Commun. Math. Phys. 390, 1271–1310 (2022)
Digital Object Identifier (DOI) https://doi.org/10.1007/s00220-021-04287-5

Communications in
Mathematical Physics

Modular Categories with Transitive Galois Actions

Siu-Hung Ng[1], **Yilong Wang**[2], **Qing Zhang**[3]

[1] Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA.
E-mail: rng@math.lsu.edu
[2] Beijing Institute of Mathematical Sciences and Applications (BIMSA), Huairou, Beijing, China.
E-mail: wyl@bimsa.cn
[3] Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA.
E-mail: zhan4169@purdue.edu

Received: 3 May 2021 / Accepted: 23 November 2021
Published online: 21 January 2022 – © The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2022

Abstract: In this paper, we study modular categories whose Galois group action on their simple objects are transitive. We show that such modular categories admit unique factorization into prime transitive factors. The representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with transitive modular categories are proven to be minimal and irreducible. Using the Verlinde formula, we characterize prime transitive modular categories as the Galois conjugates of the adjoint subcategory of the quantum group modular category $\mathcal{C}(\mathfrak{sl}_2, p-2)$ for some prime $p > 3$. As a consequence, we completely classify transitive modular categories. Transitivity of super-modular categories can be similarly defined. A unique factorization of any transitive super-modular category into s-simple transitive factors is obtained, and the split transitive super-modular categories are completely classified.

1. Introduction

Modular categories are spherical braided fusion categories over $\mathbb{C}$ whose braidings are nondegenerate. The notion of modular category has evolved from the studies of rational conformal field theory [36], topological quantum field theory [52] and the quantum invariants of knots and 3-manifolds such as the Jones polynomial [33,47]. Moreover, unitary modular categories are the mathematical foundations of topological phases of matter [56] and topological quantum computing [50,55]. Similar to the role of groups in the study of symmetries, modular categories are natural algebraic objects to organize "quantum symmetries".

An important family of examples of modular categories is obtained from the quantum group construction [3,49]. In general, for any simple Lie algebra $\mathfrak{g}$ and a *suitable* root of unity $q \in \mathbb{C}$, one can construct a modular category by taking the semisimplification of the category of tilting modules of the quantum group $U_q(\mathfrak{g})$ specialized at the root of unity q [1,2]. The associated 3-manifold invariants [4,51] and mapping class group representations [5,29] are also well-studied in the literature.

Siu-Hung Ng was partially supported by the NSF Grant DMS-1664418.

Modular categories have many striking arithmetic properties, such as the Verlinde formula, which are encoded in the matrices S and T (see Section 2). More precisely, let $\mathfrak{s} := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\mathfrak{t} := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ be the generators of the modular group $\mathrm{SL}_2(\mathbb{Z})$. For any modular category $\mathcal{C}$, the assignment $\overline{\rho}_{\mathcal{C}} : \mathfrak{s} \mapsto S, \mathfrak{t} \mapsto T$ defines a projective representation of $\mathrm{SL}_2(\mathbb{Z})$ [3,52]. Another notable arithmetic property of $\mathcal{C}$ is the fact that the kernel of $\bar{\rho}_{\mathcal{C}}$ is a congruence subgroup whose level is equal to the order of the T-matrix [43]. Moreover, $\bar{\rho}_{\mathcal{C}}$ admits liftings to linear representations of $\mathrm{SL}_2(\mathbb{Z})$ which are also shown to have congruence kernels in [22]. In addition, these liftings enjoy certain symmetries under the action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. These properties of the liftings are essential to our proofs in this paper.

Since the irreducible characters of the fusion ring of a modular category $\mathcal{C}$ can be indexed by the set $\mathrm{Irr}(\mathcal{C})$ of isomorphism classes of simple objects of $\mathcal{C}$ [15,19], the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on these characters induces a permutation action on $\mathrm{Irr}(\mathcal{C})$. The number of Galois orbits is also an invariant of modular categories.

Classification problems are always important in any mathematical theory. There have been efforts on classifying modular categories by rank [9,10,48], Frobenius–Perron dimension [8,12] and Frobenius–Schur exponent [13,54]. Note that there are finitely many modular categories up to equivalence for any given rank [11]. The number of Galois orbits plays prominent roles in most of these papers (see also [16,32]), which leads to the idea of classifying modular categories by the number of Galois orbits.

In this paper, we investigate modular categories with only one Galois orbit, which are called *transitive modular categories*. The smallest nontrivial example of a transitive modular category is the Fibonacci modular category, which can be described as the adjoint subcategory $\mathcal{C}(\mathfrak{sl}_2, 3)^{(0)}$ of the quantum group category $\mathcal{C}(\mathfrak{sl}_2, 3)$ associated to $\mathfrak{sl}_2$ at level 3. More generally, the adjoint subcategory $\mathcal{C}(\mathfrak{sl}_2, p-2)^{(0)}$ of $\mathcal{C}(\mathfrak{sl}_2, p-2)$ and its Galois conjugates are prime and transitive modular categories for any prime $p > 3$ (see Proposition 4.3). Remarkably, up to equivalence, these are all the nontrivial prime transitive modular categories. Moreover, every transitive modular category can be uniquely factorized (up to permutation of factors) into a Deligne product of prime transitive ones. Specifically, we prove the following two major theorems of this paper (cf. Theorem 6.4 and Theorem 6.5).

Theorem I. *Let $\mathcal{C}$ be a nontrivial modular category. Then $\mathcal{C}$ is prime and transitive if and only if* $\mathrm{ord}(T)$ *is a prime number $p > 3$ and $\mathcal{C}$ is equivalent to a Galois conjugate of $\mathcal{C}(\mathfrak{sl}_2, p-2)^{(0)}$ as modular categories.*

Theorem II. *Let $\mathcal{C}$ be a nontrivial modular category. Then $\mathcal{C}$ is transitive if and only if $\mathcal{C}$ is equivalent to a Deligne product of prime transitive modular categories whose T-matrices have distinct orders. In particular,* $\mathrm{ord}(T)$ *is a square-free odd integer whose prime factors are greater than 3.*

To prove these theorems, we first study factorizations of transitive modular categories in Section 3. For any modular category $\mathcal{C}$, we denote by $\mathbb{Q}(S)$ the $\mathbb{Q}$-extension by adjoining all the entries of the S-matrix, and denote by $G_{\mathcal{C}}$ the corresponding Galois group over $\mathbb{Q}$. Our first observation is that the action of $G_{\mathcal{C}}$ on $\mathrm{Irr}(\mathcal{C})$ is fixed-point free (Proposition 3.2), and so $\mathrm{Irr}(\mathcal{C})$ is a $G_{\mathcal{C}}$-torsor. Moreover, every fusion subcategory of a transitive modular category is also transitive and modular (Corollary 3.9). We conclude that any transitive modular category has a unique factorization into a Deligne product of prime transitive modular categories in Theorem 3.11. In Section 4, we study the Galois conjugates of modular categories $\mathcal{C}(\mathfrak{sl}_2, k)^{(0)}$ at odd level k. We show that for any prime $p \geq 5$, every Galois conjugate of $\mathcal{C}(\mathfrak{sl}_2, p-2)^{(0)}$ is prime and transitive.

Inspired by the Galois symmetries of the representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with modular categories, we define the notion of *minimal representations* of $\mathrm{SL}_2(\mathbb{Z})$ and the *characteristic 2-group* of a modular category in Section 5. The minimal representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with a modular category $\mathcal{C}$ are completely determined by the eigenvalues of the images of $\mathfrak{t}$ (Lemma 5.6). Moreover, the characteristic 2-group of $\mathcal{C}$ naturally gives rise to a decomposition of any representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$ (see Proposition 5.11). By studying these two notions, we prove in Theorem 5.14 that any representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with a transitive modular category $\mathcal{C}$ is minimal and irreducible, and that the order of the T-matrix of $\mathcal{C}$ is odd and square-free.

We completely classify transitive modular categories in Section 6 by characterizing the prime and transitive modular categories. Using the minimality and the irreducibility of the representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with transitive modular categories, we show that the order of the T-matrix of any prime transitive modular category $\mathcal{C}$ is a prime $p \geq 5$, and it has the same fusion rules as $\mathcal{C}(\mathfrak{sl}_2, p-2)^{(0)}$. Applying the classification result of [30], we show that $\mathcal{C}$ must be a Galois conjugate of $\mathcal{C}(\mathfrak{sl}_2, p-2)^{(0)}$ (see Theorem 6.4). Combining with the unique factorization theorem, the full classification of transitive modular categories is established in Theorem 6.5.

Finally, we discuss transitive super-modular categories in Section 7. We classify all the transitive *split* super-modular categories by using the classification of transitive modular categories (Theorem 7.4). Moreover, a unique factorization of transitive super-modular categories into s-simple transitive factors is obtained in Theorem 7.13. Then we exhibit a family of non-split transitive prime categories over sVec and conjecture that these are all the s-simple transitive super-modular categories up to Galois conjugate.

The paper is organized as follows. In Section 2, we set up notations and give a brief review on modular categories. In Section 3, we define transitive modular categories and derive some fundamental properties of them. In particular, we establish the prime factorization theorem in Theorem 3.11. In Section 4, we discuss the prime and transitive modular categories obtained from the quantum group categories $\mathcal{C}(\mathfrak{sl}_2, p-2)$ for any odd prime p. In Section 5, we study the modular group representations associated with modular categories. We show in Theorem 5.14 that the representations associated with transitive modular categories are irreducible and minimal. In Section 6, we characterize the prime transitive modular categories in Theorem 6.4, which implies the complete classification of transitive modular categories in Theorem 6.5. Finally, in Section 7, transitive super-modular categories are introduced and studied. We classify split transitive super-modular categories in Theorem 7.4 and prove a unique factorization theorem of transitive super-modular categories in Theorem 7.13.

Throughout this paper, we tacitly use the following notations: $\zeta_n = \exp(2\pi i/n)$, $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$, and $i = \zeta_4 = \sqrt{-1}$. A subcategory of any category is assumed to a full subcategory, unless stated otherwise.

2. Preliminaries

In this section, we recall some basic definitions and notations. The readers are referred to [3,27,34] for more details.

2.1. Braided fusion categories. A *fusion category* is a semisimple, $\mathbb{C}$-linear abelian, rigid monoidal category with finite-dimensional Hom-spaces and finitely many isomorphism classes of simple objects including the tensor unit $\mathbb{1}$. For any fusion category $\mathcal{C}$,

we denote by $\mathrm{Irr}(\mathcal{C})$ the set of isomorphism classes of simple objects of $\mathcal{C}$. When it is clear from the context, we will denote the isomorphism class of an object X of $\mathcal{C}$ by the same notation X.

The Grothendieck group of $\mathcal{C}$, denoted by $K_0(\mathcal{C})$, admits a ring structure given by the tensor product. More precisely, we have $X \otimes Y = \sum_{Z \in \mathrm{Irr}(\mathcal{C})} N_{X,Y}^Z Z$ for any $X, Y \in \mathrm{Irr}(\mathcal{C})$, where

$$N_{X,Y}^Z := \dim_{\mathbb{C}} \mathcal{C}(X \otimes Y, Z) \tag{2.1}$$

are called the *fusion coefficients*. The collection of fusion coefficients $N_{X,Y}^Z$ for all $X, Y, Z \in \mathrm{Irr}(\mathcal{C})$ is referred to as the *fusion rules* of $\mathcal{C}$. The *fusion matrix* N_X of $X \in \mathrm{Irr}(\mathcal{C})$ is defined as $(N_X)_{Z,Y} := N_{X,Y}^Z$ for any $Y, Z \in \mathrm{Irr}(\mathcal{C})$. The largest real eigenvalue of N_X, denoted by $\mathrm{FPdim}(X)$, is called the *Frobenius–Perron dimension of* X. The *Frobenius–Perron dimension* of $\mathcal{C}$ is defined as

$$\mathrm{FPdim}(\mathcal{C}) := \sum_{X \in \mathrm{Irr}(\mathcal{C})} \mathrm{FPdim}(X)^2.$$

Let $\mathcal{C}$ be a fusion category. For any object $X \in \mathcal{C}$, the left dual of X is a triple $(X^*, \mathrm{ev}_X, \mathrm{coev}_X)$, where X^* is an object of $\mathcal{C}$, $\mathrm{ev}_X : X^* \otimes X \to \mathbb{1}$ and $\mathrm{coev}_X : \mathbb{1} \to X \otimes X^*$ are respectively the evaluation and coevaluation morphisms associated with the left dual object X^* of X. A simple object $X \in \mathrm{Irr}(\mathcal{C})$ is called *invertible* if $X \otimes X^* \cong \mathbb{1}$. The *pointed* subcategory of $\mathcal{C}$, denoted by $\mathcal{C}_{\mathrm{pt}}$, is the full abelian subcategory generated by the invertible objects of $\mathcal{C}$. A fusion category $\mathcal{C}$ is called pointed if $\mathcal{C}_{\mathrm{pt}} = \mathcal{C}$. The *adjoint subcategory* of $\mathcal{C}$, denoted by $\mathcal{C}_{\mathrm{ad}}$ or $\mathcal{C}^{(0)}$, is the full abelian subcategory generated by the subobjects of $X \otimes X^*$ for any $X \in \mathcal{C}$ (cf. [28,31]). Both $\mathcal{C}_{\mathrm{pt}}$ and $\mathcal{C}_{\mathrm{ad}}$ are fusion subcategories of $\mathcal{C}$.

The left duality of $\mathcal{C}$ can be extended to a contravariant monoidal functor $(-)^*$, and so $(-)^{**}$ defines a monoidal functor on $\mathcal{C}$. A *pivotal structure* on a fusion category $\mathcal{C}$ is an isomorphism of monoidal functors $j : \mathrm{id}_{\mathcal{C}} \xrightarrow{\cong} (-)^{**}$. A fusion category equipped with a pivotal structure is called a *pivotal fusion category*. If $\mathcal{C}$ is a pivotal fusion category, then for any $X \in \mathcal{C}$ and $f \in \mathrm{End}_{\mathcal{C}}(X)$, the (left) *quantum trace* of f can be defined as

$$\mathrm{tr}_j(f) := \mathrm{ev}_{X^*} \circ ((j_X \circ f) \otimes \mathrm{id}_{X^*}) \circ \mathrm{coev}_X \in \mathrm{End}_{\mathcal{C}}(\mathbb{1}) \cong \mathbb{C}.$$

A pivotal structure j on $\mathcal{C}$ is called *spherical* if $\mathrm{tr}_j(f) = \mathrm{tr}_j(f^*)$ for any endomorphism f of $\mathcal{C}$. A *spherical fusion category* is a fusion category equipped with a spherical pivotal structure. When the pivotal structure is clear from the context, we will drop the subscript j. In a pivotal category $\mathcal{C}$, the *quantum dimension* d_X of any object $X \in \mathcal{C}$ is defined to be $d_X := \mathrm{tr}(\mathrm{id}_X)$. It has been shown in [28] that if $\mathcal{C}$ is a spherical fusion category, then d_X is a totally real algebraic integer for any object $X \in \mathcal{C}$.

The *global dimension* of any fusion category was introduced in [37, Def. 2.5]. If $\mathcal{C}$ is a spherical fusion category, its global dimension is given by

$$\dim(\mathcal{C}) = \sum_{X \in \mathrm{Irr}(\mathcal{C})} d_X^2.$$

In particular, $\dim(\mathcal{C})$ is a totally positive algebraic integer. We will denote the positive square root of $\dim(\mathcal{C})$ by $\sqrt{\dim(\mathcal{C})}$.

A *braiding* on a fusion category $\mathcal{C}$ is a natural isomorphism

$$\beta_{X,Y} : X \otimes Y \xrightarrow{\cong} Y \otimes X$$

satisfying the Hexagon axioms. A fusion category equipped with a braiding is called a *braided fusion category*. Let $\mathcal{C}$ be a braided fusion category, and $\mathcal{D} \subset \mathcal{C}$ a collection of objects of $\mathcal{C}$. The *Müger centralizer* of $\mathcal{D}$ in $\mathcal{C}$ (cf. [38]), denoted by $C_{\mathcal{C}}(\mathcal{D})$, is the full subcategory of $\mathcal{C}$ with the collection of objects given by

$$\{X \in \mathcal{C} \mid \beta_{Y,X} \circ \beta_{X,Y} = \mathrm{id}_{X\otimes Y},\ \forall\, Y \in \mathcal{D}\}.$$

It follows directly from the definition of a braiding that $C_{\mathcal{C}}(\mathcal{D})$ is a fusion subcategory of $\mathcal{C}$. In particular, the fusion subcategory $C_{\mathcal{C}}(\mathcal{C})$ is called the *Müger center* of $\mathcal{C}$, and is denoted by $\mathcal{C}'$. A braided fusion category $\mathcal{C}$ (or its braiding β) is called *nondegenerate* if $\mathcal{C}'$ is equivalent to Vec, the category of finite-dimensional vector spaces over $\mathbb{C}$. A braided fusion category is called a *symmetric fusion category* if $\mathcal{C}' = \mathcal{C}$. By Deligne's theorems [20,21], if $\mathcal{C}$ is a symmetric fusion category, then $\dim(\mathcal{C}) \in \mathbb{Z}$.

2.2. Modular categories and arithmetic invariants. A *premodular* category (or a ribbon fusion category) is a spherical braided fusion category. A *modular category* $\mathcal{C}$ is a premodular category whose underlying braiding β is nondegenerate. The (unnormalized) S-matrix of a premodular category $\mathcal{C}$ is defined to be

$$S_{X,Y} := \mathrm{tr}(\beta_{Y,X^*} \circ \beta_{X^*,Y}),\ X, Y \in \mathrm{Irr}(\mathcal{C}).$$

In particular, $S_{X,\mathbb{1}} = S_{\mathbb{1},X} = d_X$. It has been proved in [38] that a premodular category is modular if and only if its S-matrix is invertible. Moreover, when $\mathcal{C}$ is modular, the fusion coefficients can be expressed in terms of the S-matrix by the Verlinde formula (see, for example, [3]):

$$N_{X,Y}^{Z} = \frac{1}{\dim(\mathcal{C})} \sum_{W \in \mathrm{Irr}(\mathcal{C})} \frac{S_{X,W} S_{Y,W} S_{Z^*,W}}{S_{\mathbb{1},W}}. \tag{2.2}$$

Let $\mathcal{C}$ be a modular category. A natural isomorphism $\theta : \mathrm{id}_{\mathcal{C}} \xrightarrow{\cong} \mathrm{id}_{\mathcal{C}}$, called the *ribbon structure* of $\mathcal{C}$, can be defined using the spherical pivotal structure of $\mathcal{C}$ and the Drinfeld isomorphism (cf. [41, Sec. 2]). The ribbon structure is compatible with the braiding and the duality in the following sense:

$$\theta_{X\otimes Y} = (\theta_X \otimes \theta_Y) \circ \beta_{Y,X} \circ \beta_{X,Y} \quad \text{and} \quad \theta_{X^*} = (\theta_X)^* \tag{2.3}$$

for any objects $X, Y \in \mathcal{C}$. If $X \in \mathrm{Irr}(\mathcal{C})$, then θ_X is a nonzero scalar multiple of id_X. We will use the abuse notation to denote both this scalar and the isomorphism itself by θ_X whenever X is simple. The T-matrix of $\mathcal{C}$ is defined to be the diagonal matrix

$$T_{X,Y} := \delta_{X,Y}\theta_X,\ X, Y \in \mathrm{Irr}(\mathcal{C}).$$

It follows from [53] (see also [3, Thm. 3.1.19]) that θ_X has finite order for any $X \in \mathrm{Irr}(\mathcal{C})$, and so does the T-matrix. The pair of matrices (S, T) is called the *(unnormalized) modular data* of $\mathcal{C}$. We may denote the modular data of a modular category $\mathcal{C}$ by $(S_{\mathcal{C}}, T_{\mathcal{C}})$ when the context needs to be clarified.

For any $m \in \mathbb{Z}$, the m-th *Gauss sum* [44] of a modular category $\mathcal{C}$ is defined as

$$\tau_m(\mathcal{C}) := \sum_{X \in \mathrm{Irr}(\mathcal{C})} d_X^2 \theta_X^m.$$

If $\gcd(m, \mathrm{ord}(T)) = 1$, the m-th (multiplicative) *central charge* and the m-th *anomaly* of $\mathcal{C}$ are defined as

$$\xi_m(\mathcal{C}) := \frac{\tau_m(\mathcal{C})}{|\tau_m(\mathcal{C})|} \quad \text{and} \quad \alpha_m(\mathcal{C}) := \xi_m(\mathcal{C})^2. \tag{2.4}$$

It is well-known that $|\tau_1(\mathcal{C})| = \sqrt{\dim(\mathcal{C})}$, and $\xi_m(\mathcal{C})$ is a root of unity (cf. [3,38,44]).

2.3. Galois actions on modular categories. Let $\mathcal{C}$ be a modular category with modular data (S, T). For any complex matrix M, we denote by $\mathbb{Q}(M)$ the field extension of $\mathbb{Q}$ by adjoining the entries of M. It has been proved in [43] that $\mathbb{Q}(S) \subset \mathbb{Q}(T) = \mathbb{Q}_N$, where $N = \mathrm{ord}(T)$. In particular, $\mathbb{Q}(S)$ is an abelian extension over $\mathbb{Q}$, and its Galois group is denoted by $G_{\mathcal{C}}$. It is immediate to see that

$$\mathbb{Q}(S) = \mathbb{Q}(S_{X,Y}/d_Y \mid X, Y \in \mathrm{Irr}(\mathcal{C})).$$

By the Verlinde formula, for any $Y \in \mathrm{Irr}(\mathcal{C})$, the assignment

$$\chi_Y : \mathrm{Irr}(\mathcal{C}) \to \mathbb{C}, \ X \mapsto \frac{S_{X,Y}}{d_Y}$$

defines a character of the fusion ring $K_0(\mathcal{C})$, and $\{\chi_Y \mid Y \in \mathrm{Irr}(\mathcal{C})\}$ is the set of irreducible characters of $K_0(\mathcal{C})$ (cf. [3]). Thus, for any $\sigma \in G_{\mathcal{C}}$, $\sigma(\chi_Y) = \chi_{\hat{\sigma}(Y)}$ for some permutation $\hat{\sigma}$ on $\mathrm{Irr}(\mathcal{C})$, and the map

$$G_{\mathcal{C}} \to \mathrm{Sym}(\mathrm{Irr}(\mathcal{C})), \ \sigma \mapsto \hat{\sigma}$$

is a group monomorphism. The set of orbits under this $G_{\mathcal{C}}$-action is abbreviated as $\mathrm{Orb}(\mathcal{C})$. We will denote a Galois automorphism $\sigma \in G_{\mathcal{C}}$ as well as its associated permutation on $\mathrm{Irr}(\mathcal{C})$ by $\hat{\sigma}$.

