ON THE CLASSIFICATION OF LOW-RANK BRAIDED FUSION CATEGORIES

A Dissertation

by

PAUL JOSEPH BRUILLARD

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Eric C. Rowell
Committee Members,	Marcelo Aguiar
	Andreas Klappenecker
	Sarah Witherspoon
Head of Department,	Emil Straube

August 2013

Major Subject: Mathematics

ABSTRACT

A physical system is said to be in *topological phase* if at low energies and long wavelengths the observable quantities are invariant under diffeomorphisms. Such physical systems are of great interest in condensed matter physics and computer science where they can be applied to form topological insulators and fault–tolerant quantum computers. Physical systems in topological phase may be rigorously studied through their algebraic manifestations, (pre)modular categories. A complete classification of these categories would lead to a taxonomy of the topological phases of matter. Beyond their ties to physical systems, premodular categories are of general mathematical interest as they govern the representation theories of quasi–Hopf algebras, lead to manifold and link invariants, and provide insights into the braid group.

In the course of this work, we study the classification problem for (pre)modular categories with particular attention paid to their arithmetic properties. Central to our analysis is the question of rank finiteness for modular categories, also known as Wang's Conjecture. In this work, we lay this problem to rest by exploiting certain arithmetic properties of modular categories. While the rank finiteness problem for premodular categories is still open, we provide new methods for approaching this problem.

The arithmetic techniques suggested by the rank finiteness analysis are particularly pronounced in the (weakly) integral setting. There, we use Diophantine techniques to classify all weakly integral modular categories through rank 6 up to Grothendieck equivalence. In the case that the category is not only weakly integral, but actually integral, the analysis is further extended to produce a classification of integral modular categories up to Grothendieck equivalence through rank 7. It is observed that such classification can be extended provided some mild assumptions are made. For instance, if we further assume that the category is also odd–dimensional, then the classification up to Grothendieck equivalence is completed through rank 11.

Moving beyond modular categories has historically been difficult. We suggest new methods for doing this inspired by our work on (weakly) integral modular categories and related problems in algebraic number theory. The allows us to produce a Grothendieck classification of rank 4 premodular categories thereby extending the previously known rank 3 classification.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Dr. Eric Rowell, for his guidance and support; my thesis committee members for their patience and helpful suggestions; Zhenhan Wang and Richard Ng for enlightening discussions. I would also like to thank Tobe Hagge, César Galindo, Deepak Naidu, Matt Papanikolas, and many more for our many interesting conversations. Additionally, I would like to express my gratitude to the faculty and Texas A&M University and The University of New Hampshire for all of the knowledge they imparted and the chances they gave me. Finally, I am especially grateful for my friends and family, they have been an unending wellspring of support and inspiration in this long and arduous journey.

NOMENCLATURE

$[X : Y]$	Multiplicity of X in Y.
$\lvert\cdot\rvert_{\mathfrak{p}}$	A non-Archimedean absolute value corresponding to the prime ideal $\mathfrak{p}$ in $\mathbb{K}$.
$\lvert\cdot\rvert_{\sigma_j}$	The Archimedean absolute value corresponding to the field embedding σ_j.
$\mathfrak{A}_d$	The alternating group on d letters.
$\alpha_{X,Y,Z}$	The associativity isomorphism $(X \otimes Y) \otimes Z \cong X \otimes (Y \otimes Z)$.
α	The anomaly of the category $\mathcal{C}$, p^+/p^-.
BFC	Braided Fusion Category.
$\mathcal{C}'$	The Müger center of the category $\mathcal{C}$.
$\mathcal{C}_{ad}$	The adjoint subcategory.
$\mathcal{C}_{pt}$	The pointed subcategory.
$\mathcal{C}^{op}$	Opposite (mirror) category to $\mathcal{C}$.
coev_X	Coevaluation $\mathbb{I} \to X \otimes X^*$.
$C^2\left(G, \mathbb{K}^\times\right)$	2-cochains of G with coefficients in $\mathbb{K}^\times$.
C	The charge conjugation matrix of $\mathcal{C}$.
d_a	The categorical dimension of X_a, occasionally referred to as $\dim X_a$.
$D^\omega\left(G\right)$	The twisted quantum double of a group G.
d^ℓ	Left-pivotal dimension.
d^r	Right-pivotal dimension.
D_n	Dihedral group.
ev_X	Evaluation $X^* \otimes X \to \mathbb{I}$ in $\mathcal{C}$.
$\mathfrak{f}\left(\mathbb{K}\right)$	Conductor of an abelian number field $\mathbb{K}$ (viewed as an integer).
$\mathrm{FPdim}\left(\mathcal{C}\right)$	The Frobenius-Perron dimension of $\mathcal{C}$.
$\mathrm{FPdim}\left(X\right)$	The Frobenius-Perron dimension of an object X in $\mathcal{C}$.
Fib	The Fibonacci modular category.
$F^{abc}_{d;gf}$	The F-matrices.
$\mathrm{FSExp}\left(\mathcal{C}\right)$	Frobenius-Schur Exponent of $\mathcal{C}$.
$\mathcal{F}$	Forgetful functor.
$\mathrm{Gal}\left(\mathcal{C}\right)$	$\mathrm{Gal}\left(\mathbb{Q}\left(S\right)/\mathbb{Q}\right)$.
$\mathrm{Hom}_{\mathcal{C}}\left(X, Y\right)$	Morphisms from X to Y in $\mathcal{C}$.
$H\left(-\right)$	Projective height in a number field.
$\mathbb{I}$	The trivial object in $\mathcal{C}$.
$\mathrm{Irr}\left(\mathcal{C}\right)$	Isomorphism classes of simple objects in $\mathcal{C}$.
j_X	The double dual isomorphism in a spherical category, $X \cong X^{**}$.
$\mathcal{K}_0\left(\mathcal{C}\right)$	Grothendieck ring of $\mathcal{C}$.
$M_{X,Y}$	The double braiding $M_{X,Y} = R_{Y,X} \circ R_{X,Y}$.
MNSD	Maximally Non-Self Dual.
MTC	Modular Tensor Category.

$\mathbb{N}$	Natural numbers starting at 0.
$N_{a,b}^{c}$	The fusion coefficient given by $\dim \operatorname{Hom}_{\mathcal{C}}\left(X_a \otimes X_b, X_c\right)$.
(N, S, T)	Admissible modular datum.
$N\left(-\right)$	Absolute norm in a number field $\mathbb{K}$, i.e. $N_{\mathbb{K}/\mathbb{Q}}\left(-\right)$.
$\nu_n\left(-\right)$	n^{th} Frobenius-Schur indicator.
$\operatorname{ord}\left(M\right)$	The order of a matrix M.
$\operatorname{ord}_{\mathfrak{p}}$	The valuation on a number field defined by the prime ideal $\mathfrak{p}$.
$\mathcal{O}_{\mathbb{K},\mathcal{S}}$	The ring of $\mathcal{S}$-integers in $\mathbb{K}$.
$\mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}$	The group of $\mathcal{S}$-units in $\mathbb{K}$.
$\operatorname{Obj}\left(\mathcal{C}\right)$	Objects in the category $\mathcal{C}$.
$\operatorname{ptr}^{\ell}$	The left-pivotal trace.
ptr^{r}	The right-pivotal trace.
$p^{\pm}$	Gauss sums of the category $\mathcal{C}$.
ψ_a	The a^{th} linear character of $\mathcal{K}_0\left(\mathcal{C}\right)$.
$\mathbb{Q}\left(M\right)$	The smallest number field over which the matrix M is defined.
$\mathbb{Q}_{\text{ab}}$	maximal abelian extension of $\mathbb{Q}$ given by $\cup_{n\in\mathbb{N}}\mathbb{Q}\left(\zeta_n\right)$.
$\operatorname{Rep}\left(G\right)$	The representation category of G.
$R_{X,Y}$	The braiding isomorphism $X \otimes Y \cong Y \otimes X$.
R_{c}^{ab}	The R-matrix– braiding of $X_a \otimes X_b$ in the X_c channel.
$\mathfrak{s}$	Generator of $\operatorname{SL}\left(2,\mathbb{Z}\right)$ given by $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$.
s	The image of $\mathfrak{s}$ under a linear representation of $\operatorname{SL}\left(2,\mathbb{Z}\right)$.
S	S-matrix of a (pre)modular category obtained by tracing the square braiding.
$\mathcal{S}_{\infty}$	The infinite places of a number field.
D^2	The global dimension of a category, occasionally referred to as $\dim\mathcal{C}$.
Sem	The Semion modular category.
sVec	The category of super vector spaces.
$\mathfrak{S}_d$	The symmetric group on d letters.
$\mathfrak{t}$	Generator of $\operatorname{SL}\left(2,\mathbb{Z}\right)$ given by $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$.
t	The image of $\mathfrak{t}$ under a linear representation of $\operatorname{SL}\left(2,\mathbb{Z}\right)$.
T	T-matrix of a modular category.
$\operatorname{Tr}_{\mathcal{C}}$	The categorical trace in a spherical category.
θ_a	The twist associated to the simple object X_a.
$\theta\left(a,b,c\right)$	Theta symbol given by $\sqrt{d_a d_b d_c}$.
TQFT	Topological Quantum Field Theory.
$V_{\mathbb{K}}$	The places of a number field $\mathbb{K}$.
$v_{\mathfrak{p}}$	The place of $\mathbb{K}$ containing $\left|\cdot\right|_{\mathfrak{p}}$.
v_{σ_j}	The place of $\mathbb{K}$ containing the absolute value $\left|\cdot\right|_{\sigma_j}$.
Vec	The category of vector spaces.
$\operatorname{Vec}_{G,\omega}$	G-graded vector spaces with associativity given by $\omega \in Z^3\left(G,\mathbb{K}^{\times}\right)$.
X_a	The a^{th} (isomorphism class of) simple objects in $\mathcal{C}$.
X^{*}	The (left-) dual object to X in $\mathcal{C}$.

${}^{*}X$	The right dual object of X.
ζ_n	A primitive n^{th} root of unity.
$\mathcal{Z}\left(\mathcal{C}\right)$	The Drinfeld center of the category $\mathcal{C}$.
$Z^3\left(G, \mathbb{K}^{\times}\right)$	3-cocycles of G with coefficients in $\mathbb{K}^{\times}$.
$\overline{\mathbb{Z}}$	Ring of algebraic integers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION

The physics and properties of materials vary greatly depending on their phase– nonetheless at a fundamental level matter in different phases is constructed from the same constituent particles. This is particularly pronounced in crystals where much of the physics of the material can be abstracted to the group describing the crystal structure. Such crystals have been classified and are described by the 230 space groups. Given the rigid crystal structure it is natural to ask how these materials change phase. Understanding such phases and the transitions between them was a great success of Landau, who proposed a mechanism for spontaneous symmetry breaking. This mechanism has enjoyed wide success and has not only been used to study phase transitions in solid state physics, but also the origin of mass through the Higgs mechanism.

