X_j}(V)) &= \sigma\left(\sum_{i \in \Pi} s_{ij} v_{l,-1}^{X_i}(V)\right) = \sum_{i \in \Pi} \epsilon_\sigma(j) s_{i\hat{\sigma}(j)} \sigma(v_{l,-1}^{X_i}(V)) \\ &= \sum_{i \in \Pi} \epsilon_\sigma(j) s_{i\hat{\sigma}(j)} I_V((l, -a), i) = I_V((l, -a), \epsilon_\sigma(j) s \hat{\sigma}(j)) \\ &= I_V((l, -a), s(f_{\sigma^{-1}j})) = I_V((l, -a)s^{-1}, f_{\sigma^{-1}j}) = I_V((a, l), f_{\sigma^{-1}j}). \end{aligned}$$

It follows from (5-7) that, for all $j \in \Pi$,

$$I_V((a, l), f_{\sigma^{-1}j}) = I_V((1, 0), t^{-la}j)$$

and so

$$I_V((a, l), f_{\sigma^{-1}z}) = I_V((1, 0), t^{-la}z)$$

for all $z \in \mathcal{K}_{\mathbb{k}}(Z(\mathcal{C}))$. The assertion follows by replacing z with $f_\sigma z$. □

Remark 5.4. Some related equalities for the representation categories of semi-simple Hopf algebras were obtained in [Sommerhäuser and Zhu 2012, Corollary 12.4] with a similar strategy. Because of the conceptual differences of the definitions of generalized Frobenius–Schur indicators for spherical fusion categories and the counterpart for semisimple Hopf algebras introduced in that paper, their approach generally cannot be adapted in fusion categories.

Proof of Lemma 4.2. Let $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ and let $\sigma|_{\mathbb{Q}_N} = \sigma_a$ for some integer a relatively prime to N . Then $\sigma^{-1}|_{\mathbb{Q}_N} = \sigma_b$ where b is an inverse of a modulo N . By Dirichlet’s theorem on primes in arithmetic progressions, there exists a prime q

such that $q \equiv b \pmod{N}$ and $q \nmid a$. By Lemma 5.3 and Theorem 5.1 (iii), for $j \in \Pi$,

$$\begin{aligned} I_V((1, 0), \mathfrak{t}^{-1} \mathfrak{f}_\sigma \mathfrak{t}^q \mathfrak{f}_{\sigma^{-1}} j) &= I_V((1, 0), \mathfrak{t}^{-aq} \mathfrak{f}_\sigma \mathfrak{t}^q \mathfrak{f}_{\sigma^{-1}} j) = I_V((a, q), \mathfrak{t}^q \mathfrak{f}_{\sigma^{-1}} j) \\ &= I_V((a, q) \mathfrak{t}^{-q}, \mathfrak{f}_{\sigma^{-1}} j) = I_V((a, q - aq), \mathfrak{f}_{\sigma^{-1}} j) \\ &= I_V((1, 0), \mathfrak{t}^{-aq+a^2q} \mathfrak{f}_\sigma \mathfrak{f}_{\sigma^{-1}} j) = I_V((1, 0), \mathfrak{t}^{-1+a} j). \end{aligned} \tag{5-8}$$

Using (5-4) and (5-5), we can compute directly the two sides of (5-8). This implies

$$\theta_j^{-1} \theta_{\hat{\sigma}(j)}^q v_{1,0}^{X_j}(V) = \theta_j^{a-1} v_{1,0}^{X_j}(V)$$

for all $V \in \mathcal{C}$. Take $V = X_j$ to be the underlying \mathcal{C} -object of X_j . We then have $v_{1,0}^{X_j}(X_j) = \dim_{\mathbb{k}} \mathcal{C}(X_j, X_j) \geq 1$. Therefore, we have $\theta_j^{-1} \theta_{\hat{\sigma}(j)}^q = \theta_j^{a-1}$, and hence

$$\theta_{\hat{\sigma}(j)}^q = \theta_j^a \quad \text{or} \quad \theta_{\hat{\sigma}(j)} = \theta_j^{a^2}.$$

This is equivalent to the equality

$$\sigma^2(\tilde{t}) = G_\sigma \tilde{t} G_\sigma^{-1}.$$

Since $\tilde{t} s \tilde{t} s \tilde{t} = s$, we find that

$$\begin{aligned} G_\sigma s &= \sigma(s) = \sigma(\tilde{t} s \tilde{t} s \tilde{t}) = \tilde{t}^a s G_\sigma^{-1} \tilde{t}^a G_\sigma s \tilde{t}^a \\ &= \tilde{t}^a s G_\sigma^{-1} \tilde{t}^{a^2 b} G_\sigma s \tilde{t}^a = \tilde{t}^a s (G_\sigma^{-1} \tilde{t}^{a^2} G_\sigma)^b s \tilde{t}^a = \tilde{t}^a s \tilde{t}^b s \tilde{t}^a. \end{aligned} \tag{5-9}$$

Therefore,

$$G_\sigma = \tilde{t}^a s \tilde{t}^b s \tilde{t}^a s^{-1}. \quad \square$$

6. Anomaly of modular categories

In this section, we apply the congruence property and Galois symmetry of a modular category (Theorem II) to deduce some arithmetic relations among the global dimension, the Frobenius–Schur exponent and the order of the anomaly.

Let \mathcal{A} be a modular category over \mathbb{k} with Frobenius–Schur exponent N . Since $d(V) \in \mathbb{Q}_N$ for $V \in \mathcal{A}$ (see [Ng and Schauenburg 2010, Proposition 5.7]), the anomaly $\alpha = p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ of \mathcal{A} is a root of unity in \mathbb{Q}_N . Therefore, $\alpha^N = 1$ if N is even, and $\alpha^{2N} = 1$ if N is odd.

Let us define $J_{\mathcal{A}} = (-1)^{1+\text{ord } \alpha}$ to record the parity of the order of the anomaly α of \mathcal{A} . Note that $J_{\mathcal{A}}$ is intrinsically defined by \mathcal{A} . It will become clear that $J_{\mathcal{A}}$ is closely related to the Jacobi symbol $\left(\frac{*}{*}\right)$ in number theory. When $4 \nmid N$, the quantity $J_{\mathcal{A}}$ determines whether $\dim \mathcal{A}$ has a square root in \mathbb{Q}_N .

Theorem 6.1. *Let \mathcal{A} be a modular category over \mathbb{k} with Frobenius–Schur exponent N such that $4 \nmid N$. Then $J_{\mathcal{A}} \dim \mathcal{A}$ has a square root in \mathbb{Q}_N and $-J_{\mathcal{A}} \dim \mathcal{A}$ does not have any square root in \mathbb{Q}_N .*

Proof. Let $\zeta \in \mathbb{k}$ be a 6-th root of the anomaly $\alpha = p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ of \mathcal{A} . By Corollary 2.5, there exists a 12-th root of unity $x \in \mathbb{k}$ such that

$$\left(\frac{x}{\zeta}\right)^N = 1 \quad \text{and} \quad \frac{x^3 p_{\mathcal{A}}^+}{\zeta^3} \in \mathbb{Q}_N.$$

Note that $(p_{\mathcal{A}}^+ / \zeta^3)^2 = \dim \mathcal{A}$.

