4-3-2023

SL(2,Z) Representations and 2-Semiregular Modular Categories

Samuel Nathan Wilson
Louisiana State University and Agricultural and Mechanical College

$\mathbf{SL_2(\mathbb{Z})}$ REPRESENTATIONS AND 2-SEMIREGULAR MODULAR CATEGORIES

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Samuel Nathan Wilson
B.A., Oklahoma University, 2010
M.S., Texas State University, 2013
May 2023

Acknowledgments

For all that it has my name on it, this dissertation would be so much blank paper without the wisdom and patience of my advisor Dr. Siu-Hung Ng, as well as the positivity and keen insight of Dr. Yilong Wang. They not only taught me everything I know of modular categories, but gave guidance and support far beyond my due. Much of this dissertation is based on our joint research: [36, 37].

There are many other professors who deserve my thanks, here at LSU and elsewhere. To list them all would be a hopeless task: Dr. Pramod Achar, Dr. Richard Litherland, Dr. Shea Vela-Vick, Dr. William Adkins, Dr. Anton Zeitlin, Dr. Ling Long, Dr. Bogdan Oporowski, Dr. James Oxley, Dr. Shawn Walker, Dr. Daniela Ferrero, Dr. Susan Morey.

And of course, thanks also to my fellow students, who kept me sane along this long, long road: Joseph, Tara, Sarah, Khalid, Walter, Prerna, Cameron, Kent, Sterling, Lucas, Nurdin, SeongHee, and Vishnu, whom my mother will never forget.

This dissertation is dedicated to my parents, who taught me to ask questions, the only thing that really matters; my brother, who knows me better than he thinks; and Vanessa, who believed in me even when I didn't. Sorry for making you wait so long.

And Psyche, of course. One last trip.

Table of Contents

Abstract

We address the open question of which representations of the modular group $\mathrm{SL}_2(\mathbb{Z})$ can be realized by a modular category. In order to investigate this problem, we introduce the concept of a symmetrizable representation of $\mathrm{SL}_2(\mathbb{Z})$ and show that this property is necessary for the representation to be realized. We then prove that all congruence representations of $\mathrm{SL}_2(\mathbb{Z})$ are symmetrizable. The proof involves constructing a symmetric basis, which greatly aids in further calculation. We apply this result to the reconstruction of modular category data from representations, as well as to the classification of semiregular categories, which are defined via an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on their simple objects.

Chapter 1. Preliminaries

1.1. Introduction

The concept that would later come to be called a *modular category*[1] originally arose in the context of 2-dimensional rational conformal field theory [45]. Quantum field theories are mathematical structures designed to axiomatize and formalize the rules of quantum physics, and conformal field theories are QFTs which are invariant under conformal transformations. Moore and Seiberg [28, 29] investigated rational chiral CFTs and determined a set of data — the Moore–Seiberg data — that sufficed to describe their properties. However, their formulation was dependent upon a non-canonical choice of basis. The definition of a modular category, then, is a realization of those properties in a basis-invariant setting, and the Moore–Seiberg data can be discerned among the invariants and properties of the category: the fusion matrices (as described in Section 2.3), the S-matrix (Section 2.6), the F-matrix[2] (see [44, Chapter VI]), and the pentagon and hexagon relations (Theorem 2.1.2 and Definition 2.5.1). That many modular categories arise as the representation categories of regular vertex operator algebras [17, 18, 51] is ultimately this same fact viewed in a different context.

The connection between modular categories and RCFTs is expressed through a 3-dimensional *topological quantum field theory* (see [41, 45, 24, 50]). This is a monoidal functor from the cobordism category **3Cob** to the category Vec($\Bbbk$) of finite-dimensional vector spaces over a field $\Bbbk$, preserving the symmetric braiding (see Sections 2.1 and 2.5). Roughly speaking, the objects of **3Cob** are 2-manifolds with marked points, and the mor-

[1] Many authors prefer "modular tensor category," but there seems to be no consensus on the precise implication of the word "tensor."

[2] Also known as the $6j$-symbols.

phisms are cobordisms connecting them — here, a cobordism $M : A \to B$ is a 3-manifold whose boundary is identified with $A \sqcup B$ in the obvious way, and which contains a ribbon graph that connects the marked points of A and B. Every modular category $\mathscr{C}$ gives rise to such a TQFT, with the ribbon graphs being precisely those of the graphical calculus introduced in Section 2.1.3. See [22, 43] for a description of how the resulting TQFT can be used in constructing a RCFT.

As one might expect from their intertwined algebraic and topological structures, modular categories are closely related to algebraic topology. A number of concepts from areas such as knot theory and homology can be recognized in their study. The quantum trace (Definition 2.2.7) immediately gives rise to a family of invariants for braids and links, as a trivial example. Invariants for 3-manifolds may likewise be constructed from modular categories. The Kauffman bracket, Jones polynomial, and Jones–Wenzl idempotents may be seen as precursors to the ideas used in the graphical calculus, and the skein modules that underlie them can be used to construct modular categories. For more on this topic, see [45].

A recent application of modular categories and the TQFTs that arise from them is in the realm of quantum computation and quantum information. Quantum computation requires novel methods of fault-correction — classical methods (e.g. simple duplication of the data) are often impossible or impractical when dealing with qubits, which cannot be read or copied without causing the quantum state to collapse. The first error-correcting code for qubits was the toric code devised by Kitaev [4, 25]; this was later generalized into the Levin–Wen string-net model [26]. In these designs, information is stored in a system of anyons in a 2-manifold that exhibits a topological phase. While such a system has not yet

been constructed in reality, a physical implementation of the concept has been considered wherein the anyons take the form of quasiparticles[3] in fractional quantum Hall liquids. Such topological phases correspond, one-to-one, with (unitary) modular categories [49]. Explicitly, the anyons correspond to the simple objects of the category, their trajectories through spacetime are the ribbons of the graphical calculus, and the results of fusing them together are recorded by the fusion matrices and related statistics such as the F-matrices. Computation is then performed by braiding the anyons, and the topological invariance expressed by the ribbon structure (see Section 2.5) makes the state resistant to small-scale errors. A more complete description of topological quantum computation is given in [49].

The name "modular category" comes from the fact that each such category gives rise to a family of representations of the *modular group* $\mathrm{SL}_2(\mathbb{Z})$; this will be described in more detail in Section 3.1.2. This group and its representations appear in many areas of mathematics. For example, there is a well-studied action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half of the complex plane, $\mathbb{H}$. Namely, for $\mathfrak{g} = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, we define $\mathfrak{g}z = \frac{az+b}{cz+d}$. Then, a *modular form* of weight w on a finite-index subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ that is bounded as $z \to \infty i$ and which satisfies the symmetry condition

$$(\mathfrak{g} \cdot f)(z) \coloneqq (cz + d)^{-w} f(\mathfrak{g}z) = f(z)$$

for all $z \in \mathbb{H}$ and all $\mathfrak{g} \in \Gamma$. Modular forms are of interest primarily in analytic number theory, and are related to elliptic curves, Riemann surfaces, and Dirichlet series [1]. Modular categories give rise to modular forms; if $\mathscr{C}$ is the representation category of a regular vertex operator algebra $V = \bigoplus_{w \in \mathbb{N}} V_w$, then for each $v \in V_w$ there is a family of functions

[3] Pointlike defects, usually packets of excited particles, that behave like anyons.

$\{f_{a,v}\}_{a\in\mathrm{Irr}(\mathscr{C})}$ satisfying

$$\begin{bmatrix} (\mathfrak{g}\cdot f_{a_1,v})(z) \\ (\mathfrak{g}\cdot f_{a_2,v})(z) \\ \vdots \\ (\mathfrak{g} f_{a_{r_\mathscr{C}},v})(z) \end{bmatrix} = (cz+d)^{-w} \begin{bmatrix} f_{a_1,v}(\mathfrak{g}z) \\ f_{a_2,v}(\mathfrak{g}z) \\ \vdots \\ f_{a_{r_\mathscr{C}},v}(\mathfrak{g}z) \end{bmatrix} = \rho(\mathfrak{g}) \begin{bmatrix} f_{a_1,v}(z) \\ f_{a_2,v}(z) \\ \vdots \\ f_{a_{r_\mathscr{C}},v}(z) \end{bmatrix}$$

for all $z \in \mathbb{H}$ and $\mathfrak{g} \in \mathrm{SL}_2(\mathbb{Z})$. Here $r_\mathscr{C}$ is the rank of $\mathscr{C}$, and $\rho(\mathfrak{g})$ is one of the $\mathrm{SL}_2(\mathbb{Z})$ representations of $\mathscr{C}$ (see Section 3.1.2). It may be shown that all such representations have congruence kernels [9]. As such, taking $\Gamma := \ker\rho$, the family $\{f_{a,v}\}_{a\in\mathrm{Irr}(\mathscr{C})}$ defines a vector-valued modular form of weight w on Γ.

A full list of topics with connections to modular categories would fill many pages. For a more thorough history, we refer the reader to sources such as [13, 3, 14, 45].

There is an ongoing project to classify the modular categories (up to equivalence). It has been shown that, for any rank $r \in \mathbb{Z}^+$, there are only a finite number of equivalence classes of modular categories having that rank [7]. Following this, a series of papers by various authors ([42, 6, 33]) have classified all modular categories with rank 6 or less. Another approach is to organize modular categories according to the orbits of a certain Galois action, which we will define in Section 2.6.17. When this action is semiregular — i.e. fixed-point free — the category is called *k-semiregular*, where k is the number of orbits. In [38], the *transitive* categories, which are automatically 1-semiregular, are completely classified. Most of the results in this dissertation arose in the investigation of 2-semiregular categories, which are discussed in Chapter 4. Other approaches include classifying categories by their dimension ([5, 8]; see Definition 2.3.7) or by their Frobenius–Schur exponent ([47]; see Section 2.5.2). It is the author's hope that this dissertation will be helpful in furthering this classification project.

1.2. Overview

The structure of this dissertation is as follows.

In Chapter 2, we describe in detail the properties and data that define a modular category. In brief, a modular category is a monoidal category possessing a *fusion* structure and a compatible *ribbon* structure and satisfying a non-degeneracy condition. The fusion structure makes $\mathrm{Ob}(\mathscr{C})$ into an algebra over a field, usually taken to be $\mathbb{C}$. Meanwhile, the morphisms in any monoidal category may be represented in a visual format similar to a braid diagram in a process known as *graphical calculus*, and the presence of a ribbon structure causes these diagrams to behave in a manner similar to the braid or knot diagrams on which they are based — by remaining invariant under the Reidemeister moves, for instance. The non-degeneracy condition ensures that the generators of the fusion algebra are distinguishable in an appropriate sense. This chapter includes proofs of some properties which, while well-known, are often glossed over in the literature.

In Chapter 3, we consider *MC representations*: finite-dimensional representations of the modular group $\mathrm{SL}_2(\mathbb{Z})$ that arise from a modular category in a natural way. The question of which finite-dimensional $\mathrm{SL}_2(\mathbb{Z})$-representations occur in this way remains open, but it may be shown that any such representation must be *congruence*, and we show that it must also be *symmetrizable*. Complex congruence representations are easily classified by means of the Chinese remainder theorem. There exist finite-dimensional $\mathrm{SL}_2(\mathbb{Z})$-representations which are not symmetrizable, but all examples displaying this behavior are not congruence. It is therefore natural to inquire whether there are any complex congruence representations of $\mathrm{SL}_2(\mathbb{Z})$ which cannot be symmetrized. The primary result of this

dissertation is that this is impossible:

Theorem 3.1.10. *Every finite-dimensional complex congruence representation of* $\mathrm{SL}_2(\mathbb{Z})$ *is symmetrizable.*

To prove this theorem, we make use of the classification of congruence $\mathrm{SL}_2(\mathbb{Z})$-representations (as devised in [39, 40]), and we provide a number of proofs regarding the details of this construction.

In Chapter 4, we describe various applications of the results in the previous chapters. The techniques used in our proof of Theorem 3.1.10 can be used to construct an explicit *symmetric basis* for any congruence representation — indeed, as part of the research that led to this dissertation, we implemented a `GAP` package [36] that does so. We demonstrate how this basis can be used in addressing the question of realizability: for some representations, we find immediately a proof that they are not realizable, while for others, it is possible to reconstruct data (such as the fusion rules) of a possible category realizing them. We also consider semiregular modular categories and the Galois action by which they are characterized. By making use of symmetrizability and the properties of MC representations, we derive certain properties of semiregular categories in general and 2-semiregular categories in particular.

1.3. Definitions and notation

We denote by $\mathbf{e} : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}$ the map given by $\mathbf{e}(k) = e^{2\pi i k}$; this forms an isomorphism from the additive group $\mathbb{Q}/\mathbb{Z}$ to the group of finite roots of unity in $\mathbb{C}$. For $k \in \mathbb{N}$, $\zeta_k := \mathbf{e}\left(\frac{1}{k}\right)$ is a primitive root of unity of order k. Particularly, $i = \mathbf{e}\left(\frac{1}{4}\right) = \zeta_4$. We fix $\sqrt{\zeta_k}$ to be the positive square root ζ_{2k}.

We assume the reader is familiar with the basics of category theory, as covered in e.g. [27]. If $\mathscr{C}$ is a category, we will write $\mathscr{C} = \mathrm{Ob}(\mathscr{C})$ for the set of objects and $\mathscr{C}(a,b) = \mathrm{Mor}_{\mathscr{C}}(a,b)$ for the set of morphisms in $\mathscr{C}$ from a to b. The opposite category $\mathscr{C}^{\mathrm{op}}$ is identical to $\mathscr{C}$ except for having all arrows reversed.

For a vector space V over a field $\Bbbk$, its dual is $V^* \coloneqq \mathrm{Hom}_{\Bbbk}(V, \Bbbk)$.

For $\Bbbk$ a field, we write $\bar{\Bbbk}$ for its algebraic closure. When $n \in \mathbb{Z}^+$, the Galois field extension $\mathbb{Q}(\zeta_n)$ is also denoted $\mathbb{Q}_n$.

For G a group, its character group is $\hat{G} \coloneqq \mathrm{Hom}(G, \Bbbk^\times)$.

For $A \in \mathrm{M}_n(\Bbbk)$ and $B \in \mathrm{GL}_n(\Bbbk)$, we write $A^B \coloneqq B^{-1}AB$. When $\Bbbk = \mathbb{C}$, the conjugate transpose of A is denoted $A^\dagger \coloneqq \overline{A^{\mathrm{T}}}$; if $A^\dagger = A^{-1}$, then A is called unitary. The field extension of $\mathbb{Q}$ found by adjoining all entries of a matrix A is denoted $\mathbb{Q}(A)$.

Chapter 2. Modular Categories

We will first describe in brief the various properties defining a modular category; we refer the reader to [3, 13, 23, 27] for more detailed treatments.

2.1. Monoidal categories

2.1.1. Monoidal structures

Definition 2.1.1. Let $\mathscr{C}$ be a category. A *monoidal structure* $(\otimes, \mathbb{1}, \alpha, \lambda, \rho)$ on $\mathscr{C}$ consists of the following data:

- a bifunctor $\otimes : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$, which we call the tensor product,
- a designated object $\mathbb{1}$, called the unit object,
- a natural isomorphism $\alpha : (\bullet \otimes \bullet) \otimes \bullet \to \bullet \otimes (\bullet \otimes \bullet)$, called the associator (with a component $\alpha_{a,b,c} : (a \otimes b) \otimes c \to a \otimes (b \otimes c)$ for all $a, b, c \in \mathscr{C}$) and
- natural isomorphisms $\lambda : \mathbb{1} \otimes \bullet \to \bullet$ and $\rho : \bullet \otimes \mathbb{1} \to \bullet$, called the left and right unitors (with components $\lambda_a : \mathbb{1} \otimes a \to a$ and $\rho_a : a \otimes \mathbb{1} \to a$ for all $a \in \mathscr{C}$).

When considering multiple categories, we will label the data of $\mathscr{C}$ by $\otimes^{\mathscr{C}}$, $\mathbb{1}^{\mathscr{C}}$, $\alpha^{\mathscr{C}}$, $\lambda^{\mathscr{C}}$, and $\rho^{\mathscr{C}}$. Note that, for any morphism $\varphi \in \mathscr{C}(a, b)$ and any object $c \in \mathscr{C}$, we have $\varphi \otimes c = \varphi \otimes \mathrm{id}_c$ in $\mathscr{C}(a \otimes c, b \otimes c)$ and similarly $c \otimes \varphi \in \mathscr{C}(c \otimes a, c \otimes b)$. To save space, we will label these simply by φ when the meaning is clear from the context.

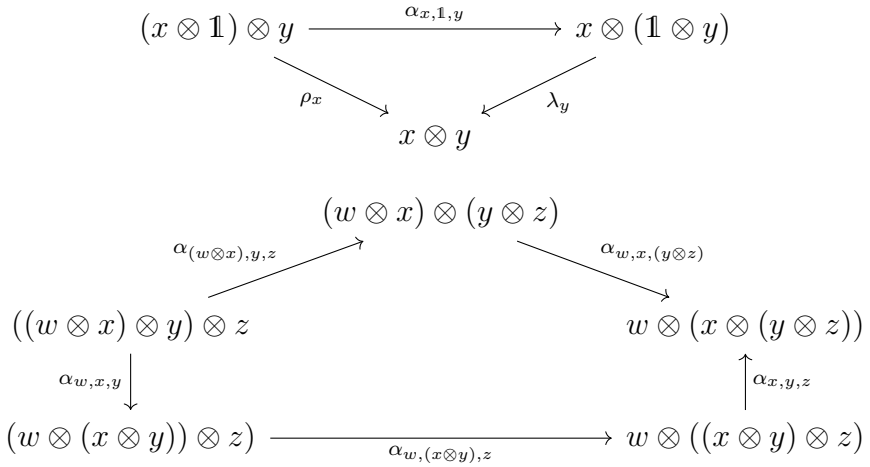
The isomorphisms α, λ, ρ must satisfy an associativity axiom. As a demonstration of this axiom, consider a sequence $[a, b, c]$ of objects in $\mathscr{C}$. This sequence corresponds to several possibly-distinct objects in $\mathscr{C}$, such as $x = (a \otimes \mathbb{1}) \otimes (b \otimes c)$ and $y = a \otimes ((b \otimes \mathbb{1}) \otimes c)$. The axiom states that α, λ, and ρ should form a unique isomorphism $x \to y$ (this being simply id_x if $x = y$). Such an isomorphism — the composition of tensor products of α, λ, ρ, and their inverses, along with the identity — is called a *legal isomorphism*. Extending this

idea to arbitrary sequences of objects in $\mathscr{C}$, we have the following:

Associativity axiom. *Consider any sequence of objects* $[a_1, a_2, \cdots, a_m]$ *with* $a_i \in \mathscr{C}$. *Suppose* x *and* y *are two objects obtained by tensoring the sequence in order and inserting parentheses and* $\mathbb{1}$*s arbitrarily. Then there is a unique legal isomorphism from* x *to* y.

This axiom may be difficult to handle directly, but the MacLane coherence theorem gives conditions which are more easily checked. For a proof of this theorem, see [27, §VII.2].

Theorem 2.1.2 (MacLane coherence theorem)**.** *The associativity axiom is equivalent to the commutativity of the following two diagrams (known as the* triangle *and* pentagon *axioms) for all* $w, x, y, z \in \mathscr{C}$*:*



A monoidal category in which $\alpha_{x,y,z}$, λ_x, and ρ_x are identities for all objects $x, y, z \in \mathscr{C}$ is called *strict*. The functor category $\mathrm{End}(\mathscr{A})$ of any abelian category $\mathscr{A}$, with $F \otimes G \coloneqq F \circ G$ and $\mathbb{1} \coloneqq \mathrm{id}_{\mathscr{A}}$, is an example of a strict monoidal category. When $\mathscr{C}$ is strict, each finite sequence $[x_1, x_2, \cdots, x_m]$ of objects in $\mathscr{C}$ corresponds to a unique object in $\mathscr{C}$; hence, by convention, we simply omit the parentheses and $\mathbb{1}$s and name that object $x_1 \otimes x_2 \otimes \cdots \otimes x_m$.

Let us now construct an explicit example of a monoidal category. Let G be a group

and ω a normalized 3-cocycle of G with coefficients in $\Bbbk^\times$ for a field $\Bbbk$; then, define the category $\mathscr{G} := \mathrm{Vec}_G^\omega(\Bbbk)$ as follows. Objects in $\mathscr{G}$ are G-graded, finite-dimensional $\Bbbk$-vector spaces; that is, each $V \in \mathscr{C}$ has the form $\bigoplus_{g\in G} V_g$ where each V_g is a finite-dimensional $\Bbbk$-vector space. Morphisms in $\mathscr{G}$ are vector space homomorphisms which preserve the grading — in other words, a morphism $V \to W$ has the form $\bigoplus_{g\in G} \varphi_g$ where each $\varphi_g : V_g \to W_g$ is a vector space homomorphism.

We may define a tensor product $\otimes$ on $\mathscr{G}$ via

$$(V \otimes W)_g := \bigoplus_{\substack{h,k\in G \\ hk=g}} V_h \otimes_\Bbbk W_k \ .$$

To define the associator, we first find that

$$((U \otimes V) \otimes W)_g := \bigoplus_{\substack{h,k,m\in G \\ hkm=g}} (U_h \otimes_\Bbbk V_k) \otimes_\Bbbk W_m$$

$$(U \otimes (V \otimes W))_g := \bigoplus_{\substack{h,k,m\in G \\ hkm=g}} U_h \otimes_\Bbbk (V_k \otimes_\Bbbk W_m) \ .$$

The associator is then the canonical associator of $\Bbbk$-vector spaces applied componentwise, multiplied by the scalar given by ω:

$$\alpha : (U_h \otimes_\Bbbk V_k) \otimes_\Bbbk W_m \xrightarrow{\omega(h,k,m)} U_h \otimes_\Bbbk (V_k \otimes_\Bbbk W_m) \ .$$

The unit object $\mathbb{1}$ of $\mathscr{G}$ is defined by $\mathbb{1}_{1_G} = \Bbbk$ and $\mathbb{1}_g = 0$ for $g \neq 1_G$, and the left and right unitors are scalar multiplication: with $c \in \mathbb{1}$, we have $c \otimes v \mapsto cv$ and $v \otimes c \mapsto cv$. These choices satisfy the conditions of Theorem 2.1.2, hence define a monoidal category. Explicitly, since ω is normalized, we have $\omega_{h,\mathbb{1},k} = 1$, so the triangle axiom is trivial, while the pentagon axiom translates directly to the 3-cocycle condition

$$\omega(h,k,mn)\cdot\omega(hk,m,n) = \omega(h,k,m)\cdot\omega(h,km,n)\cdot\omega(k,m,n) \text{ for all } h,k,m,n \in G \ .$$

2.1.2. Monoidal functors

To compare two monoidal categories, we define a monoidal functor: a standard functor plus additional data to carry the monoidal structure.

Definition 2.1.3. Let $\mathscr{C}$ and $\mathscr{D}$ be monoidal categories. A *monoidal functor*[1] $(F, \varphi_0, \varphi_2)$ from $\mathscr{C}$ to $\mathscr{D}$ consists of

- a functor $F : \mathscr{C} \to \mathscr{D}$,
- an isomorphism $\varphi_0 : \mathbb{1}^{\mathscr{D}} \to F\mathbb{1}^{\mathscr{C}}$, and
- a natural isomorphism $\varphi_2 : F(\bullet) \otimes F(\bullet) \to F(\bullet \otimes \bullet)$, called coherence,

such that the following diagrams commute for all $a, b, c \in \mathscr{C}$:

$$\begin{array}{ccc} \mathbb{1}^{\mathscr{D}} \otimes Fa & \xrightarrow{\lambda^{\mathscr{D}}_{Fa}} & Fa \\ {\scriptstyle \varphi_0}\downarrow & & \uparrow{\scriptstyle F(\lambda^{\mathscr{C}}_a)} \\ F\mathbb{1}^{\mathscr{C}} \otimes Fa & \xrightarrow{\varphi_2(\mathbb{1}^{\mathscr{C}}, a)} & F(\mathbb{1}^{\mathscr{C}} \otimes a) \end{array}$$

$$\begin{array}{ccc} Fa \otimes \mathbb{1}^{\mathscr{D}} & \xrightarrow{\rho^{\mathscr{D}}_{F(a)}} & Fa \\ {\scriptstyle \varphi_0}\downarrow & & \uparrow{\scriptstyle F(\rho^{\mathscr{C}}_a)} \\ Fa \otimes F\mathbb{1}^{\mathscr{C}} & \xrightarrow{\varphi_2(a, \mathbb{1}^{\mathscr{C}})} & F(a \otimes \mathbb{1}^{\mathscr{C}}) \end{array}$$

$$\begin{array}{ccccc} & & (Fa \otimes Fb) \otimes Fc & \xrightarrow{\alpha^{\mathscr{D}}} & Fa \otimes (Fb \otimes Fc) \\ & {\scriptstyle \varphi_2(a,b)}\swarrow & & & \searrow{\scriptstyle \varphi_2(b,c)} \\ F(a \otimes b) \otimes Fc & & & & Fa \otimes F(b \otimes c) \\ & {\scriptstyle \varphi_2(a\otimes b, c)}\searrow & & & \swarrow{\scriptstyle \varphi_2(a, b\otimes c)} \\ & & F((a \otimes b) \otimes c) & \xrightarrow{F(\alpha^{\mathscr{C}})} & F(a \otimes (b \otimes c)) \end{array}$$

If φ_2 and φ_0 are identities, we call $(F, \varphi_0, \varphi_2)$ a *strict* monoidal functor; any monoidal category $\mathscr{C}$ admits a strict monoidal functor $(\mathrm{id}, \mathrm{id}, \mathrm{id})_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$. When the monoidal structure is clear, we will denote $(F, \varphi_0, \varphi_2)$ only by F.

[1]The object defined here is sometimes called a *strong* monoidal functor, with a *lax* monoidal functor differing only in not requiring φ_0 and φ_2 to be isomorphisms.

Given two monoidal functors $(F, \varphi_0, \varphi_2) : \mathscr{C} \to \mathscr{D}$ and $(G, \gamma_0, \gamma_2) : \mathscr{D} \to \mathscr{E}$, the composition $(G, \gamma_0, \gamma_2) \circ (F, \varphi_0, \varphi_2) : \mathscr{C} \to \mathscr{E}$ is given by $(G \circ F,\ G(\varphi_0) \circ \gamma_0,\ G(\varphi_2) \circ \gamma_2)$, wherein the monoidal structure consists of the compositions

$$\mathbb{1}^{\mathscr{E}} \xrightarrow{\gamma_0} G\mathbb{1}^{\mathscr{D}} \xrightarrow{G(\varphi_0)} GF\mathbb{1}^{\mathscr{C}}$$

$$GFa \otimes GFb \xrightarrow{\gamma_2(Fa,Fb)} G(Fa \otimes Fb) \xrightarrow{G(\varphi_2(a,b))} GF(a \otimes b)\ .$$

It is easy to check that this gives another monoidal functor.

Definition 2.1.4. Let $(F, \varphi_0, \varphi_2)$ and (G, γ_0, γ_2) be monoidal functors $\mathscr{C} \to \mathscr{D}$. Then a *natural transform of monoidal functors* $\eta : (F, \varphi_0, \varphi_2) \to (G, \gamma_0, \gamma_2)$ is a natural transform $\eta : F \to G$ so that the following diagrams commute for all $a, b \in \mathscr{C}$:

$$\begin{array}{ccc} & & F\mathbb{1}^{\mathscr{C}} \\ & \overset{\varphi_0}{\nearrow} & \downarrow{\scriptstyle \eta(\mathbb{1}^{\mathscr{C}})} \\ \mathbb{1}^{\mathscr{D}} & & \\ & \underset{\gamma_0}{\searrow} & G\mathbb{1}^{\mathscr{C}} \end{array}$$

$$\begin{array}{ccc} Fa \otimes Fb & \xrightarrow{\varphi_2(a,b)} & F(a \otimes b) \\ {\scriptstyle \eta(a)\otimes\eta(b)}\downarrow & & \downarrow{\scriptstyle \eta(a\otimes b)} \\ Ga \otimes Gb & \xrightarrow{\gamma_2(a,b)} & G(a \otimes b) \end{array}$$

If η is a natural isomorphism (i.e. $\eta(a)$ is an isomorphism for all $a \in \mathscr{C}$), it is an *isomorphism of monoidal functors*; in this case we write $(F, \varphi_0, \varphi_2) \overset{\eta}{\cong} (G, \gamma_0, \gamma_2)$.

Definition 2.1.5. A monoidal functor $(F, \varphi_0, \varphi_2) : \mathscr{C} \to \mathscr{D}$ is called a *monoidal equivalence* if there exists some monoidal functor $(G, \gamma_0, \gamma_2) : \mathscr{D} \to \mathscr{C}$ such that

$$(G, \gamma_0, \gamma_2) \circ (F, \varphi_0, \varphi_2) \cong (\mathrm{id}, \mathrm{id}, \mathrm{id})_{\mathscr{C}}$$

$$(F, \varphi_0, \varphi_2) \circ (G, \gamma_0, \gamma_2) \cong (\mathrm{id}, \mathrm{id}, \mathrm{id})_{\mathscr{D}}\ .$$

In this case, we say $\mathscr{C}$ and $\mathscr{D}$ are *monoidally equivalent*.

Proposition 2.1.6. *Suppose $(F, \varphi_0, \varphi_2)$ is a monoidal functor. Then $(F, \varphi_0, \varphi_2)$ is a monoidal equivalence if and only if F is an equivalence of categories.*

Proof. Suppose we have a monoidal functor $(F, \varphi_0, \varphi_2) : \mathscr{C} \to \mathscr{D}$ wherein F is an equivalence of categories. This means there is a functor $G : \mathscr{D} \to \mathscr{C}$ and natural isomorphisms $\varepsilon : FG \to \mathrm{id}_{\mathscr{D}}$ and $\eta : \mathrm{id}_{\mathscr{C}} \to GF$. Equivalently, G is a left and right adjoint for F and both F and G are full and faithful. The right adjunction may be expressed through a natural isomorphism $\tau : \mathscr{C}(\bullet, G(\bullet)) \to \mathscr{D}(F(\bullet), \bullet)$, which acts as follows: for $a \in \mathscr{C}$ and $x \in \mathscr{D}$, τ sends a morphism $\alpha : a \to G(x)$ to the composition

$$\tau(\alpha) : Fa \xrightarrow{F(\alpha)} FGx \xrightarrow{\varepsilon_x} x$$

and τ^{-1} sends $\beta : Fa \to x$ to

$$\tau^{-1}(\beta) : a \xrightarrow{\eta_a} GFa \xrightarrow{G(\beta)} Gx \ .$$

Let us use τ to extend G to a monoidal functor. Noting that φ_0^{-1} is a natural isomorphism $F\mathbb{1}^{\mathscr{C}} \to \mathbb{1}^{\mathscr{D}}$, we first define $\gamma_0 : \mathbb{1}^{\mathscr{C}} \to G\mathbb{1}^{\mathscr{D}}$ by $\gamma_0 := \tau^{-1}(\varphi_0^{-1})$, which is an isomorphism because φ_0^{-1} is. This definition yields a commutative diagram

$$\begin{array}{ccc} \mathbb{1}^{\mathscr{D}} & \xleftarrow{\quad\varepsilon\quad} & FG\mathbb{1}^{\mathscr{D}} \\ & {\scriptstyle\varphi_0}\searrow \quad \nearrow{\scriptstyle F(\gamma_0)} & \\ & F\mathbb{1}^{\mathscr{C}} & \end{array} \tag{2.1}$$

Similarly, for each $x, y \in \mathscr{D}$, we have an isomorphism

$$\tilde{\gamma}_2 : F(Gx \otimes Gy) \xrightarrow{\varphi_2^{-1}} FGx \otimes FGy \xrightarrow{\varepsilon_x \otimes \varepsilon_y} x \otimes y \ ,$$

and we define $\gamma_2 : Gx \otimes Gy \to G(x \otimes y)$ by $\gamma_2(x, y) := \tau^{-1}(\tilde{\gamma}_2(x, y))$. This makes γ_2 a

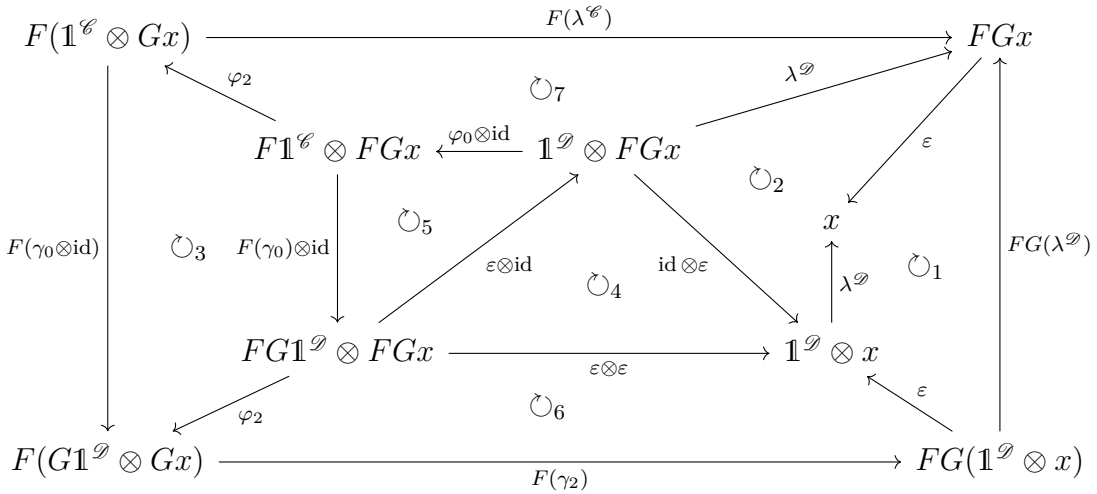
natural isomorphism, because ε, τ, and φ_2 are. The corresponding diagram is

$$\begin{array}{ccc} F(Gx \otimes Gy) & \xleftarrow{\varphi_2} & FGx \otimes FGy \\ \downarrow{\scriptstyle F(\gamma_2)} & & \downarrow{\scriptstyle \varepsilon\otimes\varepsilon} \\ FG(x \otimes y) & \xrightarrow{\varepsilon} & x \otimes y \end{array} \tag{2.2}$$

Next, we show that γ_0 and γ_2 make the diagrams from Definition 2.1.3 commute. Applying the natural isomorphism τ to the square that involves λ, we find the following square:

$$\begin{array}{ccc} F(\mathbb{1}^{\mathscr{C}} \otimes Gx) & \xrightarrow{F(\lambda^{\mathscr{C}})} & FGx \\ {\scriptstyle F(\gamma_0)}\downarrow & & \uparrow{\scriptstyle FG(\lambda^{\mathscr{D}})} \\ F(G\mathbb{1}^{\mathscr{D}} \otimes Ga) & \xrightarrow{F(\gamma_2)} & FG(\mathbb{1}^{\mathscr{D}} \otimes a) \end{array}$$

It therefore suffices to show the following diagram commutes:

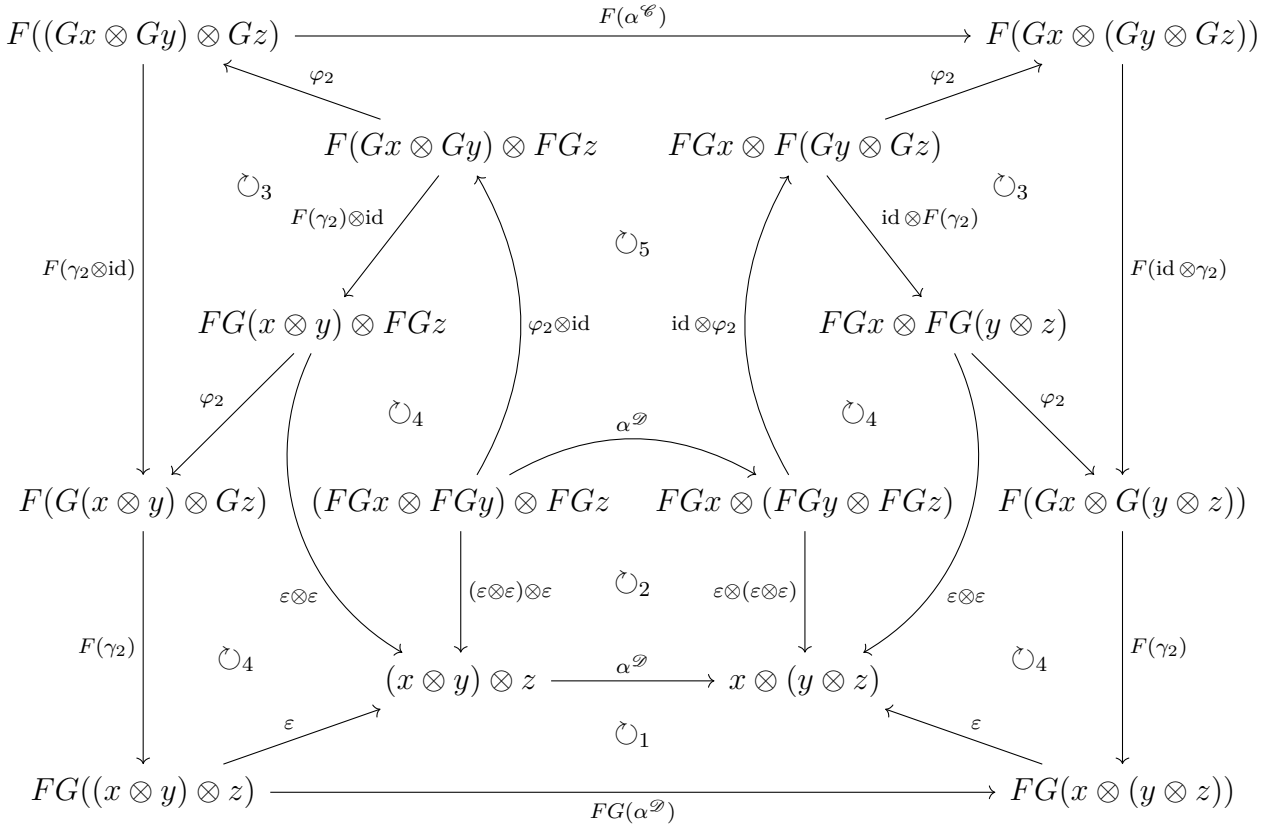


The commutativity of the various internal polygons holds as follows:

- The squares labeled $\circlearrowright_1$, $\circlearrowright_2$, and $\circlearrowright_3$ commute by the naturality of ε, $\lambda^{\mathscr{D}}$, and φ_2 respectively.
- The triangle labeled $\circlearrowright_4$ commutes by the properties of the tensor product.
- The triangle $\circlearrowright_5$ and square $\circlearrowright_6$ commute due to (2.1) and (2.2) respectively.
- The square labeled $\circlearrowright_7$ is precisely the corresponding square for φ_0 and hence commutes because F is a monoidal functor.