For any Galois extension E over $\mathbb{Q}$ containing $\mathbb{Q}(S)$, the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ acts on $\mathrm{Irr}(\mathcal{C})$ via the restriction on $\mathbb{Q}(S)$ or the surjection $\mathrm{Gal}(E/\mathbb{Q}) \xrightarrow{\mathrm{res}} G_{\mathcal{C}}$. Therefore, the $\mathrm{Gal}(E/\mathbb{Q})$-orbits in $\mathrm{Irr}(\mathcal{C})$ are identical to the $G_{\mathcal{C}}$-orbits. Using the above convention, for any $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, we use $\hat{\sigma}_{\mathcal{C}}$ to represent the restriction of σ on $\mathbb{Q}(S)$ and also its permutation on $\mathrm{Irr}(\mathcal{C})$. When it is clear from the context, $\hat{\sigma}_{\mathcal{C}}$ will simply be denoted by $\hat{\sigma}$. In particular, one can take $E = \bar{\mathbb{Q}}$ and so the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{Irr}(\mathcal{C})$. According to [19], for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $X, Y \in \mathrm{Irr}(\mathcal{C})$, we have

$$\sigma\left(\frac{S_{X,Y}}{\sqrt{\dim(\mathcal{C})}}\right) = \pm \frac{S_{\hat{\sigma}(X),Y}}{\sqrt{\dim(\mathcal{C})}}. \tag{2.5}$$

If $\mathcal{C} = \mathcal{A} \boxtimes \mathcal{B}$ for some modular categories $\mathcal{A}$ and $\mathcal{B}$, then $\mathrm{Irr}(\mathcal{C}) = \mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B})$ under the identification $X \boxtimes Y \mapsto (X, Y)$. In this case, $S_{\mathcal{C}} = S_{\mathcal{A}} \otimes S_{\mathcal{B}}$, the Kronecker product of the S-matrices. Therefore, $\mathbb{Q}(S_{\mathcal{C}}) = \mathbb{Q}(S_{\mathcal{A}})\mathbb{Q}(S_{\mathcal{B}})$, the composite field of $\mathbb{Q}(S_{\mathcal{A}})$ and $\mathbb{Q}(S_{\mathcal{B}})$. Let $\mathbb{F} = \mathbb{Q}(S_{\mathcal{A}}) \cap \mathbb{Q}(S_{\mathcal{B}})$, and $L = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$. The restrictions on

$\mathbb{F}$ define two epimorphisms $\mathrm{res}_{\mathcal{A}} : G_{\mathcal{A}} \to L$ and $\mathrm{res}_{\mathcal{B}} : G_{\mathcal{B}} \to L$. Their fiber product $G_{\mathcal{A}} \bullet G_{\mathcal{B}}$, defined as

$$G_{\mathcal{A}} \bullet G_{\mathcal{B}} := \{(\hat{\sigma}, \hat{\tau}) \in G_{\mathcal{A}} \times G_{\mathcal{B}} \mid \mathrm{res}_{\mathcal{A}}(\hat{\sigma}) = \mathrm{res}_{\mathcal{B}}(\hat{\tau})\},$$

satisfies the commutative diagram

$$\begin{array}{ccc} G_{\mathcal{A}} \bullet G_{\mathcal{B}} & \xrightarrow{p_{\mathcal{A}}} & G_{\mathcal{A}} \\ {\scriptstyle p_{\mathcal{B}}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_{\mathcal{A}}} \\ G_{\mathcal{B}} & \xrightarrow{\mathrm{res}_{\mathcal{B}}} & L \end{array}$$

where $p_{\mathcal{A}}$, $p_{\mathcal{B}}$ are coordinate projections. By the universal property of the fiber product, the restriction epimorphisms $\pi_{\mathcal{A}} : G_{\mathcal{C}} \to G_{\mathcal{A}}$ and $\pi_{\mathcal{B}} : G_{\mathcal{C}} \to G_{\mathcal{B}}$ induce a group homomorphism

$$f : G_{\mathcal{C}} \to G_{\mathcal{A}} \bullet G_{\mathcal{B}}, \quad f(\hat{\sigma}_{\mathcal{C}}) = (\hat{\sigma}_{\mathcal{A}}, \hat{\sigma}_{\mathcal{B}}) \tag{2.6}$$

for any $\hat{\sigma}_{\mathcal{C}} \in G_{\mathcal{C}}$. It follows from [24, Prop. 14.4.21] that f is an isomorphism. This proves the first part of statement (i) of the following lemma. The second part follows directly from [24, Cor. 14.4.20].

Lemma 2.1. *Let $\mathcal{C} = \mathcal{A} \boxtimes \mathcal{B}$ for some modular categories $\mathcal{A}$, $\mathcal{B}$, and let*

$$\mathbb{F} = \mathbb{Q}(S_{\mathcal{A}}) \cap \mathbb{Q}(S_{\mathcal{B}}).$$

Then:

(i) *The map $f : G_{\mathcal{C}} \to G_{\mathcal{A}} \bullet G_{\mathcal{B}}$, $f(\hat{\sigma}_{\mathcal{C}}) = (\hat{\sigma}_{\mathcal{A}}, \hat{\sigma}_{\mathcal{B}})$, defines an isomorphism of groups, and*

$$|G_{\mathcal{C}}| = \frac{|G_{\mathcal{A}}| \cdot |G_{\mathcal{B}}|}{[\mathbb{F} : \mathbb{Q}]}. \tag{2.7}$$

(ii) *For any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $X \in \mathrm{Irr}(\mathcal{A})$ and $Y \in \mathrm{Irr}(\mathcal{B})$, we have*

$$\hat{\sigma}_{\mathcal{C}}(X \boxtimes Y) = \hat{\sigma}_{\mathcal{A}}(X) \boxtimes \hat{\sigma}_{\mathcal{B}}(Y).$$

(iii) *For any $O_{\mathcal{A}} \in \mathrm{Orb}(\mathcal{A})$ and $O_{\mathcal{B}} \in \mathrm{Orb}(\mathcal{B})$, $G_{\mathcal{C}}$ acts on $O_{\mathcal{A}} \times O_{\mathcal{B}}$, under the identification of $\mathrm{Irr}(\mathcal{C}) = \mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B})$, and the number of $G_{\mathcal{C}}$-orbits in $O_{\mathcal{A}} \times O_{\mathcal{B}}$ is bounded by $[\mathbb{F} : \mathbb{Q}]$. In particular, the numbers of Galois orbits of these categories satisfy*

$$|\mathrm{Orb}(\mathcal{A})| \cdot |\mathrm{Orb}(\mathcal{B})| \leq |\mathrm{Orb}(\mathcal{C})| \leq |\mathrm{Orb}(\mathcal{A})| \cdot |\mathrm{Orb}(\mathcal{B})| \cdot [\mathbb{F} : \mathbb{Q}].$$

Proof. The equality (2.7) follows directly from [24, Cor. 14.4.20] and the definition of $G_{\mathcal{C}}$.

The action of $G_{\mathcal{C}}$ on $\mathrm{Irr}(\mathcal{C})$ is equivalent to the action of $G_{\mathcal{A}} \bullet G_{\mathcal{B}}$ on $\mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B})$ by the definition of the Galois group actions. The statement (ii) follows immediately from this observation.

To prove (iii), consider any $X \in O_A$ and $Y \in O_{\mathcal{B}}$. By definition,

$$\mathrm{Stab}_{G_{\mathcal{C}}}(X \boxtimes Y) \subset \mathrm{Stab}_{G_{\mathcal{A}}}(X) \times \mathrm{Stab}_{G_{\mathcal{B}}}(Y).$$

Therefore, by Burnside's lemma (see, for example, [24, Ex. 18.3.8]) and (2.7), we have

$$\begin{aligned} 1 &\leq \text{number of } G_{\mathcal{C}}\text{-orbits in } O_{\mathcal{A}} \times O_{\mathcal{B}} \\ &= \frac{1}{|G_{\mathcal{C}}|} \sum_{(X,Y)\in O_{\mathcal{A}}\times O_{\mathcal{B}}} |\operatorname{Stab}_{G_{\mathcal{C}}}(X \boxtimes Y)| \\ &\leq \frac{1}{|G_{\mathcal{C}}|} \sum_{(X,Y)\in O_{\mathcal{A}}\times O_{\mathcal{B}}} |\operatorname{Stab}_{G_{\mathcal{A}}}(X)| \cdot |\operatorname{Stab}_{G_{\mathcal{B}}}(Y)| \\ &= \frac{|G_{\mathcal{A}}| \cdot |G_{\mathcal{B}}|}{|G_{\mathcal{C}}|} = [\mathbb{F} : \mathbb{Q}]. \end{aligned}$$

Now, we can establish the last inequalities by summing over all $O_{\mathcal{A}} \times O_{\mathcal{B}} \in \operatorname{Orb}(\mathcal{A}) \times \operatorname{Orb}(\mathcal{B})$. □

3. Unique Factorization of Transitive Modular Categories

In this section, we introduce the definition of transitive modular categories. These modular categories have spectacular properties which provide the foundations for the classification. We prove in Theorem 3.11 that every fusion subcategory of a transitive modular category is a transitive modular subcategory and the prime factorization of a transitive modular category is unique up to permutation of prime factors.

Definition 3.1. A modular category $\mathcal{C}$ is said to be *transitive* if $G_{\mathcal{C}}$ (or $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$) acts transitively on $\operatorname{Irr}(\mathcal{C})$, i.e., $|\operatorname{Orb}(\mathcal{C})| = 1$.

Recall that a transitive subgroup G of the symmetric group $\mathfrak{S}_n$ is called *regular* if the G-action on $\{1, \ldots, n\}$ is fixed-point free (cf. [57]).

Proposition 3.2. *If $\mathcal{C}$ is a transitive modular category, then $G_{\mathcal{C}}$ is regular and $|G_{\mathcal{C}}| = |\operatorname{Irr}(\mathcal{C})|$.*

Proof. Since $\mathcal{C}$ is a transitive modular category, $G_{\mathcal{C}}$ is an abelian transitive subgroup of $\operatorname{Sym}(\operatorname{Irr}(\mathcal{C}))$. By [57, Prop. 4.4], $G_{\mathcal{C}}$ is regular. In particular, $|G_{\mathcal{C}}| = |\operatorname{Irr}(\mathcal{C})|$. □

Since $G_{\mathcal{C}}$ is regular, for any $X \in \operatorname{Irr}(\mathcal{C})$, there is a unique $\hat{\sigma} \in G_{\mathcal{C}}$ such that $X = \hat{\sigma}(\mathbb{1})$. Therefore, we simply identify $G_{\mathcal{C}}$ with $\operatorname{Irr}(\mathcal{C})$ via the identification $\hat{\sigma} \mapsto \hat{\sigma}(\mathbb{1})$. For convenience, we will use $\mathbb{1}$ and $\hat{\mathrm{id}}$ interchangeably. In particular, the action of $\hat{\sigma}$ on $\hat{\mu}$ is equal to the product $\hat{\sigma}\hat{\mu}$ for any $\hat{\sigma}, \hat{\mu} \in G_{\mathcal{C}}$.

Thus, for any transitive modular category $\mathcal{C}$, its modular data can be indexed by $G_{\mathcal{C}}$. Moreover, the S-matrix can be expressed in terms of the dimensions of simple objects as in the following lemma.

Lemma 3.3. *Let $\mathcal{C}$ be a transitive modular category. For any $\hat{\sigma}, \hat{\mu} \in \operatorname{Irr}(\mathcal{C})$, we have*

$$S_{\hat{\sigma},\hat{\mu}} = \hat{\sigma}(d_{\hat{\mu}})d_{\hat{\sigma}} = \hat{\mu}(d_{\hat{\sigma}})d_{\hat{\mu}}. \tag{3.8}$$

Consequently, all the entries of the S-matrix are totally real algebraic units, and every simple object of $\mathcal{C}$ is self-dual.

Proof. Recall from Section 2.3 that

$$\hat{\mu}\left(\frac{S_{\hat{\sigma},\mathbb{1}}}{d_{\mathbb{1}}}\right) = \frac{S_{\hat{\sigma},\hat{\mu}}}{d_{\hat{\mu}}},$$

so we have $S_{\hat{\sigma},\hat{\mu}} = \hat{\mu}(d_{\hat{\sigma}})d_{\hat{\mu}}$. Since S is symmetric, we also have $S_{\hat{\sigma},\hat{\mu}} = \hat{\sigma}(d_{\hat{\mu}})d_{\hat{\sigma}}$.

According to [11, Prop. 3.6], $d_{\hat{\sigma}} = d_{\hat{\sigma}(\mathbb{1})}$ is an algebraic unit for all $\hat{\sigma} \in G_{\mathcal{C}}$. Since both $d_{\hat{\sigma}}$ and $d_{\hat{\mu}}$ are totally real (cf. [28]), $S_{\hat{\sigma},\hat{\mu}}$ is a totally real unit. In particular, the matrix $s = \frac{1}{\sqrt{\dim(\mathcal{C})}}S$ is a unitary real symmetric matrix, and so we have $\mathrm{id} = s^2 = C$, where $C_{X,Y} = \delta_{X,Y^*}$ is the charge conjugation matrix (cf. [3,28]). Therefore, every simple object of $\mathcal{C}$ is self-dual. □

Corollary 3.4. *Let $\mathcal{C}$ be a transitive modular category. Then there exists a unique element $\hat{\sigma}_0 \in G_{\mathcal{C}}$ such that $\hat{\sigma}_0(d_{\hat{\mu}}) = \mathrm{FPdim}(\hat{\mu})$ for all $\hat{\mu} \in G_{\mathcal{C}}$, and*

$$\hat{\sigma}_0(\dim(\mathcal{C})) = \mathrm{FPdim}(\mathcal{C}).$$

Proof. Since the Frobenius–Perron dimension defines a character of the fusion ring $K_0(\mathcal{C})$ and the simple objects are in one-to-one correspondence to the characters of the fusion ring (see Section 2.3), there exists a unique simple object $\hat{\sigma}_0 \in G_{\mathcal{C}}$ such that $\chi_{\hat{\sigma}_0}(\hat{\mu}) = \mathrm{FPdim}(\hat{\mu})$ for all $\hat{\mu} \in G_{\mathcal{C}}$. Therefore, by Lemma 3.3, we have

$$\mathrm{FPdim}(\hat{\mu}) = \chi_{\hat{\sigma}_0}(\hat{\mu}) = \frac{S_{\hat{\mu},\hat{\sigma}_0}}{d_{\hat{\sigma}_0}} = \hat{\sigma}_0(d_{\hat{\mu}}).$$

The second assertion follows directly from the first statement and the definitions of $\dim(\mathcal{C})$ and $\mathrm{FPdim}(\mathcal{C})$. □

Now, we can prove the first major observation on transitive modular categories.

Theorem 3.5. *Let $\mathcal{C}$ be a transitive modular category. Then:*

(i) *For any $\hat{\sigma}, \hat{\mu} \in \mathrm{Irr}(\mathcal{C})$, if $\hat{\sigma} \neq \hat{\mu}$, then $d_{\hat{\sigma}}^2 \neq d_{\hat{\mu}}^2$. In particular, if $\hat{\mu} \neq \hat{\mathrm{id}}$, then*

$$d_{\hat{\mu}}^2 \neq 1 \quad \textit{and} \quad \hat{\mu}(\dim(\mathcal{C})) \neq \dim(\mathcal{C}).$$

(ii) *If X is an invertible object in $\mathcal{C}$, then $X \cong \mathbb{1}$. In particular, $\mathcal{C}_{\mathrm{pt}} \simeq \mathrm{Vec}$ as fusion categories.*

(iii) $\mathbb{Q}(S) = \mathbb{Q}(\dim(\mathcal{C})) = \mathbb{Q}(d_X \mid X \in \mathrm{Irr}(\mathcal{C}))$.

Proof. Suppose there exist $\hat{\sigma} \neq \hat{\mu} \in \mathrm{Irr}(\mathcal{C})$ such that $d_{\hat{\sigma}}^2 = d_{\hat{\mu}}^2$. Then $d_{\hat{\sigma}} = \varepsilon d_{\hat{\mu}}$ for some $\varepsilon \in \{\pm 1\}$. By Lemma 3.3, for any $\hat{\lambda} \in \mathrm{Irr}(\mathcal{C})$, we have

$$S_{\hat{\sigma},\hat{\lambda}} = \hat{\lambda}(d_{\hat{\sigma}})d_{\hat{\lambda}} = \hat{\lambda}(\varepsilon d_{\hat{\mu}})d_{\hat{\lambda}} = \varepsilon\hat{\lambda}(d_{\hat{\mu}})d_{\hat{\lambda}} = \varepsilon S_{\hat{\mu},\hat{\lambda}}.$$

Consequently, the rows $S_{\hat{\sigma},*}$ and $S_{\hat{\mu},*}$ of S are linearly dependent, which contradicts the invertibility of the S-matrix. This proves the first assertion of statement (i).

Note that $d_{\hat{\mathrm{id}}} = d_{\mathbb{1}} = 1$. Therefore, for any $\hat{\mu} \neq \hat{\mathrm{id}}$, we have $d_{\hat{\mu}}^2 \neq 1$. In particular, up to isomorphism, there is no other invertible object in $\mathcal{C}$ than $\mathbb{1}$, which implies statement (ii). Moreover, by (2.5), we find

$$\hat{\mu}\left(\frac{d_{\mathbb{1}}^2}{\dim(\mathcal{C})}\right) = \hat{\mu}\left(\frac{1}{\dim(\mathcal{C})}\right) = \frac{d_{\hat{\mu}}^2}{\dim(\mathcal{C})}. \tag{3.9}$$

Hence,

$$\frac{\dim(\mathcal{C})}{\hat{\mu}(\dim(\mathcal{C}))} = d_{\hat{\mu}}^2 \neq 1,$$

and we have completed the proof of statement (i).

Since $\mathbb{Q}(\dim(\mathcal{C}))$ is a subfield of $\mathbb{Q}(S)$, it is abelian and hence Galois over $\mathbb{Q}$. By (i), there is no nontrivial element of $G_{\mathcal{C}}$ fixing $\dim(\mathcal{C})$. By the Fundamental Theorem of Galois theory, $\mathbb{Q}(\dim(\mathcal{C})) = \mathbb{Q}(S)$. By the definition of $\mathbb{Q}(S)$, we always have the inclusions

$$\mathbb{Q}(\dim(\mathcal{C})) \subseteq \mathbb{Q}(d_{\hat{\mu}} \mid \hat{\mu} \in G_{\mathcal{C}}) \subseteq \mathbb{Q}(S).$$

The equality $\mathbb{Q}(\dim(\mathcal{C})) = \mathbb{Q}(S)$ implies $\mathbb{Q}(S) = \mathbb{Q}(d_{\hat{\mu}} \mid \hat{\mu} \in G_{\mathcal{C}})$. □

Corollary 3.6. *If $\mathcal{C}$ is a transitive modular category, then the underlying braided fusion category has a unique pivotal structure up to isomorphism.*

Proof. By [11, Lem. 2.4], there is a bijective correspondence between $\mathrm{Irr}(\mathcal{C}_{\mathrm{pt}})$ and isomorphism classes of pivotal structures of the underlying fusion category of $\mathcal{C}$. By Theorem 3.5 (ii), $\mathrm{Irr}(\mathcal{C}_{\mathrm{pt}})$ is trivial since $\mathcal{C}$ is transitive. Therefore, the underlying pivotal structure of the modular category $\mathcal{C}$ is the only one up to isomorphism. □

Recall that a fusion category $\mathcal{C}$ is called *weakly integral* if $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Z}$, and is said to be *trivial* if it is tensor equivalent to Vec.

Corollary 3.7. *If $\mathcal{C}$ is a transitive modular category and $\mathcal{D} \subset \mathcal{C}$ a nontrivial fusion subcategory, then $\dim(\mathcal{D}) \notin \mathbb{Z}$. In particular, $\mathcal{C}$ does not contain any nontrivial weakly integral fusion subcategories.*

Proof. Suppose $\mathcal{D}$ is a fusion subcategory of $\mathcal{C}$ such that $\dim(\mathcal{D}) \in \mathbb{Z}$. Let $\hat{\sigma}_0 \in G_{\mathcal{C}}$ be the canonical element realizing the Frobenius–Perron dimension in Corollary 3.4. Then $\hat{\sigma}_0(\dim(\mathcal{D})) = \mathrm{FPdim}(\mathcal{D})$ and hence $\mathrm{FPdim}(\mathcal{D}) \in \mathbb{Z}$. In other words, $\mathcal{D}$ is weakly integral. By [28, Prop. 8.27], for any $\hat{\mu} \in \mathrm{Irr}(\mathcal{D})$, $\hat{\sigma}_0(d_{\hat{\mu}}^2) = \mathrm{FPdim}(\hat{\mu})^2 \in \mathbb{Z}$. Therefore, $d_{\hat{\mu}}^2 \in \mathbb{Z}$. By Lemma 3.3, $d_{\hat{\mu}}$ is a real algebraic unit for any $\hat{\mu} \in G_{\mathcal{C}}$, and so $d_{\hat{\mu}}^2 = 1$. However, by Theorem 3.5, this means $\hat{\mu} = \hat{\mathrm{id}}$ and hence $\mathrm{Irr}(\mathcal{D}) = \{\mathbb{1}\}$. This proves the first statement of the corollary.

Note that every weakly integral fusion category $\mathcal{B}$ satisfies $\mathrm{FPdim}(\mathcal{B}) = \dim(\mathcal{B}) \in \mathbb{Z}$ (cf. [28]). Therefore, if $\mathcal{B}$ is a weakly integral fusion subcategory of $\mathcal{C}$, then $\mathcal{B}$ must be trivial by the preceding assertion. □

Remark 3.8. As a consequence of Corollary 3.7, if $\mathcal{C}$ is a transitive modular category satisfying $\dim(\mathcal{C}) \in \mathbb{Z}$, then $\mathcal{C}$ is trivial.

In the following, we study fusion subcategories and Deligne products of transitive modular categories.

Corollary 3.9. *Every fusion subcategory of a transitive modular category $\mathcal{C}$ is a modular subcategory of $\mathcal{C}$.*

Proof. Let $\mathcal{D}$ be a fusion subcategory of $\mathcal{C}$. Then $\mathcal{D}$ is premodular with the braiding and the spherical pivotal structure inherited from $\mathcal{C}$. Now consider the Müger center $\mathcal{D}' = C_{\mathcal{D}}(\mathcal{D})$ of $\mathcal{D}$. It is a symmetric fusion subcategory of $\mathcal{D}$ and hence of $\mathcal{C}$. Then, by [20,21], $\dim(\mathcal{D}')$ is an integer. By Corollary 3.7, $\mathcal{D}'$ is equivalent Vec as a fusion category. Therefore, $\mathcal{D}$ is modular. □

Example 3.10. The adjoint subcategory $\mathcal{C} := \mathcal{C}(\mathfrak{sl}_2, 3)^{(0)}$ of the quantum group modular category $\mathcal{C}(\mathfrak{sl}_2, 3)$ is a Fibonacci modular category. It has two isomorphism classes of simple objects $\mathbb{1}$ and τ such that $\tau \otimes \tau = \mathbb{1} \oplus \tau$ (cf. [48]). The S-matrix of $\mathcal{C}$ is given by

$$S = \begin{pmatrix} 1 & d_\tau \\ d_\tau & -1 \end{pmatrix}$$

where $d_\tau = \frac{1+\sqrt{5}}{2}$. Therefore, $\mathbb{Q}(S) = \mathbb{Q}(\sqrt{5})$ and $G_\mathcal{C} \cong \mathbb{Z}_2$ with the generator $\hat{\sigma} : \sqrt{5} \mapsto -\sqrt{5}$. Therefore, $\mathcal{C}$ is transitive.

