ON MODULAR CATEGORIES

PAUL BRUILLARD, SIU-HUNG NG, ERIC C. ROWELL, AND ZHENGHAN WANG

Abstract. We prove a rank-finiteness conjecture for modular categories that there are only finitely many modular categories of fixed rank r, up to equivalence. Our main technical advance is a Cauchy theorem for modular categories: given a modular category $\mathcal{C}$, the set of prime ideals of the global quantum dimension D^2 of $\mathcal{C}$ in the cyclotomic number field $\mathcal{O}_N$ is identical to that of the Frobenius-Schur exponent $N = \mathrm{FSexp}(\mathcal{C})$ of $\mathcal{C}$. By combining the Galois symmetry of the modular S, T matrices with the knowledge of the modular representation of $SL(2, \mathbb{Z})$, we determine all possible fusion rules for all rank=5 modular categories and describe the corresponding monoidal equivalence classes.

1 Introduction

Modular categories are intricate organizing algebraic structures appearing in a variety of mathematical subjects including topological quantum field theory [48], conformal field theory [39], representation theory of quantum groups [6], von Neumann algebras [21], and vertex operator algebras [31]. They are fusion categories with additional braiding and pivotal structures [22, 48, 6]. These extra structures endow them with some "abelian-ness" which makes the classification of modular categories possible.

Besides the intrinsic mathematical aesthetics, another motivation for pursuing a classification of modular categories comes from their application in condensed matter physics and quantum computing [52, 53]. Unitary modular categories are algebraic models of anyons in two dimensional topological phases of matter where simple objects model anyons. In topological quantum computation, anyons give rise to quantum computational models. Modular categories have also been used recently to construct physically realistic three dimensional topological insulators and superconductors [57, 3]. Therefore, a classification of modular categories is literally a classification of certain topological phases of matter.

A modular category $\mathcal{C}$ is a non-degenerate ribbon fusion category over $\mathbb{C}$ [48, 6]. A **fusion category** $\mathcal{C}$ is an abelian $\mathbb{C}$-linear semisimple rigid monoidal category with a simple unit object $\mathbf{1}$, finite-dimensional morphism spaces and finitely many isomorphism classes of simple objects. Let $\Pi_{\mathcal{C}}$ be the set of isomorphism classes of simple objects of the fusion category $\mathcal{C}$. The **rank** of $\mathcal{C}$ is the finite number $r = |\Pi_{\mathcal{C}}|$. Each modular category $\mathcal{C}$ leads to a $(2+1)$-dimensional topological quantum field theory $(V_{\mathcal{C}}, Z_{\mathcal{C}})$, in particular colored framed link invariants [48]. The invariant $\{d_a\}$ for the unknot colored by the label $a \in \Pi_{\mathcal{C}}$ is called the *quantum dimension* of

Date: August 29, 2014.

Key words and phrases. Modular categories.

The first, third and fourth authors were partially supported by NSF grant DMS1108725, and the second author was partially supported by NSF grants DMS1001566 and DMS1303253. This project began at a workshop at the American Institute of Mathematics, and was completed while E.R. was visiting the Beijing International Center for Mathematical Research, Peking University–the support and hospitality of both institutions are gratefully acknowledged. It is a pleasure to thank Vladimir Turaev and Pavel Etingof for valuable comments.

the label. The number $D = \sqrt{\sum_{a\in\Pi_{\mathcal{C}}} d_a^2}$ is an important invariant of $\mathcal{C}$, called the *quantum order*. The invariant of the Hopf link colored by a, b will be denoted as S_{ab}. The link invariant of the unknot with a right-handed kink colored by a is $\theta_a \cdot d_a$ for some root of unity θ_a, which is called the *topological twist* of the label a. The topological twists form a diagonal matrix $T = (\delta_{ab}\theta_a), a, b \in \Pi_{\mathcal{C}}$. The S-matrix and T-matrix together lead to a projective representation of the modular group $SL(2,\mathbb{Z})$ by sending the generating matrices

$$\mathfrak{s} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad \mathfrak{t} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

to S, T, respectively [48, 6]. Amazingly, the kernel of this projective representation of $\mathcal{C}$ is always a congruence subgroup of $SL(2,\mathbb{Z})$ [43]. The S-matrix determines the fusion rules through the Verlinde formula, and the T-matrix is of finite order $\mathrm{ord}(T)$ by Vafa's theorem [6]. Together, the pair S, T are called the *modular data* of the category $\mathcal{C}$.

The abelian-ness of modular categories first manifests itself in the braiding: the tensor product is commutative up to functorial isomorphism. But a deeper sense of abelian-ness is revealed in the Galois group of the number field $\mathbb{K}_{\mathcal{C}}$ obtained by adjoining all matrix entries of S to $\mathbb{Q}$: $\mathbb{K}_{\mathcal{C}}$ is an abelian extension of $\mathbb{Q}$ [5, 47]. Moreover, its Galois group is isomorphic to an abelian subgroup of the symmetric group $\mathfrak{S}_n$, where n is the rank of $\mathcal{C}$. This profound observation permits the application of deep number theory to the classification of modular categories.

The first success of the classification program was the complete classification of unitary modular categories up to rank=4 in [47]. In 2003, the fourth author conjectured that, up to equivalence, there are only finitely many modular categories of a given rank, which we will call *the rank-finiteness conjecture* [54, 47]. In this paper, we prove the rank-finiteness conjecture which implies that, in principle, modular categories can be classified by rank. Furthermore, we develop tools for a classification-by-rank program and as an application we complete a classification of all modular categories of rank=5 (up to monoidal equivalence) in Section 5.

The rank-finiteness conjecture is motivated by the classification of topological phases of matter. Topological phases of matter are states of matter which have an energy gap in the thermodynamic limit and are stable under small yet arbitrary perturbations. Thus, they cannot be continuously deformed non-trivially inside topological states of matter. Efforts to understand the rigidity first led to the discovery of the Ocneanu rigidity[1], which implies that for a fixed set of fusion rules, there are only finitely many equivalence classes of modular categories [22]. Hence, the rank-finiteness conjecture is reduced to showing that there are only finitely many possible fusion rules for any given rank. Using the Verlinde formula, we can deduce the finiteness of fusion rules for a given rank from a bound of the global quantum dimension D^2, in particular, if there are only finitely possible values of D^2 then the conjecture would follow [47]. The key step for obtaining the finiteness of possible values of D^2 for a fixed rank is our generalization of the Cauchy theorem in group theory to modular categories: the set of prime ideals in the decomposition of $\langle D^2\rangle$ is the same as the set of those in the prime decomposition of $\langle \mathrm{ord}(T)\rangle$, in the Dedekind domain of integers in $\mathbb{Q}(e^{2\pi i/\mathrm{ord}(T)})$. As a consequence, the quantum dimensions d_i and D^2 have special arithmetic properties: they are so-called $\mathcal{S}$*-units* with respect to the common ideals in the prime decomposition of D^2 and $\mathrm{ord}(T)$. Then regarding $D^2 = \sum_i d_i^2$ as an $\mathcal{S}$-unit equation, we can apply Evertse's finiteness theorem for non-degenerate $\mathcal{S}$-units solutions to this equation [25]. It

[1]Freedman asked Wenzl about rigidity of Jones-Wenzl projectors in Temperley-Lieb categories around 2000 [27].

follows that there are only finitely many $\mathcal{S}$-unit solutions to the dimension equation $D^2 = \sum_i d_i^2$, in particular only finitely many possible values of D^2 for any given rank. All steps can be made effective, so we have explicit bounds for the number of solutions to the dimension equation. The bound for the number of possible modular categories for a given rank that we obtained is absurdly large. For example for rank=2, there are only 8 modular categories while our bound is between $2^{714.447}$ and $2^{8.15885\times 10^{41}}$ for the $\mathcal{S}$-unit equation $D^2 = \sum_i d_i^2$. An immediate question is to determine if there is a better bound for the number of modular categories of rank=n. Etingof observes in Remark 3.25 that the number of modular categories of rank=r grows faster than any polynomial in r.

The content of the paper is as follows. Section 2 is a collection of necessary results on fusion and modular categories. We define admissible modular data as a pair of matrices S, T satisfying algebraic constraints with an eye towards the characterization of realizable modular data. In Section 3, we prove the rank-finiteness conjecture. The first main result of the paper is:

Theorem 3.1. *There are only finitely many modular categories of fixed rank r, up to equivalence.*

Our main technical result is a Cauchy theorem for spherical fusion categories.

Theorem 3.9. *The set of prime ideals of D^2 in $\mathcal{O}_N$ is identical to that of $N = \mathrm{FSexp}(\mathcal{C})$.*

In Section 4 we develop general arithmetic constraints on admissible modular data. One improvement to the approach in [47] is the combining of Galois symmetry of S, T matrices with the knowledge of the representation theory of $SL(2,\mathbb{Z})$. An important observation is:

Lemma 4.18. *Let $\mathcal{C}$ be a modular category of rank k and $\rho : SL(2,\mathbb{Z}) \to GL(k,\mathbb{C})$ a modular representation of $\mathcal{C}$, i.e. a lifting of projective representation of $\mathcal{C}$. Then ρ cannot be isomorphic to a direct sum of two representations with disjoint $\mathfrak{t}$-spectra.*

Finally in Section 5, we combine the analysis of Galois action on the S-matrix and $SL(2,\mathbb{Z})$ representation to determine all possible fusion rules for all rank=5 modular categories and describe their classification up to monoidal equivalence.

Our second main result of the paper is:

Theorem 5.1. *Suppose $\mathcal{C}$ is a modular category of rank 5. Then $\mathcal{C}$ is Grothendieck equivalent to one of the following:*

(i) $SU(2)_4$

(ii) $SU(2)_9/\mathbb{Z}_2$

(iii) $SU(5)_1$

(iv) $SU(3)_4/\mathbb{Z}_3$

In this paper we only classify these modular categories up to monoidal equivalence, but a complete list of all modular categories with the above fusion rules as done in [47] is possible. However, the details are not straightforward, so we will leave it to a future publication.

Our reduction of the rank-finiteness conjecture to Evertse's theorem is a black-box and it obscures the nature of rigidity in modular categories. The key to Evertse's finiteness of $\mathcal{S}$-unit solutions is the Schmidt subspace theorem, which implies finiteness theorems for some simultaneous approximations to algebraic numbers by elements of a number field. It would be more illuminating to have a more direct proof of the rank-finiteness conjecture. A better understanding of rank-finiteness for modular categories might shed light on whether or not rank-finiteness also holds for spherical fusion categories. One potential approach is taking the Drinfeld center of spherical fusion categories and then deducing rank-finiteness for spherical fusion categories from the modular case.

Topological phases of matter are phases of matter that lie beyond Landau's symmetry breaking and local order parameter paradigm for the classification of states of matter. Physicists propose to use the S, T matrices as order parameters for the classification of topological phases of matter [37]. Therefore, a natural question is if the S, T matrices determine the modular category. We believe they do. The S, T matrices satisfy many constraints, and a pair of matrices S, T with those constraints are called *admissible modular data*. It is interesting to characterize admissible modular data that can be realized by modular categories.

For application to topological quantum computation, it is important to understand the images of the representations of the mapping class groups from a modular category. In particular, when do all representations have finite images? The property F conjecture says that the representations of all mapping class groups from a modular category have finite images if and only if $D^2 \in \mathbb{Z}$ [40, 47].

Modular categories form part of the mathematical foundations of topological quantum computation. The classification program of modular categories initiated in this paper will lead to a deeper understanding of their structure and their enchanting relations to other fields, thus pave the way for applications to a futuristic field *anyonics* broadly defined as the science and technology that cover the development, behavior, and application of anyonic devices.

2 Modular Categories

In this section, we will collect some conventions and essential results on spherical fusion categories and modular categories. Most of these results can be found in [48, 6, 22, 41, 42, 43] and the references therein.

2.1 Basic Definitions

A modular category is a braided spherical fusion category in which the braiding is non-degenerate. Modular categories were first axiomatized by Turaev [49], based on earlier notions in Rational Conformal Field Theory by Moore and Seiberg [39] and related foundational work of Joyal and Street [32]. Early interesting examples arose in the work of Reshetikhin with Turaev on quantum groups and their application to low-dimensional topology. In this section we will give the precise definition and describe some further properties and consequences of the definition.

2.1.1 Fusion Categories

Recall from [22], a **fusion category** $\mathcal{C}$ is an abelian $\mathbb{C}$-linear semisimple rigid monoidal category with a simple unit object $\mathbf{1}$, finite-dimensional morphism spaces and finitely many isomorphism classes of simple objects. In a fusion category $\mathcal{C}$ with tensor product $\otimes$ and unit object $\mathbf{1}$, the left dual of $V \in \mathcal{C}$ is a triple $(V^*, \mathrm{db}_V, \mathrm{ev}_V)$ where $\mathrm{db}_V : \mathbf{1} \to V \otimes V^*$ and $\mathrm{ev}_V : V^* \otimes V \to \mathbf{1}$ are the associated coevaluation and evaluation morphisms. The left duality can be extended to a monoidal functor $(-)^* : \mathcal{C} \to \mathcal{C}^{\mathrm{op}}$, and so $(-)^{**} : \mathcal{C} \to \mathcal{C}$ defines a monoidal equivalence. Moreover we can choose $\mathbf{1}^* = \mathbf{1}$. The (linear) space of morphisms between objects V and W will be denoted $\mathrm{Hom}_{\mathcal{C}}(V, W)$. Right duals are similarly defined.

Let $\Pi_\mathcal{C}$ be the set of isomorphism classes of simple objects of the fusion category $\mathcal{C}$. The **rank** of $\mathcal{C}$ is the finite number $r = |\Pi_\mathcal{C}|$, and we denote the members of $\Pi_\mathcal{C}$ by $\{0, \dots, r-1\}$. We simply write V_i for an object in the isomorphism class $i \in \Pi_\mathcal{C}$. By convention, the isomorphism class of $\mathbf{1}$ corresponds to $0 \in \Pi_\mathcal{C}$. The rigidity of $\mathcal{C}$ defines an involutive permutation $i \mapsto i^*$ on $\Pi_\mathcal{C}$ which is given by $V_{i^*} \cong V_i^*$ for all $i \in \Pi_\mathcal{C}$.

2.1.2 Braidings

A **braiding** c of a fusion category $\mathcal{C}$ is a natural family of isomorphisms $c_{V,W} : V \otimes W \to W \otimes V$ in V and W of $\mathcal{C}$ which satisfy the hexagonal diagrams

$$\begin{tikzcd}
U \otimes (V \otimes W) \arrow[r, "c_{U,V\otimes W}"] & (V \otimes W) \otimes U \arrow[d, "\alpha"] \\
(U \otimes V) \otimes W \arrow[u, "\alpha"] \arrow[d, "c\otimes \mathrm{id}"'] & V \otimes (W \otimes U) \\
(V \otimes U) \otimes W \arrow[r, "\alpha"'] & V \otimes (U \otimes W)\,, \arrow[u, "\mathrm{id}\otimes c"']
\end{tikzcd}
\qquad
\begin{tikzcd}
(U \otimes V) \otimes W \arrow[r, "c_{U\otimes V,W}"] & W \otimes (U \otimes V) \arrow[d, "\alpha^{-1}"] \\
U \otimes (V \otimes W) \arrow[u, "\alpha^{-1}"] \arrow[d, "\mathrm{id}\otimes c"'] & (W \otimes U) \otimes V \\
U \otimes (W \otimes V) \arrow[r, "\alpha^{-1}"'] & (U \otimes W) \otimes V\,, \arrow[u, "c\otimes\mathrm{id}"']
\end{tikzcd}$$

for all $U, V, W \in \mathcal{C}$ where α is the associativity isomorphism of $\mathcal{C}$ (cf. [32]).

A **braided fusion category** is a pair $(\mathcal{C}, c)$ in which c is a braiding of the fusion category $\mathcal{C}$. We may simply call $\mathcal{C}$ a braided fusion category if the underlying braiding c is understood.

2.1.3 Spherical Fusion Categories

A **pivotal structure** of a fusion category $\mathcal{C}$ is an isomorphism $j : \mathrm{Id}_\mathcal{C} \to (-)^{**}$ of monoidal functors. One can respectively define the left and the right **pivotal traces** of an endomorphism $f : V \to V$ in $\mathcal{C}$ as

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

Note that $j_V^* = j_{V^*}^{-1}$, and so we have $\underline{\mathrm{ptr}}^\ell(f) = \underline{\mathrm{ptr}}^r(f^*)$. Since $\mathbf{1}$ is a simple object of $\mathcal{C}$, both pivotal traces $\underline{\mathrm{ptr}}^\ell(f)$ and $\underline{\mathrm{ptr}}^r(f)$ can be identified with some scalars in $\mathbb{C}$. A pivotal structure on $\mathcal{C}$ is called **spherical** if the two pivotal traces coincide for all endomorphisms f in $\mathcal{C}$.

For the purpose of this paper, a **pivotal** (resp. **spherical**) **category** $(\mathcal{C}, j)$ is a fusion category $\mathcal{C}$ equipped with a pivotal (resp. spherical) structure j. We will denote the pair $(\mathcal{C}, j)$ by $\mathcal{C}$ when there is no ambiguity. The **left** and the **right pivotal dimensions** of $V \in \mathcal{C}$ are defined as $d^\ell(V) = \underline{\mathrm{ptr}}^\ell(\mathrm{id}_V)$ and $d^r(V) = \underline{\mathrm{ptr}}^r(\mathrm{id}_V)$ respectively. In a spherical category, the pivotal traces will be denoted by $\underline{\mathrm{ptr}}(f)$.

2.1.4 Modular Categories

Following [33], a **twist** (or **ribbon structure**) of a braided fusion category $(\mathcal{C}, c)$ is an $\mathbb{C}$-linear automorphism, θ, of $\mathrm{Id}_\mathcal{C}$ which satisfies

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

for $V, W \in \mathcal{C}$. A braided fusion category equipped with a ribbon structure is called a **ribbon fusion** or **premodular** category. A premodular category $\mathcal{C}$ is called a **modular category** if the S-**matrix** of $\mathcal{C}$, defined by

$$S_{ij} = \underline{\mathrm{ptr}}(c_{V_j,V_{i^*}} \circ c_{V_{i^*},V_j}) \text{ for } i,j \in \Pi_{\mathcal{C}}\,,$$

is non-singular. Note that S is a symmetric matrix and that $d^r(V_i) = S_{0i} = S_{i0}$ for all i.

2.2 Further Properties and Basic Invariants

2.2.1 Grothendieck Ring and Dimensions

The **Grothendieck ring** $K_0(\mathcal{C})$ of a fusion category $\mathcal{C}$ is the $\mathbb{Z}$-ring generated by $\Pi_{\mathcal{C}}$ with multiplication induced from $\otimes$. The structure coefficients of $K_0(\mathcal{C})$ are obtained from:

$$V_i \otimes V_j \cong \bigoplus_{k\in\Pi_{\mathcal{C}}} N_{i,j}^k\, V_k$$

where $N_{i,j}^k = \dim(\mathrm{Hom}_{\mathcal{C}}(V_k, V_i \otimes V_j))$. This family of non-negative integers $\{N_{i,j}^k\}_{i,j,k\in\Pi_{\mathcal{C}}}$ is called the *fusion rules* of $\mathcal{C}$.

In a braided fusion category $K_0(\mathcal{C})$ is a commutative ring and the fusion rules satisfy the symmetries:

$$N_{i,j}^k = N_{j,i}^k = N_{i,k^*}^{j^*} = N_{i^*,j^*}^{k^*}, \quad N_{i,j}^0 = \delta_{i,j^*} \tag{2.1}$$

The **fusion matrix** N_i of V_i, defined by $(N_i)_{k,j} = N_{i,j}^k$, is an integral matrix with non-negative entries. In the braided fusion setting these matrices are normal and mutually commuting. The largest real eigenvalue of N_i is called the **Frobenius-Perron dimension** of V_i and is denoted by $\mathrm{FPdim}(V_i)$. Moreover, FPdim can be extended to a $\mathbb{Z}$-ring homomorphism from $K_0(\mathcal{C})$ to $\mathbb{R}$ and is the unique such homomorphism that is positive (real-valued) on $\Pi_{\mathcal{C}}$ (see [22]). The **Frobenius-Perron dimension** of $\mathcal{C}$ is defined as

$$\mathrm{FPdim}(\mathcal{C}) = \sum_{i\in\Pi_{\mathcal{C}}} \mathrm{FPdim}(V_i)^2\,.$$

We will say two fusion categories $\mathcal{C}$ and $\mathcal{D}$ are **Grothendieck equivalent** if there is a bijection between $\Pi_{\mathcal{C}}$ and $\Pi_{\mathcal{D}}$ that induces a (unital) $\mathbb{Z}$-ring isomorphism between $K_0(\mathcal{C})$ and $K_0(\mathcal{D})$.

Definition 2.1. A fusion category $\mathcal{C}$ is said to be

(i) **weakly integral** if $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Z}$.

(ii) **integral** if $\mathrm{FPdim}(V_j) \in \mathbb{Z}$ for all $j \in \Pi_{\mathcal{C}}$.

(iii) **pointed** if $\mathrm{FPdim}(V_j) = 1$ for all $j \in \Pi_{\mathcal{C}}$.

Furthermore, if $\mathrm{FPdim}(V) = 1$, then V is **invertible**.

Remark 2.2. The terminology *invertible* arises from the fact that $\mathrm{FPdim}(V) = 1$ if and only if $V \otimes V^* \cong \mathbf{1}$. The set of invertible simple objects generates a full subcategory $\mathcal{C}_{pt}$ called the **pointed subcategory** which is closed under the tensor product.

Let $\mathcal{C}$ be a pivotal category. It follows from [22, Prop. 2.9] that $d^r(V^*) = \overline{d^r(V)}$ is an algebraic integer for any $V \in \mathcal{C}$. The **global dimension** of $\mathcal{C}$ is defined by

$$D^2 = \sum_{i \in \Pi_{\mathcal{C}}} |d^r(V_i)|^2.$$

Remark 2.3. It is worth noting that the global dimension D^2 can be defined for any fusion category (cf. [22]), and does not depend on the existence, or choice of, of a pivotal structure.

By [38, 22], a pivotal structure of a fusion category $\mathcal{C}$ is spherical if, and only if, $d^r(V)$ is real for all $V \in \mathcal{C}$. In this case, $d^r(V) = d^\ell(V)$ and we simply write $d(V)$ to refer to the dimension of V, furthermore for $i \in \Pi_{\mathcal{C}}$ we adopt the shorthand $d_i = d(V_i)$.

A fusion category $\mathcal{C}$ is called **pseudo-unitary** if $D^2 = \operatorname{FPdim}(\mathcal{C})$. For a pseudo-unitary fusion category $\mathcal{C}$, it has been shown in [22] that there exists a unique spherical structure of $\mathcal{C}$ such that $d(V) = \operatorname{FPdim}(V)$ for all objects $V \in \mathcal{C}$.

2.2.2 Spherical and Ribbon Structures

Associated with a braiding c on a fusion category $\mathcal{C}$ is an isomorphism of $\mathbb{C}$-linear functors $u : \mathrm{Id}_{\mathcal{C}} \to (-)^{**}$, called the **Drinfeld isomorphism**. When $\mathcal{C}$ is a strict fusion category, u_V is the composition:

$$u_V := (V \xrightarrow{\mathrm{db} \otimes \mathrm{id}} V^* \otimes V^{**} \otimes V \xrightarrow{\mathrm{id} \otimes c^{-1}} V^* \otimes V \otimes V^{**} \xrightarrow{\mathrm{ev} \otimes \mathrm{id}} V^{**} = V)\,.$$

If u is the Drinfeld isomorphism associated with c, and θ is a ribbon structure, then

$$j = u\theta \tag{2.2}$$

is a spherical structure of $\mathcal{C}$. This equality defines a one-to-one correspondence between the spherical structures and the ribbon structures on $(\mathcal{C}, c)$.

The set of isomorphism classes of invertible objects $G(\mathcal{C})$ forms a group in $K_0(\mathcal{C})$ where $i^{-1} = i^*$ for $i \in G(\mathcal{C})$. For modular categories $\mathcal{C}$, the group $G(\mathcal{C})$ parameterizes pivotal structures on the underlying braided fusion category:[2]

Lemma 2.4. *Let $\mathcal{C}$ be a modular category. There is a bijective correspondence between the pivotal structures of the underlying braided fusion category $\mathcal{C}$ and the group of invertible objects $G(\mathcal{C})$. Under this correspondence, the inequivalent spherical structures of $\mathcal{C}$ map onto the maximal elementary abelian 2-subgroup, $\Omega_2 G(\mathcal{C})$, of $G(\mathcal{C})$.*

Proof. Let j_0 be the spherical pivotal structure of the modular category $\mathcal{C}$. For any pivotal structure j of $\mathcal{C}$, we have $j_0^{-1} j \in \mathrm{Aut}_\otimes(\mathrm{Id}_{\mathcal{C}})$, the group of automorphisms of the monoidal functor $\mathrm{Id}_{\mathcal{C}}$. Moreover, $j \mapsto j_0^{-1} j$ defines a bijection between the set of pivotal structures of $\mathcal{C}$ and $\mathrm{Aut}_\otimes(\mathrm{Id}_{\mathcal{C}})$. Note that j is spherical if, and only if, the associated dimension function is real valued, and hence for any simple V, $(j_0^{-1} j)_V = \lambda_V \,\mathrm{id}_V$ for some real scalar λ_V. By [28, Thm. 6.2], $\mathrm{Aut}_\otimes(\mathrm{Id}_{\mathcal{C}}) \cong G(\mathcal{C})$ and hence the first statement follows. In particular, $j_0^{-1} j$ has finite order. Thus, j is a spherical structure of $\mathcal{C}$ if, and only if, $(j_0^{-1} j)_V = \pm\,\mathrm{id}_V$ for any simple V, or $j_0^{-1} j \in \mathrm{Aut}_\otimes(\mathrm{Id}_{\mathcal{C}})$ is of order ≤ 2. Therefore, the second statement follows from the isomorphism $\mathrm{Aut}_\otimes(\mathrm{Id}_{\mathcal{C}}) \cong G(\mathcal{C})$. $\square$

[2] This second part of this result was pointed out to us by Naidu.