Set $N' = N$ if N is odd and $N' = N/2$ if N is even. In particular, N' is odd. Then $(x/\zeta)^{N'} = \pm 1$ and so

$$\alpha^{N'} = \zeta^{6N'} = x^{6N'} = x^6.$$

By straightforward verification, one can show that $x^6 = J_{\mathcal{A}}$. Therefore,

$$\left(\frac{x^3 p_{\mathcal{A}}^+}{\zeta^3}\right)^2 = x^6 \dim \mathcal{A} = J_{\mathcal{A}} \dim \mathcal{A}.$$

Suppose $-J_{\mathcal{A}} \dim \mathcal{A}$ also has a square root in \mathbb{Q}_N . Since $J_{\mathcal{A}} \dim \mathcal{A}$ has a square root in \mathbb{Q}_N , so does -1 . Therefore, $4 \mid N$, a contradiction. \square

When $\dim \mathcal{A}$ is an odd integer, we will show that $J_{\mathcal{A}} = \left(\frac{-1}{\dim \mathcal{A}}\right)$. Let us fix our convention in the following definition for the remainder of this paper.

Definition 6.2. Let \mathcal{A} be a modular category over \mathbb{k} .

- (i) \mathcal{A} is called *mock integral* if its global dimension $\dim \mathcal{A}$ is an integer.
- (ii) \mathcal{A} is called *integral* if $d(V) \in \mathbb{Z}$ for all $V \in \mathcal{A}$.

Remark 6.3. The standard definition of integral fusion categories is defined in terms of Frobenius–Perron dimensions. Following [Etingof et al. 2005], a fusion category \mathcal{C} is called integral (resp. weakly integral) if $\text{FPdim } V \in \mathbb{Z}$ for all $V \in \mathcal{C}$ (resp. $\text{FPdim } \mathcal{C} \in \mathbb{Z}$). Moreover, any weakly integral spherical fusion category \mathcal{C} satisfies the pseudounitary condition: $\text{FPdim } \mathcal{C} = \dim \mathcal{C}$. Therefore, weakly integral modular categories are obviously mock integral. The Deligne product of the Fibonacci modular category (see [Rowell et al. 2009, Section 5.3.2]) with its Galois conjugate is a mock integral modular category but not weakly integral.

It follows from [Hong and Rowell 2010, Lemma A.1] and [Etingof et al. 2005, Proposition 8.24] that $d(V) \in \mathbb{Z}$ for all objects V in a modular category \mathcal{A} if and only if $\text{FPdim } V \in \mathbb{Z}$ for all $V \in \mathcal{A}$. Therefore, these two definitions of *integral* modular categories are equivalent. A weakly integral modular category can also be characterized by the integrality of $d(V)^2$ as in the following lemma.

Lemma 6.4. *A modular category \mathcal{A} over \mathbb{k} is weakly integral if and only if $d(V)^2$ is an integer for any simple object $V \in \mathcal{A}$.*

Proof. By the modularity of \mathcal{A} , we have that $\text{FPdim } \mathcal{A} = \dim \mathcal{A}/d(U)^2$ for some simple object U . If $d(V)^2 \in \mathbb{Z}$ for all simple objects $V \in \mathcal{A}$, then $\dim \mathcal{A} \in \mathbb{Z}$ and hence $\text{FPdim } \mathcal{A} \in \mathbb{Z}$. Conversely, if $\text{FPdim } \mathcal{A} \in \mathbb{Z}$, then $\text{FPdim } \mathcal{A} = \dim \mathcal{A}$ and $(\text{FPdim } V)^2 \in \mathbb{Z}$ for all simple objects $V \in \mathcal{A}$ by [Etingof et al. 2005, Propositions 8.24 and 8.27]. Since $d(V)^2 \leq (\text{FPdim } V)^2$, the pseudounitariness of \mathcal{A} implies $d(V)^2 = (\text{FPdim } V)^2 \in \mathbb{Z}$. \square

Proposition 6.5. *Let \mathcal{A} be a mock integral modular category over \mathbb{k} with Frobenius–Schur exponent N and odd global dimension $\dim \mathcal{A}$. Then $J_{\mathcal{A}} = \left(\frac{-1}{\dim \mathcal{A}}\right)$. In particular,*

$$J_{\mathcal{A}} = \begin{cases} 1 & \text{if } \dim \mathcal{A} \equiv 1 \pmod{4}, \\ -1 & \text{if } \dim \mathcal{A} \equiv 3 \pmod{4}. \end{cases}$$

Moreover, the square-free part of $\dim \mathcal{A}$ is a divisor of N .

Proof. We may simply assume \mathcal{A} contains a non-unit simple object. By [Etingof 2002, Theorem 5.1], N divides $(\dim \mathcal{A})^3$. In particular, N is odd. Let $\varphi : \mathbb{Q}_N \rightarrow \mathbb{C}$ be any embedding. It follows from the proof of [Etingof et al. 2005, Proposition 2.9] that $\varphi(d_i)$ is real for $i \in \Pi_{\mathcal{A}}$, and so $\varphi(\dim \mathcal{A}) > 1$. We can identify \mathbb{Q}_N with $\varphi(\mathbb{Q}_N)$.

If $\dim \mathcal{A}$ is the square of an integer, then $J_{\mathcal{A}} = 1$ by Theorem 6.1, and we have $\left(\frac{-1}{\dim \mathcal{A}}\right) = 1$. In this case, the last statement is trivial. Suppose $\dim \mathcal{A}$ is not the square of any integer. It follows from Theorem 6.1 that $\mathbb{Q}(\sqrt{J_{\mathcal{A}} \dim \mathcal{A}})$ is a quadratic subfield of \mathbb{Q}_N . Note that $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of \mathbb{Q}_{p^ℓ} for any odd prime p and positive integer ℓ (see [Washington 1997]), where $p^* = \left(\frac{-1}{p}\right)p$, and that $\mathbb{Q}(\sqrt{m}) \neq \mathbb{Q}(\sqrt{m'})$ for any two distinct square-free integers m, m' . Let p_1, \dots, p_k be the distinct prime factors of N . By counting the order 2 elements of $\text{Gal}(\mathbb{Q}_N/\mathbb{Q})$, the quadratic subfields of \mathbb{Q}_N are of the form $\mathbb{Q}(\sqrt{d^*})$ where d is a positive divisor of $p_1 \cdots p_k$ and where $d^* = \left(\frac{-1}{d}\right)d$.