Recall that a modular category $\mathcal{C}$ is *prime* if every modular subcategory of $\mathcal{C}$ is equivalent to $\mathcal{C}$ or Vec. By [39, Thm. 4.5], every modular category admits a *prime factorization*, i.e., it is equivalent to a finite Deligne product of prime modular categories.

Theorem 3.11. *Let $\mathcal{C}$ be a transitive modular category. Then:*

(i) *every fusion subcategory of $\mathcal{C}$ is a transitive modular subcategory, and*
(ii) *the prime factorization of $\mathcal{C}$ is unique up to permutation of factors.*

Proof. Let $\mathcal{A}$ be an arbitrary fusion subcategory of $\mathcal{C}$. It follows from Corollary 3.9 that $\mathcal{A}$ is a modular subcategory of $\mathcal{C}$. Let $\mathcal{B} := C_\mathcal{C}(\mathcal{A})$, the Müger centralizer of $\mathcal{A}$ in $\mathcal{C}$. Then we have an equivalence of modular categories

$$\mathcal{C} \simeq \mathcal{A} \boxtimes \mathcal{B}$$

by the double centralizer theorem [39, Thm. 4.2].

As noted in Section 2.3, for any $X \boxtimes Y \in \mathrm{Irr}(\mathcal{C}) = \mathrm{Irr}(\mathcal{A} \boxtimes \mathcal{B})$ and any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have $\hat{\sigma}_\mathcal{C}(X \boxtimes Y) = \hat{\sigma}_\mathcal{A}(X) \boxtimes \hat{\sigma}_\mathcal{B}(Y)$. Since $\mathcal{C}$ is transitive, for any $X \in \mathrm{Irr}(\mathcal{A})$, there exists $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that

$$\hat{\sigma}_\mathcal{A}(\mathbb{1}_\mathcal{A}) \boxtimes \hat{\sigma}_\mathcal{B}(\mathbb{1}_\mathcal{B}) = \hat{\sigma}_\mathcal{C}(\mathbb{1}_\mathcal{A} \boxtimes \mathbb{1}_\mathcal{B}) = X \boxtimes \mathbb{1}_\mathcal{B}.$$

Therefore, $G_\mathcal{A}$ acts transitively on $\mathrm{Irr}(\mathcal{A})$. This completes the proof of (i).

It follows from [39, Thm. 4.5] that $\mathcal{C}$ admits a prime factorization. By Corollary 3.7, $\mathcal{C}_{\mathrm{pt}} \simeq \mathrm{Vec}$. Therefore, by [17, Prop. 2.2], the prime factorization of $\mathcal{C}$ is unique up to permutation of factors. □

Proposition 3.12. *If $\mathcal{A}, \mathcal{B}$ are transitive modular categories and $\mathcal{C} = \mathcal{A} \boxtimes \mathcal{B}$, then*

$$|\mathrm{Orb}(\mathcal{C})| = \frac{|G_\mathcal{A}| \cdot |G_\mathcal{B}|}{|G_\mathcal{C}|} = [\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) : \mathbb{Q}]. \tag{3.10}$$

In particular, if $\mathcal{A}, \mathcal{B}$ are nontrivial modular categories and they are Galois conjugate to each other, then $\mathcal{A} \boxtimes \mathcal{B}$ is not transitive.

Proof. Since $\mathcal{A}, \mathcal{B}$ are transitive, as discussed at the beginning of this section, the action of $G_\mathcal{A}$ (resp. $G_\mathcal{B}$) on $\mathrm{Irr}(\mathcal{A}) = G_\mathcal{A}$ (resp. $G_\mathcal{B} = \mathrm{Irr}(\mathcal{B})$) is just the left multiplication. By Lemma 2.1, $G_\mathcal{A} \bullet G_\mathcal{B} \cong G_\mathcal{C}$ is a subgroup of $G_\mathcal{A} \times G_\mathcal{B}$, and the action of $G_\mathcal{C}$ on $\mathrm{Irr}(\mathcal{C}) = \mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B}) = G_\mathcal{A} \times G_\mathcal{B}$ is equivalent to the left multiplication by $G_\mathcal{A} \bullet G_\mathcal{B}$. Therefore, the orbits of this $G_\mathcal{A} \bullet G_\mathcal{B}$-action are the cosets of $G_\mathcal{A} \bullet G_\mathcal{B}$ in $G_\mathcal{A} \times G_\mathcal{B}$, which implies the first equality in (3.10). The second equality in (3.10) is a direct application of Lemma 2.1(i) and Theorem 3.5(iii).

Suppose $\mathcal{A}$ and $\mathcal{B}$ are nontrivial Galois conjugate modular categories. Then the extension $\mathbb{Q}(\dim(\mathcal{A})) = \mathbb{Q}(\dim(\mathcal{B}))$ and $\mathbb{Q}(\dim(\mathcal{A}))$ is a proper extension of $\mathbb{Q}$ (cf. Theorem 3.5). Therefore, we have

$$|\operatorname{Orb}(\mathcal{A} \boxtimes \mathcal{B})| = [\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) : \mathbb{Q}] = [\mathbb{Q}(\dim(\mathcal{A})) : \mathbb{Q}] > 1,$$

which means $\mathcal{A} \boxtimes \mathcal{B}$ is not transitive. This completes the proof of the last assertion. □

The following corollary provides a necessary and sufficient condition for the transitivity of a Deligne product.

Corollary 3.13. *Let $\mathcal{C}$, $\mathcal{D}$ be modular categories. Then $\mathcal{C} \boxtimes \mathcal{D}$ is transitive if and only if the following two conditions hold: both $\mathcal{C}$, $\mathcal{D}$ are transitive and*

$$\mathbb{Q}(\dim(\mathcal{C})) \cap \mathbb{Q}(\dim(\mathcal{D})) = \mathbb{Q}.$$

Proof. If $\mathcal{C} \boxtimes \mathcal{D}$ is transitive, then, by Theorem 3.11, $\mathcal{C}$ and $\mathcal{D}$ are also transitive. By Proposition 3.12, $1 = |\operatorname{Orb}(\mathcal{C} \boxtimes \mathcal{D})| = [\mathbb{Q}(\dim(\mathcal{C})) \cap \mathbb{Q}(\dim(\mathcal{D})) : \mathbb{Q}]$, and so $\mathbb{Q}(\dim(\mathcal{C})) \cap \mathbb{Q}(\dim(\mathcal{D})) = \mathbb{Q}$.

Conversely, assume $\mathcal{C}$ and $\mathcal{D}$ are transitive modular categories and $\mathbb{Q}(\dim(\mathcal{C})) \cap \mathbb{Q}(\dim(\mathcal{D})) = \mathbb{Q}$, then $[\mathbb{Q}(\dim(\mathcal{C})) \cap \mathbb{Q}(\dim(\mathcal{D})) : \mathbb{Q}] = 1$. It follows from Proposition 3.12 that $\mathcal{C} \boxtimes \mathcal{D}$ is transitive. □

4. Primality of Transitive Quantum Group Modular Categories

A quantum group modular category $\mathcal{C}(\mathfrak{g}, k)$ can be constructed from a simple Lie algebra $\mathfrak{g}$ and a positive integer k, which is called the *level*. This modular category is a semisimplification of the tilting module category of the quantum group $U_q(\mathfrak{g})$ specialized at a root of unity q determined by k and $\mathfrak{g}$. The readers are referred to [3,49] and the references therein for details.

In this paper, we focus on the cases when $\mathfrak{g} = \mathfrak{sl}_2$. Let k be a positive integer and $q = \exp\left(\frac{\pi i}{k+2}\right)$. For any $r \in \mathbb{Q}$, we define

$$q^r := \exp\left(\frac{\pi i r}{k+2}\right).$$

The quantum integer $[n]_\zeta$ for any root of unity $\zeta \neq \pm 1$ is defined as

$$[n]_\zeta := \frac{\zeta^n - \zeta^{-n}}{\zeta - \zeta^{-1}}.$$

The isomorphism classes of simple objects of $\mathcal{C}(\mathfrak{sl}_2, k)$ are indexed by the integers $a \in [0, k]$. The modular data (S, T) of the modular category $\mathcal{C}(\mathfrak{sl}_2, k)$ is given by (cf. [3], see also [47] with a different convention)

$$S_{a,b} = [(a+1)(b+1)]_q, \quad T_{a,b} = \delta_{a,b}\, q^{a(a+2)/2}, \quad 0 \leq a, b \leq k. \tag{4.11}$$

One can replace q by any Galois conjugate $q' = q^l$ for some l relatively prime to $2(k+2)$ to get another modular category $\mathcal{C}(\mathfrak{sl}_2, k, q^l)$. The simple objects of this modular category are also indexed by the integers in $[0, k]$ and its modular data is also given by (4.11) with q replaced by q^l.

For the discussions of the remainder of this paper, we will simply write $\mathcal{A}_{k,l}$ for the modular category $\mathcal{C}(\mathfrak{sl}_2, k, q^l)$ where $\gcd(l, 2(k+2)) = 1$. Let V_a denote the isomorphism class of the simple objects of $\mathcal{A}_{k,l}$ indexed by the integer $a \in [0, k]$. Then V_0 is the isomorphism class of the tensor unit $\mathbb{1}$. The fusion rules of $\mathcal{A}_{k,l}$ are the same for any possible integer l, and they are given by (cf. [3])

$$N_{a,b}^c = \begin{cases} 1, & \text{if } |a-b| \le c \le \min(a+b, 2k-a-b) \\ & \qquad \text{and } c \equiv a+b \pmod 2; \\ 0, & \text{otherwise.} \end{cases} \tag{4.12}$$

One can observe directly from the fusion rules that $\mathcal{A}_{k,l}$ is $\mathbb{Z}_2$-graded, where the homogeneous component $A_{k,l}^{(j)}$, $j \in \{0, 1\}$, is the $\mathbb{C}$-linear subcategory (additively) generated by the simple objects V_a satisfying $a \equiv j \pmod 2$ for any integer $a \in [0, k]$. Moreover, the adjoint fusion subcategory of $\mathcal{A}_{k,l}$ is $\mathcal{A}_{k,l}^{(0)}$, which is a modular subcategory of $\mathcal{A}_{k,l}$ if and only if k is odd (cf. [6,51]), and

$$\mathrm{Irr}(\mathcal{A}_{k,l}^{(0)}) = \left\{ V_{2j} \mid 0 \le j \le \frac{k-1}{2} \right\}. \tag{4.13}$$

In particular, when $k = 1$, $\mathcal{A}_{1,l}^{(0)}$ is tensor equivalent to Vec , and when $k = 3$, $\mathcal{A}_{3,l}^{(0)}$ is a Fibonacci modular category (see Example 3.10).

For any fusion category $\mathcal{C}$, we say that a simple object $X \in \mathrm{Irr}(\mathcal{C})$ *tensor generates* $\mathcal{C}$ if every simple object of $\mathcal{C}$ is isomorphic to a summand of a tensor power of X. The following observation could be known to experts but we include it here for completeness.

Lemma 4.1. *For any positive odd integer k and $l \in (\mathbb{Z}/2(k+2)\mathbb{Z})^\times$, every nontrivial simple object of $\mathcal{A}_{k,l}^{(0)}$ tensor generates $\mathcal{A}_{k,l}^{(0)}$. In particular, $\mathcal{A}_{k,l}^{(0)}$ is a prime modular category.*

Proof. Since $\mathcal{A}_{1,l}^{(0)}$ is trivial, the statements are true for $k = 1$. We assume $k \ge 3$. By the fusion rules (4.12), when $k = 3$, $V_2 \otimes V_2 = V_0 \oplus V_2$; when $k > 3$ is odd, for any $1 \le j \le \frac{k-3}{2}$, we have

$$V_{2j} \otimes V_2 = V_{2j-2} \oplus V_{2j} \oplus V_{2j+2}.$$

Therefore, V_2 tensor generates $\mathcal{A}_{k,l}^{(0)}$. Moreover, for any $1 \le j \le \frac{k-1}{2}$, we have $2 \le \min(4j, 2k-4j)$, so $N_{2j,2j}^2 = 1$, which means V_2 is a direct summand of $V_{2j} \otimes V_{2j}$. Therefore, V_{2j} tensor generates $\mathcal{A}_{k,l}^{(0)}$. □

For any odd integer k and $l \in (\mathbb{Z}/2(k+2)\mathbb{Z})^\times$, the modular data $(S^{(0)}, T^{(0)})$ of $\mathcal{A}_{k,l}^{(0)}$ is indexed by $j = 0, \ldots, \frac{k-1}{2}$, and is given by

$$S_{j,m}^{(0)} = [(2j+1)(2m+1)]_{q^l}, \quad T_{j,m}^{(0)} = \delta_{m,j} q^{2lj(j+1)}, \quad 0 \le j, m \le \frac{k-1}{2}. \tag{4.14}$$

It is well-known that the first central charge of $\mathcal{A}_{k,1}$ is given by (cf. [3])

$$\xi_1(\mathcal{A}_{k,1}) = \exp\left(\frac{3k\pi i}{4(k+2)}\right).$$

By definition (see (2.4)), the first anomaly of $\mathcal{A}_{k,1}$ is

$$\alpha_1(\mathcal{A}_{k,1}) = \xi_1(\mathcal{A}_{k,1})^2 = \exp\left(\frac{3k\pi i}{2(k+2)}\right).$$

By the fusion rules, $\mathrm{Irr}((\mathcal{A}_{k,1})_{\mathrm{pt}}) = \{V_0, V_k\}$, and $(\mathcal{A}_{k,1})_{\mathrm{pt}}$ is a modular subcategory of $\mathcal{A}_{k,1}$. By [23, Cor. 3.27], $C_{\mathcal{A}_{k,1}}((\mathcal{A}_{k,1})_{\mathrm{pt}}) = \mathcal{A}_{k,1}^{(0)}$. Therefore,

$$\mathcal{A}_{k,1} \simeq \mathcal{A}_{k,1}^{(0)} \boxtimes (\mathcal{A}_{k,1})_{\mathrm{pt}}$$

as modular categories by the double centralizer theorem [39, Thm. 4.2]. Consequently, by [44, Lemma 3.12], $\alpha_1(\mathcal{A}_{k,1}) = \alpha_1(\mathcal{A}_{k,1}^{(0)}) \cdot \alpha_1((\mathcal{A}_{k,1})_{\mathrm{pt}})$. Following (4.11), we have

$$\alpha_1((\mathcal{A}_{k,1})_{\mathrm{pt}}) = \frac{1+i^k}{1-i^k} = i^k.$$

Therefore,

$$\alpha_1(\mathcal{A}_{k,1}^{(0)}) = \frac{\alpha_1(\mathcal{A}_{k,1})}{\alpha_1((\mathcal{A}_{k,1})_{\mathrm{pt}})} = \exp\left(\frac{(1-k)k\pi i}{2(k+2)}\right). \tag{4.15}$$

In the literature, $\mathcal{A}_{k,1}^{(0)}$ is often referred to as the quantum group modular category "SO(3) at level k" or "PSU(2) at level k". The ribbon categories with these fusion rules for odd k are completely classified in [30, Cor. 8.2.7], with a slightly different parametrization.

Lemma 4.2. *For any positive odd integer k, the modular categories*

$$\mathcal{A}_{k,l}^{(0)}, \quad l \in \left(\frac{\mathbb{Z}}{2(k+2)\mathbb{Z}}\right)^{\times}$$

form a complete list of inequivalent ribbon categories with the fusion rules of SO(3) *at level k. If $k+2 = p > 3$ is a prime, each of these modular categories is equivalent to a Galois conjugate of $\mathcal{A}_{p-2,1}^{(0)} = \mathcal{C}(\mathfrak{sl}_2, p-2)^{(0)}$.*

Proof. The first part follows directly from [30, Cor. 8.2.7]. If $k+2 = p > 3$ is a prime, there are exactly $|(\mathbb{Z}/2p\mathbb{Z})^{\times}| = p-1$ equivalence classes of ribbon categories with the fusion rules of SO(3) at level k. Note that all Galois conjugates of $\mathcal{A}_{k,1}^{(0)}$ have the same fusion rules. Hence, they are equivalent to the modular categories in the list. According to (4.15), $\alpha_1(\mathcal{A}_{p-2,1}^{(0)}) = \exp\left(\frac{(3-p)(p-2)\pi i}{2p}\right) \in \mathbb{Q}_p$, which is a root of unity of order p or $2p$ for $p > 3$. By definition, the first anomalies of the Galois conjugates of $\mathcal{A}_{k,1}^{(0)}$ are the Galois conjugates of $\alpha_1(\mathcal{A}_{k,1}^{(0)})$. Therefore, there are at least $\varphi(p) = p-1$ equivalence classes among the Galois conjugates of $\mathcal{A}_{k,1}^{(0)}$, and we are done by the first assertion. □

Now, we can show a family of these quantum group modular categories are prime and transitive in the following proposition.

Proposition 4.3. *Let p be any odd prime and $l \in (\mathbb{Z}/2p\mathbb{Z})^{\times}$. Then the modular category $\mathcal{A}_{p-2,l}^{(0)}$ is prime and transitive.*

Proof. By Lemma 4.1, $\mathcal{A}^{(0)}_{p-2,l}$ is prime. Therefore, it suffices to show that $\mathcal{A}^{(0)}_{p-2,l}$ is transitive.

The underlying root of unity q^l is the primitive $2p$-th root of unity. Since p is odd, $\mathbb{Q}_p = \mathbb{Q}(q^l) = \mathbb{Q}(q^{2l})$, it suffices to show that $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ acts transitively on $\mathrm{Irr}(\mathcal{A}^{(0)}_{p-2,l})$.

For any nonnegative integer $m \leq \frac{p-3}{2}$, $\gcd(2m+1, 2p) = 1$. So there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ such that $\sigma(q) = q^{2m+1}$. Thus, we have

$$\sigma\left(\frac{S^{(0)}_{j,0}}{S^{(0)}_{0,0}}\right) = \sigma([(2j+1)]_{q^l}) = \frac{[(2j+1)(2m+1)]_{q^l}}{[2m+1]_{q^l}} = \frac{S^{(0)}_{j,m}}{S^{(0)}_{0,m}}$$

for any nonnegative integer $j \leq \frac{p-3}{2}$. Therefore, $\hat{\sigma}(V_0) = V_{2m}$ and hence $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ acts transitively on $\mathrm{Irr}(\mathcal{A}^{(0)}_{p-2,l})$. □

Proposition 4.4. *Let $p_1, \ldots, p_\ell > 3$ be distinct primes. For any $(l_1, \ldots, l_\ell) \in (\mathbb{Z}/2p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/2p_\ell\mathbb{Z})^\times$, the Deligne product*

$$\mathcal{C} = \mathcal{A}^{(0)}_{p_1-2,l_1} \boxtimes \cdots \boxtimes \mathcal{A}^{(0)}_{p_\ell-2,l_\ell}$$

is a transitive modular category.

Proof. We proceed to prove the statement by induction on ℓ. The statement obviously holds for $\ell = 1$ by Proposition 4.3. Now we assume $p_1, \ldots, p_\ell > 3$ are distinct primes and $(l_1, \ldots, l_\ell) \in (\mathbb{Z}/2p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/2p_\ell\mathbb{Z})^\times$ for some integer $\ell > 1$. By the induction assumption, $\mathcal{C} = \boxtimes_{a=1}^{\ell-1} \mathcal{A}^{(0)}_{p_a-2,l_a}$ is a transitive modular category. Note that

$$\dim(\mathcal{C}) = \prod_{a=1}^{\ell-1} \dim(\mathcal{A}^{(0)}_{p_a-2,l_a}) \in \mathbb{Q}_{p'_\ell} \quad \text{and} \quad \dim(\mathcal{A}^{(0)}_{p_\ell-2,l_\ell}) \in \mathbb{Q}_{p_\ell},$$

where $p'_\ell = p_1 \ldots p_{\ell-1}$. Since $\mathbb{Q}_{p'_\ell} \cap \mathbb{Q}_{p_\ell} = \mathbb{Q}$, it follows from Corollary 3.13 and Proposition 4.3 that $\mathcal{C} \boxtimes \mathcal{A}^{(0)}_{p_\ell-2,l_\ell}$ is transitive. □

5. Representations of $\mathrm{SL}_2(\mathbb{Z})$ Associated with Modular Categories

In this section, we show that the representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with transitive modular categories are irreducible and minimal. As a consequence, the order of the T-matrix of any nontrivial transitive modular category is square-free and its prime factors are greater than 3.

Let $\mathcal{C}$ be a modular category with modular data (S, T). We denote by $\mathrm{GL}_\mathcal{C}(\mathbb{C})$ the group of all invertible matrices over $\mathbb{C}$ indexed by $\mathrm{Irr}(\mathcal{C})$, and $V_\mathcal{C} = K_0(\mathcal{C}) \otimes_\mathbb{Z} \mathbb{C}$ with the standard basis $E_\mathcal{C} = \{e_X \mid X \in \mathrm{Irr}(\mathcal{C})\}$. Note that $S, T \in \mathrm{GL}_\mathcal{C}(\mathbb{C})$, and the group $\mathrm{GL}_\mathcal{C}(\mathbb{C})$ acts on $V_\mathcal{C}$ via the standard basis $E_\mathcal{C}$, namely $A(e_Y) = \sum_{X \in \mathrm{Irr}(\mathcal{C})} A_{XY} e_X$ for any $A \in \mathrm{GL}_\mathcal{C}(\mathbb{C})$ and $Y \in \mathrm{Irr}(\mathcal{C})$. We often identify $\mathrm{GL}(V_\mathcal{C})$ with $\mathrm{GL}_\mathcal{C}(\mathbb{C})$ in this manner.

Recall that $\mathfrak{s} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mathfrak{t} := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are generators of the group $\mathrm{SL}_2(\mathbb{Z})$, subjected to the relations $\mathfrak{s}^4 = \mathrm{id}$ and $(\mathfrak{st})^3 = \mathfrak{s}^2$, and the assignment

$$\bar{\rho}_{\mathcal{C}} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PGL}(V_{\mathcal{C}}), \quad \mathfrak{s} \mapsto S, \quad \mathfrak{t} \mapsto T \tag{5.16}$$

defines a group homomorphism (cf. [3,52]). This projective representation $\overline{\rho}_{\mathcal{C}}$ can be lifted to an ordinary representation $(\rho, V_{\mathcal{C}})$ such that the diagram

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) & \xrightarrow{\rho} & \mathrm{GL}(V_{\mathcal{C}}) \\ & \searrow^{\overline{\rho}_{\mathcal{C}}} & \downarrow \\ & & \mathrm{PGL}(V_{\mathcal{C}}) \end{array}$$

commutes, where the vertical map $\mathrm{GL}(V_{\mathcal{C}}) \to \mathrm{PGL}(V_{\mathcal{C}})$ is the natural surjection. Any lifting $(\rho, V_{\mathcal{C}})$ of $\overline{\rho}_{\mathcal{C}}$, called a *representation of* $\mathrm{SL}_2(\mathbb{Z})$ *associated with* $\mathcal{C}$, yields an action of $\mathrm{SL}_2(\mathbb{Z})$ on $V_{\mathcal{C}}$ given by

$$\mathfrak{a} \cdot e_Y := \rho(\mathfrak{a})(e_Y) = \sum_{X \in \mathrm{Irr}(\mathcal{C})} \rho(\mathfrak{a})_{X,Y}(e_X)$$

for any $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$. We call $V_{\mathcal{C}}$ an $\mathrm{SL}_2(\mathbb{Z})$-*module of* $\mathcal{C}$ throughout this paper. If $(\rho, V_{\mathcal{C}})$ is a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$, then the pair $(s, t) := (\rho(\mathfrak{s}), \rho(\mathfrak{t}))$, called the *normalized modular data*, uniquely determines ρ, and the matrices s, t are unitary and symmetric (cf. [28]). Moreover, the group of 1-dimensional representations of $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$ by tensor product (cf. [22]).