In solid state physics, an *ordered state* appears at low temperature when a symmetry is spontaneously broken. For instance, crystal lattices break translational (Figure I.1) and rotational symmetries, liquid crystals break rotational symmetry, and magnets break time reversal symmetry.

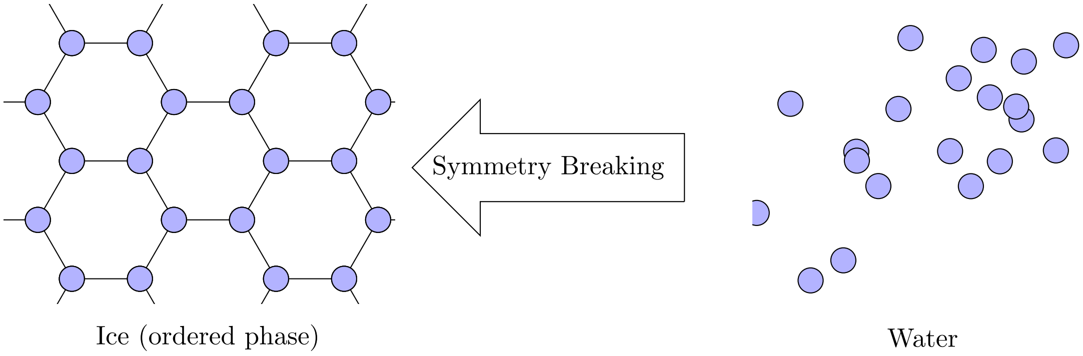


Figure I.1: Water transitioning from liquid (symmetric) to ice (ordered).

These orders are inherently described by geometric symmetries, which has allowed group theory to be employed, and the success of Landau's theory is in part due to this fact. However, in recent years, exotic phases of matter have arisen which go beyond the Landau paradigm.

A physical system is said to be in *topological phase* if at low energies and long wavelengths it is invariant under smooth local perturbations. These phases lack geometric symmetries, that is to say they cannot be described by groups, and hence, they move beyond Landau's symmetry breaking theory. While theoretically interesting, these topological phases have been physically observed. Not only do topological phases describe the fractional quantum hall effect, they have many practical applications ranging from topological insulators to fault-tolerant quantum computers. It is this last application that has drawn the greatest deal of attention and to which we will now turn.

Classically, quantum computers have been analyzed through the qudit paradigm. Heuristically, in this theory one replaces the bits of a classical computer by complex projective spaces known as qudits. A collection of unitary gates are selected and constitute a gate set. Algorithms are then implemented through initializing the qudits and applying a series of gates from the gate set. The results of the computation are then determined through measurements. It has been shown that under this method of computation one can achieve surprising results such as polynomial time integer factorization and super-polynomial search speed increases [NC1]. While successful in an ideal world, this computational model suffers from physical realities. In particular, the computers are susceptible to *decoherence*. This catchall term encompasses the non-unitary thermodynamical interactions between the environment and the computer. Heuristically, decohernece describes processes by which qudits become entangled with the external environment and information "leaks out." Expensive error-correcting codes have been developed [NC1] to combat this problem, but it is highly desirable to have a quantum computer capable of the marvels hinted at by the qudit model, but resistant to decoherence at the hardware level. *Topological quantum computation* utilizes the perturbative invariance of topological phases of matter to overcome the decoherence problems which plague the qudit model.

In order to understand the topological paradigm for quantum computation, we will first consider the canonical example of a topological phase: *fractional quantum hall liquids* (Figure I.2). Such a liquid can be obtained by selecting an appropriate conducting material such as Gallium arsenide. The material is cooled to extremely low temperatures of around 9mK, and is subjected to a strong transverse magnetic field of about 10T. Under these extreme conditions, the system is forced to obey $(2+1)$-dimensional physics. Heuristically, at such low temperatures and under such a strong transverse magnetic field, the electrons become increasingly dense and lack the kinetic energy to "hop over" neighboring electrons. In this way, the sample is convinced that it resides in two spatial dimensions and one temporal dimension. Under the appropriate conditions, an energy gap appears separating the ground state from the first excited state. This ground state is topologically protected, that is it depends only on the topology of the system. When the system is excited, defects known as *quasi-particles* appear in the fluid. These are regions in the fluid where electrons are either very dense or very sparse. These quasi-particles are emergent degrees of freedom and can be made to behave as irreducible stable particles.

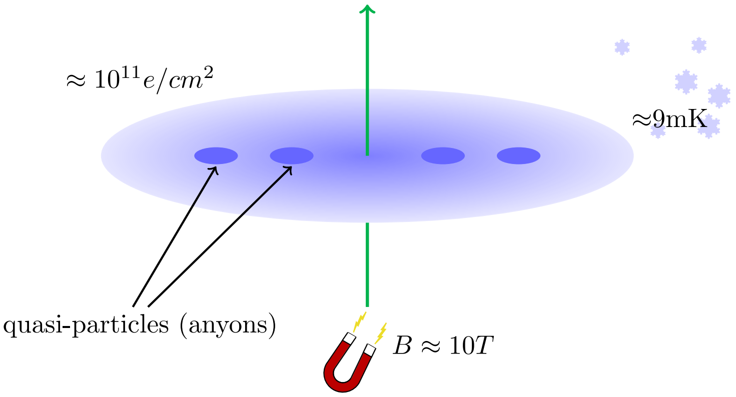


Figure I.2: A fractional quantum hall fluid. The protoypical example of a topological phase.

These quasi-particles are stable and can be moved in the plane. Viewing time as a third dimension, we can trace the path of two such quasi-particles as their positions are exchanged, Figure I.3.

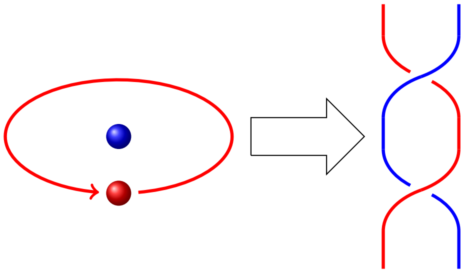


Figure I.3: Exchanging two particles can be understood through braiding their world-lines.

In 4 or more dimensions, one could find a hyperplane separating these *world-lines* and hence the apparent braid would be continuously deformable to an identity transformation, Figure I.4.

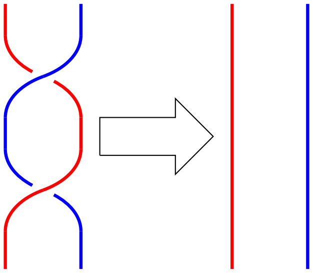


Figure I.4: There are no non-trivial braids in 4 or more dimensions.

At the level of quantum mechanics, this is expressed by saying that the wave function transforms as under a representation of the symmetric group. In particular, exchanging the particles twice results in a braid which is continuously deformable to the identity and so the wave function must be unchanged. Consequently, a single exchange can, at worst, result in a change of sign of the wave function. That is,

$$|\psi\left(z_1,z_2\right)\rangle = \pm|\psi\left(z_2,z_1\right)\rangle$$

These two signs correspond to bosons (+) and fermions (-).

Things are quite different in our $(2+1)$-dimensional system. Here, the world-lines are legitimately entangled and so the wave function no longer transforms under a representation of the symmetric group, but rather under a representation of the braid group.

$$\mathcal{B}_n = \langle \sigma_1,\ldots,\sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2, \text{ and } \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_i\rangle$$

The braid group has highly nontrivial representations that lead to a continuum of particle types known as *anyons*, which generalize the familiar bosons and fermions. As two anyons braid around each other, they continuously transform under a representation of the braid group depending on their particle type. Since the system is invariant under smooth local perturbations, such a transformation depends only on the topology of the braid. In this way, the anyons “remember” the braid topology and this can be used to perform computations. To do this, one begins with a vacuum state and produces particle/anti-particle pairs through exciting the system. These particles are then (adiabatically) braided and pair-wise fused. Since the particle has transformed in a non-trivial way in response to the topology of the braid the particle/antiparticle pairs may not fuse to produce the vacuum, and in fact, the probability of measuring the vacuum at the end of the fusion process is the computation, Figure I.5.

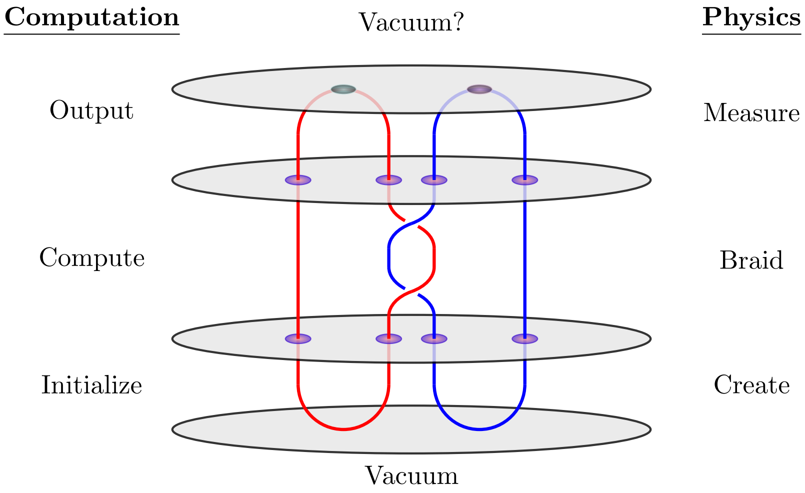


Figure I.5: Computations can be performed by braiding anyons in special topological phases. Under favorable circumstances, this model is universal for quantum computation [RSW].

While this model is conceptually simple, one can show that, under certain conditions, such a model is universal for quantum computation [RSW; W1; NR1; RW1]. Moreover, since the computation depends only on the topology of the system, it is inherently resistant to thermal jitters, that is, it is resistant to decoherence at the hardware level.