Let a be the square-free part of $\dim \mathcal{A}$. Then we have that $\left(\frac{-1}{\dim \mathcal{A}}\right) = \left(\frac{-1}{a}\right)$ and $\mathbb{Q}(\sqrt{J_{\mathcal{A}} a}) = \mathbb{Q}(\sqrt{J_{\mathcal{A}} \dim \mathcal{A}})$. By the preceding paragraph, $a \mid p_1 \cdots p_k$ and $J_{\mathcal{A}} = \left(\frac{-1}{a}\right)$. \square

Remark 6.6. In [Sommerhäuser and Zhu 2009], integral modular categories with the special Galois property

$$\sigma(\tilde{s}_{ij}) = \tilde{s}_{\hat{\sigma}(i)j} \tag{6-1}$$

were discussed. These conditions are not satisfied by some common modular categories such as the Ising and Fibonacci modular categories. However, for semisimple quasi-Hopf algebras with modular module categories, the first statement of the preceding proposition was proved in [Sommerhäuser and Zhu 2009, Theorem 5.3].

A number of new results appear in the serious revision [Sommerhäuser and Zhu 2013] of [Sommerhäuser and Zhu 2009]. In Theorem 2.6 and Proposition 3.5 of these papers, the same statement was established for integral modular categories

satisfying (6-1) by considering the quadratic subfields of \mathbb{Q}_N but using a different approach.

The following proposition on modular categories is a slight variation of [Coste and Gannon 1999, Proposition 3], and it was essentially proved [loc. cit.] under the assumption of Galois symmetry which has been proved in the previous sections.

Proposition 6.7. *Let \mathcal{A} be a modular category over \mathbb{k} , and let ρ be a modular representation of \mathcal{A} . Set $s = \rho(\mathfrak{s})$, $t = [\delta_{ij}t_i]_{i,j \in \Pi_{\mathcal{A}}} = \rho(t)$, $n = \text{ord}(t)$ and*

$$\mathbb{K}_b = \mathbb{Q}(s_{ib}/s_{0b} \mid i \in \Pi_{\mathcal{A}}) \quad \text{for } b \in \Pi_{\mathcal{A}}.$$

- (i) *Then $\sigma^2(t_b) = t_b$ for $\sigma \in \text{Gal}(\mathbb{Q}_n/\mathbb{K}_b)$.*
- (ii) *If \mathcal{A} is integral, then the anomaly $\alpha = p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ of \mathcal{A} is a 4-th root of unity.*
- (iii) *Let $\mathbb{K} = \mathbb{Q}(s_{ib}/s_{0b} \mid i, b \in \Pi_{\mathcal{A}})$, and let k be the conductor of \mathbb{K} , i.e., the smallest positive integer k such that $\mathbb{K} \subseteq \mathbb{Q}_k$. Then $\text{Gal}(\mathbb{Q}_n/\mathbb{K})$ is an elementary 2-group, and $|\text{Gal}(\mathbb{Q}_n/\mathbb{Q}_k)|$ is a divisor of 8. Moreover, n/k is a divisor of 24, and $\text{gcd}(n/k, k)$ divides 2.*

Proof. (i) For $\sigma \in \text{Gal}(\mathbb{Q}_n/\mathbb{K}_b)$, let ϵ_{σ} be the sign function determined by s (see (4-3)). Suppose $s^2 = \text{sgn}(s)C$ where $\text{sgn}(s) = \pm 1$. Then, by (4-2),

$$\frac{\text{sgn}(s)}{s_{0b}^2} = \sum_{i \in \Pi_{\mathcal{A}}} \frac{s_{ib}s_{ib}^*}{s_{0b}^2} = \sum_{i \in \Pi_{\mathcal{A}}} \left(\frac{s_{ib}}{s_{0b}}\right) \left(\frac{s_{ib}^*}{s_{0b}}\right) = \sum_{i \in \Pi_{\mathcal{A}}} \left(\frac{s_{ib}}{s_{0b}}\right) \left(\frac{s_{i^*b}}{s_{0b}}\right) \in \mathbb{K}_b.$$

Therefore, $s_{0b}^2 \in \mathbb{K}_b$ and so $\sigma(s_{0b}^2) = s_{0b}^2$. Since $\sigma(s_{0b}) = \epsilon_{\sigma}(b)s_{0\hat{\sigma}(b)}$, we have $s_{0\hat{\sigma}(b)} = \epsilon_{\sigma} s_{0b}$ for some sign ϵ . Now, for $i \in \Pi_{\mathcal{A}}$,

$$\frac{s_{ib}}{s_{0b}} = \sigma\left(\frac{s_{ib}}{s_{0b}}\right) = \frac{s_{i\hat{\sigma}(b)}}{s_{0\hat{\sigma}(b)}} = \frac{\epsilon s_{i\hat{\sigma}(b)}}{s_{0b}}.$$

Thus, $s_{ib} = \epsilon s_{i\hat{\sigma}(b)}$ for all $i \in \Pi_{\mathcal{A}}$. If $\hat{\sigma}(b) \neq b$, then the b -th and the $\hat{\sigma}(b)$ -th columns of s are linearly dependent but this contradicts the invertibility of s . Therefore, $\hat{\sigma}(b) = b$ and hence, by Theorem II (iii), $\sigma^2(t_b) = t_{\hat{\sigma}(b)} = t_b$.

(ii) If \mathcal{A} is integral, then $\mathbb{K}_0 = \mathbb{Q}$ and hence $\sigma^2(t_0) = t_0$ for all $\sigma \in \text{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Recall from Section 1.3 that $t_0 = x/\zeta$ for some 6-th root ζ of α and some 12-th root of unity $x \in \mathbb{k}$. By Lemma A.2, x/ζ is a 24-th root of unity. Therefore,

$$\alpha^4 = \zeta^{24} = (\zeta/x)^{24} = 1.$$

(iii) By (i), for $\sigma \in \text{Gal}(\mathbb{Q}_n/\mathbb{K})$, we have $\sigma^2(t_b) = t_b$ for all $b \in \Pi_{\mathcal{A}}$. Since \mathbb{Q}_n is generated by t_b ($b \in \Pi_{\mathcal{A}}$), we have $\sigma^2 = \text{id}$. Therefore, $\text{Gal}(\mathbb{Q}_n/\mathbb{K})$ is an elementary 2-group, and so is $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}_k)$. Thus, for any integer a relatively prime to n such that $a \equiv 1 \pmod{k}$, we have $a^2 \equiv 1 \pmod{n}$. By Lemma A.3, we have that n/k is

a divisor of 24 and that $\gcd(n/k, k) | 2$. Moreover, $|\text{Gal}(\mathbb{Q}_n/\mathbb{Q}_k)| = \phi(n)/\phi(k)$ is a divisor of 8. □

Remark 6.8. The proof of the preceding proposition is a mere adaptation of [Coste and Gannon 1999, Proposition 3]. For integral modular categories satisfying (6-1) (see Remark 6.6), Proposition 6.7 (ii) and (iii) also appear in the final version of [Sommerhäuser and Zhu 2013, Theorems 2.3.2 and 3.4] with similar ideas. The following corollary was also established for factorizable quasi-Hopf algebras in Theorem 4.3 of [Sommerhäuser and Zhu 2009; 2013] with a different approach.