For any positive integer m, we denote by $\pi_m : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ the natural surjection. We say that a representation $\phi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_r(\mathbb{C})$ is of level m if $\phi = \tilde{\phi} \circ \pi_m$ for some representation $\tilde{\phi} : \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{GL}_r(\mathbb{C})$ and $m = \mathrm{ord}(\phi(\mathfrak{t}))$. By [22, Thm. II], if ρ is a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$, then ρ is of level $n = \mathrm{ord}(\rho(\mathfrak{t}))$ and $\rho(\mathfrak{a})_{X,Y} \in \mathbb{Q}_n$ for any $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$ and $X, Y \in \mathrm{Irr}(\mathcal{C})$. In particular, s, t are matrices defined over $\mathbb{Q}_n$. Thus, for $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, $({}^{\sigma}\rho, V_{\mathcal{C}})$ is also a representation of $\mathrm{SL}_2(\mathbb{Z})$ where ${}^{\sigma}\rho(\mathfrak{a}) = \sigma(\rho(\mathfrak{a}))$ for any $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$, and the corresponding σ-twisted $\mathrm{SL}_2(\mathbb{Z})$-action on $V_{\mathcal{C}}$ is denoted by

$${}^{\sigma}\mathfrak{a} \cdot v = {}^{\sigma}\rho(\mathfrak{a})(v) \tag{5.17}$$

for any $v \in V_{\mathcal{C}}$.

Let $(\rho, V_{\mathcal{C}})$ be a level n representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with a modular category $\mathcal{C}$. The action of the Galois group $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ on the normalized modular data (s, t) satisfies some interesting conditions as follows: for $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, there exists a sign function $\varepsilon_\sigma : \mathrm{Irr}(\mathcal{C}) \to \{\pm 1\}$ such that

$$\sigma(s_{X,Y}) = \varepsilon_\sigma(X) s_{\hat{\sigma}(X),Y} = \varepsilon_\sigma(Y) s_{X,\hat{\sigma}(Y)} \tag{5.18}$$

for any $X, Y \in \mathrm{Irr}(\mathcal{C})$(cf. [15,19]), and

$$\sigma^2(t_{X,X}) = t_{\hat{\sigma}(X),\hat{\sigma}(X)} \tag{5.19}$$

for any $X \in \mathrm{Irr}(\mathcal{C})$ (cf. [22, Thm. II (iii)]). Moreover, the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the normalized modular data via the restriction

$$\mathrm{res}^{\bar{\mathbb{Q}}}_{\mathbb{Q}_n} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}).$$

The condition of the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on s defines a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on $V_{\mathcal{C}}$. Let $g_\sigma \in \mathrm{GL}(V_{\mathcal{C}})$ be defined by

$$(g_\sigma)_{X,Y} := \varepsilon_\sigma(X)\, \delta_{\hat{\sigma}(X),Y}.$$

Then, (5.18) and (5.19) can be rewritten as

$$\sigma(s) = g_\sigma s = s g_\sigma^{-1}, \quad \sigma^2(t) = g_\sigma t g_\sigma^{-1}, \tag{5.20}$$

and the assignment

$$\phi_\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_{\mathcal{C}}), \quad \sigma \mapsto g_\sigma, \tag{5.21}$$

defines a group homomorphism (cf. [15]). Therefore, for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have

$${}^{\sigma^2}\rho(\mathfrak{a}) = g_\sigma \rho(\mathfrak{a}) g_\sigma^{-1} \quad \text{for all } \mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z}). \tag{5.22}$$

In particular, $(\rho, V_{\mathcal{C}}) \cong ({}^{\sigma^2}\rho, V_{\mathcal{C}})$ as representations of $\mathrm{SL}_2(\mathbb{Z})$.

Now, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $V_{\mathcal{C}}$ via the representation $(\phi_\rho, V_{\mathcal{C}})$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, namely

$$\sigma \cdot e_X := g_\sigma(e_X) = \varepsilon_\sigma(X)\, e_{\hat{\sigma}(X)} \tag{5.23}$$

for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $X \in \mathrm{Irr}(\mathcal{C})$. Thus, in view of [22, Thm. II (iii)] or (5.22), for any $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$, $v \in V_{\mathcal{C}}$ and $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have

$$\sigma \cdot (\mathfrak{a} \cdot v) = g_\sigma \rho(\mathfrak{a})(v) = g_\sigma \rho(\mathfrak{a}) g_\sigma^{-1} g_\sigma(v) = {}^{\sigma^2}\mathfrak{a} \cdot (\sigma \cdot v). \tag{5.24}$$

By [22, Thm. II (iv)], if $\sigma(\zeta_n) = \zeta_n^a$ for some integer a coprime to n, then

$$g_\sigma = \rho(\mathfrak{t}^a \mathfrak{s} \mathfrak{t}^b \mathfrak{s} \mathfrak{t}^a \mathfrak{s}^{-1}), \tag{5.25}$$

where b is an inverse of a modulo n. Therefore, the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on $V_{\mathcal{C}}$ is uniquely determined by ρ, and in light of (5.25), every $\mathrm{SL}_2(\mathbb{Z})$-submodule of $V_{\mathcal{C}}$ also inherits the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

5.1. Minimal representations of $\mathrm{SL}_2(\mathbb{Z})$. To proceed, we set up the following conventions. We will denote by $\mathrm{spec}(M)$ the set of the eigenvalues of an linear operator M on a finite-dimensional complex vector space. For any finite multiplicative abelian group A,

$$A^2 := \{a^2 \mid a \in A\}$$

is a subgroup of A of order $|A|/|\Omega_2(A)|$, where $\Omega_2(A)$ is the (largest) elementary 2-subgroup of A. In particular, for any positive integer m, $\Omega_2(\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}))$ is simply denoted by Ω_2^m and we define

$$\varphi_2(m) := \left|((\mathbb{Z}/m\mathbb{Z})^\times)^2\right| = \left|\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})^2\right|.$$

It is immediately seen that φ_2 is a multiplicative function. Moreover, for any prime p, we have

$$\varphi_2(p^m) = \begin{cases} \frac{1}{2}(p-1)p^{m-1} & \text{if } p \text{ is odd;} \\ 2^{m-3} & \text{if } p = 2 \text{ and } m \geq 3; \\ 1 & \text{if } p = 2 \text{ and } m = 1, 2. \end{cases} \tag{5.26}$$

Suppose (s, t) is a normalized modular data of a modular category $\mathcal{C}$. By (5.19), the assignment $(\sigma, \zeta) \mapsto \sigma^2(\zeta)$ defines a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on $\mathrm{spec}(t)$, and the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit of $t_{X,X}$, for any $X \in \mathrm{Irr}(\mathcal{C})$, is then given by

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cdot t_{X,X} = \{\sigma^2(t_{X,X}) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})\}$$

where $m = \mathrm{ord}(t_{X,X})$. In particular, $|\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cdot t_{X,X}| = \varphi_2(m)$. We denote by $\mathrm{spec}(t)/\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ the set of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbits of $\mathrm{spec}(t)$.

Lemma 5.1. *Let $(\rho, V_{\mathcal{C}})$ be a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with a modular category $\mathcal{C}$. If $(\rho|_W, W)$ is a subrepresentation of $(\rho, V_{\mathcal{C}})$, then $\mathrm{spec}(\rho(\mathfrak{t})|_W)$ is closed under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{spec}(\rho(\mathfrak{t}))$. In particular,*

$$\mathrm{spec}(\rho(\mathfrak{t})|_W)/\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \subseteq \mathrm{spec}(\rho(\mathfrak{t}))/\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}),$$

and every direct sum decomposition of the $\mathrm{SL}_2(\mathbb{Z})$ representation $(\rho, V_{\mathcal{C}})$ determines a partition of $\mathrm{spec}(\rho(\mathfrak{t}))/\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Proof. For any $\zeta \in \mathrm{spec}(\rho(\mathfrak{t}))$, $B_\zeta = \{e_X \mid \mathfrak{t} \cdot e_X = \zeta e_X\}$ is a basis for the corresponding eigenspace of $\rho(\mathfrak{t})$. Let $\zeta \in \mathrm{spec}(\rho(\mathfrak{t})|_W)$ and $w \in W \setminus \{0\}$ such that $\mathfrak{t} \cdot w = \zeta w$. Then w is a $\mathbb{C}$-linear combination of B_ζ. Thus, for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have ${}^{\sigma^2}\mathfrak{t} \cdot w = \sigma^2(\zeta)w$ and $\sigma^{-1} \cdot w \in W$ by (5.25). It follows from (5.24) that

$$\mathfrak{t} \cdot (\sigma^{-1} \cdot w) = \sigma^{-1} \cdot ({}^{\sigma^2}\mathfrak{t} \cdot w) = \sigma^2(\zeta)\, \sigma^{-1} \cdot w,$$

and so $\sigma^2(\zeta) \in \mathrm{spec}(\rho(\mathfrak{t})|_W)$. □

The minimal possible dimension of an $\mathrm{SL}_2(\mathbb{Z})$-submodule of $V_{\mathcal{C}}$ of the preceding proposition inspires the following definition.

Definition 5.2. A level m representation (ϕ, W) of $\mathrm{SL}_2(\mathbb{Z})$ is called *minimal* if $\dim(W) = \varphi_2(m)$ and

$$\mathrm{spec}(\phi(\mathfrak{t})) = \{\sigma^2(\zeta_m^l) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})\}$$

for some $l \in (\mathbb{Z}/m\mathbb{Z})^\times$. In this case, (ϕ, W) or the corresponding $\mathrm{SL}_2(\mathbb{Z})$-module is said to be *minimal of type l*.

Corollary 5.3. *Let $(\rho, V_{\mathcal{C}})$ be a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with a modular category $\mathcal{C}$. If $(\rho|_W, W)$ is a minimal subrepresentation of $(\rho, V_{\mathcal{C}})$, then $(\rho|_W, W)$ is irreducible.*

Proof. Since $(\rho, V_{\mathcal{C}})$ is of some level $n = \mathrm{ord}(t)$, $\ker(\rho|_W)$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let m be the level of $(\rho|_W, W)$. Since $(\rho|_W, W)$ is minimal, $\dim(W) = \varphi_2(m)$ and

$$\mathrm{spec}(\rho(\mathfrak{t})|_W) = \{\sigma^2(\zeta_m^l) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})\} \quad \text{for some } l \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

In particular, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts transitively on $\mathrm{spec}(\rho(\mathfrak{t})|_W)$. If $(\rho|_U, U)$ is a nontrivial subrepresentation of $(\rho|_W, W)$ and $\zeta \in \mathrm{spec}(\rho(\mathfrak{t})|_U)$, then the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit of ζ is $\mathrm{spec}(\rho(\mathfrak{t})|_W)$. Therefore,

$$\dim(U) \geq |\mathrm{spec}(\rho(\mathfrak{t})|_W)| = \varphi_2(m) = \dim(W).$$

Therefore, $U = W$ and hence $(\rho|_W, W)$ is irreducible. □

The following examples are building blocks of all the minimal irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$.

Example 5.4. For any odd prime p, there are precisely two inequivalent irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ of level p and dimension $\varphi_2(p) = (p-1)/2$, denoted by $(\eta_j^p, \mathbb{C}^{\varphi_2(p)})$ or simply η_j^p $(j = \pm 1)$, which can be described as follows (see, for example, [25, Sec. 4]). Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, and set $j = \left(\frac{a}{p}\right)$, the Legendre symbol of a modulo p. For any integers $x, y \in [1, (p-1)/2]$,

$$\eta_j^p(\mathfrak{s})_{x,y} = \frac{2i\,j}{\sqrt{p^*}} \sin\left(\frac{4\pi\,axy}{p}\right) \text{ and } \eta_j^p(\mathfrak{t})_{x,y} = \delta_{x,y} \exp\left(\frac{2\pi\,i\,ax^2}{p}\right) \tag{5.27}$$

where

$$\sqrt{p^*} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ -i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The representation type of η_j^p is independent of the choice of a with $\left(\frac{a}{p}\right) = j$. The standard basis for $\mathbb{C}^{\varphi_2(p)}$ is an eigenbasis of $\eta_j^p(\mathfrak{t})$ and the representation η_j^p is uniquely determined by $\mathrm{spec}(\eta_j^p(\mathfrak{t}))$, which is either $\{\sigma^2(\zeta_p) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})\}$ or $\{\sigma^2(\zeta_p^a) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})\}$ where a is quadratic nonresidue modulo p. In particular, $\eta_{\pm 1}^p$ are level p minimal representations of $\mathrm{SL}_2(\mathbb{Z})$.

Example 5.5. The isomorphism classes of 1-dimensional representations of $\mathrm{SL}_2(\mathbb{Z})$ form a cyclic group of order 12 under tensor product, and they are completely determined by the images of $\mathfrak{t}$. If x is a 12-th root of unity, we denote by χ_x the 1-dimensional representation of $\mathrm{SL}_2(\mathbb{Z})$ such that $\chi_x(\mathfrak{t}) = x$. In particular, $\chi_{\zeta_3}^{\pm 1} = \chi_{\zeta_3^{\pm 1}} = \eta_{\pm 1}^3$, and the level of χ_x is the order of x. Since $\mathrm{ord}(x) \mid 12$ and $\varphi_2(d) = 1$ for any positive integer $d \mid 12$, every 1-dimensional representation of $\mathrm{SL}_2(\mathbb{Z})$ is minimal.

We close this subsection with the following characterization of minimal irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ which extends the preceding examples to a general setting.

Lemma 5.6. *Let (ϕ, V) be a level n irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$. If (ϕ, V) is minimal of type l, then $n = d \cdot p_1 \dots p_\ell$ for some positive integer $d \mid 12$ and distinct primes $p_1, \dots, p_\ell \geq 5$. In this case, there exist unique $l_0 \in (\mathbb{Z}/d\mathbb{Z})^\times$ and $l_i \in (\mathbb{Z}/p_i\mathbb{Z})^\times$ such that $\zeta_n^l = \zeta_d^{l_0} \zeta_{p_1}^{l_1} \dots \zeta_{p_\ell}^{l_\ell}$ and*

$$\phi \cong \chi_x \otimes \eta_{j_1}^{p_1} \otimes \cdots \otimes \eta_{j_\ell}^{p_\ell},$$

where $x = \zeta_d^{l_0}$ and $j_i = \left(\frac{l_i}{p_i}\right)$. In particular, ϕ is uniquely determined by ζ_n^l up to equivalence.

Proof. Let p be a prime factor of n, and m a positive integer such that $n = p^m \cdot n_2$, where n_2 is a positive integer not divisible by p. Set $n_1 = p^m$. By the Chinese Remainder Theorem, there exist irreducible representations $\phi_i : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}(V_i)$ of level n_i such that

$$\phi \cong \phi_1 \otimes \phi_2.$$

Therefore, for any $\omega \in \mathrm{spec}(\phi(\mathfrak{t}))$,

$$\omega = \omega_1 \cdot \omega_2$$

where $\omega_i \in \mathrm{spec}(\phi_i(\mathfrak{t}))$. Since (ϕ, V) is minimal of type l, $\omega = \sigma^2(\zeta_n^l)$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, which means it is a primitive n-th root of unity. Thus, ω_i is primitive n_i-th root for $i = 1, 2$. Note that the group μ_n of n-th roots of unity is an internal direct product of μ_{n_1} and μ_{n_2}, the pair (ω_1, ω_2) is uniquely determined by ω. More precisely, there exists a unique $l_i \in (\mathbb{Z}/n_i\mathbb{Z})^\times$ such that $l = l_i n/n_i$ in $\mathbb{Z}/n_i\mathbb{Z}$. Then

$$\zeta_n^l = \zeta_{n_1}^{l_1} \cdot \zeta_{n_2}^{l_2}$$

and

$$\omega_i = \sigma^2\left(\zeta_{n_i}^{l_i}\right)$$

for $i = 1, 2$. As σ runs through $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, we find

$$\{\sigma^2\left(\zeta_{n_i}^{l_i}\right) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_{n_i}/\mathbb{Q})\}$$

is a subset of $\mathrm{spec}(\phi_i(\mathfrak{t}))$. Therefore, $\dim(V_i) \geq \varphi_2(n_i)$ and so

$$\varphi_2(n) = \dim(V_1) \cdot \dim(V_2) \geq \varphi_2(n_1) \cdot \varphi_2(n_2) = \varphi_2(n).$$

This implies $\dim(V_i) = \varphi_2(n_i)$ and

$$\mathrm{spec}(\phi_i(\mathfrak{t})) = \{\sigma^2\left(\zeta_{n_i}^{l_i}\right) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_{n_i}/\mathbb{Q})\}.$$

Thus, both ϕ_1 and ϕ_2 are minimal of type l_1 and l_2 respectively.

The level p^m irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ were classified by [45,46] (see also [26, Tbl. 1–8]). Since ϕ_1 is an irreducible representation of level p^m and dimension $\varphi_2(p^m)$, whose values are given by (5.26), we find

$$m = \begin{cases} 1 & \text{if } p \text{ is odd;} \\ 1 \text{ or } 2 & \text{if } p = 2. \end{cases}$$

In this case, $\phi_1 \cong \eta_{\pm 1}^p$ if $p > 3$ (cf. Remark 5.4) and ϕ_1 is 1-dimensional if $p \leq 3$. Since p can be any prime factor of n, we obtain the factorization $n = d \cdot p_1 \dots p_\ell$ for some positive integer $d \mid 12$ and $p_1, ..., p_\ell$ are distinct primes greater than 3.

If one denotes the preceding irreducible representation ϕ_1 by ϕ^p, then, by induction, we have

$$\phi \cong \phi^d \otimes \bigotimes_{\substack{\text{prime } p>3 \\ p|n}} \phi^p, \quad \text{where} \quad \phi^d = \bigotimes_{\substack{\text{prime } p\leq 3 \\ p|n}} \phi^p$$

is 1-dimensional. There exist a unique integer $l_p \pmod p$ satisfying $l \equiv l_p n/p \pmod p$ for each odd prime divisor p of n, and a unique $l_0 \in (\mathbb{Z}/d\mathbb{Z})^\times$ satisfying $l \equiv l_0 n/d \pmod d$. Then, we have

$$\zeta_n^l = \zeta_d^{l_0} \prod_{\substack{\text{prime } p>3 \\ p|n}} \zeta_p^{l_p} \quad \text{and} \quad \zeta_d^{l_0} = \phi^d(\mathfrak{t}).$$

Therefore, $\phi^d = \chi_{\zeta_d^{l_0}}$ and $\phi^p = \eta_{j_p}^p$, where $j_p = \left(\frac{l_p}{p}\right)$ (cf. Examples 5.4 and 5.5). Consequently,

$$\phi \cong \chi_{\zeta_d^{l_0}} \otimes \bigotimes_{\substack{\text{prime } p>3 \\ p|n}} \eta_{j_p}^p.$$

□

5.2. Characteristic 2-group of modular categories. Let $\mathcal{C}$ be a modular category with the modular data (S, T). For any normalized modular data (s, t) of $\mathcal{C}$, $\mathbb{Q}(S) \subset \mathbb{Q}_N \subseteq \mathbb{Q}_n$, where $N = \text{ord}(T)$ and $n = \text{ord}(t)$ (cf. [22,43]). The restriction of the Galois automorphisms of $\mathbb{Q}_n$ to $\mathbb{Q}(S)$ defines an epimorphism $\text{res}_{\mathbb{Q}(S)}^{\mathbb{Q}_n} : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to G_{\mathcal{C}}$ of groups. Note that by [22, Prop. 6.7], we have

$$\ker(\text{res}_{\mathbb{Q}(S)}^{\mathbb{Q}_n}) = \text{Gal}(\mathbb{Q}_n/\mathbb{Q}(S)) \subseteq \Omega_2^n. \tag{5.28}$$

Definition 5.7. Let (s, t) be a normalized modular data of a modular category $\mathcal{C}$, and $n = \text{ord}(t)$. The image of the elementary 2-subgroup Ω_2^n of $\text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ under the restriction map $\text{res}_{\mathbb{Q}(S)}^{\mathbb{Q}_n} : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to G_{\mathcal{C}}$ is called the *characteristic 2-group* of $\mathcal{C}$, and denoted by $H_{\mathcal{C}}$.

In view of (5.28), we have the exact sequence of abelian groups:

$$1 \to \text{Gal}(\mathbb{Q}_n/\mathbb{Q}(S)) \xrightarrow{incl} \Omega_2^n \xrightarrow{\text{res}_{\mathbb{Q}(S)}^{\mathbb{Q}_n}} H_{\mathcal{C}} \to 1. \tag{5.29}$$

Proposition 5.8. *The characteristic 2-group $H_{\mathcal{C}}$ of $\mathcal{C}$ is independent of the choice of the normalized modular data (s, t) of $\mathcal{C}$. Moreover, if $n = \mathrm{ord}(t)$, then*

$$G_{\mathcal{C}}/H_{\mathcal{C}} \cong \frac{\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})}{\Omega_2^n}.$$

In particular, $|G_{\mathcal{C}}|/|H_{\mathcal{C}}| = \varphi_2(n)$.