Remark 2.5. The isomorphism $\mathrm{Aut}_\otimes(\mathrm{Id}_\mathcal{C}) \cong G(\mathcal{C})$ is determined by the braiding c and the spherical structure j_0 of the modular category $(\mathcal{C}, c, j_0)$. By [38, Cor. 7.11], $(\mathcal{C}, c, j)$ is a modular category for all spherical structures j of $\mathcal{C}$, so that there are exactly $|G(\mathcal{C})|$ pivotal and $|\Omega_2 G(\mathcal{C})|$ spherical structures on the fusion category $\mathcal{C}$.

In any ribbon fusion category $\mathcal{C}$ the associated ribbon structure, θ, has finite order. This celebrated fact is part of Vafa's Theorem (see [51, 6]) in the case of modular categories. However, any ribbon category embeds in a modular category (via Drinfeld centers, see [38]) so the result hold generally. Observe that, $\theta_{V_i} = \theta_i \,\mathrm{id}_{V_i}$ for some root of unity $\theta_i \in \mathbb{C}$. Since $\theta_{\mathbf{1}} = \mathrm{id}_{\mathbf{1}}$, $\theta_0 = 1$. The T-**matrix** of $\mathcal{C}$ is defined by $T_{ij} = \delta_{ij}\theta_j$ for $i, j \in \Pi_\mathcal{C}$. The **balancing equation**:

$$\theta_i\theta_j S_{ij} = \sum_{k\in\Pi_\mathcal{C}} N_{i^*j}^k d_k \theta_k \tag{2.3}$$

is a useful algebraic consequence, holding in any pre-modular category. The pair (S, T) of S and T-matrices will be called the **modular data** of a given modular category $\mathcal{C}$.

2.2.3 Modular Data and $SL(2,\mathbb{Z})$ Representations

Definition 2.6. For a pair of matrices (S, T) for which there exists a modular category with modular data (S, T) we will say (S, T) is **realizable modular data**.

The fusion rules $\{N_{i,j}^k\}_{i,j,k\in\Pi_\mathcal{C}}$ of $\mathcal{C}$ can be written in terms of the S-matrix, which is called the **Verlinde formula** [6]:

$$N_{i,j}^k = \frac{1}{D^2}\sum_{a\in\Pi_\mathcal{C}} \frac{S_{ia}S_{ja}S_{k^*a}}{S_{0a}} \quad \text{for all } i, j, k \in \Pi_\mathcal{C}\,. \tag{2.4}$$

The modular data (S, T) of a modular category $\mathcal{C}$ satisfy the conditions:

$$(ST)^3 = p^+S^2, \quad S^2 = p^+p^-C, \quad CT = TC, \quad C^2 = \mathrm{id}, \tag{2.5}$$

where $p^\pm = \sum_{i\in\Pi_\mathcal{C}} d_i^2\theta_i^{\pm1}$ are called the **Gauss sums**, and $C = (\delta_{ij^*})_{i,j\in\Pi_\mathcal{C}}$ is called the **charge conjugation matrix** of $\mathcal{C}$. In terms of matrix units the first equation in (2.5) gives the **twist equation**:

$$p^+S_{jk} = \theta_j\theta_k\sum_i \theta_i S_{ij}S_{ik}\,. \tag{2.6}$$

The quotient $\frac{p^+}{p^-}$, called the **anomaly** of $\mathcal{C}$, is a root of unity, and

$$p^+p^- = D^2. \tag{2.7}$$

Moreover, S satisfies

$$S_{ij} = S_{ji} \quad \text{and} \quad S_{ij^*} = S_{i^*j} \tag{2.8}$$

for all $i, j \in \Pi_\mathcal{C}$. These equations and the Verlinde formula imply that

$$S_{ij^*} = \overline{S_{ij}} \quad \text{and} \quad \frac{1}{D^2}\sum_{j\in\Pi_\mathcal{C}} S_{ij}\overline{S}_{jk} = \delta_{ik}. \tag{2.9}$$

In particular S is projectively unitary.

A modular category $\mathcal{C}$ is called **self-dual** if $i = i^*$ for all $i \in \Pi_\mathcal{C}$. In fact, $\mathcal{C}$ is self-dual if and only if S is a real matrix.

Let D be the positive square root of D^2. The Verlinde formula can be rewritten as

$$SN_iS^{-1} = D_i \quad \text{for } i \in \Pi_{\mathcal{C}}$$

where $(D_i)_{ab} = \delta_{ab}\frac{S_{ia}}{S_{0a}}$. In particular, the assignments $\phi_a : i \mapsto \frac{S_{ia}}{S_{0a}}$ for $i \in \Pi_{\mathcal{C}}$ determine (complex) linear characters of $K_0(\mathcal{C})$. Since S is non-singular, $\{\phi_a\}_{a\in\Pi_{\mathcal{C}}}$ is the set of *all* the linear characters of $K_0(\mathcal{C})$. Observe that FPdim is a character of $K_0(\mathcal{C})$, so that there is some $a \in \Pi_{\mathcal{C}}$ such that $\mathrm{FPdim} = \phi_a$. By the unitarity of S we have that $\mathrm{FPdim}(\mathcal{C}) = D^2/(d_a)^2$.

As an abstract group $SL(2,\mathbb{Z}) \cong \langle \mathfrak{s}, \mathfrak{t} \mid \mathfrak{s}^4 = 1, (\mathfrak{s}\mathfrak{t})^3 = \mathfrak{s}^2\rangle$. The standard choice for generators is:

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

Let $\eta : GL(\Pi_{\mathcal{C}}, \mathbb{C}) \to PGL(\Pi_{\mathcal{C}}, \mathbb{C})$ be the natural surjection. The relations (2.5) imply that

$$\overline{\rho}_{\mathcal{C}} \colon \mathfrak{s} \mapsto \eta(S) \quad \text{and} \quad \mathfrak{t} \mapsto \eta(T) \tag{2.10}$$

defines a projective representation of $SL(2,\mathbb{Z})$. Since the modular data is an invariant of a modular category, so is the associated projective representation type of $SL(2,\mathbb{Z})$. The following arithmetic properties of this projective representation will play an important role in our discussion (cf. [43]).

Theorem 2.7. *Let (S,T) be the modular data of the modular category $\mathcal{C}$ with $N = \mathrm{ord}\,(T)$. Then the entries of S are algebraic integers of $\mathbb{Q}_N$. Moreover, N is minimal such that the projective representation $\overline{\rho}_{\mathcal{C}}$ of $SL(2,\mathbb{Z})$ associated with the modular data can be factored through $SL(2,\mathbb{Z}_N)$. In other words, $\ker \overline{\rho}_{\mathcal{C}}$ is a congruence subgroup of level N.*

Definition 2.8. A **modular representation** of $\mathcal{C}$ (cf. [43]) is a representation ρ of $SL(2,\mathbb{Z})$ which satisfies the commutative diagram:

$$\begin{tikzcd} SL(2,\mathbb{Z}) \arrow[r, "\rho"] \arrow[dr, "\overline{\rho}_{\mathcal{C}}"'] & GL(\Pi_{\mathcal{C}}, \mathbb{C}) \arrow[d, "\eta"] \\ & PGL(\Pi_{\mathcal{C}}, \mathbb{C}). \end{tikzcd}$$

Let $\zeta \in \mathbb{C}$ be a fixed 6-th root of the anomaly $\dfrac{p^+}{p^-}$. For any 12-th root of unity x, it follows from (2.5) that the assignments

$$\rho_x^\zeta : \mathfrak{s} \mapsto \frac{\zeta^3}{x^3 p^+} S, \quad \mathfrak{t} \mapsto \frac{x}{\zeta} T \tag{2.11}$$

define a modular representation of $\mathcal{C}$. Moreover, $\{\rho_x^\zeta \mid x^{12} = 1\}$ is the complete set of modular representations of $\mathcal{C}$ (cf. [15, Sect. 1.3]). Note that $\rho_x^\zeta(\mathfrak{s})$ and $\rho_x^\zeta(\mathfrak{t})$ are matrices over a finite abelian extension of $\mathbb{Q}$. Therefore, modular representations of any modular category are defined over the abelian closure $\mathbb{Q}_{\mathrm{ab}}$ of $\mathbb{Q}$ in $\mathbb{C}$ (cf. [4]).

Let ρ be a modular representation of the modular category $\mathcal{C}$, and set

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

It is clear that the representation ρ is uniquely determined by the pair (s,t), which will be called a **normalized modular pair** of $\mathcal{C}$.

2.2.4 Galois Symmetry

Observe that for any choice of a normalized modular pair (s,t) we have $\frac{s_{ia}}{s_{0a}} = \frac{S_{ia}}{S_{0a}} = \phi_a$. For each $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$, $\sigma(\phi_a)$ given by $\sigma(\phi_a)(i) = \sigma\left(\frac{s_{ia}}{s_{0a}}\right)$ is again a linear character of $K_0(\mathcal{C})$ and hence $\sigma(\phi_a) = \phi_{\hat{\sigma}(a)}$ for some unique $\hat{\sigma} \in \mathrm{Sym}(\Pi_{\mathcal{C}})$. That is,

$$\sigma\left(\frac{s_{ia}}{s_{0a}}\right) = \frac{s_{i\hat{\sigma}(a)}}{s_{0\hat{\sigma}(a)}} \quad \text{for all } i, a \in \Pi_{\mathcal{C}}\,. \tag{2.12}$$

Moreover, there exists a function $\epsilon_\sigma : \Pi_{\mathcal{C}} \to \{\pm 1\}$, which depends on the choice of s, such that:

$$\sigma(s_{ij}) = \epsilon_\sigma(i) s_{\hat{\sigma}(i)j} = \epsilon_\sigma(j) s_{i\hat{\sigma}(j)} \quad \text{for all } i, j \in \Pi_{\mathcal{C}} \tag{2.13}$$

(cf. [4, App. B], [11] or [22, App.]). The group $\mathrm{Sym}(\Pi_{\mathcal{C}})$ will often be written as $\mathfrak{S}_r$ when $r = |\Pi_{\mathcal{C}}|$.

Let $G_\sigma \in GL(\Pi_{\mathcal{C}}, \mathbb{Z})$ be the signed permutation matrix defined by $(G_\sigma)_{ij} = \epsilon_\sigma(i)\delta_{\hat{\sigma}(i)j}$, or, alternatively, by $G_\sigma = \sigma(s)s^{-1}$.

The following is proved in [15, Thm. II]:

Theorem 2.9. *Let $\mathcal{C}$ be a modular category with the set of isomorphism classes of simple objects $\Pi_{\mathcal{C}}$, and T-matrix of order N. Suppose $\rho : SL(2,\mathbb{Z}) \to GL(\Pi_{\mathcal{C}}, \mathbb{C})$ is a modular representation of $\mathcal{C}$. Set $s = \rho(\mathfrak{s})$ and $t = \rho(\mathfrak{t})$. Then:*

(i) $\ker\rho$ *is a congruence subgroup of level n where $n = \mathrm{ord}\,(t)$. Moreover, $N \mid n \mid 12N$.*

(ii) ρ *is $\mathbb{Q}_n$-rational, i.e.* $\mathrm{im}\,\rho \le GL(\Pi_{\mathcal{C}}, \mathbb{Q}_n)$.

(iii) *For $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, $G_\sigma = \sigma(s)s^{-1}$ is a signed permutation matrix, and*
$$\sigma^2(\rho(\mathfrak{g})) = G_\sigma \rho(\mathfrak{g}) G_\sigma^{-1}$$
for all $\mathfrak{g} \in SL(2,\mathbb{Z})$.

(iv) *Let a be an integer relatively prime to n with an inverse b modulo n. For the automorphism σ_a of $\mathbb{Q}_n$ given by $e^{\frac{2\pi i}{n}} \mapsto e^{\frac{2a\pi i}{n}}$,*
$$G_{\sigma_a} = t^a s t^b s t^a s^{-1}\,.$$

The Galois symmetry of modular representations will play an important role for the proof the Cauchy Theorem as well as the classification of modular categories of small ranks. This was also established by Xu in the setting of conformal nets [58], and by Bantay in conformal field theory under certain assumptions [2].

We employ Galois theory to derive some constraints on modular data.

In view of Theorem 2.9, we will simply define the **level** of the normalized modular pair (s,t) of $\mathcal{C}$ as $\mathrm{ord}\,(t)$.

In the sequel, we will simply denote by $\mathbb{F}_A$ the field extension over $\mathbb{Q}$ generated by the entries of a complex matrix A. If $\mathbb{F}_A/\mathbb{Q}$ is Galois, then we simply write $\mathrm{Gal}(A)$ for the Galois group $\mathrm{Gal}(\mathbb{F}_A/\mathbb{Q})$.

In this notation, if (S,T) is the modular data of $\mathcal{C}$, then $\mathbb{F}_T = \mathbb{Q}_N$ where $N = \mathrm{ord}\,(T)$, and we have $\mathbb{F}_S \subseteq \mathbb{F}_T$ by Theorem 2.7. In particular, $\mathbb{F}_S$ is an abelian Galois extension over $\mathbb{Q}$.

For any normalized modular pair (s,t) of $\mathcal{C}$ we have $\mathbb{F}_t = \mathbb{Q}_n$, where $n = \operatorname{ord}(t)$. Moreover, by Theorem 2.9, $\mathbb{F}_S \subseteq \mathbb{F}_s \subseteq \mathbb{F}_t$. In particular, the field extension $\mathbb{F}_s/\mathbb{Q}$ is also Galois. The kernel of the restriction map $\operatorname{res} : \operatorname{Gal}(t) \to \operatorname{Gal}(S)$ is isomorphic to $\operatorname{Gal}(\mathbb{F}_t/\mathbb{F}_S)$. The following lemma, proved in [15, Prop. 6.5], will be essential to the classification of modular categories of small rank.

Lemma 2.10. *Let $\mathcal{C}$ be a modular category with modular data (S,T). For any normalized modular pair (s,t) of $\mathcal{C}$, $\operatorname{Gal}(\mathbb{F}_t/\mathbb{F}_S)$ is an elementary 2-group.*

2.2.5 Frobenius-Schur Indicators

A **strict pivotal** category is a pivotal category in which the associativity isomorphisms are identities, the pivotal structure $j : \mathrm{Id}_\mathcal{C} \to (-)^{**}$ is the identity, and the associated natural isomorphisms $\xi_{U,V} : U^* \otimes V^* \to (V \otimes U)^*$ are also identities. Moreover, we have the following theorem (cf. [41]).

Theorem 2.11. *Every pivotal category is pivotally equivalent to a strict pivotal category.*

Frobenius-Schur indicators are indispensable invariants of spherical categories introduced in [41]. They are defined for each object in a pivotal category. Here, we only provide the definition of these indicators in a *strict* spherical category. Let n be a positive integer and V an object of a strict spherical category $\mathcal{C}$. We denote by $V^{\otimes n}$ the n-fold tensor power of V. One can define a $\mathbb{C}$-linear operator $E_V^{(n)} : \operatorname{Hom}_\mathcal{C}(\mathbf{1}, V^{\otimes n}) \to \operatorname{Hom}_\mathcal{C}(\mathbf{1}, V^{\otimes n})$ given by

$$E_V^{(n)}(f) = \left(\mathbf{1} \xrightarrow{\mathrm{db}} V^* \otimes V \xrightarrow{\mathrm{id}_{V^*} \otimes f \otimes \mathrm{id}_V} V^* \otimes V^{\otimes n+1} \xrightarrow{\mathrm{ev} \otimes \mathrm{id}_V^{\otimes n}} V^{\otimes n}\right).$$

The n-th Frobenius-Schur indicator of V is defined as

$$\nu_n(V) = \operatorname{Tr}(E_V^{(n)}).$$

It follows directly from graphical calculus that $\left(E_V^{(n)}\right)^n = \mathrm{id}$, and so $\nu_n(V)$ is an algebraic integer in the n-th cyclotomic field $\mathbb{Q}_n = \mathbb{Q}(e^{\frac{2\pi i}{n}})$.

The first indicator $\nu_1(V_i)$ is the Kronecker delta function δ_{0i} on $\Pi_\mathcal{C}$, i.e. $\nu_1(V) = 1$ if $V \cong \mathbf{1}$ and 0 otherwise. The second indicator is consistent with the classical Frobenius-Schur indicator of an irreducible representation of a group, namely $\nu_2(V) = \pm 1$ if $V \cong V^*$ and 0 otherwise for any simple object V of $\mathcal{C}$. The higher indicators are more obscure in nature but they are all additive complex valued functions of the Grothendieck ring $K_0(\mathcal{C})$ of $\mathcal{C}$.

The classical definition of exponent of a finite group can be generalized to a spherical category via the following theorem [42].

Theorem 2.12. *Let $\mathcal{C}$ be a spherical category. There exists a positive integer n such that $\nu_n(V) = d(V)$ for all $V \in \mathcal{C}$. If m is minimal among such n then $d(V)$ are algebraic integers in $\mathbb{Q}_m$.*

The minimal integer $\operatorname{FSexp}(\mathcal{C}) := m$ above is called the **Frobenius-Schur exponent**. If $\mathcal{C}$ is the category of complex representations of a finite group G, then $\operatorname{FSexp}(\mathcal{C}) = \exp(G)$. For modular categories the Frobenius-Schur indicators $\nu_n(V)$ are completely determined by the modular data of $\mathcal{C}$, explicitly given in [42] (generalizing the second indicator formula in [1]):

Theorem 2.13. *Let $\mathcal{C}$ be a modular category with the T-matrix given by $[\delta_{ij}\theta_i]_{i,j\in\Pi_{\mathcal{C}}}$. Then* $\operatorname{ord}(T) = \operatorname{FSexp}(\mathcal{C})$*, and*

$$\nu_n(V_k) = \frac{1}{D^2} \sum_{i,j\in\Pi_{\mathcal{C}}} N_{i,j}^k\, d_i d_j \left(\frac{\theta_i}{\theta_j}\right)^n \tag{2.14}$$

for all $k \in \Pi_{\mathcal{C}}$ and positive integers n.

Definition 2.14. Let $S,T \in \mathrm{GL}(\mathbb{C}^r)$ and define constants $d_j := S_{0j}$, $\theta_j := T_{jj}$, $D^2 := \sum_j d_j^2$ and $p_\pm = \sum_{k=0}^{r-1}(S_{0,k})^2\theta_k^{\pm 1}$. The pair (S,T) is an **admissible modular data** of rank r if they satisfy the following conditions:

(i) $d_j \in \mathbb{R}$ and $S = S^t$ with $S\overline{S}^t = D^2\,\mathrm{Id}$. $T_{i,j} = \delta_{i,j}\theta_i$ with $N := \operatorname{ord}(T) < \infty$.

(ii) $(ST)^3 = p^+S^2$, $p_+p_- = D^2$ and $\frac{p_+}{p_-}$ is a root of unity.

(iii) $N_{i,j}^k := \frac{1}{D^2}\sum_{a=0}^{r-1}\frac{S_{ia}S_{ja}\overline{S_{ka}}}{S_{0a}} \in \mathbb{N}$ for all $0 \le i,j,k \le (r-1)$.

(iv) $\theta_i\theta_j S_{ij} = \sum_{k=0}^{r-1} N_{i^*j}^k d_k\theta_k$ where i^* is the unique label such that $N_{i,i^*}^0 = 1$.

(v) Define $\nu_n(k) := \frac{1}{D^2}\sum_{i,j=0}^{r-1} N_{i,j}^k\, d_i d_j \left(\frac{\theta_i}{\theta_j}\right)^n$. Then $\nu_2(k) = 0$ if $k \ne k^*$ and $\nu_2(k) = \pm 1$ if $k = k^*$. Moreover, $\nu_n(k) \in \mathcal{O}_{\mathbb{Q}_N}$ for all n,k.

(vi) $\mathbb{F}_S \subset \mathbb{F}_T = \mathbb{Q}_N$, $\mathrm{Gal}(\mathbb{F}_S/\mathbb{Q})$ is isomorphic to an abelian subgroup of $\mathfrak{S}_r$ and $\mathrm{Gal}(\mathbb{F}_T/\mathbb{F}_S) \cong (\mathbb{Z}/2\mathbb{Z})^k$.

(vii) The prime divisors of D^2 and N coincide in $\mathbb{Q}_N$.[3]

Theorem 2.15. *Let (S,T) be a realizable modular data. Then*

(a) (S,T) is admissible and
(b) For all $\sigma \in \operatorname{Aut}_{\mathbb{Q}}\left(\overline{\mathbb{Q}}\right)$, $(\sigma(S), \sigma(T))$ is realizable.

Proof. (a) follows from the definition of admissible modular data, while (b) follows from [22, Section 2.7] (see also [14]). □

Remark 2.16. A converse of Theorem 2.15 should be true: that is, if (S,T) is admissible then it is realizable. Indeed, a satisfactory definition of admissible would be a minimal set of conditions that guarantee realizability.

3 Rank-Finiteness and the Cauchy Theorem

The main goal of this section is to prove the following Rank-Finiteness theorem, conjectured by the fourth author in 2003 (see [54]):

Theorem 3.1 (Rank-Finiteness Theorem)**.** *There are only finitely many modular categories of fixed rank r, up to equivalence.*

Prior to this work this conjecture had only been resolved in certain restricted cases, for instance it was shown [22, Proposition 8.38] that there are finitely many weakly integral fusion categories through a classical number theoretic argument due to Landau [36].

The proof of the Rank-Finiteness Theorem relies upon several well-known reductions, a new result known as the Cauchy Theorem (for Spherical Fusion Categories 3.9) and some results in analytic number theory due to Evertse [25].

[3] See Section 3.1.

In Section 3.1, the Cauchy Theorem for Spherical Fusion Categories is proved, and in Section 3.2 we prove Theorem 3.1. We discuss efficiency and asymptotic related to Theorem 3.1 in Section 3.3.

3.1 The Cauchy Theorem

Let $\mathbb{A}$ be the ring of algebraic integers in $\mathbb{C}$. For $a, b, c \in \mathbb{A}$ with $a \neq 0$, $b \equiv c \bmod a$ means that $(b-c)/a \in \mathbb{A}$.

Suppose $\mathcal{C}$ is a modular category with $N = \mathrm{FSexp}(\mathcal{C})$ and q is prime with $(q, N) = 1$. We begin with a simple lemma which is essentially proved in [55, Lem. 1.8] and [35, Section 3.4].

Lemma 3.2. *Let W be a finite-dimensional $\mathbb{C}$-linear space. If E is a $\mathbb{C}$-linear operator on W such that $E^q = \mathrm{id}_W$ for some prime number q, then*

$$\mathrm{Tr}(E)^q \equiv \dim_{\mathbb{C}} W \bmod q\,.$$

In particular, if $\mathrm{Tr}(E) \in \mathbb{Z}$, then $\mathrm{Tr}(E) \equiv \dim_{\mathbb{C}} W \bmod q$.

Proof. Let $\zeta_q \in \mathbb{C}$ denote a primitive q-th root of unity. Then $\mathrm{Tr}(E) = \sum_{i=0}^{q-1} m_i \zeta_q^i$ where m_i is the multiplicity of the eigenvalue ζ_q^i. Thus,

$$\mathrm{Tr}(E)^q \equiv \sum_{i=0}^{q-1} m_i^q \equiv \sum_{i=0}^{q-1} m_i = \dim_{\mathbb{C}} W \bmod q\,.$$

In particular, if $\mathrm{Tr}(E) \in \mathbb{Z}$, the second statement follows from Fermat's little theorem. $\square$

Recall that the n-th Frobenius-Schur indicator $\nu_n(V)$ for $V \in \mathcal{C}$ is defined as the trace of a $\mathbb{C}$-linear operator $E_V^{(n)} : \mathrm{Hom}_{\mathcal{C}}\left(\mathbf{1}, V^{\otimes n}\right) \to \mathrm{Hom}_{\mathcal{C}}\left(\mathbf{1}, V^{\otimes n}\right)$. This operator $E_V^{(n)}$ satisfies

$$\left(E_V^{(n)}\right)^n = \mathrm{id}\ .$$

Moreover, $\nu_n(V)$ is an algebraic integer in $\mathbb{Q}_n \cap \mathbb{Q}_N$. Since q and N are relatively prime, we have

$$\nu_q(V) \in \mathbb{Q}_N \cap \mathbb{Q}_q = \mathbb{Q}\,.$$

Thus $\nu_q(V) \in \mathbb{Z}$. By the preceding lemma, we have proved

Lemma 3.3. *For any $V \in \mathcal{C}$, $\nu_q(V) \in \mathbb{Z}$ and we have*

$$\nu_q(V) \equiv \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{C}}\left(\mathbf{1}, V^{\otimes q}\right) \bmod q\,.$$

Let $\mathcal{O}_N$ be the ring of algebraic integers of $\mathbb{Q}_N$. It is well known that $\mathcal{O}_N = \mathbb{Z}[\zeta_N]$ where ζ_N is a primitive N-th root of unity in $\mathbb{C}$. Set $K_N(\mathcal{C}) = K_0(\mathcal{C}) \otimes_{\mathbb{Z}} \mathcal{O}_N$. Then $K_N(\mathcal{C})$ is an $\mathcal{O}_N$-algebra. For any non-zero element $a \in \mathcal{O}_N$ and $\alpha, \beta \in K_N(\mathcal{C})$, we write $\alpha \equiv \beta \bmod a$ if $\alpha - \beta = a\gamma$ for some $\gamma \in K_N(\mathcal{C})$.