Given the use of topological phases in the construction of fault-tolerant quantum computers, one would like to have a mathematical description of them. By definition, topological phases are governed by $(2+1)$-dimensional topological quantum field theories (TQFTs). The canonical example of such a theory is given by the so-called *Chern-Simons action*:

$$S = \frac{k}{2\pi} \int_{\mathcal{M}} \mathrm{Tr} \left(A \wedge dA + \frac{2}{3} A \wedge A \wedge A \right)$$

where $\mathcal{M}$ is a 3-manifold, A is a connection of a principle G-bundle over $\mathcal{M}$, for some (gauge) group G, and k is an integer known as the *level*. It has been conjectured that these actions with specific gauge groups and certain levels correspond exactly to fractional quantum hall fluids for certain filling fractions [W3; RR1; Wi1].[1]

Conjecture I.0.1 (Extended Read-Rezayi Conjecture)**.** *The topological quantum field theory modeling fractional quantum hall liquids at filling fraction* $\nu = 2 + \frac{k}{k+2}$ *is the* $\mathrm{SU}(2)_k$ *Chern-Simons theory.*

In order to understand $(2+1)$-TQFTs, one could attempt to determine other topologically invariant actions. However, from a mathematical perspective, this is unsatisfying. Not only are the path

[1] Recall that the *filling fraction* is the the ratio of electrons to flux quanta.

integrals of quantum field theory famously ill-defined mathematically, but the whole study lacks a certain degree of rigor. This deficiency was rectified by Atiyah who axiomatized topological quantum field theories [At1; Wal1; Wal2].

From Atiyah's axioms, it has been shown that these topological quantum field theories can be abstracted to algebraic objects known as *(pre)modular categories* [Tu1; W1; WW1; K1]. While every (pre)modular category gives rise to a TQFT, it remains at the level of conjecture that every (physical) TQFT is describable by such a category. This is similar to the study of crystals in condensed matter, where one can abstract the study of the physics away to studying the space groups. Just as a classification of space groups allows one to completely describe 3-dimensional crystals, a complete classification of (pre)modular categories would allow one to describe $(2+1)$-dimensional TQFTs. In addition to providing a description of TQFTs, (pre)modular categories describe representations of quasi-Hopf algebras and generate link, knot, and 3-manifold invariants [Tu1; W1; ENO1; DGNO1].

The classification of these categories will be the central theme of this thesis. In Chapter II, we will review (pre)modular categories and their graphical calculus. In Chapter III, we will discuss some arithmetic properties that must be satisfied by modular categories and how these number theoretic structures can be used in classification. These properties will be applied in Chapter IV to show that there are finitely many modular categories (up to equivalence) of fixed *rank* and hence classification is a computationally feasible problem. This lays to rest Wang's Conjecture [W3]:

Conjecture I.0.2. *Up to equivalence, there are finitely many modular categories of fixed rank r.*

This finiteness question has plagued the classification field since its inceptions in 2003. The proof of this finiteness statement suggests an algorithm for classification, which is explored in Chapter V. In Chapter V, we will classify (up to Grothendieck equivalence) integral modular categories through rank 7, weakly integral modular categories through rank 6, and review the classification of maximally non-self dual modular categories through rank 11 thereby extending the classification of [RSW; BR1; HR1; BNRW1]. Moving beyond the modular setting to the premodular setting has traditionally been very difficult but this problem will nonetheless be considered in Chapter VI. In Chapter VI we will extend, the classification of premodular categories (up to Grothendieck equivalence) to rank 4. This will necessitate extending the 2nd Frobenius-Schur indicator to the premodular setting. We will conclude with some future directions in Chapter VII.

CHAPTER II
PRELIMINARIES

While natural, the axiomatic structure of a (pre)modular category is rather involved and is made more clear through a gradual pedagogical approach. From a mathematical perspective, the study of (pre)modular categories is an outgrowth of *(braided) fusion categories* which can, themselves, be viewed as an axiomatization of representation theory. (Braided) fusion categories have a natural tensor and direct sum structure, a notion of semisimplicity, and a notion of duality. However, unlike in representation theory, the constituent objects in a fusion category need not have internal structure, e.g., be vector spaces, and a categorical treatment is required.

These preliminary sections should provide a basic primer on the theoretical tools and constructions required in this paper. Specialized concepts such as the Galois symmetries will be discussed in later chapters. This chapter is not meant to be comprehensive and further detail and proofs can be found in many excellent texts such as [ENO1; ENO2; DGNO1; N2; Tu1; BKi].

In Sections II.1, II.2, and II.3, we will discuss the basics of (braided) fusion and (pre)modular categories as well as introduce the graphical calculus for ribbon categories. In Section II.4, we will examine the Müger center and its relationship to the stratification of (pre)modular categories into symmetric, properly premodular, and modular. We will also briefly discuss the Drinfeld center construction. Then, in Section II.5, we will introduce the Frobenius-Perron dimension and consider its relationship to the categorical dimension. The Frobenius-Perron dimension will be used to stratify fusion categories based on the "integrality" of their dimensions. G-gradings, G-extensions, and the adjoint subcategory will be considered in Section II.6. The preliminaries will then be concluded in Section II.7 with an extended example.

II.1 Braided Fusion Categories

In this section, we will introduce the notion of a braided fusion category. These categories can be viewed as an axiomatization of representation theory. Given that representations can be viewed through rings and modules it is perhaps unsurprising that our analysis begins with the categorification of the notion of a monoid known as a monoidal category. Shortly, we will see that the structure of a monoidal category naturally captures the structure of tensor products of representations and vector spaces.

Definition II.1.1. A **monoidal category** is a category $\mathcal{C}$ equipped with:

(i) A functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ called a **tensor product** with images of objects (X, Y) and morphisms (f, g) written as $X \otimes Y$ and $f \otimes g$ respectively.

(ii) An object $\mathbb{I}$ called the **unit object**.

(iii) A family of natural isomorphisms $\alpha_{X,Y,Z} : (X \otimes Y) \otimes Z \cong X \otimes (Y \otimes Z)$ called **associativities**.

(iv) A pair of natrual isomorphisms $l_X : \mathbb{I} \otimes X \cong X$ and d$r_X : X \otimes \mathbb{I} \cong X$ for each object X in $\mathcal{C}$.

Such that the following diagrams commute:

(i) Unit Coherence Law:

$$\begin{tikzcd}
(X \otimes \mathbb{I}) \otimes Y \arrow[rr, "\alpha_{X,\mathbb{I},Y}"] \arrow[dr, "r_X \otimes \mathrm{Id}_Y"'] & & X \otimes (\mathbb{I} \otimes Y) \arrow[dl, "\mathrm{Id}_X \otimes l_Y"] \\
& X \otimes Y &
\end{tikzcd}$$

(ii) Associativity Coherence Law:[1]

$$\begin{tikzcd}
& (X \otimes (Y \otimes Z)) \otimes W \arrow[dl, "\alpha_{X,Y \otimes Z,W}"'] & \\
X \otimes ((Y \otimes Z) \otimes W) \arrow[d, "\mathrm{Id}_X \otimes \alpha_{Y,Z,W}"'] & & ((X \otimes Y) \otimes Z) \otimes W \arrow[ul, "\alpha_{X,Y,Z} \otimes \mathrm{Id}_W"'] \arrow[d, "\alpha_{X \otimes Y,Z,W}"] \\
X \otimes (Y \otimes (Z \otimes W)) & & (X \otimes Y) \otimes (Z \otimes W) \arrow[ll, "\alpha_{X,Y,Z \otimes W}"]
\end{tikzcd}$$

As previously stated, a monoidal category is a categorification of the familiar notion of a monoid. Indeed, the isomorphism classes of a small monoidal category naturally have the structure of a monoid with multiplication given by $\otimes$ and unit $\mathbb{I}$.

Example II.1.2. *The category **Set** forms a monoidal category with $\otimes$ given by Cartesian product, and the isomorphism class of $\mathbb{I}$ given by the isomorphism class of 1-element sets.*

Example II.1.3. *If G is a group, then* $\mathrm{Rep}\,(G)$*, the category of finite dimensional representations of G, is a monoidal category where:*

(i) The objects are representations of G.

(ii) The tensor product is given by the tensor product of two representations.

(iii) The Hom-spaces consist of intertwiners.

(iv) The neutral object $\mathbb{I}$ is given by the isomorphism class of the trivial representation.

While it is immediate that finite dimensional representations of a finite group form a monoidal category, it is equally clear that not all of the structure of group representations is captured by a

[1] This diagram is typically referred to as the **pentagon**.

monoidal category. For instance, all representations of a finite group can be decomposed into direct sums of irreducible representations. Additionally one can always construct dual representations of finite dimensional representations. While there is no *a priori* vector space structure on the objects of a monoidal category, it is relatively straightforward to abstract away the notion of a duality and the double dual isomorphism. These give rise to so called *rigid* and *pivotal* structures on a monoidal category.

Definition II.1.4. An object X^* in $\mathcal{C}$ is called the **left-dual** of an object X of $\mathcal{C}$ if there exist morphisms:

$$\mathrm{ev}_X : X^* \otimes X \to \mathbb{I} \quad \text{and} \quad \mathrm{coev}_X : \mathbb{I} \to X \otimes X^*$$

called **evaluation** and **coevaluation** such that the following compositions are identity morphisms:

$$\begin{gathered} X \xrightarrow{\mathrm{coev}_X \otimes id_X} (X \otimes X^*) \otimes X \xrightarrow{\alpha_{X,X^*,X}} X \otimes (X^* \otimes X) \xrightarrow{id_X \otimes \mathrm{ev}_X} X \\ X^* \xrightarrow{id_{X^*} \otimes \mathrm{coev}_X} X^* \otimes (X \otimes X^*) \xrightarrow{\alpha^{-1}_{X,X^*,X}} (X^* \otimes X) \otimes X^* \xrightarrow{\mathrm{ev}_X \otimes id_{X^*}} X^* \end{gathered} \tag{II.1}$$

Similarly, an object ${}^*X$ is said to be a **right-dual** of an object X of $\mathcal{C}$ if there exist morphisms:

$$\mathrm{ev}'_X : X \otimes {}^*X \to \mathbb{I} \quad \text{and} \quad \mathrm{coev}'_X : \mathbb{I} \to {}^*X \otimes X$$

such that the following compositions are identity morphisms:

$$\begin{gathered} X \xrightarrow{id_X \otimes \mathrm{coev}'_X} X \otimes ({}^*X \otimes X) \xrightarrow{\alpha^{-1}_{X,{}^*X,X}} (X \otimes {}^*X) \otimes X \xrightarrow{\mathrm{ev}'_X \otimes id_X} X \\ {}^*X \xrightarrow{\mathrm{coev}'_X \otimes id_{{}^*X}} ({}^*X \otimes X) \otimes {}^*X \xrightarrow{\alpha_{{}^*X,X,{}^*X}} {}^*X \otimes (X \otimes {}^*X) \xrightarrow{id_{{}^*X} \otimes \mathrm{ev}'_X} {}^*X \end{gathered}$$

These duals naturally induce dual morphisms. That is, if X and Y are objects of $\mathcal{C}$ with left-duals X^* and Y^* and $f : X \to Y$ is a morphism, then there is a **left-dual morphism** $f^* : Y^* \to X^*$ given by:

$$\begin{gathered} Y^* \xrightarrow{id_{Y^*} \otimes \mathrm{coev}_X} Y \otimes (X \otimes X^*) \xrightarrow{\alpha^{-1}_{Y^*,X,X^*}} (Y^* \otimes X) \otimes X^* \\ \xrightarrow{(id_{Y^*} \otimes f) \otimes id_{X^*}} (Y^* \otimes Y) \otimes X^* \xrightarrow{\mathrm{ev}_Y \otimes id_{X^*}} X^* \end{gathered}$$

and similarly, right-duals ${}^*X$ and ${}^*Y$ induce right-dual morphisms ${}^*f : {}^*Y \to {}^*X$.