We therefore conclude that the outer square commutes for all $x \in \mathscr{D}$.

For the hexagon, we follow the same strategy. Applying τ yields the outer hexagon of the following diagram:



The commutativity of the various internal polygons holds as follows:

- The squares labeled $\circlearrowleft_1$, $\circlearrowleft_2$, and $\circlearrowleft_3$ commute by the naturality of ε, $\alpha^{\mathscr{D}}$, and φ_2 respectively.
- The squares labeled $\circlearrowleft_4$ all commute due to (2.2).
- The hexagon labeled $\circlearrowleft_5$ is precisely the corresponding hexagon for φ_2 and hence commutes because F is a monoidal functor.

We therefore conclude that the outer hexagon commutes for all $x, y, z \in \mathscr{D}$. As such, (G, γ_0, γ_2) is a monoidal functor.

It remains only to show that $FG \cong (\mathrm{id}, \mathrm{id}, \mathrm{id})_{\mathscr{D}}$ via ε and $GF \cong (\mathrm{id}, \mathrm{id}, \mathrm{id})_{\mathscr{C}}$ via η. These follow immediately from (2.1) and (2.2); for example, the first triangle of Definition 2.1.4 applied to FG is precisely (2.1). $\square$

Note that Proposition 2.1.6 holds only if we already have a monoidal functor: the existence of an equivalence of categories $F : \mathscr{C} \longrightarrow \mathscr{D}$ does not imply that F can be equipped with a monoidal structure.

In theoretical situations, we often assume a monoidal category to be strict thanks to the following theorem [23, Thm. XI.5.3].

Theorem 2.1.7. *Every monoidal category is monoidally equivalent to a strict monoidal category.*

Proof. Let $\mathscr{C}$ be a monoidal category. Define a new category, $\mathscr{C}^{\mathrm{st}}$ (the "strictification"), as follows. The objects of $\mathscr{C}^{\mathrm{st}}$ consist of all finite sequences of objects in $\mathscr{C}$, including the empty sequence, $\varnothing = [\,]$. For the morphisms, first define a map $F : \mathscr{C}^{\mathrm{st}} \to \mathscr{C}$ by

$$F(s) \coloneqq \begin{cases} \mathbb{1}, & \text{if } s = \varnothing, \\ a_1, & \text{if } s = [a_1], \\ (\cdots(a_1 \otimes a_2) \otimes a_3) \otimes \dots) \otimes a_n, & \text{if } s = [a_1, \dots, a_n]; \end{cases} \tag{2.3}$$

then set

$$\mathscr{C}^{\mathrm{st}}(s,t) \coloneqq \mathscr{C}(F(s), F(t)) \ .$$

$\mathscr{C}^{\mathrm{st}}$ is then a category with composition inherited from $\mathscr{C}$.

We may now define a monoidal structure on $\mathscr{C}^{\mathrm{st}}$. For objects $s, t \in \mathscr{C}^{\mathrm{st}}$, we define their product $s \odot t$ to be the concatenation of the sequences s and t. The associativity axiom of $\mathscr{C}$ then provides a unique legal isomorphism $\nu_{s,t} : F(s) \otimes F(t) \to F(s \odot t)$, as these differ only in the placement of parentheses. We may therefore define $\varphi \odot \psi : s \odot t \to s' \odot t'$, canonically, as the composition

$$F(s \odot t) \xrightarrow{\nu_{s,t}^{-1}} F(s) \otimes F(t) \xrightarrow{\varphi \otimes \psi} F(s') \otimes F(t') \xrightarrow{\nu_{s',t'}} F(s' \odot t') \tag{2.4}$$

for any $\varphi : s \to s'$ and $\psi : t \to t'$. Note that $\nu : F(\bullet) \otimes F(\bullet) \to F(\bullet \odot \bullet)$, consisting of the legal isomorphisms $\nu_{s,t}$ defined above, is a natural transformation. This follows from the fact that

$$\begin{array}{ccc} Fs \otimes Ft & \xrightarrow{\nu_{s,t}} & F(s \odot t) \\ & & \downarrow{\scriptstyle \nu_{s,t}^{-1}} \\ & & Fs \otimes Ft \\ \downarrow{\scriptstyle \varphi\otimes\psi} & & \downarrow{\scriptstyle \varphi\otimes\psi} \\ & & Fs' \otimes Ft' \\ & & \downarrow{\scriptstyle \nu_{s',t'}} \\ Fs' \otimes Ft' & \xrightarrow{\nu_{s',t'}} & F(s' \odot t') \end{array}$$

clearly commutes for all relevant morphisms. This makes $\odot$ a bifunctor: for any $s, t \in \mathscr{C}'$,

$$\begin{aligned} \mathrm{id}_s \odot \mathrm{id}_t &= \nu_{s,t} \circ (\mathrm{id}_{F(s)} \otimes \mathrm{id}_{F(t)}) \circ \nu_{s,t}^{-1} \\ &= \nu_{s,t} \circ \nu_{s,t}^{-1} \\ &= \mathrm{id}_{s \odot t} \end{aligned}$$

and for $\varphi_1 : s \to s'$, $\varphi_2 : s' \to s''$, $\psi_1 : t \to t'$, and $\psi_2 : t' \to t''$,

$$\begin{aligned} (\varphi_2 \circ \varphi_1) \odot (\psi_2 \circ \psi_1) &= \nu_{s'',t''} \circ ((\varphi_2 \circ \varphi_1) \otimes (\psi_2 \otimes \psi_1)) \circ \nu_{s,t}^{-1} \\ &= \nu_{s'',t''} \circ ((\varphi_2 \otimes \psi_2) \circ (\varphi_1 \otimes \psi_1)) \circ \nu_{s,t}^{-1} \\ &= \nu_{s'',t''} \circ (\varphi_2 \otimes \psi_2) \circ \nu_{s',t'}^{-1} \circ \nu_{s',t'} \circ (\varphi_1 \otimes \psi_1) \circ \nu_{s,t}^{-1} \\ &= (\varphi_2 \odot \psi_2) \circ (\varphi_1 \odot \psi_1) \ , \end{aligned}$$

where we use the fact that $\otimes$ is itself a bifunctor.

As concatenations, $s \odot \varnothing = \varnothing \odot s = s$ and $(s \odot t) \odot u = s \odot (t \odot u)$ for all sequences $s, t, u \in \mathscr{C}^{\mathrm{st}}$. Thus, we choose $\varnothing$ as the unit object and set $\alpha^{\mathscr{C}^{\mathrm{st}}}$, $\lambda^{\mathscr{C}^{\mathrm{st}}}$, and $\rho^{\mathscr{C}^{\mathrm{st}}}$ to be identities; the associativity axiom is then trivially satisfied. It then suffices to show

that the $\alpha^{\mathscr{C}^{\mathrm{st}}}$, $\lambda^{\mathscr{C}^{\mathrm{st}}}$, and $\rho^{\mathscr{C}^{\mathrm{st}}}$ thus defined are natural isomorphisms. For $\varphi : s \to s'$,

$$\begin{aligned}\varphi \odot \mathrm{id}_{\varnothing} &= \nu_{s',\varnothing} \circ (\varphi \otimes \mathrm{id}_{\mathbb{1}}) \circ \nu_{s,\varnothing}^{-1} \\ &= \nu_{s',\varnothing} \circ \varphi \circ \nu_{s,\varnothing}^{-1} \\ &= \varphi\end{aligned}$$

by the naturality of ν. Similarly, $\mathrm{id}_{\varnothing} \odot \varphi = \varphi$. Moreover, for $\varphi : s \to s'$, $\psi : t \to t'$, and $\mu : u \to u'$, the diagram

$$\begin{array}{ccccc}
F(s \odot t) \otimes Fu & \xleftarrow[\nu^{-1}]{} & F(s \odot t \odot u) & \xrightarrow[\nu^{-1}]{} & Fs \otimes F(t \odot u) \\
\downarrow{\scriptstyle \nu^{-1}} & & & & {\scriptstyle \nu^{-1}}\downarrow \\
(Fs \otimes Ft) \otimes Fu & & \xrightarrow{\quad\alpha^{\mathscr{C}}\quad} & & Fs \otimes (Ft \otimes Fu) \\
\downarrow{\scriptstyle (\varphi\otimes\psi)\otimes\mu} & & & & {\scriptstyle \varphi\otimes(\psi\otimes\mu)}\downarrow \\
(Fs' \otimes Ft') \otimes Fu' & & \xrightarrow{\quad\alpha^{\mathscr{C}}\quad} & & Fs' \otimes (Ft' \otimes Fu') \\
\downarrow{\scriptstyle \nu} & & & & {\scriptstyle \nu}\downarrow \\
F(s' \odot t') \otimes Fu' & \xrightarrow{\nu} & F(s' \odot t' \odot u') & \xleftarrow{\nu} & Fs' \otimes (Ft' \odot Fu')
\end{array}$$

commutes by the naturality of ν (for the top and bottom pentagons) and of $\alpha^{\mathscr{C}}$; the left path is $(\varphi \odot \psi) \odot \mu$ and the right is $\varphi \odot (\psi \odot \mu)$, so they must be equal.

This confirms that $(\odot, \varnothing, \mathrm{id}, \mathrm{id}, \mathrm{id})$ is a strict monoidal structure for $\mathscr{C}^{\mathrm{st}}$.

It remains to show that $\mathscr{C}^{\mathrm{st}}$ and $\mathscr{C}$ are monoidally equivalent. The map F defined in (2.3) may be extended to a functor $\mathscr{C}^{\mathrm{st}} \to \mathscr{C}$; since $\mathscr{C}^{\mathrm{st}}(s,t) = \mathscr{C}(F(s), F(t))$ for all $s, t \in \mathscr{C}^{\mathrm{st}}$, we simply define $F(\varphi) = \varphi$ for $\varphi \in \mathscr{C}^{\mathrm{st}}(s,t)$ and then the functorial identities are trivial.

As such, we claim that (F, id, ν) is a monoidal functor $\mathscr{C}^{\mathrm{st}} \to \mathscr{C}$; here we use the identity $F(\varnothing) \xrightarrow{\mathrm{id}} \mathbb{1}^{\mathscr{C}}$. In Definition 2.1.3, the diagram

$$\begin{array}{ccc}
\mathbb{1}^{\mathscr{C}} \otimes Fs & \xrightarrow{\lambda^{\mathscr{C}}_{Fs}} & Fs \\
\downarrow{\scriptstyle \mathrm{id}} & & {\scriptstyle \mathrm{id}}\uparrow \\
F\varnothing \otimes Fs & \xrightarrow{\nu_{\varnothing,s}} & F(\varnothing \odot s)
\end{array}$$

commutes for any $s \in \mathscr{C}^{\mathrm{st}}$ because $\lambda^{\mathscr{C}}_{Fs}$ is a legal isomorphism $\mathbb{1}^{\mathscr{C}} \otimes Fs \to Fs$, but $\nu_{\varnothing,s}$ is the unique such morphism, so $\lambda^{\mathscr{C}}_{Fs} = \nu_{\varnothing,s}$. The same argument holds for the diagram involving $\rho^{\mathscr{C}}_{Fs}$. Similarly,

$$\begin{array}{ccc}
(Fs \otimes Ft) \otimes Fu & \xrightarrow{\alpha^{\mathscr{C}}} & Fs \otimes (Ft \otimes Fu) \\
{\scriptstyle \nu_{s,t}}\searrow & & \swarrow{\scriptstyle \nu_{t,u}} \\
F(s \odot t) \otimes Fu & & Fs \otimes F(t \odot u) \\
{\scriptstyle \nu_{s\odot t,u}}\searrow & & \swarrow{\scriptstyle \nu_{s,t\odot u}} \\
F(s \odot t \odot u) & \xrightarrow{\mathrm{id}} & F(s \odot t \odot u)
\end{array}$$

commutes for any $s, t, u \in \mathscr{C}^{\mathrm{st}}$ because $\alpha^{\mathscr{C}}_{Fs,Ft,Fu}$ and $\nu^{-1}_{t,u} \circ \nu^{-1}_{s,t\odot u} \circ \nu_{s\odot t,u} \circ \nu_{s,t}$ are both legal isomorphisms $(Fs \otimes Ft) \otimes Fu \to Fs \otimes (Ft \otimes Fu)$ and hence equal. This confirms that (F, id, ν) is a monoidal functor.

In light of Proposition 2.1.6, it remains only to show that F is an equivalence of categories. It suffices to show that F is full, faithful, and essentially surjective on objects [27, IV.4, Theorem 1]. For any $s, t \in \mathscr{C}^{\mathrm{st}}$, we have $\mathscr{C}^{\mathrm{st}}(s,t) = \mathscr{C}(F(s), F(t))$ by the definition of $\mathscr{C}^{\mathrm{st}}$, so F is clearly full and faithful. Also, for any $a \in \mathscr{C}$, we have $F([a]) = a$, so F is surjective. Thus, (F, id, ν) is a monoidal equivalence $\mathscr{C}^{\mathrm{st}} \to \mathscr{C}$. □

As a result of this theorem, results for strict categories will usually generalize immediately to non-strict cases. Practical applications, however, often involve non-strict categories, and as their associativity morphisms are not trivial, explicit calculation of their data must take those morphisms into account.

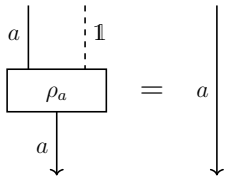
2.1.3. Graphical calculus

We often represent morphisms in a monoidal category visually by means of modified braid diagrams. This technique is called "graphical calculus." This works best for strict categories, so when we provide such diagrams, we will assume strictness; it is pos-

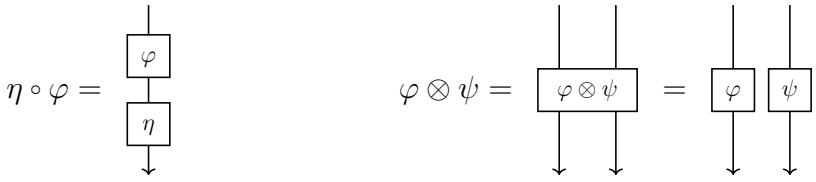
sible to extend the method to handle non-strict categories, but this sacrifices clarity.

Let $\mathscr{C}$ be a strict monoidal category. A morphism $\varphi : a \to b$ in $\mathscr{C}$ is represented by a single oriented strand with a coupon labeled appropriately; the coupon is omitted in the case of the identity:

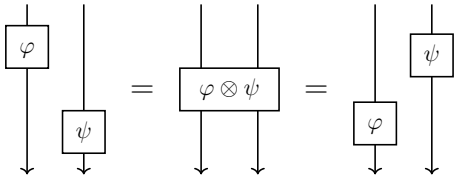
Diagrams in this dissertation are to be read from top to bottom; the arrow head may be omitted except when a strand points upwards. Also, since the category is strict, we have $a \otimes \mathbb{1} = \mathbb{1} \otimes a = a$ for all $a \in \mathscr{C}$, so strands corresponding to the unit object $\mathbb{1}$ are often not drawn. When they are useful for clarity, we will draw them as a dashed line. For example, we can represent the fact $\rho_a = \mathrm{id}_a$ with the following diagram:



Composition of morphisms is represented by stacking them vertically, while the tensor product is represented by placing the strands next to each other:



The property[2] $(\mathrm{id} \otimes \psi) \circ (\varphi \otimes \mathrm{id}) = \varphi \otimes \psi = (\varphi \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \psi)$ is thus represented as



.

Additional properties satisfied by $\mathscr{C}$, as introduced in the following sections, will add new topological properties to these diagrams.

[2]This follows from the fact that $\otimes$ is a bifunctor.

2.2. Duals and rigidity

Any vector space V over a field $\Bbbk$ has a corresponding dual vector space, namely $V^* := \mathrm{Hom}_{\Bbbk}(V, \Bbbk)$, and we may define an evaluation map $\mathrm{ev}_V : V^* \otimes V \to \Bbbk$ and a coevaluation map $\mathrm{coev}_V : \Bbbk \to V \otimes V^*$. These are given, respectively, by $\mathrm{ev}_V(\varphi \otimes v) = \varphi(v)$ and $\mathrm{coev}_V(k) = \sum_{i \in I} kv_i \otimes \varphi_i$, where $\{v_i\}_{i \in I}$ is any basis for V and $\{\varphi_i\}_{i \in I}$ the corresponding dual basis. This motivates the following definition on a monoidal category.

Definition 2.2.1. Let $\mathscr{C}$ be a monoidal category and $a \in \mathscr{C}$. A *left dual* $(a^*, \mathrm{ev}_a, \mathrm{coev}_a)$ for a consists of

- an object a^*,
- a morphism $\mathrm{ev}_a : a^* \otimes a \to \mathbb{1}$, called evaluation or annihilation, and
- a morphism $\mathrm{coev}_a : \mathbb{1} \to a \otimes a^*$, called coevaluation or creation,

satisfying the following *rigidity axioms*: the composition

$$a \xrightarrow{\lambda_a^{-1}} \mathbb{1} \otimes a \xrightarrow{\mathrm{coev}_a} (a \otimes a^*) \otimes a \xrightarrow{\alpha} a \otimes (a^* \otimes a) \xrightarrow{\mathrm{ev}_a} a \otimes \mathbb{1} \xrightarrow{\rho_a} a$$

must equal id_a and

$$a^* \xrightarrow{\rho_{a^*}^{-1}} a^* \otimes \mathbb{1} \xrightarrow{\mathrm{coev}_a} a^* \otimes (a \otimes a^*) \xrightarrow{\alpha^{-1}} (a^* \otimes a) \otimes a^* \xrightarrow{\mathrm{ev}_a} \mathbb{1} \otimes a^* \xrightarrow{\lambda_{a^*}} a^*$$

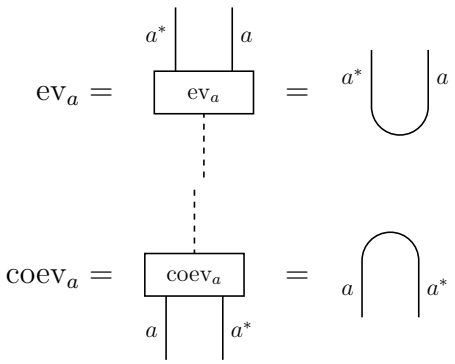
must equal id_{a^*}. In particular, neither ev_a nor coev_a can be zero morphisms.

For brevity, we sometimes denote $(a^*, \mathrm{ev}_a, \mathrm{coev}_a)$ simply by a^*.

A *right dual* for a, denoted ${}^*a$, is defined symmetrically.[3] Its morphisms are written $\mathrm{ev}'_a : a \otimes {}^*a \to \mathbb{1}$ and $\mathrm{coev}'_a : \mathbb{1} \to {}^*a \otimes a$. Results for left duals apply symmetrically to right duals, so we will mention only the former except when necessary.

[3] Some authors use the opposite convention, naming a^* a right dual and vice versa.

The evaluation and coevaluation morphisms for a left dual are represented graphically by cups and caps:



The rigidity axioms are then as follows:

If a has a left dual $(a^*, \mathrm{ev}_a, \mathrm{coev}_a)$, then the object a^* is unique up to a unique isomorphism consistent with ev_a and coev_a [13, Prop. 2.10.5] — in other words, duality is a property of $\mathscr{C}$ rather than additional data, but the precise object chosen as the dual is not canonical. Moreover, if $(a^*, \mathrm{ev}, \mathrm{coev})$ gives a left dual for a, then $(a, \mathrm{ev}, \mathrm{coev})$ gives a right dual for a^*; so, $a \cong {}^*(a^*) \cong ({}^*a)^*$ via unique isomorphisms.

The unit object $\mathbb{1}$ is always self-dual: $\mathbb{1} \otimes \mathbb{1} \cong \mathbb{1}$, so $(\mathbb{1}, \lambda_{\mathbb{1}}, \rho_{\mathbb{1}}^{-1})$ serves as a left dual.

If ev_a and coev_a are both isomorphisms, then a is called an *invertible object*.

Lemma 2.2.2 ([3, Lemma 2.1.6])**.** *Suppose a has a left dual. Then, for all $b, c \in \mathscr{C}$, there exist canonical isomorphisms*

$$\mathscr{C}(b \otimes a, c) \cong \mathscr{C}(b, c \otimes a^*)$$

$$\mathscr{C}(b, a \otimes c) \cong \mathscr{C}(a^* \otimes b, c) \ .$$

Proof. We may assume without loss of generality that $\mathscr{C}$ is strict. Define a homomorphism $f : \mathscr{C}(b \otimes a, c) \to \mathscr{C}(b, c \otimes a^*)$ by sending $\varphi : b \otimes a \to c$ to the composition

$$b \xrightarrow{b \otimes \mathrm{coev}_a} b \otimes a \otimes a^* \xrightarrow{\varphi \otimes a^*} c \otimes a^*$$

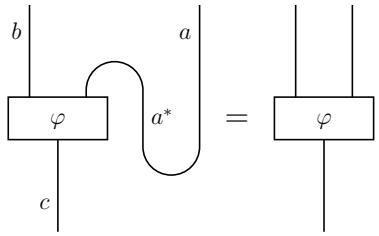
and similarly define $g : \mathscr{C}(b, c \otimes a^*) \to \mathscr{C}(b \otimes a, c)$ by sending $\eta : b \to c \otimes a^*$ to

$$b \otimes a \xrightarrow{\eta \otimes a} c \otimes a^* \otimes a \xrightarrow{c \otimes \mathrm{ev}_a} c \ .$$

Then $g \circ f(\varphi)$ is the composition

$$b \otimes a \xrightarrow{\mathrm{id}_b \otimes \mathrm{coev}_a \otimes \mathrm{id}_a} b \otimes a \otimes a^* \otimes a \xrightarrow{\varphi} c \otimes a^* \otimes a \xrightarrow{\mathrm{ev}_a} c$$

which is simply equal to φ by the rigidity axioms:



In the same way, $f \circ g(\eta) = \eta$, so we have an isomorphism. The proof of the second isomorphism is similar. □

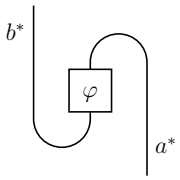
Definition 2.2.3. If both a and b have left duals, then applying both of the above isomorphisms to $\mathscr{C}(\mathbb{1}, b \otimes a^*)$ yields

$$\mathscr{C}(a, b) \cong \mathscr{C}(b^*, a^*) \ .$$

Under this isomorphism, $\varphi : a \to b$ corresponds to the composition

$$b^* \xrightarrow{\mathrm{coev}_a} b^* \otimes a \otimes a^* \xrightarrow{\varphi} b^* \otimes b \otimes a^* \xrightarrow{\mathrm{ev}_b} a^* \ ,$$

which we call the *left dual of the morphism* φ and denote $\varphi^* \in \mathscr{C}(b^*, a^*)$. Its graphical representation is

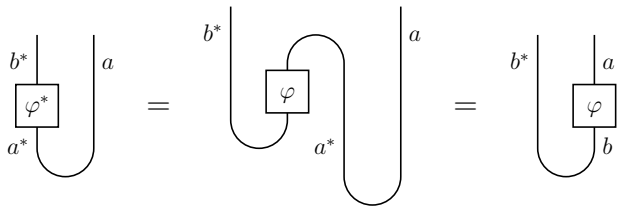


.

Lemma 2.2.4. *Suppose a, b have left duals and let $\varphi \in \mathscr{C}(a, b)$. Then:*

(2.5)

Proof. We may assume $\mathscr{C}$ is strict. Then



and similarly for the second equation. □

Now, if every object of $\mathscr{C}$ has a left dual, we say that $\mathscr{C}$ is *left rigid*. *Rigid* means simultaneously left and right rigid.

If $\mathscr{C}$ is left rigid, then we may define a functor $(\bullet)^* : \mathscr{C} \to \mathscr{C}^{\mathrm{op}}$ by fixing an arbitrary left dual $(a^*, \mathrm{ev}_a, \mathrm{coev}_a)$ for each $a \in \mathscr{C}$, sending each object to its fixed dual, and sending a morphism φ to φ^* as defined above. It may be shown that this functor is full and faithful, and that it is an equivalence of categories if and only if $\mathscr{C}$ is rigid [21, p. 71].

We may extend this to a monoidal functor by making use of the following:

Lemma 2.2.5. *If objects a and b have left duals, then $b^* \otimes a^*$ is a left dual for $a \otimes b$.*

Proof. We may assume that $\mathscr{C}$ is strict; then define

.

These are easily shown to satisfy the rigidity axioms. □

Remark 2.2.6. A problem arises in that there is often no way to choose left duals for all objects in $\mathscr{C}$ such that $(a \otimes b)^* = b^* \otimes a^*$ for all a, b. However, as they are both left duals, we do have a unique isomorphism $\psi_{a,b} : b^* \otimes a^* \to (a \otimes b)^*$. In fact, it may be shown that these isomorphisms form a natural isomorphism $\psi : (\bullet_2^* \otimes \bullet_1^*) \to (\bullet_1 \otimes \bullet_2)^*$ and that $((\bullet)^*, \psi, \mathrm{id})$ gives a monoidal functor $\mathscr{C} \to \overline{\mathscr{C}}^{\mathrm{op}}$, called the *dual functor*. Here $\overline{\mathscr{C}}$ is the monoidal category obtained from $\mathscr{C}$ by reversing the tensor product. Applying the dual functor twice gives a monoidal functor $((\bullet)^{**}, \tilde{\psi}, \mathrm{id})$ from $\mathscr{C}$ to itself, appropriately called the *double-dual functor*; the object $a^{**} = (a^*)^*$ is the "double dual" of a. Just as we did for monoidal structures, if $\psi_{a,b}$ is the identity for all a, b, so that indeed $(a \otimes b)^* = b^* \otimes a^*$, then we call $\mathscr{C}$ *strictly left rigid*. Moreover, it may be shown that every left-rigid category is equivalent to a strictly-left-rigid one, so in much the same way as before, we can often assume the rigidity is strict for theoretical purposes.

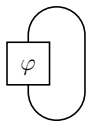
Rigidity allows us to define the following.

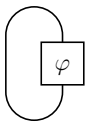
Definition 2.2.7. Let $\mathscr{C}$ be left rigid and $a \in \mathscr{C}$. For any morphism $\varphi : a \to a^{**}$, the composition

$$\mathbb{1} \xrightarrow{\mathrm{coev}_a} a \otimes a^* \xrightarrow{\varphi \otimes a^*} a^{**} \otimes a^* \xrightarrow{\mathrm{ev}_{a^*}} \mathbb{1}$$

is called the *left quantum trace* of φ and denoted $\mathrm{Tr}(\varphi) \in \mathscr{C}(\mathbb{1}, \mathbb{1})$. The *right quantum trace* Tr' is defined similarly when $\mathscr{C}$ is right rigid.

The graphical representations are as follows:

$\mathrm{Tr}(\varphi) =$ 

$\mathrm{Tr}'(\varphi) =$ 

Let us return to our example $\mathscr{G} = \mathrm{Vec}_G^{\omega}(\Bbbk)$ from Section 2.1. Consider an object $V = \bigoplus_{g \in G} V_g$. Each V_g is a vector space, so has a vector-space dual, $(V_g)^* = \mathrm{Hom}_{\Bbbk}(V_g, \Bbbk)$.

Define the (left) dual object of V, V^*, by $(V^*)_g \coloneqq (V_{g^{-1}})^*$; that is, the g grade of V^* consists of the vector-space dual of $V_{g^{-1}}$. This is clearly an object in $\mathscr{G}$. For each $g \in G$, let $\{v_i^g\}_{i\in I_g}$ be a basis for V_g and $\{\varphi_i^g\}_{i\in I_g}$ the corresponding dual basis of $(V_g)^* = (V^*)_{g^{-1}}$. Next, define $\mathrm{ev}_V : V^* \otimes V \to \Bbbk$, given on generating elementary tensors by

$$\varphi_i^h \otimes v_j^g \longmapsto \delta_{g,h}\varphi_i^g(v_j^g) = \delta_{g,h}\delta_{i,j} \ .$$

Notice that this always lies in the trivial grade, as v_j^g lies in grade g and φ_i^g in grade g^{-1}. Finally, define $\mathrm{coev}_V : \Bbbk \to V \otimes V^*$, given by

$$1 \longmapsto \sum_{g\in G}\sum_{i\in I_g} \omega^{-1}_{g,g^{-1},g} \cdot v_i^g \otimes \varphi_i^g \ .$$

To show that this gives a left dual of V, let $a = \sum_{g\in G}\sum_{i\in I_g} a_i^g v_i^g \in V$ (with $a_i^g \in \Bbbk$). Then the first rigidity axiom is satisfied as follows:

$$\begin{aligned}
a &= \sum_{g\in G}\sum_{i\in I_g} a_i^g v_i^g \\
&\xmapsto{\lambda_V^{-1}} \sum_{g\in G}\sum_{i\in I_g} a_i^g (1 \otimes v_i^g) \\
&\xmapsto{\mathrm{coev}_V} \sum_{g,h\in G}\sum_{i\in I_g}\sum_{j\in I_h} \omega^{-1}_{g,g^{-1},g} \cdot a_i^g ((v_j^h \otimes \varphi_j^h) \otimes v_i^g) \\
&\xmapsto{\alpha} \sum_{g,h\in G}\sum_{i\in I_g}\sum_{j\in I_h} \omega_{h,h^{-1},g} \cdot \omega^{-1}_{g,g^{-1},g} \cdot a_i^g (v_j^h \otimes (\varphi_j^h \otimes v_i^g)) \\
&\xmapsto{\mathrm{ev}_V} \sum_{g,h\in G}\sum_{i\in I_g}\sum_{j\in I_h} \delta_{g,h}\delta_{i,j} \cdot \omega_{h,h^{-1},g} \cdot \omega^{-1}_{g,g^{-1},g} \cdot a_i^g (v_j^h \otimes 1) \\
&\xmapsto{\rho_V} \sum_{g,h\in G}\sum_{i\in I_g}\sum_{j\in I_h} \delta_{g,h}\delta_{i,j} \cdot \omega_{h,h^{-1},g} \cdot \omega^{-1}_{g,g^{-1},g} \cdot a_i^g v_j^h \\
&= \sum_{g\in G}\sum_{i\in I_g} a_i^g v_i^g \\
&= a \ .
\end{aligned}$$

The second axiom is similar, and uses the fact that $\omega^{-1}_{g,g^{-1},g} = \omega_{g^{-1},g,g^{-1}}$ because ω is normalized. In fact, a symmetrical construction shows that V^* is also a right dual for V.

2.3. Fusion

Definition 2.3.1. Let $\mathscr{C}$ be a strictly-monoidal, left-rigid, semisimple, abelian, $\Bbbk$-linear category such that $\mathscr{C}(x, y)$ is a finite-dimensional $\Bbbk$-vector space for all $x, y \in \mathscr{C}$ and the bifunctor $\otimes$ is $\Bbbk$-bilinear on morphisms. Denote by $\mathrm{Irr}(\mathscr{C})$ a set of representatives for the isomorphism classes of simple objects in $\mathscr{C}$. Then $\mathscr{C}$ is called a *fusion* category if the following hold:

- $|\mathrm{Irr}(\mathscr{C})|$ is finite.
- $\mathbb{1} \in \mathrm{Irr}(\mathscr{C})$ (and is thus a simple object).
- For all $a, b \in \mathrm{Irr}(\mathscr{C})$, we have $\mathscr{C}(a, b) \cong \delta_{a,b} \cdot \Bbbk$. Note that this implies that each morphism in $\mathscr{C}(a, a)$ has the form $k \cdot \mathrm{id}_a$ for some $k \in \Bbbk$.

We then call $r_{\mathscr{C}} \coloneqq |\mathrm{Irr}(\mathscr{C})|$ the *rank* of $\mathscr{C}$.

If all of the above hold except that $\mathbb{1}$ is not simple, the result is called a *multi-fusion* category; for this, see [13, 14]. Fusion categories may be defined over any field, but for simplicity, we will assume all fields have characteristic zero.

Semisimplicity, together with the finite-dimensionality of the morphism spaces, then implies that any object x in a fusion category $\mathscr{C}$ may be written as a (finite) direct sum of simple objects:

$$x \cong \bigoplus_{a \in \mathrm{Irr}(\mathscr{C})} X_a \cdot a$$

for non-negative integers X_a. Since $\mathscr{C}(x, a)$ is a $\Bbbk$-vector space and a is simple, we may use Schur's Lemma to find $X_a = \dim_{\Bbbk}(\mathscr{C}(x, a))$, and moreover, comparing the decompositions gives $\dim_{\Bbbk}(\mathscr{C}(x, y)) = \dim_{\Bbbk}(\mathscr{C}(y, x))$ for all $x, y \in \mathscr{C}$.

As a particular case, consider any $a, b \in \mathrm{Irr}(\mathscr{C})$; then we have

$$a \otimes b \cong \bigoplus_{c \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^c \cdot c$$

where each $N_{a,b}^c = \dim_{\Bbbk}(\mathscr{C}(a \otimes b, c))$ is a non-negative integer. We call $\{N_{a,b}^c\}_{a,b,c \in \mathrm{Irr}(\mathscr{C})}$ the *fusion coefficients* of $\mathscr{C}$, as they characterize the "fusion" structure—that is, the action of the tensor product of $\mathscr{C}$. This fusion structure is recorded in the Grothendieck ring $K_0(\mathscr{C})$, the free abelian group generated by $\mathrm{Irr}(\mathscr{C})$ equipped with the multiplication rule $a \cdot b = \sum_c N_{a,b}^c c$. We often consider the "Grothendieck algebra" $K_{\mathbb{F}}(\mathscr{C}) \coloneqq K_0(\mathscr{C}) \otimes_{\mathbb{Z}} \mathbb{F}$ for $\mathbb{F}$ a field, especially when $\mathbb{F} = \Bbbk$.

Definitions given for fusion categories vary. For example, many authors define fusion categories to be rigid (i.e. from both sides), but we require only left rigidity; this is due to the following lemma.

Lemma 2.3.2. *Let $\mathscr{C}$ be a fusion category. Then $\mathscr{C}$ is also right rigid. For each $a \in \mathscr{C}$, we have ${}^*a \cong a^*$ and $a \cong a^{**}$.*

Proof. Let $a \in \mathrm{Irr}(\mathscr{C})$; by semisimplicity, the results may be extended linearly to all objects. First, we have an isomorphism $\mathscr{C}(a, a) \to \mathscr{C}(a^*, a^*)$ given by taking the left dual (Definition 2.2.3); thus $\dim_{\Bbbk}(\mathscr{C}(a^*, a^*)) = \dim_{\Bbbk}(\mathscr{C}(a, a)) = 1$. We conclude that a^* is simple, and hence also a^{**}.

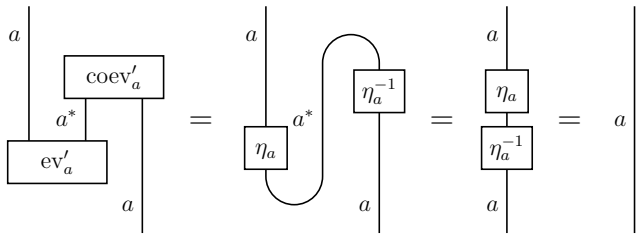
Thus, $\mathscr{C}(a, a^{**})$ is non-zero if and only if $a \cong a^{**}$. However, by Lemma 2.2.2, we have $\mathscr{C}(a, a^{**}) \cong \mathscr{C}(a \otimes a^*, \mathbb{1})$, and by semisimplicity, $\dim(\mathscr{C}(a \otimes a^*, \mathbb{1})) = \dim(\mathscr{C}(\mathbb{1}, a \otimes a^*))$. The latter space is certainly non-zero, as it contains coev_a. Hence $a \cong a^{**}$.

Choose an arbitrary isomorphism $\eta_a : a \to a^{**}$. Then a^*, along with the morphisms

$$\mathrm{ev}'_a := \mathrm{ev}_{a^*} \circ (\eta_a \otimes \mathrm{id}_{a^*}) : a \otimes a^* \to \mathbb{1}$$

$$\mathrm{coev}'_a := (\mathrm{id}_{a^*} \otimes \eta_a^{-1}) \circ \mathrm{coev}_{a^*} : \mathbb{1} \to a^* \otimes a$$

gives a right dual for a. That ev'_a and coev'_a satisfy the rigidity axioms follows from the fact that ev_a and coev_a do, and is easiest to see graphically:



The other axiom is similar. Hence we have a right dual; as a result, if ${}^*a$ is any right dual for a, we have ${}^*a \cong a^*$ [13, Prop. 2.10.5]. □

We therefore call a^* simply the dual of a in this case. When $a \in \mathrm{Irr}(\mathscr{C})$, we assert $a^* \in \mathrm{Irr}(\mathscr{C})$ as well. Note that, though we can always choose a family of isomorphisms $\{\eta_a : a \to a^{**}\}_{a \in \mathscr{C}}$, there is generally no way to do so canonically [3, Rmk. 2.4.2].

Now let $a, b, c \in \mathrm{Irr}(\mathscr{C})$. We may use the fact that $N_{a,b}^c = \dim(\mathscr{C}(a \otimes b, c)) = \dim(\mathscr{C}(c, a \otimes b))$ to relate the corresponding fusion coefficients. Lemma 2.2.2 gives

$$\mathscr{C}(a \otimes b, c) \cong \mathscr{C}(a, c \otimes b^*) \cong \mathscr{C}(c^* \otimes a, b^*) \qquad \text{and} \qquad \mathscr{C}(c, a \otimes b) \cong \mathscr{C}(a^* \otimes c, b)$$

so we have $N_{a,b}^c = N_{c^*,a}^{b^*} = N_{a^*,c}^b$. Similarly, $\mathbb{1} \otimes a \cong a \otimes \mathbb{1} \cong a$, so $N_{\mathbb{1},a}^b = N_{a,\mathbb{1}}^b = \delta_{a,b}$. Combining these results yields a number of identities:

$$N_{a,b}^c = N_{c^*,a}^{b^*} = N_{b,c^*}^{a^*} = N_{a^*,c}^b = N_{b^*,a^*}^{c^*} = N_{c,b^*}^a$$

$$N_{\mathbb{1},a}^b = N_{a,\mathbb{1}}^b = \delta_{a,b}$$

$$N_{a,b}^{\mathbb{1}} = N_{b,a}^{\mathbb{1}} = \delta_{b,a^*} \ .$$

Definition 2.3.3. For each $a \in \mathrm{Irr}(\mathscr{C})$, consider the *fusion matrix* N_a, defined by $[N_a]_{b,c} := N_{a,b}^c$ for $b, c \in \mathrm{Irr}(\mathscr{C})$. This (real) matrix has non-negative integer entries, so by the Frobenius–Perron theorem [13, Thm. 3.2.1], it has a real, non-negative eigenvalue with magnitude greater than or equal to that of any other. That eigenvalue is called the *Frobenius–Perron dimension* of a and denoted $\mathrm{FPdim}(a)$. The function $\mathrm{FPdim} : a \mapsto \mathrm{FPdim}(a)$ is a character of the Grothendieck ring $K_0(\mathscr{C})$, and the only one with all non-negative values [13, Prop. 3.3.6]. In fact, for each $a \in \mathrm{Irr}(\mathscr{C})$, $\mathrm{FPdim}(a)$ is an algebraic integer and $\mathrm{FPdim}(a) \geq 1$ [13, Prop. 3.3.4].