By [42], $\nu_q : K_0(\mathcal{C}) \to \mathbb{Z}$ is a group homomorphism; however, the assignment $V \mapsto \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{C}}\left(\mathbf{1}, V^{\otimes q}\right)$ is not. We can extend the ν_q to an $\mathcal{O}_N$-linear map from $K_N(\mathcal{C})$ to $\mathcal{O}_N$, and we continue to denote such an extension by ν_q. Similarly, we can extend the dimension function $d : K_0(\mathcal{C}) \to \mathcal{O}_N$ to an $\mathcal{O}_N$-linear map from $K_N(\mathcal{C})$ to $\mathcal{O}_N$. However, it is important to note that this extension is an $\mathcal{O}_N$-*algebra* homomorphism.

Note that $K_N(\mathcal{C})$ is a free $\mathcal{O}_N$-module with $\Pi_\mathcal{C}$ as a basis. For $\alpha = \sum_{i\in\Pi_\mathcal{C}} \alpha_i i \in K_N(\mathcal{C})$, we define $\delta(\alpha) = \alpha_0$. Obviously, $\delta : K_N(\mathcal{C}) \to \mathcal{O}_N$ is $\mathcal{O}_N$-linear. Even though $\delta(\alpha^q)$ is not $\mathcal{O}_N$-linear in α, but it satisfies the following congruence.

Lemma 3.4. *For $\alpha \in K_N(\mathcal{C})$, then we have*

$$\delta(\alpha^q) \equiv \sigma_q(\nu_q(\alpha)) \bmod q$$

where $\sigma_q \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$ defined by $\sigma_q(\zeta_N) = \zeta_N^q$.

Proof. Let $\alpha = \sum_{i\in\Pi_\mathcal{C}} \alpha_i i$. Then $\alpha^q \equiv \sum_{i\in\Pi_\mathcal{C}} \alpha_i^q i^q \bmod q$. Since δ is $\mathcal{O}_N$-linear, we have

$$\delta(\alpha^q) \equiv \delta(\sum_{i\in\Pi_\mathcal{C}} \alpha_i^q i^q) = \sum_{i\in\Pi_\mathcal{C}} \alpha_i^q \delta(i^q) \bmod q\,.$$

Since $\delta(i^q) = \dim_\mathbb{C} \mathrm{Hom}_\mathcal{C}(\mathbf{1}, V_i^{\otimes q})$, it follows from Lemma 3.3 that

$$\delta(i^q) \equiv \nu_q(V) \bmod q\,.$$

Thus, we find

$$\delta(\alpha^q) \equiv \sum_{i\in\Pi_\mathcal{C}} \alpha_i^q \nu_q(V_i) \bmod q\,.$$

Note that for $a \in \mathcal{O}_N$, $a = \sum_j a_j \zeta_N^j$ where $a_j \in \mathbb{Z}$. Therefore,

$$a^q \equiv \sum_j a_j^q \zeta_N^{qj} \equiv \sum_j a_j \sigma_q(\zeta_N^j) = \sigma_q(a) \bmod q\,.$$

Hence, we have

$$\delta(\alpha^q) \equiv \sum_{i\in\Pi_\mathcal{C}} \sigma_q(\alpha_i)\nu_q(V_i) = \sigma_q(\nu_q(\alpha)) \bmod q\,.$$

The last equality follows from the $\mathcal{O}_N$-linearity of ν_q, and $\nu_q(V_i) \in \mathbb{Z}$ for all $i \in \Pi_\mathcal{C}$. $\square$

By [42], $d_i \in \mathcal{O}_N$ for $i \in \Pi_\mathcal{C}$. Therefore, $R = \sum_{i\in\Pi_\mathcal{C}} d_i i$ is an element of $K_N(\mathcal{C})$.

Notice that R defines a rank 1 ideal of $K_N(\mathcal{C})$ as $iR = d_i R$ for all $i \in \Pi_\mathcal{C}$. Thus, for $\alpha \in K_N(\mathcal{C})$, $\alpha R = d(\alpha)R$ where $d : K_N(\mathcal{C}) \to \mathcal{O}_N$ is the $\mathcal{O}_N$-linear extension of the dimension function from $K_0(\mathcal{C})$ to $\mathcal{O}_N$. In particular, d is a $\mathcal{O}_N$-algebra homomorphism. Therefore,

$$R^n = R^{n-1}R = d(R^{n-1})R = D^{2(n-1)}R\,.$$

Now, we can write our first proposition for the indicators of the *pseudo* object R.

Proposition 3.5. *Let $R = \sum_{i\in\Pi_\mathcal{C}} d_i i \in K_N(\mathcal{C})$, and q a prime number not dividing N. Then we have*

$$\sigma_q\left(\nu_q(R)\right) \equiv D^{2(q-1)} \bmod q\,.$$

Proof. By the preceding discussion, we have $R^q = D^{2(q-1)}R$. Since $\delta(R) = d_0 = 1$, we have $\delta(R^q) = D^{2(q-1)}$. By Lemma 3.4,

$$\sigma_q(\nu_q(R)) \equiv D^{2(q-1)} \bmod q\,. \quad \square$$

Proposition 3.6. *For any $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})$, $d_{\hat\sigma(0)}$ is a unit of $\mathcal{O}_N$.*

Proof. Without loss of generality, we may assume $\hat{\sigma}(0) = 1$. Then
$$\sigma(\frac{1}{D^2}) = d_1^2/D^2 \quad \text{or} \quad d_1^2 = D^2/\sigma(D^2).$$
Obviously, the norm of $D^2/\sigma(D^2)$ is 1, and so is d_1^2. Therefore d_1 is a unit in $\mathcal{O}_N$. □

Remark 3.7. The preceding is another proof of the fact proved in [44] that D^2 is a d-number.

Proposition 3.8. $\nu_q(R) = d^2_{\hat{\sigma}_q^{-1}(0)}$.

Proof. Note that
$$\nu_q(R) = \sum_k d_k \nu_q(V_k) = \frac{1}{D^2} \sum_{i,j,k} d_k N_{ij}^k d_i d_j \frac{\theta_i^q}{\theta_j^q} = \frac{1}{D^2} \left(\sum_i d_i^2 \theta_i^q \right) \left(\sum_j d_j^2 \theta_j^{-q} \right) .$$
Reexpressing equation (2.7) in terms of $s = S/D$, we find that:
$$s_{00}^2 = \left(\sum_i s_{0i}^2 \theta_i \right) \left(\sum_j s_{0j}^2 \theta_j^{-1} \right) .$$
Applying $\tau = \sigma_q^{-1}$ to the equation, we find
$$s_{\hat{\tau}(0)0}^2 = \left(\sum_i s_{0\hat{\tau}(i)}^2 \tau(\theta_i) \right) \left(\sum_j s_{0\hat{\tau}(j)}^2 \tau(\theta_i)^{-1} \right) .$$
By Galois symmetry, Theorem 2.9(iii), we have
$$d_{\hat{\tau}(0)}^2 s_{00}^2 = \left(\sum_i s_{0\hat{\tau}(i)}^2 \theta_{\hat{\tau}(i)}^q \right) \left(\sum_j s_{0\hat{\tau}(j)}^2 \theta_{\hat{\tau}(j)}^{-q} \right) .$$
Therefore,
$$d_{\hat{\tau}(0)}^2 = \frac{1}{D^2} \left(\sum_i d_i^2 \theta_i^q \right) \left(\sum_j d_j^2 \theta_j^{-q} \right) = \nu_q(R) . \quad \square$$

We can now prove the following generalization of [43, Thm. 8.4] in which the result is proved for *integral* fusion categories. Moreover, it provides an affirmative answer to Question 6.9 of [15].

Theorem 3.9 (Cauchy Theorem for Spherical Fusion Categories)**.** *Let $\mathcal{C}$ be a spherical fusion category. Then set of prime ideals of D^2 is identical to that of $N = \mathrm{FSexp}(\mathcal{C})$ in $\mathcal{O}_N$.*

Proof. We first consider the case when $\mathcal{C}$ is a modular category. Since $N \mid D^6$ [24], every prime ideal factor of N in $\mathcal{O}_N$ is a factor of D^2. Suppose $\mathfrak{p}$ is a prime ideal factor of D^2. By Propositions 3.5 and 3.8, we find the congruence
$$\sigma_q(d_i^2) \equiv D^{2(q-1)} \bmod q$$
for any prime $q \nmid N$ where $i = \hat{\sigma}_q^{-1}(0)$. By Proposition 3.6, d_i is a unit of $\mathcal{O}_N$. Therefore, we have $\mathcal{O}_N = (D^2) + (q)$ of ideals. This implies that $q \notin \mathfrak{p}$. Therefore, $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime $p \mid N$. Hence, $\mathfrak{p}$ is a prime factor of N in $\mathcal{O}_N$.

Now, we assume $\mathcal{C}$ is a general spherical fusion category. Then its Drinfeld center $Z(\mathcal{C})$ is modular and $\dim Z(\mathcal{C}) = (\dim \mathcal{C})^2$ by [38]. Since $N = \mathrm{FSexp}(\mathcal{C}) = \mathrm{FSexp}(Z(\mathcal{C}))$ by [43], the theorem follows from the modular case *i.e.* N and $(\dim \mathcal{C})^2$ have the same set of prime ideal factors in $\mathcal{O}_N$. $\square$

Remark 3.10. If $\mathcal{C}$ is the category of representations of a finite group G, then $\mathrm{FSexp}(\mathcal{C}) = \exp(G)$ and $\dim \mathcal{C} = |G|$. The preceding theorem implies that p is a prime factor of $|G|$ if, and only if, $p \mid \exp(G)$; this is simply an equivalent statement of the classical Cauchy Theorem for finite groups.

3.2 Proof of Rank-Finiteness

To prove Theorem 3.1 we first reduce to proving that there are finitely many possible fusion rules using (braided) Ocneanu Rigidity, due to Ocneanu, Blanchard and Wassermann (unpublished):

Theorem 3.11. [22] *There are only finitely many (braided, modular) fusion categories which have the same fusion rules up to (braided, modular) monoidal equivalence.*

Remark 3.12. Ocneanu Rigidity for fusion categories was first proved by Blanchard and Wasserman, and the extension to the braided case can be found in [22, Remark 2.33]. For the finiteness of spherical structures see Lemma 2.4.

Next we may reduce to bounding the FP-dimension using (see eg. [22, Proposition 8.38] and [47, Proposition 6.2]):

Corollary 3.13. *There are finitely many (braided, modular) fusion categories $\mathcal{C}$ satisfying* $\mathrm{FPdim}\,(\mathcal{C}) \leq M$ *for any fixed number $M > 0$, up to (braided, modular) monoidal equivalence.*

For the reader's convenience we provide an explicit bound on the N_{ij}^k in terms of $\mathrm{FPdim}(\mathcal{C})$ for fusion categories.

Scholium 3.14. *If $\mathcal{C}$ is a rank n fusion category, then for $a \in \Pi_{\mathcal{C}}$, we have the inequality:*

$$\|N_a\|_{max} \leq \mathrm{FPdim}\,(V_a) \leq n\|N_a\|_{max}$$

where $\|A\|_{max}$ is the max-norm of the complex matrix A given by

$$\|A\|_{max} = \max_{i,j} |A_{ij}| \ .$$

Proof. Note that

$$R_0 = \sum_{a \in \Pi_{\mathcal{C}}} \mathrm{FPdim}(a) a$$

generates a 1-dimensional ideal of $K_{\mathbb{C}}(\mathcal{C}) = K_0(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$, and that $aR_0 = \mathrm{FPdim}(V_a)R_0$ for all $a \in \Pi_{\mathcal{C}}$. In particular, there is unit vector x with positive components such that $N_a x = \mathrm{FPdim}(V_a)x$ for all $a \in \Pi_{\mathcal{C}}$.

Let $\rho\,(A)$ denote the spectral radius of an $n \times n$ complex matrix A. Recall that the 2-norm of A is given by $\|A\|_2 = \sqrt{\rho\,(A^*A)}$. Thus, for $a \in \Pi_{\mathcal{C}}$, $\|N_a\|_2 \geq \mathrm{FPdim}(V_a)$. On the other hand,

$$\begin{aligned}\|N_a\|_2^2 = \rho(N_a^* N_a) = \rho(N_{a^*} N_a) &= \rho\left(\sum_{b \in \Pi_{\mathcal{C}}} N_{a^*,a}^b N_b\right) \\ &\leq \sum_{b \in \Pi_{\mathcal{C}}} N_{a^*,a}^b \,\mathrm{FPdim}(V_b) = \mathrm{FPdim}(V_a^*)\,\mathrm{FPdim}(V_a) = \mathrm{FPdim}(V_a)^2\,.\end{aligned}$$

Therefore, $\|N_a\|_2 = \mathrm{FPdim}(V_a)$ for all $a \in \Pi_{\mathcal{C}}$. The result then follows by the inequality

$$\|A\|_{max} \leq \|A\|_2 \leq n\|A\|_{max}$$

for any $n \times n$ complex matrix A. $\square$

Next we give an explicit bound on $\operatorname{ord}(T)$ in terms of the rank of $\mathcal{C}$.

Proposition 3.15. *If $\mathcal{C}$ is a modular category of rank r with modular data (S, T), then* $\operatorname{ord}(T) \leq 2^{2r/3+8}3^{2r/3}$.

Proof. By [5], any abelian subgroup G of $\mathfrak{S}_r$ satisfies $|G| \leq 3^{r/3}$. On the other hand, $[\mathbb{Q}(T) : \mathbb{Q}(S)] \leq 2^m$ where $m-1$ is the number of prime factors of $\operatorname{ord}(T)$. The Fundamental Theorem of Galois Theory can be utilized to relate m and $[\mathbb{Q}(S) : \mathbb{Q}]$. To do this, we note that $\mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q}(S))$. In particular, the structure of $\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q}(S))$ ensures that at least $m-3$ (non-trivial) cyclic factors survive in the quotient (the three possible exceptions correspond to primes 2 and 3 in $\operatorname{ord}(T)$.) In particular, the structure of the maximal abelian subgroup of $\mathfrak{S}_r$ ensures that $m - 3 \leq r/3 + 1$. In particular:

$$[\mathbb{Q}(T) : \mathbb{Q}] = [\mathbb{Q}(T) : \mathbb{Q}(S)]\,[\mathbb{Q}(S) : \mathbb{Q}] \leq 2^m 3^{r/3} \leq 2^{r/3+4}3^{r/3}$$

On the other hand, $\mathbb{Q}(T) = \mathbb{Q}_{\operatorname{ord}(T)}$ and so $[\mathbb{Q}(T) : \mathbb{Q}] = \varphi(\operatorname{ord}(T))$. In particular, if $\operatorname{ord}(T) \neq 2$ or 6, then $[\mathbb{Q}(T) : \mathbb{Q}] \geq \sqrt{\operatorname{ord}(T)}$. Thus $\operatorname{ord}(T) \leq 2^{2r/3+8}3^{2r/3}$ since $2^{2/3+8}3^{2/3} > 6$. $\square$

The last ingredient of the proof of Theorem 3.1 is a deep result from analytic number theory, which necessitates some further notational background.

Definition 3.16. Let $\mathbb{K}$ be a number field and $\mathcal{S}$ be a finite set of prime ideals in $\mathcal{O}_{\mathbb{K}}$. An element $\alpha \in \mathbb{K}^\times$ is a **$\mathcal{S}$-unit** if the prime factors of the principal fractional ideal (α) are all in $\mathcal{S}$.

Remark 3.17. The $\mathcal{S}$-units form a finitely generated multiplicative abelian group which we will denote by $\mathcal{O}_{\mathbb{K},\mathcal{S}}^\times$ [56].

Remark 3.18. It should be noted that $\mathcal{S}$-units are often treated adelically in which case a more delicate treatment involving places is required. While we will not need this level of detail here, it should be mentioned that it is utilized in [25]. A detailed introduction to $\mathcal{S}$-units and their relationship to adeles can be found in most modern texts on advanced number theory e.g. [56].

The $\mathcal{S}$-units arise in a wide range of subdisciplines in number theory and are typically found to obey an **$\mathcal{S}$-unit equation**:

$$x_0 + \cdots + x_n = 0, \quad \text{such that} \quad x_a \in \mathcal{O}_{\mathbb{K},\mathcal{S}}^\times$$

Such an equation is said to be a **proper $\mathcal{S}$-unit equation** if one requires that

$$x_{i_0} + \cdots + x_{i_r} \neq 0$$

for each proper, non-empty subset $\{i_0, i_1, \ldots, i_r\}$ of $\{0, 1, \ldots, n\}$.

In 1984, Evertse took up a study of $\mathcal{S}$-units and the $\mathcal{S}$-unit equation through analyzing the projective height [25]. By bounding the projective height, he showed that $\mathcal{S}$-units obey a remarkable finiteness condition *loc. cit.*:

Theorem 3.19. *If $\mathbb{K}$ is a number field, $\mathcal{S}$ a finite set of primes of $\mathbb{K}$, and n is a fixed positive integer, then there are only finitely many projective points $X = [x_0 : \cdots : x_n] \in \mathbb{P}^n\mathbb{K}$ satisfying the proper $\mathcal{S}$-unit equation:*

$$x_0 + \cdots + x_n = 0$$

With this last ingredient we can now proceed to the

Proof of the Rank-Finiteness Theorem. For fixed rank r, [2, Prop. 6] (or Proposition 3.15) ensures that $\operatorname{ord}(T)$ is bounded strictly in terms of r. For such $\operatorname{ord}(T)$, let $\mathcal{S}$ be the (finite) set of primes in $\mathbb{Q}_{\operatorname{ord}(T)}$ dividing $\operatorname{ord}(T)$. The Cauchy Theorem (Theorem 3.9) coupled with [17, Lem. 1.2] then implies that D^2 and d_a are $\mathcal{S}$-units for all simple objects V_a. Furthermore, the definition of the global dimension of the category, $0 = D^2 - d_0^2 - \cdots - d_{r-1}^2$, and the condition that d_a^2 and D^2 are real positive algebraic integers for all a implies that $\left(D^2, -d_0^2, \ldots, -d_{r-1}^2\right)$ satisfies a proper $\mathcal{S}$-unit equation. In particular, Theorem 3.19 shows that there are finitely many projective solutions to this equation. Recalling that $d_0^2 = 1$ allows us to fix the normalization and conclude that there is a upper bound on D^2 and a lower bound on d_a for all a.

On the other hand, $\operatorname{FPdim}(\mathcal{C}) = D^2/d_a^2$ for some simple dimension d_a. Consequently, the lower bound on d_a and an upper bound on D^2 imply an upper bound on $\operatorname{FPdim}(\mathcal{C})$. The result then follows from Corollary 3.13 and the observation that these bounds depend only on the rank. □

Corollary 3.20. *There are finitely many modularizable, pre-modular categories of rank r.*

Proof. We follow the notation in [13]. Let $\mathcal{D}$ be a pre-modular category such that $\mathcal{D}' \cong \operatorname{Rep}(G)$ is Tannakian and $\mathcal{D}_G = \mathcal{C}$ its modularization. Note that the equivariantization $\mathcal{C}^G \cong \mathcal{D}$ by [13]. First observe that under the (faithful) forgetful functor $\mathcal{D} \to \mathcal{C}$ the image of each simple object in $X \in \mathcal{D}$ is a sum of at most $|G|$ distinct simple objects in $\mathcal{C}$ (see [9, Prop. 2.1]). Since the rank of $\operatorname{Rep}(G)$ is at most r, $|G|$ is bounded as a function of r ([36]). Therefore, the rank of $\mathcal{D}_G$ is bounded in terms of r. By Theorem 3.1 there are only finitely many modularizations of rank r pre-modular categories. On the other hand, each modular category $\mathcal{C}$ has only finitely many equivariantizations, since the group of tensor autoequivalences $\operatorname{Aut}_{\otimes}(\mathcal{C})$ is finite. □

3.3 Asymptotics

The proof of Theorem 3.1 can be naively algorithmized to determine possible sets of fusion rules for modular categories of a given rank r.

Recall that $\mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}$ is a finitely generated abelian group [56]. A set of generators for the free part of $\mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}$ is known as a **system of fundamental $\mathcal{S}$-units** and there are known algorithms for computing such a system, e.g. [10]. We have:

Algorithm 3.21.

(0) Specify the rank, r.
(1) For each integer N with $1 \leq N \leq 2^{2r/3+8}3^{2r/3}$ perform steps 2-6.
(2) Form the set of primes $\mathcal{S}$, consisting of the prime factors of N over $\mathbb{Q}(\zeta_N)$.
(3) Determine a fundamental system of $\mathcal{S}$-units, $\epsilon_1, \ldots, \epsilon_{s-1}$.

(4) Solve the exponential Diophantine system:
$$1=\epsilon_1^{a_{r,1}}\cdots\epsilon_{s-1}^{a_{r,s-1}}-\sum_{j=1}^{r-1}\epsilon_1^{a_{j,1}}\cdots\epsilon_{s-1}^{a_{j,s-1}},\quad a_{j,k}\in\mathbb{Z}\,. \tag{3.1}$$
(5) Set $D^2=\epsilon_1^{a_{s,1}}\cdots\epsilon_{s-1}^{a_{s,s-1}}$ and $d_j^2=\epsilon_1^{a_{j,1}}\cdots\epsilon_{s-1}^{a_{j,s-1}}$.
(6) Determine the possible sets of fusion rules $N_{a,b}^c$ using Scholium 3.14 and the fact that $\mathrm{FPdim}(V_a)\le\mathrm{FPdim}(\mathcal{C})\le\max\{D^2/d_j^2:0\le j\le r-1\}$.

Remark 3.22. Given all possible sets of fusion rules in a given rank we can solve for all admissible modular data. The balancing equation (2.3) determines the S-matrix given all d_i, θ_i and N_{ij}^k, which Algorithm 3.21 provides.

We can also effectively decide whether a particular set of fusion rules corresponds to a modular category, using Tarski's Theorem (see [14]). We cannot, however, effectively determine all modular categories in a given rank, or even count them up to equivalence.

In any case, Algorithm 3.21 is very inefficient, and does not admit any obvious improvements for several reasons.

Firstly, we cannot expect a bound on $\mathrm{ord}\,(T)$ that is polynomial in the rank. For example, $\mathrm{ord}\,(T)$ for $\mathcal{C}=\mathrm{Rep}\,(D\mathfrak{S}_n)$ grows faster than any polynomial in the rank of $\mathcal{C}$. Indeed, $\mathrm{ord}(T)=\exp(\mathfrak{S}_n)=\mathrm{lcm}(1,\ldots,n)\approx e^n$, while the rank of $\mathrm{Rep}(D\mathfrak{S}_n)$ is superpolynomial but subexponential, with generating function: $\Pi_{k=1}^{\infty}(1-x^k)^{-\sigma(k)}$ where $\sigma(k)=\sum_{d|k}d$ [8]. However, for modular categories coming from quantum groups, $\mathrm{ord}(T)$ is linearly bounded in r. Secondly, the known algorithms for computing fundamental systems of $\mathcal{S}$-units rely on computing a shortest vector in a lattice, a problem which is known to be NP-hard. Thirdly, solving equation (3.1) is very difficult–the best bound on the number of solutions is quadruplely exponential:

Proposition 3.23. *For fixed rank r there are at most*
$$\sum_{m=1}^{2^{2r/3+8}3^{2r/3}}\left(2^{35}r^2\right)^{r^3\left(\varphi(m)^{\log_2(m)}+\varphi(m)/2+1\right)-r/2}$$
possible solutions to the dimension equation:
$$D^2=1+d_1^2+\cdots+d_{r-1}^2\,.$$

Proof. First note that by [26, Theorem 3], that there are at most $\left(2^{35}r^2\right)^{r^3(s+r_1+r_2)-r/2}$ solutions to the proper $\mathcal{S}$-unit equation:
$$x_1+x_2+\cdots+x_r=1$$
subject to $x_j\le x_{j+1}$ over a field $\mathbb{K}$, where s is the cardinality of $\mathcal{S}$, r_1 is the number of real embeddings of $\mathbb{K}$ and r_2 is the number of conjugate pair complex embeddings.