Remark II.1.5.

(i) If X^* is a a left-dual of an object X, then X is the right-dual of X^* with $\mathrm{ev}'_{X^*} = \mathrm{ev}_X$ and $\mathrm{coev}'_{X^*} = \mathrm{coev}_X$.

(ii) It can be shown that if X has a right (resp. left) dual object, then it is unique up to isomorphism [N2].

Definition II.1.6. A monoidal category such that every object has left- and right-duals is said to be **rigid**.

Remark II.1.7. The fact that these duals (when they exist) are unique implies that rigidity is a property that certain monoidal categories possess, not a structure to be imposed.

As alluded to above, these dualities provide a categorification of the notion of a vector space duality.

Example II.1.8. *If V is a finite dimensional $\mathbb{K}$-vector space with basis $\{v_i\}$, and $V^\vee = \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K})$ is the dual vector space with dual basis $\{v^i\}$, then we can form maps:*

$$\begin{aligned} \mathrm{ev}_V : V^\vee \otimes V \to \mathbb{K} \quad & \nu \otimes v \mapsto \nu(v) \\ \mathrm{coev}_V : \mathbb{K} \to V \otimes V^\vee \quad & k \mapsto \sum_j k v_j \otimes v^j \end{aligned}$$

These maps can be used to make $V^\vee$ a left (and right) dual of V.

This duality structure extends to the finite dimensional representations of groups in a natural way.

Example II.1.9. *If G is a group, then the category $\mathrm{Rep}(G)$ is rigid. The left- and right-dual of $\rho : G \to GL(V)$ coincide and are given by the dual representation $\rho^* : G \to GL(V^\vee)$ where $\rho^*(g) = \rho(g^{-1})^\vee$.*

While in a rigid category, it is true that the left- and right-dual functions are quasi-inverses [N2], i.e. ${}^*(X^*) \cong X \cong ({}^*X)^*$, there is no *a priori* notion of the double dual isomorphism of representation theory. However, one can impose such a structure.

Definition II.1.10. If $\mathcal{C}$ is a rigid monoidal category, then a **pivotal structure** on $\mathcal{C}$ is an isomorphism of monoidal functors: $j_X : X \tilde{\to} X^{**}$. That is to say, it is a collection of morphisms $j_X : X \tilde{\to} X^{**}$ such that for all objects X and Y in $\mathcal{C}$ we have:

(i) $j_{X \otimes Y} = j_X \otimes j_Y$.

(ii) $j_{\mathbb{I}} = \mathrm{Id}_{\mathbb{I}}$.

(iii) $j_{X^*} = (j_X^*)^{-1}$.

Remark II.1.11. In a pivotal category, we can always express the right-dual ${}^*X$ in terms of the left-dual X^*. Indeed, ${}^*X \cong {}^*j_X(X) = {}^*(X^{**}) \cong X^*$, where the last isomorphism follows from the afore mentioned fact that the left- and right-duals are mutually quasi-inverses in $\mathcal{C}$. For this reason, we will cease discussion of the right-dual and simply consider the left-dual; furthermore the object X^* will simply be called the **dual** of X.

In a pivotal monoidal category, one has two, *a priori* different, notions of trace on $\mathrm{End}_{\mathcal{C}}(X)$ for any object X of $\mathcal{C}$. For X in $\mathcal{C}$ and $f \in \operatorname{End}_{\mathcal{C}}(X)$, we have the **left- (resp. right-) pivotal traces** $\operatorname{ptr}^{\ell}(f)$ (resp. $\operatorname{ptr}^{r}(f)$) respectively given by:

$$\mathbb{I} \xrightarrow{\operatorname{coev}_X} X \otimes X^* \xrightarrow{f \otimes id_{X^*}} X \otimes X^* \xrightarrow{j_X \otimes id_{X^*}} X^{**} \otimes X^* \xrightarrow{\operatorname{ev}_{X^*}} \mathbb{I}$$

$$\mathbb{I} \xrightarrow{\operatorname{coev}_{X^*}} X^* \otimes X^{**} \xrightarrow{id_{X^*} \otimes j_X^{-1}} X^* \otimes X \xrightarrow{id_{X^*} \otimes f} X^* \otimes X \xrightarrow{\operatorname{ev}_X} \mathbb{I}$$

These traces allow us to associate certain elements of $\operatorname{End}_{\mathcal{C}}(\mathbb{I})$ to each object in the category.

Definition II.1.12. If X is an object in a pivotal category $\mathcal{C}$, then the **left- (resp. right-) pivotal dimensions** of X are respectively given by

$$d^{\ell}(X) := \operatorname{ptr}^{\ell}(id_X), \quad \text{and} \quad d^{r}(X) := \operatorname{ptr}^{r}(id_X)$$

It follows from the definition of pivotal trace that the left- (resp. right-) pivotal dimension of X and X^{**} coincide. Furthermore, it can be shown that $d^{\ell}(X) = d^{r}(X^*)$ [N2].

Example II.1.13. *Returning to our finite dimensional $\mathbb{K}$-vector space example, we have the usual double dual isomorphism $j_V : V \to V^{**}$ given by $j_V(v)(\phi) = \phi(v)$ for any $v \in V$ and $\phi \in V^{\vee}$. Thus, we can compute the right-pivotal trace of $T \in \operatorname{End}_{\mathbb{K}}(V)$. For this computation, we will express T as an element of $V \otimes V^{\vee}$, explicitly we have $T = \sum_{i,j} T^i_j v_i \otimes v^j$. We can now compute the right-pivotal trace as follows:*

$$1 \mapsto \sum_j v_j \otimes v^j \mapsto \sum_j T(v_j) \otimes v^j \mapsto \sum_{i,j} T^i_j \operatorname{ev}_{V^{\vee}}\left(j_V(v_i) \otimes v^j\right) = \sum_j T^j_j = \operatorname{Tr}(T)$$

That is $\operatorname{ptr}^{r}(T) \in \operatorname{End}_{\mathbb{K}}(\mathbb{K}) \cong \mathbb{K}$ *is simply the usual trace* $\operatorname{Tr}(T)$. *An analogous calculation reveals that* $\operatorname{ptr}^{\ell}(T) = \operatorname{Tr}(T)$.

Similarly, the left- (resp. right-) pivotal traces in $\operatorname{Rep}(G)$ coincide and produce the degree of the representation. One might hope that in general the left-and right-pivotal traces agree; sadly, this is not always true.

Definition II.1.14. A pivotal monoidal category is said to be **spherical** if for all objects X, we have $d^{\ell}(X) = d^{r}(X)$.

Remark II.1.15. Clearly, sphericality is a property of certain pivotal categories and not a structure. However, in the spherical setting, one often refers to the pivotal structure as a spherical structure. It can be shown that in *modular categories*, the number of distinct spherical structures is indexed by the number of self-dual invertible objects [BNRW1].

Remark II.1.16. We will see later (Proposition II.1.31) that in the situations that are of interest to us, this spherical condition will guarantee that $\operatorname{ptr}^{r}(f) = \operatorname{ptr}^{\ell}(f)$ for any f.

Note that currently these traces reside in the group $\operatorname{End}_{\mathcal{C}}(\mathbb{I})$, while in the vector space setting, this trace was seen to be a number by virtue of $\mathrm{End}_{\mathbb{K}}(\mathbb{K}) \cong \mathbb{K}$ for some field $\mathbb{K}$. Clearly, a necessary condition for a category to begin to capture this structure is that $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$ is a (1-dimensional) $\mathbb{K}$-vector space for some field $\mathbb{K}$. This leads to the notion of $\mathbb{K}$-linearity.

Definition II.1.17. If $\mathbb{K}$ is a field, then a category $\mathcal{C}$ is said to be **$\mathbb{K}$-linear** if $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is a $\mathbb{K}$-vector space for all objects X and Y, and composition of morphisms is bilinear.

One might wonder if there are certain settings in which the field $\mathbb{K}$ naturally arises from the categorical data. In fact there are, but first there are several additional structures that must be imposed. These additional structures are natural in the context of representation theory and allow one to speak of direct sums, kernels, and semisimplicity. We will take some time to discuss these structures which can then be married with the notions of $\mathbb{K}$-linearity and pivotal structures to produce an axiomatization of representations of finite groups known as a fusion category. In the fusion setting, the field $\mathbb{K}$ naturally arises as $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$.

To begin our discussion of semisimplicity, we need a notion of direct sums. The exact categorical notion is that of an **abelian category** [Mac; BKi].

Definition II.1.18. A category $\mathcal{C}$ is **abelian** if:

(i) For any two objects X, Y in $\mathcal{C}$, the set $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is an abelian group with binary operation $+$ and identity denoted by 0 such that the composition of morphisms is bilinear.

(ii) $\mathcal{C}$ admits a **zero object** denoted 0 such that for all X in $\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(X, 0)$ and $\mathrm{Hom}_{\mathcal{C}}(0, X)$ contains exactly 1 morphism, i.e. 0 is both an initial and terminal object.

(iv) $\mathcal{C}$ admits finite direct sums (a biproduct).

(v) Every arrow has a kernel and cokernel.

(vi) Every monic arrow is a kernel and every epi is a cokernel. In particular, if f is monic, then $f = \ker(\mathrm{coker}(f))$ and if f is epi, then $f = \mathrm{coker}(\ker(f))$.

Abelian actually gives quite a lot more than direct sums. For instance, an abelian category is exactly the required structure for the use of kernel and cokernel in the familiar homological way, e.g. there are analogs of the Snake Lemma and the (Short) Five-Lemma. Given the homological importance of abelian categories, it is perhaps not surprising that they are prevalent in modern mathematics.