Corollary 6.9. *Let \mathcal{A} be an integral modular category with anomaly $\alpha = p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$. If $\dim \mathcal{A}$ is odd, then $\alpha = \left(\frac{-1}{\dim \mathcal{A}}\right)$.*

Proof. If $\dim \mathcal{A}$ is odd, then so is the Frobenius–Schur exponent N of \mathcal{A} , as $N | (\dim \mathcal{A})^3$. Since $\alpha \in \mathbb{Q}_N$ and $\alpha^4 = 1$, we have $\alpha^2 = 1$. It follows from Proposition 6.5 that

$$\alpha = (-1)^{1+\text{ord} \alpha} = J_{\mathcal{A}} = \left(\frac{-1}{\dim \mathcal{A}}\right). \quad \square$$

The Ising modular category is an example of a weakly integral modular category (see [Rowell et al. 2009, Section 5.3.4]) and its central charge is $\mathbf{c} = 1/2$. Therefore, its anomaly is $e^{\pi i/4}$, an eighth root of unity, and this holds for every weakly integral modular category.

Theorem 6.10. *The anomaly $\alpha = p_{\mathcal{A}}^+ / p_{\mathcal{A}}^-$ of any weakly integral modular category \mathcal{A} is an eighth root of unity.*

Proof. Suppose $\zeta \in \mathbb{k}$ is a 6-th root of the anomaly α of a weakly integral modular category \mathcal{A} . Then $\lambda = p_{\mathcal{A}}^+ / \zeta^3$ is a square root of $\dim \mathcal{A}$. Consider the modular representation ρ^ζ of \mathcal{A} given by

$$\rho^\zeta : \mathfrak{s} \mapsto s := \frac{1}{\lambda} \tilde{s}, \quad \mathfrak{t} \mapsto t := \frac{1}{\zeta} \tilde{t}.$$

Let $\tilde{t} = [\delta_{ij} \theta_i]_{i,j \in \Pi_{\mathcal{A}}}$ be the T -matrix of \mathcal{A} . Since $s_{0i}^2 = d_i^2 / \dim \mathcal{A} \in \mathbb{Q}$, we have, for $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$,

$$s_{0i}^2 = \sigma(s_{0i}^2) = s_{0\hat{\sigma}(i)}^2$$

or $d_i^2 = d_{\hat{\sigma}(i)}^2$ for all $i \in \Pi_{\mathcal{A}}$. By Theorem II (iii),

$$\sigma^2 \left(\sum_{i \in \Pi_{\mathcal{A}}} d_i^2 \frac{\theta_i}{\zeta} \right) = \sum_{i \in \Pi_{\mathcal{A}}} d_i^2 \frac{\theta_{\hat{\sigma}(i)}}{\zeta} = \sum_{i \in \Pi_{\mathcal{A}}} d_{\hat{\sigma}(i)}^2 \frac{\theta_{\hat{\sigma}(i)}}{\zeta} = \sum_{i \in \Pi_{\mathcal{A}}} d_i^2 \frac{\theta_i}{\zeta}.$$

Thus, we have

$$\frac{\sigma^2(p_{\mathcal{A}}^+)}{p_{\mathcal{A}}^+} = \frac{\sigma^2(\zeta)}{\zeta}.$$

Since $\dim \mathcal{A}$ is a positive integer, $\sigma^2(\lambda) = \lambda$ and so

$$\frac{\sigma^2(\zeta^3)}{\zeta^3} = \frac{\sigma^2(p_{\mathcal{A}}^+/\lambda)}{p_{\mathcal{A}}^+/\lambda} = \frac{\sigma^2(p_{\mathcal{A}}^+)}{p_{\mathcal{A}}^+} = \frac{\sigma^2(\zeta)}{\zeta}.$$

Therefore, we find $\sigma^2(\zeta^2)/\zeta^2 = 1$ for all $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$. It follows from Lemma A.2 that $\zeta^{48} = 1$ and so $\alpha^8 = 1$. \square

Corollary 6.9 and the Cauchy theorem for Hopf algebras [Kashina et al. 2006] as well as quasi-Hopf algebras [Ng and Schauenburg 2007a] suggest a more general version of the Cauchy theorem may hold for spherical fusion categories or modular categories over \mathbb{k} . We finish this paper with two equivalent questions.

Question 6.11. Let \mathcal{C} be a spherical fusion category over \mathbb{k} with Frobenius–Schur exponent N . Let \mathcal{O} denote the ring of integers of \mathbb{Q}_N . Must the principal ideals $\mathcal{O}(\dim \mathcal{C})$ and $\mathcal{O}N$ of \mathcal{O} have the same prime ideal factors?

Since $Z(\mathcal{C})$ is a modular category over \mathbb{k} and $(\dim \mathcal{C})^2 = \dim Z(\mathcal{C})$, the preceding question is equivalent to the following:

Question 6.12. Let \mathcal{A} be a modular category over \mathbb{k} with Frobenius–Schur exponent N . Let \mathcal{O} denote the ring of integers of \mathbb{Q}_N . Must the principal ideals $\mathcal{O}(\dim \mathcal{A})$ and $\mathcal{O}N$ of \mathcal{O} have the same prime ideal factors?

By [Etingof 2002], $(\dim \mathcal{A})^3/N \in \mathcal{O}$. Therefore, the prime ideal factors of $\mathcal{O}N$ are a subset of $\mathcal{O} \dim \mathcal{A}$. The converse is only known to be true for the representation categories of semisimple quasi-Hopf algebras, by [Ng and Schauenburg 2007a, Theorem 8.4]. Question 6.11 was originally raised for semisimple Hopf algebras in [Etingof and Gelaki 1999, Question 5.1], which had been solved in [Kashina et al. 2006, Theorem 3.4].

Appendix

The first lemma in this appendix could be known to some experts. An analogous result for $\text{PSL}_2(\mathbb{Z})$ was proved by Wohlfahrt [1964, Theorem 2] (see also Newman’s proof [1972, Theorem VIII.8]). However, we do not see the lemma as an immediate consequence of Wohlfahrt’s theorem for $\text{PSL}_2(\mathbb{Z})$.