However, s depends on the prime factorization of $\mathrm{ord}\,(T)$. In particular, if p is a rational prime of $\mathrm{ord}\,(T)$, and there are at worst $\varphi\left(\mathrm{ord}\,(T)\right)$ primes lying over p in $\mathbb{Q}\left(\zeta_{\mathrm{ord}(T)}\right)$. Thus there are at most $\mathrm{ord}\,(T)^{\omega(\mathrm{ord}(T))}$ primes in $\mathcal{S}$, where $\omega\,(m)$ is defined to be the number of rational prime divisors of m. Elementary analysis reveals that $\omega\,(m)\le\log_2(m)$ and so $s\le\varphi\left(\mathrm{ord}\,(T)\right)^{\log_2(\mathrm{ord}(T))}+r_1+r_2$ where r_1 is the number of distinct real field embeddings of $\mathbb{K}$ into $\mathbb{C}$, and r_2 is the number of conjugate pair complex field embeddings. However, it is well-known that a non-trivial cyclotomic field has no real embeddings, in particular $r_2=\varphi\left(\mathrm{ord}\,(T)\right)/2$ and $s+r_1+r_2\le\varphi\left(\mathrm{ord}\,(T)\right)^{\log_2\mathrm{ord}(T)}+\varphi\left(\mathrm{ord}\,(T)\right)/2+1$. Combining these two results reveals that an upper bound on the number of possible dimension tuples $\left(D^2, 1, d_1^2, \ldots, d_{r-1}^2\right)$ for a rank r modular category with T-matrix of order $\operatorname{ord}(T)$ is $\left(2^{35}r^2\right)^{r^3\left(\varphi(\operatorname{ord}(T))^{\log_2(\operatorname{ord}(T))}+\varphi(\operatorname{ord}(T))/2+1\right)-r/2}$. The result then follows by summing over all possible values of $\operatorname{ord}(T)$ as determined by Proposition 3.15. □

It is interesting to ask whether or not this bound is asymptotically sharp. It is a widely held belief that modular categories are "sparse", a belief which is borne out in small rank, e.g., compare the 2 actual solutions in rank 2 with the theoretical bound of $\approx 2^{10^{78}}$. However, asymptotic analysis is still lacking and so one might ask:

Question 3.24. *Is there an asymptotic bound on the number of modular categories (up to equivalence) in terms of the rank which is better than those implied by Proposition* 3.23*?*

Remark 3.25. Etingof has pointed out ([16]) that the number of modular categories of rank r is not polynomially bounded. His example is as follows: Consider $V = (\mathbb{Z}/p)^m$, a vector space over F_p of dimension m, where $p > 3$ is a prime and m is large. It is well known that $H^3(V, \mathbb{C}^*) = S^2V^* \oplus \wedge^3 V^*$, (see e.g. [18, Lem. 7.6(iii)]). Because of the summand $\wedge^3 V^*$, the number of such cohomology classes for large m is at least p^{Cm^3}, for some $C > 0$, even if we mod out by automorphisms (which form a group of order at most p^{m^2}). Now take the category $\mathrm{Vec}(V, \omega)$ of V-graded vector spaces with associativity defined by the cohomology class ω, and let $Z(V, \omega)$ be the Drinfeld center of such a category. It is known [23] that such categories $Z(V, \omega)$ and $Z(V, \omega')$ are braided equivalent if and only if $\mathrm{Vec}(V, \omega)$ is Morita equivalent to $\mathrm{Vec}(V, \omega')$ via an indecomposable module category. But the indecomposable module categories over $\mathrm{Vec}(V, \omega)$ are known to be parameterized [45] by subspaces $W \subset V$ and 2-cochain ψ on W such that $d\psi = \omega|_W$, up to gauge transformation. There are at most p^{m^2} subspaces, and freedom in choosing ψ is in $\wedge^2 W^*$, so again there are at most p^{m^2}. As m^3 dominates m^2, we still have at least p^{Cm^3} such categories, even up to Morita equivalence, and hence modular categories up to equivalence. On the other hand, $\mathrm{FPdim}(Z(V, \omega)) = p^{2m}$, so the rank is at most p^{2m}. Thus we get that the number of modular categories of rank$\leq r$ is at least $e^{(c\log(r)^3)} = r^{c\log(r)^2}$, for some $c > 0$, which is faster than any polynomial in r.

Along similar lines, one might ask

Question 3.26. *Is there an explicit upper bound on* $\mathrm{FPdim}(\mathcal{C})$ *solely in terms of the rank?*

Remark 3.27. This question seems tractable as the analysis of Evertse shows that the projective height of $\left[-D^2 : 1 : d_1^2 : \cdots : d_{r-1}^2\right]$ can be bounded in terms of field data and hence in terms of $\operatorname{ord}(T)$. This suggests that the relationship between the FP-dimension and the categorical dimension can be combined, as in the proof of Theorem 3.1, to study this question.

Etingof asked [16]:

Question 3.28. *Can* $\left|D^2 - 1\right|$ *be explicitly bounded in terms of the rank?*

Remark 3.29. This question can be reduced to the problem of finding a shortest vector by exploiting the lattice structure of $\mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}$ under an appropriate embedding into Euclidean space.

4 Arithmetic Properties of Modular Categories

4.1 Galois Action on Modular Data

In this subsection we derive some consequences of the results in Subsection 2.2.4.

Let $\mathcal{C}$ be a modular category with admissible modular data (S,T). The splitting field of $K_0(\mathcal{C})$ is $\mathbb{K}_{\mathcal{C}} = \mathbb{Q}\left(\frac{S_{ij}}{S_{0j}} \mid i,j \in \Pi_{\mathcal{C}}\right) = \mathbb{F}_S$, and we define $\mathrm{Gal}(\mathcal{C}) = \mathrm{Gal}(\mathbb{K}_{\mathcal{C}}/\mathbb{Q}) = \mathrm{Gal}(S)$. We denote by $\mathbb{K}_j = \mathbb{Q}\left(\frac{S_{ij}}{S_{0j}} \mid i \in \Pi_{\mathcal{C}}\right)$ for $j \in \Pi_{\mathcal{C}}$. Obviously, $\mathbb{K}_{\mathcal{C}}$ is generated by the subfields $\mathbb{K}_j$, $j \in \Pi_{\mathcal{C}}$.

As in Subsection 2.2.4 there exists a unique $\hat{\sigma} \in \mathrm{Sym}(\Pi_{\mathcal{C}})$ such that

$$\sigma\left(\frac{S_{ij}}{S_{0j}}\right) = \frac{S_{i\hat{\sigma}(j)}}{S_{0\hat{\sigma}(j)}}$$

for all $i,j \in \Pi_{\mathcal{C}}$. In particular the map $\sigma \to \hat{\sigma}$ defines an isomorphism between $\mathrm{Gal}(\mathcal{C})$ and an (abelian) subgroup of the symmetric group $\mathrm{Sym}(\Pi_{\mathcal{C}})$. We will often abuse notation and identify $\mathrm{Gal}(\mathcal{C})$ with its image in $\mathrm{Sym}(\Pi_{\mathcal{C}})$, and the $\mathrm{Gal}(\mathcal{C})$-orbit of $j \in \Pi_{\mathcal{C}}$ is simply denoted by $\langle j \rangle$. Complex conjugation corresponds to the permutation $i \mapsto i^*$ for $i \in \Pi_{\mathcal{C}}$. In view of (2.9), $j \in \Pi_{\mathcal{C}}$ is self-dual if, and only if, $\mathbb{K}_j$ is real subfield.

Remark 4.1. Since $\mathbb{K}_{\mathcal{C}}$ is Galois over $\mathbb{Q}$, for any Galois extension $\mathbb{A}$ over $\mathbb{K}_{\mathcal{C}}$ in $\mathbb{C}$, the restriction $\mathrm{res} : \mathrm{Aut}(\mathbb{A}) \to \mathrm{Gal}(\mathcal{C})$ defines a surjective group homomorphism. Therefore, the group $\mathrm{Aut}(\mathbb{A})$ acts on $\Pi_{\mathcal{C}}$ via the restriction maps onto $\mathrm{Gal}(\mathcal{C})$, and so the $\mathrm{Aut}(\mathbb{A})$-orbits are the same as the $\mathrm{Gal}(\mathcal{C})$-orbits. Again, we denote by $\hat{\sigma}$ the associated permutation of $\sigma \in \mathrm{Aut}(\mathbb{A})$. Then we have $\hat{\sigma} = \mathrm{id}_{\Pi_{\mathcal{C}}}$ if, and only if, $\sigma \in \mathrm{Gal}(\mathbb{A}/\mathbb{K}_{\mathcal{C}})$.

Lemma 4.2. *For $j \in \Pi_{\mathcal{C}}$ and $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$, $\mathbb{K}_{\hat{\sigma}(j)} = \mathbb{K}_j$. Moreover, $[\mathbb{K}_j : \mathbb{Q}] = |\langle j \rangle| \le |\Pi_{\mathcal{C}}|$. If j is self-dual, then every class in the orbit $\langle j \rangle$ is self-dual. In particular, every class in the orbit $\langle 0 \rangle$ is self-dual.*

Proof. As we have seen, $\phi_j : K_0(\mathcal{C}) \to \mathbb{K}_{\mathcal{C}}$, $\phi_j(i) = \frac{S_{ij}}{S_{0j}}$, defines a linear character of $K_0(\mathcal{C})$. Therefore,

$$\frac{S_{aj}}{S_{0j}}\frac{S_{bj}}{S_{0j}} = \sum_{c \in \Pi_{\mathcal{C}}} N_{ab}^c \frac{S_{cj}}{S_{0j}}\,.$$

Thus, the $\mathbb{Q}$-linear span of $\{S_{ij}/S_{0j} \,|\, i \in \Pi_{\mathcal{C}}\}$ is field, and hence equals to $\mathbb{K}_j$. Since $\mathbb{K}_j$ is a subfield of $\mathbb{K}_{\mathcal{C}}$, $\mathbb{K}_j/\mathbb{Q}$ is a normal extension. Therefore,

$$\mathbb{K}_j = \sigma(\mathbb{K}_j) = \mathbb{Q}\left(\sigma\left(\frac{S_{ij}}{S_{0j}}\right) \,\middle|\, i \in \Pi_{\mathcal{C}}\right) = \mathbb{Q}\left(\frac{S_{i\hat{\sigma}(j)}}{S_{0\hat{\sigma}(j)}} \,\middle|\, i \in \Pi_{\mathcal{C}}\right) = \mathbb{K}_{\hat{\sigma}(j)}\,.$$

Let $\mathbb{A}/\mathbb{Q}$ be any finite Galois extension containing $\mathbb{K}_j$, and H the kernel of the restriction map $\mathrm{res} : \mathrm{Gal}(\mathbb{A}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{K}_j/\mathbb{Q})$. Then $\sigma \in H$ if, and only if,

$$S_{ij}/S_{0j} = \sigma(S_{ij}/S_{0j}) = S_{i\hat{\sigma}(j)}/S_{0\hat{\sigma}(j)}$$

for all $i \in \Pi_{\mathcal{C}}$. Thus, H is equal to the stabilizer of j, and hence

$$[\mathbb{K}_j : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{K}_j/\mathbb{Q})| = |\mathrm{Aut}(\mathbb{A})/H| = |\langle j \rangle|.$$

The last assertion follows immediately from the fact that j is self-dual if, and only if, $\mathbb{K}_j$ is a real abelian extension over $\mathbb{Q}$. $\square$

Lemma 4.3. *Let $\mathcal{C}$ be a modular category with modular data (S,T).*

(i) *$\mathcal{C}$ is pseudo-unitary if and only if $d_i = \pm\,\mathrm{FPdim}(V_i)$ for all $i \in \Pi_{\mathcal{C}}$.*

(ii) *$\mathcal{C}$ is integral if, and only if, $d_i \in \mathbb{Z}$ for all $i \in \Pi_{\mathcal{C}}$ if, and only if, $|\langle 0 \rangle| = 1$.*

(iii) *If $|\langle j \rangle| = 1$ for all $j \notin \langle 0 \rangle$, then there exists an $\sigma \in \mathrm{Aut}\left(\overline{\mathbb{Q}}\right)$ such that $(\sigma(S), \sigma(T))$ is realizable modular data for some pseudo-unitary modular category.*

Proof. The pseudo-unitarity condition is: $\sum_{j\in\Pi_{\mathcal{C}}} d_j^2 = \sum_{j\in\Pi_{\mathcal{C}}} \mathrm{FPdim}(V_j)^2$, and $|d_i| \leq \mathrm{FPdim}(V_i)$ so pseudo-unitarity fails if and only if $|d_i| < \mathrm{FPdim}(V_i)$ for some i. This proves (i).

For (ii), first observe that $|\langle 0\rangle| = 1$ if and only if $d_i \in \mathbb{Z}$ for all i proving the second equivalence in (b). By [22, Prop. 8.24] weakly integral fusion categories are pseudo-unitary. Applying (a) we see that $d_i \in \mathbb{Z}$ if $\mathrm{FPdim}(V_i) \in \mathbb{Z}$. On the other hand, if $d_i \in \mathbb{Z}$ for all i we have $D^2 = \sum_i d_i^2 \in \mathbb{Z}$ and $\mathrm{FPdim}(V_i) = S_{i,j}/d_j \in \mathbb{R}$ for some j. Since $\sum_i (S_{i,j})^2 = D^2 \in \mathbb{Z}$, $d_j^2 \sum_i (\mathrm{FPdim}(V_i))^2 \in \mathbb{Z}$, and in particular $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Q}$. But $\mathrm{FPdim}(\mathcal{C})$ is an algebraic integer, so we see that in this case $\mathcal{C}$ is weakly integral, and hence pseudo-unitary.

We have $\mathrm{FPdim}(V_i) = S_{i,j}/d_j = \phi_j(i)$ for some j. If $|\langle j\rangle| = 1$ then $S_{i,j}/d_j \in \mathbb{Z}$ for $i \in \Pi_{\mathcal{C}}$, and so $\mathcal{C}$ is pseudo-unitary. If $|\langle j\rangle| > 1$, then $j \in \langle 0\rangle$ by assumption. Let $\sigma \in \mathrm{Aut}\left(\overline{\mathbb{Q}}\right)$ such that $\hat{\sigma}(0) = j$ (which exists by extension). We consider a Galois conjugate modular category $\mathcal{C}'$ with the (realizable) modular data $(\sigma(S), \sigma(T))$. It is immediate to see that $\mathcal{C}'$ is pseudo-unitary since $\sigma(\phi_j)$ is the first row/column of $\sigma(S)$. This completes the proof of (iii). $\square$

Note that, by Lemma 4.2, a modular category which satisfies the condition (c) of the preceding lemma must be self-dual.

Now we consider a normalized modular pair (s,t) of $\mathcal{C}$. Since $\frac{s_{ij}}{s_{0j}} = \frac{S_{ij}}{S_{0j}}$ we have

$$\mathbb{K}_j = \mathbb{Q}\left(\frac{s_{ij}}{s_{0j}} \mid i \in \Pi_{\mathcal{C}}\right) \text{ and } \mathbb{K}_{\mathcal{C}} = \mathbb{Q}\left(\frac{s_{ij}}{s_{0j}} \mid i,j \in \Pi_{\mathcal{C}}\right).$$

For any $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$, (2.13) implies that

$$S_{ij} = \epsilon_\sigma(i)\epsilon_{\sigma^{-1}}(j) S_{\hat{\sigma}(i)\hat{\sigma}^{-1}(j)}\,. \tag{4.1}$$

for some sign function $\epsilon_\sigma : \Pi_{\mathcal{C}} \to \{\pm 1\}$ depending on s.

Remark 4.4.

(i) Observe that while $\epsilon_\sigma(i)$ depends on the choice of the normalized pair (s,t), the quantity $\epsilon_\sigma(i)\epsilon_{\sigma^{-1}}(j)$ does not.

(ii) Observe that $G : \mathrm{Aut}(\overline{\mathbb{Q}}) \to GL(\Pi_{\mathcal{C}}, \mathbb{Z})$, $\sigma \mapsto G_\sigma := \sigma(s)s^{-1}$, defines a group homomorphism. If G_σ is a diagonal matrix or, equivalently, $\hat{\sigma} = \mathrm{id}_{\Pi_{\mathcal{C}}}$, then $\sigma(s_{ij}) = \epsilon_\sigma(j)s_{ij} = \epsilon_\sigma(i)s_{ij}$ for all $i,j \in \Pi_{\mathcal{C}}$. In particular, $\epsilon_\sigma(j)s_{0j} = \epsilon_\sigma(0)s_{0j}$. Since $s_{0j} \neq 0$ for all $j \in \Pi_{\mathcal{C}}$, $\epsilon_\sigma(j) = \epsilon_\sigma(0) = \pm 1$ for all $j \in \Pi_{\mathcal{C}}$. Therefore, $G_\sigma = \pm I$ if $\hat{\sigma} = \mathrm{id}_{\Pi_{\mathcal{C}}}$ (cf. [2, Lem. 5]). Therefore, $\mathrm{im}\, G$ is either isomorphic to $\mathrm{Gal}(\mathcal{C})$ or an abelian extension of $\mathrm{Gal}(\mathcal{C})$ by $\mathbb{Z}_2$.

The following results will be useful in Section 5.

Lemma 4.5. *If $\hat{\sigma}$ is an order 2 permutation in $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}})$, such that $\hat{\sigma}$ has a fixed point (for example if the rank of $\mathcal{C}$ is odd) then $\epsilon_\sigma(j) = \epsilon_\sigma(\hat{\sigma}(j))$ and*

$$S_{ij} = \epsilon_\sigma(i)\epsilon_\sigma(j) S_{\hat{\sigma}(i)\hat{\sigma}(j)}$$

for all $i,j \in \Pi_{\mathcal{C}}$. In particular,

$$S_{ii} = S_{\hat{\sigma}(i)\hat{\sigma}(i)}$$

for all $i \in \Pi_{\mathcal{C}}$.

Proof. Let ℓ be a fixed point of $\hat{\sigma}$. Thus $\sigma^2(s_{0\ell}) = s_{0\ell}$ and so $\epsilon_{\sigma^2}(\ell) = 1$. Since G_{σ^2} is diagonal and the ℓ-th diagonal entry is 1, $G_{\sigma^2} = \mathrm{id}$ by Remark 4.4. Thus,

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

for all j. Therefore, $\epsilon_\sigma(j) = \epsilon_\sigma(\hat{\sigma}(j))$ for all j. On the other hand, we always have $\epsilon_\sigma(j)\epsilon_{\sigma^{-1}}(\hat{\sigma}(j)) = 1$, we find $\epsilon_\sigma = \epsilon_{\sigma^{-1}}$. Thus, by (4.1), we have

$$S_{ij} = \epsilon_\sigma(i)\epsilon_{\sigma^{-1}}(j)S_{\hat{\sigma}(i)\hat{\sigma}^{-1}(j)} = \epsilon_\sigma(i)\epsilon_\sigma(j)S_{\hat{\sigma}(i)\hat{\sigma}(j)}\,. \quad \square$$

Lemma 4.6. *If $\mathcal{C}$ is a rank $r \geq 5$ modular category with modular data (S,T) such that* $\mathrm{Gal}\,(\mathcal{C}) = \langle (0\;1) \rangle$ *then:*

(i) $d_1 > 0$,

(ii) $\frac{1}{d_1} + d_1$, D^2/d_1, *and* d_i^2/d_1 *are rational integers for* $i \geq 2$.

(iii) *Defining* $\epsilon_j = \frac{S_{1j}}{d_j}$ *for each* $j \geq 2$ *we have*

  (a) $\epsilon_j \in \{\pm 1\}$.

  (b) *There exist* i, j *such that* $\epsilon_i = -\epsilon_j$, *and in this case* $S_{ij} = 0$.

Proof. By Lemma 4.5 we see that $S_{11} = 1$. Therefore, the trace of d_1 is $d_1 + 1/d_1$ and the norm of d_i for $i \geq 2$ is d_i^2/d_1 so these must be integers. This implies that $D^2/d_1 = d_1 + 1/d_1 + \sum_{i=2}^{r-1} d_i^2/d_1 \in \mathbb{Z}$.

If the Frobenius-Perron dimension were a multiple of column j for some $j > 1$ then $\mathrm{FPdim}(V_i) = S_{ij}/d_j$ is an integer for all i as as $|\langle j \rangle| = 1$. Then $\mathcal{C}$ would be integral, and so $d_i \in \mathbb{Z}$ by Lemma 4.3(ii) for all i. However, this contradicts the fact that $|\langle 0 \rangle| = 2$. So the FP-dimension must be a scalar multiple of one of the first two columns. In any of these two cases, we find $d_1 > 0$.

By (4.1), we have $S_{1j} = \pm S_{0j}$ for $j \geq 2$, so $\epsilon_j := \frac{S_{1j}}{d_j} = \pm 1$ proving (iii)(c). Now orthogonality of the first two rows of S gives us: $2d_1 + \sum_{j\geq 2}\epsilon_j d_j^2 = 0$ or $2 = -\sum_{j\geq 2}\epsilon_j d_j^2/d_1$, a sum of integers. Since $r \geq 5$ we see that it is impossible for all of the ϵ_j to have identical signs. On the other hand we have $\epsilon_j d_j = S_{1j} = \epsilon_\sigma(1)\epsilon_\sigma(j)S_{0j}$ for each $j \geq 2$, so $\epsilon_j = \epsilon_\sigma(1)\epsilon_\sigma(j)$. If $\epsilon_i = -\epsilon_j$ then $\epsilon_\sigma(i) = -\epsilon_\sigma(j)$ so that $S_{ij} = \epsilon_\sigma(i)\epsilon_\sigma(j)S_{\hat{\sigma}(i)\hat{\sigma}(j)} = -S_{ij}$ by Lemma 4.5. Hence $S_{ij} = 0$. $\square$

Lemma 4.7. *Suppose $\mathcal{C}$ is a modular category of* odd *rank $r \geq 5$. Then* $(0\,1)(2\,\cdots\,r-1) \notin \mathrm{Gal}(\mathcal{C})$.

Proof. Suppose $\hat{\sigma} = (0\,1)(2\,\cdots\,r-1)$ for some $\sigma \in \mathrm{Gal}(\mathcal{C})$. Since $S_{ij} = \pm S_{\hat{\sigma}(i)\hat{\sigma}^{-1}(j)}$ and r odd,

$$S_{11} = \epsilon \text{ and } S_{ij} = \epsilon_{ij}S_{02} = \epsilon_{ij}d_2$$

for all $0 \leq i \leq 1$, $2 \leq j \leq r-1$, where ϵ, ϵ_{ij} are ± 1. In particular, the first two rows of the matrix S are real, $\sigma(d_2) = \epsilon_{12}d_2/d_1$, and $\frac{S_{1j}}{S_{0j}} = \frac{\epsilon_{1j}}{\epsilon_{0j}} \in \mathbb{Z}$ for $j \geq 2$. Thus

$$\frac{\epsilon_{1j}}{\epsilon_{0j}} = \frac{S_{1j}}{S_{0j}} = \sigma\left(\frac{S_{1j}}{S_{0j}}\right) = \frac{S_{1\hat{\sigma}(j)}}{S_{0\hat{\sigma}(j)}} \text{ for all } j \geq 2\,,$$

and hence $\frac{S_{1j}}{S_{0j}} = \frac{\epsilon_{12}}{\epsilon_{02}} = \epsilon'$ for $j \geq 2$. By orthogonality of the first two rows of S, we find

$$0 = d_1(1+\epsilon) + \sum_{j\geq 2} S_{1j}S_{0j} = d_1(1+\epsilon) + \epsilon'\sum_{j\geq 2} S_{0j}^2 = d_1(1+\epsilon) + \epsilon'(r-2)d_2^2\,.$$

Since $r-2 \neq 0$, $\epsilon = 1$ and $2 = -\epsilon'(r-2)d_2^2/d_1$. Note that both d_2/d_1 and d_2 are algebraic integers.The equation implies $d_2^2/d_1 \in \mathbb{Z}$ and so $(r-2) \mid 2$. This is absurd as $r-2 \geq 3$. $\square$

Lemma 4.8. *Suppose $\mathcal{C}$ is a modular category of* odd *rank $r \geq 5$. If the isomorphism classes $r-2, r-1$ are self-dual, then*

$$(0\,1\,\cdots\,r-3)(r-2\;r-1) \notin \mathrm{Gal}(\mathcal{C}).$$

Proof. Suppose $\hat{\sigma} = (0\,1\,\cdots\,r-3)(r-2\;r-1) \in \mathrm{Gal}(\mathcal{C})$. Since $S_{ij} = \pm S_{\hat{\sigma}(i)\hat{\sigma}^{-1}(j)}$ and r odd,

$$S_{r-1,r-1} = \epsilon S_{r-2,r-2} \text{ and } S_{i,j} = \epsilon_{ij} S_{0,r-2} = \epsilon_{ij} d_{r-2}$$

for all $0 \leq i \leq r-3$, $r-2 \leq j \leq r-1$, where ϵ, ϵ_{ij} are ± 1. Therefore, for $0 \leq i \leq r-3$, $\frac{S_{i,r-1}}{d_{r-1}} = \sigma\left(\frac{S_{i,r-2}}{d_{r-2}}\right) = \frac{S_{i,r-2}}{d_{r-2}}$. Since the last two columns are real and orthogonal, we find

$$0 = S_{r-1,r-2}S_{r-1,r-1}(1+\epsilon) + \sum_{i=0}^{r-3} S_{i,r-2}S_{i,r-1} = S_{r-1,r-2}S_{r-1,r-1}(1+\epsilon) + (r-2)d_{r-1}d_{r-2}\,.$$

Since $(r-2)d_{r-1}d_{r-2} \neq 0$ we must have $\epsilon = 1$, therefore $2\frac{S_{r-1,r-2}}{d_{r-2}}\frac{S_{r-1,r-1}}{d_{r-1}} = r-2$. Since $\frac{S_{r-1,r-2}}{d_{r-2}}\frac{S_{r-1,r-1}}{d_{r-1}}$ is an algebraic integer, the equation implies it is a rational integer and so $r-2$ is even, a contradiction. $\square$

For weakly integral modular categories, a positive dimension function is constant on the orbits of the Galois action on $\Pi_{\mathcal{C}}$ (via $\sigma \to \hat{\sigma}$):

Lemma 4.9. *Let $\mathcal{C}$ is a weakly integral modular in which $d_a > 0$ for all $a \in \Pi_{\mathcal{C}}$. Then we have $d_{\hat{\sigma}(a)} = d_a$ for all $\sigma \in \mathrm{Gal}\,(\mathcal{C})$ and $a \in \Pi_{\mathcal{C}}$.*

Proof. Since $\mathcal{C}$ is weakly integral, $d_a^2/D^2 \in \mathbb{Q}$. Consider the Galois group action on the normalized S-matrix $s = \frac{1}{D}S$. We find $d_a^2/D^2 = \sigma(d_a^2/D^2) = d_{\hat{\sigma}(a)}^2/D^2$ for all $\sigma \in \mathrm{Gal}\,(\mathcal{C})$ and $a \in \Pi_{\mathcal{C}}$, and so the result follows. $\square$

4.2 Modularly Admissible Fields

The abelian number fields $\mathbb{F}_t, \mathbb{F}_T, \mathbb{F}_s$ and $\mathbb{F}_S$ described in Section 2.2.4 (see also [15, 47]) have the lattice relations

$$\begin{tikzcd}[column sep=small] & \mathbb{F}_t \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{F}_T \arrow[dr, dash] & & \mathbb{F}_s \arrow[dl, dash] \\ & \mathbb{F}_S & \end{tikzcd} \quad . \tag{4.2}$$

Moreover, by Lemma 2.10, the Galois group $\mathrm{Gal}(\mathbb{F}_t/\mathbb{F}_S)$ is an elementary 2-group. This implies all the subextensions among these fields will satisfy the same condition. We will call the extension $\mathbb{L}/\mathbb{K}$ **modularly admissible** if $\mathbb{L}$ is a cyclotomic field and $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is an elementary 2-group, i.e. $\mathbb{L}$ is a multi-quadratic extension of $\mathbb{K}$. In this section we will describe the order of a cyclotomic field $\mathbb{L}$ when $\mathbb{L}/\mathbb{K}$ is modularly admissible and $[\mathbb{K} : \mathbb{Q}]$ is a prime power.