Example II.1.19. *The following categories are abelian:*

(i) The category of left R-modules for any ring R. In particular, abelian groups are abelian categories.

(ii) The category of complexes of left R-modules for any ring R.

(iii) The category of sheaves of abelian groups over a topological space.

Abelian categories are the natural arena for discussing semisimplicity. Such a notion is vital to understanding representation theory. Indeed, when studying representations of a finite group, it is well-known that all representations can be constructed from distinguished (irreducible) representations. These irreducible representations are simple in the module sense and one says that $\mathrm{Rep}\left(G\right)$ is semisimple, since every object can be described by a direct sum of the simple ones. More generally, one can define simplicity and semisimplicity in an abelian category.

Definition II.1.20. If $\mathcal{C}$ is an abelian category, then an object X is **simple** if it is not isomorphic to the zero object and any subobject of X is isomorphic to X or 0.

The notion of simplicity allows one to prove a version of Schur's Lemma for abelian categories [N2].

Theorem II.1.21 (Schur's Lemma)**.** *If $\mathcal{C}$ is an abelian category and X and Y simple objects, then any non-zero morphism $f \in \mathrm{Hom}_{\mathcal{C}}\left(X, Y\right)$ is an isomorphism. In particular, if X is not isomorphic to Y, then $\mathrm{Hom}_{\mathcal{C}}\left(X, Y\right) = 0$ and $\mathrm{End}_{\mathcal{C}}\left(X\right)$ is a division algebra.*

Proof. Suppose that $f \in \mathrm{Hom}_{\mathcal{C}}\left(X, Y\right)$ is a non-zero morphism. Then $\ker\left(f\right)$ exists since $\mathcal{C}$ is abelian and is a subobject of X. Since X is simple and f is non-zero, we can conclude that $\ker\left(f\right) = 0$. Similarly, $\mathrm{coker}\left(f\right)$ is a quotient object of Y which is necessarily 0 by simplicity of Y. Thus f is an isomorphism. The rest of the statement follows. □

Remark II.1.22. The collection of isomorphism classes of simple objects in an abelian category, $\mathcal{C}$, will be denoted by $\mathrm{Irr}\left(\mathcal{C}\right)$ and the isomorphism classes will be labeled by X_a. Occasionally, X_a will be used to also denote a representative of this equivalence class, though from context no confusion should arise. By standard abuse of notation, we will often use $\mathrm{Irr}\left(\mathcal{C}\right)$ to denote the label set of the isomorphism classes of simple objects, that is we might say $a \in \mathrm{Irr}\left(\mathcal{C}\right)$ rather than $X_a \in \mathrm{Irr}\left(\mathcal{C}\right)$.

Finally, we may define semisimplicity as in [BKi].

Definition II.1.23. An abelian category, $\mathcal{C}$, is **semisimple** if any object X in $\mathcal{C}$ is isomorphic to a direct sum of simple objects:

$$X \cong \bigoplus_{a \in \mathrm{Irr}(\mathcal{C})} \mu_a X_a$$

where the $\mu_a \in \mathbb{N}$ and only finitely many are non-zero.

These notions can be combined to form a *(multi)fusion category.*

Definition II.1.24. A category $\mathcal{C}$ is a **fusion category** if it is an abelian, pivotal, semisimple, $\mathbb{K}$-linear, monoidal category for some field $\mathbb{K}$, such that:

(i) $\mathbb{I}$ is simple.

(ii) There are finitely many isomorphism classes of simple objects. The number of such isomorphism classes is called the **rank**.

(iii) $\mathcal{C}$ is locally finite. That is:

(a) $\mathcal{C}$ is essentially small, i.e. the isomorphism classes of objects form sets.

(b) For any two objects X and Y in $\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is a finite dimensional $\mathbb{K}$-vector space.

(c) Every object has finite length, i.e. for every object X in $\mathcal{C}$, there is a finite sequence of subobjects $0 = X_0 \subset X_1 \subset \ldots \subset X_n = X$ such that X_k/X_{k-1} is simple [N1].[2]

Remark II.1.25. If one does not assume that $\mathbb{I}$ is simple in the above definition, then the category is said to be a **multifusion category**. Very little is known about multifusion categories and we will not consider them further in our analysis.

Remark II.1.26. We will continue to refer to the isomorphism classes of simple objects as X_a in the fusion setting. However, we will select an ordering of the objects such that X_0 corresponds to the isomorphism class of $\mathbb{I}$.

In the fusion setting, there are several nice coincidences. First, there are pronounced ring and module structures, which are particularly powerful when the field $\mathbb{K}$ is algebraically closed.

Proposition II.1.27. *If $\mathcal{C}$ is an abelian monoidal category, then $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$ is a ring. Furthermore, for any two objects X and Y of $\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is an $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$-module.*

Proof. First note that since $\mathcal{C}$ is abelian, we know that $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$ is an additive abelian group. Associativity of $\mathcal{C}$ and functoriality of $\otimes$ establish that $+$ and $\otimes$ are compatible in the ring sense. Thus, it follows that $(\mathrm{End}_{\mathcal{C}}(\mathbb{I}), +, \otimes)$ is a ring.

Next note, that if $f \in \mathrm{End}_{\mathcal{C}}(\mathbb{I})$ and $g \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, then $f \otimes g \in \mathrm{Hom}_{\mathcal{C}}(\mathbb{I} \otimes X, \mathbb{I} \otimes Y) \cong \mathrm{Hom}_{\mathcal{C}}(X, Y)$ establishes an action of $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$ on $\mathrm{Hom}_{\mathcal{C}}(X, Y)$. The fact that this action satisfies the module axioms follows immediately from functoriality of $\otimes$ and associativity of $\mathcal{C}$. □

The ring $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$ is called the **ground ring** of $\mathcal{C}$ and is typically denoted by $K_{\mathcal{C}}$. In the case that $\mathbb{K}$ is an algebraically closed field and $\mathcal{C}$ is a fusion category, the ground ring coincides with the field $\mathbb{K}$. In this setting, one often speaks of the **ground field**. In fact, something slightly stronger can be said which not only allows one to extract the ground field from the hom-spaces, but also provides a simple method for testing simplicity of objects.

Proposition II.1.28. *If $\mathbb{K}$ is an algebraically closed field and $\mathcal{C}$ is a fusion category over $\mathbb{K}$, then X is simple in $\mathcal{C}$ if and only if $\mathrm{End}_{\mathcal{C}}(X) \cong \mathbb{K}$.*

Proof. If X is simple, then Theorem II.1.21 implies that $\mathrm{End}_{\mathcal{C}}(X)$ is a division algebra and so by $\mathbb{K}$-linearity, it is a $\mathbb{K}$-algebra. However, the only finite dimensional division algebra over an algebraically closed field $\mathbb{K}$ is $\mathbb{K}$, and thus $\mathbb{K} \cong \mathrm{End}_{\mathcal{C}}(X)$. The converse statement follows by semisimplicity, Schur's Lemma, and dimension count. □

[2] This assumption is superfluous in the fusion setting due to semisimplicity. However, it is typically included in the defnition of locally finite and so we state it for completeness.

Corollary II.1.29. *Let $\mathbb{K}$ be an algebraically closed field and $\mathcal{C}$ be a fusion category over $\mathbb{K}$. If X_a and X_b are isomorphism classes of simple objects in $\mathcal{C}$, then* $\operatorname{Hom}_{\mathcal{C}}(X_a, X_b) \cong \mathbb{K}\delta_{a,b}$.

Proof. This follows immediately from Theorem II.1.21 and Proposition II.1.28. □

This structure can be utilized to show that the traces are well behaved in spherical fusion categories. In particular, we need not distinguish between left- and right-pivotal traces [N2].

Proposition II.1.30. *If $\mathcal{C}$ is a pivotal abelian category, $f \in \operatorname{End}_{\mathcal{C}}(X)$, and $g \in \operatorname{End}_{\mathcal{C}}(Y)$, then:*

(i) $\operatorname{ptr}^r(f \oplus g) = \operatorname{ptr}^r(f) + \operatorname{ptr}^r(f)$

(ii) $\operatorname{ptr}^r(f \otimes g) = \operatorname{ptr}^r(f)\operatorname{ptr}^r(g)$

and similarly for prt^{ℓ}.

This result allows us to show that the left-and right-pivotal traces coincide in a spherical fusion category over an algebraically closed field.

Proposition II.1.31. *If $\mathcal{C}$ is a spherical fusion category over an algebraically closed field $\mathbb{K}$, then* $\operatorname{ptr}^{\ell}(f) = \operatorname{ptr}^r(f)$ *for any $f \in \operatorname{End}_{\mathcal{C}}(X)$ and any X in $\mathcal{C}$.*

Proof. Suppose that $f \in \operatorname{End}_{\mathcal{C}}(X)$. Then since $X \cong \bigoplus_a \mu_a X_a$ for some $\mu_a \in \mathbb{N}$, it suffices to consider $f \in \operatorname{End}_{\mathcal{C}}(X_a)$. By Proposition II.1.28, we know that $\operatorname{End}_{\mathcal{C}}(X_a)$ is a 1-dimensional $\mathbb{K}$-vector space. In particular, $\exists k \in \mathbb{K}$ such that $f = k \operatorname{Id}_{X_a}$. Thus

$$\operatorname{ptr}^r(f) = \operatorname{ptr}^r(k \operatorname{Id}_{X_a}) = kd^r(X_a) = kd^{\ell}(X_a) = \operatorname{ptr}^{\ell}(k \operatorname{Id}_{X_a}) = \operatorname{ptr}^{\ell}(f)$$

□

Remark II.1.32. In light of this result, we will refer to the trace, $\operatorname{Tr}_{\mathcal{C}}$, in a spherical fusion category over an algebraically closed field $\mathbb{K}$ and will not consider the left- and right-pivotal traces seperately.