Proof. Let (s, t) and (s', t') be normalized modular data of $\mathcal{C}$ and let $(\rho, V_{\mathcal{C}})$ and $(\rho', V_{\mathcal{C}})$ be the corresponding representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$ respectively. Then $\rho' \cong \chi \otimes \rho$ for some 1-dimensional character of $\mathrm{SL}_2(\mathbb{Z})$. Since $\chi^{12} = 1$, $t' = xt$ for some 12-th root of unity x. Let $m = \mathrm{ord}(t')$, and $l = \mathrm{lcm}(m, n)$. Then $\mathbb{Q}_l = \mathbb{Q}_m(x) = \mathbb{Q}_n(x)$. By definition, $\mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}_n}(\Omega_2^l) \subseteq \Omega_2^n$. For any $\sigma \in \Omega_2^n$, there exists an extension $\tau \in \mathrm{Gal}(\mathbb{Q}_l/\mathbb{Q})$ such that $\tau|_{\mathbb{Q}_n} = \sigma$. Since $x^{12} = 1$, $\tau^2(x) = x$. Thus, $\tau^2 = \mathrm{id}$ and hence $\tau \in \Omega_2^l$. Therefore,

$$\mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}_n}(\Omega_2^l) = \Omega_2^n.$$

By the same argument, we also have

$$\mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}_m}(\Omega_2^l) = \Omega_2^m.$$

Since the diagram

$$\begin{array}{ccc}
\mathrm{Gal}(\mathbb{Q}_l/\mathbb{Q}) & \xrightarrow{\mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}_m}} & \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}) \\
\downarrow{\scriptstyle \mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}_n}} & \searrow^{\mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}(S)}} & \downarrow{\scriptstyle \mathrm{res}^{\mathbb{Q}_m}_{\mathbb{Q}(S)}} \\
\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) & \xrightarrow[\mathrm{res}^{\mathbb{Q}_n}_{\mathbb{Q}(S)}]{} & G_{\mathcal{C}}
\end{array}$$

of restriction maps is commutative, we have

$$\mathrm{res}^{\mathbb{Q}_m}_{\mathbb{Q}(S)}(\Omega_2^m) = \mathrm{res}^{\mathbb{Q}_l}_{\mathbb{Q}(S)}(\Omega_2^l) = \mathrm{res}^{\mathbb{Q}_n}_{\mathbb{Q}(S)}(\Omega_2^n).$$

This proves the first assertion of the statement.

By (5.29), we also have the following commutative diagram of abelian groups with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(S)) & \xrightarrow{incl} & \Omega_2^n & \xrightarrow{\mathrm{res}^{\mathbb{Q}_n}_{\mathbb{Q}(S)}} & H_{\mathcal{C}} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle incl} & & \downarrow{\scriptstyle incl} & & \\
1 & \longrightarrow & \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(S)) & \xrightarrow{incl} & \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) & \xrightarrow{\mathrm{res}^{\mathbb{Q}_n}_{\mathbb{Q}(S)}} & G_{\mathcal{C}} & \longrightarrow & 1.
\end{array}$$

Therefore,

$$G_{\mathcal{C}}/H_{\mathcal{C}} \cong \frac{\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(S))}{\Omega_2^n/\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(S))} \cong \frac{\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})}{\Omega_2^n}.$$

□

Corollary 5.9. *Let $\mathcal{C}$ be a modular category with the modular data (S, T). If $N = \mathrm{ord}(T)$ is not a multiple of 4, then*

$$H_{\mathcal{C}} = \mathrm{res}^{\mathbb{Q}_N}_{\mathbb{Q}(S)}(\Omega_2^N).$$

Proof. Since $4 \nmid N$, by [22, Lem. 2.2], there exists a level N representation $(\rho, V_{\mathcal{C}})$ of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$. Therefore, $\rho(\mathfrak{t}) = t$ has order N. Now, the result follows directly from Definition 5.7 of $H_{\mathcal{C}}$. □

Example 5.10. Let A be a finite abelian group and $q : A \to \mathbb{C}^\times$ a nondegenerate quadratic form. The pointed modular category $\mathcal{C} = \mathcal{C}(A, q)$ has the S- and T-matrices given by

$$S_{a,b} = \frac{q(a)q(b)}{q(ab)}, \quad T_{a,b} = \delta_{a,b}q(a)$$

for any $a, b \in A$.

(i) If $|A|$ is odd, then $\mathbb{Q}(S) = \mathbb{Q}(T) = \mathbb{Q}_N$, where $N = \mathrm{ord}(T)$. Since $|A|$ is odd, and so is N. Therefore, by Corollary 5.9, $H_{\mathcal{C}} = \Omega_2^N$ is nontrivial.
(ii) If $A = \langle a \rangle$ is a cyclic group of order 2 and and $q(a) = \pm i$, then $\mathcal{C}$ is called a *semion category*. In this case, $\mathrm{ord}(T) = 4$ and $\mathbb{Q}(S) = \mathbb{Q}$. Therefore, $H_{\mathcal{C}}$ is trivial.

Let $(\rho, V_{\mathcal{C}})$ be a level n representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$, and (s, t) the corresponding normalized modular data. Since $\Omega_2^n \xrightarrow{\mathrm{res}} H_{\mathcal{C}}$ is an epimorphism of elementary 2-groups, there exists a subgroup $\tilde{H}_{\mathcal{C}} \subset \Omega_2^n$ such that

$$\mathrm{res}^{\mathbb{Q}_n}_{\mathbb{Q}(S)} : \tilde{H}_{\mathcal{C}} \xrightarrow{\sim} H_{\mathcal{C}} \tag{5.30}$$

is an isomorphism. Now, recall that the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on $V_{\mathcal{C}}$ via ϕ_ρ factors through $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ (cf. (5.21)). Therefore, $\tilde{H}_{\mathcal{C}}$ acts on $V_{\mathcal{C}}$ in the same way (cf. (5.23)), namely

$$\sigma \cdot e_X = g_\sigma(e_X) = \varepsilon_\sigma(X) e_{\hat{\sigma}(X)}$$

for any $\sigma \in \tilde{H}_{\mathcal{C}}$. One can decompose $V_{\mathcal{C}}$ as an $\tilde{H}_{\mathcal{C}}$-module into its isotypic components

$$V_{\mathcal{C}} = \bigoplus_{\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})} V_{\mathcal{C}}^{\chi},$$

where $\mathrm{Irr}(\tilde{H}_{\mathcal{C}})$ denotes the set of irreducible characters of $\tilde{H}_{\mathcal{C}}$, and $V_{\mathcal{C}}^{\chi}$ the isotypic component of $V_{\mathcal{C}}$ corresponding to the irreducible character χ of $\tilde{H}_{\mathcal{C}}$.

Proposition 5.11. *Let $\mathcal{C}$ be a modular category and $(\rho, V_{\mathcal{C}})$ a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$. Then for any $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$, the isotypic component $V_{\mathcal{C}}^{\chi}$ is an $\mathrm{SL}_2(\mathbb{Z})$-submodules of $V_{\mathcal{C}}$, and*

$$V_{\mathcal{C}} = \bigoplus_{\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})} V_{\mathcal{C}}^{\chi} \tag{5.31}$$

is a decomposition of $\mathrm{SL}_2(\mathbb{Z})$-modules. Moreover, if there exists a simple object $X \in \mathrm{Irr}(\mathcal{C})$ such that $\mathrm{Stab}_{H_{\mathcal{C}}}(X) = \{\mathrm{id}\}$, then all the $V_{\mathcal{C}}^{\chi}$'s are non-zero and pairwise inequivalent.

Proof. By (5.24), for any $v \in V_{\mathcal{C}}^{\chi}$, $\sigma \in \tilde{H}_{\mathcal{C}}$, and $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$,

$$\sigma \cdot (\mathfrak{a} \cdot v) = {}^{\sigma^2}\mathfrak{a} \cdot (\sigma \cdot v) = \chi(\sigma)\, \mathfrak{a} \cdot v.$$

Therefore, $V_{\mathcal{C}}^{\chi}$ is an $\mathrm{SL}_2(\mathbb{Z})$-invariant subspace of $(\rho, V_{\mathcal{C}})$, and the $\mathrm{SL}_2(\mathbb{Z})$-module decomposition (5.31) follows immediately.

Let χ, χ' be distinct irreducible characters of $\tilde{H}_{\mathcal{C}}$ such that $V_{\mathcal{C}}^{\chi} \neq 0$ and $V_{\mathcal{C}}^{\chi'} \neq 0$. Then, there exists $\sigma \in \tilde{H}_{\mathcal{C}}$ such that $\chi(\sigma) \neq \chi'(\sigma)$. By (5.25), $g_\sigma = \rho(\mathfrak{a})$ for some $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$, and the restrictions of $\rho(\mathfrak{a})$ on $V_{\mathcal{C}}^{\chi}$ and $V_{\mathcal{C}}^{\chi'}$ are the distinct scalars $\chi(\sigma)$ and $\chi'(\sigma)$ respectively. Therefore, $V_{\mathcal{C}}^{\chi}$ and $V_{\mathcal{C}}^{\chi'}$ are inequivalent representations of $\mathrm{SL}_2(\mathbb{Z})$.

For each $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$,

$$P_\chi := \frac{1}{|\tilde{H}_{\mathcal{C}}|} \sum_{\sigma \in \tilde{H}_{\mathcal{C}}} \chi(\sigma) g_\sigma$$

is an idempotent operator on $V_{\mathcal{C}}$ commuting with the action $\mathrm{SL}_2(\mathbb{Z})$ such that $V_{\mathcal{C}}^{\chi} = P_\chi(V_{\mathcal{C}})$. Therefore, $V_{\mathcal{C}}^{\chi} = 0$ if and only if $P_\chi = 0$. If $\{g_\sigma \mid \sigma \in \tilde{H}_{\mathcal{C}}\}$ is $\mathbb{C}$-linearly independent, then $P_\chi \neq 0$ and hence $V_{\mathcal{C}}^{\chi} \neq 0$ for all $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$.

Let $X \in \mathrm{Irr}(\mathcal{C})$ be such that $\mathrm{Stab}_{H_{\mathcal{C}}}(X) = \{\mathrm{id}\}$. Suppose $\sum_{\sigma \in \tilde{H}_{\mathcal{C}}} \alpha_\sigma g_\sigma = 0$ for some $\alpha_\sigma \in \mathbb{C}$. Then

$$\sum_{\sigma \in \tilde{H}_{\mathcal{C}}} \alpha_\sigma g_\sigma(e_X) = \sum_{\sigma \in \tilde{H}_{\mathcal{C}}} \alpha_\sigma \varepsilon_\sigma(X) e_{\hat{\sigma}(X)} = 0.$$

Since $\mathrm{Stab}_{H_{\mathcal{C}}}(X) = \{\mathrm{id}\}$, $\{e_{\hat{\sigma}(X)} \mid \hat{\sigma} \in H_{\mathcal{C}}\}$ is a set of distinct basis elements of $V_{\mathcal{C}}$ and hence $\alpha_\sigma = 0$ for all $\sigma \in \tilde{H}_{\mathcal{C}}$. Therefore, $\{g_\sigma \mid \sigma \in \tilde{H}_{\mathcal{C}}\}$ is $\mathbb{C}$-linearly independent, and so $V_{\mathcal{C}}^{\chi} \neq 0$ for all $\chi \in \tilde{H}_{\mathcal{C}}$. This completes the proof of the proposition. □

Proposition 5.12. *Let $(\rho, V_{\mathcal{C}})$ be a level n representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with a modular category $\mathcal{C}$. If ρ is irreducible, then $H_{\mathcal{C}}$ is trivial, the S-matrix of $\mathcal{C}$ is real, and $\mathcal{C}$ is self-dual. Moreover, there exists $X \in \mathrm{Irr}(\mathcal{C})$ such that $\rho(\mathfrak{t})_{X,X}$ is a primitive n-th root of unity.*

Proof. If ρ is an irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$, the decomposition (5.31) of ρ, determined by the characteristic 2-subgroup $H_{\mathcal{C}}$, must be trivial. Suppose there exists a nontrivial element $\hat{\sigma}$ in $H_{\mathcal{C}}$. Then $\hat{\sigma}(X) \neq X$ for some $X \in \mathrm{Irr}(\mathcal{C})$ and so the eigenspaces $E_\pm$ of g_σ corresponding to the eigenvalues ± 1 are nontrivial. Note that both E_+ and E_- are stable under the $\mathrm{SL}_2(\mathbb{Z})$ action, and $V_{\mathcal{C}} = E_+ \oplus E_-$. This contradicts the irreducibility of $V_{\mathcal{C}}$. Therefore, $H_{\mathcal{C}}$ is trivial.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ denote the complex conjugation. Then $\hat{\sigma}(X) = X^*$ for $X \in \mathrm{Irr}(\mathcal{C})$. Since $H_{\mathcal{C}}$ is trivial, $\sigma|_{\mathbb{Q}(S)} = \mathrm{id}$ and so $X^* = \hat{\sigma}(X) = X$ for $X \in \mathrm{Irr}(\mathcal{C})$. Therefore, $S_{\mathcal{C}}$ is real and $\mathcal{C}$ is self-dual.

Let $n = p_1^{n_1} \dots p_\ell^{n_\ell}$ be the prime factorization of n, where $p_1, \dots, p_\ell$ are distinct prime factors of n. Since ρ is irreducible, by the Chinese Remainder Theorem, there exists a level $p_i^{n_i}$ irreducible representation (ρ_i, V_i) of $\mathrm{SL}_2(\mathbb{Z})$ for each $i = 1, \dots, \ell$ such that

$$(\rho, V_{\mathcal{C}}) \cong (\rho_1, V_1) \otimes \cdots \otimes (\rho_\ell, V_\ell).$$

Since (ρ_i, V_i) is of level $p_i^{n_i}$, there exists a nonzero eigenvector $v_i \in V_i$ of $\rho_i(\mathrm{t})$ with an eigenvalue ω_i which is a primitive $p_i^{n_i}$-th root of unity. Thus, $\rho(\mathrm{t})$ has an eigenvalue $\zeta = \omega_1 \dots \omega_\ell$ which is a primitive n-th root of unity. Since $\{e_X \mid X \in \mathrm{Irr}(\mathcal{C})\}$ is an eigenbasis for $\rho(\mathrm{t})$, there exists $X \in \mathrm{Irr}(\mathcal{C})$ such that $\rho(\mathrm{t})_{X,X} = \zeta$. □

5.3. The $\mathrm{SL}_2(\mathbb{Z})$*-modules of transitive modular categories.* In this section, we show that the representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with any transitive modular category $\mathcal{C}$ is minimal and irreducible, and that the order of $T_\mathcal{C}$ is odd and square-free.

Let $\mathcal{C}$ be a transitive modular category, $(\rho, V_\mathcal{C})$ a level n representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$, and (s, t) the corresponding normalized modular data. As before, the Galois group $G_\mathcal{C}$ is identified with $\mathrm{Irr}(\mathcal{C})$ via the bijection $\hat{\sigma} \mapsto \hat{\sigma}(\mathbb{1})$. Then, we have

$$\mathrm{spec}(t) = \{t_{\hat{\sigma},\hat{\sigma}} \mid \hat{\sigma} \in G_\mathcal{C}\} = \{\sigma^2(\zeta) \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})\}, \tag{5.32}$$

where $\zeta = t_{\mathbb{1},\mathbb{1}}$. Here, the last equality is a consequence of (5.19). Therefore, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{spec}(t)$ transitively, and so every eigenvalue of t is a primitive n-th root of unity. In particular,

$$\mathbb{Q}(t) = \mathbb{Q}_n = \mathbb{Q}(\zeta).$$

Lemma 5.13. *The characteristic 2-group $H_\mathcal{C}$ is given by*

$$H_\mathcal{C} = \{\hat{\sigma} \in G_\mathcal{C} \mid t_{\hat{\sigma},\hat{\sigma}} = t_{\mathbb{1},\mathbb{1}}\}.$$

Moreover, for any $\hat{\sigma}, \hat{\tau} \in G_\mathcal{C}$, $t_{\hat{\sigma},\hat{\sigma}} = t_{\hat{\tau},\hat{\tau}}$ if and only if $\hat{\sigma} H_\mathcal{C} = \hat{\tau} H_\mathcal{C}$. In particular, each eigenvalue of t has algebraic multiplicity $|H_\mathcal{C}|$.

Proof. Let $\zeta = t_{\mathbb{1},\mathbb{1}}$. Since $\mathbb{Q}(\zeta) = \mathbb{Q}_n$, we have

$$\Omega_2^n = \{\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \mid \sigma^2(\zeta) = \zeta\} = \{\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \mid t_{\hat{\sigma},\hat{\sigma}} = \zeta\}.$$

Thus, if $\hat{\sigma} \in H_\mathcal{C}$, then there exists $\sigma \in \Omega_2^n$ such that $\sigma|_{\mathbb{Q}(S)} = \hat{\sigma}$, which means $t_{\hat{\sigma},\hat{\sigma}} = \zeta$. Conversely, if $\hat{\sigma} \in G_\mathcal{C}$ such that $t_{\hat{\sigma},\hat{\sigma}} = \zeta$, then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ such that $\sigma|_{\mathbb{Q}(S)} = \hat{\sigma}$. By (5.19), $\sigma^2(\zeta) = t_{\hat{\sigma},\hat{\sigma}} = \zeta$. Thus, $\sigma \in \Omega_2^n$, and hence $\hat{\sigma} \in H_\mathcal{C}$. This proves the first statement.

Let $\hat{\sigma}, \hat{\tau} \in G_\mathcal{C}$, and $\tau \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ such that $\tau|_{\mathbb{Q}(S)} = \hat{\tau}$. If $t_{\hat{\sigma},\hat{\sigma}} = t_{\hat{\tau},\hat{\tau}}$, then $t_{\hat{\sigma},\hat{\sigma}} = \tau^2(\zeta)$ or

$$\zeta = \tau^{-2}(t_{\hat{\sigma},\hat{\sigma}}) = t_{\hat{\tau}^{-1}\hat{\sigma},\hat{\tau}^{-1}\hat{\sigma}}.$$

Therefore, $\hat{\tau}^{-1}\hat{\sigma} \in H_\mathcal{C}$ and so $\hat{\tau} H_\mathcal{C} = \hat{\sigma} H_\mathcal{C}$. Conversely, if $\hat{\tau} H_\mathcal{C} = \hat{\sigma} H_\mathcal{C}$, then $\hat{\sigma} = \hat{\tau}\hat{\mu}$ for some $\hat{\mu} \in H_\mathcal{C}$, and hence

$$t_{\hat{\sigma},\hat{\sigma}} = t_{\hat{\tau}\hat{\mu},\hat{\tau}\hat{\mu}} = \tau^2(t_{\hat{\mu},\hat{\mu}}) = \tau^2(t_{\mathbb{1},\mathbb{1}}) = t_{\hat{\tau},\hat{\tau}}.$$

□

Now, we can prove the major theorem of this section.

Theorem 5.14. *Let $\mathcal{C}$ be a nontrivial transitive modular category. Then every representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$ is minimal and irreducible. Moreover, the order of the T-matrix T of $\mathcal{C}$ is odd and square-free, and every prime factor of $\mathrm{ord}(T)$ is greater than 3.*

Proof. Let $(\rho, V_{\mathcal{C}})$ be a level n representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$, and $H_{\mathcal{C}}$ the characteristic 2-group of $\mathcal{C}$. By Propositions 3.2 and 5.11, with $\tilde{H}_{\mathcal{C}}$ defined in (5.30), $V_{\mathcal{C}}$ admits an $\mathrm{SL}_2(\mathbb{Z})$-module decomposition

$$V_{\mathcal{C}} = \bigoplus_{\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})} V_{\mathcal{C}}^{\chi}$$

such that $V_{\mathcal{C}}^{\chi} \neq 0$ for all $\chi \in \tilde{H}_{\mathcal{C}}$. We proceed to determine $V_{\mathcal{C}}^{\chi}$ for each $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$.

Recall that the $\tilde{H}_{\mathcal{C}}$-action on $V_{\mathcal{C}}$ is given by

$$\sigma \cdot e_{\hat{\mu}} = g_{\sigma}(e_{\hat{\mu}}) = \varepsilon_{\sigma}(\hat{\mu}) e_{\hat{\sigma}\hat{\mu}}$$

for any $\sigma \in \tilde{H}_{\mathcal{C}}$ and $\hat{\mu} \in G_{\mathcal{C}}$. For any $\hat{\mu} \in G_{\mathcal{C}}$, the subspace $V_{\hat{\mu}}$ of $V_{\mathcal{C}}$ spanned by $\{e_{\hat{\sigma}\hat{\mu}} \mid \hat{\sigma} \in H_{\mathcal{C}}\}$ is closed under this $\tilde{H}_{\mathcal{C}}$-action, and $\mathfrak{t}$ acts as the scalar $t_{\hat{\mu},\hat{\mu}}$ on $V_{\hat{\mu}}$ by Lemma 5.13. Therefore, $V_{\hat{\mu}}$ admits an isotypic decomposition

$$V_{\hat{\mu}} = \bigoplus_{\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})} V_{\hat{\mu}}^{\chi}.$$

Since $g_{\mathrm{id}} = \mathrm{id}_{V_{\mathcal{C}}}$, the character $\psi_{\hat{\mu}}$ of $\tilde{H}_{\mathcal{C}}$ afforded by $V_{\hat{\mu}}$ is given by

$$\psi_{\hat{\mu}}(\sigma) = |H_{\mathcal{C}}| \cdot \delta_{\sigma,\mathrm{id}} \quad \text{for any } \sigma \in \tilde{H}_{\mathcal{C}}.$$

Therefore, as an $\tilde{H}_{\mathcal{C}}$-module, $V_{\hat{\mu}}$ is equivalent to the regular representation of $\tilde{H}_{\mathcal{C}}$. Consequently, $\dim(V_{\hat{\mu}}^{\chi}) = 1$ for each $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$.

Let Λ be a complete set of coset representatives of $H_{\mathcal{C}}$ in $G_{\mathcal{C}}$. Then,

$$V_{\mathcal{C}} = \bigoplus_{\hat{\mu} \in \Lambda} V_{\hat{\mu}}$$

is a decomposition of $\tilde{H}_{\mathcal{C}}$-modules. Therefore,

$$V_{\mathcal{C}}^{\chi} = \bigoplus_{\hat{\mu} \in \Lambda} V_{\hat{\mu}}^{\chi}$$

for each $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$, and $\dim(V_{\mathcal{C}}^{\chi}) = |G_{\mathcal{C}}|/|H_{\mathcal{C}}| = \varphi_2(n)$ by Proposition 5.8. Let $(\rho^{\chi}, V_{\mathcal{C}}^{\chi})$ denote the corresponding subrepresentation of $(\rho, V_{\mathcal{C}})$. Then

$$\mathrm{spec}(\rho^{\chi}(\mathfrak{t})) = \{t_{\hat{\sigma},\hat{\sigma}} \mid \hat{\sigma} \in \Lambda\} = \{\sigma^2(t_{\mathbb{1},\mathbb{1}}) \mid \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\}$$

by Lemma 5.13. Therefore, for any $\chi \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$, the level n representation $(\rho^{\chi}, V_{\mathcal{C}}^{\chi})$ of $\mathrm{SL}_2(\mathbb{Z})$ is minimal of type $l \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, where l is determined by $\zeta_n^l = t_{\mathbb{1},\mathbb{1}}$. Hence, by Corollary 5.3, $(\rho^{\chi}, V_{\mathcal{C}}^{\chi})$ is irreducible for each $\chi \in \tilde{H}_{\mathcal{C}}$.