Remark 4.10. If $\mathbb{L}/\mathbb{K}$ is modularly admissible, then $\mathbb{L}'/\mathbb{K}'$ is also modularly admissible for any subextensions $\mathbb{K}' \subset \mathbb{L}'$ of $\mathbb{K}$ in $\mathbb{L}$. In particular, $\mathbb{Q}_{\mathfrak{f}}/\mathbb{K}$ is modularly admissible where $\mathfrak{f} := \mathfrak{f}(\mathbb{K})$ is the *conductor* of $\mathbb{K}$, i.e. the smallest integer n such that $\mathbb{K}$ embeds into $\mathbb{Q}_n$.

A restatement of [15, Prop. 6.5] in this terminology is:

Proposition 4.11. *If $\mathbb{Q}_n/\mathbb{K}$ is modularly admissible and $\mathfrak{f}$ is the conductor of $\mathbb{K}$, then*

(i) $\frac{n}{\mathfrak{f}} \mid 24$ *and* $\gcd(\frac{n}{\mathfrak{f}}, \mathfrak{f}) \mid 2$ *and*

(ii) $\mathrm{Gal}\,(\mathbb{Q}_n/\mathbb{Q}_{\mathfrak{f}})$ *is subgroup of* $(\mathbb{Z}/2\mathbb{Z})^3$. □

Recall that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and that for any subfield $\mathbb{K}$ of $\mathbb{Q}_n$, we have the exact sequence

$$1 \to \mathrm{Gal}(\mathbb{Q}_n/\mathbb{K}) \to \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \xrightarrow{\mathrm{res}} \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \to 1\,. \tag{4.3}$$

In addition, if $\mathbb{Q}_n/\mathbb{K}$ is modularly admissible, then $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{K})$ is isomorphic to a subgroup of the maximal elementary 2-subgroup, $\Omega_2(\mathbb{Z}/n\mathbb{Z})^\times$, of $(\mathbb{Z}/n\mathbb{Z})^\times$. In particular, $\frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/n\mathbb{Z})^\times}$ is a homomorphic image of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Lemma 4.12. *If $\mathbb{Q}_n/\mathbb{K}$ is modularly admissible and $[\mathbb{K}:\mathbb{Q}]$ is odd, then $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/n\mathbb{Z})^\times}$ and $q \equiv 3 \mod 4$ for any odd prime $q \mid n$. If, in addition, $[\mathbb{K}:\mathbb{Q}]$ is a power of an odd prime p, then every prime factor $q > 3$ of n is a simple factor of the form $q = 2p^r + 1$ for some integer $r \geq 1$. Moreover, if $p > 3$, then r must be odd and $p \equiv 2 \mod 3$.*

Proof. It follows from the exact sequence 4.3 that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{K})$ is a Sylow 2-subgroup of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ and hence $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{K}) = \Omega_2\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Therefore, we obtain the isomorphism $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/n\mathbb{Z})^\times}$. Suppose $q > 3$ is a prime factor of n and ℓ is the largest integer such that $q^\ell \mid n$. Then, by the Chinese Remainder Theorem $(\mathbb{Z}/q^\ell\mathbb{Z})^\times$ is a direct summand of $(\mathbb{Z}/n\mathbb{Z})^\times$, and hence $\frac{(\mathbb{Z}/q^\ell\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/q^\ell\mathbb{Z})^\times}$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. In particular, $\varphi(q^\ell)/2 = q^\ell\left(\frac{q-1}{2}\right)$ is odd, and this implies $q \equiv 3 \mod 4$.

If, in addition, $[\mathbb{K}:\mathbb{Q}] = p^h$ for some $h \geq 0$, then $q^{\ell-1}\left(\frac{q-1}{2}\right) \mid p^h$ when $q > 3$. This forces $\ell = 1$ and $q = 2 \cdot p^r + 1$ for some positive integer $r \leq h$. Furthermore, if $p > 3$, then $q = 2 \cdot p^r + 1 \equiv 0 \mod 3$ whenever r is even or $p \equiv 1 \mod 3$. The last statement then follows. □

When the abelian number field $\mathbb{K}$ has a prime power degree over $\mathbb{Q}$, more refined statements on a modularly admissible extension $\mathbb{Q}_n/\mathbb{K}$ can now be stated as

Proposition 4.13. *Let $\mathbb{Q}_n/\mathbb{K}$ be a modularly admissible extension and*

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_m}\mathbb{Z}$$

for some prime p and $0 < r_1 \leq \cdots \leq r_m$, and set $q_j = 2 \cdot p^{r_j} + 1$ for $j = 1, \ldots, m$. Then:

(i) *If $p > 3$, then n admits the factorization $n = f \cdot q_1 \cdots q_m$ where $f \mid 24$ and $q_1, \ldots, q_m$ are distinct primes. In particular, $r_1, \ldots, r_m$ are distinct odd integers and $p \equiv 2 \mod 3$.*

(ii) *For $p = 3$, one of the following two statements holds.*

   (a) *$9 \nmid n$ and $n = f \cdot q_1 \cdots q_m$ where $f \mid 24$ and $q_1, \ldots, q_m$ are distinct primes.*

   (b) *$9 \mid n$, and there exists $i \in \{1, \ldots, m\}$ such that $\{q_j \mid j \neq i\}$ is a set of $m-1$ distinct primes and $n = f \cdot 3^{r_i+1} \cdot q_1 \cdots q_{r_{i-1}} \cdot q_{r_{i+1}} \cdots q_m$ where $f \mid 8$.*

(iii) *For $p = 2$, $n = 2^a \cdot p_1 \cdots p_l$ where $p_1, \ldots, p_l$ are distinct Fermat primes and a is a non-negative integer.*

Proof. For $p = 2$, the exact sequence 4.3 implies that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is a 2-group and so $\varphi(n)$ is a power of 2. Hence, (iii) follows.

For any odd prime p, it follows from Lemma 4.12 that $n = 2^a 3^b q_1 \cdots q_l$ for some integers $a, b \geq 0$ and odd primes $q_1 < \cdots < q_l$ of the form $q_j = 2p^{a_j} + 1$ for some integer $a_j \geq 1$. Therefore,

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/n\mathbb{Z})^\times} \cong \frac{(\mathbb{Z}/2^a\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/2^a\mathbb{Z})^\times} \times \frac{(\mathbb{Z}/3^b\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/3^b\mathbb{Z})^\times} \times \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_l}\mathbb{Z}\,. \tag{4.4}$$

For $p > 3$, $(\mathbb{Z}/2^a\mathbb{Z})^\times \times (\mathbb{Z}/3^b\mathbb{Z})^\times$ must be an elementary 2-group otherwise the p power $\left|\frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/n\mathbb{Z})^\times}\right|$ has a factor of 2 or 3. Therefore, $0 \leq a \leq 3$, $0 \leq b \leq 1$ (or equivalently, $f = 2^a 3^b$ is a divisor of 24), and

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_l}\mathbb{Z}\,.$$

By the uniqueness of invariant factors, $l = m$ and $a_j = r_j$ for $j = 1, \ldots, m$. The last statement of (i) follows directly from Lemma 4.12.

For $p = 3$ and $9 \nmid n$, the argument for the case $p > 3$ can be repeated here to arrive the same conclusion (iii)(a). For $p = 3$ and $9 \mid n$, $b \leq 2$ and so

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \frac{(\mathbb{Z}/2^a\mathbb{Z})^\times}{\Omega_2(\mathbb{Z}/2^a\mathbb{Z})^\times} \times \mathbb{Z}/3^{b-1}\mathbb{Z} \times \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_l}\mathbb{Z}\,.$$

Therefore, $(\mathbb{Z}/2^a\mathbb{Z})^\times$ is an elementary 2-group, or $0 \leq a \leq 3$. By the uniqueness of invariant factors $l = m - 1$, $b - 1 = r_i$ for some i and $(a_1, \ldots, a_{m-1}) = (r_1, \ldots, \hat{r_i}, \ldots r_m)$. This proves (iii)(b). $\square$

Corollary 4.14. *If $\mathbb{Q}_n/\mathbb{K}$ is modularly admissible and $\mathbb{K}/\mathbb{Q}$ is a multi-quadratic extension, then $n \mid 240$.*

Proof. Since $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{K})$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ are elementary 2-groups, in view of (4.3), $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ is an abelian 2-group whose exponent $e \mid 4$. By Proposition 4.13 (iii), $n = 2^a p_1 \cdots p_l$ where $a \geq 0$ and $p_1 < \cdots < p_l$ are Fermat primes. If $p_l > 5$, then $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ has a cyclic subgroup of order $p_l - 1 > 4$; this contradicts $e \mid 4$. On the other hand, if $a \geq 5$, $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ has a cyclic subgroup of order 8 which is also absurd. Therefore, n must be a factor of $2^4 \cdot 3 \cdot 5 = 240$. $\square$

These techniques combined with the Cauchy Theorem 3.9 can be used to classify low rank integral modular categories with a given Galois group. For example:

Lemma 4.15. *There are no rank 7 integral modular categories satisfying $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}/5\mathbb{Z}$.*

Proof. We may assume $d_a > 0$ for all $a \in \Pi_{\mathcal{C}}$, by Lemma 4.3. By applying Lemma 4.9 we see that the dimensions are 1, d_1 (with multiplicity 5) and d_2 (with multiplicity 1). In this case Proposition 4.13(i) and the Cauchy Theorem imply that the prime divisors of d_1, d_2 and D^2 lie in $\{2, 3, 11\}$. Moreover, $D \in \mathbb{Z}$ since $|\mathrm{Gal}(\mathcal{C})|$ is odd. Examining the dimension equation $D^2 = 1 + d_1^2 + 5d_2^2$ modulo 5 we obtain $D^2 = 1 + d_1^2$. The non-zero squares modulo 5 are ± 1, so $D^2, d_1^2 \in \{\pm 1\}$ which give no solutions. $\square$

4.3 Representation Theory of $SL(2,\mathbb{Z})$

Definition 4.16. Let $\rho : SL(2,\mathbb{Z}) \to GL(r,\mathbb{C})$ be a representation of $SL(2,\mathbb{Z})$.

(i) ρ is said to be **non-degenerate** if the r eigenvalues of $\rho(\mathfrak{t})$ are distinct.

(ii) ρ is said to be **admissible** if there exists modular category $\mathcal{C}$ over $\mathbb{C}$ of rank r such that ρ is a modular representation of $\mathcal{C}$ relative to certain ordering of $\Pi_{\mathcal{C}} = \{V_0, V_1, \dots, V_{r-1}\}$ with V_0 the unit object of $\mathcal{C}$. In this case, we say that ρ can be **realized** by the modular category $\mathcal{C}$.

(iii) $\overline{\mathrm{Rep}}(SL(2,\mathbb{Z}))$ denotes the set of all complex admissible $SL(2,\mathbb{Z})$-representation.

By [15], an admissible representation $\rho : SL(2,\mathbb{Z}) \to GL(r,\mathbb{C})$ must factor through $SL(2,\mathbb{Z}_n)$ where $n = \operatorname{ord}\rho(\mathfrak{t})$, and ρ is $\mathbb{Q}_n$-rational. It follows from [19, Lem. 1] that each non-degenerate admissible representation of $SL(2,\mathbb{Z})$ is absolutely irreducible. Moreover, by [50] any irreducible representation of $SL(2,\mathbb{Z})$ of dimension at most 5 must be non-degenerate.

Lemma 4.17. *Let ρ be a degree r non-degenerate admissible representation of $SL(2,\mathbb{Z})$ with $t = \rho(\mathfrak{t})$ and $s = \rho(\mathfrak{s})$. Suppose $\rho' \in \overline{\mathrm{Rep}}(SL(2,\mathbb{Z}))$ is equivalent to ρ with $t' = \rho'(\mathfrak{t})$ and $s' = \rho'(\mathfrak{s})$. Then $\rho'(\mathfrak{g}) = U^{-1}\rho(\mathfrak{g})U$ for a signed permutation matrix $U \in GL(r,\mathbb{C})$ of the permutation ς on $\{0,\dots,r-1\}$ defined by $t'_{\varsigma(i)} = t_i$.*

If, in addition, $t_0 = t'_0$, then ς defines an isomorphism of fusion rules associated to ρ and ρ'.

Proof. Since ρ and ρ' are equivalent, t and t' have the same eigenvalues. By the non-degeneracy of ρ, there exists a unique permutation ς on $\{0,\dots,r-1\}$ defined by $t'_{\varsigma(i)} = t_i$. Let $D_\varsigma = [\delta_{\varsigma(i)j}]_{i,j}$ be the permutation matrix of ς. Then $\rho'' = D_\varsigma \rho' D_\varsigma^{-1}$ is equivalent to ρ and $\rho''(\mathfrak{t}) = t$. There exists $Q \in GL(r,\mathbb{C})$ such that $Q\rho'' = \rho Q$. Since $Qt = tQ$ and t has distinct eigenvalues, Q is a diagonal matrix. Suppose $Q = [\delta_{ij}Q_i]_{i,j\in\Pi_{\mathcal{C}}}$. Then

$$s'_{\varsigma(i)\varsigma(j)} = \frac{Q_j}{Q_i} s_{ij}\,.$$

Both s and s' are symmetric, and so we have

$$\frac{Q_0}{Q_j} s_{0j} = \frac{Q_j}{Q_0} s_{j0} = \frac{Q_j}{Q_0} s_{0j}\,.$$

Since $s_{0j} \neq 0$, $\frac{Q_j}{Q_0} = \pm 1$. Let $Q' = \frac{1}{Q_0} Q$ and $U = Q' D_\varsigma$. Then $Q'^2 = I$, U is a signed permutation matrix of ς, and $s' = U^{-1} s U$. Since there are finitely many signed permutation matrices in $GL(r,\mathbb{C})$, the equivalence class of admissible representations of ρ is finite.

If, in addition, $t_0 = t'_0$, then $\varsigma(0) = 0$. Let $(s')^{-1} = [\overline{s}'_{i'j'}]_{i',j'\in\Pi_{\mathcal{C}'}}$ and $s^{-1} = [\overline{s}_{ij}]_{i,,j\in\Pi_{\mathcal{C}}}$. By the Verlinde formula,

$$N_{\varsigma(i)\varsigma(j)}^{\varsigma(k)} = \sum_{a=0}^{r-1} \frac{s'_{\varsigma(i)\varsigma(a)} s'_{\varsigma(j)\varsigma(a)} \overline{s}'_{\varsigma(k)\varsigma(a)}}{s'_{0\varsigma(a)}} = Q'_i Q'_j Q'_k \sum_{a=0}^{r-1} \frac{s_{ia} s_{ja} \overline{s}_{ka}}{s_{0a}} = Q'_i Q'_j Q'_k N_{ij}^k\,.$$

Thus, $Q'_i Q'_j Q'_k = 1$ whenever $N_{ij}^k \neq 0$. Moreover, ς defines an isomorphism between the fusion rules of $\mathcal{C}$ and $\mathcal{C}'$. $\square$

Let $\rho : SL(2,\mathbb{Z}) \to GL(n,\mathbb{C})$ a representation. The set of eigenvalues of $\rho(\mathfrak{t})$ is called the $\mathfrak{t}$-*spectrum* of ρ.

Lemma 4.18. *Let $\mathcal{C}$ be a modular category of rank r, and $\rho : SL(2,\mathbb{Z}) \to GL(r,\mathbb{C})$ a modular representation of $\mathcal{C}$. Then ρ cannot be isomorphic to a direct sum of two representations with disjoint $\mathfrak{t}$-spectra. In particular, if ρ is non-degenerate, then it is absolutely irreducible.*

Proof. Let $s = \rho(\mathfrak{s})$ and $t = \rho(\mathfrak{t})$. Then $\frac{s_{0j}}{s_{00}}$ is the quantum dimension of the simple object j. In particular, every entry of the first row of s is non-zero. Thus, for any permutation matrix Q, there exists a row of $Q^{-1}sQ$ which has no zero entry.

Suppose ρ is isomorphic a direct sum of two matrix representations ρ_1, ρ_2 of $SL(2,\mathbb{Z})$ with disjoint $\mathfrak{t}$-spectra. Since $\rho(\mathfrak{t})$ has finite order, and so are $\rho_i(\mathfrak{t})$, $i = 1, 2$. Without loss of generality, we can assume $\rho_1(\mathfrak{t})$ and $\rho_2(\mathfrak{t})$ are diagonal matrices. There exists a permutation matrix Q such that $Q^{-1}tQ = \left[\begin{array}{c|c} \rho_1(\mathfrak{t}) & 0 \\ \hline 0 & \rho_2(\mathfrak{t}) \end{array}\right]$. Since the representation $\rho^Q : SL(2,\mathbb{Z}) \to GL(k,\mathbb{C})$, $\mathfrak{s} \mapsto Q^{-1}sQ, \mathfrak{t} \mapsto Q^{-1}tQ$ is also equivalent to $\rho_1 \oplus \rho_2$, there exists $P \in GL(k,\mathbb{C})$ such that

$$P \left[\begin{array}{c|c} \rho_1(\mathfrak{t}) & 0 \\ \hline 0 & \rho_2(\mathfrak{t}) \end{array}\right] = \left[\begin{array}{c|c} \rho_1(\mathfrak{t}) & 0 \\ \hline 0 & \rho_2(\mathfrak{t}) \end{array}\right] P \quad \text{and} \quad Q^{-1}sQ = P \left[\begin{array}{c|c} \rho_1(\mathfrak{s}) & 0 \\ \hline 0 & \rho_2(\mathfrak{s}) \end{array}\right] P\,.$$

Since ρ_1 and ρ_2 have disjoint $\mathfrak{t}$-spectra, P must be of the block form $\left[\begin{array}{c|c} P_1 & 0 \\ \hline 0 & P_2 \end{array}\right]$. This implies every row of $Q^{-1}sQ$ has at least one zero entry, a contradiction. $\square$

Corollary 4.19. *Suppose $\mathcal{C}$ is a modular category of rank $r > 2$, and ρ is a modular representation of $\mathcal{C}$. Then:*

(i) *ρ cannot be a direct sum of 1-dimensional representations of $SL(2,\mathbb{Z})$.*

(ii) *If ρ_1 is a subrepresentation of degree $r-2$, then the $\mathfrak{t}$-spectrum of ρ_1 must contain a 120-th root of unity.*

Proof. The statement (i) was proved in [19] using a simpler version of Lemma 4.18.

Suppose ρ_1 is a degree $r-2$ subrepresentation of ρ such that $\omega^{120} \neq 1$ for all eigenvalues ω of $\rho_1(\mathfrak{t})$. Then there exists a 2-dimensional representation ρ_2 of $SL(2,\mathbb{Z})$ such that $\rho \cong \rho_1 \oplus \rho_2$.

If ρ_2 is a sum of 1-dimensional subrepresentations, then $\rho_2(\mathfrak{t})^{12} = \mathrm{id}$. If ρ_2 is irreducible, then $\rho_2 \cong \xi \otimes \phi$ for some linear character ϕ, and an irreducible representation ξ of prime power level. It follows from Table A1 of Eholzer's paper that $\rho_2(\mathfrak{t})^{120} = \mathrm{id}$. Thus, for both cases, ρ_1 and ρ_2 have disjoint $\mathfrak{t}$-spectra. However, this contradicts Lemma 4.18. $\square$

For any representation ρ of $SL(2,\mathbb{Z})$, we say that ρ is **even** (resp. **odd**) if $\rho(\mathfrak{s})^2 = \mathrm{id}$ (resp. $\rho(\mathfrak{s})^2 = -\mathrm{id}$). We denote the set of primitive q-th roots of unity by μ_q, the set of all q-th roots of unity by $\overline{\mu}_q$, and $\mu_{q*} = \bigcup\limits_{n\in\mathbb{N}} \mu_{qn}$.

Remark 4.20. If ρ is even, then the linear representation $\det\rho$ of $SL(2,\mathbb{Z})$ is also even, and so $\det\rho(\mathfrak{t}) \in \overline{\mu}_6$. In general, a representation of $SL(2,\mathbb{Z})$ may neither even nor odd. However, if $\mathcal{C}$ is a self-dual modular category, then $\mathcal{C}$ admits an *even* modular representation given by the normalized modular pair $(\frac{1}{D}S, \frac{1}{\zeta}T)$ for any 3-rd root ζ of $\frac{D}{p^-}$. Let ρ be a modular representation of $\mathcal{C}$. Then for any linear character χ of $SL(2,\mathbb{Z})$, there exists a modular representation $\rho' \cong \rho\otimes\chi$ as representations of $SL(2,\mathbb{Z})$. In addition, if ρ and χ are even, then so is ρ'.

Lemma 4.21. *Suppose $\mathcal{C}$ is a self-dual modular category of rank r, and ρ is an even modular representation of $\mathcal{C}$. If $\rho \cong \phi_1 \oplus (\phi_2 \otimes \xi)$ for some degree 1 representations ϕ_1, ϕ_2 and a degree $r-1$ non-degenerate irreducible representation ξ of $SL(2,\mathbb{Z})$ with odd level, then ϕ_1, ϕ_2 and ξ are all even.*

Proof. Let $\omega_1 = \phi_1(\mathfrak{t})$ and $\omega_2 = \phi_2(\mathfrak{t})$. Note that $\phi_i(\mathfrak{s}) = \omega_i^{-3}$ for all $i = 1, 2$, and $\omega_i^{12} = 1$. Since ρ is even, ϕ_1 and $\phi_2 \otimes \xi$ are even. In particular, $\omega_1^6 = 1$. Since ρ is reducible and ξ is non-degenerate, by Lemma 4.18, $\omega_1\omega_2^{-1}$ must be in the spectrum of $\xi(\mathfrak{t})$. Therefore, $\omega_1\omega_2^{-1}$ is of odd order, and hence $\omega_2^6 = 1$. Therefore, ϕ_2 is even. Since $\phi_2 \otimes \xi$ is even, ξ is also even. □

Remark 4.22. If ρ is a modular representation of a modular category $\mathcal{C}$, then the order of its T-matrix is equal to the *projective order* of $\rho(\mathfrak{t})$, i.e. the small positive integer N such that $\rho(\mathfrak{t})^N$ is a scalar multiple of the identity.

Lemma 4.23. *Let $\mathcal{C}$ be a fusion category such that $G(\mathcal{C})$ is trivial and $\mathcal{K}_0(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Z}_N$ is isomorphic to $\mathcal{K}_0(SU(N)_k)$ for some integer k relatively prime to N. Then $\mathcal{C}$ is monoidally equivalent to a Galois conjugate of $SU(N)_k/\mathbb{Z}_N$.*[4]

Proof. Let $\mathcal{S}$ be a rank N fusion category with fusion rules $\mathbb{Z}_N$ (or $\mathrm{Vec}(\mathbb{Z}_N)$). Now, we have

$$\mathcal{K}_0(\mathcal{C} \boxtimes \mathcal{S}) \cong \mathcal{K}_0(\mathcal{C}) \otimes \mathcal{K}_0(\mathcal{S}) \cong \mathcal{K}_0(SU(N)_k)$$

as based rings. By the classification in [34], $\mathcal{C} \boxtimes \mathcal{S}$ is monoidally equivalent to $\mathcal{D} \boxtimes \mathrm{Vec}(\mathbb{Z}_N, \omega)$ for some 3-cocycle ω of $\mathbb{Z}_N$ and Galois conjugate $\mathcal{D}$ of $SU(N)_k/\mathbb{Z}_N$ (*i.e.* a choice of a root of unity). As these categories are $\mathbb{Z}_N$-graded and the adjoint subcategories ($\mathcal{C}$ and $\mathcal{D}$ respectively) are the 0-graded components we have that $\mathcal{C}$ is monoidally equivalent to $\mathcal{D}$. □

Theorem 4.24. *Let $\mathcal{C}$ be a modular category such that $|\Pi_{\mathcal{C}}| = [\mathbb{K}_0 : \mathbb{Q}] = p$ is a prime. Then :*

(i) *Every modular representation of $\mathcal{C}$ is non-degenerate and hence absolutely irreducible.*

(ii) *$q = 2p + 1$ is a prime.*

(iii) $\mathrm{FSexp}(\mathcal{C}) = q$.