Remark 2.3.4. As $N_{a,b}^c = N_{a^*,c}^b$, we have $N_a = (N_{a^*})^{\mathrm{T}}$; hence N_a and N_{a^*} have the same spectrum and $\mathrm{FPdim}(a) = \mathrm{FPdim}(a^*)$. In the same way, $N_{\mathbb{1}} = \mathrm{id}$, so $\mathrm{FPdim}(\mathbb{1}) = 1$.

Definition 2.3.5 ([30, Prop. 2.4])**.** Consider again an arbitrary isomorphism $\eta_a : a \to a^{**}$. Define the *squared norm* of a as the product

$$|a|^2 := \mathrm{Tr}(\eta_a) \cdot \mathrm{Tr}\left((\eta_a^{-1})^*\right) . \tag{2.6}$$

We observe that this definition does not depend upon our choice of isomorphism: since $\mathscr{C}(a, a^{**}) \cong \Bbbk$, any isomorphism therein is a scalar multiple of η_a, and the trace is $\Bbbk$-linear. The quantum trace is a morphism in $\mathscr{C}(\mathbb{1}, \mathbb{1}) \cong \Bbbk$, so it has the form $k\,\mathrm{id}_{\mathbb{1}}$ for some $k \in \Bbbk$; we therefore view it, and hence the squared norm, simply as an element of $\Bbbk$.

As an aside, the name "squared norm" raises the question of what "norm" it might be the square of; this will be addressed in the next section by Lemma 2.4.6.

Lemma 2.3.6. *For any $a \in \mathrm{Irr}(\mathscr{C})$, we have $|a|^2 \neq 0$.*

Proof. Consider $\mathrm{Tr}(\eta_a)$, which is the composition

$$\mathbb{1} \xrightarrow{\mathrm{coev}_a} a \otimes a^* \xrightarrow{\eta_a \otimes a^*} a^{**} \otimes a^* \xrightarrow{\mathrm{ev}_{a^*}} \mathbb{1} .$$

Denote $\mu \coloneqq \mathrm{ev} \circ (\eta_a \otimes \mathrm{id}_{a^*})$ and suppose $\mathrm{Tr}(\eta_a) = 0$. Then $\mathrm{Im}(\mathrm{coev}_a) \hookrightarrow \ker(\mu)$, and since coev_a is injective and non-zero, $\mathrm{Im}(\mathrm{coev}_a) \cong \mathbb{1}$. On the other hand, ev_{a^*} is non-zero and η_a is an isomorphism, so $\mathrm{Im}(\mu) \neq 0$. As $\mathbb{1}$ is simple, this means $\mathrm{Im}(\mu) \cong \mathbb{1}$ as well. We have $a \otimes a^* \cong \ker(\mu) \oplus \mathrm{Im}(\mu)$, so $\dim(\mathscr{C}(\mathbb{1}, a \otimes a^*)) \geq 2$. However, applying Lemma 2.2.2, $\dim(\mathscr{C}(\mathbb{1}, a \otimes a^*)) = \dim(\mathscr{C}(a, a)) = 1$. By contradiction, $\mathrm{Tr}(\eta_a)$ must be non-zero. A similar argument works for $\mathrm{Tr}((\eta_a^{-1})^*)$, and the statement follows. □

Definition 2.3.7. The *global Frobenius–Perron dimension* of $\mathscr{C}$ is defined as

$$\mathrm{FPdim}(\mathscr{C}) \coloneqq \sum_{a \in \mathrm{Irr}(\mathscr{C})} \mathrm{FPdim}(a)^2 \ ,$$

while the *global (categorical) dimension* is

$$\dim(\mathscr{C}) \coloneqq \sum_{a \in \mathrm{Irr}(\mathscr{C})} |a|^2 \ .$$

Remark 2.3.8. When $\Bbbk = \mathbb{C}$, these two concepts of global dimension are interrelated. It may be shown that, for all $a \in \mathscr{C}$, the squared norm $|a|^2 \in \mathbb{C}$ is real and totally positive [13, Prop. 7.21.14], and for all $a \in \mathrm{Irr}(\mathscr{C})$, we have [14, Prop. 8.21]

$$0 < |a|^2 \leq \mathrm{FPdim}(a)^2 \ .$$

Thus, $\dim(\mathscr{C}) \leq \mathrm{FPdim}(\mathscr{C})$. If $\dim(\mathscr{C}) = \mathrm{FPdim}(\mathscr{C})$ then $\mathscr{C}$ is called *pseudounitary*; this is equivalent to having $|a|^2 = \mathrm{FPdim}(a)^2$ for all $a \in \mathrm{Irr}(\mathscr{C})$.

Remark 2.3.9. If $\mathrm{FPdim}(\mathscr{C}) \in \mathbb{Z}$, then $\mathscr{C}$ is called *weakly-integral*; if $\mathrm{FPdim}(a) \in \mathbb{Z}$ for all $a \in \mathrm{Irr}(\mathscr{C})$, it is called *integral*. A weakly-integral category defined over $\mathbb{C}$ is automatically pseudounitary [13, Prop. 9.6.5].

In $\mathscr{G} = \mathrm{Vec}_G^\omega(\Bbbk)$, any object V is isomorphic to

$$\bigoplus_{g \in G} \dim_\Bbbk(V_g) \cdot e_g \ ,$$

where e_g is defined by $(e_g)_g = \Bbbk$ and $(e_g)_h = 0$ for $h \neq g$ (so in particular $e_{1_G} = \mathbb{1}$). As a 1-dimensional vector space, each e_g is simple; hence, $\mathscr{G}$ is semisimple with $\mathrm{Irr}(\mathscr{G}) = \{e_g\}_{g \in G}$. The other fusion properties follow immediately from the definition, so $\mathscr{G}$ is a fusion category. It is then straightforward to see that $(e_g)^* = e_{g^{-1}}$ and that

$$[N_{e_g}]_{e_h, e_k} = N_{e_g, e_h}^{e_k} = \delta_{gh,k}$$

describes the fusion structure.

2.4. Pivotal and spherical structures

Consider again the double-dual functor $(\bullet)^{**}$ from Remark 2.2.6. As noted in the previous section, $a \cong a^{**}$ for any a in a fusion category, but there is generally no consistent way to choose a complete set of isomorphisms [3, Rmk. 2.4.2]. There are also categories where a and a^{**} fail to be isomorphic, such as the category of finite-dimensional comodules over the quantum group $U_q(\mathfrak{sl}_2)$ [13, §5.6 and Ex. 7.19.5]. When a consistent set of isomorphisms does exist, it is called a pivotal structure:

Definition 2.4.1. Let $\mathscr{C}$ be a left-rigid monoidal category. A *pivotal structure* on $\mathscr{C}$ is an isomorphism of monoidal functors

$$\xi : \mathrm{id}_{\mathscr{C}} \longrightarrow (\bullet)^{**}$$

with components $\xi_a : a \to a^{**}$ for $a \in \mathscr{C}$. A category equipped with a designated pivotal structure is called *pivotal*.

We only need to assume left rigidity here: the same argument as in Lemma 2.3.2 (with ξ_a itself as the relevant isomorphism) shows that any pivotal category is rigid.

Definition 2.4.2. In the presence of a pivotal structure, we may extend our definition of

the quantum trace (Definition 2.2.7): for any morphism $\varphi : a \to a$, define

$$\mathrm{Tr}_\xi(\varphi) \coloneqq \mathrm{Tr}(\xi_a \circ \varphi)$$

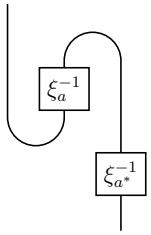
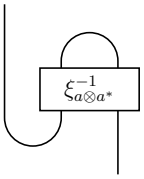
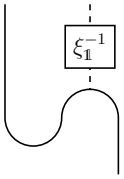
$$\mathrm{Tr}'_\xi(\varphi) \coloneqq \mathrm{Tr}'(\varphi \circ \xi_a^{-1}) \ .$$

In particular, we call $\dim_\xi(a) \coloneqq \mathrm{Tr}_\xi(\mathrm{id}_a) = \mathrm{Tr}(\xi_a)$ and $\dim'_\xi(a) \coloneqq \mathrm{Tr}'_\xi(\mathrm{id}_a) = \mathrm{Tr}'(\xi_a^{-1})$ the left and right *quantum dimensions* of the object a.

When the pivotal structure is unambiguous, we will abuse the notation slightly and omit the subscript ξ.

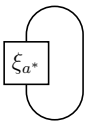
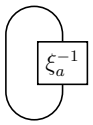
Lemma 2.4.3. *Let ξ be a pivotal structure on $\mathscr{C}$. For any $a \in \mathscr{C}$, we have $(\xi_a^{-1})^* = \xi_{a^*}$, and hence $\dim_\xi(a^*) = \dim'_\xi(a)$.*

Proof. We may assume $\mathscr{C}$ is strict and strictly rigid, and hence use graphical calculus:

$(\xi_{a^*})^{-1} \circ (\xi_a^{-1})^* =$  $=$  $=$  $= \mathrm{id}_a \ ,$

where the third equality is due to the naturality of ξ, and $\xi_{\mathbb{1}} = \mathrm{id}_{\mathbb{1}}$ by the first diagram of Definition 2.1.4. A similar process shows that $(\xi_a^{-1})^* \circ (\xi_{a^*})^{-1} = \mathrm{id}_{a^{***}}$, confirming the first statement.

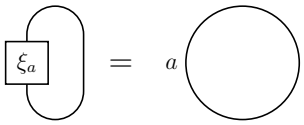
Applying this, along with Lemma 2.2.4, to $\dim_\xi(a^*)$ gives

$\dim_\xi(a^*) =$  $=$  $= \dim'_\xi(a) \ ,$

which confirms the latter statement. □

Once more, there is a concept of strictness to consider; if $(\bullet)^{**} = \mathrm{id}_{\mathscr{C}}$ as monoidal functors and ξ is the identity (so $a = a^{**}$ and $\xi_a = \mathrm{id}_a$ for every $a \in \mathscr{C}$), then we say $\mathscr{C}$

is *strictly pivotal*, and as usual we may assume this for most theoretical purposes.[4] As a result, ξ is often omitted from graphical diagrams. For instance:

$\dim_\xi(a) =$  $=$

Definition 2.4.4. Suppose ξ is a pivotal structure on $\mathscr{C}$. If $\mathrm{Tr}_\xi(\varphi) = \mathrm{Tr}'_\xi(\varphi)$ for all endomorphisms φ of $\mathscr{C}$, we call ξ a *spherical structure* and $\mathscr{C}$ *spherical*.

Lemma 2.4.3 shows that $\dim(a^*) = \dim(a)$ for any a in a spherical category.

Let us now consider the relationship between fusion and pivotal structures.

Remark 2.4.5. If $\mathscr{C}$ is fusion and has a pivotal structure ξ, then $\dim_\xi : a \mapsto \dim_\xi(a)$ (and similarly $\dim'_\xi$) is a character of the Grothendieck group $K_0(\mathscr{C})$ [13, Prop. 4.7.12]. This means $\dim(\mathbb{1}) = 1$ and $\dim(a \otimes b) = \dim(a) \cdot \dim(b)$ for all $a, b \in \mathrm{Irr}(\mathscr{C})$. Moreover, $\dim_\xi(a)$ and $\dim'_\xi(a)$ are non-zero for any simple object a [13, Prop. 4.8.4].

Lemma 2.4.6. *Suppose $\mathscr{C}$ is fusion and spherical. Then $(\dim_\xi(a))^2 = |a|^2$ for all $a \in \mathscr{C}$. In particular, $\dim_\xi(a) \neq 0$.*

Proof. We may take $\xi_a : a \to a^{**}$ as the isomorphism in (2.6). Then

$$|a|^2 = \mathrm{Tr}(\xi_a) \cdot \mathrm{Tr}(\xi_{a^*}) = \dim_\xi(a) \cdot \dim_\xi(a^*) = \dim_\xi(a) \cdot \dim'_\xi(a) = (\dim_\xi(a))^2$$

by Lemma 2.4.3 and sphericality. The last statement follows from Lemma 2.3.6. □

Note that $|a|^2$ does not depend on ξ: the squared norm exists independently of the choice (or existence) of pivotal structure.

Corollary 2.4.7. *If $\mathscr{C}$ is fusion and spherical over $\mathbb{C}$, then $\dim_\xi(a) \in \mathbb{R} \smallsetminus 0$ for $a \in \mathrm{Irr}(\mathscr{C})$.*

Proof. This follows from the fact that $|a|^2$ is real and totally positive (Remark 2.3.8). □

[4] Every pivotal category is equivalent, as a pivotal category, to a strictly-pivotal one [34, Thm. 2.2].

Corollary 2.4.8. *If $\mathscr{C}$ is spherical and pseudounitary,* $\dim_\xi(a) = \pm \operatorname{FPdim}(a)$ *for all* $a \in \operatorname{Irr}(\mathscr{C})$.

It has been conjectured that every fusion category admits a pivotal structure, and indeed a spherical one, but while this holds for every currently known example, the general case remains unproven [13, Question 4.8.3]. However, it is known to hold in the pseudounitary case:

Proposition 2.4.9 ([13, Prop. 9.5.1])**.** *If $\mathscr{C}$ is a pseudounitary fusion category, then there is a unique spherical structure ξ^+ on $\mathscr{C}$ satisfying* $\dim_{\xi^+}(a) = \operatorname{FPdim}(a)$ *for all* $a \in \operatorname{Irr}(\mathscr{C})$. *In particular, all such dimensions are positive and real.*

Importantly, ξ^+ is unique in satisfying $\dim_{\xi^+}(a) = \operatorname{FPdim}(a)$ for all $a \in \operatorname{Irr}(\mathscr{C})$, but there may be other pivotal (and possibly spherical) structures on $\mathscr{C}$ not satisfying that condition. For example, $\mathscr{G} = \operatorname{Vec}_G^\omega(\Bbbk)$ has a distinct pivotal structure ξ^χ arising from each linear character $\chi \in \hat{G}$, with the component

$$\xi^\chi_{e_g} : e_g \to (e_g)^{**} = e_g$$

given by multiplication by $\chi(g)$. Said structure is spherical if and only if $\chi^2 = 1$, and ξ^+ corresponds to the trivial character.

2.5. Braids and ribbons

2.5.1. Braidings

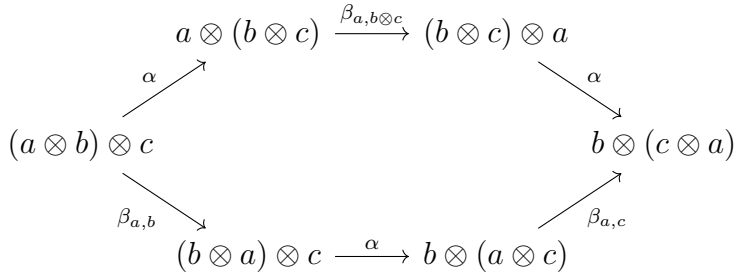
Definition 2.5.1. Let $\mathscr{C}$ be a monoidal category. A choice of *braiding* on $\mathscr{C}$ is a natural isomorphism

$$\beta : (\bullet_1 \otimes \bullet_2) \longrightarrow (\bullet_2 \otimes \bullet_1) \ ;$$

that is,

$$\beta : \otimes \longrightarrow \otimes \circ \tau$$

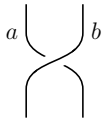
where τ simply swaps the coordinates of $\mathscr{C} \times \mathscr{C}$. The components of β are $\beta_{a,b} : a \otimes b \to b \otimes a$ for $a, b \in \mathscr{C}$. Further, the following diagram, as well as the same diagram involving β^{-1} instead of β, must commute (these diagrams are called the *hexagon axioms*):

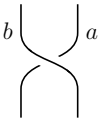


A category equipped with a designated braiding is called *braided*.

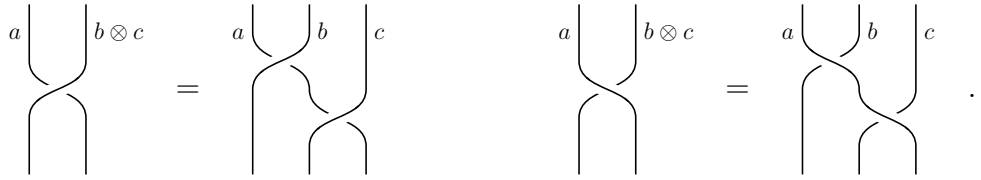
It is immediate from the definition that, if β is a braiding for $\mathscr{C}$, then so is β^{-1}.

A braiding is represented graphically by crossing the strands, hence the name:

$\beta_{a,b} =$ 

$\beta^{-1}_{a,b} =$ 

The hexagon axioms are then represented by

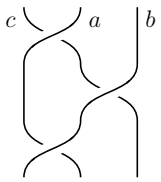


.

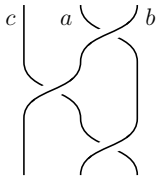
Since all the morphisms involved in the hexagon axioms are isomorphisms, we may take inverses of both sides to show that they imply the "other" two hexagon axioms:

As was the case for the triangle and pentagon axioms, the hexagon axioms imply a more general axiom. Consider the following example. Choose a set (rather than a sequence) of objects in $\mathscr{C}$, say $\{a, b, c\}$. Let x and y be two objects obtained by tensoring these objects, along with $\mathbb{1}$, in any order — say, $x = ((c \otimes a) \otimes \mathbb{1}) \otimes b$ and $y = (\mathbb{1} \otimes b) \otimes (a \otimes c)$. A *braided legal isomorphism* from x to y is the composition of tensor products of α, λ, ρ, β, and their inverses, along with the identity. Such an isomorphism has an obvious image as an actual braid, specifically its graphical representation. For instance, here are the images of two such isomorphisms:

$$\lambda_b^{-1} \circ \beta_{a\otimes c,b} \circ \rho_{a\otimes c} \circ \beta_{c,a} \longmapsto$$



$$\alpha^{-1}_{\mathbb{1},b,c\otimes a} \circ \beta_{c\otimes a,b} \circ \alpha_{\mathbb{1},c\otimes a,b} \circ \beta_{c\otimes a,\mathbb{1}} \longmapsto$$



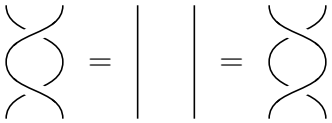
The images of these two isomorphisms are isotopic as braids, so the axiom states that they should be identical as morphisms. The general statement is as follows:

Braid axiom. *Consider any set of objects $\{a_1, a_2, \cdots, a_m\}$ with $a_i \in \mathscr{C}$. Suppose x and y are two objects obtained by tensoring the sequence in any order and inserting parentheses and $\mathbb{1}$s arbitrarily. Then two braided legal isomorphisms from x to y are identical if and only if their diagrams are ambient isotopic as braids with labeled strands.*

Theorem 2.5.2 (Joyal-Street coherence theorem [21, Cor. 2.6])**.** *The hexagon axioms of Definition 2.5.1 imply that $\mathscr{C}$ satisfies the braid axiom when equipped with the braiding β.*

Braidings satisfy a number of topological properties when interpreted graphically, including in particular Reidemeister moves II and III. The obvious identity $\beta_{a,b}^{-1} \circ \beta_{a,b} =$

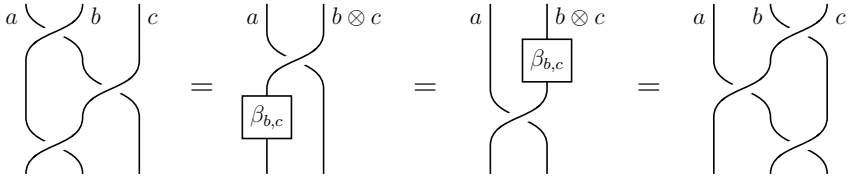
$\mathrm{id}_{a\otimes b} = \beta_{b,a} \circ \beta_{b,a}^{-1}$ translates to Reidemeister IIa and IIb:



(2.7)

Further, the naturality of β translates to

and the same with reversed braidings; combining this with the hexagon axioms yields



(2.8)

That is,

$$\beta_{b,c} \circ \beta_{a,c} \circ \beta_{a,b} = \beta_{a,b} \circ \beta_{a,c} \circ \beta_{b,c} \ .$$

This, along with the corresponding equation involving β^{-1}, corresponds to Reidemeister IIIa and IIIb. This identity is also known as the Yang–Baxter equation; aside from the obvious connection to knots and braids, it occurs in the context of quantum physics and statistical mechanics.[5]

It is possible to create a braided category out of any monoidal category (including one which is already braided), as follows.

Definition 2.5.3 ([31, Def. 3.1])**.** Let $\mathscr{C}$ be a strict monoidal category. A *half-braiding* ψ for an object $a \in \mathscr{C}$ is a natural isomorphism $a \otimes \bullet \to \bullet \otimes a$ (with components $\psi_b : a \otimes b \to b \otimes a$ for each $b \in \mathscr{C}$) satisfying the braid relation

$$\psi_{b\otimes c} = (\mathrm{id}_b \otimes \psi_c) \circ (\psi_b \otimes \mathrm{id}_c) \ .$$

[5]See, for example, [19].

The *Drinfeld center*[6] of $\mathscr{C}$, denoted $Z_1(\mathscr{C})$, is the monoidal category in which

- the objects consist of all pairs (a, ψ) where $a \in \mathscr{C}$ and ψ is a half-braiding for a,
- the morphisms $(a, \psi) \to (b, \eta)$ consist of all $\varphi \in \mathscr{C}(a, b)$ that are consistent with ψ and η in the sense that $(\mathrm{id}_c \otimes \varphi) \circ \psi_c = \eta_c \circ (\varphi \otimes \mathrm{id}_c)$ for all $c \in \mathscr{C}$, and
- the tensor product $\odot$ is given by $(a, \psi) \odot (b, \eta) \coloneqq (a \otimes b, (\psi \otimes \mathrm{id}_b) \circ (\mathrm{id}_a \otimes \eta))$.

Then $Z_1(\mathscr{C})$ admits a braiding β^1 defined by $\beta^1_{(a,\psi),(b,\eta)} = \psi_b$. That β^1 satisfies the conditions of Definition 2.5.1 follows from the conditions on the half-braiding.

When $\mathscr{C}$ is not strict, the construction of $Z_1(\mathscr{C})$ merely requires inserting the obvious legal isomorphisms. If we have an actual braiding β for $\mathscr{C}$, then $\mathscr{C}$ embeds into $Z_1(\mathscr{C})$ as a braided subcategory via $a \mapsto (a, \beta_{a,\bullet})$. The notation $Z_1(\mathscr{C})$ for the Drinfeld center is to distinguish this construction from the Müger center $Z_2(\mathscr{C})$, which we will describe in Definition 2.6.2.

Returning to our example, the category $\mathscr{G} = \mathrm{Vec}^{\omega}_G(\Bbbk)$ admits a braiding only if G is abelian. In this case, braidings are in 1-to-1 correspondence with maps $\gamma : G \times G \to \Bbbk^\times$ satisfying

$$\omega(h,k,g) \cdot \gamma(g,hk) \cdot \omega(g,h,k) = \gamma(g,k) \cdot \omega(h,g,k) \cdot \gamma(g,h)$$

$$\omega^{-1}(k,g,h) \cdot \gamma(gh,k) \cdot \omega^{-1}(g,h,k) = \gamma(g,k) \cdot \omega^{-1}(g,k,h) \cdot \gamma(h,k)$$

for all $g, h, k \in G$; the pair (ω, γ) is called an *abelian 3-cocycle* of G on $\Bbbk$ [21, Prop. 3.1]. The corresponding braiding has $\beta^\gamma : e_g \otimes e_h \mapsto e_h \otimes e_g$ given by multiplication by $\gamma(g, h)$. The equalities above ensure that β^γ satisfies the hexagon axioms. Moreover, given such a braiding, we can define a quadratic form $q(x) \coloneqq \gamma(x, x)$, and this gives an isomorphism between the cohomology group $H^3_{\mathrm{ab}}(G, \Bbbk^\times)$ (i.e. the group of abelian 3-cocycles) and the

[6] Also called the *quantum double*.

group of quadratic functions $G \to \Bbbk^\times$. Two abelian 3-cocycles of G on $\Bbbk^\times$ give rise to the same quadratic form if and only if there is a braided monoidal equivalence between the resulting categories [21, Thm. 3.3].

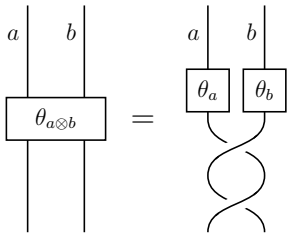
2.5.2. Twists and ribbon structures

As discussed in the previous sections, the morphisms in a rigid, braided monoidal category obey most of the Reidemeister moves: the rigidity axioms correspond to plane isotopy, while (2.7) and (2.8) correspond to Reidemeister II and III. For Reidemeister I, the only move that alters the writhe of a knot, we need an additional structure.

Definition 2.5.4. Let $\mathscr{C}$ be a rigid, braided monoidal category. A *twist*[7] is a natural transformation

$$\theta : \mathrm{id}_{\mathscr{C}} \to \mathrm{id}_{\mathscr{C}}$$

satisfying $\theta_{a\otimes b} = \beta_{b,a} \circ \beta_{a,b} \circ (\theta_a \otimes \theta_b)$ for all $a, b \in \mathscr{C}$. This condition is represented by



(2.9)

The component $\theta_a : a \to a$ of θ is called the twist of the object a. A category equipped with a designated twist is called *twisted* or *balanced*.

A twist is called a *ribbon structure* if $\theta_{a^*} = (\theta_a)^*$ for all $a \in \mathscr{C}$, and a category equipped with a ribbon structure is called *ribbon* itself.

Note that, if $\mathscr{C}$ is fusion and $a \in \mathscr{C}$ is simple, then we may view $\theta_a \in \mathscr{C}(a, a)$ as an element of $\Bbbk$, just as we did with the quantum trace. It is immediate that $\theta_{\mathbb{1}} = 1$. If θ is also ribbon, then rigidity implies that $\theta_a = \theta_{a^*}$ as elements of $\Bbbk$.

[7] Also called a *balancing transformation*.

Definition 2.5.5. If $\mathscr{C}$ admits a twist θ, we define the *T-matrix* of $\mathscr{C}$ by $[T]_{a,b} \coloneqq \delta_{a,b}\theta_a$ for $a, b \in \mathscr{C}$. The T-matrix acts on the Grothendieck ring $K_0(\mathscr{C})$ as follows:

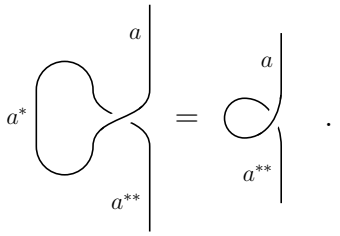
$$T \cdot x = T \cdot \bigoplus_{b \in \mathrm{Irr}(\mathscr{C})} X_b b = \bigoplus_{a,b \in \mathrm{Irr}(\mathscr{C})} \delta_{a,b}\theta_a X_b b = \bigoplus_{a \in \mathrm{Irr}(\mathscr{C})} \theta_a X_a a \ .$$

If $\mathscr{C}$ additionally admits any spherical structure, the order of T is finite[8] and is called the *Frobenius–Schur exponent* of $\mathscr{C}$; it is sometimes denoted $\mathrm{FSexp}(\mathscr{C})$.

There is a close connection between twists and pivotal structures. Let $\mathscr{C}$ be a rigid, braided monoidal category and $a \in \mathscr{C}$. Then we may define the *Drinfeld isomorphism* $\upsilon_a : a \to a^{**}$: if $\mathscr{C}$ is strict, it has the form

$$a \xrightarrow{\mathrm{coev}_{a^*} \otimes \mathrm{id}_a} a^* \otimes a^{**} \otimes a \xrightarrow{\beta_{a^{**},a}} a^* \otimes a \otimes a^{**} \xrightarrow{\mathrm{ev}_a \otimes \mathrm{id}_{a^{**}}} a^{**}$$

and diagram



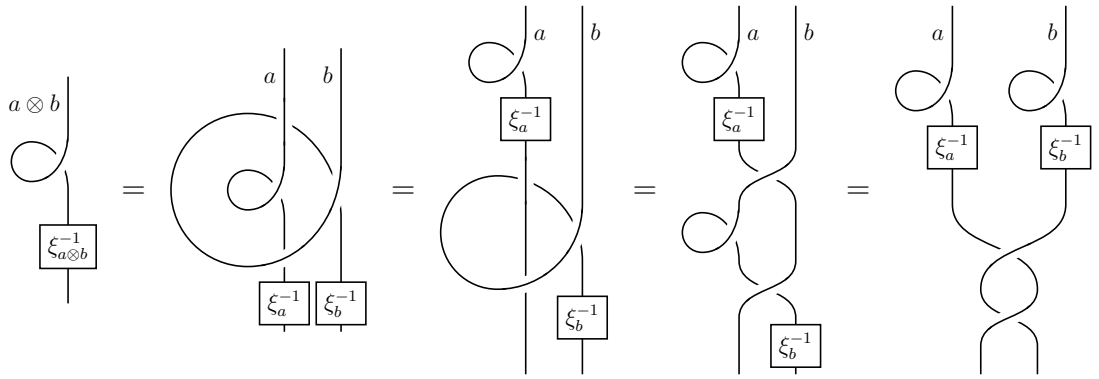
If $\mathscr{C}$ is non-strict, υ_a may be defined similarly by inserting the obvious legal isomorphisms. It is straightforward to show that the Drinfeld isomorphisms $\{\upsilon_a\}_{a \in \mathscr{C}}$ form a natural isomorphism $\upsilon : \mathrm{id}_{\mathscr{C}} \to (\bullet)^{**}$. This isomorphism may then be used to construct a twist from a pivotal structure and vice versa:

Proposition 2.5.6. *Let $\mathscr{C}$ be a rigid, braided monoidal category. Then pivotal structures and twists on $\mathscr{C}$ are in one-to-one correspondence: the relation between a pivotal structure ξ and the corresponding twist θ is*

$$\theta = \xi^{-1} \circ \upsilon \ .$$

[8] This follows from Vafa's theorem; see [34, Thm. 5.5] and Remark 2.6.7.

Proof. We may assume $\mathscr{C}$ is strictly rigid and use graphical calculus. Suppose ξ is a pivotal structure on $\mathscr{C}$. Then we may define $\theta := \xi^{-1} \circ \upsilon$ from $\mathrm{id}_{\mathscr{C}}$ to $\mathrm{id}_{\mathscr{C}}$, which is a natural isomorphism because ξ and υ are. That θ satisfies the condition of Definition 2.5.4 follows from the naturality of β and (2.8):



Hence θ is a twist.

For the converse, suppose θ is a twist on $\mathscr{C}$. Define $\xi : \mathrm{id}_{\mathscr{C}} \to (\bullet)^{**}$ to be $\upsilon \circ \theta^{-1}$, which is a natural isomorphism because υ and θ are. We must then show that the diagrams of Definition 2.1.4 commute. Since we have assumed that $\mathscr{C}$ is strictly rigid,[9] these become

$$\begin{array}{ccc} & \xrightarrow{\mathrm{id}} & \mathbb{1} \\ \mathbb{1} & & \downarrow \mathrm{id} \\ & \xrightarrow[\mathrm{id}]{} & \mathbb{1}^{**} = \mathbb{1} \end{array}$$

$$\begin{array}{ccc} a \otimes b & \xrightarrow{\mathrm{id}} & a \otimes b \\ {\scriptstyle \eta(a)\otimes\eta(b)}\downarrow & & \downarrow{\scriptstyle \eta(a\otimes b)} \\ a^{**} \otimes b^{**} & \xrightarrow{\mathrm{id}} & (a \otimes b)^{**} \end{array}$$

Hence ξ is a pivotal structure.

The maps thus defined are clearly inverses, giving the correspondence. □

Note that Proposition 2.5.6 does not mean that, if a given category $\mathscr{C}$ is equipped with a pivotal structure and a twist, then those structures will correspond in this way; in

[9] Otherwise, we must use the fact that $\tilde{\psi}_{a,b}$ is the unique isomorphism $a^{**} \otimes b^{**} \to (a \otimes b)^{**}$ to see that the bottom rectangle commutes.

other words, if $\mathscr{C}$ is pivotal, then the proposition lets us find a twist on $\mathscr{C}$, but it may be one of several possible choices of twist (and vice versa).

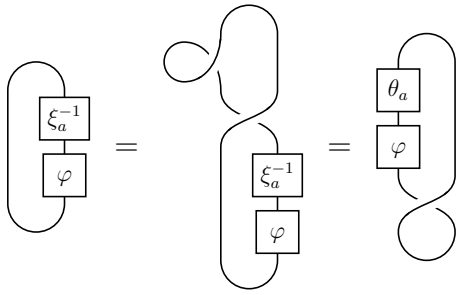
If, however, a pivotal category $\mathscr{C}$ is equipped with the corresponding twist, then

$$\mathrm{Tr}_\xi(\theta_a) = \mathrm{Tr}(\xi_a^{-1} \circ \theta_a) = \mathrm{Tr}(\xi_a^{-1} \circ (\xi_a \circ \upsilon_a)) = \mathrm{Tr}(\upsilon_a) \ ,$$

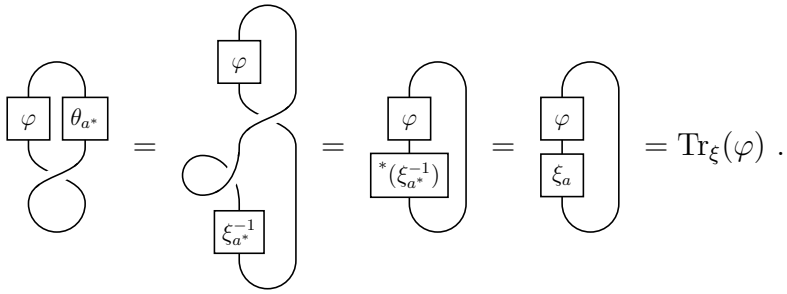
so this trace is independent of our choice of pivotal structure (and similarly for $\mathrm{Tr}'_\xi(\theta_a)$).

Proposition 2.5.7. *In the context of Proposition 2.5.6, if θ is a ribbon structure, then the corresponding pivotal structure ξ is spherical.*

Proof. We may assume $\mathscr{C}$ is strict. Consider any endomorphism $\varphi : a \to a$ in $\mathscr{C}$. Then we have

$\mathrm{Tr}'_\xi(\varphi) =$  $=$ $=$

Since $(\theta_a)^* = \theta_{a^*}$ by assumption, this becomes



$= \mathrm{Tr}_\xi(\varphi)$.

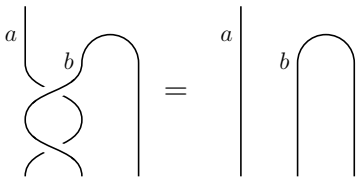
Here we used the right-sided form of Lemma 2.4.3. We conclude that ξ is spherical. □

The converse of Proposition 2.5.7 holds, at least for fusion categories. To show this, we first need this lemma:

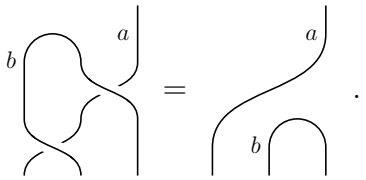
Lemma 2.5.8. *Let $\mathscr{C}$ be a rigid, braided, strict monoidal category. Then*

and the same with reversed braidings.

Proof. For the first equality, we compose both sides with the isomorphism $\beta_{a,b}^{-1} \otimes \mathrm{id}_{b^*}$. On the left, we have



while on the right, the hexagon axioms and naturality of β give



Since the results are isotopic as braids, they are identical by the braid axiom. The other three equations may be proved in the same way. □

Proposition 2.5.9. *Let ξ be a spherical structure on a fusion category $\mathscr{C}$ in the context of Proposition 2.5.6. Then the corresponding twist θ is ribbon.*

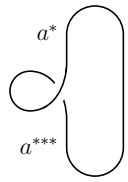
Proof. We may again assume $\mathscr{C}$ is strictly rigid. It suffices to show that $\theta_{a^*} = (\theta_a)^*$ for all $a \in \mathrm{Irr}(\mathscr{C})$, as the result then follows by semisimplicity. Let $a \in \mathrm{Irr}(\mathscr{C})$. Both θ_{a^*} and $(\theta_a)^*$ lie in $\mathscr{C}(a^*, a^*)$, and since a^* is simple, we have

$$\theta_{a^*} = t_1 \cdot \mathrm{id}_{a^*} \qquad (\theta_a)^* = t_2 \cdot \mathrm{id}_{a^*}$$

$$\mathrm{Tr}_\xi(\theta_{a^*}) = t_1 \cdot \dim_\xi(a^*) \qquad \mathrm{Tr}_\xi((\theta_a)^*) = t_2 \cdot \dim_\xi(a^*)$$

for $t_1, t_2 \in \Bbbk$. It is therefore enough to show that these traces are identical. To do so, we apply graphical calculus. Immediately,

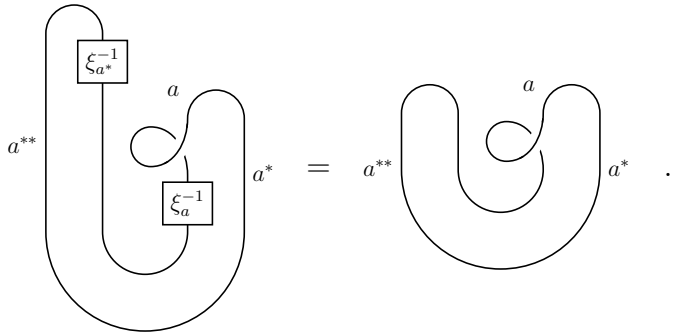
$$\mathrm{Tr}_\xi(\theta_{a^*}) = \mathrm{Tr}(\upsilon_{a^*}) =$$



.

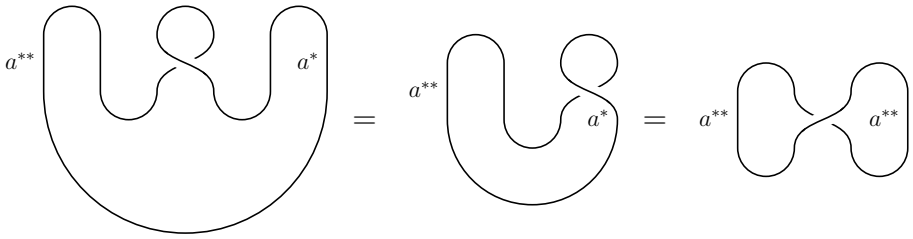
On the other hand, using our assumption of strict rigidity (so that $\xi_{a^*}^{-1} \otimes \xi_a^{-1} = \xi_{a^* \otimes a}^{-1}$) and the naturality and sphericality of ξ, we have

$$\mathrm{Tr}_\xi((\theta_a)^*) = \mathrm{Tr}'_\xi((\theta_a)^*) =$$



.