It follows from Lemma 5.6 that $V_{\mathcal{C}}^{\chi} \cong V_{\mathcal{C}}^{\chi'}$ as $\mathrm{SL}_2(\mathbb{Z})$-modules for any $\chi, \chi' \in \mathrm{Irr}(\tilde{H}_{\mathcal{C}})$. In view of Proposition 5.11, $\tilde{H}_{\mathcal{C}}$ must be trivial and so does $H_{\mathcal{C}}$. Therefore, $(\rho, V_{\mathcal{C}})$ is minimal and irreducible, and $n = d \cdot p_1 \dots p_\ell$ where $d \mid 12$ and $p_1, \dots, p_\ell$ are distinct primes greater than 3. Moreover,

$$\rho \cong \chi \otimes \rho'$$

for some 1-dimensional representation χ and a level $m = p_1 \dots p_\ell$ minimal representation (ρ', V') of $\mathrm{SL}_2(\mathbb{Z})$. By tensoring ρ with the dual representation χ^* of χ, we find (ρ', V') is equivalent to a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$. By [22, Thm II (i)], we have

$$\mathrm{ord}(T) \mid m \mid 12\,\mathrm{ord}(T)$$

which implies $\mathrm{ord}(T) = m$ since $\gcd(m, 12) = 1$. □

6. Classification of Transitive Modular Categories

In this section, we prove that a nontrivial prime and transitive modular category must be equivalent to $\mathcal{A}^{(0)}_{p-2,l}$ for some prime $p > 3$ and $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$. In view of Theorem 3.11, we complete the classification of transitive modular categories in Theorem 6.5. The minimal irreducibility of the representations of $\mathrm{SL}_2(\mathbb{Z})$ associated with transitive modular categories is crucial to the characterization of the prime ones.

We begin with the realization of minimal irreducible representations of $\mathrm{SL}_2(\mathbb{Z})$ by transitive modular categories.

Lemma 6.1. *Let $p > 3$ be a prime. Then every level p minimal irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{A}^{(0)}_{p-2,l}$ for some $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$.*

Proof. Recall from Proposition 4.3 that $\mathcal{A}^{(0)}_{p-2,l}$ is a prime and transitive modular category for any prime $p > 3$ and $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$. Moreover, the order of the T-matrix of $\mathcal{A}^{(0)}_{p-2,l}$ is p. By [22, Lemma 2.2], there exists a level p representation $(\rho, \mathbb{C}^{\varphi_2(p)})$ of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{A}^{(0)}_{p-2,1}$, and we set $t = \rho(\mathfrak{t})$. Then, by Theorem 5.14, $(\rho, \mathbb{C}^{\varphi_2(p)})$ is a minimal irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$ of type a where $\zeta_p^a = t_{\mathbb{1},\mathbb{1}}$. Therefore, by Lemma 5.6,

$$(\rho, \mathbb{C}^{\varphi_2(p)}) \cong (\eta_j^p, \mathbb{C}^{\varphi_2(p)}), \quad \text{where } j = \left(\frac{a}{p}\right).$$

For any $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$, define $\sigma_l \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ by $\sigma_l(\zeta_p) = \zeta_p^l$. Since $\rho(\mathfrak{a})$ is a matrix over $\mathbb{Q}_p$ for any $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$ (cf. [22, Thm. II]), $\rho_l(\mathfrak{a}) := \sigma_l(\rho(\mathfrak{a}))$ defines another level p representation of $\mathrm{SL}_2(\mathbb{Z})$, and $(\rho_l, \mathbb{C}^{\varphi_2(p)})$ is a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{A}^{(0)}_{p-2,l}$. Since $\sigma_l(t_{\mathbb{1},\mathbb{1}}) = \zeta_p^{al}$, we have

$$(\rho_l, \mathbb{C}^{\varphi_2(p)}) \cong (\eta_{j_l}^p, \mathbb{C}^{\varphi_2(p)}), \quad \text{where } j_l = \left(\frac{al}{p}\right).$$

Therefore, every level p minimal irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{A}^{(0)}_{p-2,l}$ for some $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$, as desired. □

Corollary 6.2. *Let $n = p_1 \dots p_\ell$ for some distinct primes $p_1, \dots, p_\ell > 3$. Then every level n minimal irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated to a transitive modular category*

$$\mathcal{D} = \mathcal{A}^{(0)}_{p_1-2,l_1} \boxtimes \cdots \boxtimes \mathcal{A}^{(0)}_{p_\ell-2,l_\ell}$$

for some $l_a \in (\mathbb{Z}/2p_a\mathbb{Z})^\times$, $a = 1, \dots, \ell$.

Proof. Let (ϕ, V) be a level n minimal irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$. By Lemma 5.6, there exists level p_a minimal irreducible representation $(\eta^{p_a}_{j_a}, V_a)$ of $\mathrm{SL}_2(\mathbb{Z})$ for each $a = 1, \dots, \ell$ such that

$$(\phi, V) \cong (\eta^{p_1}_{j_1}, V_1) \otimes \cdots \otimes (\eta^{p_\ell}_{j_\ell}, V_\ell)$$

where $V_a = \mathbb{C}^{\varphi_2(p_a)}$. By Lemma 6.1, $(\eta^{p_a}_{j_a}, V_a)$ is equivalent to a representation $(\rho_a, V_{\mathcal{D}_a})$ of $\mathrm{SL}_2(\mathbb{Z})$ associated with a transitive modular category $\mathcal{D}_a = \mathcal{A}^{(0)}_{p_a-2,l_a}$ for some $l_a \in (\mathbb{Z}/2p_a\mathbb{Z})^\times$. Let $\mathcal{D} = \mathcal{D}_1 \boxtimes \cdots \boxtimes \mathcal{D}_\ell$. Then $\mathcal{D}$ is transitive by Proposition 4.4 and

$$(\rho, V_{\mathcal{D}}) = (\rho_1, V_{\mathcal{D}_1}) \otimes \cdots \otimes (\rho_\ell, V_{\mathcal{D}_\ell})$$

is a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{D}$. Now, we have

$$(\phi, V) \cong (\rho, V_{\mathcal{D}}).$$

□

Theorem 6.3. *Let $\mathcal{C}$ be a nontrivial prime and transitive modular category. Then the order of the T-matrix is a prime number greater than 3.*

Proof. By Theorem 5.14, $\mathrm{ord}(T_{\mathcal{C}}) = N$ is odd and has a prime factor $p > 3$. It follows from [22, Lem. 2.2] that there exists a level N representation $(\rho, V_{\mathcal{C}})$ of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$. Again, by Theorem 5.14, $(\rho, V_{\mathcal{C}})$ is minimal and irreducible.

Suppose N is not a prime. Then $N = pq$ for some odd square-free integer q not divisible by p and all the prime factors of q are greater than 3. In particular, $\varphi_2(q) > 1$. In view of Lemma 5.6, there exist minimal and irreducible $\mathrm{SL}_2(\mathbb{Z})$-representations (ϕ_1, V_1) and (ϕ_2, V_2) of levels p and q respectively such that

$$(\rho, V_{\mathcal{C}}) \cong (\phi_1, V_1) \otimes (\phi_2, V_2). \tag{6.33}$$

It follows from Lemma 6.1 and Corollary 6.2 that there exist modular categories $\mathcal{B}_1, \mathcal{B}_2$ such that (ϕ_i, V_i) is equivalent to a representation $(\rho_i, V_{\mathcal{B}_i})$ associated with $\mathcal{B}_i$ and

$$\mathcal{B}_1 = \mathcal{A}^{(0)}_{p-2,l} \quad \text{for some } l \in (\mathbb{Z}/2p\mathbb{Z})^\times.$$

Note that $(\rho_1, V_{\mathcal{B}_1}) \otimes (\rho_2, V_{\mathcal{B}_2})$ is a representation of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{B} = \mathcal{B}_1 \boxtimes \mathcal{B}_2$ and

$$(\rho, V_{\mathcal{C}}) \cong (\rho_1, V_{\mathcal{B}_1}) \otimes (\rho_2, V_{\mathcal{B}_2}). \tag{6.34}$$

Note that the eigenvalues of $\rho(\mathfrak{t})$ are all distinct.

Let E_i be the standard basis for $V_{\mathcal{B}_i}$. Then, E_i is an eigenbasis of $\rho_i(\mathfrak{t})$ and

$$E_{\mathcal{B}} = \{x_1 \otimes x_2 \mid (x_1, x_2) \in E_1 \times E_2\}$$

is an eigenbasis of $\rho_1(\mathfrak{t})\otimes\rho_2(\mathfrak{t})$ for $V_{\mathcal{B}} = V_{\mathcal{B}_1}\otimes V_{\mathcal{B}_2}$. Since $E_{\mathcal{C}} = \{e_X \mid X \in \mathrm{Irr}(\mathcal{C})\}$ is an eigenbasis of $\rho(\mathfrak{t}) = t$ for $V_{\mathcal{C}}$, the equivalence (6.34) implies there exists a bijection $\Phi : \mathrm{Irr}(\mathcal{C}) \to E_1 \times E_2$, which is defined as follows: for any $X \in \mathrm{Irr}(\mathcal{C})$, there exists a unique pair $(x_1, x_2) \in E_1 \times E_2$ satisfying

$$(\rho_1(\mathfrak{t})\otimes\rho_2(\mathfrak{t}))(x_1\otimes x_2) = t_{X,X}\cdot x_1\otimes x_2,$$

and we define $\Phi(X) := (x_1, x_2)$.

Let $\Phi(\mathbb{1}) = (b_1, b_2)$, and $D := \Phi^{-1}(E_1 \times \{b_2\}) \subseteq \mathrm{Irr}(\mathcal{C})$. Let $\mathcal{D}$ be the full subcategory of $\mathcal{C}$ additively generated by the simple objects whose isomorphism classes are in D, i.e. $\mathcal{D}$ is a semisimple subcategory of $\mathcal{C}$ with $\mathrm{Irr}(\mathcal{D}) = D$. We proceed to show $\mathcal{D}$ is a fusion subcategory of $\mathcal{C}$.

By [10, Lem. 3.17], there exists an intertwining operator $U : (\rho, V_{\mathcal{C}}) \to (\rho_1\otimes\rho_2, V_{\mathcal{B}})$ such that for any $X \in \mathrm{Irr}(\mathcal{C})$, $U(e_X) = U_{(x_1,x_2)}\, x_1\otimes x_2$ for some scalar $U_{(x_1,x_2)} = \pm 1$ where $\Phi(X) = (x_1, x_2)$. Let $s^{(i)} = \rho_i(\mathfrak{s})$ for $i = 1, 2$ and $s = \rho(\mathfrak{s})$. Then for any $X, Y \in \mathrm{Irr}(\mathcal{C})$, we have

$$s_{X,Y} = s^{(1)}_{x_1,y_1} s^{(2)}_{x_2,y_2} U_{(x_1,x_2)} U_{(y_1,y_2)},$$

where $\Phi(X) = (x_1, x_2)$, $\Phi(Y) = (y_1, y_2) \in E_1 \times E_2$. By the Verlinde formula, for any $X, Y \in D$ and $Z \in \mathrm{Irr}(\mathcal{C})$, we have

$$\begin{aligned} N^Z_{X,Y} &= \sum_{W\in\mathrm{Irr}(\mathcal{C})} \frac{s_{X,W} s_{Y,W} \overline{s_{Z,W}}}{s_{\mathbb{1},W}} \\ &= \sum_{(w_1,w_2)\in B} \frac{s^{(1)}_{x_1,w_1} s^{(1)}_{y_1,w_1} \overline{s^{(1)}_{z_1,w_1}} \left(s^{(2)}_{b_2,w_2}\right)^2 \overline{s^{(2)}_{z_2,w_2}} U_{(x_1,b_2)} U_{(y_1,b_2)} U_{(z_1,z_2)} U^3_{(w_1,w_2)}}{s^{(1)}_{b_1,w_1} s^{(2)}_{b_2,w_2} U_{(b_1,b_2)} U_{(w_1,w_2)}} \end{aligned}$$

where $\Phi(X) = (x_1, b_2)$, $\Phi(Y) = (y_1, b_2)$, $\Phi(Z) = (z_1, z_2)$ and $\Phi(W) = (w_1, w_2)$. Since $U^2_{(w_1,w_2)} = 1$, we have

$$\begin{aligned} N^Z_{X,Y} &= \frac{U_{(x_1,b_2)} U_{(y_1,b_2)} U_{(z_1,z_2)}}{U_{(b_1,b_2)}} \sum_{w_1\in B_1} \frac{s^{(1)}_{x_1,w_1} s^{(1)}_{y_1,w_1} \overline{s^{(1)}_{z_1,w_1}}}{s^{(1)}_{b_1,w_1}} \sum_{w_2\in B_2} s^{(2)}_{b_2,w_2} \overline{s^{(2)}_{z_2,w_2}} \\ &= \delta_{b_2,z_2} \frac{U_{(x_1,b_2)} U_{(y_1,b_2)} U_{(z_1,z_2)}}{U_{(b_1,b_2)}} \sum_{w_1\in B_1} \frac{s^{(1)}_{x_1,w_1} s^{(1)}_{y_1,w_1} \overline{s^{(1)}_{z_1,w_1}}}{s^{(1)}_{b_1,w_1}}, \end{aligned}$$

where the last equality is based on the fact that $s^{(2)}$ is symmetric and unitary. Therefore, $N^Z_{X,Y} = 0$ whenever $Z \notin D$. Thus, $\mathcal{D}$ is closed under the tensor product of $\mathcal{C}$ and hence a fusion subcategory.

By Theorem 3.9, $\mathcal{D}$ is a modular subcategory of $\mathcal{C}$. Since $p > 3$, we have $|\mathrm{Irr}(\mathcal{D})| = |E_1| = \varphi_2(p) > 1$ so $\mathcal{D}$ is nontrivial. Moreover, since $\mathcal{C}$ is prime, $\mathcal{C} = \mathcal{D}$ and so $\varphi_2(p) = |\mathrm{Irr}(\mathcal{C})|$. Therefore, $\varphi_2(q) = 1$, a contradiction! Therefore, N is a prime. □

Now, we can prove our major theorem of this section.

Theorem 6.4. *Let $\mathcal{C}$ be a nontrivial transitive prime modular category. Then $\mathcal{C}$ is equivalent to $\mathcal{A}^{(0)}_{p-2,l}$ for some prime $p > 3$ and $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$ as modular categories. Moreover, the set*

$$\{\mathcal{A}^{(0)}_{p-2,l} \mid l \in (\mathbb{Z}/2p\mathbb{Z})^\times\}$$

is a complete set of inequivalent transitive prime modular categories whose T-matrices are of order p.

Proof. Suppose $\mathcal{C}$ is a nontrivial transitive prime modular category, then by Theorem 6.3, $\mathrm{ord}(T_\mathcal{C})$ is a prime $p > 3$. It follows from [22, Lem. 2.2] that there exists a level p representation $(\rho, V_\mathcal{C})$ of $\mathrm{SL}_2(\mathbb{Z})$ associated with $\mathcal{C}$. Let (s, t) denote the corresponding normalized modular data (s, t) of $\mathcal{C}$. By Theorem 5.14, $(\rho, V_\mathcal{C})$ is minimal and irreducible. In view of Lemma 6.1, there exists a modular category $\mathcal{D} = \mathcal{A}^{(0)}_{p-2,l}$ for some $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$ and a level p representation $(\rho', V_\mathcal{D})$ associated with $\mathcal{D}$ such that

$$(\rho, V_\mathcal{C}) \cong (\rho', V_\mathcal{D}).$$

Let (s', t') be the normalized modular data of $\mathcal{D}$ corresponding to $(\rho', V_\mathcal{D})$. Recall that $\mathrm{Irr}(\mathcal{D}) = \{V_d \mid d \in D\}$ where $D = \{2j \mid 0 \le j \le (p-3)/2\}$. We simply write e_a for the basis element e_{V_a} for $V_\mathcal{D}$, and the entry $\rho'(\mathfrak{a})_{V_a,V_b}$ as $\rho'(\mathfrak{a})_{a,b}$ for any $\mathfrak{a} \in \mathrm{SL}_2(\mathbb{Z})$. As in the proof of Theorem 6.3, we have a bijection $\Phi : D \to \mathrm{Irr}(\mathcal{C})$ by comparing the eigenvalues of the images of $\mathfrak{t}$: for $a \in D$, we define $\Phi(a) := X \in \mathrm{Irr}(\mathcal{C})$ if $\rho(\mathfrak{t})_{X,X} = \rho'(\mathfrak{t})_{a,a}$.

To simplify notations, we denote $s_{\Phi(a),\Phi(b)}$ by $s_{a,b}$ for any $a, b \in D$. By [10, Lem. 3.17], there exists a diagonal matrix U, indexed by D, of order at most 2 such that

$$s = Us'U.$$

Let $x = \Phi^{-1}(\mathbb{1})$. Then for any $a, b, c \in D$, the Verlinde formula yields the equations

$$N^{\Phi(c)}_{\Phi(a),\Phi(b)} = \sum_{j\in D} \frac{s_{a,j}s_{b,j}\overline{s_{c,j}}}{s_{x,j}} = \frac{U_{a,a}U_{b,b}U_{c,c}}{U_{x,x}} \sum_{j\in D} \frac{s'_{a,j}s'_{b,j}\overline{s'_{c,j}}}{s'_{x,j}}.$$

Since $\mathcal{D}$ is transitive, there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ such that $\hat{\sigma}(V_x) = V_0$ and we simply write $\hat{\sigma}(x) = 0$. Applying σ to the preceding equation, we find

$$\begin{aligned} N^{\Phi(c)}_{\Phi(a),\Phi(b)} &= \frac{U_{a,a}U_{b,b}U_{c,c}}{U_{x,x}} \sum_{j\in D} \frac{\varepsilon_\sigma(a)\varepsilon_\sigma(b)\varepsilon_\sigma(c)}{\varepsilon_\sigma(x)} \frac{s'_{\hat{\sigma}(a),j}s'_{\hat{\sigma}(b),j}\overline{s'_{\hat{\sigma}(c),j}}}{s'_{0,j}} \\ &= \pm N^{V_{\hat{\sigma}(c)}}_{V_{\hat{\sigma}(a)},V_{\hat{\sigma}(b)}}. \end{aligned}$$

Since the fusion coefficients $N^{\Phi(c)}_{\Phi(a),\Phi(b)}$ and $N^{V_{\hat{\sigma}(c)}}_{V_{\hat{\sigma}(a)},V_{\hat{\sigma}(b)}}$ are nonnegative, we have $N^{\Phi(c)}_{\Phi(a),\Phi(b)} = N^{V_{\hat{\sigma}(c)}}_{V_{\hat{\sigma}(a)},V_{\hat{\sigma}(b)}}$ for all $a, b, c \in D$. Therefore, the assignment

$$\Phi(a) \mapsto V_{\hat{\sigma}(a)}, \quad \text{for } a \in D,$$

defines a $\mathbb{Z}_+$-based ring isomorphism between $K_0(\mathcal{C})$ and $K_0(\mathcal{D})$. By Lemma 4.2, $\mathcal{C}$ is equivalent to $\mathcal{A}^{(0)}_{p-2,l}$ as modular categories for some $l \in (\mathbb{Z}/2p\mathbb{Z})^\times$.

The second statement is an immediate consequence of Lemma 4.2 and Proposition 4.3. □

Finally, we establish the complete classification of nontrivial transitive modular categories.

Theorem 6.5. *Let $\mathcal{C}$ be a nontrivial modular category. Then $\mathcal{C}$ is transitive if and only if $\mathcal{C}$ is equivalent to a Deligne product $\boxtimes_{a=1}^{\ell}\mathcal{A}^{(0)}_{p_a-2,l_a}$ as modular categories for some distinct primes $p_1,\dots,p_\ell>3$ and $l_a\in(\mathbb{Z}/2p_a\mathbb{Z})^\times$.*

Proof. If $\mathcal{C}$ is transitive, then by Theorem 5.14, $\mathrm{ord}(T_\mathcal{C})=p_1\dots p_\ell$ for some distinct primes $p_1,\dots,p_\ell>3$. It follows from Theorem 3.11, $\mathcal{C}$ can be uniquely factorized into a Deligne product of prime transitive modular categories up to the ordering of factors. Therefore, by Theorem 6.4, $\mathcal{C}$ is equivalent to $\boxtimes_{a=1}^{\ell}\mathcal{A}^{(0)}_{p_a-2,l_a}$ as modular categories for some $l_a\in(\mathbb{Z}/2p_a\mathbb{Z})^\times$.

The converse of the statement follows directly from Proposition 4.4. □

In view of Theorem 6.5, nontrivial transitive modular categories $\mathcal{C}$ up to equivalence are uniquely parameterized by a pair (n,l) in which $n=\mathrm{ord}(T_\mathcal{C})$ is a square-free integer relatively prime to 6 and l is a congruence class in $(\mathbb{Z}/2n\mathbb{Z})^\times$, which can be determined by the anomaly $\alpha_1(\mathcal{C})$.

7. Transitivity of Super-Modular Categories

In this section, we investigate super-modular categories with transitive Galois actions. We first recall the definition of super-modular categories and the Galois group actions on their *reduced* S-matrices.

The tensor category of $\mathbb{Z}/2\mathbb{Z}$-graded finite-dimensional vector spaces over $\mathbb{C}$ equipped with the super braiding β is denoted by sVec. This braided fusion category sVec is symmetric and it can be endowed with two inequivalent spherical structures. The nontrivial simple object $f\in\mathrm{sVec}$ is a *fermion* that means $f\otimes f\cong\mathbb{1}$ and $\beta_{f,f}=-\mathrm{id}_{f\otimes f}$. The two inequivalent spherical structures on sVec are distinguished by $d_f=\pm1$. The corresponding premodular categories are respectively denoted by $\mathrm{sVec}_\varepsilon$ with $d_f=\varepsilon$.

A premodular category $\mathcal{C}$ is called *super-modular* or a *super-modular category over* $\mathrm{sVec}_\varepsilon$ if $\mathcal{C}'$ is equivalent to $\mathrm{sVec}_\varepsilon$ as premodular categories for some $\varepsilon=\pm1$. Let f be the transparent fermion of $\mathcal{C}$. Then, for any $X\in\mathrm{Irr}(\mathcal{C})$, we have $d_{X\otimes f}=\varepsilon d_X$ and $\theta_{X\otimes f}=-\varepsilon\theta_X$ by the twist equation (2.3). Hence, $f\otimes X\ncong X$. The transparent fermion $f\in\mathcal{C}$ may also be denoted by $f_\mathcal{C}$ if the context needs to be clarified.

The group $\mathrm{Irr}(\mathcal{C}')=\{\mathbb{1},f\}\cong\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Irr}(\mathcal{C})$ by tensor product. We denote by $\overline{X}$ the $\mathbb{Z}/2\mathbb{Z}$-orbit $\{X,f\otimes X\}$ of $\mathrm{Irr}(\mathcal{C})$, and set of $\mathbb{Z}/2\mathbb{Z}$-orbits by $\overline{\mathrm{Irr}(\mathcal{C})}$. By the above discussions, this $\mathbb{Z}/2\mathbb{Z}$-action is fixed-point free, and so there exists a complete set of representatives $\Pi_\mathcal{C}$ of $\overline{\mathrm{Irr}(\mathcal{C})}$ such that $\mathbb{1}\in\Pi_\mathcal{C}$ and $\Pi_\mathcal{C}$ is closed under taking duals. We call such a set $\Pi_\mathcal{C}$ of simple objects of $\mathcal{C}$ a *basic subset of* $\mathrm{Irr}(\mathcal{C})$, and we simply denote $\Pi_\mathcal{C}$ by Π when there is no ambiguity. In general, $\mathrm{Irr}(\mathcal{C})=\Pi\cup(f\otimes\Pi)$ and there is no canonical choice of Π unless $\mathcal{C}$ is a *split* super-modular category, i.e., $\mathcal{C}\simeq\mathcal{D}\boxtimes\mathrm{sVec}_\varepsilon$ as premodular categories for some modular category $\mathcal{D}$ and some $\varepsilon\in\{\pm1\}$. We call a super-modular category $\mathcal{C}$ *non-split* if $\mathcal{C}$ is not a split super-modular category.