(iv) *The underlying fusion category of $\mathcal{C}$ is monoidally equivalent to a Galois conjugate of $SU(2)_{2p-1}/\mathbb{Z}_2$.*

Proof. The cases $p = 2, 3$ follow from the classification in [47, pp. 375–377]. We may assume $p > 3$.

Let ρ be a modular representation of $\mathcal{C}$, and set $s = \rho(\mathfrak{s})$, $t = \rho(\mathfrak{t})$ and $n = \mathrm{ord}(t)$. By Lemma 4.2, $|\langle 0 \rangle| = [\mathbb{K}_0 : \mathbb{Q}] = |\Pi_{\mathcal{C}}|$. Thus, $\mathbb{K}_{\mathcal{C}} = \mathbb{K}_0$ and so $|\mathrm{Gal}(\mathcal{C})| = p$. Thus, $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}_p$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ such that $\sigma|_{\mathbb{K}_{\mathcal{C}}}$ is a generator of $\mathrm{Gal}(\mathcal{C})$, and hence $\hat{\sigma} = (0, \hat{\sigma}(0), \hat{\sigma}^2(0), \ldots, \hat{\sigma}^{p-1}(0))$. By Theorem 2.9, $t_{\hat{\sigma}^i(0)} = \sigma^{2i}(t_0)$. Thus, $\mathbb{Q}_n = \mathbb{Q}(t_0)$. Suppose $t_{\hat{\sigma}^i(0)} = t_{\hat{\sigma}^j(0)}$ for some non-negative integers $i < j \le p-1$. This is not possible for $p = 2$ for otherwise $t = t_0 I$ and so $s = t_0^{-3} I$; ρ is then a direct sum of two isomorphic representation of $SL(2,\mathbb{Z})$ which contradicts Lemma 4.18. We can assume $p > 2$. Then $\sigma^{2(j-i)}(t_0) = t_0$ and so $\sigma^{2(j-i)} = \mathrm{id}$. This implies $\hat{\sigma}^{2l} = \mathrm{id}$ for some positive integer $l \le p-1$, and hence $p \mid 2l$, a contradiction. Therefore, $t_{\hat{\sigma}^i(0)} \ne t_{\hat{\sigma}^j(0)}$ for all non-negative integers $i < j \le p-1$, and hence ρ is non-degenerate. By Lemma 4.18, ρ is absolutely irreducible.

[4] See Section 5 for notation.

Note that $(\mathbb{F}_S, \mathbb{F}_t)$ is a modularly admissible, and $\mathbb{F}_S = \mathbb{K}_\mathcal{C}$ and $\mathbb{F}_t = \mathbb{Q}_n$. Since $[\mathbb{K}_0 : \mathbb{Q}] = |\langle 0\rangle| = |\Pi_\mathcal{C}|$, $\mathbb{K}_0 = \mathbb{K}_\mathcal{C}$. By Proposition 4.13 (since $p > 3$) we have $q = 2p+1$ is a prime and $q \mid n \mid 24q$.

Since $(q, 24) = 1$, by the Chinese Remainder Theorem, $\rho \cong \chi \otimes R$ for some irreducible representations χ and R of levels n/q and q respectively. Since $q \mid n$ and $12 \nmid q$, R is not linear. Thus, the prime degree p of ρ implies that $\deg R = p$ and $\deg \chi = 1$. Since $\rho(\mathfrak{t})^q = \chi(\mathfrak{t})^q \otimes \mathrm{id}$, $\mathrm{FSexp}(\mathcal{C}) \mid q$ by Remark 4.22, and hence $\mathrm{FSexp}(\mathcal{C}) = q$.

Since $\mathrm{FSexp}(\mathcal{C}) = q$ is odd, there exists a modular representation ρ of $\mathcal{C}$ with level q by [15, Lem. 2.2]. There is a dual pair of such irreducible representations of $SL(2, \mathbb{Z}_q)$. Realizations can be obtained from the modular data for $\mathcal{D} = SU(2)_{2p-1}/\mathbb{Z}_2$ (see e.g. [6]):

$$S_{i,j} = \frac{\sin\left(\frac{(2i+1)(2j+1)\pi}{q}\right)}{\sin\left(\frac{\pi}{q}\right)}, \quad \theta_j = e^{\frac{2\pi i(j^2+j)}{q}} \tag{4.5}$$

where $0 \le j \le (p-1) = \frac{q-3}{2}$. Since the θ_j are distinct and the T-matrix has order q, we can normalize $(S_\mathcal{D}, T_\mathcal{D})$ to a pseudo-unitary modular pair $(\tilde{s}, \tilde{t})$ corresponding to a degree p and level q irreducible representation of $SL(2, \mathbb{Z})$. Complex conjugation gives the other inequivalent such representation, and both have the first column a multiple of the Frobenius-Perron dimension.

By Lemma 4.3(iii) we may replace the modular data $(S_\mathcal{C}, T_\mathcal{C})$ by an admissible pseudo-unitary modular data (S', T'). After normalizing and taking the complex conjugates (if necessary) we can assume that the resulting pair (s', t') is conjugated to $(\tilde{s}, \tilde{t})$ by a signed permutation ς, by Lemma 4.17. The first row/column of both s' and $\tilde{s}$ are projectively positive. The first column of s' is mapped to the first column of $\tilde{s}$ under ς. In particular ς fixes the label 0 (as the Frobenius-Perron dimension is the unique projectively positive column of any S-matrix) so the last part of Lemma 4.17 implies that the fusion rules coincide. Now, statement (iv) follows from Lemma 4.23 as there are exactly N invertible objects in $SU(N)_k$, labeled by weights at the corners of the Weyl alcove. □

Lemma 4.25. *Let $p > 3$ be a prime. Then the unique degree p irreducible representation ψ of $SL(2, \mathbb{Z}_p)$ is not admissible.*

Proof. The result was established in [20] by using the integrality of fusion rules and Verlinde formula. Here we provide another proof by using the rationality of modular representations of any modular category. Suppose there exists a modular category $\mathcal{C}$ of rank p which admits a modular representation ρ equivalent to ψ as representations of $SL(2, \mathbb{Z})$. The representation ψ is given by

$$\begin{aligned}
\psi(\mathfrak{t})_{jk} &= \delta_{jk} e^{\frac{2\pi i k}{p}} \\
\psi(\mathfrak{s})_{00} &= \frac{-1}{p} \\
\psi(\mathfrak{s})_{0k} = \psi(\mathfrak{s})_{k0} &= \frac{\sqrt{p+1}}{p} \quad \text{for } 0 < k < p, \\
\psi(\mathfrak{s})_{jk} &= \frac{1}{p}\sum_{a=1}^{p-1} e^{\frac{2\pi i}{p}(aj + a^{-1}k)} \quad \text{for } 0 < j, k < p\,.
\end{aligned}$$

In particular, ρ is non-degenerate and $\psi(\mathfrak{s}) \notin GL(p, \mathbb{Q}_p)$ since $\sqrt{p+1} \notin \mathbb{Q}_p$ for $p > 3$. By Lemma 4.17, there exists a signed permutation matrix U such that $U\rho(\mathfrak{s})U^{-1} = \psi(\mathfrak{s})$. By Theorem 2.9, $\rho(\mathfrak{s}) \in GL(p, \mathbb{Q}_p)$, and so is $\psi(\mathfrak{s})$, a contradiction. □

5 Applications to Classification

5.1 Rank 5 Modular Categories

In this section we will classify modular categories of rank 5 as fusion subcategories of twisted versions of familiar categories associated to quantum groups of type A.

Fix two integers $N \geq 2$ and $\ell > N$. For any q such that q^2 is a primitive ℓth root of unity we obtain a modular category $\mathcal{C}(\mathfrak{sl}_N, q, \ell)$ as a subquotient of the category of representations of $U_q\mathfrak{sl}_N$. See [46] for a survey on the construction of such categories, which were first constructed as braided fusion categories by Anderson and collaborators and as modular categories by Turaev and Wenzl (see the references of [46]). The fusion rules of $\mathcal{C}(\mathfrak{sl}_N, q, \ell)$ do not depend on the choice of q, *i.e.* for fixed N and ℓ the categories $\mathcal{C}(\mathfrak{sl}_N, q, \ell)$ are all Grothendieck equivalent. We will denote by $SU(N)_k$ the modular category obtained from the choice $q = e^{\pi i/(N+k)}$, i.e. $SU(N)_k = \mathcal{C}(\mathfrak{sl}_N, e^{\pi i/(N+k)}, N+k)$ where $k \geq 1$. When ℓ and N are relatively prime the category $\mathcal{C}(\mathfrak{sl}_N, q, \ell)$ factors as a (Deligne) product of two modular categories, one of which is (the maximal pointed modular subcategory) of rank N with fusion rules like the group $\mathbb{Z}_N$. For $SU(N)_k$ we will denote the corresponding quotient (modular) category by $SU(N)_k/\mathbb{Z}_N$.[5]

We will prove:

Theorem 5.1. *Suppose $\mathcal{C}$ is a modular category of rank 5. Then $\mathcal{C}$ is Grothendieck equivalent to one of the following:*

(i) $SU(2)_4$,

(ii) $SU(2)_9/\mathbb{Z}_2$,

(iii) $SU(5)_1$, *or*

(iv) $SU(3)_4/\mathbb{Z}_3$.

Proof. This follows from Lemma 5.4 and Propositions 5.5, 5.7, 5.9, 5.10, 5.11, 5.12. □

Remark 5.2. Although this result only classifies rank 5 modular categories up to fusion rules, a classification up to equivalence of monoidal categories can be obtained using [34]. Indeed, by *loc. cit.* Theorem A_ℓ modular categories with fusion rules as in (i) resp. (iii) are monoidally equivalent to a Galois conjugate of $SU(2)_4$ followed by a twist of the associativities, resp. a Galois conjugate of $SU(5)_1$ (the non-trivial twists of $SU(5)_1$ have no modular structure). Modular categories Grothendieck equivalent to $SU(2)_9/\mathbb{Z}_2$ (resp. $SU(3)_4/\mathbb{Z}_3$) are monoidally equivalent to a Galois conjugate of $SU(2)_9/\mathbb{Z}_2$ (resp. $SU(3)_4/\mathbb{Z}_3$) by Lemma 4.23.

By [34, Thm. A_ℓ] there are *at most* $N\varphi(2(k+N))$ (Euler-φ) inequivalent fusion categories that are Grothendieck equivalent to $SU(N)_k$ and *at most* $\varphi(2(k+N))$ for $SU(N)_k/\mathbb{Z}_N$. The factor of N comes from twisting the associativities that is trivial on the quotient $SU(N)_k/\mathbb{Z}_N$ and the $\varphi(2(k+N))$ factor corresponds to a choice of a primitive $2(k+N)$th root of unity. We do not know how many distinct modular categories with these underlying fusion categories there are.

[5] This notation is conventional in conformal field theory where the term *orbifold* is used.

We first reduce to the case where $\mathcal{C}$ is non-integral and self-dual by the following:

Proposition 5.3. [30, Thms. 3.1 and 3.7] Suppose $\mathcal{C}$ is a rank 5 modular category. Then

(a) if $\mathcal{C}$ is integral then $\mathcal{C}$ is Grothendieck equivalent to $SU(5)_1$;

(b) if $\mathcal{C}$ is non-integral and not self-dual then $\mathcal{C}$ is Grothendieck equivalent to $SU(3)_4/\mathbb{Z}_3$.

We therefore assume $\mathcal{C}$ is a non-integral, self-dual modular category of rank 5 with Frobenius-Schur exponent N, and ρ is an *even* modular representation of level n. In particular the S-matrix has real entries and is projectively in $SO(5)$. Next we enumerate the possible Galois groups $\mathrm{Gal}(\mathcal{C})$ for rank 5 modular categories $\mathcal{C}$.

Lemma 5.4. *Suppose $\mathcal{C}$ is a self-dual non-integral modular category of rank 5. Then up to reordering the isomorphism classes of simple objects we have $\mathrm{Gal}(\mathcal{C})$ is cyclic and generated by one of the following:* $(0\ 1)$, $(0\ 1\ 2)$, $(0\ 1\ 2\ 3)$, $(0\ 1\ 2\ 3\ 4\ 5)$, $(0\ 1)\,(2\ 3)$*; or it is a Klein 4 group given by either* $\langle (0\ 1)\,, (2\ 3)\rangle$, *or* $\langle (0\ 1)(2\ 3), (0\ 2)(1\ 3)\rangle$

Proof. Since we have assumed $\mathcal{C}$ is not integral, Lemma 4.3 implies 0 is not fixed by $\mathrm{Gal}(\mathcal{C})$. Relabeling the simple objects if necessary we arrive at a list of possible groups. The groups $\langle (0\ 1\ 2)\,(3\ 4)\rangle$ and $\langle (0\ 1)\,(2\ 3\ 4)\rangle$ can be excluded by Lemmas 4.7 and 4.8. □

First observe that the case $\mathrm{Gal}\,(\mathcal{C}) \cong \mathbb{Z}_5 \cong \langle (0\ 1\ 2\ 3\ 4)\rangle$ has been considered in Theorem 4.24.

Proposition 5.5. *If $\mathcal{C}$ is a rank 5 modular category with $(0\ 1\ 2\ 3\ 4) \in \mathrm{Gal}(\mathcal{C})$ then $\mathcal{C}$ is equivalent to $SU(2)_9/\mathbb{Z}_2$ as fusion categories.*

Next we will consider the case that $\mathrm{Gal}(\mathcal{C}) = \langle (0\ 1)\rangle$. The following lemma will be useful.

Lemma 5.6. *Let a, b be non-zero rational integers. Suppose*

$$0 = a + bi + c_\alpha \alpha + c_\beta \beta \tag{5.1}$$

for some non-zero rational integers c_α, c_β and roots of unity α, β with $\mathrm{ord}(\alpha) \le \mathrm{ord}(\beta)$. Then $\alpha = \pm 1$, $\beta = \pm i$ and

$$a + \alpha c_\alpha = 0\,, \quad b - i\beta_2 c_\beta = 0$$

Proof. If $\alpha, \beta \in \mathbb{Q}(i)$, then α, β are fourth roots unity. The $\mathbb{Q}$-linear independence of $\{1, i\}$ implies that $\alpha = \pm 1$ and $\beta = \pm i$. Thus, the remainder equalities follow immediately. Therefore, it suffices to show that $\alpha, \beta \in \mathbb{Q}(i)$.

Suppose that α or β is not in $\mathbb{Q}(i)$. Then (5.1) implies that $[\mathbb{Q}(i,\alpha) : \mathbb{Q}(i)] = [\mathbb{Q}(i,\beta) : \mathbb{Q}(i)]$. Hence, both α, β are not in $\mathbb{Q}(i)$. Note that α, β are $\mathbb{Q}(i)$-linearly independent otherwise $\alpha, \beta \in \mathbb{Q}(i)$. By [12, Thm. 1], there exist $x, y \in \{\alpha, \beta\}$ such that $x, y/i$ have squarefree orders, and

$$a + c_x x = 0, \quad ib + c_y y = 0\,.$$

These equations force $\alpha = x = \pm 1$ and $\beta = y = \pm i$, and hence $\alpha, \beta \in \mathbb{Q}(i)$, a contradiction. □

We have:

Proposition 5.7. *If $\mathrm{Gal}(\mathcal{C}) = \langle (0\ 1)\rangle$ then $\mathcal{C}$ is Grothendieck equivalent to $SU(2)_4$.*

Proof. Suppose $\mathcal{C}$ is a rank 5 modular category with $\mathrm{Gal}(\mathcal{C}) = \langle(0\ 1)\rangle$. By (4.1) and Lemma 4.6, the S-matrix is of the form

$$S = \begin{bmatrix} 1 & d_1 & d_2 & d_3 & d_4 \\ d_1 & 1 & \epsilon_2 d_2 & \epsilon_3 d_3 & \epsilon_4 d_4 \\ d_2 & \epsilon_2 d_2 & S_{22} & S_{23} & S_{24} \\ d_3 & \epsilon_3 d_3 & S_{32} & S_{33} & S_{34} \\ d_4 & \epsilon_4 d_4 & S_{42} & S_{43} & S_{44} \end{bmatrix}$$

where $\epsilon_i = \pm 1$ and $(\epsilon_2, \epsilon_3, \epsilon_4) \neq (-1,-1,-1)$ or $(1,1,1)$. After renumbering, we may therefore assume that $(\epsilon_2, \epsilon_3, \epsilon_4) \in \{(1,1,-1),(1,-1,-1)\}$.

Suppose that $(\epsilon_2, \epsilon_3, \epsilon_4) = (1,1,-1)$. We first use Lemma 4.6 to conclude that $S_{24} = S_{34} = 0$ and orthogonality of the first and last columns of S to obtain $S_{44} = d_1 - 1$. Then we use the twist equation (2.6) for $(j,k) = (2,4)$, $(0,4)$ and $(4,4)$ to obtain

$$\begin{aligned} 0 = p^+ S_{24} &= \theta_2\theta_4(d_2d_4 - \theta_1 d_2 d_4), && (5.2)\\ p^+ d_4 &= \theta_4(d_4 - \theta_1 d_1 d_4 + \theta_4 d_4(d_1 - 1)), && (5.3)\\ p^+(d_1 - 1) &= \theta_4^2(d_4^2 + \theta_1 d_4^2 + \theta_4(d_1-1)^2)\,. && (5.4)\end{aligned}$$

It follows immediately from (5.2) that $\theta_1 = 1$ and hence, by (5.3),

$$p^+ = (d_1 - 1)\theta_4(\theta_4 - 1)\,.$$

Therefore,

$$D^2 = 2(d_1-1)^2(1 - Re(\theta_4)) \text{ and } d_1 \notin \mathbb{Q}\,.$$

Since $\frac{S_{i4}}{d_4}$ is an algebraic integer fixed by $\mathrm{Gal}(\mathcal{C})$, $\frac{S_{i4}}{d_4} \in \mathbb{Z}$ for all i. In particular,

$$n_{44} = \frac{d_1 - 1}{d_4} \in \mathbb{Z}.$$

and

$$D^2 = (2 + n_{44}^2)d_4^2\,.$$

It follows from (5.4) that

$$p^+ = (d_1 - 1)(\frac{2}{n_{44}^2}\theta_4^2 + \theta_4^3)$$

and this implies $\frac{2}{n_{44}^2}\theta_4^2 + \theta_4^3 = \theta_4(\theta_4 - 1)$ or

$$\theta_4^2 + (\frac{2}{n_{44}^2} - 1)\theta_4 + 1 = 0\,.$$

Thus, $[\mathbb{Q}(\theta_4) : \mathbb{Q}] \leq 2$ and so $\theta_4 \in \overline{\mu}_4 \cup \overline{\mu}_6$. Note that $\frac{2}{n_{44}^2} - 1 \notin \{0,-1,\pm 2\}$. Therefore, $\theta_4 \notin \overline{\mu}_4 \cup \mu_6$. Thus, $\theta_4 \in \mu_3$ and $n_{44} = \pm 1$. Now, we find $D = \sqrt{3}|d_1 - 1|$, $p^+ = -2iIm(\theta_4)(d_1 - 1) = \pm i\sqrt{3}(d_1 - 1)$. By [47, Thm. 2.7(5)], $D \in \mathbb{K}_{\mathcal{C}}$ and so $\sqrt{3} \in \mathbb{K}_{\mathcal{C}}$. Since $[\mathbb{K}_{\mathcal{C}} : \mathbb{Q}] = 2$, $\mathbb{K}_{\mathcal{C}} = \mathbb{Q}(\sqrt{3})$.

We now return to the equation

$$p^+ = 1 + d_1^2 + (d_1 - 1)^2\theta_4 + \theta_2 d_2^2 + \theta_3 d_3^2 \qquad (5.5)$$

which can be rewritten as

$$0 = 2 + \mathrm{Tr}(d_1) + 2iIm(\theta_4)(d_1 - 1/d_1) + 2\theta_2 N(d_2) + 2\theta_3 N(d_3)\,. \tag{5.6}$$

Note that $2+\mathrm{Tr}(d_1)$, $N(d_2)$ and $N(d_3)$ are non-zero integers. Since $\mathbb{Z}[\sqrt{3}]$ is the ring of algebraic integers in $\mathbb{Q}(\sqrt{3})$, $2Im(\theta_4)(d_1 - 1/d_1)$ is also a non-zero integer. We may simply assume $\mathrm{ord}(\theta_2) \le \mathrm{ord}(\theta_3)$. By Lemma 5.6, $\theta_2 = \pm 1$ and

$$2 + \mathrm{Tr}(d_1) + 2\theta_2 N(d_2) = 0\,.$$

Since $2 + \mathrm{Tr}(d_1)$ and $2N(d_2)$ are positive, $\theta_2 = -1$ and $2d_2^2 = (d_1+1)^2$. Thus, $\sqrt{2} = \pm\frac{d_1+1}{d_2} \in \mathbb{Q}(\sqrt{3})$, a contradiction.

Therefore we must have $(\epsilon_2, \epsilon_3, \epsilon_4) = (1, -1, -1)$ and, by Lemma 4.6,

$$S = \begin{bmatrix} 1 & d_1 & d_2 & d_3 & d_4 \\ d_1 & 1 & d_2 & -d_3 & -d_4 \\ d_2 & d_2 & S_{22} & 0 & 0 \\ d_3 & -d_3 & 0 & S_{33} & S_{34} \\ d_4 & -d_4 & 0 & S_{34} & S_{44} \end{bmatrix}.$$

By the orthogonality of the columns of S, $S_{22} = -(d_1+1)$. Since $\frac{S_{22}}{d_2}$ is fixed by $\mathrm{Gal}(\mathcal{C})$,

$$n_{22} = \frac{S_{22}}{d_2} = \frac{-(d_1+1)}{d_2} \in \mathbb{Z}.$$

By Lemma 4.3 the vector of FP-dimensions is in one of the first two rows, so $d_1, d_2 > 0$ and $n_{22} < 0$. We now apply the twist equation (2.6) for $(j,k) = (2,0)$, $(2,2)$ and $(2,3)$ to obtain

$$\begin{aligned} p^+ d_2 &= \theta_2(d_2 + \theta_1 d_1 d_2 - \theta_2 d_2(d_1+1)), & (5.7)\\ -p^+(d_1+1) &= \theta_2^2(d_2^2 + \theta_1 d_2^2 + \theta_2(d_1+1)^2), & (5.8)\\ 0 = p^+ S_{23} &= \theta_2\theta_3(d_2 d_3 - \theta_1 d_2 d_3)\,. & (5.9) \end{aligned}$$

The equation (5.9) implies $\theta_1 = 1$, and so equations (5.7), (5.8) become

$$\begin{aligned} \frac{p^+}{d_1+1} &= \theta_2(1-\theta_2), & (5.10)\\ -\frac{p^+}{d_1+1} &= \theta_2^2(\frac{2}{n_{22}^2} + \theta_2). & (5.11) \end{aligned}$$

Thus, θ_2 satisfies the quadratic equation

$$\theta_2^2 + (\frac{2}{n_{22}^2} - 1)\theta_2 + 1 = 0\,.$$

Since n_{22} is a negative integer, $\frac{2}{n_{22}^2} - 1 \ne 0, -1, \pm 2$. Therefore, $\theta_2 \in \mu_3$, $n_{22} = -1$ and $d_2 = d_1 + 1$. Moreover,

$$p^+ = 2iIm(\theta_2)(d_1+1) = \pm i\sqrt{3}(d_1+1), \quad \text{and} \quad D^2 = 3(d_1+1)^2.$$

In particular, $D = \sqrt{3}(d_1+1)$. By [47, Thm. 2.7(5)], $\sqrt{3} \in \mathbb{K}_{\mathcal{C}}$ and hence $\mathbb{K}_{\mathcal{C}} = \mathbb{Q}(\sqrt{3})$.

We now return to the equation

$$p^+ = 1 + d_1^2 + (d_1+1)^2\theta_2 + \theta_3 d_3^2 + \theta_4 d_4^2 \tag{5.12}$$

which can be rewritten as

$$0 = -2 + \mathrm{Tr}(d_1) + 2iIm(\theta_2)(d_1 - 1/d_1) + 2\theta_3\frac{d_3^2}{d_1} + 2\theta_4\frac{d_4^2}{d_1}\,. \tag{5.13}$$

Without loss of generality, we may simply assume $\mathrm{ord}(\theta_3) \le \mathrm{ord}(\theta_4)$. We first prove that $d_1 \in \mathbb{Q}$. Suppose not. Since $-2+\mathrm{Tr}(d_1)$, $2iIm(\theta_2)(d_1-1/d_1)$, $\frac{d_3^2}{d_1}$ and $\frac{d_4^2}{d_1}$ are non-zero integers, by Lemma 5.6, we find $\theta_3 = \pm 1$ and

$$-2 + \mathrm{Tr}(d_1) + 2\theta_3\frac{d_3^2}{d_1} = 0\,.$$

Since $-2 + \mathrm{Tr}(d_1), \frac{d_3^2}{d_1} > 0$, $\theta_3 = -1$ and $2d_3^2 = (d_1 - 1)^2$. However, this implies $\sqrt{2} = \pm\frac{d_1-1}{d_3} \in \mathbb{Q}(\sqrt{3})$, a contradiction. Therefore $d_1 \in \mathbb{Q}$.