Applying Lemma 2.5.8 to this yields



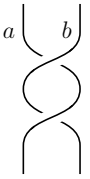
which is isotopic to the diagram for $\mathrm{Tr}_\xi(\theta_{a^*})$. We conclude that $t_1 = t_2$ and therefore that $\theta_{a^*} = (\theta_a)^*$. □

2.6. Modularity

2.6.1. Double braidings

Let $\mathscr{C}$ be a braided category with braiding β. Define the *double braiding* (or *monodromy*) of two objects $a, b \in \mathscr{C}$ to be

$$\beta_{a,b}^2 = \beta_{b,a} \circ \beta_{a,b} =$$



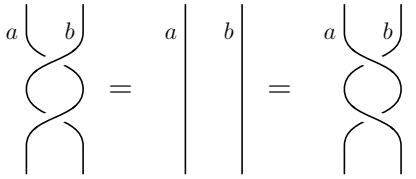
$\in \mathscr{C}(a \otimes b, a \otimes b)$.

A consequence of the braid axiom is that, for any $a \in \mathscr{C}$, we have $\beta^2_{\mathbb{1},a} = \mathrm{id}_{\mathbb{1},a}$ and similarly $\beta^2_{a,\mathbb{1}} = \mathrm{id}_{a,\mathbb{1}}$ [23, Proposition XIII.1.2]. This motivates the following definition:

Definition 2.6.1. An object a of a braided category $\mathscr{C}$ is called *transparent* or *central* if $\beta^{-1}_{a,b} = \beta_{b,a}$ for all $b \in \mathscr{C}$, so that

$$\beta^2_{a,b} = (\beta^{-1})^2_{b,a} = \mathrm{id}_{a\otimes b} \qquad\qquad \beta^2_{b,a} = (\beta^{-1})^2_{a,b} = \mathrm{id}_{b\otimes a} \ .$$

Graphically, strands labeled by a can "pass through" any other strand:



If all objects are transparent, then $\mathscr{C}$ (or rather its braiding) is called *symmetric*.

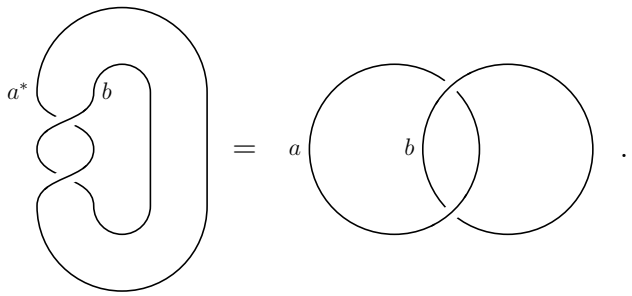
Definition 2.6.2 ([32, Def. 2.9])**.** The *Müger center* $Z_2(\mathscr{C})$ of a braided category $\mathscr{C}$ is the full subcategory of $\mathscr{C}$ consisting of the transparent objects of $\mathscr{C}$. Clearly $Z_2(\mathscr{C}) = \mathscr{C}$ if and only if $\mathscr{C}$ is symmetric.

If $\mathscr{C}$ is semisimple, then it suffices to consider the transparency of the simple objects; thus, we can view $\mathrm{Irr}(Z_2(\mathscr{C}))$ as a subset of $\mathrm{Irr}(\mathscr{C})$. In this case, we say the Müger center is trivial if $\mathrm{Irr}(Z_2(\mathscr{C})) = \{\mathbb{1}\}$.

Now, if $\mathscr{C}$ is braided and spherical, then for a, b in $\mathscr{C}$, we may consider

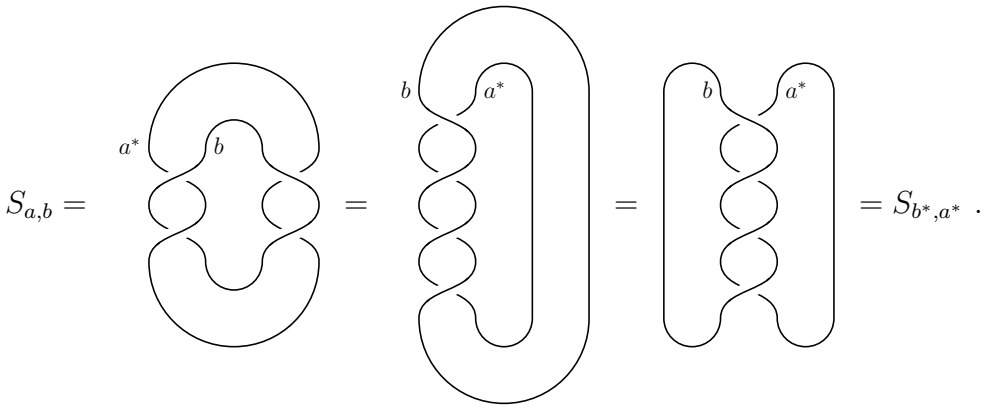
$$S_{a,b} = \mathrm{Tr}(\beta^2_{a^*,b}) \ .$$

Omitting the pivotal morphisms, this is represented by



.

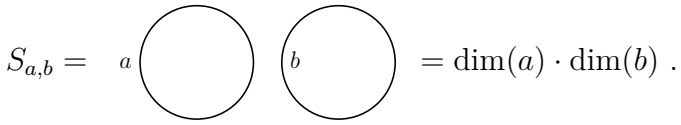
It follows from sphericality and Lemma 2.5.8 that



A similar procedure shows that $S_{a,b} = S_{b,a}$; hence

$$S_{a,b} = S_{b,a} = S_{a^*,b^*} = S_{b^*,a^*} \ . \tag{2.10}$$

Further, if $\beta^2_{a^*,b} = \mathrm{id}_{a^*,b}$, then clearly



In particular, since $\mathbb{1}$ is transparent, $S_{\mathbb{1},a} = S_{a,\mathbb{1}} = \dim(a)$.

2.6.2. The S-matrix

Definition 2.6.3. Let $\mathscr{C}$ be a ribbon, fusion category over a field $\Bbbk$ with $\operatorname{char} \Bbbk = 0$; such a category is sometimes called *premodular*. We may then view $S_{a,b} \in \mathscr{C}(\mathbb{1}, \mathbb{1})$ as an element of $\Bbbk$ and define the *S-matrix* of $\mathscr{C}$ by

$$[S]_{a,b \in \mathrm{Irr}(\mathscr{C})} \coloneqq S_{a,b} \ .$$

We further define the *C-matrix* (also known as the *charge conjugation matrix*) by

$$[C]_{a,b \in \mathrm{Irr}(\mathscr{C})} \coloneqq \delta_{b,a^*}$$

and the m^{th} *Gauss sum*

$$\tau^m \coloneqq \sum_{a \in \mathrm{Irr}(\mathscr{C})} \theta_a^m \dim(a)^2$$

for $m \in \mathbb{Z}$. We write $\tau^{\pm}$ for $\tau^{\pm 1}$.

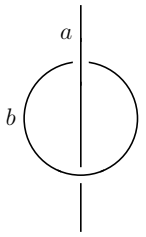
Lemma 2.6.4 ([3, Thm. 3.1.7])**.** *Let $\mathscr{C}$ be premodular. Then C commutes with S and T, and $C^2 = 1$. Further,*

$$(ST)^3 = \tau^+ S^2 \tag{2.11}$$

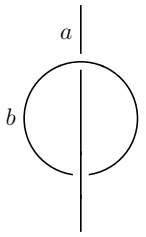
$$(ST^{-1})^3 = \tau^- S^2 C \ . \tag{2.12}$$

Proof. The given properties of C follow immediately from (2.10), $\theta_a = \theta_{a^*}$, and $a \cong a^{**}$. The others are most easily shown by graphical calculus. □

Lemma 2.6.5. *For any $a \in \mathrm{Irr}(\mathscr{C})$ in a premodular category, we have the following:*

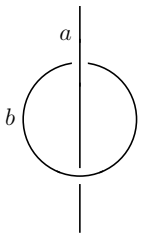


$$= \frac{S_{a,b}}{\dim(a)} \, \mathrm{id}_a \tag{2.13}$$



$$= \frac{S_{a,b^*}}{\dim(a)} \, \mathrm{id}_a \tag{2.14}$$

Proof. We will prove the first equation. Since a is simple, we have



$$= \mu \, \mathrm{id}_a \tag{2.15}$$

for some $\mu \in \Bbbk$. Taking the trace of both sides, we have

$$S_{a,b} = \mu \dim(a) \ . \tag{2.16}$$

The second equation is similar. □

Lemma 2.6.6. *Let $\mathscr{C}$ be premodular. For $a, b, c \in \mathrm{Irr}(\mathscr{C})$, we have*

$$S_{a,b} = \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^{d} \frac{\theta_d}{\theta_a \theta_b} \dim(d) \tag{2.17}$$

$$\dim(a)\dim(b) = \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^{d} \dim(d) \tag{2.18}$$

$$S_{a,b} S_{a,c} = \dim(a) \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{b,c}^{d} S_{a,d} \ . \tag{2.19}$$

Proof. By (2.9), we have $\beta_{a,b}^2 = \theta_{a\otimes b} \circ (\theta_a^{-1} \otimes \theta_b^{-1})$. Using the additivity of the trace [13, Proposition 4.7.3], we have

$$S_{a,b} = \quad = \theta_a^{-1}\theta_b^{-1} \operatorname{Tr}(\theta_{a\otimes b})$$

$$= \theta_a^{-1}\theta_b^{-1} \sum_{c \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^{c} \operatorname{Tr}(\theta_c)$$

$$= \theta_a^{-1}\theta_b^{-1} \sum_{c \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^{c} \theta_c \operatorname{Tr}(\mathrm{id}_c)$$

$$= \sum_{c \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^{c} \frac{\theta_c}{\theta_a \theta_b} \dim(c) \ .$$

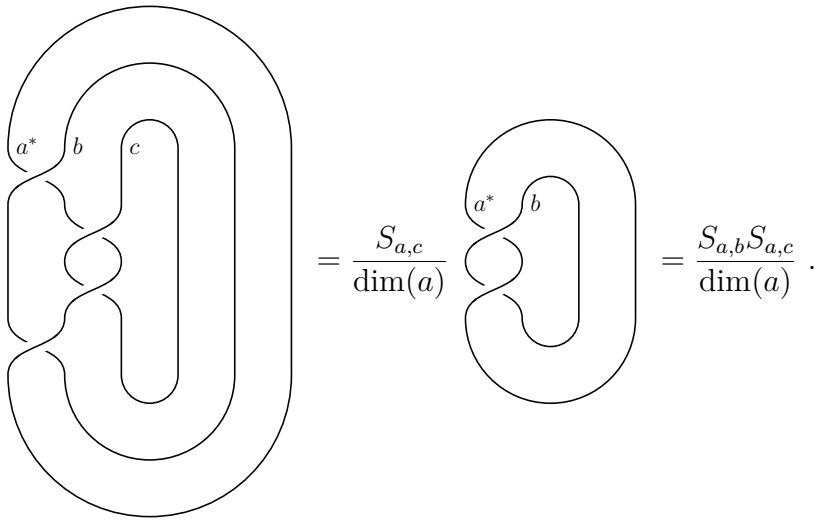
In the same way, $\dim(a)\dim(b) = \dim(a \otimes b) = \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^{d} \dim(d)$.

For the third equation, the hexagon axiom yields

$$=$$

Consider taking the trace of both sides. The right becomes $S_{a,(b\otimes c)}$. On the left, we may

apply Lemma 2.6.5 to find



Then, in the same manner as before, we have

$$\frac{S_{a,b}S_{a,c}}{\dim(a)} = S_{a,b\otimes c}$$

$$S_{a,b}S_{a,c} = \dim(a)\sum_{d\in \mathrm{Irr}(\mathscr{C})} N_{b,c}^{d} S_{a,d} \ ,$$

which confirms the statement. □

Vafa's theorem ([46]). *Suppose $\mathscr{C}$ is premodular. Then, for each $a \in \mathrm{Irr}(\mathscr{C})$, the twist θ_a is a finite root of unity.*

Remark 2.6.7. Note that Vafa's theorem is more commonly stated only for modular categories (as defined in the next section), but may be extended to premodular categories via Proposition 2.6.12 — the twists of objects in $\mathscr{C}$ will be the same as their images when $\mathscr{C}$ is embedded into the modular category $Z_1(\mathscr{C})$. If $\mathscr{C}$ is in fact modular, then $(\frac{\tau^+}{\tau^-})^{\frac{1}{6}}$ is also a root of unity, but that value could be zero for a premodular category.

Proposition 2.6.8. *Let $a \in \mathrm{Irr}(\mathscr{C})$ for a premodular category $\mathscr{C}$. Define $\chi_a : \mathrm{Irr}(\mathscr{C}) \to \Bbbk$ by setting*

$$\chi_a(b) := \frac{S_{a,b}}{\dim(a)} \ .$$

Then χ_a extends to a homomorphism $K_0(\mathscr{C}) \to \Bbbk$, that is, a character of the Grothendieck ring $K_0(\mathscr{C})$. This character is irreducible (because 1-dimensional). In particular, $\chi_{\mathbb{1}}$ coincides with the character $\dim : b \mapsto \dim(b)$.

Proof. As an additive group, $K_0(\mathscr{C})$ is free, so χ_a extends to a group homomorphism. Clearly $\chi_a(\mathbb{1}) = 1$. It suffices to show that $\chi_a(b \otimes c) = \chi_a(b) \cdot \chi_a(c)$. Applying (2.19),

$$\begin{aligned}
\chi_a(b \otimes c) &= \frac{S_{a,b\otimes c}}{\dim(a)} \\
&= \frac{1}{\dim(a)} \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{b,c}^d S_{a,d} \\
&= \frac{1}{(\dim(a))^2} S_{a,b} S_{a,c} \\
&= \chi_a(b) \cdot \chi_a(c)
\end{aligned}$$

for all $b, c \in \mathrm{Irr}(\mathscr{C})$ and hence for all elements of $K_0(\mathscr{C}) = \langle \mathrm{Irr}(\mathscr{C}) \rangle$. □

Recall from Section 2.6.1 that, when $\beta^2_{a^*,b} = \mathrm{id}_{a^*\otimes b}$, we have $S_{a,b} = \dim(a) \cdot \dim(b)$. For a partial converse, we have the following generalization of [32, Prop. 2.5]:

Proposition 2.6.9. *Let $\mathscr{C}$ be premodular over a number field $\Bbbk$,*[10] *and suppose that there exists an automorphism $\sigma \in \mathrm{Aut}(\bar{\Bbbk})$ such that $\sigma(\dim) = \mathrm{FPdim}$ as characters of $K_0(\mathscr{C})$ (cf. Definition 2.6.17). Then, any pair $a, b \in \mathrm{Irr}(\mathscr{C})$ satisfying $S_{a,b} = \dim(a) \cdot \dim(b)$ also satisfies $\beta^2_{a^*,b} = \mathrm{id}_{a^*\otimes b}$.*

[10] Otherwise $\dim : K_0(\mathscr{C}) \to \Bbbk^\times$ and $\mathrm{FPdim} : K_0(\mathscr{C}) \to \mathbb{C}^\times$ are not comparable.

Proof. Suppose $S_{a,b} = \dim(a) \cdot \dim(b)$ for some $a, b \in \mathrm{Irr}(\mathscr{C})$. Then, by Lemma 2.6.6, we have

$$\sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^d \frac{\theta_d}{\theta_a \theta_b} \dim(d) = \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^d \dim(d) \ .$$

Applying σ to both sides yields

$$\sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^d \ \sigma\left(\frac{\theta_d}{\theta_a \theta_b}\right) \mathrm{FPdim}(d) = \sum_{d \in \mathrm{Irr}(\mathscr{C})} N_{a,b}^d \, \mathrm{FPdim}(d)$$

which we then restrict to summands with $N_{a,b}^d \neq 0$:

$$0 = \sum_{\substack{d \in \mathrm{Irr}(\mathscr{C}) \\ N_{a,b}^d \neq 0}} N_{a,b}^d \left(1 - \sigma\left(\frac{\theta_d}{\theta_a \theta_b}\right)\right) \mathrm{FPdim}(d)$$

By Vafa's theorem, for any $d \in \mathrm{Irr}(\mathscr{C})$, $\frac{\theta_d}{\theta_a \theta_b}$ is a root of unity; hence, so is $\sigma\left(\frac{\theta_d}{\theta_a \theta_b}\right)$. Consider the embedding into $\mathbb{C}$; then $\left|\sigma\left(\frac{\theta_d}{\theta_a \theta_b}\right)\right| \leq 1$. Since $N_{a,b}^d \, \mathrm{FPdim}(d)$ is strictly positive, we then have

$$\mathfrak{Re}\left(N_{a,b}^d \left(1 - \sigma\left(\frac{\theta_d}{\theta_a \theta_b}\right)\right) \mathrm{FPdim}(d)\right) \geq 0$$

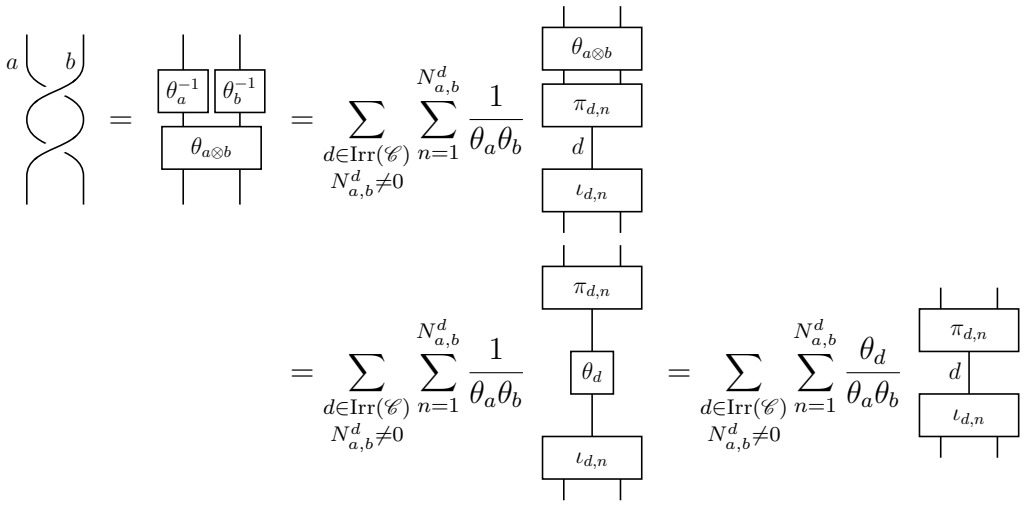
with equality if and only if $\sigma\left(\frac{\theta_d}{\theta_a \theta_b}\right) = 1$, or equivalently, $\theta_d = \theta_a \theta_b$. We conclude that this holds for every d with $N_{a,b}^d \neq 0$.

Now, we have $a \otimes b \cong \sum_d N_{a,b}^d d$. For each d with $N_{a,b}^d \neq 0$, let $\{\pi_{d,n}\}_{n=1}^{N_{a,b}^d}$ be a basis for $\mathscr{C}(a \otimes b, d)$. Let $\iota_{d,n}$ be the section corresponding to $\pi_{d,n}$. Then

$$\pi_{d,n} \circ \iota_{d,n} = \mathrm{id}_d$$

$$\sum_{\substack{d \in \mathrm{Irr}(\mathscr{C}) \\ N_{a,b}^d \neq 0}} \sum_{n=1}^{N_{a,b}^d} \iota_{d,n} \circ \pi_{d,n} = \mathrm{id}_{a \otimes b} \ .$$

We may now use these, along with (2.9), to show that



$$= \sum_{\substack{d\in \mathrm{Irr}(\mathscr{C}) \\ N_{a,b}^d \neq 0}} \sum_{n=1}^{N_{a,b}^d} \frac{1}{\theta_a \theta_b} = \sum_{\substack{d\in \mathrm{Irr}(\mathscr{C}) \\ N_{a,b}^d \neq 0}} \sum_{n=1}^{N_{a,b}^d} \frac{\theta_d}{\theta_a \theta_b}$$

which is equal to $\mathrm{id}_{a\otimes b}$ by applying the above properties once more. □

Note that the condition of Proposition 2.6.9 is fulfilled when $\mathscr{C}$ is pseudounitary with the canonical spherical structure ξ^+, as there Corollary 2.6.16 applies and we have $\sigma = \mathrm{id}$.

Lemma 2.6.10. *Let $\mathscr{C}$ be premodular and $a \in \mathrm{Irr}(\mathscr{C})$. If $a \in Z_2(\mathscr{C})$, then $\chi_a = \chi_{\mathbb{1}}$. As a partial converse, if the conditions of Proposition 2.6.9 hold and $\chi_a = \chi_{\mathbb{1}}$, then $a \in Z_2(\mathscr{C})$.*

Proof. For the first part, suppose a is transparent. Then $S_{a,b} = \dim(a) \cdot \dim(b)$ for all $b \in \mathscr{C}$, and hence $\chi_a = \chi_{\mathbb{1}}$.

For the second part, suppose the conditions of Proposition 2.6.9 hold and $\chi_a = \chi_{\mathbb{1}}$; this means $S_{a,b} = \dim(a)\dim(b)$ for all $b \in \mathscr{C}$. Applying the proposition gives $\beta^2_{a^*,b} = \mathrm{id}_{a^*\otimes b}$. It is easy to show that $Z_2(\mathscr{C})$ is closed under taking duals, so we conclude that a is transparent. □

2.6.3. Modular categories

Definition 2.6.11. A *modular* category $\mathscr{C}$ is a premodular category whose S-matrix is invertible – that is, the columns of S are linearly independent.

We now mention some well-known properties of modular categories.

Proposition 2.6.12 ([31, Prop. 5.10])**.** *If $\mathscr{C}$ is spherical and fusion, then $Z_1(\mathscr{C})$ is modular. If $\mathscr{C}$ is also ribbon, then it embeds into $Z_1(\mathscr{C})$ as a ribbon subcategory.*[11]

Lemma 2.6.13 ([13, Prop. 8.14.2 and 8.15.4])**.** *If $\mathscr{C}$ is modular, then*

$$\tau^+\tau^- = \dim(\mathscr{C}) \tag{2.20}$$

$$S^2 = \dim(\mathscr{C})C \ . \tag{2.21}$$

Verlinde formula ([13, Cor. 8.14.4])**.** *For all $a, b, c \in \mathrm{Irr}(\mathscr{C})$ with $\mathscr{C}$ modular, we have*

$$N_{a,b}^c = \frac{1}{\dim(\mathscr{C})} \sum_{d \in \mathrm{Irr}(\mathscr{C})} \frac{S_{a,d} S_{b,d} S_{c^*,d}}{\dim(d)} \ .$$

Corollary 2.6.14. *Let $\mathscr{C}$ be modular. For each a in $\mathrm{Irr}(\mathscr{C})$, define the diagonal matrix D_a by*

$$[D_a]_{b,c \in \mathrm{Irr}(\mathscr{C})} := \delta_{b,c} \frac{S_{a,b^*}}{\dim(b)} \ .$$

Then $SN_aS^{-1} = D_a$ for all $a \in \mathrm{Irr}(\mathscr{C})$. This fact is often stated as "the S-matrix diagonalizes the fusion rules."

Proof. We have

$$[D_aS]_{b,c} = \sum_{d \in \mathrm{Irr}(\mathscr{C})} [D_a]_{b,d} S_{d,c} = \sum_{d \in \mathrm{Irr}(\mathscr{C})} \delta_{b,d} \frac{S_{a,b^*}}{\dim(b)} S_{d,c} = \frac{S_{a,b^*} S_{b,c}}{\dim(b)} \ .$$

[11] Via the embedding given in Definition 2.5.3.

On the other hand, using (2.21),

$$\begin{aligned}
[SN_a]_{b,c} &= \sum_{d\in \mathrm{Irr}(\mathscr{C})} S_{b,d} N_{a,d}^{c} \\
&= \frac{1}{\dim(\mathscr{C})} \sum_{d,e\in \mathrm{Irr}(\mathscr{C})} \frac{S_{b,d} S_{a,e} S_{d,e} S_{c^*,e}}{\dim(e)} \\
&= \frac{1}{\dim(\mathscr{C})} \sum_{e\in \mathrm{Irr}(\mathscr{C})} \frac{[S^2]_{b,e} S_{a,e} S_{c^*,e}}{\dim(e)} \\
&= \frac{1}{\dim(\mathscr{C})} \sum_{e\in \mathrm{Irr}(\mathscr{C})} \frac{\delta_{e,b^*} \dim(\mathscr{C}) S_{a,e} S_{c^*,e}}{\dim(e)} \\
&= \frac{S_{a,b^*} S_{c^*,b^*}}{\dim(b^*)} \\
&= \frac{S_{a,b^*} S_{b,c}}{\dim(b)} \ .
\end{aligned}$$

Thus $SN_aS^{-1} = D_a$. □

Corollary 2.6.15. *Let $\mathscr{C}$ be modular over $\mathbb{C}$. Then $S_{a^*,b} = \overline{S_{a,b}}$ for all $a, b \in \mathrm{Irr}(\mathscr{C})$.*

Proof. Define $\mathbf{v}_b$ to be the b^{th} row vector of S. Then, by the calculations in the previous corollary, we have

$$\mathbf{v}_b N_a = \frac{S_{a,b^*}}{\dim(b)} \mathbf{v}_b \ .$$

On the other hand, the fusion matrices N_a are real and satisfy $N_a = (N_{a^*})^{\mathrm{T}}$ (Remark 2.3.4). As such,

$$[N_a \mathbf{v}_b^\dagger]_c = \sum_d N_{a,c}^d \, \overline{S_{b,d}} = \overline{\sum_d S_{d,b} \, N_{a^*,d}^c}$$

and so, recalling that $\dim(b)$ is real (Corollary 2.4.7), we have

$$N_a \mathbf{v}_b^\dagger = (\mathbf{v}_b N_{a^*})^\dagger = \left(\frac{S_{a^*,b^*}}{\dim(b)} \mathbf{v}_b \right)^\dagger = \frac{\overline{S_{a^*,b^*}}}{\dim(b)} \mathbf{v}_b^\dagger \ .$$

Combining these two results, we have

$$\frac{S_{a,b^*}}{\dim(b)} |\mathbf{v}_b|^2 = \mathbf{v}_b N_a \mathbf{v}_b^\dagger = \frac{\overline{S_{a^*,b^*}}}{\dim(b)} |\mathbf{v}_b|^2 \ .$$

Since $|\mathbf{v}_b|^2 = |b|^2$ is non-zero by Lemma 2.3.6, this completes the proof. □

Corollary 2.6.16. *A premodular category $\mathscr{C}$ is modular if and only if the characters of the Grothendieck ring $K_0(\mathscr{C})$ are precisely $\{\chi_a\}_{a\in\mathrm{Irr}(\mathscr{C})}$ (with χ_a defined as in Proposition 2.6.8). In this case, if $\Bbbk = \mathbb{C}$, there exists an object $\mathbb{Y} \in \mathrm{Irr}(\mathscr{C})$, called the* Frobenius–Perron object*, such that $\chi_{\mathbb{Y}} = \mathrm{FPdim}$. We have $\mathbb{Y} = \mathbb{1}$ if and only if $\mathscr{C}$ is pseudounitary with the canonical spherical structure ξ^+ (as in Proposition 2.4.9).*

Proof. $K_0(\mathscr{C})$ is a commutative algebra of dimension $|\mathrm{Irr}(\mathscr{C})|$, so has $|\mathrm{Irr}(\mathscr{C})|$ distinct irreducible characters; thus, some character of $K_0(\mathscr{C})$ fails to appear among the $|\mathrm{Irr}(\mathscr{C})|$ irreducible characters χ_a if and only if $\chi_a = \chi_b$ for $a, b \in \mathrm{Irr}(\mathscr{C})$. By definition, $\mathscr{C}$ is modular if and only if the columns of S are linearly independent, which corresponds to χ_a being distinct characters. □

When $\mathscr{C}$ is modular, we may use these characters to define a useful Galois group action on $\mathrm{Irr}(\mathscr{C})$:

Definition 2.6.17. Let $\mathscr{C}$ be modular over a field $\Bbbk$ and let $\sigma \in \mathrm{Aut}(\overline{\Bbbk})$. For each $a \in \mathrm{Irr}(\mathscr{C})$, consider $\sigma(\chi_a)$, which must also be a character of $K_0(\mathscr{C})$. In light of Corollary 2.6.16, there is a unique element of $\mathrm{Irr}(\mathscr{C})$, which we denote by $\hat{\sigma}(a)$, such that

$$\chi_{\hat{\sigma}(a)} = \sigma(\chi_a) \ .$$

Moreover, as σ is invertible, the map $\hat{\sigma} : \mathrm{Irr}(\mathscr{C}) \to \mathrm{Irr}(\mathscr{C})$ defined in this way is bijective — in other words, $\hat{\sigma}$ is a permutation of $\mathrm{Irr}(\mathscr{C})$. This may be viewed as an action of $\mathrm{Aut}(\overline{\Bbbk})$ on $\mathrm{Irr}(\mathscr{C})$.

As a particular case, when $\Bbbk = \mathbb{C}$, we may consider the field $\mathbb{Q}(S)$ and denote its

Galois group by $\mathrm{Gal}_{\mathscr{C}} := \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. Then the action defined above factors through the action of $\mathrm{Gal}_{\mathscr{C}}$ on $\mathrm{Irr}(\mathscr{C})$. In fact, the field $\mathbb{Q}(S)$ is cyclotomic:

Theorem 2.6.18 ([35, Prop. 5.7])**.** *Let $\mathscr{C}$ be modular over $\mathbb{C}$. Then $\mathbb{Q}(S) \leq \mathbb{Q}(T) = \mathbb{Q}(\zeta_N)$, where $N := \mathrm{ord}(T)$ (the* Frobenius–Schur exponent *of $\mathscr{C}$) is finite. Moreover, for all $a, b \in \mathrm{Irr}(\mathscr{C})$, both $S_{a,b}$ and $\chi_a(b) = \frac{S_{a,b}}{\dim(a)}$ are cyclotomic integers in $\mathbb{Z}[\zeta_N]$.*

This Galois action will be explored further in Chapter 4.

A modular category is, in a sense, one which is "as far from symmetric as possible":

Lemma 2.6.19. *If $\mathscr{C}$ is modular, then $Z_2(\mathscr{C})$ is trivial. In particular, if $\mathscr{D}$ is braided, spherical, and fusion, then $Z_2(Z_1(\mathscr{D}))$ is trivial.*

As a partial converse, if $\mathscr{C}$ is premodular and pseudounitary with the spherical structure ξ^+, and $Z_2(\mathscr{C})$ is trivial, then $\mathscr{C}$ is modular.

Proof. The first statement follows from Lemma 2.6.10 and Corollary 2.6.16; the second follows from applying this to Proposition 2.6.12.

For the partial converse, if $\mathscr{C}$ has the given properties but is not modular, then there exists some $a \in \mathrm{Irr}(\mathscr{C})$ such that $a \ncong \mathbb{1}$ and $\chi_a = \chi_{\mathbb{1}}$. Applying Lemma 2.6.10, we see that $a \in Z_2(\mathscr{C})$, so $Z_2(\mathscr{C})$ is not trivial. □

Chapter 3. Representations and Symmetrizability

3.1. Representations of $\mathrm{SL}_2(\mathbb{Z})$

3.1.1. Definitions

Consider the modular group $\mathrm{SL}_2(\mathbb{Z})$. Denote $\mathfrak{s} := \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $\mathfrak{t} := \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Then $\mathrm{SL}_2(\mathbb{Z}) = \langle \mathfrak{s}, \mathfrak{t} \rangle$, subject to the relations

$$\mathfrak{s}^4 = \mathrm{id} \qquad\qquad (\mathfrak{s}\mathfrak{t})^3 = \mathfrak{s}^2 \,.$$

Definition 3.1.1. A *projective representation* of $\mathrm{SL}_2(\mathbb{Z})$ over a field $\Bbbk$ is a group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PGL}_r(\Bbbk)$ for some $r \in \mathbb{Z}^+$, while a *(linear) representation* of $\mathrm{SL}_2(\mathbb{Z})$ is a group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_r(\Bbbk)$ for some $r \in \mathbb{Z}^+$. The dimension r is called the *degree* of the representation.

A *lift* of a projective representation $\tilde{\rho}$ is a linear representation ρ so that $\tilde{\rho} = \pi \circ \rho$, where $\pi : \mathrm{GL}_r(\Bbbk) \to \mathrm{PGL}_r(\Bbbk)$ is the canonical projection.

In this dissertation, representations are linear unless specified to be projective.

From the above presentation, we can see that any pair of $r \times r$ matrices (S, T) with

$$S^4 = a\,\mathrm{id}_r \qquad\qquad (ST)^3 = bS^2 \tag{3.1}$$

for some $a, b \in \Bbbk^\times$ defines a projective representation $\tilde{\rho}$ of $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\tilde{\rho}(\mathfrak{s}) = S \qquad\qquad \tilde{\rho}(\mathfrak{t}) = T \,.$$

If in fact $a = b = 1$, then the same definition defines a linear representation. Conversely, any projective representation $\tilde{\rho}$ can be described by such a pair, namely by (arbitrarily-chosen) representatives of $\tilde{\rho}(\mathfrak{s})$ and $\tilde{\rho}(\mathfrak{t})$ in $\mathrm{GL}_r(\Bbbk)$, so we may abuse the notation accordingly.

In light of this, consider a projective representation $\tilde{\rho}$ given by (S,T) and let a, b be as defined in (3.1). If $\Bbbk^\times$ contains elements α, β so that $\alpha^{12} = a$ and $\beta^3 = b$, then the assignment $(s \coloneqq \alpha^{-3}S,\ t \coloneqq \alpha\beta^{-1}T)$ defines a lift ρ of $\tilde{\rho}$:

$$s^4 = \frac{a}{\alpha^{12}}\,\mathrm{id}_r = \mathrm{id}_r \qquad\qquad (st)^3 = \frac{b}{\alpha^6\beta^3}S^2 = \Big(\frac{1}{\alpha^3}S\Big)^2 = s^2\ .$$

Further, suppose that (s', t') gives another lift of $\tilde{\rho}$; then $\pi(s') = \pi(s) = S$, so $s' = \lambda s$ for $\lambda \in \Bbbk^\times$. Similarly, $t' = \mu t$ for $\mu \in \Bbbk^\times$. Solving (3.1) then yields $\lambda^4 = 1$ and $\lambda^3\mu^3 = \lambda^2$, so we conclude that $\mu^{12} = 1$ and $\lambda = \mu^{-3}$. Thus, all lifts of (S,T) have the form $(\mu^{-3}s, \mu t)$ where μ is a 12^{th} root of unity in $\Bbbk$; in particular, there are at most 12 distinct lifts up to equivalence [9, Section 1.2].

3.1.2. Representations from modular categories

Definition 3.1.2. Let $\mathscr{C}$ be a modular category over a field $\Bbbk$ and consider the associated pair of matrices (S,T), which we call the *modular data* of $\mathscr{C}$. From Lemmas 2.6.4 and 2.6.13, we see that (S,T) satisfies

$$S^4 = \dim(\mathscr{C})^2\,\mathrm{id}_{r_\mathscr{C}} \qquad\qquad (ST)^3 = \tau^+ S^2\,.$$

As we assumed $\mathrm{char}(\Bbbk) = 0$, both $\dim(\mathscr{C})^2$ and τ^+ are non-zero. Thus, (S,T) defines a projective representation $\tilde{\rho}_\mathscr{C} : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}(V) \cong \mathrm{GL}_{r_\mathscr{C}}(\Bbbk)$, where $V \coloneqq K_\Bbbk(\mathscr{C})$ is the Grothendieck algebra defined in Section 2.3. The degree of $\tilde{\rho}_\mathscr{C}$ is $r_\mathscr{C} = |\mathrm{Irr}(\mathscr{C})| < \infty$.

The lifts of $\tilde{\rho}_\mathscr{C}$ are called the *modular category (MC) representations* arising from $\mathscr{C}$ [35]. As described in the previous section, each lift ρ is defined by $s \coloneqq \rho(\mathfrak{s}) = \lambda S$ and $t \coloneqq \rho(\mathfrak{t}) = \mu T$ for some $\lambda, \mu \in \Bbbk^\times$; the matrices (s,t) are therefore sometimes called *normalized modular data*.

When working with a MC representation ρ, we will generally assume it is expressed in terms of matrices with respect to the natural basis of V given by $\mathrm{Irr}(\mathscr{C})$. Given this, the following important properties immediately hold.

- The matrix $s = \rho(\mathfrak{s})$ is symmetric (by (2.10)).
- The matrix $t = \rho(\mathfrak{t})$ is diagonal (by the definition of T).

These properties motivate the following definition.

Definition 3.1.3. Let ρ be a representation of $\mathrm{SL}_2(\mathbb{Z})$. A basis $\mathcal{B}$ is called a *symmetric basis* for ρ if, with respect to $\mathcal{B}$, the matrix $\rho(\mathfrak{s})$ is symmetric and $\rho(\mathfrak{t})$ is diagonal. If such a basis exists, then ρ is called *symmetrizable*.

For simplicity, we may call ρ itself *symmetric* to indicate that it is equipped with a fixed symmetric basis; then, a representation of $\mathrm{SL}_2(\mathbb{Z})$ is symmetrizable if and only if it is equivalent to a symmetric representation.

Remark 3.1.4. Any permutation of a symmetric basis for ρ is also a symmetric basis for ρ. Further, symmetrizability is preserved under direct sum and tensor product of representations: if ρ_1, ρ_2 admit symmetric bases $\mathcal{B}_1$, $\mathcal{B}_2$ respectively, then

$$\{(v_1, 0) \mid v_1 \in \mathcal{B}_1\} \cup \{(0, v_2) \mid v_2 \in \mathcal{B}_2\} \qquad \text{and} \qquad \{v_1 \otimes v_2 \mid v_1 \in \mathcal{B}_1, v_2 \in \mathcal{B}_2\}$$

are symmetric bases for $\rho_1 \oplus \rho_2$ and $\rho_1 \otimes \rho_2$ respectively.

Definition 3.1.5. A finite-dimensional representation ρ of $\mathrm{SL}_2(\mathbb{Z})$ is called *congruence* if it factors through $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ for some positive integer n. The smallest such n is called the *level* of ρ and denoted $\ell(\rho)$. Equivalently, ρ is congruence of level n if $\ker(\rho) \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup of level n.

Note that there exist representations of $\mathrm{SL}_2(\mathbb{Z})$ which are not congruence [15], and

among these there are examples which are symmetrizable and some which are not; some examples of both are described in our paper [37]. However, it has been shown that all MC representations are congruence:

Proposition 3.1.6 ([9, Theorem II(i)])**.** *Let ρ be a MC representation arising from a modular category $\mathscr{C}$. Then ρ is congruence, and $\ell(\rho) = \mathrm{ord}(t) < \infty$.*

In the complex case, we may specialize the above as follows.