The reader may have noticed that while $\operatorname{Rep}(G)$ (for a finite group G) is a fusion category, it has one additional structure which a general fusion category lacks. Indeed, if (r, V) and (σ, W) are representations of G, then $(\rho \otimes \sigma, V \otimes W)$ and $(\sigma \otimes \rho, W \otimes V)$ are isomorphic representations of G. However, in a fusion category, there is no, *a priori*, reason to have $X \otimes Y \cong Y \otimes X$ for objects X and Y of $\mathcal{C}$. Such a commutative structure is called a *braiding.*

Definition II.1.33. A fusion category $\mathcal{C}$ is **braided** if it is equipped with a natural family of isomorphisms, $R_{X,Y} : X \otimes Y \to Y \otimes X$, which are compatible with associativity. That is, the braiding and the associativities must satisfy the **hexagons**:

$$\begin{tikzcd}
& X \otimes (Y \otimes Z) \arrow[r, "R_{X,Y\otimes Z}"] \arrow[dl, "\alpha_{X,Y,Z}"'] & (Y \otimes Z) \otimes X & \\
(X \otimes Y) \otimes Z \arrow[dr, "R_{X,Y} \otimes \mathrm{Id}_Z"'] & & & Y \otimes (Z \otimes X) \arrow[ul, "\alpha_{Y,Z,X}"'] \\
& (Y \otimes X) \otimes Z \arrow[r, "\alpha_{Y,X,Z}"'] & Y \otimes (X \otimes Z) \arrow[ur, "\mathrm{Id}_Y \otimes R_{X,Z}"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
& (X \otimes Y) \otimes Z \arrow[r, "R_{X\otimes Y,Z}"] \arrow[dl, "\alpha_{Z,X,Y}"'] & Z \otimes (X \otimes Y) & \\
X \otimes (Y \otimes Z) \arrow[dr, "R_{X,Z} \otimes \mathrm{Id}_Y"'] & & & (Z \otimes X) \otimes Y \arrow[ul, "\alpha_{X,Y,Z}"'] \\
& X \otimes (Z \otimes Y) \arrow[r, "\alpha_{X,Z,Y}"'] & (X \otimes Z) \otimes Y \arrow[ur, "\mathrm{Id}_X \otimes R_{Y,Z}"'] &
\end{tikzcd}$$

Remark II.1.34. The entire fusion structure is not required for a braiding. In fact, one can discuss braided monoidal categories also known as braided tensor categories. We will not need this level of generality in this work, but in several of the references, this terminology is used.

While (braided) fusion categories are interesting in their own right, we will primarily be interested in (braided) fusion categories which are also spherical.

Definition II.1.35. A spherical braided fusion category is called **premodular**.

Remark II.1.36. It is an open question as to whether or not every fusion category admits a spherical structure. At the time of this writing, there are no known counter examples [EGNO1]. Furthermore, there are methods for constructing spherical fusion categories from fusion categories, which often make the spherical hypothesis unnecessary [ENO1].

Shortly, we will see that there is a natural stratification of premodular categories in which representations of a finite group are in some sense trivial, see Definition II.3.6. Nonetheless, finite group representations comprise an important example of premodular categories.

Example II.1.37. *If G is a finite group, then* $\mathrm{Rep}\,(G)$ *is a premodular category. The objects in this category are representations of G, the simple objects are irreducible representations of G, and the ground ring is $\mathbb{C}$. We can further take the associativity and braiding to be the trivial (familiar)* *maps:*

$$R_{X,Y} : X \otimes Y \to Y \otimes X, \quad x \otimes y \mapsto y \otimes x$$
$$\alpha_{X,Y,Z} : X \otimes (Y \otimes Z) \to (X \otimes Y) \otimes Z, \quad x \otimes (y \otimes z) \mapsto (x \otimes y) \otimes z$$

If we take duality to be the dual on the underlying vector space, and take the pivotal structure to be the canonical double-dual isomorphism on vector spaces, then $\mathrm{Rep}(G)$ *is a premodular category.*

It should be noted that this example holds over more general base fields $\mathbb{K}$*, provided that the order of the group is prime to the characteristic of the base field [ENO1]. Furthermore, the spherical structure described above may not be the only one [D1].*

While this category provided the motivating example for constructing fusion categories, more complicated structures can arise. For instance, the associativity need not be trivial as is illustrated by the following example.

Example II.1.38. *Let G be a finite group and $\omega \in Z^3(G, \mathbb{C}^\times)$ a normalized 3-cocycle.*[3] *Then, we can form the fusion category $Vec_{G,\omega}$ whose objects are G-graded vector spaces. The simple objects in the category are indexed by $g \in G$ and are given by the 1-dimensional vector spaces concentrated in the g-graded component (evaluation modules). The tensor product, dual, and trivial object are immediately inherited from the group structure:*

$$X_g \otimes X_h = X_{gh}, \quad X_g^* = X_{g^{-1}}, \quad \text{and} \quad \mathbb{I} = X_e$$

Given this duality, it is clear that the pivotal structure can be taken to be the identity morphism. Finally, the associativity is specified by the 3-cocycle: $\alpha_{X_g,X_h,X_k} = \omega(g,h,k)\,\mathrm{Id}$. *In this setting, the pentagon corresponds exactly to the 3-cocycle condition, see e.g. [ENO1]:*

$$\omega(h,k,\ell)\,\omega(g,hk,\ell)\,\omega(g,h,k) = \omega(gh,k,\ell)\,\omega(g,h,k\ell)$$

It should further be noted that $Vec_{G,\omega}$ is only braided when G is an abelian group.

Due to the presence of simple objects in a (braided) fusion category, a certain collection of direct sum decompositions are distinguished. In particular, the direct sum decomposition of the tensor product of two simple objects is a **fusion rule** and the corresponding multiplicities are known as **fusion coefficients**.

Utilizing the fusion coefficients and the isomorphism classes of simple objects, one can associate a unital based ring (fusion ring) to any fusion category. In fact, fusion categories can be viewed as a categorification of the notion of such a ring. Given a fusion category, $\mathcal{C}$, the corresponding fusion

[3] "Normalized" is required to satisfy the unit axiom. I would like to thank Marcelo Aguiar for pointing this out.

ring is called the **Grothendieck ring**[4] and has presentation:

$$\mathcal{K}_0(\mathcal{C}) = \langle X_a \in \operatorname{Irr}(\mathcal{C}) \mid X_a \otimes X_b = \bigoplus_{X_c \in \operatorname{Irr}_{\mathcal{C}}} N_{a,b}^c X_c, \quad \forall X_a, X_b \in \operatorname{Irr}(\mathcal{C}) \rangle \tag{II.2}$$

where $N_{a,b}^c = \dim \operatorname{Hom}_{\mathcal{C}}(X_a \otimes X_b, X_c)$ are the **fusion coefficients**.

Given a fusion ring, it is an open question as to when a categorification exists and if it is unique. Indeed, there are examples of fusion rings which do not admit categorifications as well as examples of such rings which admit several categorifications [JL1, Theorem 1.4]. Given this many-to-one relationship, one might wonder what value there is in studying fusion rings. As it turns out, a result due to Adrian Ocneanu shows that a great deal of the categorical data of a fusion category can be captured by its Grothendieck ring [ENO1].

Theorem II.1.39 (Ocneanu Rigidity)**.** *Up to equivalence, there are finitely many fusion categories with a fixed Grothendieck ring.*

This indicates that a study of fusion categories can largely be undertaken by studying their associated Grothendieck rings. In fact, many researchers have done exactly this and studied fusion categories up to **Grothendieck equivalence**.[5] This neatly avoids the monumental problem of solving the hexagon and pentagon relations, that is determining a coherent set of associativities and braidings. One might worry that such a study may lead to a classification of certain fusion rings without an indication as to whether or not they admit categorifications. Oddly enough, this is often not a problem, as we will see below.

In much of this paper, we will be concerned with categories only up to Grothendieck equivalence; however, we will occasionally need to make use of the braiding and associativities. For this reason, we will need to take a short detour to discuss the *fusion* and *splitting spaces* as well as the R- and F*-matrices.*

Since we are concerned with $\mathbb{K}$-linear categories, all of the morphisms can be expressed as linear transformations. In this context one can attempt to select a nice basis so as to diagonalize the braiding, the resulting linear transformations are referred to as R-matrices. When this is done, the associativities can be viewed as a specific change of basis known as the F-matrices.[6] To clearly treat this subject, we will make use of a convenient graphical calculus associated with premodular categories. This calculus will have the added benefit of making clear the need for a spherical structure, as well as providing tools for studying premodular categories.

[4] Often, authors will consider the Grothendieck semiring with presentation (II.2).

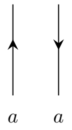
[5] Two categories are Grothendieck equivalent if they have isomorphic Grothendieck rings.

[6] Here, F actually stands for fusion, but should not be confused with the fusion matrices. The reasons for this nomenclature will be made clear when we discuss the graphical representation of these transformations.

II.2 Graphical Calculus and Ribbon Categories

Mathematically, the graphical calculus of this section is motivated by the category of $\mathcal{C}$-colored ribbon tangles (for some category $\mathcal{C}$). Heuristically, this category consists of all oriented non-intersecting ribbons in $\mathbb{R}^3$, which are colored by objects of $\mathcal{C}$ and are permitted to end on coupons. An excellent introduction to this category can be found in [BKi]. This category is not only where ribbon categories derive their name, but can be seen to be universal for ribbon categories in the following sense: For any ribbon category $\mathcal{C}$ there is a ribbon tensor functor from the category of ribbon tangles labeled by $\mathrm{Irr}\,(\mathcal{C})$ whose image is $\mathcal{C}$ [M3]. This fact is what that makes the following graphical calculus mathematically rigorous. However, rather than dwell on this abstract mathematical construct, we will take a more physically motivated approach to the the graphical calculus. This allows one to determine a dictionary between the graphical calculus and the corresponding physical theory [W1, Table 6.1][P1].

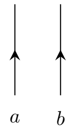
From a physics perspective, the isomorphism classes of simple objects in a fusion category label the irreducible particle types in a TQFT, while mathematically, they are often used to label strands in a link or knot. For this reason, we will take an upward directed line labeled by a to correspond to the isomorphism class X_a and the reversed a-labeled arrow to correspond to a the dual object X_a^*. This conforms to the physical notion of a worldline with time moving upward.[7]



Technically, each vertical segment of these diagrams corresponds to a morphism. For instance, the vertical lines above correspond to $\mathrm{Id}_{X_a} \in \mathrm{Hom}_{\mathcal{C}}\,(X_a, X_a)$ and $\mathrm{Id}_{X_a^*} \in \mathrm{Hom}_{\mathcal{C}}\,(X_a^*, X_a^*)$. This makes sense from the worldline perspective where a vertical line corresponds to a stationary particle.