With respect to the decomposition $\mathrm{Irr}(\mathcal{C})=\Pi\cup(f\otimes\Pi)$, the S-matrix of $\mathcal{C}$ admits the block form

$$S=\begin{pmatrix}\hat{S} & d_f\hat{S}\\ d_f\hat{S} & \hat{S}\end{pmatrix},$$

where $\hat{S}$ is a symmetric invertible matrix indexed by Π, called the *reduced S-matrix* of $\mathcal{C}$. The reduced S-matrix $\hat{S}$ of $\mathcal{C}$ has the unitary normalization $\hat{s} = \frac{\sqrt{2}}{\sqrt{\dim(\mathcal{C})}}\hat{S}$ which satisfies a Verlinde-like formula [40]. Since $\mathcal{C}$ embeds into $Z(\mathcal{C})$ as a premodular subcategory, S is defined over $\mathbb{Q}_N$ where N is the Frobenius–Schur exponent of $\mathcal{C}$ or the order of the T-matrix of $Z(\mathcal{C})$ (cf. [43]). The reduced S-matrix of $\mathcal{C}$ will be denoted by $\hat{S}_{\mathcal{C}}$ when the clarification is necessary.

It is immediate to see that $\mathbb{Q}(\hat{S}) = \mathbb{Q}(S) \subseteq \mathbb{Q}_N$. Similar to modular categories, we define $G_{\mathcal{C}} := \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. By [40, Sec. 2.2], for any Galois extension E over $\mathbb{Q}$ containing $\mathbb{Q}(S)$ and $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, there exists a unique permutation $\hat{\sigma}$ on Π satisfying

$$\sigma\left(\frac{\hat{S}_{X,Y}}{\hat{S}_{\mathbb{1},Y}}\right) = \frac{\hat{S}_{X,\hat{\sigma}(Y)}}{\hat{S}_{\mathbb{1},\hat{\sigma}(Y)}} \tag{7.35}$$

for any $X, Y \in \Pi$ (see also [14]). The permutation $\hat{\sigma}$ on Π induces a permutation on $\overline{\mathrm{Irr}(\mathcal{C})}$, namely $\hat{\sigma}(\overline{X}) := \overline{\hat{\sigma}(X)}$ for $X \in \Pi$, and we denote this permutation on $\overline{\mathrm{Irr}(\mathcal{C})}$ by the same notation $\hat{\sigma}$. This gives rise to an action of $\mathrm{Gal}(E/\mathbb{Q})$ on $\overline{\mathrm{Irr}(\mathcal{C})}$ by the restriction to $\mathbb{Q}(S)$. In particular, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\overline{\mathrm{Irr}(\mathcal{C})}$. Note that the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\overline{\mathrm{Irr}(\mathcal{C})}$ is independent of the choices of Π.

Since the group homomorphism $\hat{\cdot} : G_{\mathcal{C}} \to \mathrm{Sym}(\overline{\mathrm{Irr}(\mathcal{C})})$ is injective, we will identify $G_{\mathcal{C}}$ with the image of $\hat{\cdot}$ as for modular categories. In other words, for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we use $\hat{\sigma}$ to denote both the Galois automorphism on $\mathbb{Q}(S)$ and the associated permutation on $\overline{\mathrm{Irr}(\mathcal{C})}$. Again, we denote the set of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbits of $\overline{\mathrm{Irr}(\mathcal{C})}$ by $\mathrm{Orb}(\mathcal{C})$.

Definition 7.1. We call a super-modular category $\mathcal{C}$ *transitive* if the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on $\overline{\mathrm{Irr}(\mathcal{C})}$ is transitive.

We first derive some properties of the Galois actions on super-modular categories. The following lemma is an analog of [11, Prop. 3.6].

Lemma 7.2. *Let $\mathcal{C}$ be a super-modular category. Then for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, d_X is a totally real algebraic unit for $X \in \hat{\sigma}(\overline{\mathbb{1}})$.*

Proof. Let Π be a basic subset of $\mathrm{Irr}(\mathcal{C})$. By [40, Lem. 2.2], for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have

$$d^2_{\hat{\sigma}(\mathbb{1})} = \frac{\dim(\mathcal{C})}{\sigma(\dim(\mathcal{C}))}. \tag{7.36}$$

Since $\frac{\dim(\mathcal{C})}{\sigma(\dim(\mathcal{C}))}$ has algebraic norm 1, and $d_{\hat{\sigma}(\mathbb{1})}$ is a totally real algebraic integer (see [28]), $d_{\hat{\sigma}(\mathbb{1})}$ is a a totally real algebraic unit. Now the statement follows from the fact that $\hat{\sigma}(\overline{\mathbb{1}}) = \{\hat{\sigma}(\mathbb{1}), f \otimes \hat{\sigma}(\mathbb{1})\}$ and $d^2_{f\otimes\hat{\sigma}(\mathbb{1})} = d^2_{\hat{\sigma}(\mathbb{1})}$. □

On split transitive super-modular categories, we begin with the following lemma.

Lemma 7.3. *Let $\mathcal{D}$ be a modular category. Then the split super-modular category $\mathcal{C} = \mathcal{D} \boxtimes \mathrm{sVec}_\varepsilon$ for any $\varepsilon = \pm 1$ is transitive if and only if $\mathcal{D}$ is transitive.*

Proof. We can take $\Pi = \mathrm{Irr}(\mathcal{D})$. The $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on $\overline{\mathrm{Irr}(\mathcal{C})}$ is equivalent to its action on Π, which coincides with the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-action on the modular category $\mathcal{D}$. Therefore, the statement follows. □

Combining Lemma 7.3 and Theorem 6.5, we obtain the full classification of split transitive super-modular categories.

Theorem 7.4. *Let $\mathcal{C}$ be a nontrivial split super-modular category. Then $\mathcal{C}$ is transitive if and only if $\mathcal{C}$ is equivalent to $\left(\boxtimes_{a=1}^{\ell}\mathcal{A}_{p_a-2,l_a}^{(0)}\right)\boxtimes \mathrm{sVec}_{\varepsilon}$ as premodular categories for some $\varepsilon\in\{\pm 1\}$, distinct primes $p_1,\ldots,p_\ell>3$ and $(l_1,\ldots,l_\ell)\in(\mathbb{Z}/2p_1\mathbb{Z})^\times\times\cdots\times(\mathbb{Z}/2p_\ell\mathbb{Z})^\times$.* □

Transitive super-modular categories have similar properties as transitive modular categories. For example, the following lemma is parallel to Proposition 3.2.

Lemma 7.5. *If $\mathcal{C}$ is a transitive super-modular category, then we have $|G_{\mathcal{C}}|=|\operatorname{Irr}(\mathcal{C})|/2$.*

Proof. Since $G_{\mathcal{C}}$ acts transitively on $\overline{\operatorname{Irr}(\mathcal{C})}$, $G_{\mathcal{C}}$ is regular and so

$$|G_{\mathcal{C}}|=|\overline{\operatorname{Irr}(\mathcal{C})}|=|\operatorname{Irr}(\mathcal{C})|/2.$$

□

Therefore, for any transitive super-modular category $\mathcal{C}$ with a basic subset Π of $\operatorname{Irr}(\mathcal{C})$, we can identify $G_{\mathcal{C}}$ with Π via $\hat{\sigma}\mapsto\hat{\sigma}(\mathbb{1})$. Under this identification, we will simply denote $f\otimes\hat{\sigma}$ by $f\hat{\sigma}$ for any $\hat{\sigma}\in G_{\mathcal{C}}$. Now, we can compare the following theorem to Lemma 3.3 and Theorem 3.5.

Theorem 7.6. *Let $\mathcal{C}$ be a transitive super-modular category with a basic subset Π of $\operatorname{Irr}(\mathcal{C})$. Let $\hat{S}$ be the reduced S-matrix of $\mathcal{C}$ indexed by $G_{\mathcal{C}}$ according to the preceding identification of $G_{\mathcal{C}}$ and Π. Then:*

(i) *For any $\hat{\sigma},\hat{\mu}\in G_{\mathcal{C}}$, we have $\hat{S}_{\hat{\sigma},\hat{\mu}}=\hat{\sigma}(d_{\hat{\mu}})d_{\hat{\sigma}}=\hat{\mu}(d_{\hat{\sigma}})d_{\hat{\mu}}$. In particular, all entries of $\hat{S}$ and S are totally real algebraic units.*

(ii) *For any $\hat{\sigma},\hat{\mu}\in G_{\mathcal{C}}$, if $\hat{\sigma}\neq\hat{\mu}$, then $d_{\hat{\mu}}^2\neq d_{\hat{\mu}}^2$. In particular, if $\hat{\mu}\neq\mathbb{1}$, then $d_{\hat{\mu}}^2\neq 1$ and $\hat{\mu}(\dim(\mathcal{C}))\neq\dim(\mathcal{C})$.*

(iii) *For any $X\in\operatorname{Irr}(\mathcal{C})$, if $d_X^2\in\mathbb{Z}$, then $X\in\{\mathbb{1},f\}$. For any fusion subcategory $\mathcal{D}\subset\mathcal{C}$, if $f\in\mathcal{D}$, then $\mathcal{D}$ is a super-modular category, otherwise, $\mathcal{D}$ is a modular category. In particular, $\mathcal{C}$ has no nontrivial Tannakian subcategory.*

(iv) $\mathbb{Q}(\hat{S})=\mathbb{Q}(\dim(\mathcal{C}))=\mathbb{Q}(d_{\hat{\sigma}}\mid\hat{\sigma}\in G_{\mathcal{C}})$.

Proof. The first equality of statement (i) follows from (7.35) by setting $X=\hat{\mu}$, $Y=\mathbb{1}$, and the second equality follows from the fact that $\hat{S}$ is symmetric. Consequently, by Lemma 7.2, all entries of $\hat{S}$ and S are totally real algebraic units.

Now we have (i) and (7.36), the proof of (ii) and (iv) are the same as that of Theorem 3.5 (i) and (iii) by replacing S by $\hat{S}$.

For statement (iii), assume $X\in\operatorname{Irr}(\mathcal{C})$ satisfies $d_X^2\in\mathbb{Z}$. By the above discussions, since $\mathcal{C}$ is transitive, there exists $\hat{\sigma}\in G_{\mathcal{C}}$ such that $X=\hat{\sigma}$ or $X=f\hat{\sigma}$. In either case, we have $d_X^2=d_{\hat{\sigma}}^2\in\mathbb{Z}$. By Lemma 7.2, $d_{\hat{\sigma}}$ is a real algebraic unit, so $d_X^2=d_{\hat{\sigma}}^2=1$. Consequently, by (ii), we have $\hat{\sigma}=\mathbb{1}$. Therefore, $X=\mathbb{1}$ or $X=f$.

Let $\mathcal{D}\subset\mathcal{C}$ be any fusion subcategory. Then $\mathcal{D}$ is a premodular subcategory of $\mathcal{C}$. Since the Müger center $\mathcal{D}'$ of $\mathcal{D}$ is a symmetric fusion subcategory of $\mathcal{C}$, we have $d_X^2\in\mathbb{Z}$ for any $X\in\mathcal{D}'$. Therefore, we have $\operatorname{Irr}(\mathcal{D}')\subset\{\mathbb{1},f\}$ and hence $\mathcal{D}$ is super-modular (resp. modular) if and only if $f\in\mathcal{D}$ (resp. $f\notin\mathcal{D}$). Finally, if $\mathcal{D}$ is a Tannakian subcategory of $\mathcal{C}$, then $f\notin\mathcal{D}$ and so $\mathcal{D}$ is modular. Therefore, $\mathcal{D}$ braided equivalent to Vec , and this completes the proof of the theorem. □

By definition, a super-modular category over $\mathrm{sVec}_\varepsilon$ for some $\varepsilon = \pm 1$ is a nondegenerate braided fusion category over sVec according to [18]. Therefore, if $\mathcal{A}$ and $\mathcal{B}$ are super-modular categories over $\mathrm{sVec}_\varepsilon$, then their tensor product $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B} = (\mathcal{A} \boxtimes \mathcal{B})_A$ is a nondegenerate braided fusion category over sVec, where $A = \mathbb{1}_\mathcal{A} \boxtimes \mathbb{1}_\mathcal{B} \oplus f_\mathcal{A} \boxtimes f_\mathcal{B}$ is a connected étale algebra in $\mathcal{A} \boxtimes \mathcal{B}$. It is immediate to see that $\dim(A) = 2$ and $\theta_A = \mathrm{id}_A$ for any $\varepsilon = \pm 1$. Therefore, $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ admits a spherical structure inherited from $\mathcal{A} \boxtimes \mathcal{B}$ by [35] , which implies that $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ is a super-modular category.

Consider the forgetful functor $G : \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B} \to \mathcal{A} \boxtimes \mathcal{B}$, and the free-module functor $F : \mathcal{A} \boxtimes \mathcal{B} \to \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ defined by $F(X \boxtimes Y) = (X \boxtimes Y) \otimes A$ for $X \in \mathcal{A}$, $Y \in \mathcal{B}$. According to [35], F is a surjective tensor functor, and G is right adjoint to F. Let $\dim_A(M)$ denote the categorical dimension of any object $M \in \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$. We have

$$\dim_A(F(X \boxtimes Y)) = \dim_{\mathcal{A}\boxtimes\mathcal{B}}(X \boxtimes Y) = \dim_\mathcal{A}(X) \cdot \dim_\mathcal{B}(Y)$$

for any $X \in \mathcal{A}$ and $Y \in \mathcal{B}$. Therefore, $F : \mathcal{A} \boxtimes \mathcal{B} \to \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ preserves the spherical structures (cf. [42]).

Since $f_\mathcal{A} \boxtimes f_\mathcal{B}$ acts freely on $\mathrm{Irr}(\mathcal{A} \boxtimes \mathcal{B})$, $F(X \boxtimes Y)$ is simple for any $X \in \mathrm{Irr}(\mathcal{A})$ and $Y \in \mathrm{Irr}(\mathcal{B})$. The transparent fermion of $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ is given by

$$F(f_\mathcal{A} \boxtimes \mathbb{1}_\mathcal{B}) \cong f_\mathcal{A} \boxtimes \mathbb{1}_\mathcal{B} \oplus \mathbb{1}_\mathcal{A} \boxtimes f_\mathcal{B} \cong F(\mathbb{1}_\mathcal{A} \boxtimes f_\mathcal{B}) \tag{7.37}$$

and

$$\dim_A(F(f_\mathcal{A} \boxtimes \mathbb{1}_\mathcal{B})) = \dim_\mathcal{A}(f_\mathcal{A}) = \varepsilon.$$

Therefore, $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ is a super-modular category over $\mathrm{sVec}_\varepsilon$. This proves the first statement of the following lemma.

Lemma 7.7. *Let $\mathcal{A}$ and $\mathcal{B}$ be super-modular categories over $\mathrm{sVec}_\varepsilon$ for some $\varepsilon \in \{\pm 1\}$. Then:*

(i) $\mathcal{C} := \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ *is a super-modular category over* $\mathrm{sVec}_\varepsilon$,

$$\mathrm{Irr}(\mathcal{C}) = \{F(X \boxtimes Y) \mid (X, Y) \in \mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B})\},$$

and

$$\dim_A(F(X \boxtimes Y)) = d_X d_Y$$

for any $X \in \mathcal{A}$ and $Y \in \mathcal{B}$.

(ii) *Let $\Pi_\mathcal{A}$ and $\Pi_\mathcal{B}$ be basic subsets of* $\mathrm{Irr}(\mathcal{A})$ *and* $\mathrm{Irr}(\mathcal{B})$ *respectively. Then*

$$\Pi_\mathcal{C} = \{F(X \boxtimes Y) \mid (X, Y) \in \Pi_\mathcal{A} \times \Pi_\mathcal{B}\}$$

is a basic subset of $\mathrm{Irr}(\mathcal{C})$. *Moreover, the corresponding reduced S-matrix $\hat{S}_\mathcal{C}$ of $\mathcal{C}$ is given by the Kronecker product $\hat{S}_\mathcal{C} = \hat{S}_\mathcal{A} \otimes \hat{S}_\mathcal{B}$.*

Proof. We continue the preceding discussions to prove (ii). For any $X \in \mathrm{Irr}(\mathcal{A})$ and $Y \in \mathrm{Irr}(\mathcal{B})$, we have

$$GF(X \boxtimes Y) \cong X \boxtimes Y \oplus (X \otimes f_\mathcal{A}) \boxtimes (Y \otimes f_\mathcal{B}).$$

Therefore, for any $(X, Y) \neq (X', Y') \in \mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B})$,

$$F(X \boxtimes Y) \cong F(X' \boxtimes Y') \text{ if and only if } X' \boxtimes Y' \cong (X \otimes f_{\mathcal{A}}) \boxtimes (Y \otimes f_{\mathcal{B}}).$$

For any $(X, Y), (X', Y') \in \Pi_{\mathcal{A}} \times \Pi_{\mathcal{B}}$, $X' \boxtimes Y' \ncong (X \otimes f_{\mathcal{A}}) \boxtimes (Y \otimes f_{\mathcal{B}})$ by the definition of a basic subset. Since F is a tensor functor, $\mathbb{1}_{\mathcal{C}} \in \Pi_{\mathcal{C}}$ and $\Pi_{\mathcal{C}}$ is closed under taking dual. It follows from (7.37) that

$$\mathrm{Irr}(\mathcal{C}) = \Pi_{\mathcal{C}} \cup (f_{\mathcal{C}} \otimes \Pi_{\mathcal{C}})$$

where $f_{\mathcal{C}} = F(\mathbb{1}_{\mathcal{A}} \boxtimes f_{\mathcal{B}})$. Therefore, $\Pi_{\mathcal{C}}$ is a basic subset of $\mathrm{Irr}(\mathcal{C})$.

By [35, Thm. 4.1], for any $(X, Y), (X', Y') \in \Pi_{\mathcal{A}} \times \Pi_{\mathcal{B}}$,

$$\begin{aligned} \dim(A)(S_{\mathcal{C}})_{\underline{X \boxtimes Y}, \underline{X' \boxtimes Y'}} &= (S_{\mathcal{A} \boxtimes \mathcal{B}})_{X \boxtimes Y, X' \boxtimes Y'} + (S_{\mathcal{A} \boxtimes \mathcal{B}})_{X \boxtimes Y, (f_{\mathcal{A}} \otimes X') \boxtimes (f_{\mathcal{B}} \otimes Y')} \\ &= 2(S_{\mathcal{A}})_{X, X'} (S_{\mathcal{B}})_{X', Y'} \end{aligned}$$

where $\underline{X \boxtimes Y} = F(X \boxtimes Y)$. Since $\dim(A) = 2$, we have

$$(S_{\mathcal{C}})_{\underline{X \boxtimes Y}, \underline{X' \boxtimes Y'}} = (S_{\mathcal{A}})_{X, X'} (S_{\mathcal{B}})_{X', Y'},$$

which is equivalent to $\hat{S}_{\mathcal{C}} = \hat{S}_{\mathcal{A}} \otimes \hat{S}_{\mathcal{B}}$. □

Recall the definition of the fiber product in Section 2.3.

Corollary 7.8. *Let $\mathcal{A}, \mathcal{B}$ be super-modular categories over $\mathrm{sVec}_\varepsilon$ for some $\varepsilon = \pm 1$ with basic subsets $\Pi_{\mathcal{A}}$ and $\Pi_{\mathcal{B}}$ of simple objects of $\mathcal{A}$ and $\mathcal{B}$ respectively. Let $\mathcal{C} := \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ and $\mathbb{F} = \mathbb{Q}(S_{\mathcal{A}}) \cap \mathbb{Q}(S_{\mathcal{B}})$. Then:*

(i) *The map $g : G_{\mathcal{C}} \to G_{\mathcal{A}} \bullet G_{\mathcal{B}}$, $g(\hat{\sigma}_{\mathcal{C}}) = (\hat{\sigma}_{\mathcal{A}}, \hat{\sigma}_{\mathcal{B}})$, defines an isomorphism of groups, and*

$$|G_{\mathcal{C}}| = \frac{|G_{\mathcal{A}}| \cdot |G_{\mathcal{B}}|}{[\mathbb{F} : \mathbb{Q}]}.$$

(ii) *For any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $X \in \Pi_{\mathcal{A}}$ and $Y \in \Pi_{\mathcal{B}}$, we have*

$$\hat{\sigma}_{\mathcal{C}}(F(X \boxtimes Y)) = F(\hat{\sigma}_{\mathcal{A}}(X) \boxtimes \hat{\sigma}_{\mathcal{B}}(Y)).$$

(iii) $|\operatorname{Orb}(\mathcal{A})| \cdot |\operatorname{Orb}(\mathcal{B})| \leq |\operatorname{Orb}(\mathcal{C})| \leq |\operatorname{Orb}(\mathcal{A})| \cdot |\operatorname{Orb}(\mathcal{B})| \cdot [\mathbb{F} : \mathbb{Q}]$.

(iv) *If $\mathcal{A}$ and $\mathcal{B}$ are transitive, then*

$$|\operatorname{Orb}(\mathcal{C})| = \frac{|G_{\mathcal{A}}| \cdot |G_{\mathcal{B}}|}{|G_{\mathcal{C}}|} = [\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) : \mathbb{Q}].$$

Proof. In view of Lemma 7.7, by replacing $\mathrm{Irr}(\mathcal{A}), \mathrm{Irr}(\mathcal{B}), \mathrm{Irr}(\mathcal{C})$ respectively with $\Pi_{\mathcal{A}}, \Pi_{\mathcal{B}}$, and the associated $\Pi_{\mathcal{C}}$, the statements (i)-(iii) can be proved in the same way as Lemma 2.1, and the proof of (iv) is similar to that of Proposition 3.12. □

Proposition 7.9. *Let $\mathcal{C}$ be a super-modular category over $\mathrm{sVec}_\varepsilon$ for some $\varepsilon = \pm 1$. If $\mathcal{A}$ is a super-modular subcategory of $\mathcal{C}$, then both $\mathcal{A}$ and its Müger centralizer $\mathcal{B} = C_{\mathcal{C}}(\mathcal{A})$ are super-modular categories over $\mathrm{sVec}_\varepsilon$, and there is an equivalence of premodular categories over* sVec,

$$\mathcal{C} \simeq \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}. \tag{7.38}$$

Proof. It is clear that $\mathcal{A}$ is a super-modular over $\mathrm{sVec}_\varepsilon$. Note that $\mathcal{C}'$ is a premodular subcategory of $\mathcal{B}$, which is a nondegenerate braided fusion category over sVec by [18, Prop. 4.3]. Therefore, by Lemma 7.7, $\mathcal{B}$ and $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ are super-modular categories over $\mathrm{sVec}_\varepsilon$.