Lemma 3.1.7. *Let ρ be a MC representation arising from a modular category $\mathscr{C}$ over $\mathbb{C}$. Then ρ is a unitary representation, and for any $\mathfrak{g} \in \mathrm{SL}_2(\mathbb{Z})$ the (unitary) matrix $\rho(\mathfrak{g})$ is defined over $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$, where $n = \mathrm{ord}(t)$.*

Proof. For unitarity, it suffices to show that $S^{-1} = \frac{1}{\dim(\mathscr{C})} S^\dagger$ and $T^{-1} = T^\dagger$ hold.[1] The latter is immediate, as T is diagonal and all entries are roots of unity by Vafa's theorem.

For the former, we recall that $\overline{S_{a,b}} = S_{b,a^*}$ (by (2.10) and Corollary 2.6.15). Also, by (2.21), we have $\sum_{c \in \mathrm{Irr}(\mathscr{C})} S_{a,c} S_{c,b} = \dim(\mathscr{C}) \delta_{b,a^*}$. We then find

$$\begin{aligned}
\Big[S \cdot \frac{1}{\dim_{\mathscr{C}}} S^\dagger \Big]_{a,b} &= \frac{1}{\dim(\mathscr{C})} \sum_{c \in \mathrm{Irr}(\mathscr{C})} S_{a,c} S^\dagger_{c,b} \\
&= \frac{1}{\dim(\mathscr{C})} \sum_{c \in \mathrm{Irr}(\mathscr{C})} S_{a,c} \overline{S_{b,c}} \\
&= \frac{1}{\dim(\mathscr{C})} \sum_{c \in \mathrm{Irr}(\mathscr{C})} S_{a,c} S_{c,b^*} \\
&= \delta_{a,b} \ .
\end{aligned}$$

Lifting $\tilde{\rho}_{\mathscr{C}}$ then normalizes away the factor of $\dim(\mathscr{C})$, so ρ is unitary.

The point regarding $\mathbb{Q}_n$ follows from Proposition 3.1.6; see also [35]. □

[1] These properties imply that $\tilde{\rho}_{\mathscr{C}}$ is unitary in the sense appropriate to a projective representation.

It is now natural to ask which representations of $\mathrm{SL}_2(\mathbb{Z})$ actually arise from modular categories in the way we have described. Hence, the following definition.

Definition 3.1.8. A representation ρ of $\mathrm{SL}_2(\mathbb{Z})$ is called *realizable*[2] if it is equivalent to a MC representation arising from some modular category $\mathscr{C}$. In that case, we say that ρ is *realized* by $\mathscr{C}$. Note that a representation may be realized by more than one category.[3]

As of this writing, it is largely an open question as to which representations are realizable, though results have been found for some cases [10]. It is therefore useful to consider criteria by which we may show that a representation *cannot* be realized. The above discussions yield the following.

Lemma 3.1.9. *In order for a representation ρ to be realizable, it is necessary for it to have finite degree and be congruence and symmetrizable.*

As noted above, complex representations of $\mathrm{SL}_2(\mathbb{Z})$ can indeed fail to be symmetrizable; by the lemma, these cannot be realized by any modular category. However, our examples for this behavior are noncongruence representations, and hence are not very helpful in the study of realizability, as they have already been eliminated from consideration. Therefore, we may ask whether symmetrizability can fail in the congruence case as well. We will show that this is not possible:

Theorem 3.1.10. *Every finite-dimensional complex congruence representation of* $\mathrm{SL}_2(\mathbb{Z})$ *is symmetrizable.*

This result appears in our recent paper as [37, Thm. 2.10]. In the next chapter, we will describe our proof of this theorem and provide some information on the process

[2]Sometimes called *admissible*.

[3]In the known cases where this occurs, the categories differ only by Galois conjugation.

beyond that found in that paper.

3.2. Quadratic modules and Weil representations

3.2.1. Definitions

Remark 3.2.1. Let ρ be a finite-dimensional complex congruence representation of $\mathrm{SL}_2(\mathbb{Z})$. We may then decompose it as a direct sum:

$$\rho \cong \bigoplus_{j \in J} \rho_j \ ,$$

where $|J| < \infty$ and each ρ_j is an irreducible representation. Note $\ell(\rho) = \mathrm{lcm}(\{\rho_j\}_{j \in J})$. The representations ρ_j are called the *irreducible components* of ρ. Each ρ_j can be further decomposed as a tensor product by applying the Chinese remainder theorem:

$$\rho_j \cong \bigotimes_{k \in K_j} \hat{\rho}_{j,k} \ ,$$

where $|K_j| < \infty$ and $\{\hat{\rho}_{j,k}\}_{k \in K_j}$ are irreducible representations whose levels are all powers of distinct primes.[4] The representations $\hat{\rho}_{j,k}$ are called the *tensor components* of ρ.

To classify all finite-dimensional complex congruence representations, it therefore suffices to examine irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ for primes p and positive integers λ. Representations of this type have been completely classified by Nobs and Wolfart through the use of subrepresentations of Weil representations arising from quadratic modules [40] (which are defined below). We will detail their classification in Section 3.3.

Definition 3.2.2. Let M be an additive abelian group. A *nondegenerate quadratic form* on M is a function $Q : M \to {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}}$ such that

(i) $Q(-a) = Q(a)$ for all $a \in M$ and

(ii) $B(a, b) := Q(a + b) - Q(a) - Q(b)$ defines a nondegenerate bilinear map.

[4] The level $\ell(\rho_j)$ is then the product of those prime powers.

The pair (M, Q) is then called a (nondegenerate) *quadratic module*.

The subgroup $\{\omega \in \mathrm{Aut}(M) \mid Q(\omega x) = Q(x) \text{ for all } x \in M\}$ of automorphisms fixing Q is denoted $\mathrm{Aut}(M, Q)$.

Quadratic modules are closely related to *pointed* modular categories — a modular category $\mathscr{C}$ is called pointed if the tensor product makes $\mathrm{Irr}(\mathscr{C})$ into a group.[5] Precisely: given any pointed modular category $\mathscr{C}$, we may take $M = \mathrm{Irr}(\mathscr{C})$ and $Q(a) = \theta_a$, and then (M, Q) is a quadratic module; on the other hand, given a quadratic module (M, Q), one can use the Eilenberg–MacLane theorem [11, 12] on abelian 3-cocycles to construct a unique (up to equivalence) pointed modular category $\mathscr{C}(M, Q)$ [20, 21].[6]

Each quadratic module has an associated projective representation of $\mathrm{SL}_2(\mathbb{Z})$:

Definition 3.2.3. Let (M, Q) be a quadratic module and denote by $V \coloneqq \mathbb{C}^M$ the space of complex-valued functions on M. This space is equipped with a natural Hermitian form

$$\langle f, g \rangle \coloneqq \sum_{a \in M} f(a)\overline{g(a)}\,,$$

and we denote the vector norm of $f \in V$ by $\|f\| \coloneqq \sqrt{\langle f, f \rangle}$. Note that V admits a standard orthonormal basis: $\{\delta_a \mid a \in M\}$, where δ_a is the function defined by $\delta_a(b) = \delta_{a,b}$. As described in [39, Satz 2 & §2], we then have a projective representation

$$W(M, Q) : \mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z}) \to \mathrm{PGL}(V)$$

defined by

$$\begin{aligned} \mathfrak{s}\,\delta_a &\coloneqq W(M, Q)(\mathfrak{s})(\delta_a) = \frac{\tau_Q}{|M|} \sum_{b \in M} \mathbf{e}(-B(a, b))\,\delta_b\,, \\ \mathfrak{t}\,\delta_a &\coloneqq W(M, Q)(\mathfrak{t})(\delta_a) = \mathbf{e}(Q(a))\,\delta_a\,. \end{aligned} \tag{3.2}$$

[5] In other words, for each $a \in \mathrm{Irr}(\mathscr{C})$, we have $a \otimes a^* \cong \mathbb{1}$ and can view a^* as an "inverse object" for a; see, for example, [14, Sec. 8].

[6] See also [13, Thm. 8.4.9].

Here $\tau_Q := \sum_{a \in M} \mathbf{e}(Q(a))$ is the *Gauss sum* of (M, Q). This representation is called the *Weil representation* associated to (M, Q).

In fact, $W(M, Q)$ is precisely the projective representation $\tilde{\rho}_{\mathscr{C}(M,Q)}$ arising from the pointed modular category $\mathscr{C}(M, Q)$, as described in Definition 3.1.2; the modular data (S, T) of $\mathscr{C}(M, Q)$ are given explicitly by

$$S_{a,b} = \mathbf{e}(-B(a, b)) \qquad \text{and} \qquad T_{a,b} = \mathbf{e}(Q(a)) \cdot \delta_{a,b}$$

for $a, b \in M$. The Gauss sum τ_Q coincides with the $+1$ Gauss sum τ^+ of $\mathscr{C}(M, Q)$, as defined in Definition 2.6.3. Since $W(M, Q)$ is realizable in this way, any lift thereof to a linear representation of $\mathrm{SL}_2(\mathbb{Z})$ will be congruence and symmetric by Lemma 3.1.9.

As we can always take a lift of $W(M, Q)$, we will assume going forward that the projective representation $W(M, Q)$ is in fact a linear representation of $\mathrm{SL}_2(\mathbb{Z})$ (and hence congruence and symmetric). Conveniently, the Weil representations used in the classification at hand[7] are all linear representations as presented.

3.2.2. Symmetrizability

Though $W(M, Q)$ itself is symmetric, subrepresentations of a symmetric representation are not always symmetrizable [37, Ex. 2.8]. To prove Theorem 3.1.10, it is therefore prudent to determine conditions under which a subrepresentation of $W(M, Q)$ is guaranteed to be symmetrizable, as follows.

Lemma 3.2.4. *Let $\eta : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{U}(n)$ be a symmetric representation. Suppose $U \in \mathrm{U}(n)$ commutes with $\eta(\mathfrak{g})$ for all $\mathfrak{g} \in \mathrm{SL}_2(\mathbb{Z})$. Let $\psi(x) = Ux$ and $\overline{\psi}(x) = \overline{Ux}$ for $x \in \mathbb{C}^n$; note that $\overline{\psi}$ is an antilinear operator. Then:*

[7] See Table 3.1.

(i) For any $x, y \in \mathbb{C}^n$, we have $\langle \eta(\mathfrak{s})x,\, y\rangle = \langle \eta(\mathfrak{s})\overline{\psi}(y),\, \overline{\psi}(x)\rangle$.

(ii) If ρ is a subrepresentation of η and there exists an orthonormal eigenbasis $\mathcal{S}$ for $\rho(\mathfrak{t})$ such that each element of $\mathcal{S}$ is fixed by $\overline{\psi}$, then $\mathcal{S}$ is a symmetric basis for ρ.

Proof. Since $\eta(\mathfrak{s})$ is symmetric, $\overline{\eta(\mathfrak{s})} = \eta(\mathfrak{s})^{-1}$, which implies

$$\langle \eta(\mathfrak{s})\overline{x},\, \overline{y}\rangle = \overline{\langle \eta(\mathfrak{s})^{-1}x, y\rangle} = \langle \eta(\mathfrak{s})y,\, x\rangle$$

for any $x, y \in \mathbb{C}^n$. As a result, we have

$$\langle \eta(\mathfrak{s})\overline{\psi}(y),\, \overline{\psi}(x)\rangle = \langle \eta(\mathfrak{s})\psi(x),\, \psi(y)\rangle = \langle \psi(\eta(\mathfrak{s})x),\, \psi(y)\rangle = \langle \eta(\mathfrak{s})x,\, y\rangle\,,$$

which proves (i). Then, for any $x, y \in \mathcal{S}$, the matrix coefficients of $\rho(\mathfrak{s})$ are given by

$$\rho(\mathfrak{s})_{y,x} = \langle \eta(\mathfrak{s})x, y\rangle = \langle \eta(\mathfrak{s})\overline{\psi}(y), \overline{\psi}(x)\rangle = \langle \eta(\mathfrak{s})y, x\rangle = \rho(\mathfrak{s})_{x,y}\,,$$

which means $\rho(\mathfrak{s})$ is symmetric with respect to $\mathcal{S}$. Since $\mathcal{S}$ is an eigenbasis for $\rho(\mathfrak{t})$, this confirms that it is a symmetric basis for ρ. □

Now consider a quadratic module (M, Q) and some $\omega \in \mathrm{Aut}(M, Q)$. We define the associated $\mathbb{C}$-linear map $\varphi_\omega : V \to V$ by $\varphi_\omega(\delta_a) \coloneqq \delta_{\omega a}$ and the antilinear map $\overline{\varphi}_\omega$ as the composition of φ_ω and complex conjugation, relative to the standard basis $\{\delta_a \mid a \in M\}$ for V. Note that φ_ω preserves $\langle \cdot, \cdot \rangle$, hence is an isometry on V in the usual sense.

Proposition 3.2.5. *Let ρ be a subrepresentation of $W(M, Q)$ on the subspace $Y \subseteq V$. Suppose $\omega \in \mathrm{Aut}(M, Q)$ is an involution and $\mathcal{B}$ an orthonormal basis for Y such that*

(i) each element of $\mathcal{B}$ is an eigenvector of $\rho(\mathfrak{t})$,

(ii) for any $f \in \mathcal{B}$ such that f and $\overline{\varphi}_\omega(f)$ are linearly independent, we have $\overline{\varphi}_\omega(f) \in \mathcal{B}$.

Then ρ is symmetrizable.

Proof. Let $\mathcal{B}_1 \coloneqq \{f \in \mathcal{B} \mid f \text{ and } \overline{\varphi}_\omega(f) \text{ are linearly dependent}\}$. This means that, for each $f \in \mathcal{B}_1$, there exists some $\eta_f \in \mathrm{U}(1)$ with $\overline{\varphi}_\omega(f) = \eta_f f$. In particular, we have $\overline{\varphi}_\omega(\sqrt{\eta_f} f) = \overline{\sqrt{\eta_f}} \cdot \overline{\varphi}_\omega(f) = \sqrt{\eta_f} f$.

Now, since $\omega^2 = \mathrm{id}$, $\overline{\varphi}_\omega^2 = \mathrm{id}$. So, applying (ii), we see that all elements of $\mathcal{B} \smallsetminus \mathcal{B}_1$ come in pairs: $\{f,\ \overline{\varphi}_\omega(f)\}$. Choose $\mathcal{B}_2 \subset \mathcal{B} \smallsetminus \mathcal{B}_1$ to consist of one element from each pair, so that $\mathcal{B}_2 \cap \overline{\varphi}_\omega(\mathcal{B}_2) = \varnothing$ and $\mathcal{B} = \mathcal{B}_1 \sqcup \mathcal{B}_2 \sqcup \overline{\varphi}_\omega(\mathcal{B}_2)$. This construction ensures that

$$\mathcal{S} \coloneqq \left\{\sqrt{\eta_f} f \;\middle|\; f \in \mathcal{B}_1\right\} \sqcup \left\{\frac{1}{\sqrt{2}}(f + \overline{\varphi}_\omega(f)) \;\middle|\; f \in \mathcal{B}_2\right\} \sqcup \left\{\frac{i}{\sqrt{2}}(f - \overline{\varphi}_\omega(f)) \;\middle|\; f \in \mathcal{B}_2\right\}$$

is an orthonormal basis for Y. As $\overline{\varphi}_\omega$ is antilinear, $\overline{\varphi}_\omega(h) = h$ for all $h \in \mathcal{S}$.

Finally, for each $f \in \mathcal{B}$, we have $\rho(\mathfrak{t})(f) = \xi_f f$ for some $\xi_f \in \mathrm{U}(1)$. Then

$$\rho(\mathfrak{t})\overline{\varphi}_\omega(f) = \overline{\varphi}_\omega \rho(\mathfrak{t})^{-1}(f) = \overline{\varphi}_\omega(\xi_f^{-1} f) = \xi_f \overline{\varphi}_\omega(f)\,.$$

Therefore, $\mathcal{S}$ is an eigenbasis for $\rho(\mathfrak{t})$. By Lemma 3.2.4, $\mathcal{S}$ is a symmetric basis for ρ, which means that ρ is symmetrizable. □

3.3. Irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$

We will now describe the method devised by Nobs and Wolfart for constructing congruence representations of $\mathrm{SL}_2(\mathbb{Z})$. We refer the reader to [39, 40] for full details. In this section we will prove a number of results about said representations and then use them to prove Theorem 3.1.10.

3.3.1. Nobs–Wolfart quadratic modules

Fix some prime p and positive integer λ. Throughout, we denote $A_\mu \coloneqq \mathbb{Z}/p^\mu\mathbb{Z}$. To construct irreducible representations of $\mathrm{SL}_2(A_\lambda)$ (or, equivalently, congruence representations of $\mathrm{SL}_2(\mathbb{Z})$ with level p^λ) we consider the types of quadratic modules (M, Q) described in Table 3.1, wherein M is an A_λ-module (see [39, Def. 3]).

Table 3.1. Types of quadratic modules with at most two elementary divisors.

Type	p^λ	M	Q	Other parameters
D_{p^λ}	$\lambda \geq 1$	$A_\lambda \oplus A_\lambda$	$\dfrac{xy}{p^\lambda}$	
N_{p^λ}	$p = 2$ $\lambda \geq 1$	$A_\lambda \oplus A_\lambda$	$\dfrac{x^2 + xy + y^2}{2^\lambda}$	
	p odd $\lambda \geq 1$	$A_\lambda \oplus A_\lambda$	$\dfrac{x^2 + xy + \frac{1+t}{4}y^2}{p^\lambda}$	$t \in \mathbb{N}$, $(\frac{-t}{p}) = -1$ $t \equiv 3 \mod 4$
$R^\sigma_{p^\lambda}(r,t)$	$p = 2$ $\lambda \geq 2$	$A_{\lambda-1} \oplus A_{\lambda-\sigma-1}$	$\dfrac{r(x^2 + 2^\sigma t y^2)}{2^\lambda}$	$0 \leq \sigma \leq \lambda - 2$ $r, t \in \mathbb{N}$ and odd
	p odd $\lambda \geq 2$	$A_\lambda \oplus A_{\lambda-\sigma}$	$\dfrac{r(x^2 + p^\sigma t y^2)}{p^\lambda}$	$1 \leq \sigma \leq \lambda - 1$ $r, t \in \{1, u\}$
$R_{p^\lambda}(r)$	p odd $\lambda \geq 1$	A_λ	$\dfrac{rx^2}{p^\lambda}$	$r \in \{1, u\}$

Here u is a fixed quadratic nonresidue mod p. In view of the number of cyclic factors of M, we will call type $R_{p^\lambda}(r)$ a *unary* quadratic module and all the others *binary* quadratic modules. Type $R^{\lambda-2}_{2^\lambda}(r,t)$, which we will call the *extremal* case, is of particular interest: the second factor of M is simply $\mathbb{Z}/2\mathbb{Z}$, which has implications for the structure of $\mathrm{Aut}(M, Q)$ (see the appendix).

We equip each choice of M with a ring structure. For types D_{p^λ} and $R_{p^\lambda}(r)$, we use the natural ring structure. For the others, we identify M with a quotient ring via the mapping $(x, y) \mapsto x + Xy$, with X defined as follows:

- for type N_{2^λ}, let $X := \frac{1}{2}(1 + \sqrt{-3})$, and then $M := A_\lambda \oplus A_\lambda \cong \mathbb{Z}[X]/(2^\lambda)$,
- for type N_{p^λ} with p odd, let $X := \frac{1}{2}(1+\sqrt{-t})$, and then $M := A_\lambda \oplus A_\lambda \cong \mathbb{Z}[X]/(p^\lambda)$,
- for type $R^\sigma_{2^\lambda}(r,t)$, let $X := \sqrt{-2^\sigma t}$, and then $M := A_{\lambda-1} \oplus A_{\lambda-\sigma-1} \cong \mathbb{Z}[X]/(2^{\lambda-\sigma-1}X)$,
- for type $R^\sigma_{p^\lambda}(r,t)$ with p odd, let $X := \sqrt{-p^\sigma t}$, and then $M := A_\lambda \oplus A_{\lambda-\sigma} \cong \mathbb{Z}[X]/(p^{\lambda-\sigma}X)$.

The A_λ-module M then inherits the multiplication and complex conjugation of the quotient ring, as well as the norm (denoted Nm) of $\mathbb{Z}[X]$. In particular, for N_{p^λ}, we have $Q(x,y) = \mathrm{Nm}(x,y)/p^\lambda$; for $R^\sigma_{p^\lambda}(r,t)$, we have $Q(x,y) = r \cdot \mathrm{Nm}(x,y)/p^\lambda$.

For all of the above types, the projective Weil representation $W(M,Q)$ described in Definition 3.2.3 is in fact a linear representation of $\mathrm{SL}_2(A_\lambda)$ [39, §2].

The structure of $\mathrm{Aut}(M,Q)$ for each of these representation types is as follows:

Proposition 3.3.1. *Let (M,Q) be a quadratic module of one of the types given in Table 3.1. Then we may define a group homomorphism* $\det : \mathrm{Aut}(M) \to A_\lambda^\times$ *(except for type $R^\sigma_{p^\lambda}$, where the codomain is $A^\times_{\lambda-\sigma-1}$ for $p = 2$ and $A^\times_{\lambda-\sigma}$ otherwise). By abuse of notation, we write* det *for the restriction* $\det|_{\mathrm{Aut}(M,Q)}$. *Then:*

- $\mathfrak{C} \coloneqq \mathrm{Im}(\det)$ *is trivial in the extremal case, and is otherwise equal to $\langle -1 \rangle$.*
- *The subgroup*

  $$\mathfrak{A} \coloneqq \ker(\det) = \{\omega \in \mathrm{Aut}(M) \mid Q(\omega x) = Q(x) \text{ for all } x \in M \text{ and } \det(\omega) = 1\}$$

  is abelian and satisfies $[\mathrm{Aut}(M,Q) : \mathfrak{A}] = |\mathfrak{C}| \leq 2$.
- *The short exact sequence*

  $$1 \longrightarrow \mathfrak{A} \hookrightarrow \mathrm{Aut}(M,Q) \xrightarrow{\det} \mathfrak{C} \longrightarrow 1$$

  is right-split; as such, $\mathrm{Aut}(M,Q) \cong \mathfrak{A} \rtimes \mathfrak{C}$. *In the extremal case,* $\mathrm{Aut}(M,Q) \cong \mathfrak{A}$.

The proof of Proposition 3.3.1, the explicit definitions for det, and a deeper investigation of the structure of $\mathrm{Aut}(M,Q)$ and $\mathfrak{A}$ are given in the appendix. Note that, when $\mathfrak{C}$ is not trivial, finding a section for det amounts to choosing $\kappa \in \mathrm{Aut}(M,Q)$ such that $\mathrm{ord}(\kappa) = 2$ and $\det(\kappa) = -1$. The subgroup $\mathfrak{A}$ and corresponding involution κ will be highly relevant in the upcoming sections: we will generally view elements of $\mathrm{Aut}(M,Q)$ as either ω or $\kappa \circ \omega$, where $\omega \in \mathfrak{A}$.

3.3.2. Standard irreducible representations

The most prominent representations of $\mathrm{SL}_2(A_\lambda)$ arise in a standard way from the binary quadratic modules (types D_{p^λ}, N_{p^λ}, and $R^\sigma_{p^\lambda}(r,t)$). To address these, we will use the following lemma.

Lemma 3.3.2. *Let (M,Q) be a binary quadratic module. For any $\omega \in \mathfrak{A}$, $(\kappa \circ \omega)^2 = \mathrm{id}$.*

Proof. Indeed, for type D_{p^λ}, we have

$$(\kappa \circ \omega)^2(x,y) = \kappa(\omega(\omega y, \omega^{-1}x)) = (x,y)$$

for all $(x,y) \in M$. For type N_{p^λ} or $R^\sigma_{p^\lambda}(r,t)$, we have $\overline{\omega} = \omega^{-1}$ and thus

$$(\kappa \circ \omega)^2(a) = \kappa(\omega(\overline{\omega}\,\overline{a})) = a$$

for all $a \in M$. Incidentally, the extremal case has $\kappa = \mathrm{id}$, and it is easy to show that $\mathfrak{A}$ has exponent 2; the condition $(\kappa \circ \omega)^2 = \mathrm{id}$ follows trivially. □

Characters of $\mathfrak{A}$ naturally give rise to subrepresentations of $W(M,Q)$ (see Definition 3.2.3). More precisely:

Definition 3.3.3. Denote by $\hat{\mathfrak{A}}$ the character group of $\mathfrak{A}$. Then, for any $\chi \in \hat{\mathfrak{A}}$,

$$V^\chi := \{f \in \mathbb{C}^M \mid f(\omega a) = \chi(\omega) \cdot f(a) \text{ for all } a \in M \text{ and } \omega \in \mathfrak{A}\} \tag{3.3}$$

is an $\mathrm{SL}_2(A_\lambda)$-invariant subspace of V. The restriction of $W(M,Q)$ to V^χ is denoted by $W(M,Q,\chi)$.

Using (3.3) and Lemma 3.3.2, it is straightforward to verify that φ_κ (as defined in Section 3.2.2) maps V^χ to $V^{\overline{\chi}}$. In fact, $W(M,Q,\chi)$ is equivalent to $W(M,Q,\overline{\chi})$ via φ_κ.

A basis for V^χ can be chosen as follows (cf. [40]). For any $\chi \in \hat{\mathfrak{A}}$ and $a \in M$, define

$$\tilde{f}_a^\chi := \sum_{\varepsilon \in \mathfrak{A}} \chi(\varepsilon)\, \delta_{\varepsilon a} \ .$$

Clearly, $\tilde{f}_a^\chi \in V^\chi$. Whenever $\tilde{f}_a^\chi \neq 0$ (which occurs if and only if $\mathrm{Stab}(a) \subseteq \ker(\chi)$), define

$$f_a^\chi := \frac{\tilde{f}_a^\chi}{\|\tilde{f}_a^\chi\|} \ .$$

Let θ be a complete set of representatives for the orbits of $\mathfrak{A}$ on M chosen so that, for each $a \in \theta$ with $\kappa a \notin \mathfrak{A}a$, we have $\kappa a \in \theta$. Define

$$\theta^\chi := \theta \cap \{a \in M \mid \mathrm{Stab}(a) \subseteq \ker(\chi)\} \ .$$

By Lemma 3.3.2, $\mathrm{Stab}(\kappa a) = \mathrm{Stab}(a)$ for any $a \in M$, so any pairs $\{a, \kappa a\}$ lie in the same character space; that is, for each $a \in \theta^\chi$ with $\kappa a \notin \mathfrak{A}a$, we have $\kappa a \in \theta^\chi$. Moreover, since the $\mathfrak{A}$-orbits are disjoint, the set

$$\mathcal{B}^\chi := \{f_a^\chi \mid a \in \theta^\chi\}$$

is an orthonormal basis for V^χ.

Proposition 3.3.4. *Let (M, Q) be a binary quadratic module. Then, for any character $\chi \in \hat{\mathfrak{A}}$, the subrepresentation $W(M, Q, \chi)$ is symmetrizable.*

Proof. It suffices to show that the basis $\mathcal{B}^\chi$ defined above satisfies the conditions in Proposition 3.2.5.

Recall that for, any $a \in \theta^\chi$ and $\omega \in \mathfrak{A}$, we have $Q(\omega a) = Q(a)$. As such, (3.2) yields

$$\mathfrak{t} f_a^\chi = \frac{1}{\|\tilde{f}_a^\chi\|} \sum_{\omega \in \mathfrak{A}} \chi(\omega) \mathfrak{t}\, \delta_{\omega a} = \frac{1}{\|\tilde{f}_a^\chi\|} \sum_{\omega \in \mathfrak{A}} \chi(\omega) \mathbf{e}(Q(\omega a))\, \delta_{\omega a} = \mathbf{e}(Q(a)) f_a^\chi \ . \tag{3.4}$$

Thus, $\mathcal{B}^\chi$ is an eigenbasis for $\mathfrak{t}$.

Further, by definition and Lemma 3.3.2, for any $a \in \theta^\chi$, we have

$$\overline{\varphi}_\kappa(f_a^\chi) = \frac{1}{\|\tilde{f}_a^\chi\|} \sum_{\omega \in \mathfrak{A}} \chi(\omega^{-1})\, \delta_{\kappa\omega a} = \frac{1}{\|\tilde{f}_a^\chi\|} \sum_{\omega \in \mathfrak{A}} \chi(\omega^{-1})\, \delta_{\omega^{-1}\kappa a} = f_{\kappa a}^\chi \ , \tag{3.5}$$

noting that $\|\tilde{f}_a^\chi\| = \|\tilde{f}_{\kappa a}^\chi\|$. If $\kappa a \in \mathfrak{A}a$, then $\kappa a = \mu_a a$ for some $\mu_a \in \mathfrak{A}$. This implies $f_{\kappa a}^\chi = f_{\mu_a a}^\chi = \chi(\mu_a^{-1}) f_a^\chi$, and hence f_a^χ and $\overline{\varphi}_\kappa(f_a^\chi)$ are linearly dependent. Thus, if f_a^χ and $\overline{\varphi}_\kappa(f_a^\chi)$ are linearly independent, then $\kappa a \notin \mathfrak{A}a$. By the assumption on θ and the preceding discussion, $\kappa a \in \theta^\chi$, and so $f_{\kappa a}^\chi = \overline{\varphi}_\kappa(f_a^\chi) \in \mathcal{B}^\chi$. The statement now follows from Proposition 3.2.5. □

Remark 3.3.5. Let $\theta_1^\chi \coloneqq \{a \in \theta^\chi \mid \kappa a \in \mathfrak{A}a\}$. Then, by the proof of Proposition 3.2.5, there is a choice of subset $\theta_2^\chi \subset \theta^\chi$ such that $\theta_2^\chi \cap \kappa(\theta_2^\chi) = \varnothing$ and $\theta^\chi = \theta_1^\chi \sqcup \theta_2^\chi \sqcup \kappa(\theta_2^\chi)$. A symmetric basis of $W(M, Q, \chi)$ can then be chosen to be

$$\mathcal{S}^\chi = \Big\{ \sqrt{\chi(\mu_a^{-1})} f_a^\chi \;\Big|\; a \in \theta_1^\chi \Big\} \cup \Big\{ \frac{1}{\sqrt{2}} (f_a^\chi + f_{\kappa a}^\chi) \;\Big|\; a \in \theta_2^\chi \Big\} \cup \Big\{ \frac{i}{\sqrt{2}} (f_a^\chi - f_{\kappa a}^\chi) \;\Big|\; a \in \theta_2^\chi \Big\} \ ,$$

where the notation μ_a is as in the proof of Proposition 3.3.4.

When $\chi^2 = 1$ (i.e. $\chi = \overline{\chi}$), φ_κ becomes an auto-equivalence of V^χ, so if $\varphi_\kappa|_{V^\chi} \neq \mathrm{id}$, then $W(M, Q, \chi)$ admits a further decomposition into eigenspaces of φ_κ:

$$V_\pm^\chi \coloneqq \{ f \in V^\chi \mid f(\kappa a) = \pm f(a) \text{ for all } a \in M \} \ .$$

The corresponding subrepresentations are denoted by $W(M, Q, \chi)_\pm$.

Proposition 3.3.6. *Let (M, Q) be a binary quadratic module. Then, for any $\chi \in \hat{\mathfrak{A}}$ satisfying $\chi^2 = 1$ and $\varphi_\kappa|_{V^\chi} \neq \mathrm{id}$, the subrepresentations $W(M, Q, \chi)_\pm$ are both symmetrizable.*

Proof. It suffices to show that every element in the symmetric basis $\mathcal{S}^\chi$ for V^χ in Remark 3.3.5 is a ± 1 eigenvector of φ_κ, since this will imply that $\mathcal{S}_\pm^\chi \coloneqq V_\pm^\chi \cap \mathcal{S}^\chi$ are symmetric bases for $W(M, Q, \chi)_\pm$.

By (3.5), for any $a \in \theta^\chi$, we have $\varphi_\kappa(f_a^\chi) = \overline{f_{\kappa a}^\chi}$. Moreover, since $\chi^2 = 1$, we have $\overline{f_{\kappa a}^\chi} = f_{\kappa a}^\chi$, which means $\varphi_\kappa(f_a^\chi) = f_{\kappa a}^\chi$. Therefore, for any $a \in \theta_2^\chi$, it is readily seen that $\frac{1}{\sqrt{2}}(f_a^\chi + f_{\kappa a}^\chi) \in V_+^\chi$, and $\frac{i}{\sqrt{2}}(f_a^\chi - f_{\kappa a}^\chi) \in V_-^\chi$.

Finally, for any $a \in \theta_1^\chi$, we have $\kappa a = \mu_a a$ for some $\mu_a \in \mathfrak{A}$. In this case, the same computation as in the proof of Proposition 3.3.4 shows that $\varphi_\kappa(f_a^\chi) = f_{\kappa a}^\chi = \chi(\mu_a^{-1}) f_a^\chi$, which equals $\pm f_a^\chi$ (because $\chi^2 = 1$). This completes the proof. □

The question of which characters $\chi \in \hat{\mathfrak{A}}$ give rise to irreducible $W(M, Q, \chi)$ was answered as a remarkable result of [40]; we need the following definition for the statement.

Definition 3.3.7. Let (M, Q) be a binary quadratic module which is not extremal, and let $\mathfrak{A} \leq \mathrm{Aut}(M, Q)$ be as defined in Proposition 3.3.1. A character $\chi \in \hat{\mathfrak{A}}$ is called *primitive* if there exists some $\varepsilon \in \mathfrak{A}$ such that $\chi(\varepsilon) \neq 1$ and ε fixes pM pointwise.

Nobs and Wolfart showed that most primitive characters of $\mathfrak{A}$ give rise to irreducible representations. More precisely, they proved the following theorem.

Theorem 3.3.8 ([40, Hauptsatz 1])**.** *Let (M, Q) be a quadratic module of type D_{p^λ}, N_{p^λ}, or non-extremal $R^\sigma_{p^\lambda}(r, t)$, and let $\mathfrak{A} \leq \mathrm{Aut}(M, Q)$ be the corresponding subgroup. If $\chi \in \hat{\mathfrak{A}}$ is primitive and not an involution, then $W(M, Q, \chi)$ is an irreducible representation of $\mathrm{SL}_2(\mathbb{Z})$ with $\ell(W(M, Q, \chi)) = p^\lambda$.*

Moreover, suppose that (M_1, Q_1) and (M_2, Q_2) are two such quadratic modules, denote by $\mathfrak{A}_1$ and $\mathfrak{A}_2$ the corresponding subgroups, and let $\chi_1 \in \hat{\mathfrak{A}}_1$ and $\chi_2 \in \hat{\mathfrak{A}}_2$ be primitive characters that are not involutions. Then $W(M_1, Q_1, \chi_1) \cong W(M_2, Q_2, \chi_2)$ if, and only if:

- *(M_1, Q_1) and (M_2, Q_2) are equivalent as quadratic modules (i.e. there exists a group isomorphism $\eta : M_1 \to M_2$ with $Q_1(a) = Q_2(\eta(a))$ for all $a \in M_1$), and*
- *under that equivalence, we have either $\chi_1 = \chi_2$ or $\chi_1 = \overline{\chi_2}$.*

The case of $\chi^2 = 1$ is not directly covered by the theorem, but $W(M, Q, \chi)_\pm$ turns out to be irreducible in many cases. The precise details can be found in the complete list of irreducible representations of $\mathrm{SL}_2(A_\lambda)$ in [40, pp. 521-525]. When χ is not primitive, the resulting subrepresentation is usually reducible. The exceptions will be detailed in the next section.

Definition 3.3.9. Let p be a prime and λ a positive integer. We will call an irreducible representation ρ of $\mathrm{SL}_2(A_\lambda)$ a *standard irreducible representation* if there is some binary quadratic module (M, Q) and some character $\chi \in \hat{\mathfrak{A}}$ so that ρ is equivalent to $W(M, Q, \chi)$, or, when the latter is reducible, to one of $W(M, Q, \chi)_\pm$.

Combining Propositions 3.3.4 and 3.3.6, we have:

Proposition 3.3.10. *For any prime p and positive integer λ, every standard irreducible representation of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$ is symmetrizable.* □

3.3.3. Special irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/2^\lambda\mathbb{Z})$

There is a family of representations for $p = 2$ that are not covered by Proposition 3.3.10 and must therefore be handled separately. For a quadratic module (M, Q) of type $R^\sigma_{2^\lambda}(r, t)$ and $\chi \in \hat{\mathfrak{A}}$, we denote the representation $W(M, Q, \chi)$ of $\mathrm{SL}_2(\mathbb{Z}/2^\lambda\mathbb{Z})$ by $R^\sigma_{2^\lambda}(r, t, \chi)$. A representation of the form $R^\sigma_{2^\lambda}(r, t, \chi)$ is usually reducible when χ is not primitive, as expected. However, some cases with $\sigma = \lambda - 2$ or $\lambda - 3$ will contain a unique irreducible subrepresentation of level 2^λ that does not occur among the standard representations [40, Sec. 6]. We will call the irreducible representations appearing this way *special*; they are denoted by $R^\sigma_{2^\lambda}(r, t, \chi)_1$. We list all the special irreducible representations (up to equivalence), together with a choice of basis for each, in Table 3.2.

Table 3.2. Special irreducible representations.