Lemma A.1. *Let H be a congruence normal subgroup of $\text{SL}_2(\mathbb{Z})$. Then the level of H is equal to the order of $\mathfrak{t}H$ in $\text{SL}_2(\mathbb{Z})/H$.*

Proof. Let m be the level of H and let $n = \text{ord } \mathfrak{t}H$. Since $\mathfrak{t}^m \in \Gamma(m) \leq H$, we have $\mathfrak{t}^m \in H$ and hence $n \mid m$.

Suppose $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(n)$. Since $ad - bc = 1$, by Dirichlet's theorem, there exists a prime $p \nmid m$ such that $p = d + kc$ for some integer k . Then

$$\mathfrak{t}^{-k} \gamma \mathfrak{t}^k = \begin{bmatrix} a' & b' \\ c & p \end{bmatrix} \in \Gamma(n)$$

for some integers a', b' . In particular,

$$a'p - b'c = 1, \quad p \equiv a' \equiv 1 \pmod{n} \quad \text{and} \quad c \equiv b' \equiv 0 \pmod{n}.$$

Since $p \nmid m$, there exists an integer q such that $pq \equiv 1 \pmod{m}$. Thus we have $pq \equiv 1 \pmod{n}$ and so $q \equiv 1 \pmod{n}$. One can verify directly that

$$\begin{bmatrix} a' & b' \\ c & p \end{bmatrix} \equiv \mathfrak{t}^{b'q} \mathfrak{s}^{-1} \mathfrak{t}^{(-c+1)p} \mathfrak{s} \mathfrak{t}^q \mathfrak{s} \mathfrak{t}^p \pmod{m}.$$

Therefore,

$$\mathfrak{t}^{-k} \gamma \mathfrak{t}^k H = \mathfrak{t}^{b'q} \mathfrak{s}^{-1} \mathfrak{t}^{(-c+1)p} \mathfrak{s} \mathfrak{t}^q \mathfrak{s} \mathfrak{t}^p H = \mathfrak{s}^{-1} \mathfrak{t} \mathfrak{s} \mathfrak{t} \mathfrak{s} H = \mathfrak{s}^{-1} \mathfrak{s} H = H.$$

This implies $\mathfrak{t}^{-k} \gamma \mathfrak{t}^k \in H$, and hence $\gamma \in H$. Therefore, $\Gamma(n) \leq H$ and so $m \mid n$. \square

The following fact should be well-known. We include the proof here for the convenience of the reader.

Lemma A.2. *Let ζ be a root of unity in \mathbb{k} . Then $\sigma^2(\zeta) = \zeta$ for all $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$ if and only if $\zeta^{24} = 1$.*

Proof. Let m be the order of ζ . Then $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U(\mathbb{Z}_m)$. Note that the group $U(\mathbb{Z}_m)$ has exponent at most 2 if and only if $m \mid 24$. Since $\mathbb{Q}(\zeta)$ is a Galois extension over \mathbb{Q} , the restriction map $\text{Aut}(\mathbb{Q}_{\text{ab}}) \xrightarrow{\text{res}} \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is surjective. Thus, if $\sigma^2(\zeta) = \zeta$ for all $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$, then the exponent of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is at most 2, and hence $m \mid 24$. Conversely, if $m \mid 24$, then the exponent of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is at most 2, and so $\sigma^2(\zeta) = \zeta$ for all $\sigma \in \text{Aut}(\mathbb{Q}_{\text{ab}})$. \square

The next lemma is a variation of the argument used in the proof of [Coste and Gannon 1999, Proposition 3].

Lemma A.3. *Let k be a positive divisor of a positive integer n . Suppose that, for any integer a relatively prime to n such that $a \equiv 1 \pmod{k}$, we have $a^2 \equiv 1 \pmod{n}$. Then $\text{gcd}(n/k, k)$ divides 2 and n/k is a divisor of 24. Moreover, $\phi(n)/\phi(k)$ is a divisor of 8.*

Proof. Let $\pi : U(\mathbb{Z}_n) \rightarrow U(\mathbb{Z}_k)$ be the reduction map. The assumption implies that $\ker \pi$ is an elementary 2-group. It follows from the exact sequence

$$0 \rightarrow \ker \pi \rightarrow U(\mathbb{Z}_n) \xrightarrow{\pi} U(\mathbb{Z}_k) \rightarrow 0$$

that $\phi(n)/\phi(k)$ is a power of 2, and so is $\text{gcd}(n/k, k)$. Thus, if $2 \nmid \text{gcd}(n/k, k)$, then $\text{gcd}(n/k, k) = 1$. By the Chinese remainder theorem, for any integer y relatively

prime to n/k , there exists an integer a such that $a \equiv y \pmod{n/k}$ and $a \equiv 1 \pmod{k}$. Thus, $a^2 \equiv 1 \pmod{n}$, and hence $y^2 \equiv 1 \pmod{n/k}$. This implies the exponent of $U(\mathbb{Z}_{n/k})$ is at most 2, and therefore $n/k \mid 24$. Moreover, $\phi(n)/\phi(k) = \phi(n/k)$ is a factor of 8.

Suppose $2 \mid \gcd(n/k, k)$. Then $k = 2^u k'$ for some positive integer u and odd integer k' . The aforementioned conclusion implies $n = 2^v n' k'$ where $v > u$ and $\gcd(n', 2^v k') = 1$. By the Chinese remainder theorem, the given condition implies the kernel of the reduction map $U(\mathbb{Z}_{2^v}) \rightarrow U(\mathbb{Z}_{2^u})$ is an elementary 2-group. Therefore, $2 \leq v \leq 3$ if $u = 1$, and $v = u + 1$ if $u > 1$. In both cases, $\gcd(n/k, k) = 2$ and $\phi(2^v)/\phi(2^u)$ is a divisor of 4. By the aforementioned argument, for any integer y relatively prime to n' , we have $y^2 \equiv 1 \pmod{n'}$. Therefore, $n' \mid 24$ and hence $n' \mid 3$. Thus, $n/k = n' 2^{v-u} \mid 12$, and

$$\frac{\phi(n)}{\phi(k)} = \phi(n') \frac{\phi(2^v)}{\phi(2^u)}$$

is also a divisor of 8. □

Acknowledgements

Part of this paper was carried out while Ng was visiting the National Center for Theoretical Sciences and Shanghai University. He would like to thank these institutes for their generous hospitality, especially Ching-Hung Lam, Wen-Ching Li and Xiuyun Guo for being wonderful hosts. He particularly thanks Ling Long for many invaluable discussions, and Eric Rowell for his suggestions and stimulative discussions after the first version of this paper was posted on the arXiv.