Since $1/d_1$ is a Galois conjugate of d_1, $d_1 = 1$. Now, (5.13) becomes $0 = \theta_3\frac{d_3^2}{d_1} + \theta_4\frac{d_4^2}{d_1}$ or

$$\theta_3/\theta_4 = -\frac{d_4^2/d_1}{d_3^2/d_1} \in \mathbb{Q}\,.$$

This forces $\theta_3 = -\theta_4$ and $d_4^2 = d_3^2$. Since

$$12 = D^2 = 1 + 1 + 2^2 + 2d_3^2,$$

we obtain $d_3 = \pm\sqrt{3}$.

Suppose $d_3 = \nu_1\sqrt{3}$ and $d_4 = \nu_1'\sqrt{3}$ for some signs ν_1, ν_1'. The fusion rule $N_{23}^4 = \nu_1\nu_1'$ implies $\nu_1 = \nu_1'$. It follows from the orthogonality of the S-matrix that

$$0 = S_{33} + S_{34} = S_{34} + S_{44} = 6 + (S_{33} + S_{44})S_{34}, \quad S_{33}^2 + S_{34}^2 = 6 = S_{34}^2 + S_{44}^2\,.$$

Therefore,

$$S_{33} = S_{44} = -\nu_2\sqrt{3}, \quad S_{34} = \nu_2\sqrt{3}$$

for any sign ν_2. We find

$$S = \begin{bmatrix} 1 & 1 & 2 & \nu_1\sqrt{3} & \nu_1\sqrt{3} \\ 1 & 1 & 2 & -\nu_1\sqrt{3} & -\nu_1\sqrt{3} \\ 2 & 2 & -2 & 0 & 0 \\ \nu_1\sqrt{3} & -\nu_1\sqrt{3} & 0 & -\nu_2\sqrt{3} & \nu_2\sqrt{3} \\ \nu_1\sqrt{3} & -\nu_1\sqrt{3} & 0 & \nu_2\sqrt{3} & -\nu_2\sqrt{3} \end{bmatrix}.$$

On can check directly the four possible S-matrices of $\mathcal{C}$ generate the same fusion rules using the Verlinde formula. These fusion rules coincide with those of $SU(2)_4$.

We return to the twist equation (2.6) with $(j, k) = (0, 3)$ to obtain

$$\theta_3^2 = -\nu_2 2i\,Im(\theta_2)/\sqrt{3} = -\nu_2\nu_3 i$$

where $\nu_3 = \pm 1$ is determined by $\theta_2 = e^{\nu_3 2\pi i/3}$. One can check directly that for any $\theta_2 \in \mu_3$ and $\theta_3 \in \mu_8$ satisfying the above equation, the twist equation will hold for $T = \mathrm{diag}(1, 1, \theta_2, \theta_3, -\theta_3)$. Thus, there are 16 possible pairs of S and T-matrices for $\mathcal{C}$. $\square$

Remark 5.8. Each of the 16 possible pairs of S and T matrices are realized. By applying a Galois automorphism we may assume $\nu_1 = 1$, that is, $d_i = \mathrm{FPdim}(V_i)$ for all i. Then the corresponding 8 pairs (S, T) appear in [29, Example 5D].

Next we show

Proposition 5.9. *If $\mathcal{C}$ is a self-dual modular category of rank* 5*, then* $\mathrm{Gal}(\mathcal{C}) \not\cong \mathbb{Z}_3$*.*

Proof. Suppose that $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}_3$ and ρ is an *even* level n modular representation of $\mathcal{C}$ (cf. Remark 4.20). Since $(\mathbb{K}_\mathcal{C}, \mathbb{Q}_n)$ is admissible, by Proposition 4.13 we have either $7 \mid n \mid 24 \cdot 7$ or $9 \mid n \mid 8 \cdot 9$. We will eliminate these two possibilities.

Suppose $7 \mid n \mid 24 \cdot 7$. Then ρ has an irreducible subrepresentation ρ_1 of level $7f$ where $(7, f) = 1$ and $7f \mid n$. Thus, $\rho_1 \cong \xi \otimes \phi$ for some irreducible representations ξ and ϕ of levels 7 and f respectively. By [19, Table 1], $\deg \xi = 3, 4$ and hence $\deg \phi = 1$.

If $\deg \xi = 3$, then, by Table A.1, its $\mathfrak{t}$-spectrum is a subset of μ_7. This is not possible by Corollary 4.19. If $\deg \xi = 4$, then by Table A.1 ξ is odd; this contradicts Lemma 4.21.

Now suppose $9 \mid n \mid 8 \cdot 9$. Then ρ has an irreducible subrepresentation ρ_1 of level $9f$ where $(3, f) = 1$ and $9f \mid n$. Thus, $\rho_1 \cong \xi \otimes \phi$ for some irreducible representations ξ and ϕ of levels 9 and f respectively. By [19, Table 2], $\deg \xi = 4$ and hence $\deg \phi = 1$. Thus, $\rho \cong \phi' \oplus (\phi \otimes \xi)$ for some degree 1 representation ϕ'.

By Lemma 4.21, ξ, ϕ', ϕ are all even. Therefore, $(\phi')^* \otimes \rho \cong \chi_0 \oplus ((\phi')^* \otimes \phi \otimes \xi)$ where χ_0 is the trivial representation of $SL(2, \mathbb{Z})$. Note that $(\phi')^* \otimes \rho$ is isomorphic to another even modular representation ρ' of $\mathcal{C}$.

Let $\rho_1 = ((\phi')^* \otimes \phi \otimes \xi)$. By Lemma 4.18, $\rho_1(\mathfrak{t})$ has an eigenvalue 1 and so $((\phi')^* \otimes \phi)^3 = \chi_0$. Therefore, ρ_1 is a level 9 irreducible representation of $SL(2, \mathbb{Z})$. By [19, Table A3], ρ_1 is isomorphic to R or R^* defined by

$$R(\mathfrak{s}) := \frac{2}{3}\begin{bmatrix} s_1 & s_5 & s_7 & s_6 \\ s_5 & -s_7 & -s_1 & s_6 \\ s_7 & -s_1 & s_5 & -s_6 \\ s_6 & s_6 & -s_6 & 0 \end{bmatrix}, \quad R(\mathfrak{t}) := \mathrm{diag}(\zeta, \zeta^7, \zeta^4, 1)$$

with $s_j = \sin(\pi j/18)$ and $\zeta = \exp(2\pi i/9)$. Note that $R(\mathfrak{s}) = R^*(\mathfrak{s})$.

Since $\rho' \cong \rho_1 \oplus \chi_0$, ρ is of level 9 and $\rho'(\mathfrak{s})$ is a matrix over $\mathbb{Q}_9$. Let $R' = R \oplus \chi_0$. Then, there exists a permutation matrix P and a unitary matrix U such that

$$P\rho'(\mathfrak{t})P^{-1} = R'(\mathfrak{t}) = \mathrm{diag}(\omega_1, \omega_2, \omega_3, 1, 1) = U^{-1}R'(\mathfrak{t})U,$$

where $\omega_1, \omega_2, \omega_3$ are distinct 9-th roots of unity. Moreover,

$$P\rho'(\mathfrak{t})P^{-1} = U^{-1}R'(\mathfrak{t})U, \quad P\rho'(\mathfrak{s})P^{-1} = U^{-1}R'(\mathfrak{s})U.$$

This implies that U is of the form

$$\begin{bmatrix} u_1 & 0 & 0 & 0 & 0 \\ 0 & u_2 & 0 & 0 & 0 \\ 0 & 0 & u_3 & 0 & 0 \\ 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & -\overline{b} & \overline{a} \end{bmatrix}$$

where $|u_1| = |u_2| = |u_3| = 1$ and $|a|^2 + |b|^2 = 1$. We can further assume that $u_1 = 1$. Since $P\rho'(\mathfrak{s})P^{-1}$ is symmetric, u_1, u_2 are ± 1 and a, b are real. Thus, the $(1, 4)$ and $(1, 5)$ entries of

$P\rho'(\mathfrak{s})P^{-1}$ are $\frac{a}{\sqrt{3}}$ and $\frac{b}{\sqrt{3}} \in \mathbb{Q}_9$. This implies $ab \in \mathbb{Q}_9$ and $\frac{1}{3} + \frac{2ab}{\sqrt{3}} = (\frac{a}{\sqrt{3}} + \frac{b}{\sqrt{3}})^2 \in \mathbb{Q}_9$. Hence, $\sqrt{3} \in \mathbb{Q}_9$ but this contradicts that the conductor of $\sqrt{3}$ is 12. □

Proposition 5.10. *If $\mathcal{C}$ is a self-dual non-integral modular category of rank 5 then* $\mathrm{Gal}(\mathcal{C}) \not\cong \mathbb{Z}_4$.

Proof. Assume to the contrary. Let ρ be a level n even modular representation of $\mathcal{C}$ (see Remark 4.20), and $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ be such that $\hat{\sigma} = (0\ 1\ 2\ 3) \in \mathfrak{S}_5$ is a generator of the image of $\mathrm{Gal}(\mathcal{C})$ in $\mathfrak{S}_5$. It follows from Proposition 4.13 that the level n of ρ satisfies one of the following cases:

(i) $5 \mid n \mid 24 \cdot 5$,

(ii) $16 \mid n \mid 3 \cdot 16$,

(iii) $32 \mid n \mid 3 \cdot 32$.

By [19, Table 7], the smallest irreducible representation of level 32 is 6-dimensional. Therefore, case (iii) is impossible.

In cases (i) and (ii) we find that $\mathbb{Z}_n^* = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ has exponent 4, so that $\sigma^4 = \mathrm{id}$. Applying Theorem 2.9(iii) we find that $\rho(\mathfrak{t}) = t = \mathrm{diag}(z, \sigma^2(z), z, \sigma^2(z), w)$ where $w \in \overline{\mu}_{24}$ and z is a root of unity such that $5 \mid \mathrm{ord}(z) \mid 24 \cdot 5$ or $16 \mid \mathrm{ord}(z) \mid 3 \cdot 16$. By [50] ρ cannot have an irreducible subrepresentation of dimension more than 3. Moreover, ρ cannot have 1-dimensional subrepresentations: z cannot be the image of $\mathfrak{t}$ in a 1-dimensional $SL(2,\mathbb{Z})$-representation as $z^{24} \neq 1$, and by Lemma 4.18 w cannot be the image of $\mathfrak{t}$ in a 1-dimensional representation either, since w is distinct from z and $\sigma^2(z)$.

We can therefore conclude that ρ is a direct sum of even irreducible representations ρ_2 and ρ_3 of degrees 2 and 3 respectively. The corresponding partition of the $\mathfrak{t}$-spectrum of ρ is $\{\{z, \sigma^2(z)\}, \{z, \sigma^2(z), w\}\}$. In particular, the levels of these representations are multiple of $\mathrm{ord}(z)$. If $16 \mid n \mid 48$, then $16 \mid \mathrm{ord}(z)$ and there must be an irreducible representation of level 16 and degree 2. By Table A.1, this is not possible and we conclude that $5 \mid n \mid 24 \cdot 5$.

The representation $\rho_3 \cong \psi \otimes \chi$ for some irreducible representations ψ of degree 3 and level 5, and χ of degree 1. By Table A.1, ψ is even, and so must be χ. Thus, the spectrum of $\rho_3(\mathfrak{t})$ is $\{w\zeta, w/\zeta, w\}$ for some $\zeta \in \mu_5$ and $w \in \overline{\mu}_6$. This forces the $\mathfrak{t}$-spectrum of ρ_2 to $\{w\zeta, w/\zeta\}$ and so $\rho_2 \cong \psi' \otimes \chi$ for some irreducible representations ψ' of degree 2 and level 5. By Table A.1, ψ' is odd, and so must be ρ_2. This contradicts that ρ is even. □

Proposition 5.11. *If $\mathcal{C}$ is a self-dual non-integral modular category of rank 5 then* $\mathrm{Gal}(\mathcal{C}) \not\cong \langle (0\ 1), (2\ 3) \rangle$

Proof. Suppose $\mathrm{Gal}(\mathcal{C}) = \langle \sigma, \tau \rangle$ such that $\hat{\sigma} = (0\ 1)$ and $\hat{\tau} = (2\ 3)$. For notational convenience we set $\delta_i = \epsilon_\tau(i)$ and $\epsilon_i = \epsilon_\sigma(i)$. Galois symmetry (with respect to σ) applied to $S_{i,(i+1)}$ gives us the following condition for each $i \geq 2$: *either* $S_{i,(i+1)} = 0$ *or* $\epsilon_i = \epsilon_{i+1}$. Similarly, Galois symmetry with respect to τ applied to $S_{0i} = d_i$ gives us: $\delta_0 = \delta_1 = d_4$ and $\delta_2 = \delta_3$. With this in mind we set $e_1 = \epsilon_0\epsilon_2$, $e_2 = \epsilon_0\epsilon_3$, $e_3 = \epsilon_0\epsilon_4$ and $a = \delta_0\delta_2$. Applying σ and τ we obtain:

$$S = \begin{bmatrix} 1 & d_1 & d_2 & ad_2 & d_4 \\ d_1 & 1 & e_1 d_2 & e_2 a d_2 & e_3 d_4 \\ d_2 & e_1 d_2 & S_{22} & S_{23} & S_{24} \\ ad_2 & e_2 a d_2 & S_{23} & S_{22} & aS_{24} \\ d_4 & e_3 d_4 & S_{24} & aS_{24} & S_{44} \end{bmatrix}.$$

Since $\sigma(d_2) = e_1 d_2/d_1 = e_2 d_2/d_1$ we immediately see that $e_2 = e_1$. Orthogonality then implies that either $S_{24} = 0$ or $e_1 = e_3$, and

$$\{d_1 + 1/d_1, d_2^2/d_1, d_4^2/d_1, (S_{22} + aS_{23})/d_2, S_{22}S_{23}/d_2^2\} \subset \mathbb{Z}.$$

We claim that $S_{24} = 0$. If $e_i = 1$ for all i then orthogonality of the first two rows gives: $2 = -2d_2^2/d_1 - d_4^2/d_1$ with d_1 negative. If $e_i = -1$ for each i then orthogonality of the first two rows gives us: $2 = 2d_2^2/d_1 + d_4^2/d_1$. In either case, we have: $2 = 2x + y$ for some $x, y \geq 1$, which is absurd.

So we may assume that $S_{24} = 0$ and $-e_3 = e_1 = e_2$. In particular, the FP-dimension must be one of the first two rows. Therefore, $a = 1$ and $d_1 > 0$. Orthogonality now implies:

$$1 + e_3 = 0, \tag{5.14}$$
$$1 + e_1 d_1 + S_{22} + S_{23} = 0, \tag{5.15}$$
$$1 + e_3 d_1 + S_{44} = 0\,. \tag{5.16}$$

Thus $e_2 = e_1 = 1 = -e_3$, $S_{44} = d_1 - 1$ and $1 + d_1 + S_{22} + S_{23} = 0$. Note that this implies $M = (1 + d_1)/d_2 \in \mathbb{Z}$.

Using the twist equation (2.6) we proceed as in the proof of Proposition 5.7 to obtain: $d_4 = \pm(d_1 - 1)$, $p^+ = \pm i\sqrt{3}(d_1 - 1)$ and $p^+/p^- = -1$ and $\theta_4 \in \mu_3$. Thus, we have

$$p^+ + p^- = 2(1 + d_1^2) + 2d_2^2 Re(\theta_2 + \theta_3) - (d_1 - 1)^2 = 0$$

or $2Re(\theta_2 + \theta_3) = -M^2$. Setting $N = d_2^2/d_1$, we obtain the Diophantine equation $(M^2 - 2)N = 6$ from orthogonality of the first two rows (*i.e.* $d_1^2 - 4d_1 + 1 = 2d_2^2$). Since each of M and N are positive integers we obtain $(M, N) = (2, 3)$ as the only solution. Therefore, $Re(\theta_2 + \theta_3) = -2$. Hence $\theta_2 = \theta_3 = -1$, and $\mathbb{F}_T = \mathbb{Q}_3$. However, we also find $d_1 = 5 + 2\sqrt{6} \notin \mathbb{Q}_3$ which contradicts Theorem 2.7. □

Two cases remain: either $\mathrm{Gal}(\mathcal{C})$ is generated by $\hat{\sigma} = (0\ 1)\,(2\ 3)$, or contains $\hat{\sigma}$ and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ acting transitively on $\{0, 1, 2, 3\}$ fixing the label 4. In either case, $\exp(\mathrm{Gal}(\mathcal{C}))) = 2$ so $\mathbb{K}_{\mathcal{C}}$ is a multi-quadratic extension of $\mathbb{Q}$.

Proposition 5.12. *There is no self-dual non-integral modular category $\mathcal{C}$ of rank 5 such that every non-trivial element of* $\mathrm{Gal}(\mathcal{C})$ *is a product of two disjoint transpositions.*

Proof. In the following series of reductions, we will show that $\mathrm{FSExp}\,(\mathcal{C})$ can only be 2,3,4,6. In particular, $\mathcal{C}$ is integral by [7, Thm. 3.1], a contradiction.

Let ρ be an even modular representation of $\mathcal{C}$ of level n. Without loss of generality we may assume that $\hat{\sigma} = (0\ 1)(2\ 3) \in \mathrm{Gal}(\mathcal{C})$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. By Theorem 2.9 (Galois symmetry),

$$\rho(\mathfrak{t}) = t = \mathrm{diag}(t_0, \sigma^2(t_0), t_2, \sigma^2(t_2), t_4)\,. \tag{5.17}$$

Moreover, $s = \rho(\mathfrak{s})$ is a real symmetric matrix in $GL(5, \mathbb{Q}_n)$ of order 2 . Since $\tau^2(t_4) = t_{\hat{\tau}(4)} = t_4$ and $\tau(s_{i4}/s_{04}) = s_{i\hat{\tau}(4)}/s_{0\hat{\tau}(4)} = s_{i4}/s_{04}$ for all $\tau \in \mathrm{Aut}(\mathbb{Q}_{\mathrm{ab}})$, $t_4 \in \overline{\mu}_{24}$ and $s_{i4}/s_{04} \in \mathbb{Z}$ for all $i = 0, \ldots, 4$.

By Corollary 4.14, $n \mid 240$. We first show that $n \mid 48$, *i.e.* $5 \nmid n$.

Suppose $5 \mid n$. Then $\rho \cong (\xi_5 \otimes \chi) \oplus \rho_1$ where ρ_1 is an even subrepresentation of ρ, ξ_5 and χ are irreducible representations of $SL(2, \mathbb{Z}_5)$ and $SL(2, \mathbb{Z}_{48})$ respectively, and ξ_5 is of level 5. Since $\deg \xi_5 \geq 2$, $\deg \xi \leq 2$. However, if $\deg \chi = 2$, then $\deg \xi_5 = 2$ and $\deg \rho_1 = 1$. By Table A.1, the $\mathfrak{t}$-spectrum of ξ_5 is $\{\zeta, \overline{\zeta}\}$ for some $\zeta_5 \in \mu_5$. Thus the orders of the eigenvalues of $\xi_5 \otimes \chi$ are multiple of 5, and so the $\mathfrak{t}$-spectra of $\xi_5 \otimes \chi$ and ρ_1 are disjoint; this contradicts Lemma 4.18. Therefore, χ is linear.

Now, we set ρ' be the modular representation of $\mathcal{C}$ equivalent to $\chi^{-1} \otimes \rho$ and $\rho'_1 = \chi^{-1} \otimes \rho_1$. Then $\rho' \cong \xi_5 \oplus \rho'_1$.

If $\deg \xi_5 = 5$, then $\xi_5 \cong \rho'$, but this contradicts Lemma 4.25. Therefore, $\deg \xi_5 < 5$.

If $\deg \xi_5 = 4$, then the $\mathfrak{t}$-spectrum of ξ_5 is equal to μ_5 but ρ'_1 is linear. Thus, ξ_5 and ρ'_1 have disjoint $\mathfrak{t}$-spectra. Therefore, $\deg \xi_5 = 4$ is not possible.

If $\deg \xi_5 = 2$, then ξ_5 is odd and the $\mathfrak{t}$-spectrum of ξ_5 is $\{\omega, \overline{\omega}\}$ for some $\omega \in \mu_5$. Thus, χ is odd and so are ρ' and ρ'_1. If ρ'_1 is reducible, then $\rho'_1 \cong \rho'_2 \oplus \rho'_3$ for some representations ρ'_2 and ρ'_3. We may assume $\deg \rho'_3 = 1$. By Lemma 4.18, the $\mathfrak{t}$-spectrum of ρ'_2 must contain ω or $\overline{\omega}$. Therefore, ρ' is also irreducible and has the same $\mathfrak{t}$-spectrum ξ_5. However, this means ρ'_3 and $\xi_5 \oplus \rho'_2$ have disjoint $\mathfrak{t}$-spectra. Therefore, ρ_1 must be irreducible and the $\mathfrak{t}$-spectra of ρ'_1 and ξ_5 are not disjoint. This implies ρ'_1 is of level 5, and it must be even, a contradiction. Therefore, $\deg \xi_5 \neq 2$.

If $\deg \xi_5 = 3$, then ξ_5 is even and so are χ and ρ'. We may assume $\rho \cong \xi_5 \oplus \rho_1$ by replacing ρ with ρ' if necessary. The $\mathfrak{t}$-spectrum of ξ_5 is $\{\omega, \overline{\omega}, 1\}$ for some $\omega \in \mu_5$.

If ρ_1 is reducible, then ρ_1 is a direct sum $\chi_1 \oplus \chi_2$ of linear characters. In view of Lemma 4.18, both of χ_1 and χ_2 are the trivial character and so ρ is of level 5. If ρ_1 is irreducible, then the $\mathfrak{t}$-spectrum of ρ_1 cannot contain ω or $\overline{\omega}$ for otherwise ρ_1 is the level 5 degree 2 irreducible representation which is odd. Thus, 1 is an eigenvalue of $\rho_1(\mathfrak{t})$ and so ρ_1 is the level 2 degree 2 irreducible representation with $\mathfrak{t}$-spectrum $\{1, -1\}$. In particular, ρ is of level 10. Hence, by (5.17), we find

$$\rho(\mathfrak{t}) = t = \operatorname{diag}(\omega, \overline{\omega}, 1, 1, \pm 1) \text{ or } \operatorname{diag}(1, 1, \omega, \overline{\omega}, \pm 1)$$

for both cases of ρ_1. Moreover, $\mathbb{F}_t = \mathbb{Q}_5$ and $\mathbb{F}_s$ is a real subfield of $\mathbb{F}_t$. Therefore, $\mathbb{F}_s = \mathbb{Q}(\sqrt{5})$. Since both generators of $\mathrm{Gal}(\mathbb{Q}_5/\mathbb{Q})$ have the same non-trivial restriction on $\mathbb{Q}(\sqrt{5})$, we can assume $\sigma : \omega \mapsto \omega^2$ and $\hat{\sigma} = (0\ 1)(2\ 3)$. By the twist equation (2.6), we find

$$s_{44} = s_{04}^2 t_0 + s_{14}^2 t_1 + s_{24}^2 t_2 + s_{34}^2 t_3 + s_{44}^2 t_4 \,. \tag{5.18}$$

Note that s_{i4}^2 is fixed by σ for all i, and $s_{24}^2 = s_{34}^2$, $s_{04}^2 = s_{14}^2$. By applying σ to (5.18),

$$\sigma(s_{44}) = \epsilon_\sigma(4) s_{4\hat{\sigma}(4)} = \epsilon_\sigma(4) s_{44} = s_{40}^2 t_0^2 + s_{14}^2 t_1^2 + s_{24}^2 t_2^2 + s_{34}^2 t_3^2 + s_{44}^2 t_4 \,. \tag{5.19}$$

These equations imply

$$(1 - \epsilon_\sigma(4)) s_{44} = s_{40}^2((t_0 + t_1) - (t_0^2 + t_1^2)) + s_{24}^2(t_2 + t_3 - (t_2^2 + t_3^2)) \,. \tag{5.20}$$

If $t = \operatorname{diag}(\omega, \overline{\omega}, 1, 1, \pm 1)$, then $(1 - \epsilon_\sigma(4)) s_{44} = s_{40}^2((\omega + \omega^4) - (\omega^2 + \omega^3))$. Since the right hand side of this equation is non-zero, $s_{44} \neq 0$ and $\epsilon_\sigma(4) = -1$. Thus, we obtain

$$\begin{aligned} 0 &= s_{40}^2(\omega + \omega^4 + \omega^2 + \omega^3) + 4 s_{24}^2 + 2 s_{44}^2 t_4 \\ &= -s_{40}^2 + 4 s_{24}^2 + 2 s_{44}^2 t_4 \end{aligned}$$

and hence

$$1 = 2\left(2\frac{s_{24}^2}{s_{04}^2} + \frac{s_{44}^2}{s_{04}^2} t_4\right) .$$

Since $s_{j4}/s_{04} \in \mathbb{Z}$ for all i, we find $2 \mid 1$, a contradiction. Therefore, $t = \mathrm{diag}(1,1,\omega,\overline{\omega},\pm 1)$ and the equation (5.20) becomes

$$(1-\epsilon_\sigma(4))s_{44} = s_{24}^2((\omega+\omega^4)-(\omega^2+\omega^3))\,.$$

If $s_{24} \neq 0$, then $s_{44} \neq 0$ and $\epsilon_\sigma(4) = -1$. By the same argument

$$\left(\frac{s_{24}}{s_{04}}\right)^2 = 4 + 2\left(\frac{s_{44}}{s_{04}}\right)^2 t_4\,.$$

The integral equation forces $t_4 = 1$ and so $s_{24}^2/2 = 2s_{04}^2 + s_{44}^2$. By the unitarity of s, we also have

$$1 = 2s_{24}^2 + 2s_{04}^2 + s_{44}^2 = \frac{5}{2}s_{24}^2.$$

This implies $s_{24} = \pm\sqrt{\frac{2}{5}} \in \mathbb{Q}(\sqrt{5})$ and hence $\sqrt{2} \in \mathbb{Q}(\sqrt{5})$, a contradiction. Therefore, $s_{24} = 0$ and hence $s_{34} = 0$. Now, the equation (5.18) becomes $s_{44} = 2s_{04}^2 + s_{44}^2 t_4$. In particular, the integer s_{44}/s_{04} is a root of $t_4X^2 - X + 2 = 0$. This forces $t_4 = -1$ and $s_{44}/s_{04} = 1$ or -2. By the unitarity of s again, $1 = 3s_{04}^2$ or $1 = 6s_{04}^2$. Both equations imply $\sqrt{3} \in \mathbb{Q}(\sqrt{5})$, a contradiction. Now, we can conclude that $5 \nmid n$, so that $n \mid 48$.