Type	M	Basis in [40]
$R^0_{2^2}(1,3,\chi_1)_1$	$A_1 \oplus A_1$	$\delta_{(1,0)}$, $\delta_{(0,1)}$, $\delta_{(0,0)} - \delta_{(1,1)}$
$R^0_{2^3}(1,3,\chi_1)_1$	$A_2 \oplus A_2$	$\delta_{(0,0)} - \delta_{(2,2)}$, $\delta_{(2,0)} - \delta_{(0,2)}$, $\delta_{(1,0)} + \delta_{(-1,0)}$, $\delta_{(1,2)} - \delta_{(-1,2)}$, $\delta_{(0,1)} + \delta_{(0,-1)}$, $\delta_{(2,1)} + \delta_{(2,-1)}$
$R^2_{2^4}(r,3,\chi_1)_1$ $r \in \{1,3\}$	$A_3 \oplus A_1$	$\delta_{(1,0)} + \delta_{(-1,0)}$, $\delta_{(3,0)} + \delta_{(-3,0)}$, $\delta_{(1,1)} + \delta_{(-1,1)}$, $\delta_{(3,1)} + \delta_{(-3,1)}$, $\delta_{(0,0)} - \delta_{(4,0)}$, $\delta_{(0,1)} - \delta_{(4,1)}$
$R^2_{2^5}(r,1,\chi_1)_1$ $r \in \{1,3\}$	$A_4 \oplus A_2$	$\tilde{f}^{\chi_1}_a$ for $a \in \{1,3,5,7\} \times \{0,1\}$, $\tilde{f}^{\chi_1}_{(2,0)} - \tilde{f}^{\chi_1}_{(6,0)}$, $\tilde{f}^{\chi_1}_{(2,2)} - \tilde{f}^{\chi_1}_{(6,2)}$, $\tilde{f}^{\chi_1}_{(0,0)} - \tilde{f}^{\chi_1}_{(8,0)}$, $\tilde{f}^{\chi_1}_{(0,2)} - \tilde{f}^{\chi_1}_{(8,2)}$
$R^2_{2^5}(r,1,\chi_2)_1$ $r \in \{1,3\}$	$A_4 \oplus A_2$	$\tilde{f}^{\chi_2}_a$ for $a \in \{1,3,5,7\} \times \{0,1\}$, $\tilde{f}^{\chi_2}_{(4,0)}$, $\tilde{f}^{\chi_2}_{(4,2)}$, $\tilde{f}^{\chi_2}_{(2,0)} - \tilde{f}^{\chi_2}_{(6,0)}$, $\tilde{f}^{\chi_2}_{(2,2)} - \tilde{f}^{\chi_2}_{(6,2)}$
$R^4_{2^6}(r,t,\chi_1)_1$ $(r,t) \in \{1,3,5,7\} \times \{1,3\}$	$A_5 \oplus A_1$	$\tilde{f}^{\chi_1}_{(x,0)}$ for odd $1 \le x \le 15$, $\tilde{f}^{\chi_1}_{(0,0)} - \tilde{f}^{\chi_1}_{(16,0)}$, $\tilde{f}^{\chi_1}_{(4,0)} - \tilde{f}^{\chi_1}_{(12,0)}$, $\tilde{f}^{\chi_1}_{(2,1)} - \tilde{f}^{\chi_1}_{(14,1)}$, $\tilde{f}^{\chi_1}_{(6,1)} - \tilde{f}^{\chi_1}_{(10,1)}$
$R^{\lambda-3}_{2^\lambda}(r,t,\chi)_1$ $(r,t) \in \{1,3,5,7\} \times \{1,3\}$, $\lambda \ge 7, \chi \in \langle\chi_3\rangle$	$A_{\lambda-1} \oplus A_2$	See table at [40, p. 512]. The basis elements are of the form $\tilde{f}^{\chi}_a$ for some $a \in Y_0$, or $\tilde{f}^{\chi}_{(x,y)} - \tilde{f}^{\chi}_{(2^{\lambda-2}-x,y)}$ for some $(x,y) \in Y_1$.

In this table we use the following notation. Let χ_1 denote the trivial character. For $R^2_{2^5}(r,1)$, we have $\mathfrak{A} = \langle(-1,0)\rangle \times \langle(9,2)\rangle$, and χ_2 denotes the character determined by $\ker(\chi_2) = \langle(9,2)\rangle$. Finally, for $R^{\lambda-3}_{2^\lambda}(r,t)$ with $\lambda \ge 7$, we have $\mathfrak{A} = \langle(-1,0)\rangle \times \langle\alpha\rangle$, where $\alpha = (1 - 2^{\lambda-4}t - 2^{2\lambda-9}, 1)$, and χ_3 denotes the character determined by $\ker(\chi_3) = \langle(-1,0)\rangle$. The sets Y_0 and Y_1 are defined as the following disjoint unions:

$$Y_0 \coloneqq \{(x,0) \mid x \text{ odd}\} \sqcup \{(x,y) \mid y \in \{0,2\},\ x = 4 - 2y + 8j,\ 0 \le j \le 2^{\lambda-6} - 1\} ,$$

$$Y_1 \coloneqq \{(x,y) \mid y \in \{0,2\},\ x = 2y + 8j,\ 0 \le j \le 2^{\lambda-6} - 1\}$$
$$\sqcup \{(x,0) \mid x = 2 + 4k,\ 0 \le k \le 2^{\lambda-5} - 1\} .$$

We may now prove the following proposition.

Proposition 3.3.11. *Each of the special irreducible representations listed in Table 3.2 is symmetrizable.*

Proof. We will apply Lemma 3.2.4 to show that each basis in the table is a symmetric basis for the corresponding representation.

First, we observe that each basis in the table is an orthogonal basis. Indeed, this is clear for the first six rows, as δ_a and δ_b are orthogonal for all $a \neq b$. For the last row, it follows from the fact that Y_0 and Y_1 are disjoint.

Next, we claim that each basis element in the table is fixed by $\overline{\varphi}_\kappa$, as follows. Recall that $\kappa(x,y) = \overline{(x,y)} = (x,-y)$ for this type. It is immediate from this that each basis element in the first three rows is fixed by $\overline{\varphi}_\kappa$.

For $R^2_{2^5}(r,1)$, direct computation yields $(9,2) \cdot (x,1) = (x,-1)$ for each $x \in \{1,3,5,7\}$. If $\chi = \chi_1$ or χ_2, then $\chi^2 = 1$, so

$$\overline{\varphi}_\kappa(\tilde{f}^\chi_{(x,1)}) = \varphi_\kappa(\tilde{f}^\chi_{(x,1)}) = \tilde{f}^\chi_{(x,-1)} = \chi(9,2)\tilde{f}^\chi_{(x,1)} = \tilde{f}^\chi_{(x,1)}$$

for any $x \in \{1,3,5,7\}$. Moreover, since $M = A_4 \oplus A_2$, for any $(x,y) \in A_4 \times \{0,2\}$, we have

$$\overline{\varphi}_k(\tilde{f}^\chi_{(x,y)}) = \varphi_k(\tilde{f}^\chi_{(x,y)}) = \tilde{f}^\chi_{(x,-y)} = \tilde{f}^\chi_{(x,y)} \ .$$

This confirms that each basis element in the 4^{th} and 5^{th} rows is fixed by $\overline{\varphi}_\kappa$.

For $R^4_{2^6}(r,t)$, $M = A_5 \oplus A_1$, so κ acts trivially on M. Hence, for any $a \in M$, the function $\tilde{f}^{\chi_1}_a$ is fixed by $\overline{\varphi}_\kappa$. Since $\overline{\varphi}_\kappa$ is antilinear, it also fixes the other basis elements, as each is a $\mathbb{Z}$-linear combination of $\tilde{f}^{\chi_1}_a$.

Similarly, for $R^{\lambda-3}_{2^\lambda}(r,t)$ with $\lambda \geq 7$, we have $M = A_{\lambda-1} \oplus A_2$, so (again) $\kappa(x,y) = (x,y)$ for any $(x,y) \in A_{\lambda-1} \times \{0,2\}$. Therefore, for any $(x,y) \in A_{\lambda-1} \times \{0,2\}$, the function $\tilde{f}^\chi_{(x,y)}$ is fixed by $\overline{\varphi}_\kappa$. Since $\overline{\varphi}_\kappa$ is antilinear, it also fixes the rest of the basis elements.

Finally, we claim that each basis element in the table is an eigenvector for $\mathfrak{t}$. Indeed, for any quadratic module (M,Q) of type $R^\sigma_{2^\lambda}(r,t)$, (3.2) and (3.4) show that any

function of the form δ_a or $\tilde{f}_a^\chi$ for $a \in M$ and $\chi \in \hat{\mathfrak{A}}$ is an eigenvector of $\mathfrak{t}$ with eigenvalue $\mathbf{e}(Q(a))$. To show a basis element in Table 3.2 is an eigenvector of $\mathfrak{t}$, it suffices to show that the value of $Q(a)$ is the same for each index $a \in M$ among its summands. Recall that $Q(x,y) = r(x^2 + 2^\sigma t y^2)/2^\lambda \in \mathbb{Q}/\mathbb{Z}$ in this case. In particular, for $(x,y) \in M$, we have $Q(x,y) = Q(-x,y) = Q(x,-y)$. Our claim then follows from the computations below.

- For $R^0_{2^2}(1,3)$, $Q(0,0) = Q(1,1) = 0$.
- For $R^0_{2^3}(1,3)$, $Q(0,0) = Q(2,2) = 0$ and $Q(2,0) = Q(0,2) = \frac{1}{2}$.
- For $R^2_{2^4}(r,3)$, $Q(0,0) = Q(4,0) = 0$ and $Q(0,1) = Q(4,1) = \frac{3r}{4}$.
- For $R^2_{2^5}(r,1)$, $Q(2,0) = Q(6,0) = \frac{r}{8}$, $Q(2,2) = Q(6,2) = \frac{5r}{8}$, $Q(0,0) = Q(8,0) = 0$, and $Q(0,2) = Q(8,2) = \frac{r}{2}$.
- For $R^4_{2^6}(r,t,\chi)_1$, the basis elements are either of the form $\tilde{f}_a^{\chi_1}$ for some $a \in M$, or of the form $\tilde{f}^{\chi_1}_{(2x,y)} - \tilde{f}^{\chi_1}_{(16-2x,y)}$ for some $(2x,y) \in M$. As such, it suffices to verify the following equality for any $(2x,y) \in M$:

$$Q(16-2x,y) = \frac{r((16-2x)^2 + 16ty^2)}{64} = \frac{r(4x^2+16ty^2)}{64} = Q(2x,y)\ .$$

- For $R^{\lambda-3}_{2^\lambda}(r,t)$ with $\lambda \geq 7$, any element in Y_1 is of the form $(2u,v) \in A_{\lambda-1} \times \{0,2\}$ by definition. Now, we find

$$\begin{aligned} Q(2^{\lambda-2} - 2u, v) &= \frac{r((2^{\lambda-2}-2u)^2 + 2^{\lambda-3}tv^2)}{2^\lambda} \\ &= \frac{r(2^{2\lambda-4} - 2^\lambda u + 4u^2 + 2^{\lambda-3}tv^2)}{2^\lambda} \\ &= Q(2u,v)\ . \end{aligned}$$

In summary, each of the bases in Table 3.2 is an orthogonal eigenbasis for $\mathfrak{t}$ with basis elements all fixed by $\overline{\varphi}_\kappa$. Applying Lemma 3.2.4, we see that the normalization of each basis is a symmetric basis for the corresponding representation. □

3.3.4. Unary representations

Unary quadratic modules are those of type $R_{p^\lambda}(r)$, where p is an odd prime and $M = A_\lambda$ is cyclic. In this case, it is easy to see $\mathrm{Aut}(M, Q) = \{\pm 1\}$, and we define

$$\kappa : M \to M \ , \qquad a \mapsto -a \ .$$

The representation $W(M, Q)$, denoted simply by $R_{p^\lambda}(r)$, decomposes into two subrepresentations $R_{p^\lambda}(r)_\pm$ corresponding to the (± 1)-eigenspaces of φ_κ. For $\lambda = 1$, these are irreducible. For $\lambda \geq 2$, each contains a unique irreducible subrepresentation of level p^λ, denoted $(R_{p^\lambda}(r)_\pm)_1$. Specifically, [40, Satz 8] shows that

$$R_{p^\lambda}(r) \cong (R_{p^\lambda}(r)_+)_1 \oplus (R_{p^\lambda}(r)_-)_1 \oplus R_{p^{\lambda-2}}(r)$$

wherein $R_1(r)$ is the trivial representation. We will call the irreducible representations $R_p(r)_\pm$ $(\lambda = 1)$ and $(R_{p^\lambda}(r)_\pm)_1$ $(\lambda \geq 2)$ for any odd prime p the *unary irreducible representations* of $\mathrm{SL}_2(\mathbb{Z}/p^\lambda\mathbb{Z})$.

With some minor changes from [40],[8] an orthonormal basis for each unary irreducible representation can be chosen as follows. For $x \in M = A_\lambda$ and $\varepsilon \in \{\pm 1\}$, define

$$\tilde{f}_{x,\varepsilon} := \sqrt{\varepsilon}\delta_x + \overline{\sqrt{\varepsilon}}\delta_{-x} = \sqrt{\varepsilon}\delta_x + \overline{\varphi}_\kappa(\sqrt{\varepsilon}\delta_x) \qquad \text{and} \qquad f_{x,\varepsilon} := \frac{1}{\sqrt{2}}\tilde{f}_{x,\varepsilon} \ .$$

It is then straightforward to show that

$$\overline{\varphi}_\kappa(\tilde{f}_{x,\varepsilon}) = \tilde{f}_{x,\varepsilon} \qquad \text{and} \qquad \overline{\varphi}_\kappa(f_{x,\varepsilon}) = f_{x,\varepsilon} \ . \tag{3.6}$$

Also, by (3.2) and $Q(x) = Q(-x) = rx^2/p^\lambda$, both $\tilde{f}_{x,\varepsilon}$ and $f_{x,\varepsilon}$ are eigenvectors of $\mathbf{t}$.

[8] Cf. [40, p. 509]. With $g_{y,k,\varepsilon}$ as defined in loc. cit., here we have $h_{y,k,\varepsilon,\eta} = \frac{1}{2\sqrt{p}}(g_{y,k,\varepsilon} + \varepsilon\eta g_{(p^{\lambda-1}-y),k,\varepsilon})$.

Further, for $0 \leq y < p^{\lambda-1}$, $1 \leq k < p$, and $\varepsilon, \eta \in \{\pm 1\}$, define

$$h_{y,k,\varepsilon,\eta} \coloneqq \frac{1}{\sqrt{p}} \sum_{a \in A_1} \left(\sqrt{\eta} \zeta_p^{ka} + \overline{\sqrt{\eta} \zeta_p^{ka}} \right) \tilde{f}_{(py + ap^{\lambda-1}),\, \varepsilon} \ .$$

By (3.6) and the antilinearity of $\overline{\varphi}_\kappa$, we find that $h_{y,k,\varepsilon,\eta} = \overline{\varphi}_\kappa(h_{y,k,\varepsilon,\eta})$. Moreover, for any $\lambda \geq 2$ and any integers y and a,

$$Q(py + ap^{\lambda-1}) = \frac{r(py + ap^{\lambda-1})^2}{p^\lambda} = \frac{r((py)^2 + 2ap^\lambda + a^2 p^{2\lambda-2})}{p^\lambda} = \frac{r(py)^2}{p^\lambda} = Q(py) \in \mathbb{Q}/\mathbb{Z} \ .$$

Therefore, for $\lambda \geq 2$, $h_{y,k,\varepsilon,\eta}$ is an eigenvector of $\mathfrak{t}$. Then, denoting

$$\mathcal{F}_\varepsilon \coloneqq \left\{ f_{x,\varepsilon} \;\middle|\; x \in M^\times \text{ with } 1 \leq x \leq \frac{p^\lambda - 1}{2} \right\} \ ,$$
$$\mathcal{H}_\varepsilon \coloneqq \left\{ h_{y,k,\varepsilon,\eta} \;\middle|\; 1 \leq y \leq \frac{p^{\lambda-2} - 1}{2},\ 1 \leq k \leq \frac{p-1}{2},\ \eta \in \{\pm 1\} \right\} \ ,$$

we have the following orthonormal eigenbases for $\mathfrak{t}$:

- For $R_p(r)_+$, $\mathcal{B} \coloneqq \mathcal{F}_{+1} \cup \{\delta_0\}$.
- For $R_p(r)_-$, $\mathcal{B} \coloneqq \mathcal{F}_{-1}$.
- For $(R_{p^\lambda}(r)_\varepsilon)_1$ with $\lambda \geq 2$,

$$\mathcal{B} \coloneqq \mathcal{F}_\varepsilon \cup \mathcal{H}_\varepsilon \cup \left\{ \frac{1}{\sqrt{2}} h_{0,k,\varepsilon,\varepsilon} \;\middle|\; 1 \leq k \leq \frac{p-1}{2} \right\} \ .$$

In summary, each unary irreducible representation admits an orthonormal basis $\mathcal{B}$ that is an eigenbasis for $\mathfrak{t}$ and is fixed by $\overline{\varphi}_\kappa$ elementwise. We conclude by Lemma 3.2.4 that $\mathcal{B}$ is a symmetric basis. In other words, we have the following proposition.

Proposition 3.3.12. *Every unary irreducible representation is symmetrizable.* □

3.3.5. Proof of Theorem 3.1.10

In light of the decomposition described in Remark 3.2.1, Theorem 3.1.10 now follows immediately from the following proposition.

Proposition 3.3.13. *Let p be a prime and λ be a positive integer. Every irreducible complex representation of $\mathrm{SL}_2(A_\lambda)$ is symmetrizable.*

Proof. According to [40, Hauptsatz 2] and the tables in [40, pp. 521-525], every irreducible representation of $\mathrm{SL}_2(A_\lambda)$ is equivalent to one of the following:

- a standard irreducible representation,
- a special irreducible representation,
- a unary irreducible representation, or
- a tensor product of two representations of the above three types.

Since symmetrizability is preserved under taking tensor product (see Remark 3.1.4) and each of the first three types of representations is symmetrizable by Propositions 3.3.10, 3.3.11, and 3.3.12, we are done. □

Chapter 4. Applications

4.1. Corollaries of Theorem 3.1.10

Lemma 4.1.1. *Suppose ρ is a unitary complex representation of $\mathrm{SL}_2(\mathbb{Z})$ that is irreducible and symmetric. Then $\rho(\mathfrak{s}) = \tilde{s}$ or $i \cdot \tilde{s}$ for some real symmetric matrix $\tilde{s}$.*

Proof. Denote $s \coloneqq \rho(\mathfrak{s})$. Since ρ is unitary and s is symmetric, $s^{-1} = s^\dagger = \overline{s}$. Because $\mathfrak{s}^2$ is in the center of $\mathrm{SL}_2(\mathbb{Z})$, Schur's Lemma shows that $s^2 \in \mathbb{C} \cdot \mathrm{id}$. Since $s^4 = \mathrm{id}$, $s^2 = \pm \mathrm{id}$ and $\overline{s} = s^3$.

Combining these, we find that if $s^2 = \mathrm{id}$, then $\overline{s} = s$ and so $\tilde{s} \coloneqq s$ is real; otherwise, $(i \cdot s)^2 = \mathrm{id}$ and so $\tilde{s} \coloneqq -i \cdot s$ is real. □

Corollary 4.1.2. *Every irreducible complex congruence representation of $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to a representation ρ such that $\rho(\mathfrak{s}) = \tilde{s}$ or $i \cdot \tilde{s}$ for some real symmetric matrix $\tilde{s}$.*

Proof. This follows immediately Theorem 3.1.10 and Lemma 4.1.1. □

Corollary 4.1.3. *Let ρ be an irreducible complex congruence representation. Then $\rho(\mathfrak{t})$ has an eigenvalue of order $n = \mathrm{ord}(\rho(\mathfrak{t})) = \ell(\rho)$ and no eigenvalues of higher order.*

Proof. First, Theorem 3.1.10 lets us express ρ with respect to a symmetric basis. Since $n = \mathrm{ord}(\rho(\mathfrak{t}))$ is finite, every eigenvalue (i.e. diagonal entry) of $\rho(\mathfrak{t})$ is a finite root of unity.[1] It is then clear that

$$n = \mathrm{lcm}\left(\{\mathrm{ord}(\theta) \mid \theta \in \mathrm{spec}(\rho(\mathfrak{t}))\}\right) .$$

In particular, the statement holds if n is a prime power.

[1] Cf. Vafa's theorem.

Otherwise, as in Remark 3.2.1, we have

$$\rho \cong \bigoplus_{j=1}^{m} \hat{\rho}_j$$

where each $\hat{\rho}_j$ is irreducible with $\ell(\hat{\rho}_j) = p_j^{\lambda_j}$ and $n = \prod_{j=1}^{m} p_j^{\lambda_j}$. Applying the previous paragraph to each $\hat{\rho}_j$ gives, for each j, an eigenvalue $\theta_j \in \mathrm{spec}(\hat{\rho}_j(\mathfrak{t}))$ with order $p_j^{\lambda_j}$. Since all these orders are coprime, the order of $\theta_1 \otimes \cdots \otimes \theta_m \in \mathrm{spec}(\rho(\mathfrak{t}))$ will be n. □

Note that the converse of Corollary 4.1.3 is false — knowing the $\mathfrak{t}$-spectrum of ρ is not enough to determine whether ρ is congruence.

4.2. Reconstruction

4.2.1. Strategies for reconstruction

Suppose we are given a finite-dimensional complex congruence representation ρ. It is then reasonable to ask what information we can determine regarding any potential category or categories realizing ρ. That is, suppose some modular category $\mathscr{C}$ realizes ρ. If this leads to a contradiction — by implying there exists $a \in \mathrm{Irr}(\mathscr{C})$ with $\dim(a) = 0$ in violation of Remark 2.4.5, for instance — we can conclude that ρ must not be realizable. Otherwise, we can endeavor to reconstruct some of the data of $\mathscr{C}$, specifically the S and T matrices and fusion rules, from the data of ρ.

Theorem 3.1.10 is helpful in this task, as it allows us to assume the existence of a symmetric basis for ρ. Indeed, the techniques used in the proof of the theorem can be used to construct such a basis explicitly; we have implemented a `GAP` package, `SL2Reps` [36], which generates a symmetric basis for any given irreducible congruence representation ρ and outputs the corresponding matrices $\rho(\mathfrak{s})$ and $\rho(\mathfrak{t})$ (reducible representations may be handled by applying Remark 3.1.4). To relate the resulting data to that of our potential

category, we use the fact that two symmetric bases are always related by a real orthogonal matrix [33, Theorem 3.4]. In fact, we have the following description of said matrix.

Lemma 4.2.1. *Let ρ be a complex representation of $\mathrm{SL}_2(\mathbb{Z})$ and suppose $\mathcal{B}$ is a symmetric basis for ρ. Denote $s = \rho(\mathfrak{s})$ and $t = \rho(\mathfrak{t})$ with respect to $\mathcal{B}$. Now suppose $\mathcal{B}'$ is some other symmetric basis for ρ and let U be the orthogonal change-of-basis matrix from $\mathcal{B}$ to $\mathcal{B}'$, so that s^U is the matrix for $\rho(\mathfrak{s})$ with respect to $\mathcal{B}'$ and similarly for t. Then $U_{a,b} = 0$ for all $a, b \in \mathcal{B}$ with different t-eigenvalues. In other words, U is a block-diagonal matrix: the blocks correspond to the distinct eigenvalues of t, and each has size equal to the corresponding multiplicity.*

In particular, for any eigenvalue of multiplicity 1, let a be the corresponding eigenvector in $\mathcal{B}$; then $U_{a,b} = U_{b,a} = \pm\delta_{a,b}$ for all $b \in \mathcal{B}$.

Proof. Both t and t^U are diagonal matrices and have the same eigenvalues; as per Remark 3.1.4, we may assume without loss of generality that the eigenvalues are in the same order. This means t and t^U are in fact identical. Then $Ut = tU$, and the main statement follows.

For the last remark, the above gives $U_{a,b} = U_{b,a} = u_a\delta_{a,b}$ for some $u_a \in \mathbb{C}$; then $t_{a,a} = (t^U)_{a,a} = u_a^2 t_{a,a}$, so $u_a \in \{\pm 1\}$. □

4.2.2. Examples

Example 4.2.2. Consider $\rho := R_{7^1}(1)_-$, which has level 7 and degree 3. We have a symmetric basis $\mathcal{S} = \{f_{1,-}, f_{2,-}, f_{3,-}\}$ for ρ (as given in Section 3.3.4). We find the following matrices with respect to $\mathcal{S}$.

$$\rho(\mathfrak{s}) = \frac{i}{\sqrt{7}} \cdot \begin{bmatrix} \zeta_7^2 - \zeta_7^5 & -\zeta_7^3 + \zeta_7^4 & -\zeta_7 + \zeta_7^6 \\ -\zeta_7^3 + \zeta_7^4 & \zeta_7 - \zeta_7^6 & -\zeta_7^2 + \zeta_7^5 \\ -\zeta_7 + \zeta_7^6 & -\zeta_7^2 + \zeta_7^5 & -\zeta_7^3 + \zeta_7^4 \end{bmatrix} \qquad \rho(\mathfrak{t}) = \begin{bmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^4 & 0 \\ 0 & 0 & \zeta_7^2 \end{bmatrix}$$

Now suppose ρ is realized by some $\mathscr{C}$. Denote by $\mathcal{B}$ the basis given by $\mathrm{Irr}(\mathscr{C})$. We attempt to reconstruct the change-of-basis matrix U so that $\mathcal{S}' := \mathcal{S}^U = \mathcal{B}$. The eigenvalues of $\rho(\mathfrak{t})$ are all distinct, so by Lemma 4.2.1, U must be diagonal with diagonal entries in $\{\pm 1\}$.

We next consider which element of $\mathcal{S}'$ will correspond to the unit object in $\mathcal{B}$. We denote the elements of $\mathcal{S}'$ by x_1, x_2, x_3.

Let us first suppose x_1 is our unit object. Then $\chi_a(b) := \pm\left|\frac{\rho(\mathfrak{s})_{a,b}}{\rho(\mathfrak{s})_{a,1}}\right|$ for $a, b \in \mathcal{S}'$. To identify the Frobenius–Perron object $\mathbb{Y}$,[2] we calculate $D_a := \sum_{b\in\mathcal{S}'}\left|\frac{\rho(\mathfrak{s})_{a,b}}{\rho(\mathfrak{s})_{a,1}}\right|^2$ for each $a \in \mathcal{S}'$:

$$D_1 = 5 - \zeta_7^2 + 2\zeta_7^3 + 2\zeta_7^4 - \zeta_7^5 \approx 1.8412$$

$$D_2 = 5 + 2\zeta_7 - \zeta_7^3 - \zeta_7^4 + 2\zeta_7^6 \approx 9.2959$$

$$D_3 = 5 - \zeta_7 + 2\zeta_7^2 + 2\zeta_7^5 - \zeta_7^6 \approx 2.8629$$

We chose $x_1 = \mathbb{1}$, which makes $D_1 = \dim(\mathscr{C})$. As per Remark 2.3.8, the largest value we found, D_2, must be $\mathrm{FPdim}(\mathscr{C})$. We conclude that $x_2 = \mathbb{Y}$. In turn, this determines the entries of U, as all entries of the row of $\rho(\mathfrak{s})^U$ corresponding to $\mathbb{Y}$ must have the same sign (see Definition 2.3.3). Finally, we normalize $\rho(\mathfrak{s})^U$ and $\rho(\mathfrak{t})^U$ so that $\dim(\mathbb{1}) = \theta_{\mathbb{1}} = 1$:

$$S = \begin{bmatrix} 1 & -\zeta_7^2 - \zeta_7^5 & 1 + \zeta_7^3 + \zeta_7^4 \\ -\zeta_7^2 - \zeta_7^5 & -1 - \zeta_7^3 - \zeta_7^4 & 1 \\ 1 + \zeta_7^3 + \zeta_7^4 & 1 & \zeta_7^2 + \zeta_7^5 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_7^3 & 0 \\ 0 & 0 & \zeta_7 \end{bmatrix}.$$

The other two choices yield similar, but distinct, results. If x_2 is the unit object, we have $\chi_a(b) := \pm\left|\frac{\rho(\mathfrak{s})_{a,b}}{\rho(\mathfrak{s})_{a,2}}\right|$; repeating the above process, we find $\dim(\mathscr{C}) \approx 2.8629$, $\mathrm{FPdim}(\mathscr{C}) \approx 9.2959$, $\mathbb{Y} = x_1$, and

$$S = \begin{bmatrix} \zeta_7 + \zeta_7^6 & 1 + \zeta_7^2 + \zeta_7^5 & 1 \\ 1 + \zeta_7^2 + \zeta_7^5 & 1 & -\zeta_7 - \zeta_7^6 \\ 1 & -\zeta_7 - \zeta_7^6 & -1 - \zeta_7^2 - \zeta_7^5 \end{bmatrix} \qquad T = \begin{bmatrix} \zeta_7^4 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_7^5 \end{bmatrix}.$$

[2] As defined in Corollary 2.6.16.

Finally, if x_3 is the unit object, we have $\dim(\mathscr{C}) = \mathrm{FPdim}(\mathscr{C}) \approx 9.2959$ and $\mathbb{Y} = x_3 = \mathbb{1}$ (in other words, $\mathscr{C}$ will be pseudounitary with the canonical spherical structure ξ^+ in this case). Then

$$S = \begin{bmatrix} -1-\zeta_7-\zeta_7^6 & 1 & -\zeta_7^3-\zeta_7^4 \\ 1 & \zeta_7^3+\zeta_7^4 & 1+\zeta_7+\zeta_7^6 \\ -\zeta_7^3-\zeta_7^4 & 1+\zeta_7+\zeta_7^6 & 1 \end{bmatrix} \qquad T = \begin{bmatrix} \zeta_7^6 & 0 & 0 \\ 0 & \zeta_7^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The three different results differ only by permutation of the basis elements and Galois action. Specifically, the order-3 Galois action defined by $\zeta_7 \mapsto \zeta_7^2$ sends the first result to the third, then to the second, then back to the first.

We can now calculate the fusion structure by applying the Verlinde formula. The first pair (S, T) found above yields the following fusion matrices.

$$N_1 = \mathrm{id} \qquad N_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad N_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

We observe that all entries are non-negative integers, as required. The other two pairs give the same output (up to basis permutation).

Unfortunately, successfully "reconstructing" the S and T matrices and fusion rules in this way does not guarantee that a modular category with such data actually exists. However, modular categories realizing this ρ (and thus having the above fusion rules) do exist — they are well-known and were classified in [16].

Example 4.2.3. Consider the representation $\rho := R^1_{3^2}(1, 1, \chi_{1,1})$, which has level 9 and degree 4. Here $M \cong \mathbb{Z}/9\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}$, and

$$\mathfrak{A} \cong \{a \in M \mid \mathrm{Nm}(a) = 1\} = \langle \alpha \rangle \times \langle -1 \rangle$$

where $\alpha = (4,1)$ has order 3 and $-1 = (8,0)$ has order 2. The character $\chi := \chi_{1,1}$ is defined by $\alpha \mapsto \mathbf{e}(\frac{1}{3})$ and $-1 \mapsto \mathbf{e}(\frac{1}{2}) = -1$; it is primitive, so ρ is a standard irreducible representation (see Section 3.3.2).

We first construct a symmetric basis for ρ, as follows. We choose a complete set of representatives for the orbits of $\mathfrak{A}$ on $M^\times$, say $\theta = \{(1,0),(2,0),(4,0),(0,1)\}$. Each has trivial stabilizer in $\mathfrak{A}$, giving an orthonormal basis $\mathcal{B}^\chi = \{f^\chi_{(1,0)}, f^\chi_{(2,0)}, f^\chi_{(4,0)}, f^\chi_{(0,1)}\}$ for ρ. To symmetrize this, we observe that

$$\overline{\varphi}_\kappa(f^\chi_{(0,1)}) = f^\chi_{\kappa(0,1)} = f^\chi_{(0,2)} = -f^\chi_{(0,1)}$$

and all the other basis elements are fixed by $\overline{\varphi}_\kappa$. Thus, as in the proof of Proposition 3.2.5, a symmetric basis is $\mathcal{S} = \{f^\chi_{(1,0)}, f^\chi_{(2,0)}, f^\chi_{(4,0)}, i \cdot f^\chi_{(0,1)}\}$.

Applying (3.2) yields the following matrices with respect to $\mathcal{S}$.

$$\rho(\mathfrak{s}) = \frac{1}{3} \cdot \begin{bmatrix} \zeta_9^4 + \zeta_9^5 & -\zeta_9 - \zeta_9^8 & \zeta_9^2 + \zeta_9^7 & -\sqrt{3} \\ -\zeta_9 - \zeta_9^8 & \zeta_9^2 + \zeta_9^7 & -\zeta_9^4 - \zeta_9^5 & \sqrt{3} \\ \zeta_9^2 + \zeta_9^7 & -\zeta_9^4 - \zeta_9^5 & \zeta_9 + \zeta_9^8 & -\sqrt{3} \\ -\sqrt{3} & \sqrt{3} & -\sqrt{3} & 0 \end{bmatrix} \qquad \rho(\mathfrak{t}) = \begin{bmatrix} \zeta_9 & 0 & 0 & 0 \\ 0 & \zeta_9^4 & 0 & 0 \\ 0 & 0 & \zeta_9^7 & 0 \\ 0 & 0 & 0 & \zeta_3 \end{bmatrix}$$

Define U and $\mathcal{S}' := \mathcal{S}^U$ as in the previous example; again, the eigenvalues of $\rho(\mathfrak{t})$ are distinct, so U is diagonal with diagonal entries in $\{\pm 1\}$. This is enough to conclude that ρ is not realizable: the entries of $\rho(\mathfrak{s})^U$ must lie in $\mathbb{Q}(\zeta_{\mathrm{ord}(\rho(\mathfrak{t}))}) = \mathbb{Q}(\zeta_9)$ (see Theorem 2.6.18 and [33, Theorem 3.7]), but regardless of our choices for U, $\rho(\mathfrak{s})^U$ will have $\pm\sqrt{3}$ as an entry, and $\sqrt{3} \notin \mathbb{Q}(\zeta_9)$.

Alternatively, we can use the fusion rules to reach the same conclusion. Denote the elements of $\mathcal{S}'$ by $x_1, \ldots, x_4$. It is immediate that x_4 cannot be the unit object: regardless of the entries of U, we have $(\rho(\mathfrak{s})^U)_{4,4} = 0$, and this would imply $\dim(\mathbb{1}) = 0$. For the same

reason, $x_4 \neq \mathbb{Y}$.

Suppose then that x_1 is the unit object. We find

$$D_1 = 27 + 27\zeta_9^2 + 18\zeta_9^4 + 18\zeta_9^5 + 27\zeta_9^7 \approx 2.5481$$

$$D_2 = 27 - 18\zeta_9^2 + 9\zeta_9^4 + 9\zeta_9^5 - 18\zeta_9^7 \approx 3.8342$$

$$D_3 = 27 - 9\zeta_9^2 - 27\zeta_9^4 - 27\zeta_9^5 - 9\zeta_9^7 \approx 74.6177\,,$$

so we conclude that $x_3 = \mathbb{Y}$ and determine the entries of U as appropriate. However, applying the Verlinde formula to the resulting data yields the specious "fusion matrices"

$$N_1 = \mathrm{id} \qquad N_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 2 & 2 & \sqrt{3} \\ 0 & 2 & 1 & \sqrt{3} \\ 0 & \sqrt{3} & \sqrt{3} & 2 \end{bmatrix}$$

$$N_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & \sqrt{3} \\ 1 & 1 & 1 & \sqrt{3} \\ 0 & \sqrt{3} & \sqrt{3} & 1 \end{bmatrix} \qquad N_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & \sqrt{3} & \sqrt{3} & 2 \\ 0 & \sqrt{3} & \sqrt{3} & 1 \\ 1 & 2 & 1 & \sqrt{3} \end{bmatrix}.$$

These have non-integer values, so cannot come from any fusion category. The other choices of $\mathbb{1}$ have similar results, and hence are also impossible. We conclude that it is not possible for ρ to be realized by any modular category.

In contrast, the superficially-similar representation $R^1_{3^2}(1, 1, \chi_{1,0})$ turns out to be realizable. A category realizing it is described in [42, 5.3.10]; that paper classifies all modular categories of rank 4 or less.

Let us now consider a reducible representation. It was shown in [10] that $R_{p^1}(1)_+$ with p odd (which has level p and degree $\frac{1}{2}(p+1)$) is not realizable. Taking the direct sum

with another representation, however, may yield a realizable representation, as shown in the following example.

Example 4.2.4. Let $\rho_1 \coloneqq R_{5^1}(1)_+$ and $\rho_2 \coloneqq R^0_{2^2}(1,3,\chi_1)_1$ (see Sections 3.3.4 and 3.3.3 respectively) and consider $\rho \coloneqq \rho_1 \oplus \rho_2$. Recalling Remark 3.1.4, we have a symmetric basis

$$\mathcal{S} \coloneqq \Big\{(\delta_0, 0),\ \Big(0, \frac{\delta_{(0,0)} - \delta_{(1,1)}}{\sqrt{2}}\Big),\ (f_{1,+}, 0),\ (f_{2,+}, 0),\ (0, \delta_{(1,0)}),\ (0, \delta_{(0,1)})\Big\}$$

for ρ (cf. the symmetric bases for ρ_1 and ρ_2). We then have the following matrices with respect to $\mathcal{S}$.

$$\rho(\mathfrak{s}) = \frac{1}{10} \cdot \begin{bmatrix} 2\sqrt{5} & 0 & 2\sqrt{10} & 2\sqrt{10} & 0 & 0 \\ 0 & 0 & 0 & 0 & 5\sqrt{2} & 5\sqrt{2} \\ 2\sqrt{10} & 0 & -5-\sqrt{5} & 5-\sqrt{5} & 0 & 0 \\ 2\sqrt{10} & 0 & 5-\sqrt{5} & -5-\sqrt{5} & 0 & 0 \\ 0 & 5\sqrt{2} & 0 & 0 & -5 & 5 \\ 0 & 5\sqrt{2} & 0 & 0 & 5 & -5 \end{bmatrix} \quad \rho(\mathfrak{t}) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_5^4 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \end{bmatrix}$$

The $\rho(\mathfrak{t})$-eigenvalue 1 has multiplicity 2, meaning U is not necessarily diagonal in this case. Applying Lemma 4.2.1 and switching the first two basis elements if necessary, we may assume without loss of generality that the change-of-basis matrix U has the form

$$U = \begin{bmatrix} u & v & 0 & 0 & 0 & 0 \\ v & -u & 0 & 0 & 0 & 0 \\ 0 & 0 & e_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & e_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & e_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & e_6 \end{bmatrix} \tag{4.1}$$

where $e_3, e_4, e_5, e_6 \in \{\pm 1\}$ and $u, v \in \mathbb{R}$ with $u^2 + v^2 = 1$.

As usual, we denote the elements of $\mathcal{S}' \coloneqq \mathcal{S}^U$ by $x_1, \ldots, x_6$. We find

$$\rho(\mathfrak{s})^U = \frac{1}{10} \cdot \begin{bmatrix} 2u^2\sqrt{5} & 2uv\sqrt{5} & 2ue_3\sqrt{10} & 2ue_4\sqrt{10} & 5ve_5\sqrt{2} & 5ve_6\sqrt{2} \\ 2uv\sqrt{5} & 2v^2\sqrt{5} & 2ve_3\sqrt{10} & 2ve_4\sqrt{10} & -5ue_5\sqrt{2} & -5ue_6\sqrt{2} \\ 2ue_3\sqrt{10} & 2ve_3\sqrt{10} & -5-\sqrt{5} & e_3e_4(5-\sqrt{5}) & 0 & 0 \\ 2ue_4\sqrt{10} & 2ve_4\sqrt{10} & e_3e_4(5-\sqrt{5}) & -5-\sqrt{5} & 0 & 0 \\ 5ve_5\sqrt{2} & -5ue_5\sqrt{2} & 0 & 0 & -5 & 5e_5e_6 \\ 5ve_6\sqrt{2} & -5ue_6\sqrt{2} & 0 & 0 & 5e_5e_6 & -5 \end{bmatrix}$$

It is clear from the zeroes in this matrix that the only possible choices for $\mathbb{1}$ are x_1 and x_2.