References

- [Abe et al. 2004] T. Abe, G. Buhl, and C. Dong, “Rationality, regularity, and C_2 -cofiniteness”, *Trans. Amer. Math. Soc.* **356**:8 (2004), 3391–3402. MR 2005c:17041 Zbl 1070.17011
- [Bakalov and Kirillov 2001] B. Bakalov and A. Kirillov, Jr., *Lectures on tensor categories and modular functors*, University Lecture Series **21**, American Mathematical Society, Providence, RI, 2001. MR 2002d:18003 Zbl 0965.18002
- [Bantay 1997] P. Bantay, “The Frobenius–Schur indicator in conformal field theory”, *Phys. Lett. B* **394**:1–2 (1997), 87–88. MR 98c:81195 Zbl 0925.81331
- [Bantay 2003] P. Bantay, “The kernel of the modular representation and the Galois action in RCFT”, *Comm. Math. Phys.* **233**:3 (2003), 423–438. MR 2004g:81240 Zbl 1035.81055
- [Bauer et al. 1997] M. Bauer, A. Coste, C. Itzykson, and P. Ruelle, “Comments on the links between $\text{su}(3)$ modular invariants, simple factors in the Jacobian of Fermat curves, and rational triangular billiards”, *J. Geom. Phys.* **22**:2 (1997), 134–189. MR 98g:81189 Zbl 0895.14009
- [Beyl 1986] F. R. Beyl, “The Schur multiplier of $\text{SL}(2, \mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property”, *Math. Z.* **191**:1 (1986), 23–42. MR 87b:20071 Zbl 0581.20050
- [de Boer and Goeree 1991] J. de Boer and J. Goeree, “Markov traces and II_1 factors in conformal field theory”, *Comm. Math. Phys.* **139**:2 (1991), 267–304. MR 93i:81211 Zbl 0760.57002

- [Cappelli et al. 1987a] A. Cappelli, C. Itzykson, and J.-B. Zuber, “Modular invariant partition functions in two dimensions”, *Nuclear Phys. B* **280**:3 (1987), 445–465. MR 88i:81132 Zbl 0661.17017
- [Cappelli et al. 1987b] A. Cappelli, C. Itzykson, and J.-B. Zuber, “The A-D-E classification of minimal and $A_1^{(1)}$ conformal invariant theories”, *Comm. Math. Phys.* **113**:1 (1987), 1–26. MR 89b:81178 Zbl 0639.17008
- [Cardy 1986] J. L. Cardy, “Operator content of two-dimensional conformally invariant theories”, *Nuclear Phys. B* **270**:2 (1986), 186–204. MR 87k:17017 Zbl 0689.17016
- [Coste and Gannon 1994] A. Coste and T. Gannon, “Remarks on Galois symmetry in rational conformal field theories”, *Phys. Lett. B* **323**:3–4 (1994), 316–321. MR 95h:81031
- [Coste and Gannon 1999] A. Coste and T. Gannon, “Congruence subgroups and rational conformal field theory”, preprint, 1999. arXiv math/9909080
- [Dong and Jiang 2010] C. Dong and C. Jiang, “A characterization of vertex operator algebra $L(1/2, 0) \otimes L(1/2, 0)$ ”, *Comm. Math. Phys.* **296**:1 (2010), 69–88. MR 2011c:17049 Zbl 1207.17034
- [Dong and Jiang 2011] C. Dong and C. Jiang, “A characterization of vertex operator algebras $V_{\mathbb{Z}\alpha}^+$, I”, 2011. To appear in *J. Reine Angew. Math.* arXiv 1110.1882
- [Dong and Jiang 2013] C. Dong and C. Jiang, “A characterization of the rational vertex operator algebra $V_{\mathbb{Z}\alpha}^+$, II”, *Adv. Math.* **247** (2013), 41–70. MR 3096793 Zbl 1292.17021
- [Dong and Mason 1996] C. Dong and G. Mason, “Vertex operator algebras and Moonshine: a survey”, pp. 101–136 in *Progress in algebraic combinatorics* (Fukuoka, 1993), edited by E. Bannai and A. Munemasa, Adv. Stud. Pure Math. **24**, Math. Soc. Japan, Tokyo, 1996. MR 97h:17027 Zbl 0861.17018
- [Dong and Zhang 2008] C. Dong and W. Zhang, “On classification of rational vertex operator algebras with central charges less than 1”, *J. Algebra* **320**:1 (2008), 86–93. MR 2009c:17045 Zbl 1163.17029
- [Dong et al. 1997] C. Dong, H. Li, and G. Mason, “Regularity of rational vertex operator algebras”, *Adv. Math.* **132**:1 (1997), 148–166. MR 98m:17037 Zbl 0902.17014
- [Dong et al. 1998a] C. Dong, H. Li, and G. Mason, “Twisted representations of vertex operator algebras”, *Math. Ann.* **310**:3 (1998), 571–600. MR 99d:17030 Zbl 0890.17029
- [Dong et al. 1998b] C. Dong, H. Li, and G. Mason, “Vertex operator algebras and associative algebras”, *J. Algebra* **206**:1 (1998), 67–96. MR 99i:17029 Zbl 0911.17017
- [Dong et al. 2000] C. Dong, H. Li, and G. Mason, “Modular-invariance of trace functions in orbifold theory and generalized Moonshine”, *Comm. Math. Phys.* **214**:1 (2000), 1–56. MR 2001k:17043 Zbl 1061.17025
- [Dong et al. 2001] C. Dong, G. Mason, and K. Nagatomo, “Quasi-modular forms and trace functions associated to free boson and lattice vertex operator algebras”, *Internat. Math. Res. Notices* **8** (2001), 409–427. MR 2002b:11060 Zbl 0990.17022
- [Dong et al. 2013] C. Dong, X. Jiao, and F. Xu, “Quantum dimensions and quantum Galois theory”, *Trans. Amer. Math. Soc.* **365**:12 (2013), 6441–6469. MR 3105758 Zbl 06218191
- [Eholzer 1995] W. Eholzer, “On the classification of modular fusion algebras”, *Comm. Math. Phys.* **172**:3 (1995), 623–659. MR 96e:11060 Zbl 0884.17018
- [Eholzer and Skoruppa 1995] W. Eholzer and N.-P. Skoruppa, “Modular invariance and uniqueness of conformal characters”, *Comm. Math. Phys.* **174**:1 (1995), 117–136. MR 96k:11052 Zbl 0884.17019
- [Etingof 2002] P. Etingof, “On Vafa’s theorem for tensor categories”, *Math. Res. Lett.* **9**:5–6 (2002), 651–657. MR 2003i:18009 Zbl 1035.18004
- [Etingof and Gelaki 1999] P. Etingof and S. Gelaki, “On the exponent of finite-dimensional Hopf algebras”, *Math. Res. Lett.* **6**:2 (1999), 131–140. MR 2000f:16045 Zbl 0954.16028