By [18, Prop. 4.3], there exists a braided tensor equivalence $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B} \simeq \mathcal{C}$ over sVec. In fact, the tensor product functor $\otimes : \mathcal{A} \boxtimes \mathcal{B} \to \mathcal{C}$, $X \boxtimes Y \mapsto X \otimes Y$, for any $X \in \mathcal{A}$ and $Y \in \mathcal{B}$, defines an essentially surjective braided tensor functor. This braided tensor functor descends to a braided tensor equivalence $\overline{\otimes} : \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B} \xrightarrow{\sim} \mathcal{C}$ over sVec, which satisfies the commutative diagram

$$\begin{array}{ccc} \mathcal{A} \boxtimes \mathcal{B} & \xrightarrow{\otimes} & \mathcal{C} \\ & {\scriptstyle F} \searrow \quad \nearrow {\scriptstyle \overline{\otimes}} & \\ & \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B} & \end{array} . \tag{7.39}$$

By Lemma 7.7, any simple object in $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ is isomorphic to $F(X \boxtimes Y)$ for some $(X, Y) \in \mathrm{Irr}(\mathcal{A}) \times \mathrm{Irr}(\mathcal{B})$ and

$$\dim_A(F(X \boxtimes Y)) = d_X d_Y = d_{X \otimes Y} = d_{\overline{\otimes}(F(X \boxtimes Y))}.$$

Therefore, $\overline{\otimes}$ preserves spherical structures, and hence is an equivalence of premodular categories. □

Corollary 7.10. *Let $\mathcal{C}$ be a transitive super-modular category. Then any fusion subcategory of $\mathcal{C}$ is transitive modular or super-modular.*

Proof. By Theorem 7.6 (iii), any fusion subcategory $\mathcal{A} \subset \mathcal{C}$ is either modular or super-modular. Assume first that $\mathcal{A}$ is super-modular. In view of Proposition 7.9 and Corollary 7.8, the proof of transitivity of $\mathcal{A}$ is the same as that of Theorem 3.11 with the sets $\mathrm{Irr}(\mathcal{A})$, $\mathrm{Irr}(\mathcal{B})$ and $\mathrm{Irr}(\mathcal{C})$ of irreducible objects replaced by basic sets of simple objects $\Pi_{\mathcal{A}}$, $\Pi_{\mathcal{B}}$ and the corresponding $\Pi_{\mathcal{C}}$. Now, we assume $\mathcal{A}$ is modular. Then $\mathcal{D} := \mathcal{A} \vee \mathcal{C}'$, the fusion subcategory of $\mathcal{C}$ generated by $\mathcal{A}$ and $\mathcal{C}'$, is a super-modular subcategory of $\mathcal{C}$. By the above discussions, $\mathcal{D}$ is transitive. Therefore, by Lemma 7.3, $\mathcal{A}$ is transitive. □

Corollary 7.11. *Let $\mathcal{A}$, $\mathcal{B}$ be super-modular over $\mathrm{sVec}_\varepsilon$ for some $\varepsilon = \pm 1$. Then $\mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ is transitive if and only if the following two conditions hold: both $\mathcal{A}$, $\mathcal{B}$ are transitive, and $\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) = \mathbb{Q}$.*

Proof. Let $\mathcal{C} = \mathcal{A} \underset{\mathrm{sVec}}{\boxtimes} \mathcal{B}$ be transitive. Then both $\mathcal{A}$ and $\mathcal{B}$ are transitive by Corollary 7.10. Therefore, by Corollary 7.8 (iv), we have

$$|\operatorname{Orb}(\mathcal{C})| = [\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) : \mathbb{Q}] = 1,$$

and so $\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) = \mathbb{Q}$.

Conversely, it follows immediately from Corollary 7.8 (iv) that if $\mathcal{A}$ and $\mathcal{B}$ are transitive, and $\mathbb{Q}(\dim(\mathcal{A})) \cap \mathbb{Q}(\dim(\mathcal{B})) = \mathbb{Q}$, then $\mathcal{C}$ is transitive. □

The following definition generalizes the primality of modular categories.

Definition 7.12. Let $\mathcal{E}$ be a symmetric fusion category, and $\mathcal{C}$ a nondegenerate braided fusion category $\mathcal{C}$ over $\mathcal{E}$. We say that $\mathcal{C}$ is *$\mathcal{E}$-prime* if it has no nondegenerate braided fusion subcategory over $\mathcal{E}$ except $\mathcal{E}$ and $\mathcal{C}$. An $\mathcal{E}$-prime braided fusion category is called *$\mathcal{E}$-simple* if it is not pointed. For $\mathcal{E} = \mathrm{sVec}$, we simply use the terms s-prime and s-simple instead of sVec-prime and sVec-simple.

Note the definition of $\mathcal{E}$-simple categories is consistent with the definition of s-simple categories introduced in [18]. We will call a super-modular category *trivial* if it is braided equivalent to sVec. In particular, $\mathrm{sVec}_{\pm 1}$ are trivial. In view of Theorem 7.6 (iii), nontrivial s-prime transitive super-modular categories are s-simple. Now we can state and prove the prime decomposition theorem for transitive super-modular categories (cf. Theorem 3.11).

Theorem 7.13. *Let $\mathcal{C}$ be a nontrivial transitive super-modular category over* $\mathrm{sVec}_\varepsilon$ *for some $\varepsilon = \pm 1$. Then*

$$\mathcal{C} \simeq \mathcal{C}_1 \underset{\mathrm{sVec}}{\boxtimes} \cdots \underset{\mathrm{sVec}}{\boxtimes} \mathcal{C}_m, \tag{7.40}$$

as premodular categories, where $\mathcal{C}_1, \ldots, \mathcal{C}_m$ form the complete list of inequivalent s-simple subcategories of $\mathcal{C}$. Moreover, such factorization into s-simple super-modular categories over $\mathrm{sVec}_\varepsilon$ *of $\mathcal{C}$ is unique up to permutation of factors.*

Proof. By Theorem 7.6 (iii), $\mathcal{C}$ has no Tannakian subcategory other than Vec and $\mathcal{C}_{\mathrm{pt}} = \mathcal{C}' \simeq \mathrm{sVec}_\varepsilon$. According to [18, Thm. 4.13] (i) and Proposition 7.9

$$\mathcal{C} \simeq \mathcal{C}_1 \underset{\mathrm{sVec}}{\boxtimes} \cdots \underset{\mathrm{sVec}}{\boxtimes} \mathcal{C}_m$$

as premodular categories for some s-simple subcategories $\mathcal{C}_1, \ldots, \mathcal{C}_m$ of $\mathcal{C}$. It follows from Corollary 7.11 that $\mathcal{C}_1, ..., \mathcal{C}_m$ are transitive and

$$\mathbb{Q}(\dim(\mathcal{C}_i)) \cap \mathbb{Q}(\dim(\mathcal{C})/\dim(\mathcal{C}_i)) = \mathbb{Q}$$

for any $i = 1, \ldots, m$. In particular, these s-simple super-modular subcategories of $\mathcal{C}$ have distinct global dimensions. According to [18, Thm. 4.13] (ii), $\mathcal{C}_1, \ldots, \mathcal{C}_m$ are all the s-simple super-modular subcategories of $\mathcal{C}$. Thus, if

$$\mathcal{C} \simeq \mathcal{D}_1 \underset{\mathrm{sVec}}{\boxtimes} \cdots \underset{\mathrm{sVec}}{\boxtimes} \mathcal{D}_n$$

as premodular categories for some s-simple super-modular categories $\mathcal{D}_1, \ldots, \mathcal{D}_n$ over $\mathrm{sVec}_\varepsilon$, then they are equivalent to a complete list of inequivalent s-simple super-modular subcategories of $\mathcal{C}$. Therefore, $m = n$ and the statement follows. □

Now, we demonstrate a family of transitive non-split super-modular categories derived from quantum group modular categories.

According to [7], for any $k \geq 0$ and $l \in (\mathbb{Z}/8(k+1)\mathbb{Z})^\times$, the category $\mathcal{C} = \mathcal{A}^{(0)}_{4k+2,l}$ (see Section 4) is super-modular with $\mathrm{Irr}(\mathcal{C}) = \{V_{2j} \mid 0 \leq j \leq 2k+1\}$. The fermion of $\mathcal{C}$ is V_{4k+2}. By the fusion rules (4.12), we have $V_{2j} \otimes V_{4k+2} = V_{4k+2-2j}$. In the following discussions, we choose

$$\Pi_0 = \{V_{2j} \mid 0 \leq j \leq k\}.$$

When $k = 0$, $\mathcal{C}$ is braided equivalent to sVec, and when $k \geq 1$, $\mathcal{C}$ is non-split.

Proposition 7.14. *For any $k \geq 1$, the super-modular category $\mathcal{A}^{(0)}_{4k+2,l}$ is s-simple.*

Proof. First, we show that any nontrivial fusion subcategory of $\mathcal{C}$ is either $\mathcal{C}$ or $\mathcal{C}'$.

Recall that $\mathcal{C}_{\mathrm{pt}} = \mathcal{C}'$ and $\mathrm{Irr}(\mathcal{C}') = \{\mathbb{1}, V_{4k+2}\}$. Assume that $\mathcal{D}$ is a nontrivial fusion subcategory of $\mathcal{C}$ and $\mathcal{D}$ is not pointed. Then $\mathcal{D}$ has a simple object X which is not invertible, and so $X \cong V_{2j}$ for some $1 \leq j \leq 2k$. In particular, we have $4j \geq 4$, and $2(4k+2) - 4j \geq 4$. So by the fusion rules, $N^2_{2j,2j} = 1$, which means $\mathcal{D}$ contains V_2. Since V_2 tensor generates $\mathcal{C}$, we have $\mathcal{D} = \mathcal{C}$. Therefore, $\mathcal{C}$ is s-prime. Since $k \geq 1$, $\mathcal{C} \neq \mathrm{sVec}$, so it is s-simple. □

Proposition 7.15. *Let $\mathcal{C} = \mathcal{A}^{(0)}_{4k+2,l}$ for some integer $k \geq 1$ and $l \in (\mathbb{Z}/8(k+1)\mathbb{Z})^\times$. Then $\mathcal{C}$ is transitive if and only if $k = 2^x - 1$ for $x \geq 1$.*

Proof. Recall that the quantum parameter of $\mathcal{C}$ is $q^l = \exp(\frac{l\pi i}{4(k+1)})$, and $\mathbb{Q}(S)$ is a real subfield of $\mathbb{Q}_{8(k+1)}$, so $|G_{\mathcal{C}}|$ divides $\varphi(8(k+1))/2$, where φ is the Euler phi function. Assume $\mathcal{C}$ is transitive. Then $|\Pi_0| = k+1$ must divide $\varphi(8(k+1))/2$.

We first observe that k must be odd. Suppose k is even. Then $k+1 \geq 3$ is an odd integer, and so $\varphi(8(k+1))/2 = 2\varphi(k+1)$. Therefore, $k+1 \mid \varphi(8(k+1))/2$ implies $k+1 \mid \varphi(k+1)$. This divisibility does not hold for any $k > 0$. Therefore, k must be odd.

Let $k+1 = 2^x w$, where $x \geq 1$ and w is odd. Then $\varphi(8(k+1))/2 = 2^{x+1}\varphi(w)$. Since $k+1$ divides $\varphi(8(k+1))/2$, we have $w \mid 2\varphi(w)$ and hence $w \mid \varphi(w)$. This can only happen when $w = 1$, or equivalently, $k = 2^x - 1$.

Conversely, assume $k = 2^x - 1$ for $x \geq 1$ and $\mathcal{C} = \mathcal{A}^{(0)}_{4k+2,l}$. With respect to our choice of Π_0, for any $0 \leq a, b \leq k$, we have

$$\hat{S}_{2a,2b} = [(2a+1)(2b+1)]_{q^l}.$$

Following the same argument as in the proof of Proposition 4.3, one can show that $\mathcal{C}$ is transitive. More precisely, since $\mathbb{Q}(S) \subset \mathbb{Q}_{8(k+1)} = \mathbb{Q}_{2^{x+3}}$, for any $0 \leq j \leq k$, we have $\gcd(2j+1, 2^{x+3}) = 1$. So there exists $\sigma \in \mathbb{Q}_{2^{x+3}}$ such that $\sigma(q) = q^{2j+1}$. Therefore,

$$\sigma\left(\frac{\hat{S}_{2i,0}}{\hat{S}_{0,0}}\right) = \sigma([2i+1]_{q^l}) = \frac{[(2i+1)(2j+1)]_{q^l}}{[2j+1]_{q^l}} = \frac{\hat{S}_{2i,2j}}{\hat{S}_{0,2j}}.$$

In other words, $\hat{\sigma}(V_0) = V_{2j}$, and hence $\mathcal{C}$ is transitive. □

In light of Theorem 6.5, it is natural to ask whether there are other non-split transitive super-modular categories that are s-simple, and we propose the following question at the end this paper.

Conjecture 7.16. *The quantum group categories in Proposition 7.15 are all the s-simple non-split transitive super-modular categories up to Galois conjugates and spherical structures.*

Acknowledgements. This paper is based upon work supported by the National Science Foundation under the Grant No. DMS-1440140 while the first and the last authors were in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2020 semester. They would also like to thank Eric Rowell for fruitful discussions.

References

1. Andersen, H.H.: Tensor products of quantized tilting modules. Commun. Math. Phys. **149**(1), 149–159 (1992)
2. Andersen, H.H., Paradowski, J.: Fusion categories arising from semisimple Lie algebras. Commun. Math. Phys. **169**(3), 563–588 (1995)
3. Bakalov, B., Kirillov, A., Jr.: Lectures on Tensor Categories and Modular Functors. University Lecture Series, vol. 21. American Mathematical Society, Providence (2001)
4. Blanchet, C., Habegger, N., Masbaum, G., Vogel, P.: Three-manifold invariants derived from the Kauffman bracket. Topology **31**(4), 685–699 (1992)
5. Blanchet, C., Habegger, N., Masbaum, G., Vogel, P.: Topological quantum field theories derived from the Kauffman bracket. Topology **34**(4), 883–927 (1995)
6. Bruguières, A.: Catégories prémodulaires, modularisations et invariants des variétés de dimension 3. Math. Ann. **316**(2), 215–236 (2000)
7. Bruillard, P., Galindo, C., Hagge, T., Ng, S.-H., Plavnik, J.Y., Rowell, E.C., Wang, Z.: Fermionic modular categories and the 16-fold way. J. Math. Phys. **58**(4), 31 (2017)
8. Bruillard, P., Galindo, C., Hong, S.-M., Kashina, Y., Naidu, D., Natale, S., Plavnik, J.Y., Rowell, E.C.: Classification of integral modular categories of Frobenius–Perron dimension pq^4 and p^2q^2. Can. Math. Bull. **57**(4), 721–734 (2014)
9. Bruillard, P., Galindo, C., Ng, S.-H., Plavnik, J.Y., Rowell, E.C., Wang, Z.: On the classification of weakly integral modular categories. J. Pure Appl. Algebra **220**(6), 2364–2388 (2016)
10. Bruillard, P., Ng, S.-H., Rowell, E.C., Wang, Z.: On classification of modular categories by rank. Int. Math. Res. Not. IMRN **2016**(24), 7546–7588 (2016)
11. Bruillard, P., Ng, S.-H., Rowell, E.C., Wang, Z.: Rank-finiteness for modular categories. J. Am. Math. Soc. **29**(3), 857–881 (2016)
12. Bruillard, P., Plavnik, J.Y., Rowell, E.C.: Modular categories of dimension p^3m with m square-free. Proc. Am. Math. Soc. **147**(1), 21–34 (2019)
13. Bruillard, P., Rowell, E.C.: Modular categories, integrality and Egyptian fractions. Proc. Am. Math. Soc. **140**(4), 1141–1150 (2012)
14. Bruillard, P., Plavnik, J.Y., Rowell, E.C., Zhang, Q.: On classification of super-modular categories of rank 8. J. Algebra Appl. **20**(1), Article ID 2140017 (2021)
15. Coste, A., Gannon, T.: Remarks on Galois symmetry in rational conformal field theories. Phys. Lett. B **323**(3–4), 316–321 (1994)
16. Creamer, D.: A computational approach to classifying low rank modular tensor categories. PhD thesis, Texas A&M University (2018)
17. Davydov, A., Müger, M., Nikshych, D., Ostrik, V.: The Witt group of non-degenerate braided fusion categories. J. Reine Angew. Math. **677**, 135–177 (2013)
18. Davydov, A., Nikshych, D., Ostrik, V.: On the structure of the Witt group of braided fusion categories. Sel. Math. (N.S.) **19**(1), 237–269 (2013)
19. de Boer, J., Goeree, J.: Markov traces and II_1 factors in conformal field theory. Commun. Math. Phys. **139**(2), 267–304 (1991)
20. Deligne, P.: Catégories tannakiennes. In: The Grothendieck Festschrift, vol. II. Progress in Mathematics, vol. 87, pp. 111–195. Birkhäuser Boston (1990)
21. Deligne, P.: Catégories tensorielles. Mosc. Math. J. **2**(2), 227–248 (2002)
22. Dong, C., Lin, X., Ng, S.-H.: Congruence property in conformal field theory. Algebra Number Theory **9**(9), 2121–2166 (2015)
23. Drinfeld, V., Gelaki, S., Nikshych, D., Ostrik, V.: On braided fusion categories: I. Sel. Math. (N.S.) **16**(1), 1–119 (2010)
24. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3rd edn. Wiley, Hoboken (2004)
25. Eholzer, W.: Fusion algebras induced by representations of the modular group. Int. J. Mod. Phys. A **8**(20), 3495–3507 (1993)
26. Eholzer, W.: On the classification of modular fusion algebras. Commun. Math. Phys. **172**(3), 623–659 (1995)
27. Etingof, P., Gelaki, S., Nikshych, D., Ostrik, V.: Tensor Categories. Mathematical Surveys and Monographs, vol. 205. American Mathematical Society, Providence (2015)
28. Etingof, P., Nikshych, D., Ostrik, V.: On fusion categories. Ann. Math. (2) **162**(2), 581–642 (2005)
29. Freedman, M.H., Walker, K., Wang, Z.: Quantum SU(2) faithfully detects mapping class groups modulo center. Geom. Topol. **6**, 523–539 (2002)
30. Fröhlich, J., Kerler, T.: Quantum Groups, Quantum Categories and Quantum Field Theory. Lecture Notes in Mathematics, vol. 1542. Springer, Berlin (1993)
31. Gelaki, S., Nikshych, D.: Nilpotent fusion categories. Adv. Math. **217**(3), 1053–1071 (2008)

32. Green, D.: Classification of rank 6 modular categories with galois group $\langle(012)(345)\rangle$. arXiv preprint arXiv:1908.07128 (2019)
33. Jones, V.F.R.: Hecke algebra representations of braid groups and link polynomials. Ann. Math. **126**(2), 335–388 (1987)
34. Kassel, C.: Quantum Groups. Graduate Texts in Mathematics Graduate Texts in Mathematics, vol. 155. Springer, New York (1995)
35. Kirillov, A., Jr., Ostrik, V.: On a q-analogue of the McKay correspondence and the ADE classification of $\mathfrak{sl}_2$ conformal field theories. Adv. Math. **171**(2), 183–227 (2002)
36. Moore, G., Seiberg, N.: Lectures on RCFT. In: Physics, Geometry, and Topology (Banff, AB, 1989). NATO Advanced Science Institutes Series B: Physics, vol. 238, pp. 263–361. Plenum, New York (1990)
37. Müger, M.: From subfactors to categories and topology I Frobenius algebras in and Morita equivalence of tensor categories. J. Pure Appl. Algebra **180**(1–2), 81–157 (2003)
38. Müger, M.: From subfactors to categories and topology. II. The quantum double of tensor categories and subfactors. J. Pure Appl. Algebra **180**(1–2), 159–219 (2003)
39. Müger, M.: On the structure of modular categories. Proc. Lond. Math. Soc. (3) **87**(2), 291–308 (2003)
40. Ng, S.-H., Rowell, E.C., Wang, Y., Zhang, Q.: Higher central charges and Witt groups. arXiv e-prints. arXiv:2002.03570v2 (2020)
41. Ng, S.-H., Schauenburg, P.: Frobenius–Schur indicators and exponents of spherical categories. Adv. Math. **211**(1), 34–71 (2007)
42. Ng, S.-H., Schauenburg, P.: Higher Frobenius–Schur indicators for pivotal categories. In: Hopf Algebras and Generalizations. Contemporary Mathematics, vol. 441, pp. 63–90. American Mathematical Society, Providence (2007)
43. Ng, S.-H., Schauenburg, P.: Congruence subgroups and generalized Frobenius–Schur indicators. Commun. Math. Phys. **300**(1), 1–46 (2010)
44. Ng, S.-H., Schopieray, A., Wang, Y.: Higher Gauss sums of modular categories. Sel. Math. (N.S.) **25**(4), 1–32 (2019)
45. Nobs, A.: Die irreduziblen Darstellungen der Gruppen $SL_2(\mathbb{Z}_p)$, insbesondere $SL_2(\mathbb{Z}_2)$: I. Comment. Math. Helv. **51**(4), 465–489 (1976)
46. Nobs, A., Wolfart, J.: Die irreduziblen Darstellungen der Gruppen $SL_2(\mathbb{Z}_p)$, insbesondere $SL_2(\mathbb{Z}_p)$: II. Comment. Math. Helv. **51**(4), 491–526 (1976)
47. Reshetikhin, N., Turaev, V.G.: Invariants of 3-manifolds via link polynomials and quantum groups. Invent. Math. **103**(3), 547–597 (1991)
48. Rowell, E., Stong, R., Wang, Z.: On classification of modular tensor categories. Commun. Math. Phys. **292**(2), 343–389 (2009)
49. Rowell, E.C.: From quantum groups to unitary modular tensor categories. In: Representations of Algebraic Groups, Quantum Groups, and Lie Algebras. Contemporary Mathematics, vol. 413, pp. 215–230. American Mathematical Society, Providence (2006)
50. Rowell, E.C., Wang, Z.: Mathematics of topological quantum computing. Bull. Am. Math. Soc. (N.S.) **55**(2), 183–238 (2018)
51. Turaev, V., Wenzl, H.: Quantum invariants of 3-manifolds associated with classical simple Lie algebras. Int. J. Math. **4**(2), 323–358 (1993)
52. Turaev, V.G.: Quantum Invariants of Knots and 3-Manifolds. De Gruyter Studies in Mathematics, vol. 18, Revised Walter de Gruyter & Co., Berlin (2010)
53. Vafa, C.: Toward classification of conformal theories. Phys. Lett. B **206**(3), 421–426 (1988)
54. Wan, Z., Wang, Y.: Classification of spherical fusion categories of Frobenius–Schur exponent 2. Algebra Colloq. **28**(1), 39–50 (2021)
55. Wang, Z.: Topological Quantum Computation. CBMS Regional Conference Series in Mathematics, vol. 112. Published for the Conference Board of the Mathematical Sciences, Washington, DC. American Mathematical Society, Providence (2010)
56. Wen, X.-G.: Theory of the edge states in fractional quantum Hall effects. Int. J. Mod. Phys. B **6**, 1711–1762 (1992)
57. Wielandt, H.: Finite Permutation Groups. Translated from the German by R. Bercov. Academic Press, New York (1964)

Communicated by C. Schweigert