Suppose $x_1 = \mathbb{1}$. By Theorem 2.6.18 and [33, Theorem 3.7], we know that

$$\frac{S_{3,2}}{S_{3,1}} = \pm\frac{(\rho(\mathfrak{s})^U)_{3,2}}{(\rho(\mathfrak{s})^U)_{3,1}} = \pm\frac{2ve_3\sqrt{10}}{2ue_3\sqrt{10}} = \pm\frac{v}{u}$$

and

$$\frac{S_{5,2}}{S_{5,1}} = \pm\frac{(\rho(\mathfrak{s})^U)_{5,2}}{(\rho(\mathfrak{s})^U)_{5,1}} = \pm\frac{-5ue_5\sqrt{2}}{5ve_5\sqrt{2}} = \mp\frac{u}{v}$$

must lie in $\mathbb{Z}[\zeta_{\mathrm{ord}(\rho(\mathfrak{t}))}] = \mathbb{Z}[\zeta_{20}]$. As u and v are real, the only possibility is that $u/v = \pm 1$, and since $u^2 + v^2 = 1$, we conclude that $u, v \in \{\pm 1/\sqrt{2}\}$. We write $u = e_1/\sqrt{2}$, $v = e_2/\sqrt{2}$ with $e_1, e_2 \in \{\pm 1\}$:

$$\rho(\mathfrak{s})^U = \frac{1}{10} \cdot \begin{bmatrix} \sqrt{5} & e_1e_2\sqrt{5} & 2e_1e_3\sqrt{5} & 2e_1e_4\sqrt{5} & 5e_2e_5 & 5e_2e_6 \\ e_1e_2\sqrt{5} & \sqrt{5} & 2e_2e_3\sqrt{5} & 2e_2e_4\sqrt{5} & -5e_1e_5 & 5e_1e_6 \\ 2e_1e_3\sqrt{5} & 2e_2e_3\sqrt{5} & -5-\sqrt{5} & e_3e_4(5-\sqrt{5}) & 0 & 0 \\ 2e_1e_4\sqrt{5} & 2e_2e_4\sqrt{5} & e_3e_4(5-\sqrt{5}) & -5-\sqrt{5} & 0 & 0 \\ 5e_2e_5 & -5e_1e_5 & 0 & 0 & -5 & 5e_5e_6 \\ 5e_2e_6 & -5e_1e_6 & 0 & 0 & 5e_5e_6 & -5 \end{bmatrix}$$

Now, as $x_1 = \mathbb{1}$, we calculate $D_1 = D_2 = 20$: either x_1 or x_2 could be $\mathbb{Y}$. If we

choose $x_1 = \mathbb{1} = \mathbb{Y}$, we have

$$S = \begin{bmatrix} 1 & 1 & 2 & 2 & \sqrt{5} & \sqrt{5} \\ 1 & 1 & 2 & 2 & -\sqrt{5} & -\sqrt{5} \\ 2 & 2 & -1-\sqrt{5} & -1+\sqrt{5} & 0 & 0 \\ 2 & 2 & -1+\sqrt{5} & -1-\sqrt{5} & 0 & 0 \\ \sqrt{5} & -\sqrt{5} & 0 & 0 & -\sqrt{5} & \sqrt{5} \\ \sqrt{5} & -\sqrt{5} & 0 & 0 & \sqrt{5} & -\sqrt{5} \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_5^4 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \end{bmatrix}.$$

On the other hand, if $x_2 = \mathbb{Y}$,

$$S = \begin{bmatrix} 1 & 1 & 2 & 2 & -\sqrt{5} & -\sqrt{5} \\ 1 & 1 & 2 & 2 & \sqrt{5} & \sqrt{5} \\ 2 & 2 & -1-\sqrt{5} & -1+\sqrt{5} & 0 & 0 \\ 2 & 2 & -1+\sqrt{5} & -1-\sqrt{5} & 0 & 0 \\ -\sqrt{5} & \sqrt{5} & 0 & 0 & -\sqrt{5} & \sqrt{5} \\ -\sqrt{5} & \sqrt{5} & 0 & 0 & \sqrt{5} & -\sqrt{5} \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_5^4 & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \end{bmatrix}.$$

We observe that, in both cases, $\mathscr{C}$ is pseudounitary and weakly-integral (because $\mathrm{FPdim}(\mathscr{C}) = \dim(\mathscr{C}) = 20 \in \mathbb{Z}$), but is not integral (because, for example, $\mathrm{FPdim}(x_5) = \sqrt{5} \notin \mathbb{Z}$). Note that the first pair is the case with the canonical spherical structure described in Section 2.4.9. Both pairs produce the fusion matrices

$$N_1 = \mathrm{id} \qquad N_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad N_3 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$N_4 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad N_5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \quad N_6 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

On the other hand, if we choose $x_2 = \mathbb{1}$, then there is no way to choose the other unknowns consistently — we ensured that $x_1 = \mathbb{1}$ by our assumption in (4.1).

These fusion rules (and the most well-known category having them) are called $\mathrm{SO}(5)_2$. The family of modular categories with $\mathrm{SO}(p)_2$ fusion rules, where p is an odd prime, are known as *metaplectic modular categories*. Such categories were classified in [2]; explicit fusion rules may be found in [48, Section 4.2.1], and from these we can see that the metaplectic modular categories with $p = 5$ do in fact realize ρ.

4.3. Semiregular modular categories

4.3.1. Galois orbits

Let $\mathscr{C}$ be a modular category over $\mathbb{C}$ and consider the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. As described in Definition 2.6.17, we have an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Irr}(\mathscr{C})$; to wit, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ corresponds to $\hat{\sigma} \in \mathrm{Sym}(\mathrm{Irr}(\mathscr{C}))$ with $\chi_{\hat{\sigma}(a)} = \sigma(\chi_a)$ for all $a \in \mathrm{Irr}(\mathscr{C})$. We denote by $G_{\mathscr{C}}$ the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Sym}(\mathrm{Irr}(\mathscr{C}))$; when unambiguous, we will just write G. The set of G-orbits in $\mathrm{Irr}(\mathscr{C})$ is denoted $\mathrm{Orb}(\mathscr{C})$ and will be the focus of this chapter. The G-orbit of a simple object $a \in \mathrm{Irr}(\mathscr{C})$ is denoted

$$G \cdot a \coloneqq \{\hat{\sigma}(a) \mid \sigma \in G\} = \{b \in \mathrm{Irr}(\mathscr{C}) \mid \chi_b = \sigma(\chi_a) \text{ for some } \sigma \in G\} \ .$$

Let ρ be one of the MC representations of $\mathscr{C}$ and (s, t) the corresponding normalized modular data (see Definition 3.1.2). In light of Theorem 3.1.10, we may assume ρ is a matrix representation with respect to some symmetric basis; t is then diagonal, so for brevity we write $t_a \coloneqq t_{a,a}$ for $a \in \mathrm{Irr}(\mathscr{C})$. Recall that each t_a is a root of unity by Vafa's Theorem. The level of ρ is $n \coloneqq \mathrm{ord}(t)$, so s and t are matrices over $\mathbb{Q}_n$ ([9, Theorem II]; cf. Theorem 2.6.18). The action of G therefore factors through $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$,

and it suffices to consider the action of this finite subgroup.

Lemma 4.3.1 ([38, Eqn. 5.19])**.** *For each $\sigma \in G$, we have*

$$\sigma^2(t_a) = t_{\hat{\sigma}(a)}$$

for all $a \in \mathrm{Irr}(\mathscr{C})$. Moreover, there exists a sign function $\iota_\sigma : \mathrm{Irr}(\mathscr{C}) \to \{\pm 1\}$ so that

$$\sigma(s_{a,b}) = \iota_\sigma(a) \cdot s_{\hat{\sigma}(a),b} = \iota_\sigma(b) \cdot s_{a,\hat{\sigma}(b)}$$

for all $a, b \in \mathrm{Irr}(\mathscr{C})$.

Definition 4.3.2. The *quadratic orbit* of $\alpha \in \overline{\mathbb{Q}}$ is

$$G^2 \cdot \alpha = \{\sigma^2(\alpha) \mid \sigma \in G\} \ .$$

In particular, for $k \in \mathbb{Z}^+$ and m coprime to k,

$$G^2 \cdot \zeta_k^m = \{\zeta_k^{j^2 m} \mid j \in (\mathbb{Z}/q\mathbb{Z})^\times \text{ with } j < \frac{k}{2}\}$$

Corollary 4.3.3. *If $a, b \in \mathrm{Irr}(\mathscr{C})$ lie in the same G-orbit, then t_a and t_b have the same order (as roots of unity) and lie in the same quadratic orbit.*

Also, for any $\alpha \in \mathrm{spec}(t)$, any element in the quadratic orbit of α will have the same multiplicity as α. The number of quadratic orbits present in $\mathrm{spec}(t)$ *is less than or equal to* $|\mathrm{Orb}(\mathscr{C})|$.

Proof. For the first part, write $t_a = \zeta_k^m$ with $k = \mathrm{ord}(t_a)$ and m coprime to k. Let $\sigma \in G$ be the element so that $b = \hat{\sigma}(a)$. As σ is a Galois action, it must send $\zeta_k \mapsto \zeta_k^j$ for j coprime to k. We then apply Lemma 4.3.1 to find $t_b = \sigma^2(t_a) = \zeta_k^{j^2 m}$.

Next, consider some $\alpha \in \mathrm{spec}(t)$ and denote its multiplicity by $m(\alpha)$. Then $m(\alpha) = \sum_{O \in \mathrm{Orb}(\mathscr{C})} m_O(\alpha)$ where $m_O(\alpha)$ is the multiplicity when restricting to the elements of the

orbit O. If $m_O(\alpha) = 0$, then Lemma 4.3.1 gives that $m_O(\sigma^2(\alpha)) = 0$ as well. Otherwise, there exists some $a \in O$ such that $t_a = \alpha$. Consider the subgroup

$$H_a := \{\sigma \in G \mid t_{\hat{\sigma}(a)} = t_a\} .$$

For any $\sigma \in G$, the orbit-stabilizer theorem yields

$$m_O(\alpha) = m_O(t_a) = \frac{|H_a|}{|H_a \cap \mathrm{Stab}_G(a)|} = \frac{|H_a|}{|H_a \cap \mathrm{Stab}_G(\hat{\sigma}(a))|} = m_O(t_{\hat{\sigma}(a)}) = m_O(\sigma^2(\alpha)) .$$

By summing over all orbits, we find that $m(\alpha) = m(\sigma^2(\alpha))$ for any $\sigma \in G$.

The last statement follows immediately from the first. □

Define $\mathrm{ord} : \mathrm{Orb}(\mathscr{C}) \to \mathbb{Z}^+$ by $\mathrm{ord}(G \cdot a) = \mathrm{ord}(t_a)$. The above corollary shows that this map does not depend on the choice of a within its orbit.

4.3.2. Semiregularity

Recall that a group action on a set X is called *fixed-point free* or *semiregular* if $\mathrm{Stab}(x)$ is trivial for all $x \in X$.

Definition 4.3.4. When the action of the group G on $\mathrm{Irr}(\mathscr{C})$ is semiregular, we say that $\mathscr{C}$ is *k-semiregular*, where $k = |\mathrm{Orb}(\mathscr{C})|$.

Lemma 4.3.5. *Let $\mathscr{C}$ be a k-semiregular modular category. Then:*

- *For any $a \in \mathrm{Irr}(\mathscr{C})$, $|G \cdot a| = |G|$. In particular, all orbits are of the same size, and the rank of $\mathscr{C}$ is $r_{\mathscr{C}} = k \cdot |G|$.*
- *$\mathbb{Q}(S) = \mathbb{Q}(\mathrm{dim}) := \mathbb{Q}(\{\mathrm{dim}(a) \mid a \in \mathrm{Irr}(\mathscr{C})\})$. This field is real, so S is a real matrix.*
- *Each object in $\mathrm{Irr}(\mathscr{C})$ is self-dual.*

Proof. For the first point, the orbit-stabilizer theorem gives $|G \cdot a| = |G|/|\mathrm{Stab}(a)| = |G|$.

Next, it is immediate that $\mathbb{Q}(\dim) \subseteq \mathbb{Q}(S)$. For the converse, we recall that $\mathbb{Q}(S)$ is an abelian extension,[3] so $\mathbb{Q}(S)$ is a Galois extension of $\mathbb{Q}(\dim)$ and we may consider the Galois group $H \coloneqq \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q}(\dim))$. Let $\eta \in H$ and observe that, for each $a \in \mathrm{Irr}(\mathscr{C})$,

$$\chi_{\hat{\eta}(\mathbb{1})}(a) = \eta(\chi_{\mathbb{1}}(a)) = \eta(\dim(a)) \ .$$

By definition, η fixes $\dim(a)$ for all $a \in \mathrm{Irr}(\mathscr{C})$. Thus, $\chi_{\hat{\eta}(\mathbb{1})} = \chi_{\mathbb{1}} = \dim$, which implies that $\hat{\eta}(\mathbb{1}) = \mathbb{1}$; since the action is fixed-point free, this implies $\hat{\eta} = \mathrm{id}$. As this holds for all of H, the action of H is trivial, and $\mathbb{Q}(S) = \mathbb{Q}(\dim)$ via Galois correspondence. That $\mathbb{Q}(\dim)$ is a real field follows from Corollary 2.4.7.

Finally, (2.21) gives $S^2 = \dim(\mathscr{C})C$. Since S is real and symmetric, the proof of Lemma 3.1.7 yields $S^{-1} = \frac{1}{\dim(\mathscr{C})}S^\dagger = \frac{1}{\dim(\mathscr{C})}S$, and we conclude that $C = \mathrm{id}$. □

4.3.3. 2-semiregular modular categories

It was shown in [38] that the 1-semiregular categories are precisely those where the action of G is transitive, and such categories were completely classified. Let us now consider the case with $|\mathrm{Orb}(\mathscr{C})| = 2$. While the classification of 2-semiregular categories remains incomplete, we can eliminate or classify certain cases. For example, we have the following.

Proposition 4.3.6. *Let $\mathscr{C}$ be a 2-semiregular modular category and ρ any of its MC representations. Then ρ cannot have any representation of type $D_{p^\lambda}(\chi)$ as a tensor component (as defined in Remark 3.2.1).*

Proof. Consider any semiregular category $\mathscr{C}$ and MC representation ρ thereof and suppose $\eta = D_{p^\lambda}(\chi)$ occurs as a tensor component of ρ. Let ρ' be the irreducible component of ρ

[3] Theorem 2.6.18.

containing η, so

$$\rho' \cong \eta \otimes \gamma$$

where $q := \ell(\gamma)$ is coprime to p. Since ρ is symmetric, we may assume that η is given with respect to the symmetric basis $\mathcal{B}^\chi$ constructed in Remark 3.3.5 and that γ is given with respect to some fixed symmetric basis $\mathcal{S}$, so

$$\{a \otimes b \mid a \in \mathcal{B}^\chi \text{ and } b \in \mathcal{S}\}$$

is a symmetric basis for ρ'. We may calculate that, with respect to $\mathcal{B}^\chi$,

$$\operatorname{spec}(\eta(\mathfrak{t})) = \{\zeta_{p^\lambda}^m \mid m \in \mathbb{Z}/p^\lambda\mathbb{Z}\}$$

with the multiplicity being 1 whenever $m \in (\mathbb{Z}/p^\lambda\mathbb{Z})^\times$ and 2 otherwise. In particular, we can find $x, y, z \in \mathcal{B}^\chi$ so that $[\eta(\mathfrak{t})]_x = 1$, $[\eta(\mathfrak{t})]_y = \zeta_{p^\lambda}$, and $[\eta(\mathfrak{t})]_z = \zeta_{p^\lambda}^u$, where u is a quadratic non-residue mod p^λ. Choose some arbitrary $b \in \mathcal{S}$ and note that $[\gamma(\mathfrak{t})]_b$ is a root of unity of the form ζ_q^v (where v is not necessarily coprime to q). Then

$$[\rho'(\mathfrak{t})]_{x\otimes b} = \zeta_q^v$$

$$[\rho'(\mathfrak{t})]_{y\otimes b} = \zeta_{p^\lambda} \cdot \zeta_q^v$$

$$[\rho'(\mathfrak{t})]_{z\otimes b} = \zeta_{p^\lambda}^u \cdot \zeta_q^v \ .$$

Now, since q is coprime to p, we can see that no two of the above three values will share a quadratic orbit. Applying Corollary 4.3.3, we find that $|\mathrm{Orb}(\mathscr{C})| \geq 3$. □

Now, for any congruence $\mathrm{SL}_2(\mathbb{Z})$ representation ρ, denote by $\Omega(\rho)$ the set of orders of roots of unity in $\operatorname{spec}(\rho(\mathfrak{t}))$.

Lemma 4.3.7. *Let $\mathscr{C}$ be 2-semiregular and choose an object $z \notin G \cdot \mathbb{1}$ so that*

$$\mathrm{Irr}(\mathscr{C}) = G \cdot \mathbb{1} \sqcup G \cdot z \ .$$

Denote $n_{\mathbb{1}} \coloneqq \mathrm{ord}(G \cdot \mathbb{1})$ and $n_z \coloneqq \mathrm{ord}(G \cdot z)$. Then either $n_z \mid n_{\mathbb{1}} = n$ or $n_{\mathbb{1}} \mid n_z = n$ (or both: $n_{\mathbb{1}} = n_z = n$).

Proof. As noted in the proof of Corollary 4.1.3, we have $n = \mathrm{lcm}(n_{\mathbb{1}}, n_z)$. If $n_{\mathbb{1}} = n_z$, the statement is therefore trivial. So, assume $n_{\mathbb{1}} \neq n_z$. We decompose ρ into its irreducible components, writing

$$\rho = \bigoplus_{j=1}^{m} \rho_j \ .$$

Suppose that some j exists such that $\Omega(\rho_j) = \{n_{\mathbb{1}}, n_z\}$, i.e. $\mathrm{spec}(\rho_j(\mathfrak{t}))$ contains a root of order $n_{\mathbb{1}}$ and another of order n_z. Then ρ_j is of level n. As a result, Corollary 4.1.3 guarantees that $\mathrm{spec}(\rho_j(\mathfrak{t}))$ contains a root of order n, and since $\mathrm{spec}(\rho_j(\mathfrak{t})) \subseteq \mathrm{spec}(t)$, the statement holds.

On the other hand, suppose that the above never occurs, which means that for each j either $\Omega(j) = \{n_{\mathbb{1}}\}$ or $\Omega(j) = \{n_z\}$. Rearranging the labels if necessary, we then have

$$\rho = \Big(\bigoplus_{j=1}^{\ell} \rho_j\Big) \oplus \Big(\bigoplus_{j=\ell+1}^{m} \rho_j\Big)$$

with the two summands having $\mathfrak{t}$-spectra $\{n_{\mathbb{1}}\}$ and $\{n_z\}$ respectively. This is, however, impossible: no MC representation can be isomorphic to the direct sum of two representations with disjoint $\mathfrak{t}$-spectra [6, Thm. 3.18]. □

This lemma immediately implies that either $\Omega(\rho) = \{n\}$ or $\Omega(\rho) = \{m, n\}$ with $m \mid n$, $m \neq n$. Let us consider the latter case. We will use the following minor result of the classification from [39, 40] that we discussed in Section 3.3:

Lemma 4.3.8. *Let η be an irreducible congruence representation of $\mathrm{SL}_2(\mathbb{Z})$. If none of η's tensor components are equivalent to a representation of type $D_{p^\lambda(\chi)}$, then*

$$\sum_{\substack{\alpha\in\mathrm{spec}(\eta(\mathfrak{t}))\\ \mathrm{ord}(\alpha)<\ell(\eta)}} \mathrm{mult}(\alpha) < \sum_{\substack{\xi\in\mathrm{spec}(\eta(\mathfrak{t}))\\ \mathrm{ord}(\xi)=\ell(\eta)}} \mathrm{mult}(\xi)\ .$$

In other words, if we include multiplicities, there are more $\mathfrak{t}$-eigenvalues of the highest order than of all other orders combined.

Proof. From the classification given in [39, 40] and calculation of (3.2), we can determine that the statement holds for every standard, special, and unary representation except $D_{p^\lambda(\chi)}$. It then extends to tensor products thereof, which covers all cases. □

Proposition 4.3.9. *Let $\mathscr{C}$ be a 2-semiregular modular category and ρ one of its MC representations, and suppose $\Omega(\rho) = \{m, n\}$ with $m \mid n$, $m \neq n$. Then ρ has at least one subrepresentation η with $\Omega(\eta) = \{m, n\}$ and at least one subrepresentation ν with $\Omega(\nu) = \{m\}$.*

Proof. We first note that if no subrepresentation η with $\Omega(\eta) = \{m, n\}$ exists, then we can use the same argument used in the proof of Lemma 4.3.7: we can decompose ρ as a direct sum of representations with disjoint spectra, which gives a contradiction. On the other hand, if no subrepresentation ν with $\Omega(\nu) = \{m\}$ exists, then by applying Lemma 4.3.8 (and noting that its condition is fulfilled because of Lemma 4.3.6), we have

$$|\{a \in \mathrm{Irr}(\mathscr{C}) \mid \mathrm{ord}(t_a) = m\}| < |\{a \in \mathrm{Irr}(\mathscr{C}) \mid \mathrm{ord}(t_a) = n\}|\ .$$

This is impossible, because there are only two orbits. Explicitly, all elements within a given orbit must have the same order by Corollary 4.3.3, so one of the above sets must be $G \cdot \mathbb{1}$ and the other $G \cdot z$. However, by Lemma 4.3.5, we have $|G \cdot \mathbb{1}| = |G \cdot z| = |G|$. □

Appendix. Structure of $\mathrm{Aut}(M,Q)$ and $\mathfrak{A}$

In this appendix we will consider in detail the structure of the group $\mathrm{Aut}(M,Q)$ and its abelian subgroup $\mathfrak{A}$ for the representation types described in Section 3.3.1. In particular, we will prove Proposition 3.3.1, which is repeated here for convenience:

Proposition 3.3.1. *Let (M,Q) be a quadratic module of one of the types given in Table 3.1. Then there is a group homomorphism $\det : \mathrm{Aut}(M) \to A_\lambda^\times$ (except for type $R^\sigma_{p^\lambda}$, where the codomain is $A^\times_{\lambda-\sigma-1}$ for $p=2$ and $A^\times_{\lambda-\sigma}$ otherwise). By abuse of notation, we write $\det$ for the restriction $\det|_{\mathrm{Aut}(M,Q)}$. Then:*

- $\mathfrak{C} \coloneqq \mathrm{Im}(\det)$ *is trivial in the extremal case, and is otherwise equal to $\langle -1\rangle$.*
- *The subgroup*

  $$\mathfrak{A} \coloneqq \ker(\det) = \{\omega \in \mathrm{Aut}(M) \mid Q(\omega x) = Q(x) \text{ for all } x \in M \text{ and } \det(\omega) = 1\}$$

  is abelian and satisfies $[\mathrm{Aut}(M,Q) : \mathfrak{A}] = |\mathfrak{C}| \leq 2$.
- *The short exact sequence*

  $$1 \longrightarrow \mathfrak{A} \hookrightarrow \mathrm{Aut}(M,Q) \xrightarrow{\det} \mathfrak{C} \longrightarrow 1$$

  is right-split; as such, $\mathrm{Aut}(M,Q) \cong \mathfrak{A} \rtimes \mathfrak{C}$. In the extremal case, $\mathrm{Aut}(M,Q) \cong \mathfrak{A}$.

We prove Proposition 3.3.1 by considering each type in turn. When $\mathfrak{C}$ is not trivial, our proof will hinge on finding an involution $\kappa \in \mathrm{Aut}(M,Q)$ with $\det(\kappa) = -1$, as this will define a section for $\det$ (as mentioned in Section 3.3.1). Let us first dispense with the unary case.

Lemma A.0.1. *For type $R_{p^\lambda}(r)$, $\mathrm{Aut}(M,Q) \cong \mathbb{Z}/2\mathbb{Z}$; that is, $\mathfrak{A}$ is trivial and $\kappa = -1$.*

Proof. Recall that type $R_{p^\lambda}(r)$ is only defined for $p \neq 2$. Here $M = A_\lambda$, so $\mathrm{Aut}(M) \cong A_\lambda^\times$; we define $\det = \mathrm{id}_{A_\lambda^\times}$.

For this case, $Q(x) = \frac{rx^2}{p^\lambda}$. Thus, an element $\alpha \in A_\lambda^\times$ lies in $\mathrm{Aut}(M,Q)$ if and only

if $r\alpha^2x^2 \equiv rx^2 \mod p^\lambda$ for all $x \in M$. We recall that r is coprime to p, so this implies $\alpha^2 \equiv 1 \mod p^\lambda$; since $p \neq 2$, we have only two solutions: $\alpha \equiv \pm 1 \mod p^\lambda$. Both clearly fix Q, confirming the statement. □

Lemma A.0.2. *For type D_{p^λ}, $\mathrm{Aut}(M,Q) \cong \mathfrak{A} \rtimes \langle\kappa\rangle$ with $\mathfrak{A} \cong A_\lambda^\times$ acting on M via $\alpha(x,y) = (\alpha^{-1}x, \alpha y)$ and $\kappa : (x,y) \mapsto (y,x)$.*

Proof. Since $M \cong A_\lambda \oplus A_\lambda$, we have $\mathrm{Aut}(M) = \mathrm{GL}_2(A_\lambda)$, the group of 2×2 matrices over A_λ with determinants in $A_\lambda^\times$. Let det be the standard determinant.

Now, an element $\omega = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{Aut}(M)$ stabilizes $Q(x,y) = \frac{xy}{p^\lambda}$ if and only if

$$Q(x,y) = \frac{xy}{p^\lambda} \equiv \frac{(ax+by)(cx+dy)}{p^\lambda} = Q(\omega(x,y)) \in \mathbb{Q}/\mathbb{Z} \ ,$$

or equivalently,

$$xy \equiv (ax+by)(cx+dy) = acx^2 + (ad+bc)xy + bdy^2 \mod p^\lambda \ , \tag{A.1}$$

for all $(x,y) \in M$. It is immediate that (A.1) implies

$$\begin{cases} 0 \equiv ac \mod p^\lambda \\ 0 \equiv bd \mod p^\lambda \\ 1 \equiv ac + bd + ad + bc \equiv ad + bc \mod p^\lambda \end{cases}$$

and vice versa. Hence, $\omega \in \mathrm{Aut}(M,Q)$ if and only if these three equations hold.

Assume then that $\omega \in \mathrm{Aut}(M,Q)$. We have $ac \equiv 0 \mod p^\lambda$, and this implies that either $a \equiv 0$ or $c \equiv 0$. Explicitly, if $a \not\equiv 0$ and $c \not\equiv 0$, then $p \mid a$ and $p \mid c$. Then, however, $p \mid (ad - bc)$, contradicting the invertibility of $\det(\omega)$. In the same way, either $b \equiv 0$ or $d \equiv 0$. However, if $a \equiv b \equiv 0$ or $a \equiv c \equiv 0$ or $b \equiv d \equiv 0$ or $c \equiv d \equiv 0 \mod p^\lambda$, then $ad - bc \equiv 0$, so these cases are impossible.

The remaining possibilities are $\omega = \left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]$ and $\omega = \left[\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right]$. Since $ad + bc \equiv 1$, we have two possible matrices for ω:

$$\begin{bmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{bmatrix} \qquad \text{or} \qquad \begin{bmatrix} 0 & \alpha^{-1} \\ \alpha & 0 \end{bmatrix} = \begin{bmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

with $\alpha \in A_\lambda^\times$. Conversely, both matrices clearly satisfy the three equations above, so this precisely comprises $\mathrm{Aut}(M, Q)$.

Clearly $\mathfrak{C} = \langle -1 \rangle$. We have $\mathfrak{A} = \left\{ \left[\begin{smallmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{smallmatrix}\right] \;\middle|\; \alpha \in A_\lambda^\times \right\}$, and κ acts as $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$; note that $\mathrm{ord}(\kappa) = 2$ and $\det(\kappa) = -1$. We conclude that $\mathrm{Aut}(M, Q) = \mathfrak{A} \rtimes \langle \kappa \rangle$ as required. □

Lemma A.0.3. *For type N_{p^λ}, $\mathrm{Aut}(M, Q) \cong \mathfrak{A} \rtimes \langle \kappa \rangle$ with $\mathfrak{A} \cong \{ (a, c) \in M \mid \mathrm{Nm}(a, c) = 1 \}$ acting on M by multiplication and $\kappa : (x, y) \mapsto \overline{(x, y)}$.*

Proof. As in Lemma A.0.2, $M = A_\lambda \oplus A_\lambda$, so $\mathrm{Aut}(M) = \mathrm{GL}_2(A_\lambda)$, and we use the standard determinant. In this case, however, M is equipped with a quotient ring structure, as described in Section 3.3.1. Explicitly, we have a norm $\mathrm{Nm}(a, c) = a^2 + ac + \dot{u}c^2 \in A_\lambda$ (where $\dot{u} = \frac{1+u}{4}$), and multiplication by $(a, c) \in M$ corresponds to the matrix $\left[\begin{smallmatrix} a & -\dot{u}c \\ c & a+c \end{smallmatrix}\right]$ (which has determinant $\mathrm{Nm}(a, c)$). Complex conjugation corresponds to $\kappa = \left[\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right]$, which has order 2 and determinant -1 as required.

An element $\omega = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{Aut}(M)$ fixes $Q(x, y) = \frac{\mathrm{Nm}(x,y)}{p^\lambda}$ if and only if

$$Q(x, y) = \frac{\mathrm{Nm}(x, y)}{p^\lambda} \equiv \frac{\mathrm{Nm}(ax + by, cx + dy)}{p^\lambda} = Q(\omega(x, y)) \in \mathbb{Q}/\mathbb{Z}$$

or, equivalently,

$$x^2 + xy + \dot{u}y^2 \equiv \mathrm{Nm}(a, c)x^2 + (2ab + ad + bc + 2\dot{u}cd)xy + \mathrm{Nm}(b, d)y^2 \mod p^\lambda$$

for all $(x, y) \in M$. As in Lemma A.0.2, we find that this is equivalent to

$$\begin{cases} 1 & \equiv \mathrm{Nm}(a, c) \mod p^\lambda & \text{(A.2a)} \\ \dot{u} & \equiv \mathrm{Nm}(b, d) \mod p^\lambda & \text{(A.2b)} \\ 1 & \equiv 2ab + ad + bc + 2\dot{u}cd \mod p^\lambda \ . & \text{(A.2c)} \end{cases}$$

It is worth handling the case $p = 2$, $\lambda = 1$ separately here. In this case, direct calculation shows that

$$\mathrm{Aut}(M, Q) = \mathrm{Aut}(M) \cong S_3 \ ,$$

generated by the order-3 element $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ and $\kappa = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. We therefore assume in the following that either $p \neq 2$ or $\lambda > 1$.

Suppose that $\omega = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{Aut}(M, Q)$. Then we claim that at least one of $v \coloneqq 2a + c$ and $w \coloneqq a + 2\dot{u}c$ is not divisible by p (and is hence invertible mod p^λ). Assume otherwise; then $(2w - v) \equiv uc \equiv (2\dot{u}v - w) \equiv ua \equiv 0 \mod p$. Recall that $p \nmid u$, so $a \equiv c \equiv 0 \mod p$, and so $\mathrm{Nm}(a, c) = a^2 + ac + \dot{u}c^2 \equiv 0 \mod p$, contradicting (A.2a).

Therefore, we assume first that $p \nmid v$. Multiplying (A.2b) by v^2 yields

$$\dot{u}v^2 \equiv v^2(b^2 + bd + \dot{u}d^2) \equiv (vb)^2 + vb \cdot vd + \dot{u}v^2d^2 \mod p^\lambda \ .$$

By (A.2c), we have $vb \equiv 1 - wd \mod p^\lambda$, so

$$0 \equiv (1 - wd)^2 + (1 - wd)vd + \dot{u}v^2d^2 - \dot{u}v^2 \mod p^\lambda \ .$$

Rewriting v and w in terms of a and c and expanding the right hand side of the above equation in powers of d, we have

$$0 \equiv (4\dot{u} - 1)\,\mathrm{Nm}(a, c)d^2 + (1 - 4\dot{u})cd + (1 - 4\dot{u})(1 - \mathrm{Nm}(a, c) + a^2 + ac) \mod p^\lambda \ .$$

By (A.2a) and the fact that $4\dot{u} - 1 = u$,

$$0 \equiv u(d^2 - cd - (a^2 + ac)) \mod p^\lambda \ .$$

Since u is invertible mod p^λ, we conclude that $0 \equiv (d - a - c)(d + a) \mod p^\lambda$.

Now, if $(d - a - c) \not\equiv 0 \mod p^\lambda$ and $(d + a) \not\equiv 0 \mod p^\lambda$, then p divides both of them. But then also $p \mid (d + a - (d - a - c)) = v$, a contradiction. Thus one must be equivalent to zero. If $d - a - c \equiv 0 \mod p^\lambda$, then we have $d \equiv a + c \mod p^\lambda$ and

$$\begin{aligned} vb &\equiv 1 - w(a + c) \mod p^\lambda \\ vb &\equiv (a + \dot{u}c)(2a + c) \\ b &\equiv a + \dot{u}c \ , \end{aligned}$$

while if $d + a \equiv 0 \mod p^\lambda$, we have $d \equiv -a \mod p^\lambda$ and

$$\begin{aligned} vb &\equiv 1 + wa \mod p^\lambda \\ vb &\equiv (-\dot{u}c)(2a + c) \\ b &\equiv -\dot{u}c \ . \end{aligned}$$

This results in two possible matrices for ω:

$$\begin{bmatrix} a & -\dot{u}c \\ c & a + c \end{bmatrix} \qquad \text{or} \qquad \begin{bmatrix} a & a + \dot{u}c \\ c & -a \end{bmatrix} = \begin{bmatrix} a & -\dot{u}c \\ c & a + c \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$$

for $(a, c) \in M$ with $N(a, c) = 1$.

On the other hand, suppose $p \nmid w$. Then, multiplying (A.2b) by w^2 and proceeding in the same way yields

$$0 \equiv (b + \dot{u}c)(b - a - \dot{u}c) \mod p^\lambda \ .$$

As before, if $(b + \dot{u}c) \not\equiv 0$ and $(b - a - \dot{u}c) \not\equiv 0$, then p divides both and hence also w, a contradiction. We therefore have $b \equiv -\dot{u}c$ or $b \equiv a + \dot{u}c$ and arrive at the same two matrices as above.

We can easily check that these two matrices satisfy (A.2a) – (A.2c) for any element $(a, c) \in M$ with norm 1. This confirms the statement. □

Lemma A.0.4. *For type $R^{\sigma}_{p^\lambda}(r, t)$ with $p \neq 2$ and $1 \leq \sigma \leq \lambda - 1$, $\mathrm{Aut}(M, Q) \cong \mathfrak{A} \rtimes \langle \kappa \rangle$ with $\mathfrak{A} \cong \{\ (a, c) \in M \mid \mathrm{Nm}(a, c) = 1\ \}$ acting on M by multiplication and $\kappa : (x, y) \mapsto \overline{(x, y)}$.*

Proof. Here $M = A_\lambda \oplus A_{\lambda-\sigma}$, so we must consider the definition of $\mathrm{Aut}(M)$ more carefully. Write M_1, M_2 for the cyclic factors of M. Any endomorphism $\omega : M \to M$ has the form

$$\omega(x, y) = (\omega_{1,1}(x) + \omega_{2,1}(y),\ \omega_{1,2}(x) + \omega_{2,2}(y))$$

where:

- $\omega_{1,1} \in \mathrm{Hom}(M_1, M_1) \cong A_\lambda$ acts as multiplication within A_λ.
- $\omega_{2,1} \in \mathrm{Hom}(M_2, M_1) \cong A_{\lambda-\sigma}$ has image lying in the unique subgroup of M_1 isomorphic to M_2, namely $\langle p^\sigma \rangle$. Thus, there is a unique $b \in A_{\lambda-\sigma}$ so that $\omega_{2,1}(y) = p^\sigma t(by)$ for all $y \in M_2$. Note that $p^\sigma t(by) \equiv p^\sigma t\hat{b}\hat{y} \mod p^\lambda$ for all lifts $\hat{b}$ and $\hat{y}$ (of b and y respectively) into A_λ. We will therefore use the notation $\hat{b}$ to refer to an arbitrary lift of b.
- $\omega_{1,2} \in \mathrm{Hom}(M_1, M_2) \cong A_{\lambda-\sigma}$ is defined uniquely by $c := \omega_{1,2}(1)$. Explicitly, $\omega_{1,2}(x) = c \cdot \pi(x)$ for all $x \in M_1$, where π is the canonical projection $A_\lambda \to A_{\lambda-\sigma}$.
- $\omega_{2,2} \in \mathrm{Hom}(M_2, M_2) \cong A_{\lambda-\sigma}$ acts as multiplication within $A_{\lambda-\sigma}$.