- [Etingof et al. 2005] P. Etingof, D. Nikshych, and V. Ostrik, “On fusion categories”, *Ann. of Math.* (2) **162**:2 (2005), 581–642. MR 2006m:16051 Zbl 1125.16025
- [Frenkel et al. 1988] I. Frenkel, J. Lepowsky, and A. Meurman, *Vertex operator algebras and the Monster*, Pure and Applied Mathematics **134**, Academic Press, Boston, 1988. MR 90h:17026 Zbl 0674.17001
- [Frenkel et al. 1993] I. B. Frenkel, Y.-Z. Huang, and J. Lepowsky, “On axiomatic approaches to vertex operator algebras and modules”, *Mem. Amer. Math. Soc.* **104**:494 (1993), viii+64. MR 94a:17007 Zbl 0789.17022
- [Fuchs and Schweigert 2003] J. Fuchs and C. Schweigert, “Category theory for conformal boundary conditions”, pp. 25–70 in *Vertex operator algebras in mathematics and physics* (Toronto, ON, 2000), edited by S. Berman et al., Fields Inst. Commun. **39**, Amer. Math. Soc., Providence, RI, 2003. MR 2005b:17056 Zbl 1084.17012
- [Fuchs et al. 1999] J. Fuchs, A. C. Ganchev, K. Szlachányi, and P. Vecsernyés, “ S_4 symmetry of $6j$ symbols and Frobenius–Schur indicators in rigid monoidal C^* categories”, *J. Math. Phys.* **40**:1 (1999), 408–426. MR 99k:81111 Zbl 0986.81044
- [Gannon 2005] T. Gannon, “Modular data: the algebraic combinatorics of conformal field theory”, *J. Algebraic Combin.* **22**:2 (2005), 211–250. MR 2006h:81254 Zbl 1103.17007
- [Gannon 2006] T. Gannon, *Moonshine beyond the Monster*, Cambridge University Press, 2006. MR 2008a:17032 Zbl 1146.11026
- [Hong and Rowell 2010] S.-m. Hong and E. Rowell, “On the classification of the Grothendieck rings of non-self-dual modular categories”, *J. Algebra* **324**:5 (2010), 1000–1015. MR 2011k:18018 Zbl 1210.18006
- [Huang 1995] Y.-Z. Huang, “A theory of tensor products for module categories for a vertex operator algebra, IV”, *J. Pure Appl. Algebra* **100**:1–3 (1995), 173–216. MR 98a:17050 Zbl 0841.17015
- [Huang 2008a] Y.-Z. Huang, “Rigidity and modularity of vertex tensor categories”, *Commun. Contemp. Math.* **10**:suppl. 1 (2008), 871–911. MR 2009i:17041 Zbl 1169.17019
- [Huang 2008b] Y.-Z. Huang, “Vertex operator algebras and the Verlinde conjecture”, *Commun. Contemp. Math.* **10**:1 (2008), 103–154. MR 2009e:17056 Zbl 1180.17008
- [Huang and Lepowsky 1995a] Y.-Z. Huang and J. Lepowsky, “A theory of tensor products for module categories for a vertex operator algebra, I”, *Selecta Math. (N.S.)* **1**:4 (1995), 699–756. MR 98a:17047 Zbl 0854.17032
- [Huang and Lepowsky 1995b] Y.-Z. Huang and J. Lepowsky, “A theory of tensor products for module categories for a vertex operator algebra, II”, *Selecta Math. (N.S.)* **1**:4 (1995), 757–786. MR 98a:17047 Zbl 0854.17033
- [Huang and Lepowsky 1995c] Y.-Z. Huang and J. Lepowsky, “A theory of tensor products for module categories for a vertex operator algebra, III”, *J. Pure Appl. Algebra* **100**:1–3 (1995), 141–171. MR 98a:17049 Zbl 0841.17014
- [Kac 1990] V. G. Kac, *Infinite-dimensional Lie algebras*, 3rd ed., Cambridge University Press, 1990. MR 92k:17038 Zbl 0716.17022
- [Kac and Peterson 1984] V. G. Kac and D. H. Peterson, “Infinite-dimensional Lie algebras, theta functions and modular forms”, *Adv. in Math.* **53**:2 (1984), 125–264. MR 86a:17007 Zbl 0584.17007
- [Karpilovsky 1985] G. Karpilovsky, *Projective representations of finite groups*, Monographs and Textbooks in Pure and Applied Mathematics **94**, Marcel Dekker, New York, 1985. MR 86m:20014 Zbl 0568.20016
- [Kashina et al. 2006] Y. Kashina, Y. Sommerhäuser, and Y. Zhu, “On higher Frobenius–Schur indicators”, *Mem. Amer. Math. Soc.* **181**:855 (2006), viii+65. MR 2007k:16071 Zbl 1163.16029

- [Kassel 1995] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics **155**, Springer, New York, 1995. MR 96e:17041 Zbl 0808.17003
- [Kiritsis 1989] E. B. Kiritsis, “Proof of the completeness of the classification of rational conformal theories with $c = 1$ ”, *Phys. Lett. B* **217**:4 (1989), 427–430. MR 89k:81150
- [Knopp and Mason 2003] M. Knopp and G. Mason, “On vector-valued modular forms and their Fourier coefficients”, *Acta Arith.* **110**:2 (2003), 117–124. MR 2004j:11043 Zbl 1044.11020
- [Lepowsky and Li 2004] J. Lepowsky and H. Li, *Introduction to vertex operator algebras and their representations*, Progress in Mathematics **227**, Birkhäuser, Boston, 2004. MR 2004k:17050 Zbl 1055.17001
- [Linchenko and Montgomery 2000] V. Linchenko and S. Montgomery, “A Frobenius–Schur theorem for Hopf algebras”, *Algebr. Represent. Theory* **3**:4 (2000), 347–355. MR 2001k:16073 Zbl 0971.16018
- [Mason and Ng 2005] G. Mason and S.-H. Ng, “Central invariants and Frobenius–Schur indicators for semisimple quasi-Hopf algebras”, *Adv. Math.* **190**:1 (2005), 161–195. MR 2005h:16066 Zbl 1100.16033
- [Mennicke 1967] J. Mennicke, “On Ihara’s modular group”, *Invent. Math.* **4** (1967), 202–228. MR 37 #1485 Zbl 0189.02504
- [Moore 1987] G. Moore, “Atkin–Lehner symmetry”, *Nuclear Phys. B* **293**:1 (1987), 139–188. MR 89c:81151a
- [Moore and Seiberg 1990] G. Moore and N. Seiberg, “Lectures on RCFT”, pp. 263–361 in *Physics, geometry, and topology* (Banff, AB, 1989), edited by H. C. Lee, NATO Adv. Sci. Inst. Ser. B Phys. **238**, Plenum, New York, 1990. MR 93m:81133b Zbl 0728.57012
- [Müger 2003a] M. Müger, “From subfactors to categories and topology, I: Frobenius algebras in and Morita equivalence of tensor categories”, *J. Pure Appl. Algebra* **180**:1–2 (2003), 81–157. MR 2004f:18013 Zbl 1033.18002
- [Müger 2003b] M. Müger, “From subfactors to categories and topology, II: The quantum double of tensor categories and subfactors”, *J. Pure Appl. Algebra* **180**:1–2 (2003), 159–219. MR 2004f:18014 Zbl 1033.18003
- [Newman 1972] M. Newman, *Integral matrices*, Pure and Applied Mathematics **45**, Academic Press, New York-London, 1972. MR 49 #5038 Zbl 0254.15009
- [Ng and Schauenburg 2007a] S.-H. Ng and P. Schauenburg, “Frobenius–Schur indicators and exponents of spherical categories”, *Adv. Math.* **211**:1 (2007), 34–71. MR 2008b:16067 Zbl 1138.16017
- [Ng and Schauenburg 2007b] S.-H. Ng and P. Schauenburg, “Higher Frobenius–Schur indicators for pivotal categories”, pp. 63–90 in *Hopf algebras and generalizations*, edited by L. H. Kauffman et al., *Contemp. Math.* **441**, American Mathematical Society, Providence, RI, 2007. MR 2008m:18015 Zbl 1153.18008
- [Ng and Schauenburg 2008] S.-H. Ng and P. Schauenburg, “Central invariants and higher indicators for semisimple quasi-Hopf algebras”, *Trans. Amer. Math. Soc.* **360**:4 (2008), 1839–1860. MR 2009d:16065 Zbl 1141.16028
- [Ng and Schauenburg 2010] S.-H. Ng and P. Schauenburg, “Congruence subgroups and generalized Frobenius–Schur indicators”, *Comm. Math. Phys.* **300**:1 (2010), 1–46. MR 2012g:81193 Zbl 1206.18007
- [Rocha-Caridi 1985] A. Rocha-Caridi, “Vacuum vector representations of the Virasoro algebra”, pp. 451–473 in *Vertex operators in mathematics and physics* (Berkeley, Calif., 1983), edited by J. Lepowsky et al., *Math. Sci. Res. Inst. Publ.* **3**, Springer, New York, 1985. MR 87b:17011 Zbl 0557.17005