Next we show that $n \mid 24$, *i.e.* $16 \nmid n$.

Suppose to the contrary that $16 \mid n$. Then $\rho \cong (\xi_{16} \otimes \chi) \oplus \rho_1$ for some subrepresentation ρ_1 of ρ, an irreducible representations ξ_{16} of level 16, and an irreducible representation χ of $SL(2,\mathbb{Z}_3)$. Then $\deg \xi_{16} = 3$, and $\deg \chi = 1$ and hence they are both even. By tensoring with χ^{-1}, we may assume $\rho \cong \xi_{16} \oplus \rho_1$ for some even subrepresentation ρ_1 of ρ. The $\mathfrak{t}$-spectrum of ξ_{16} is $\{\omega, -\omega, \gamma\}$ for some $\omega \in \mu_{16}$ and $\gamma \in \mu_8$. Since $\deg \rho_1 = 2$, the level of ρ_1 cannot be 16 and so $\pm\omega$ are not in the $\mathfrak{t}$-spectrum of ρ_1. Therefore, γ must be an eigenvalue of $\rho_1(\mathfrak{t})$ and hence ρ_1 is an irreducible representation of level 8. Thus, the $\mathfrak{t}$-spectrum of ρ_1 is $\{\gamma, -\overline{\gamma}\}$ (cf. Table A.1). In particular, ρ is of level $n = 16$. In view of (5.17),

$$\rho(\mathfrak{t}) = t = \mathrm{diag}(\gamma,\gamma,\omega,-\omega,-\overline{\gamma}) \text{ or } \mathrm{diag}(\omega,-\omega,\gamma,\gamma,-\overline{\gamma}).$$

By the (2.6), we find

$$\begin{aligned} s_{44} &= \overline{\gamma}^2(s_{04}^2 t_0 + s_{14}^2 t_1 + s_{24}^2 t_2 + s_{34}^2 t_3 - s_{44}^2\overline{\gamma}) \\ &= s_{04}^2\overline{\gamma}^2(t_0+t_1) + s_{24}^2\overline{\gamma}^2(t_2+t_3) + s_{44}^2\gamma\,. \end{aligned}$$

If $t = \mathrm{diag}(\gamma,\gamma,\omega,-\omega,-\overline{\gamma})$, then $s_{44} = 2s_{04}^2\overline{\gamma} + s_{44}^2\gamma$. The imaginary parts of both sides of this equation imply $2s_{04}^2 = s_{44}^2$. Therefore, $\frac{s_{44}}{s_{04}} = \pm\sqrt{2}$ is not an integer, a contradiction.

If $t = \mathrm{diag}(\omega,-\omega,\gamma,\gamma,\gamma')$, then $s_{44} = 2s_{24}^2\overline{\gamma} + s_{44}^2\gamma$. If $s_{24} \neq 0$, then by the same argument as the preceding case we will arrive the conclusion that $s_{44}/s_{24} \notin \mathbb{Q}$. However, this is absurd as both $\frac{s_{44}}{s_{04}}$ and $\frac{s_{24}}{s_{04}}$ are integers. Therefore, $s_{24} = 0$ and hence $s_{34} = 0 = s_{44}$. Orthogonality of s and the action σ imply

$$s_{04} = \pm\frac{1}{\sqrt{2}}, \quad s_{14} = -\epsilon_\sigma(0)s_{04}, \quad s_{1j} = \epsilon_\sigma(0)s_{0j}$$

for $j = 0,\ldots,3$. In particular, $s_{12}^2 = s_{02}^2$. Consider the twist equation

$$s_{22} = \gamma^2(s_{20}^2\omega - s_{21}^2\omega + (s_{22}^2 + s_{23}^2)\gamma) = (s_{22}^2 + s_{23}^2)\gamma^3\,.$$

This implies $s_{22} = s_{23} = 0$ and hence $s_{33} = 0$. Consequently, the third and the fourth rows of s are multiples of $(1,\epsilon_\sigma(0),0,0,0)$. This contradicts that s is invertible.

Next we show that $n \mid 12$, *i.e.* $8 \nmid n$. In particular $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}_2$.

Since $n \mid 24$, $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ has exponent 2. Galois symmetry and (5.17) imply

$$t = \mathrm{diag}(t_0, t_0, t_2, t_2, t_4). \tag{5.21}$$

In particular, t has at most 3 distinct eigenvalues. By [50], every irreducible subrepresentation of ρ has degree ≤ 3. Thus, if $\xi \otimes \chi$ is isomorphic to an irreducible subrepresentation of ρ for some representations ξ, χ of $SL(2, \mathbb{Z})$, then ξ or χ must be linear.

Suppose that $8 \mid n$. Then $\rho \cong (\xi_8 \otimes \chi) \oplus \rho_1$ for some representations ξ_8, χ and ρ_1 of $SL(2, \mathbb{Z})$ such that ξ_8 is irreducible of level 8, χ is irreducible of level 1 or 3, and ρ_1 is even. Since $\deg \xi_8 \geq 2$, $\deg \chi = 1$. Therefore, χ is even, and so is ξ_8. By tensoring with χ^{-1}, we may assume $\rho \cong \xi_8 \oplus \rho_1$.

Suppose $\deg \xi_8 = 3$. Then the eigenvalues of $\xi_8(\mathfrak{t})$ are $\{\omega, -\omega, \gamma\}$ for some $\omega \in \mu_8$ and $\gamma \in \mu_4$ (cf. Table A.1). In view of (5.21), the $\mathfrak{t}$ spectrum of ρ_1 is $\{\omega, -\omega\}$. In particular, $\det \rho_1(\mathfrak{t}) = \pm i$ which contradicts that ρ_1 is even (cf. Remark 4.20). Therefore, $\deg \xi_8 = 2$, and the $\mathfrak{t}$-spectrum of ξ_8 is $\{\gamma, -\overline{\gamma}\}$ for some $\gamma \in \mu_8$. Since $\rho_1(\mathfrak{t})$ and ξ_8 must have a common eigenvalue, the level of ρ_1 is also a multiple of 8. By the preceding argument, $\rho_1 = \xi_8' \oplus \rho_2$ for some degree 2 irreducible representation of level 8, ξ_8', and a degree 1 even representation ρ_2. However, ρ_2 and $\xi_8 \oplus \xi_8'$ have disjoint $\mathfrak{t}$-spectra, a contradiction. Therefore, $n \mid 12$

Finally we will show that the Frobenius-Schur exponent N must be $2, 3, 4$ or 6. Since $N \mid n \mid 12$, it is enough to show $4 \nmid n$.

Suppose $4 \mid n$. We claim that ρ admits a subrepresentation isomorphic to $\xi_4 \otimes \chi$ for some irreducible representations ξ_4 of level 4 and degree > 1 and $\chi \in \mathrm{Rep}(SL(2, \mathbb{Z}_3))$. Assume the contrary. Since any linear subrepresentation of ρ can only have a level dividing 6, ρ admits an irreducible subrepresentation ρ' of degree > 1 and level a multiple of 4. Then $\rho' \cong \xi_4 \otimes \chi$ for some level 4 degree 1 representation ξ_4 and an irreducible representation $\chi \in \mathrm{Rep}(SL(2, \mathbb{Z}_3))$. Then χ must be odd since ξ_4 is odd. This forces χ to be of level 3 and degree 2. In particular, ρ' is of level 12 and the $\mathfrak{t}$-spectrum of ρ' is a subset of μ_{4*}. Now, $\rho \cong \rho' \oplus \rho_1$ for some even representation ρ_1 of degree 3. By Lemma 4.18, the level of ρ_1 is also a multiple of 4. Following the same reason, ρ_1 admits a degree 2 level 12 even irreducible subrepresentation ρ'' with its $\mathfrak{t}$- spectrum a subset of μ_{4*}. Now, $\rho \cong \rho' \oplus \rho'' \oplus \rho_2$ for some degree 1 even representation ρ_2. However, ρ_2 and $\rho' \oplus \rho''$ have disjoint $\mathfrak{t}$-spectra, a contradiction. This completes the proof. $\square$

A Irreducible Representations of Degree ≤ 4

The 12 degree one representations C_j of $SL(2,\mathbb{Z})$, $j=0,1,\ldots,11$ are defined by $C_j(\mathfrak{t})=e^{2\pi j i/12}$. Thus, C_j is even if, and only if, j is even which is equivalent to the fact that $\operatorname{ord}(C_j)\mid 6$. The $\mathfrak{t}$-spectra of irreducible representations of degree ≤ 4 and of level p^λ are illustrated in the following table.

Table A.1. $\mathfrak{t}$-spectra of level p^λ irreducible representations of degree ≤ 4

degree	parity	level	$\mathfrak{t}$-spectra
2	even	2	$\{1,-1\}$
	odd	3	$\{e^{2\pi ri/3}, e^{-2\pi(r+1)i/3}\}$, $r=0,1,2$
	odd	4	$\{i,-i\}$
	odd	5	$\{e^{2\pi i/5}, e^{-2\pi i/5}\}, \{e^{4\pi i/5}, e^{-4\pi i/5}\}$
	even	8	$\{e^{5\pi i/4}, e^{7\pi i/4}\}$, $\{e^{\pi i/4}, e^{3\pi i/4}\}$
	odd	8	$\{e^{3\pi i/4}, e^{5\pi i/4}\}, \{e^{7\pi i/4}, e^{\pi i/4}\}$
3	even	3	$\{e^{2\pi(r+1)i/3}, e^{2\pi(r+2)i/3}, e^{2\pi ri/3}\}$, $r=0,1,2$
	odd	4	$\{i,-1,1\}$, $\{-i,1,-1\}$
	even	4	$\{-1,-i,i\}$, $\{1,i,-i\}$
	even	5	$\{1,e^{2\pi ri/5}, e^{-2\pi ri/5}\}$, $r=1,2$
	even	7	$\{e^{4\pi i/7}, e^{2\pi i/7}, e^{8\pi i/7}\}$,
			$\{e^{-4\pi i/7}, e^{-2\pi i/7}, e^{-8\pi i/7}\}$
	odd	8	$\{-1,-e^{\pi i/4}, e^{\pi i/4}\}$, $\{1, e^{\pi i/4}, -e^{\pi i/4}\}$
			$\{-1,-e^{3\pi i/4}, e^{3\pi i/4}\}$, $\{1, e^{3\pi i/4}, -e^{3\pi i/4}\}$
	even	8	$\{-i,-e^{\pi 3i/4}, e^{\pi 3i/4}\}$, $\{i, e^{\pi 3i/4}, -e^{\pi 3i/4}\}$
			$\{i,-e^{\pi i/4}, e^{\pi i/4}\}$, $\{-i, e^{\pi i/4}, -e^{\pi i/4}\}$
	odd	16	$\{-e^{\pi i/4}, e^{\pi i/8}, -e^{\pi i/8}\}$, $\{e^{\pi i/4}, -e^{\pi i/8}, e^{\pi i/8}\}$
			$\{e^{\pi i/4}, e^{5\pi i/8}, -e^{5\pi i/8}\}$, $\{-e^{\pi i/4}, -e^{5\pi i/8}, e^{5\pi i/8}\}$
			$\{-e^{\pi 3i/4}, e^{3\pi i/8}, -e^{3\pi i/8}\}$, $\{e^{\pi 3i/4}, -e^{3\pi i/8}, e^{3\pi i/8}\}$
			$\{e^{3\pi i/4}, -e^{7\pi i/8}, e^{7\pi i/8}\}$, $\{-e^{3\pi i/4}, -e^{7\pi i/8}, e^{7\pi i/8}\}$
	even	16	$\{-e^{3\pi i/4}, e^{5\pi i/8}, -e^{\pi 5i/8}\}$, $\{e^{3\pi i/4}, -e^{5\pi i/8}, e^{\pi 5i/8}\}$
			$\{e^{3\pi i/4}, -e^{\pi i/8}, e^{\pi i/8}\}$, $\{-e^{3\pi i/4}, e^{\pi i/8}, -e^{\pi i/8}\}$
			$\{-e^{\pi i/4}, -e^{7\pi i/8}, e^{7\pi i/8}\}$, $\{e^{\pi i/4}, e^{7\pi i/8}, -e^{7\pi i/8}\}$
			$\{-e^{\pi i/4}, e^{3\pi i/8}, -e^{3\pi i/8}\}$, $\{e^{\pi i/4}, -e^{3\pi i/8}, e^{3\pi i/8}\}$
4	odd	5	$\{e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}\}$
	even	5	$\{e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}\}$
	odd	7	$\{1, e^{2\pi i/7}, e^{8\pi i/7}, e^{4\pi i/7}\}$
	odd	7	$\{1, e^{12\pi i/7}, e^{6\pi i/7}, e^{10\pi i/7}\}$
	odd	8	$\{e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}\}$
	even	8	$\{e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}\}$
	odd	9	$\{e^{2\pi i(\frac{1}{9}+\frac{r}{3})}, e^{2\pi i(\frac{4}{9}+\frac{r}{3})}, e^{2\pi i(\frac{7}{9}+\frac{r}{3})}, e^{2\pi i(\frac{1}{3}+\frac{r}{3})}\}$, $r=0,1,2$
			$\{e^{2\pi i(\frac{8}{9}+\frac{r}{3})}, e^{2\pi i(\frac{5}{9}+\frac{r}{3})}, e^{2\pi i(\frac{2}{9}+\frac{r}{3})}, e^{2\pi i(\frac{2}{3}+\frac{r}{3})}\}$, $r=0,1,2$
	even	9	$\{e^{2\pi i(\frac{1}{9}+\frac{r}{3})}, e^{2\pi i(\frac{4}{9}+\frac{r}{3})}, e^{2\pi i(\frac{7}{9}+\frac{r}{3})}, e^{2\pi i(\frac{1}{3}+\frac{r}{3})}\}$, $r=0,1,2$
			$\{e^{2\pi i(\frac{8}{9}+\frac{r}{3})}, e^{2\pi i(\frac{5}{9}+\frac{r}{3})}, e^{2\pi i(\frac{2}{9}+\frac{r}{3})}, e^{2\pi i(\frac{2}{3}+\frac{r}{3})}\}$, $r=0,1,2$

References

[1] P. Bantay, *The Frobenius-Schur indicator in conformal field theory*, Phys. Lett. B **394** (1997), no. 1-2, 87–88.

[2] P. Bantay, *The Kernel of the Modular Representation and the Galois Action in RCFT*, Comm. Math. Phys. **233** (2003), 423–438.

[3] F. J. Burnell, X. Chen, L. Fidowski, and A. Vishwanath, *Exactly Soluble Models of a 3D Symmetry Protected Topological Phase of Bosons with Surface Topological Order*, (2013). preprint: arXiv:1302.7072v1 [cond-mat.str-el].

[4] J. de Boer and J. Goeree, *Markov Traces and II_1 Factors in Conformal Field Theory*, Commun. Math. Phys. **139** (1991), 267–304.

[5] J. M. Burns and B. Goldsmith, *Maximal Order Abelian Subgroups of Symmetric Groups*, Bull. London Math. Soc. **21** (1980), 70–72.

[6] B. Bakalov and A. K. Jr., *Lectures on Tensor Categories and Modular Functors*, vol. 21, University Lecture Series, Amer. Math. Soc., 2001.

[7] P. Bruillard and E. Rowell, *Modular Categories, Integrality and Egyptian Fractions*, Proc. Amer. Math. Soc. **140** (2012), no. 4, 1141–1150.

[8] J. R. Britnell, *A formal identity involving commuting triples of permutations*, J. Combin. Theory Ser. A **120** (2013), no. 4, 941–943.

[9] S. Burciu and S. Natale, *Fusion rules of equivariantizations of fusion categories*, J. Math. Phys. (2013), no. 54, 013511.

[10] H. Cohen, *Advanced Topics in Computational Number Theory*, ed. by S. Axler, F. W. Gehring, and R. A. Ribet, Graduate Texts in Mathematics, no. 193, Springer, 2000.

[11] A. Coste and T. Gannon, *Remarks on Galois symmetry in rational conformal field theories*, Phys. Lett. B **323** (1994), no. 3-4, 316–321.

[12] J. H. Conway and A. J. Jones, *Trigonometric Diophantine equations (On vanishing sums of roots of unity)*, Acta Arith. **30** (1976), no. 3, 229–240.

[13] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, *On Braided Fusion Categories I*, Selecta Math. **16** (2010), no. 1, 1–119.

[14] O. Davidovich, T. Hagge, and Z. Wang, *On Arithmetic Modular Categories*, (2013). preprint: arXiv:1305.2229.

[15] C. Dong, X. Lin, and S.-H. Ng, *Congruence Property in Conformal Field Theory*, (2012). preprint: arXiv:1201.6644v4.

[16] P. Etingof, *Private Communication*, Feb. 2013.

[17] P. Etingof and S. Gelaki, *Some Properties of Finite-Dimensional Semisimple Hopf Algebras*, Math. Res. Lett. **5** (1998), no. 1–2, 191–197.

[18] P. Etingof, S. Gelaki, and V. Ostrik, *Classification of Fusion Categories of Dimension pq*, Int. Math. Res. Not. (2004), no. 57, 3041–3056.

[19] W. Eholzer, *On the Classification of Modular Fusion Algebras*, Comm. Math. Phys. **172** (1995), no. 3, 623–659.

[20] W. Eholzer, *Fusion algebras induced by representations of the modular group*, Internat. J. Modern Phys. A **8** (1993), no. 20, 3495–3507.

[21] D. E. Evans and Y. Kawahigashi, *Quantum symmetries on operator algebras*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998, Oxford Science Publications.

[22] P. Etingof, D. Nikshych, and V. Ostrik, *On Fusion Categories*, Ann. of Math. **162** (2005), no. 2, 581–642.

[23] P. Etingof, D. Nikshych, and V. Ostrik, *Fusion Categories and Homotopy Theory*, Quantum Topol. **1** (2010), no. 3, 209–273.

[24] P. Etingof, *On Vafa's Theorem for Tensor Categories*, Mathematical Research Letters **9** (2002), 651–657.

[25] J.-H. Evertse, *On Sums of S-Units and Linear Recurrences*, Compositio Mathematica (1984), no. 53, 225–244.

[26] J.-H. Evertse, *The Number of Solutions of Decomposable Form Equations*, Invent. Math. (1995), no. 122, 559–601.

[27] M. H. Freedman, *A Magnetic Model with a Possible Chern-Simons Phase. With an appendix by F. Goodman and H. Wenzl.*, Comm. Math. Phys. **234** (2003), no. 1, 129–183.

[28] S. Gelaki and D. Nikshych, *Nilpotent Fusion Categories*, Adv. Math. **217** (2008), no. 3, 1053–1071.

[29] S. Gelaki, D. Naidu, and D. Nikshych, *Centers of Graded Fusion Categories*, Algebra Number Theory **3** (2009), no. 8, 959–990.

[30] S.-M. Hong and E. Rowell, *On the Classification of the Grothendieck Rings of Non-Self Dual Modular Categories*, J. Algebra **324** (2010), no. 5, 1000–1015.

[31] Y.-Z. Huang, *Vertex operator algebras, the Verlinde conjecture, and modular tensor categories*, Proc. Natl. Acad. Sci. USA **102** (2005), no. 15, 5352–5356 (electronic).

[32] A. Joyal and R. Street, *Braided Tensor Categories*, Adv. Math. **102** (1993), no. 1, 20–78.

[33] C. Kassel, *Quantum groups*, Springer-Verlag, New York, 1995.

[34] D. Kazhdan and H. Wenzl, *Reconstructing monoidal categories*, Adv. in Soviet Math. **16** (1993), 111–136.

[35] Y. Kashina, Y. Sommerhäuser, and Y. Zhu, *On Higher Frobenius-Schur Indicators*, Mem. Amer. Math. Soc. **181** (2006), no. 855.

[36] E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante*, Math. Ann. **50** (1903), 671–676.

[37] F. Liu, Z. Wang, Y.-Z. You, and X.-G. Wen, *Quantum fidelity, modular transformations, and topological orders in two dimensions*, (2013). preprint: arXiv:1303.0829.

[38] M. Müger, *From Subfactors to Categories and Topology II: The Quantum Doubles of Tensor Categories and Subfactors*, J. Pure Appl. Algebra **180** (2003), no. 1–2, 159–219.

[39] G. Moore and N. Seiberg, *Classical and quantum conformal field theory*, Comm. Math. Phys. **123** (1989), no. 2, 177–254.

[40] D. Naidu and E. C. Rowell, *A Finiteness Property for Braided Fusion Categories*, Algebr. Represent. Theory **14** (2011), no. 5, 837–855.

[41] S.-H. Ng and P. Schauenburg, "Higher Frobenius-Schur indicators for pivotal categories", *Hopf algebras and generalizations*, vol. 441, Contemp. Math. Amer. Math. Soc., Providence, RI, 2007, pp. 63–90.

[42] S.-H. Ng and P. Schauenburg, *Frobenius-Schur Indicators and Exponents of Spherical Categories*, Adv. Math. **211** (2007), no. 1, 34–71.

[43] S.-H. Ng and P. Schauenburg, *Congruence Subgroups and Generalized Frobenius-Schur Indicators*, Comm. Math. Phys. **300** (2010), no. 1, 1–46.

[44] V. Ostrik, *On Formal Codegrees of Fusion Categories*, Math. Res. Lett. **16** (2009), no. 5, 895–901.

[45] V. Ostrik, *Module Categories over the Drinfeld Double of a Finite Group*, Int. Math. Res. Not. (2003), no. 27, 1507–1520.

[46] E. C. Rowell, *From Quantum Groups to Unitary Modular Tensor Categories*, Contemp. Math. **413** (2006).

[47] E. Rowell, R. Stong, and Z. Wang, *On Classification of Modular Tensor Categories*, Comm. Math. Phys. **292** (2009), no. 2, 343–389.
[48] V. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, De Gruyter Studies in Mathematics, Walter de Gruyter, 1994.
[49] V. G. Turaev, *Modular categories and 3-manifold invariants*, Internat. J. Modern Phys. B **6** (1992), no. 11-12, 1807–1824, Topological and quantum group methods in field theory and condensed matter physics.
[50] I. Tuba and H. Wenzl, *Representations ofthe braid group* B_3 *and* $SL(2,\mathbb{Z})$, Pacific J. Math. **197** (2001), 491–510.
[51] C. Vafa, *Toward classification of conformal theories*, Phys. Lett. B **206** (1988), no. 3, 421–426.
[52] Z. Wang, *Topological Quantum Computation*, CBMS Regional Conference Series in Mathematics, no. 112, Amer. Mathematical Society, 2010.
[53] Z. Wang, "Quantum Computing: A Quantum Group Approach", *Symmetries and groups in contemporary physics–Proceedings of the XXIX International Colloquium on Group-Theoretical Methods in Physics*, Tianjin, China, 2012, pp. 41–50.
[54] Z. Wang, "Topologization of electron liquids with Chern-Simons theory and quantum computation", *Differential geometry and physics*, vol. 10, Nankai Tracts Math. World Sci. Publ., Hackensack, NJ, 2006, pp. 106–120.
[55] L. Washington, *Introduction to Cyclotomic Fields*, Second Edition, Graduate Texts in Mathematics, Springer, 1996.
[56] E. Weiss, *Algebraic Number Theory*, Second (unaltered) Edition, Chelsea Publishing Company, 1976.
[57] K. Walker and Z. Wang, *(3+1)-TQFTS and Topological Insulators*, Front. Phys. **7** (2012), no. 2, 150–159.
[58] F. Xu, *Some computations in the cyclic permutations of completely rational nets*, Comm. Math. Phys. **267** (2006), no. 3, 757–782.

E-mail address: pjb2357@gmail.com

Department of Mathematics, Texas A&M University, College Station, TX U.S.A.

Current address: Pacific Northwest National Laboratory, 902 Battelle Boulevard, Richland, WA U.S.A

E-mail address: rng@math.lsu.edu

Department of Mathematics, Louisiana State University, Baton Rouge, LA U.S.A.

Department of Mathematics, Iowa State University, Ames, IA U.S.A.

E-mail address: rowell@math.tamu.edu

Department of Mathematics, Texas A&M University, College Station, TX U.S.A.

E-mail address: zhenghwa@microsoft.com

Microsoft Research Station Q and Department of Mathematics, University of California, Santa Barbara, CA U.S.A.