We therefore define

$$\Gamma := \{\ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mid a \in A_\lambda \text{ and } b, c, d \in A_{\lambda-\sigma}\ \}$$

with the action of Γ on M given by

$$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right](x, y) = (ax + p^\sigma t(by),\ c\pi(x) + dy) = (ax + p^\sigma t\hat{b}\hat{y},\ c\pi(x) + dy)\ .$$

Under this action, Γ is a monoid (with identity $\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$). To see this, we first observe that, for any $x \in A_\lambda$, we have $p^\sigma t(\pi(x)) \equiv p^\sigma tx \mod p^\lambda$; similarly, for any $y \in A_{\lambda-\sigma}$, we have $\pi(p^\sigma t\hat{y}) \equiv p^\sigma ty \mod p^{\lambda-\sigma}$. The multiplication in Γ is therefore given by

$$\begin{aligned}
\begin{bmatrix} f & g \\ h & j \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}(x,y) &= \begin{bmatrix} f & g \\ h & j \end{bmatrix}(ax + p^\sigma t\hat{b}\hat{y},\ c\pi(x) + dy) \\
&= \Big(fax + fp^\sigma t\hat{b}\hat{y} + p^\sigma t\hat{g}\hat{c}x + p^\sigma t\hat{g}\hat{d}\hat{y}, \\
&\qquad h\pi(ax) + hp^\sigma tby + jc\pi(x) + jdy\Big) \\
&= \Big((fa + p^\sigma t\hat{g}\hat{c})x + p^\sigma t((\pi(f)b + gd)y), \\
&\qquad (h\pi(a) + jc)\pi(x) + (p^\sigma thb + jd)y\Big) \\
&= \begin{bmatrix} fa + p^\sigma t\hat{g}\hat{c} & \pi(f)b + gd \\ h\pi(a) + jc & p^\sigma thb + jd \end{bmatrix}(x,y)\ .
\end{aligned}$$

Define $\det : \Gamma \to A_{\lambda-\sigma}$ by $\det(\left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right]) = \pi(a)d - p^\sigma tbc$. From the multiplication above we can easily find that det is a homomorphism. We claim that $\omega = \left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right] \in \Gamma$ is invertible if and only if $\det(\omega) \not\equiv 0$, as expected. Precisely: an element $\left[\begin{smallmatrix}f & g\\ h & j\end{smallmatrix}\right]$ is the inverse of ω if and only if, for all $(x,y) \in M$,

$$\begin{cases}
1 \equiv fa + p^\sigma t\hat{g}\hat{c} & \mod p^\lambda & \text{(A.3a)} \\
0 \equiv \pi(f)b + gd & \mod p^{\lambda-\sigma} & \text{(A.3b)} \\
0 \equiv h\pi(a) + jc & \mod p^{\lambda-\sigma} & \text{(A.3c)} \\
1 \equiv p^\sigma thb + jd & \mod p^{\lambda-\sigma}\ . & \text{(A.3d)}
\end{cases}$$

Suppose that $\det(\omega) \in A^\times_{\lambda-\sigma}$. Fix a lift $\hat{d}_0$ of d and let $\widehat{\det}_0(\omega) = a\hat{d}_0 - p^\sigma t\hat{b}\hat{c} \in A^\times_\lambda$ be the corresponding lift of $\det(\omega)$; note that the choice of $\hat{b}$ and $\hat{c}$ are immediately irrelevant mod p^λ, and we will show later that the choice of $\hat{d}_0$ is as well. First, (A.3b) yields

$$0 \equiv p^\sigma tf\hat{b} + p^\sigma t\hat{g}\hat{d} \mod p^\lambda$$

for all relevant lifts. Multiplying (A.3a) by $\hat{d}_0$, we then find

$$\begin{aligned}
\hat{d}_0 &\equiv \hat{d}_0 f a + \hat{d}_0 p^\sigma t \hat{g} \hat{c} \mod p^\lambda \\
\hat{d}_0 &\equiv \hat{d}_0 f a + p^\sigma t f \hat{b} \hat{c} \mod p^\lambda \\
\hat{d}_0 &\equiv f \cdot \widehat{\det}_0(\omega) \mod p^\lambda \\
f &\equiv \widehat{\det}_0(\omega)^{-1} \hat{d}_0 \mod p^\lambda \ .
\end{aligned}$$

To show that this does not depend on the choice of $\hat{d}_0$, let $\hat{d}_1 \coloneqq \hat{d}_0 + p^{\lambda-\sigma} q$, with $q \in A_\sigma$, be another lift. The corresponding lift of $\det(\omega)$ is $\widehat{\det}_1(\omega) = a\hat{d}_1 - p^\sigma t \hat{b}\hat{c} = \widehat{\det}_0(\omega) + p^{\lambda-\sigma} q a$. We arrive at the same result:

$$\begin{aligned}
\hat{d}_1 &\equiv f \cdot \widehat{\det}_1(\omega) \mod p^\lambda \\
\hat{d}_0 + p^{\lambda-\sigma} q &\equiv f(\widehat{\det}_0(\omega) + p^{\lambda-\sigma} q a) \mod p^\lambda \\
\hat{d}_0 &\equiv f \cdot \widehat{\det}_0(\omega) + p^{\lambda-\sigma} q (f a - 1) \mod p^\lambda \\
\hat{d}_0 &\equiv f \cdot \widehat{\det}_0(\omega) + p^{\lambda-\sigma} q (p^\sigma t \hat{g} \hat{c}) \mod p^\lambda \\
\hat{d}_0 &\equiv f \cdot \widehat{\det}_0(\omega) \mod p^\lambda \ .
\end{aligned}$$

We find $g \equiv -\det(\omega)^{-1} b$, $h \equiv -\det(\omega)^{-1} c$, and $j \equiv \det(\omega)^{-1} \pi(a) \mod p^{\lambda-\sigma}$ by similar calculations, so the inverse of ω is uniquely determined as

$$\omega^{-1} = \begin{bmatrix} \widehat{\det}_0(\omega)^{-1} \hat{d}_0 & -\det(\omega)^{-1} b \\ -\det(\omega)^{-1} c & \det(\omega)^{-1} \pi(a) \end{bmatrix} \in \Gamma \ .$$

The converse follows from det being a homomorphism. It is now clear that

$$\mathrm{Aut}(M) \cong \Gamma^\times = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \;\middle|\; a \in A_\lambda \text{ and } b, c, d \in A_{\lambda-\sigma} \text{ with } (\pi(a) d - p^\sigma t b c) \in A_{\lambda-\sigma}^\times \right\}$$

and det is a group homomorphism $\mathrm{Aut}(M) \to A_{\lambda-\sigma}^\times$.

We now recall the quotient ring structure of M described in Section 3.3.1, particularly the norm $\mathrm{Nm}(x,y) = x^2 + p^\sigma t y^2$. Under the convention established above, multiplication by $(a,c) \in M$ corresponds to $\left[\begin{smallmatrix} a & -c \\ c & \pi(a) \end{smallmatrix}\right]$ (with determinant $\pi(\mathrm{Nm}(a,c))$) and complex conjugation corresponds to $\kappa = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ (with order 2 and determinant -1).

Now, $\omega = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{Aut}(M)$ stabilizes $Q(x,y) = \frac{r\,\mathrm{Nm}(x,y)}{p^\lambda}$ if and only if

$$Q(x,y) = \frac{r\,\mathrm{Nm}(x,y)}{p^\lambda} \equiv \frac{r\,\mathrm{Nm}(ax + p^\sigma t(by), c\pi(x) + dy)}{p^\lambda} = Q(\omega(x,y)) \in \mathbb{Q}/\mathbb{Z}$$

or, equivalently,

$$r(x^2 + p^\sigma t y^2) \equiv r(\,\mathrm{Nm}(a,c)x^2 + (2p^\sigma t\pi(a)b + 2p^\sigma tcd)xy + (p^{2\sigma}t^2b^2 + p^\sigma td^2)y^2) \mod p^\lambda\ .$$

Since $r \in A_\lambda^\times$, the same process as in Lemma A.0.2 shows that this is equivalent to

$$\begin{cases} 1 & \equiv \mathrm{Nm}(a,c) \mod p^\lambda & \text{(A.4a)} \\ p^\sigma t & \equiv p^\sigma t(d^2 + p^\sigma t b^2) \mod p^\lambda & \text{(A.4b)} \\ 0 & \equiv 2p^\sigma t(\pi(a)b + cd) \mod p^\lambda\ . & \text{(A.4c)} \end{cases}$$

Assume $\omega \in \mathrm{Aut}(M,Q)$, so that the above hold. In particular, (A.4a) implies $a^2 \equiv 1 \mod p^\sigma$, and since $\sigma \geq 1$ this implies $p \nmid a$. Then we use (A.4c) to find

$$0 \equiv 2p^\sigma t(\pi(a)b + cd) \mod p^\lambda$$

$$0 \equiv \pi(a)b + cd \mod p^{\lambda-\sigma}$$

$$\pi(a)b \equiv -cd \mod p^{\lambda-\sigma}$$

and then substitute into (A.4b):

$$\begin{aligned}
p^\sigma t &\equiv p^\sigma t(d^2 + p^\sigma t b^2) \mod p^\lambda \\
1 &\equiv d^2 + p^\sigma t b^2 \mod p^{\lambda-\sigma} \\
\pi(a)^2 &\equiv \pi(a)^2 d^2 + p^\sigma t \pi(a)^2 b^2 \mod p^{\lambda-\sigma} \\
\pi(a)^2 &\equiv \pi(a)^2 d^2 + p^\sigma t (-cd)^2 \mod p^{\lambda-\sigma} \\
0 &\equiv d^2(\pi(a)^2 + p^\sigma t c^2) - \pi(a)^2 \mod p^{\lambda-\sigma} \\
0 &\equiv d^2 - \pi(a)^2 \mod p^{\lambda-\sigma} \\
0 &\equiv (d + \pi(a))(d - \pi(a)) \mod p^{\lambda-\sigma} .
\end{aligned}$$

If $(d + \pi(a)) \not\equiv 0 \mod p^{\lambda-\sigma}$ and $(d - \pi(a)) \not\equiv 0 \mod p^{\lambda-\sigma}$, then p divides both, in which case $p \mid 2\pi(a)$; since $p \neq 2$, this implies $p \mid \pi(a)$, a contradiction. Thus $d \equiv \pm\pi(a) \mod p^{\lambda-\sigma}$, and it then follows from (A.4c) that $b \equiv \mp c \mod p^{\lambda-\sigma}$. This results in two possible matrices for ω:

$$\begin{bmatrix} a & -c \\ c & \pi(a) \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} a & c \\ c & -\pi(a) \end{bmatrix} = \begin{bmatrix} a & -c \\ c & \pi(a) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} .$$

It is again easy to check that these satisfy (A.4a) through (A.4c) for any $(a, c) \in M$ with norm 1, which confirms the statement. □

Lemma A.0.5. *For type $R^\sigma_{2^\lambda}(r, t)$ with $0 \leq \sigma \leq \lambda - 3$, we have $\mathrm{Aut}(M, Q) \cong \mathfrak{A} \rtimes \langle\kappa\rangle$ with $\mathfrak{A} \cong \{\ (a, c) \in M \mid \mathrm{Nm}(a, c) = 1\ \}$ acting on M by multiplication and $\kappa : (x, y) \mapsto \overline{(x, y)}$.*

For the extremal case $R^{\lambda-2}_{2^\lambda}(r, t)$, instead $\mathrm{Aut}(M, Q) \cong \mathfrak{A} = \{\ a \in M \mid \mathrm{Nm}(a) = 1\ \}$.

Proof. Here $M = A_{\lambda-1} \oplus A_{\lambda-\sigma-1}$, so we use the same convention as in Lemma A.0.4:

$$\mathrm{Aut}(M) \cong \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \,\middle|\, a \in A_{\lambda-1},\ b, c, d \in A_{\lambda-\sigma-1} \text{ with } (\pi(a)d - 2^\sigma tbc) \in A^\times_{\lambda-\sigma-1} \right\} .$$

The extremal case differs only in that $M_2 \cong \mathbb{Z}/2\mathbb{Z}$, which means $\kappa = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = \mathrm{id}$.

The argument is largely the same as in that lemma, as well. In this case, $\omega = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ fixes Q if and only if

$$\begin{cases} 1 & \equiv \mathrm{Nm}(a,c) \mod 2^\lambda & \text{(A.5a)} \\ 2^\sigma t & \equiv 2^\sigma t(d^2 + 2^\sigma t b^2) \mod 2^\lambda & \text{(A.5b)} \\ 0 & \equiv 2^{\sigma+1} t(\pi(a)b + cd) \mod 2^\lambda\ . & \text{(A.5c)} \end{cases}$$

First consider the case where $1 \leq \sigma \leq \lambda - 2$. Suppose $\omega \in \mathrm{Aut}(M, Q)$, so that the above hold. In particular, (A.5a) implies $a^2 \equiv 1 \mod 2^\sigma$, and since $\sigma \geq 1$ this implies $2 \nmid a$. Then we use (A.5c) to find

$$\begin{aligned} 0 &\equiv 2^{\sigma+1} t(\pi(a)b + cd) \mod 2^\lambda \\ 0 &\equiv \pi(a)b + cd \mod 2^{\lambda-\sigma-1} \\ \pi(a)b &\equiv -cd \mod 2^{\lambda-\sigma-1} \end{aligned}$$

and then substitute into (A.5b):

$$\begin{aligned} 2^\sigma t &\equiv 2^\sigma t(d^2 + 2^\sigma t b^2) \mod 2^\lambda \\ 1 &\equiv d^2 + 2^\sigma t b^2 \mod 2^{\lambda-\sigma} \\ \pi(a)^2 &\equiv \pi(a)^2 d^2 + 2^\sigma t \pi(a)^2 b^2 \mod 2^{\lambda-\sigma} \\ \pi(a)^2 &\equiv \pi(a)^2 d^2 + 2^\sigma t(-cd)^2 \mod 2^{\lambda-\sigma} \\ 0 &\equiv d^2(\pi(a)^2 + 2^\sigma t c^2) - \pi(a)^2 \mod 2^{\lambda-\sigma} \\ 0 &\equiv d^2 - \pi(a)^2 \mod 2^{\lambda-\sigma} \\ 0 &\equiv (d + \pi(a))(d - \pi(a)) \mod 2^{\lambda-\sigma}\ . \end{aligned}$$

Now, we claim that this implies $(d+\pi(a)) \equiv 0 \mod 2^{\lambda-\sigma-1}$ or $(d-\pi(a)) \equiv 0 \mod 2^{\lambda-\sigma-1}$. Suppose not; then 2 divides both. We have $2 \nmid \pi(a)$ and $2 \mid (d - \pi(a))$, so $2 \nmid d$. Thus both

$\pi(a)$ and d lie in $A^{\times}_{\lambda-\sigma-1}$. We therefore have

$$\pi(a)^2 \equiv d^2 \mod 2^{\lambda-\sigma}$$

$$1 \equiv (\pi(a)^{-1}d)^2 \mod 2^{\lambda-\sigma} ;$$

that is, $\pi(a)^{-1}d$ lies in $\ker\eta$, with $\eta : A^{\times}_{\lambda-\sigma} \to \left(A^{\times}_{\lambda-\sigma}\right)^2$ given by $x \mapsto x^2$. We recall that

$$\ker\eta = \begin{cases} \{\pm 1\}, & \text{for } \sigma \geq \lambda - 2 \\ \{\pm 1,\ 2^{\lambda-\sigma-1} \pm 1\}, & \text{otherwise.} \end{cases}$$

In either case, we have $d \equiv \pm\pi(a) \mod 2^{\lambda-\sigma-1}$ and hence $b \equiv \mp c \mod 2^{\lambda-1}$.

Now suppose $\sigma = 0$ (so $M = A_{\lambda-1} \oplus A_{\lambda-1}$ and $\pi = \mathrm{id}$). The equations (A.5a) - (A.5c) become

$$\begin{cases} 1 \equiv \mathrm{Nm}(a,c) \mod 2^{\lambda} & \text{(A.6a)} \\ 1 \equiv d^2 + tb^2 \mod 2^{\lambda} & \text{(A.6b)} \\ 0 \equiv 2(ab+cd) \mod 2^{\lambda} . & \text{(A.6c)} \end{cases}$$

From (A.6c) we have $ab \equiv -cd \mod 2^{\lambda-1}$. Also, since $2 \nmid (ad - tbc)$, at least one of ad and bc must be odd.

Suppose first that ad is odd (and hence $a, d \in A^{\times}_{\lambda-1}$). From (A.6b) we find

$$a^2 \equiv a^2d^2 + ta^2b^2 \mod 2^{\lambda}$$

$$a^2 \equiv a^2d^2 + t(-cd)^2 \mod 2^{\lambda-1}$$

$$a^2 \equiv d^2(a^2 + tc^2) \mod 2^{\lambda-1}$$

$$a^2 \equiv d^2 \mod 2^{\lambda-1}$$

$$0 \equiv a^{-2}d^2 \mod 2^{\lambda-1} .$$

Thus $a^{-1}d \in \ker \eta$, with $\eta : A_{\lambda-1}^{\times} \to \left(A_{\lambda-1}^{\times}\right)^2$ given by $x \mapsto x^2$. We recall that

$$\ker \eta = \begin{cases} \{\pm 1\}, & \text{for } \lambda \leq 3 \\ \{\pm 1,\ 2^{\lambda-2} \pm 1\}, & \text{otherwise.} \end{cases}$$

Suppose $a^{-1}d \equiv 2^{\lambda-2} \pm 1 \mod 2^{\lambda-1}$, so $d \equiv (2^{\lambda-2} \pm 1)a \mod 2^{\lambda-1}$. We then have

$$\begin{aligned} ab &\equiv -c((2^{\lambda-2} \pm 1)a) \mod 2^{\lambda-1} \\ b &\equiv -c(2^{\lambda-2} \pm 1) \mod 2^{\lambda-1}, \end{aligned}$$

but then

$$\begin{aligned} b^2 + td^2 &= (-(2^{\lambda-2} \pm 1)c)^2 + t((2^{\lambda-2} \pm 1)a)^2 \\ &= (2^{2\lambda-4} \pm 2^{\lambda-1} + 1)c^2 + (2^{2\lambda-4} \pm 2^{\lambda-1} + 1)ta^2 \\ &= (2^{2\lambda-4} \pm 2^{\lambda-1})(a^2 + tc^2) + (a^2 + tc^2) \\ &\equiv \pm 2^{\lambda-1} + 1 \mod 2^{\lambda}, \end{aligned}$$

which contradicts (A.6b). We conclude that $d \equiv \pm a \mod 2^{\lambda-1}$ and $b \equiv \mp c \mod 2^{\lambda-1}$.

If bc is odd, a symmetrical argument leads to the same conclusion.

Thus, regardless of whether $\sigma = 0$, we have two possible matrices for ω:

$$\begin{bmatrix} a & -c \\ c & \pi(a) \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} a & c \\ c & -\pi(a) \end{bmatrix} = \begin{bmatrix} a & -c \\ c & \pi(a) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

These are easily checked to satisfy (A.5a) through (A.5c). Recalling that κ is trivial for the extremal case and has order 2 otherwise, we conclude the proof. □

Having thus covered all relevant representation types, we conclude that Proposition 3.3.1 holds. □

The specific structure of $\mathfrak{A}$ is largely irrelevant to our proof of Theorem 3.1.10 and is given in [40]; however, we will detail here a case where the structure differs from that given in that paper. Here $q^n \parallel b$ means that q^n *exactly divides* b; that is, $q^n \mid b$ and $q^{n+1} \nmid b$.

Proposition A.0.6. *If (M, Q) is of type $R^1_{3^\lambda}(r, 1)$ with $\lambda \geq 3$, then*

$$\mathfrak{A} \cong \mathbb{Z}\big/(2 \cdot 3^{\lambda-2})\mathbb{Z} \times \mathbb{Z}\big/3\mathbb{Z} \ .$$

For all other cases of type $R^\sigma_{p^\lambda}(r, t)$ with odd p, $\mathfrak{A}$ is cyclic:

$$\mathfrak{A} \cong \mathbb{Z}\big/(2 \cdot p^{\lambda-\sigma})\mathbb{Z} \ .$$

Proof. First note that, for all cases, $|\mathfrak{A}| = 2 \cdot p^{\lambda-\sigma}$. To see this, fix some $c \in A_{\lambda-\sigma}$; then $(a, c) \in M$ has norm 1 if and only if

$$a^2 \equiv 1 - p^\sigma t c^2 \mod p^\lambda \ .$$

Since $\sigma \geq 1$, we have $1 - p^\sigma t c^2 \equiv 1 \mod p$; 1 is a quadratic residue mod p, so $1 - p^\sigma t c^2$ is a quadratic residue mod p^λ. Moreover, $p \neq 2$, so there are exactly two choices of $a \in A_\lambda$ solving the above. This confirms that $|\mathfrak{A}| = 2 \cdot |A_{\lambda-\sigma}| = 2 \cdot p^{\lambda-\sigma}$.

Now suppose $p = 3$, $\lambda \geq 3$, and $\sigma = t = 1$. We calculate that, for any $(a, c) \in \mathfrak{A}$,

$$\begin{aligned}(a, c)^3 &= (a^3 - 9ac^2,\ 3a^2c - 3c^3) \\ &= (a^3 - 9ac^2,\ 3c - 12c^3) \\ &= (a^3 - 9ac^2,\ 3c(1 + 2c)(1 - 2c)) \ .\end{aligned}$$

We now show that, for any $(a, c) \in \mathfrak{A}$ and any $k \geq 1$, the second coordinate of $(a, c)^{3^k}$ is divisible by 3^{k+1}. We proceed by induction. For the base case ($k = 1$), observe that,

for any $c \in A_{\lambda-\sigma}$, exactly one of c, $(1+2c)$, and $(1-2c)$ is divisible by 3. Therefore, $3^2 \parallel 3c(1+2c)(1-2c)$. Assuming then that the statement holds for a given k, we have

$$(a,c)^{3^{k+1}} = \left((a,c)^{3^k}\right)^3 = (b, 3^{k+1}d)^3$$

for some $b \in A_\lambda$, $d \in A_{\lambda-1}$. Then

$$(b, 3^{k+1}d)^3 = \left(b^3 - 9b(3^{k+1}d)^2,\ 3(3^{k+1}d)(1+2(3^{k+1}d))(1-2(3^{k+1}d))\right) .$$

Since 3^{k+2} clearly divides the second coordinate, this confirms the statement.

In particular, $3^{\lambda-1}$ divides the second coordinate of $(a,c)^{3^{\lambda-2}}$, so $(a,c)^{3^{\lambda-2}} = (g,0)$ for some $g \in A_\lambda$. Since this still lies in $\mathfrak{A}$, we have $\mathrm{Nm}(g,0) = g^2 \equiv 1 \mod 3^\lambda$, and we conclude $g = \pm 1$. Thus the order of each $(a,c) \in \mathfrak{A}$ is at most $2 \cdot 3^{\lambda-2}$.

Taking $c = 1 \in A_{\lambda-\sigma}$, the earlier discussion shows that there exists some $a \in A_\lambda$ so that $(a,1) \in \mathfrak{A}$. We then claim that, for $k \geq 1$, the second coordinate of $(a,1)^{3^k}$ has the form $3^{k+1}d$ for $3 \nmid d$. For the base case, we have

$$(a,1)^3 = (a^3 - 9a, -9) = (a^3 - 9a, 9(-1)) .$$

For the inductive step, suppose the statement holds for some given $k \geq 1$; then, as above,

$$(a,1)^{3^{k+1}} = (b, 3^{k+1}d)^3 = \left(b^3 - 9b(3^{k+1}d)^2,\ 3(3^{k+1}d)(1+3^{k+1}\cdot 2d)(1-3^{k+1}\cdot 2d)\right) .$$

Since $k \geq 1$, we have

$$\frac{3(3^{k+1}d)(1+3^{k+1}\cdot 2d)(1-2(3^{k+1}d))}{3^{k+2}} \equiv d(1+3^{k+1}\cdot 2d)(1-3^{k+1}\cdot 2d) \equiv d \not\equiv 0 \mod 3 .$$

As a result, for all $1 \leq k < 3^{\lambda-2}$, the second coordinate of $(a,1)^k$ is not equivalent to 0 mod $3^{\lambda-\sigma}$, and hence $(a,1)^k \neq (\pm 1, 0)$. Thus $\mathrm{ord}(a,1) \geq 3^{\lambda-2}$, and we conclude that either $\mathrm{ord}(a,1) = 2 \cdot 3^{\lambda-2}$ or $\mathrm{ord}(-(a,1)) = 2 \cdot 3^{\lambda-2}$. Denote whichever has this order by α.

Now, consider $\beta := \alpha^{2\cdot 3^{\lambda-3}}$. The above calculations show that

$$\beta = (b, 3^{\lambda-2}d)$$

with $3^{\lambda-2}d \not\equiv 0$, and then we have

$$\begin{aligned} b^2 + 3(3^{\lambda-2}d)^2 &\equiv 1 \mod 3^\lambda \\ b^2 + 3^{2\lambda-3}d^2 &\equiv 1 \mod 3^\lambda \\ b^2 &\equiv 1 \mod 3^\lambda \ , \end{aligned}$$

since $\lambda \leq 3$ implies $2\lambda - 3 \geq \lambda$. Hence $b = \pm 1$. Note that β generates the unique order-3 subgroup of $\langle\alpha\rangle$, namely $\{(1,0), (1, 3^{\lambda-2}), (1, 2\cdot 3^{\lambda-2})\}$ (which are, incidentally, precisely the elements of $\mathfrak{A}$ that fix $3M$ pointwise).

On the other hand, consider $(a, c) = (2^{-1} \mod 3^\lambda, 2^{-1} \mod 3^{\lambda-1})$. Then, writing $2a = 1 + 3^\lambda k$ and $2c = 1 + 3^{\lambda-1}\ell$ for some $k, \ell \in \mathbb{Z}$, we have

$$\begin{aligned} 4\,\mathrm{Nm}(a, c) &= (2a)^2 + 3(2c)^2 \\ &= (1 + 3^\lambda k)^2 + 3(1 + 3^{\lambda-1}\ell)^2 \\ &= 1 + 2\cdot 3^\lambda k + 3^{2\lambda}k^2 + 3 + 2\cdot 3^\lambda \ell + 3^{2\lambda-1}\ell^2 \\ &\equiv 4 \mod 3^\lambda \\ \mathrm{Nm}(a, c) &\equiv 1 \mod 3^\lambda \end{aligned}$$

so $(a, c) \in \mathfrak{A}$. The second coordinate of $(a, c)^3$ is

$$3c(1 - 2c)(1 + 2c) \equiv 0 \mod 3^{\lambda-1} \ ,$$

so, in the same way as before, we have $(a, c)^3 = (\pm 1, 0)$ and thus either $\mathrm{ord}(a, c) = 3$ or $\mathrm{ord}(-(a, c)) = 3$. Denote whichever has this order by ζ. Clearly $\zeta \notin \langle\beta\rangle$, so we conclude

that

$$\mathfrak{A} \cong \langle \alpha \rangle \times \langle \zeta \rangle \ .$$

Now we consider the remaining cases. For $p = 3$ and $\lambda \leq 2$, the statement can be checked directly. So suppose that $p = 3$ and $\lambda \geq 3$, but either $\sigma > 1$ or $t = 2$ (recall $t = 1$ or u with u a non-residue mod $p = 3$). We calculate

$$(a, c)^3 = \left(a^3 - 3^{\sigma+1} t a c^2,\ 3c(1 - 4 \cdot 3^{\sigma-1} t c^2)\right) \ .$$

By the same argument as before, there exists some $a \in A_\lambda$ so that $(a, 1) \in \mathfrak{A}$. We claim that, for all $k \geq 1$, the second coordinate of $(a, 1)^{3^k}$ is exactly divisible by 3^k. For the base case,

$$(a, 1)^3 = \left(a^4 - 3^{\sigma+1} t a, 3(1 - 4 \cdot 3^{\sigma-1} t)\right) \ .$$

If $\sigma > 1$, then $1 - 4 \cdot 3^{\sigma-1} t \equiv 1 \mod 3$. If $\sigma = 1$ but $t = 2$, then $1 - 4 \cdot 3^{\sigma-1} t = -7 \equiv 2 \mod 3$. In either case, the second coordinate is exactly divisible by 3. Next, suppose that the statement holds for a given k, so $(a, c)^{3^k} = (b, 3^k d)$ for $3 \nmid d$. Then we have

$$\begin{aligned} (a, c)^{3^{k+1}} &= \left((a, c)^{3^k}\right)^3 \\ &= \left(b^3 - 3^{\sigma+1} t b (3^k d)^2, 3(3^k d)(1 - 4 \cdot 3^{\sigma-1} t (3^k d)^2)\right) \end{aligned}$$

and clearly $1 - 4 \cdot 3^{\sigma-1} t (3^k d)^2 \equiv 1 \mod 3$, confirming the statement. We may therefore conclude that $\mathrm{ord}(a, 1) \geq 3^{\lambda-\sigma}$, and hence that either $\mathrm{ord}(a, 1) = 2 \cdot 3^{\lambda-\sigma}$ or $\mathrm{ord}(-(a, 1)) = 2 \cdot 3^{\lambda-\sigma}$. Denoting the element with that order by α, we then have

$$\mathfrak{A} \cong \langle \alpha \rangle \ .$$

Finally, suppose $p \geq 5$. We then have

$$(a,c)^p = \left(\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-p^\sigma t)^j a^{p-2j} c^{2j},\ \sum_{\ell=0}^{\frac{p-1}{2}} \binom{p}{2\ell+1} (-p^\sigma t)^\ell a^{p-2\ell-1} c^{2\ell+1} \right) .$$

As in the previous cases, there exists some element $(a,1) \in \mathfrak{A}$. We claim that the second coordinate of $(a,1)^{p^k}$ is exactly divisible by p^k. For the base case, denote by γ_1 the second coordinate of $(a,1)^p$. Then, noting that $\frac{p-1}{2} \geq 2$, we have

$$\begin{aligned}
\gamma_1 &= \sum_{\ell=0}^{\frac{p-1}{2}} \binom{p}{2\ell+1} (-p^\sigma t)^\ell a^{p-2\ell-1} \\
&= pa^{p-1} + (-p^\sigma t)^{\frac{p-1}{2}} + \sum_{\ell=1}^{\frac{p-1}{2}-1} \binom{p}{2\ell+1} (-p^\sigma t)^\ell a^{p-2\ell-1} \\
&= pa^{p-1} + p^2 \left((-1)^{\frac{p-1}{2}} p^{\frac{\sigma(p-1)}{2}-2} + \sum_{\ell=1}^{\frac{p-1}{2}-1} \frac{1}{2\ell+1} \binom{p-1}{2\ell} (-t)^\ell p^{\sigma\ell-1} a^{p-2\ell-1} \right) .
\end{aligned}$$

Denoting by y the term in the parentheses, this becomes

$$\gamma_1 = p\left(a^{p-1} + py\right) .$$

Since $p \nmid a$ (as otherwise $\mathrm{Nm}(a,1) = a^2 + p^\sigma t \not\equiv 1$), $p \parallel p(a^{p-1} + py)$. For the inductive step, suppose that the statement holds for some given $k \geq 1$, so that we may write

$$(a,1)^{p^k} = (b, p^k d)$$

with $p \nmid d$. Then, denoting the second coordinate of $(a,1)^{p^{k+1}} = ((a,1)^{p^k})^p$ by γ_{k+1}, we have

$$\begin{aligned}
\gamma_{k+1} &= \sum_{\ell=0}^{\frac{p-1}{2}} \binom{p}{2\ell+1} (-p^\sigma t)^\ell b^{p-2\ell-1} (p^k d)^{2\ell+1} \\
&= p^{k+1} b^{p-1} d + (-p^\sigma t)^{\frac{p-1}{2}} (p^k d)^p + \sum_{\ell=1}^{\frac{p-1}{2}-1} \binom{p}{2\ell+1} (-p^\sigma t)^\ell b^{p-2\ell-1} (p^k d)^{2\ell+1} \\
&= p^{k+1} b^{p-1} d \\
&\quad + p^{k+2} \left((-1)^{\frac{p-1}{2}} p^{\frac{\sigma(p-1)}{2}+p(k-1)-2} d^p + \sum_{\ell=1}^{\frac{p-1}{2}-1} \frac{1}{2\ell+1} \binom{p-1}{2\ell} (-t)^\ell p^{\sigma\ell+2\ell k-1} b^{p-2\ell-1} d^{2\ell+1} \right) .
\end{aligned}$$

Denoting by y the term in the parentheses, this becomes

$$\gamma_{k+1} = p^{k+1}(b^{p-1}d + py) \ .$$

As before, $p \nmid b$, so $p^{k+1} \parallel p^{k+1}(b^{p-1}d + py)$.

As in the previous case, we conclude that $\mathrm{ord}(a, 1) \geq p^{\lambda-\sigma}$, and hence that either $\mathrm{ord}(a, 1) = 2 \cdot p^{\lambda-\sigma}$ or $\mathrm{ord}(-(a, 1)) = 2 \cdot p^{\lambda-\sigma}$. Denoting the element with that order by α, we then have

$$\mathfrak{A} \cong \langle \alpha \rangle \ ,$$

which concludes the proof. □

Bibliography

[1] T. M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*, volume 41 of *Graduate Texts in Mathematics*. Springer New York, NY, 1990.

[2] E. Ardonne, P. E. Finch, and M. Titsworth. Classification of metaplectic fusion categories. *arXiv preprint*, 1608.03762, 2016.

[3] B. Bakalov and A. Kirillov, Jr. *Lectures on tensor categories and modular functors*, volume 21 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2001.

[4] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary, 1998.

[5] P. Bruillard, C. Galindo, S.-M. Hong, Y. Kashina, D. Naidu, S. Natale, J. Y. Plavnik, and E. C. Rowell. Classification of integral modular categories of Frobenius-Perron dimension pq^4 and p^2q^2. *Canad. Math. Bull.*, 57(4):721–734, 2014.

[6] P. Bruillard, S.-H. Ng, E. C. Rowell, and Z. Wang. On classification of modular categories by rank. *Int. Math. Res. Not. IMRN*, 2016(24):7546–7588, 2016.

[7] P. Bruillard, S.-H. Ng, E. C. Rowell, and Z. Wang. Rank-finiteness for modular categories. *J. Amer. Math. Soc.*, 29(3):857–881, 2016.

[8] P. Bruillard, J. Y. Plavnik, and E. C. Rowell. Modular categories of dimension p^3m with m square-free. *Proc. Amer. Math. Soc.*, 147(1):21–34, 2019.

[9] C. Dong, X. Lin, and S.-H. Ng. Congruence property in conformal field theory. *Algebra Number Theory*, 9(9):2121–2166, 2015.

[10] W. Eholzer. Fusion algebras induced by representations of the modular group. *Internat. J. Modern Phys. A*, 8(20):3495–3507, 1993.

[11] S. Eilenberg and S. MacLane. Cohomology theory in abstract groups. I. *Ann. of Math. (2)*, 48:51–78, 1947.

[12] S. Eilenberg and S. MacLane. Cohomology theory in abstract groups. II. Group extensions with a non-Abelian kernel. *Ann. of Math. (2)*, 48:326–341, 1947.

[13] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik. *Tensor categories*, volume 205 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2015.

[14] P. Etingof, D. Nikshych, and V. Ostrik. On fusion categories. *Ann. of Math. (2)*, 162(2):581–642, 2005.

[15] A. Fiori and C. Franc. The unbounded denominator conjecture for the noncongruence subgroups of index 7. *J. Number Theory*, 2022. doi: 10.1016/j.jnt.2021.11.014.

[16] J. Fröhlich and T. Kerler. *Quantum groups, quantum categories and quantum field theory*, volume 1542 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1993.

[17] Y.-Z. Huang. Vertex operator algebras, the Verlinde conjecture, and modular tensor categories. *Proc. Natl. Acad. Sci. USA*, 102(15):5352–5356, 2005.

[18] Y.-Z. Huang. Rigidity and modularity of vertex tensor categories. *Commun. Contemp. Math.*, 10(suppl. 1):871–911, 2008.

[19] M. Jimbo. Introduction to the Yang-Baxter equation. *International Journal of Modern Physics A*, 04(15):3759–3777, 1989.

[20] A. Joyal and R. Street. Braided monoidal categories. *Macquarie Math. Reports*, NO. 850067, 1985.

[21] A. Joyal and R. Street. Braided tensor categories. *Adv. Math.*, 102(1):20–78, 1993.

[22] C. S. Jürgen Fuchs, Ingo Runkel. TFT construction of RCFT correlators i: partition functions. *Nuclear Physics B*, 646(3):353–497, dec 2002.

[23] C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[24] T. Kerler and V. V. Lyubashenko. *Non-semisimple topological quantum field theories for 3-manifolds with corners*, volume 1765 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2001.

[25] A. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, jan 2003.

[26] M. Larsen and Z. Wang. Density of the SO(3) TQFT representation of mapping class groups. *Comm. Math. Phys.*, 260(3):641–658, 2005.

[27] S. Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[28] G. Moore and N. Seiberg. Classical and quantum conformal field theory. *Comm. Math. Phys.*, 123(2):177–254, 1989.

[29] G. Moore and N. Seiberg. *Lectures on RCFT*, pages 263–361. Springer US, Boston, MA, 1990.

[30] M. Müger. From subfactors to categories and topology. I. Frobenius algebras in and Morita equivalence of tensor categories. *J. Pure Appl. Algebra*, 180(1-2):81–157, 2003.

[31] M. Müger. From subfactors to categories and topology. II. The quantum double of tensor categories and subfactors. *J. Pure Appl. Algebra*, 180(1-2):159–219, 2003.

[32] M. Müger. On the structure of modular categories. *Proc. London Math. Soc. (3)*, 87(2):291–308, 2003.

[33] S.-H. Ng, E. C. Rowell, Z. Wang, and Z.-G. Wen. Reconstruction of modular data from $\mathrm{SL}_2(\mathbb{Z})$ representations. *arXiv preprint*, 2022.

[34] S.-H. Ng and P. Schauenburg. Frobenius-Schur indicators and exponents of spherical categories. *Adv. Math.*, 211(1):34–71, 2007.

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

[36] S.-H. Ng, Y. Wang, and S. Wilson. SL2Reps, Constructing symmetric representations of $\mathrm{SL}(2,\mathbb{Z})$, Version 1.1, Nov 2022. GAP package. `https://snw-0.github.io/sl2-reps`.

[37] S.-H. Ng, Y. Wang, and S. Wilson. On symmetric representations of $\mathrm{SL}_2(\mathbb{Z})$. *Proc. Amer. Math. Soc.*, 151(4):1415–1431, 2023.

[38] S.-H. Ng, Y. Wang, and Q. Zhang. Modular categories with transitive Galois actions. *arXiv preprint*, 2007.01366, 2020.

[39] A. Nobs. Die irreduziblen Darstellungen der Gruppen $\mathrm{SL}_2(\mathbb{Z}_p)$, insbesondere $\mathrm{SL}_2(\mathbb{Z}_2)$. I. *Comment. Math. Helv.*, 51(4):465–489, 1976.

[40] A. Nobs and J. Wolfart. Die irreduziblen Darstellungen der Gruppen $\mathrm{SL}_2(\mathbb{Z}_p)$, insbesondere $\mathrm{SL}_2(\mathbb{Z}_2)$. II. *Comment. Math. Helv.*, 51(4):491–526, 1976.

[41] N. Reshetikhin and V. G. Turaev. Invariants of 3-manifolds via link polynomials and quantum groups. *Invent. Math.*, 103(3):547–597, 1991.

[42] E. Rowell, R. Stong, and Z. Wang. On classification of modular tensor categories. *Comm. Math. Phys.*, 292(2):343–389, 2009.

[43] I. Runkel. Algebra in braided tensor categories and conformal field theory. 55(2):183–238, 2010.

[44] V. G. Turaev. *Quantum invariants of knots and 3-manifolds*, volume 18 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, 1994.

[45] V. G. Turaev. *Quantum invariants of knots and 3-manifolds*, volume 18 of *De Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, revised edition, 2010.

[46] C. Vafa. Toward classification of conformal theories. *Phys. Lett. B*, 206(3):421–426, 1988.

[47] Z. Wan and Y. Wang. Classification of spherical fusion categories of frobenius-schur exponent 2. *arXiv preprint*, 1811.02004, 2018.

[48] Y. Wang. *On integrality of SO(n)-level 2 TQFTs*. PhD thesis, Ohio State University, 2018.

[49] Z. Wang. *Topological quantum computation*, volume 112 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2010.

[50] E. Witten. Quantum field theory and the Jones polynomial. *Comm. Math. Phys.*, 121(3):351–399, 1989.

[51] Y. Zhu. Modular invariance of characters of vertex operator algebras. *J. Amer. Math. Soc.*, 9(1):237–302, 1996.

Vita

Samuel Wilson was born in San Marcos, Texas. As a child, he was lucky enough to visit a variety of distant places, from Malaysia to Romania to Ireland. His interests include category theory and knot theory. He completed a B.A. in Mathematics at the University of Oklahoma in 2010 and an M.S. in Mathematics at Texas State University in 2013, where his advisor was Dr. Daniela Ferrero. In 2017, he became a Ph.D. student at Louisiana State University in Baton Rouge, where his advisor is Dr. Siu-Hung "Richard" Ng. He anticipates receiving his Ph.D. in May of 2023.