- [Rowell et al. 2009] E. Rowell, R. Stong, and Z. Wang, “On classification of modular tensor categories”, *Comm. Math. Phys.* **292**:2 (2009), 343–389. MR 2011b:18013 Zbl 1186.18005
- [Schauenburg 2004] P. Schauenburg, “On the Frobenius–Schur indicators for quasi-Hopf algebras”, *J. Algebra* **282**:1 (2004), 129–139. MR 2005h:16068 Zbl 1071.16037
- [Sommerhäuser and Zhu 2009] Y. Sommerhäuser and Y. Zhu, “On the central charge of a factorizable Hopf algebra”, preprint, 2009. arXiv 0906.3471
- [Sommerhäuser and Zhu 2012] Y. Sommerhäuser and Y. Zhu, “Hopf algebras and congruence subgroups”, *Mem. Amer. Math. Soc.* **219**:1028 (2012), vi+134. MR 2985696 Zbl 1314.16021
- [Sommerhäuser and Zhu 2013] Y. Sommerhäuser and Y. Zhu, “On the central charge of a factorizable Hopf algebra”, *Adv. Math.* **236** (2013), 158–223. MR 3019720 Zbl 1280.16028
- [Turaev 2010] V. G. Turaev, *Quantum invariants of knots and 3-manifolds*, 2nd ed., de Gruyter Studies in Mathematics **18**, Walter de Gruyter & Co., Berlin, 2010. MR 2011f:57023 Zbl 1213.57002
- [Vafa 1988] C. Vafa, “Toward classification of conformal theories”, *Phys. Lett. B* **206**:3 (1988), 421–426. MR 89k:81178
- [Verlinde 1988] E. Verlinde, “Fusion rules and modular transformations in 2D conformal field theory”, *Nuclear Phys. B* **300**:3 (1988), 360–376. MR 89h:81238 Zbl 1180.81120
- [Wang 2010] Z. Wang, *Topological quantum computation*, CBMS Regional Conference Series in Mathematics **112**, American Mathematical Society, Providence, RI, 2010. MR 2011f:81054 Zbl 1239.81005
- [Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997. MR 97h:11130 Zbl 0966.11047
- [Weibel 1994] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, 1994. MR 95f:18001 Zbl 0797.18001
- [Wohlfahrt 1964] K. Wohlfahrt, “An extension of F. Klein’s level concept”, *Illinois J. Math.* **8** (1964), 529–535. MR 29 #4805 Zbl 0135.29101
- [Xu 2006] F. Xu, “Some computations in the cyclic permutations of completely rational nets”, *Comm. Math. Phys.* **267**:3 (2006), 757–782. MR 2007h:81199 Zbl 1138.81510
- [Zhang and Dong 2009] W. Zhang and C. Dong, “ W -algebra $W(2, 2)$ and the vertex operator algebra $L(1/2, 0) \otimes L(1/2, 0)$ ”, *Comm. Math. Phys.* **285**:3 (2009), 991–1004. MR 2009k:17048 Zbl 1194.17015
- [Zhu 1996] Y. Zhu, “Modular invariance of characters of vertex operator algebras”, *J. Amer. Math. Soc.* **9**:1 (1996), 237–302. MR 96c:17042 Zbl 0854.17034

Communicated by Susan Montgomery

Received 2015-03-05

Revised 2015-07-20

Accepted 2015-08-19

dong@ucsc.edu

*Department of Mathematics, UC Santa Cruz,
194 Baskin Engineering, Santa Cruz, CA 95064, United States*

xingjunlin88@gmail.com

*Department of Mathematics, Sichuan University,
Chengdu, 610064, China*

rng@math.lsu.edu

*Department of Mathematics, Louisiana State University,
Baton Rouge, LA 70803, United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Roger Heath-Brown	Oxford University, UK	Michel van den Bergh	Hasselt University, Belgium
Craig Huneke	University of Virginia, USA	Marie-France Vignéras	Université Paris VII, France
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Kei-Ichi Watanabe	Nihon University, Japan
János Kollár	Princeton University, USA	Efim Zelmanov	University of California, San Diego, USA
Yuri Manin	Northwestern University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US \$255/year for the electronic version, and \$440/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2015 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 9 No. 9 2015

Families of nearly ordinary Eisenstein series on unitary groups XIN WAN	1955
Classifying orders in the Sklyanin algebra DANIEL ROGALSKI, SUSAN J. SIERRA and J. TOBY STAFFORD	2055
Congruence property in conformal field theory CHONGYING DONG, XINGJUN LIN and SIU-HUNG NG	2121
An averaged form of Chowla's conjecture KAISA MATOMÄKI, MAKSYM RADZIWIŁŁ and TERENCE TAO	2167



1937-0652(2015)9:9;1-0