The tensor product of two simple objects will be graphically denoted by juxtaposition. Thus, the morphism $\mathrm{Id}_{X_a \otimes X_b} = \mathrm{Id}_{X_a} \otimes \mathrm{Id}_{X_b}$ will be graphically depicted by:

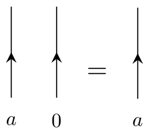
$\mathrm{Id}_{X_a \otimes X_b} =$



By convention, the trivial object, $\mathbb{I} = X_0$ will have no associated line. Physically, the lines correspond to worldlines and the trivial object corresponds to the vacuum label. Thus, it is sensible that the strand corresponding to the trivial object is omitted. Mathematically, we have $X_a \otimes \mathbb{I} \cong X_a$

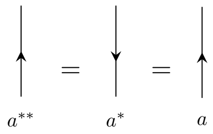
[7] Some authors select a reversed direction with upward arrows corresponding to X_a^*. In such a convention, diagrams must be read from top to bottom rather than bottom to top as it is for us. This is akin to the choice of function composition, e.g. does one select $f \circ g$ or $g \circ f$ to denote f followed by g.

and since the lines depicting object actually correspond to isomorphism classes, we would have:

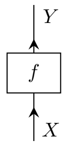


From this perspective, it is natural to simply omit the line corresponding to the trivial object.

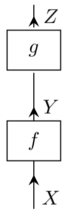
It should be further noted that because the diagrams correspond to isomorphism classes, the double dual isomorphism $j_X : X \to X^{**}$ specified by the pivotal structure need not be explicitly placed in diagram, that is:



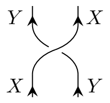
Given the current state of affairs, it is perhaps unsurprising to note that every morphism should have a corresponding diagram. Formally, the diagram corresponding to $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ is graphically depicted by:



Furthermore, composition of morphisms will correspond to vertical stacking of the diagrams, that is if $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, then $g \circ f \in \mathrm{Hom}_{\mathcal{C}}(X, Z)$ is graphically depicted by:

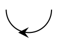
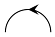


Specifying a map by a box is somewhat unsatisfying and often there are special diagrams corresponding to distinguished maps. For instance, the braiding $R_{X,Y} \in \mathrm{Hom}_{\mathcal{C}}(X \otimes Y, Y \otimes X)$ is graphically depicted by:



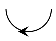
While it would be nice to have diagrams for every morphism in $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, this seems like an insurmountable task. However, $\mathbb{K}$-linearity and semisimplicity imply that we need only specify a basis for **fusion space**, $V^{c}_{a,b} := \mathrm{Hom}_{\mathcal{C}}(X_a \otimes X_b, X_c)$, and the **splitting space**, $V^{a,b}_{c} := \mathrm{Hom}_{\mathcal{C}}(X_c, X_a \otimes X_b)$, as X_a, X_b and X_c range over $\mathrm{Irr}(\mathcal{C})$; this will allow us to express any morphism we like in terms of these bases.

To see how this can be accomplished, we will begin by examining the coevaluation and evaluation maps, which are elements of $\mathrm{Hom}_{\mathcal{C}}(X^* \otimes X, \mathbb{I})$ and $\mathrm{Hom}_{\mathcal{C}}(\mathbb{I}, X \otimes X^*)$ respectively. By convention, we will take their graphical depiction to be of the form:

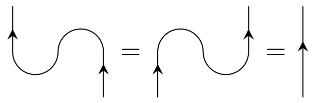
coev =  ev = 

Taking a cue from the physical motivation of a $(2+1)$-TQFT as discussed in Chapter I, one might be tempted to assign the physical meaning of pair-production and annihilation to these two diagrams, and this is exactly right.

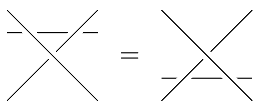
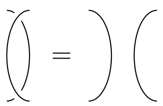
$\mathbb{K}$-linearity of our category tells us that $\mathrm{Hom}_{\mathcal{C}}(X_a^* \otimes X_a, \mathbb{I})$ and $\mathrm{Hom}_{\mathcal{C}}(\mathbb{I}, X_a \otimes X_a^*)$ are $\mathbb{K}$-vector spaces. As it turns out, they are 1-dimensional and so coevaluation and evaluation span these spaces as $\mathbb{K}$-vector spaces. Thus, an arbitrary element of $\mathrm{Hom}_{\mathcal{C}}(\mathbb{I}, X_a \otimes X_a^*)$ is of the form $\lambda\, \mathrm{coev}_{X_a}$ and has graphical depiction:

$\lambda\, \mathrm{coev} = \lambda$ 

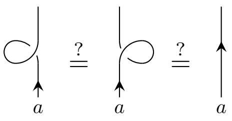
Before we move on to discuss the bases for the fusion and splitting spaces, we must tidy up the rules for our graphical calculus. Indeed, the astute reader may have noticed that certain diagrams can be formed and express certain axioms discussed above. For instance, the rigidity axioms II.1 have the following intuitive graphical interpretation:



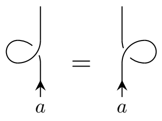
Furthermore, the equation $\mathrm{Id}_X \circ \mathrm{Id}_X = \mathrm{Id}_X$ indicates that the height of a diagrams should not matter. Similar observations lead to the first few rules of the graphical calculus:

 and 

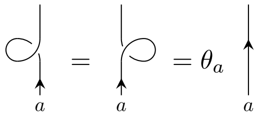
This is highly reminiscent of the Reidemeister moves from knot theory. However, one move is missing:



These are elements of $\mathrm{Hom}_{\mathcal{C}}\left(X_a, X_a\right)$, a 1-dimensional $\mathbb{K}$-vector space, and hence, are scalar multiples of Id_{X_a}. The conventional Riedemiester moves would imply that these diagrams are in fact both equal to Id_{X_a}. However, this is not the case in this context. In fact, in a general braided fusion category there is no, *a priori*, reason that these diagrams should be related at all. The condition that:



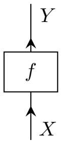
is known as **sphericality** or a **spherical structure** and a braided fusion category with a spherical structure (a spherical braided fusion category) is a special type of **ribbon category** known as **premodular**.[8] Thus in the premodular setting, we have the rule:



and the scalar θ_a is known as a **twist**.

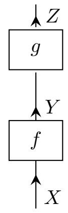
Remark II.2.1. A twist is actually special type of natural tensor automorphism. However, it is common to refer to the associated scalar, $\theta_a \in \mathbb{K}$, as a twist in addition to the endomorphism $\theta_a \in \mathrm{End}_{\mathcal{C}}\left(X_a\right) \cong \mathbb{K}$.

This leads to the so-called **Kirby calculus** of ribbon categories [BKi; Tu1]. That is, all morphisms $f \in \mathrm{Hom}_{\mathcal{C}}\left(X, Y\right)$ correspond to a diagram:

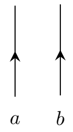


[8] Technically a ribbon category is a spherical (and hence pivotal) braided $\mathbb{K}$-linear abelian monoidal category, there is no need for a semisimple or finite structure, however this level of generality will not needed here.

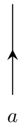
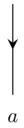
composition of morphisms corresponds to stacking:



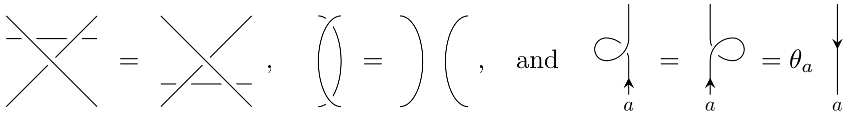
All strands are labeled by objects in the category with tensor product corresponding to juxtaposition:

$\mathrm{Id}_{X_a \otimes X_b} =$ 

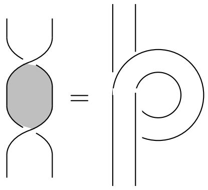
with the convention that:

$\mathrm{Id}_{X_a} =$  and $\mathrm{Id}_{X_a^*} =$ 

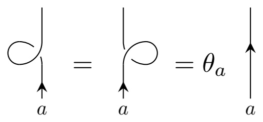
Finally, all diagrams are considered up to ambient isotopy subject to the following rules:



The terminology *ribbon* arises from the fact that the strings must track a framing. That is, if we physically imagine the strands as corresponding to worldlines, then the framing for the particle at any given point must be tracked. This is of importance in $(2+1)$-dimensions where particles can acquire an Aharonov-Bohm-like phase through self-interactions whereby the particle winds around itself, i.e. twists. This frame can be tracked by "fattening" the line to a ribbon. However, if one performs a full twist of a physical ribbon and flattens it out, then one can form the following diagram:



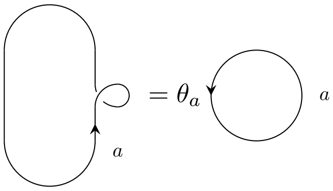
However, it is generally considered more convenient to work with lines rather than extended ribbons and simply implement the twist relation:



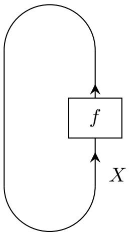
(II.3)

As previously mentioned, this graphical relation exactly corresponds to the sphericality condition. Furthermore, it highlights the origin of the term *spherical.* Indeed, if one has this relation II.3, then the diagrams can be viewed as residing on a sphere, in which case equation (II.3) exactly corresponds to sliding the string around the sphere.

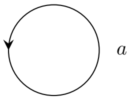
It can be noted that the twists in a premodular setting can be extracted by forming the diagram:



This is an equation in $\mathrm{End}_{\mathcal{C}}(\mathbb{I}) \cong \mathbb{K}$ and allows one to extract θ_a. In fact, this graphical construction of elements of $\mathrm{End}_{\mathcal{C}}(\mathbb{I})$ exactly corresponds to the categorical trace in a spherical category. Indeed, for any $f \in \mathrm{End}_{\mathcal{C}}(X)$, we can form the trace:



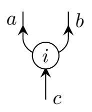
Often in these diagrams, the labeled loop appears:



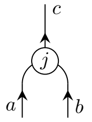
This exactly corresponds to $\mathrm{Tr}_{\mathcal{C}}(\mathrm{Id}_{X_a})$ and is called the **categorical dimension** of X_a, or simply **dimension**, throughout we will denote it by d_a.

Remark II.2.2. Occasionally, it is more convenient to denote the categorical dimensions by $d_a = \dim(X_a)$. This is typically done to avoid double subscripts or when discussing the dimension of a non-simple object.

In the premodular setting, we can make full use of the graphical calculus to determine a basis for the fusion space, $V^{c}_{a,b} := \mathrm{Hom}_{\mathcal{C}}\left(X_a \otimes X_b, X_c\right)$, and the splitting space, $V^{a,b}_{c} := \mathrm{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_b\right)$. Bases for these spaces will be graphically depicted by:



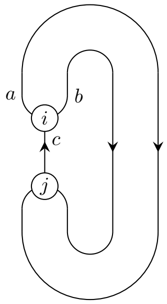
and



(II.4)

We shall always take the fusion basis to be projectively dual to the splitting basis under the categorical trace, that is we have the normalizing condition:

$$\theta\left(a,b,c\right)\delta_{ij} =$$



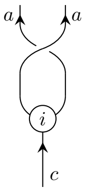
(II.5)

where here $\theta\left(a,b,c\right)$ is called the **theta-symbol** and is given by:

$$\theta\left(a,b,c\right) = \sqrt{d_a d_b d_c}$$

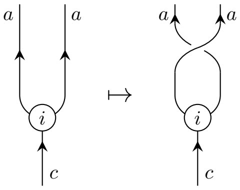
with d_a the categorical dimensions defined above.

Having specified the fusion basis in terms of a splitting basis, it remains to choose a basis for $V^{a,b}_{c}$. This is partially accomplished by selecting a basis that diagonalizes the braidings: $R_{X_a,X_a} \in \mathrm{End}_{\mathcal{C}}\left(X_a \otimes X_a\right)$. This may sound a bit odd, but $\mathrm{End}_{\mathcal{C}}\left(X_a \otimes X_a\right)$ is a vector space and so R_{X_a,X_a} is a vector, not a linear transformation. However, selecting a basis of the splitting space $V^{a,b}_{c}$ as in equation (II.4), we can then compose a basis element of $\mathrm{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_a\right)$ with R_{X_a,X_a} to arrive at:



$\in \mathrm{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_a\right)$

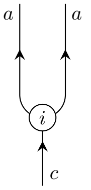
In this way, we may view $R_c^{a,a}$ as the map defined by:



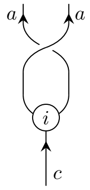
However, $\operatorname{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_a\right)$ is a vector space, and so we may view $R_c^{a,b}$ as an endomorphism on this space. In particular, it may be viewed as a linear transformation.

Next, recall that R_{X_a,X_a} is quasiunipotent, i.e. $R^N_{X_a,X_a}$ is unipotent for some N [Eti1, Theorem 4.1], and hence, $R_c^{a,a}$ may be diagonalized as a linear transformation $\operatorname{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_a\right) \to \operatorname{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_a\right)$. In particular, there are constants $R_{c,i}^{a,a}$ such that:

$$R_{c,i}^{a,a}$$



$$=$$

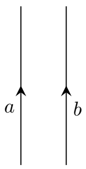


Remark II.2.3. In an analogous way, one can form the linear transformations:

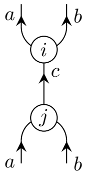
$$R_c^{a,b} : \operatorname{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_b\right) \to \operatorname{Hom}_{\mathcal{C}}\left(X_c, X_b \otimes X_a\right)$$

These $R_c^{a,b}$ are collectively referred to as the ***R*-matrices**. In this writing, we are only concerned with $R_c^{a,a}$ and so we need not concern ourselves with determining bases for $\operatorname{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_b\right)$ such that $R_c^{a,b}$ has a nice expression. When needed, we will simply refer to a basis of $\operatorname{Hom}_{\mathcal{C}}\left(X_c, X_a \otimes X_b\right)$ for $a \neq b$ as in equation (II.4) and equation (II.5). One natural choice is to select bases diagonalizing $R_c^{a,b} \circ R_c^{b,a}$.

In our bases for the splitting and fusion spaces, we may graphically express semisimplicity as:



$$= \sum_{c\in\operatorname{Irr}\mathcal{C}} \sum_{i\in V_c^{ab}} \sum_{j\in V_{ab}^c} \frac{d_c}{\theta\left(a,b,c\right)} \qquad \text{(II.6)}$$

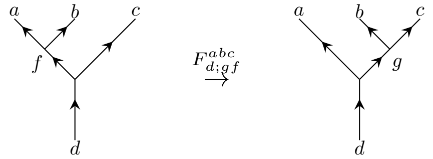


Having established the existence of a diagonalizing basis, it remains to elucidate the role of the associativities in this. While we will largely be concerned with categories up to Grothendieck equivalence, a complete treatment of the subject necessitates a brief discussion of the F-matrices.

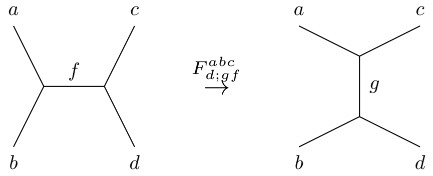
Recall that the associativities are natural transformations:

$$\alpha_{X,Y,Z} : (X \otimes Y) \otimes Z \to X \otimes (Y \otimes Z)$$

Graphically, these arise as a change of basis and can be expressed as F-matrices. That is, $X_a \otimes X_b \otimes X_c$ can be formed in two ways: $(X_a \otimes X_b) \otimes X_c$ and $X_a \otimes (X_b \otimes X_c)$. This gives rise to two bases for the space $\operatorname{Hom}_{\mathcal{C}}(X_d, (X_a \otimes X_b) \otimes X_c)$ and the associativities give the change of basis[9]



Remark II.2.4. If we, for the moment, abandon our up-down convention for the diagrams, then we can see the F-matrices correspond to the following transformation [W1]:



This “fusion” type equation, reminiscent of a Feynman diagram, is the origin of the “F” in the term F(usion)-matrix.

Remark II.2.5. The F-matrices are only defined up to a gauge. We will not need this level of detail here, but the interested reader should consult [W1].

Solving the hexagon and pentagon relations for the R- and F-matrices is a very difficult problem when classifying premodular categories [H1]. As previously mentioned, this is largely the reason that we will consider categories only up to Grothendieck equivalence. In Chapter VI, we will discuss the braiding a little more, but beyond that very little will be said regarding the R- and F-matrices.

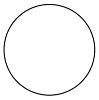
II.3 Premodular Datum

In the context of premodular categories, tracing (applying $\operatorname{Tr}_{\mathcal{C}}$ to) distinguished morphisms can lead to certain numeric invariants associated to the morphism. This is reminiscent of linear algebra, where the trace of a linear transformation leads to an invariant of the map. We have seen that tracing the identity morphisms on simple objects, Id_{X_a}, leads to the categorical dimensions. These numbers bear the name dimensions for a variety of reasons. On one hand, in representation categories, they recover the dimension of irreducible representations; while physically, they specify the asymptotic

[9] For notational simplicty, we assume that $N^c_{a,b} \leq 1$ here. When this is not true, one needs to appropriately decorate the vertices.

dimension of certain Hilbert spaces [P1]. These dimensions are commonly collected to form the dimension of the category $\mathcal{C}$, or **global dimension**:

$$D^2 = \sum_{a \in \mathrm{Irr}(\mathcal{C})} d_a^2 = \qquad \text{(II.7)}$$

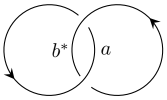


In the context of physics, this number is used in normalizing certain vectors and probabilities[P1], while mathematically, it is simply a useful invariant. It should be noted that while the global dimension appears as a square, this is for historical reasons, and the number is not the square of anything meaningful. Often the square-root of the global dimension, D^2, is referred to as the **quantum order**, but we will not make use of this terminology here.

Remark II.3.1. Just as the categorical dimensions are occasionally denoted by $\dim(X_a)$, it is occasionally convenient to denote the global dimension by $\dim \mathcal{C} = D^2$. This notation will occasionally be adopted when it it not clear from context which category the global dimension is referring to.

In addition to considering the trace of the identity morphisms, which leads to the dimensions, and the twist morphism which leads to the twists, one might consider tracing the square of the braiding, $M_{a,b} = R_{b,a}R_{a,b}$. This is a common enough practice that the trace of the braiding on simple objects has a special notation:

$$S_{a,b} = \mathrm{Tr}_{\mathcal{C}}\left(M_{a,b^*}\right) = \qquad \text{(II.8)}$$



Given our convention that $\mathrm{Id}_{\mathbb{I}}$ should have no associated strand in the graphical calculus, it follows immediately that $S_{0,a} = S_{a,0} = d_a$ and $d_0 = 1$. In fact, formal manipulations of the graphical calculus lead to the following additional relations:

$$S^*_{a^*,b} = S_{a,b} = S_{b,a} = S_{a^*,b^*}, \quad \text{and} \quad S_{a,0} = d_a. \qquad \text{(II.9)}$$

If we collect these numbers into a matrix indexed by $\mathrm{Irr}(\mathcal{C})$, we arrive at a symmetric matrix known as the S**-matrix**. It is common to similarly collect the twists and fusion rules into matrices:

$$T_{a,b} = \theta_a \delta_{a,b}, \quad (N_a)_{b,c} = N^c_{a,b} := \dim_{\mathbb{K}} \mathrm{Hom}_{\mathcal{C}}\left(X_a \otimes X_b, X_c\right)$$

respectively known as the T**-matrix** and **fusion matrices**. A result known as **Vafa's Theorem** greatly restricts the structure of T.

Theorem II.3.2 (Vafa)**.** *The twists θ_a are roots of unity (of finite order).*

To classify the Grothendieck rings of fixed rank, it suffices to understand the fusion matrices of fixed rank. However, it is common practice to go one step further and determine admissible tuples (N_a, S, T) called *(pre)modular datum.*

Definition II.3.3. If r is an integer, $N_a \in Mat_{r\times r}(\mathbb{N})$ for $0 \leq a \leq r-1$, $S \in Mat_{r\times r}(\mathbb{C})$, and T an $r \times r$ diagonal invertible matrix whose non-zero entries are roots of unity, then (N_a, S, T) is **(pre)modular datum** if the N_a, S, and T satisfy all algebraic relations of a (pre)modular category with fusion matrices N_a, S-matrix S, and T-matrix T.

Remark II.3.4. This should not be confused with the concept of modular datum as defined by Gannon, e.g. [CGR1].

The reason for defining premodular datum in this fashion is to refer to the S-, T-, and fusion matrices of a modular category without needing to be concerned with the F- or R-matrices. This neatly allows us to side-step the existence problems of certain categories, that is given (N_a, S, T) or (N_a, S, T, R, F) satisfying all relations following from the definition of a modular category, does such a category exist?

Remark II.3.5. (N_a, S, T, R, F) is sufficient to define the skeleton of a (pre)modular category. The issue of it actually determining a (pre)modular category is related to the notion of "evil" in category theory, that is to say one needs to be concerned with breaking equivalence invariance [TCo1].

We will not concern ourselves with such metaphysical issues in this writing and will instead focus on understanding (pre)modular datum and categories up to Grothendieck equivalence.

Premodular datum is highly constrained; for instance, it can be shown that the (S, T) satisfy the relations:

$$(ST)^3 = p^+ S^2, \quad \left(ST^{-1}\right)^3 = p^- S^2 C \tag{II.10}$$

where $p^\pm$ are the **Gauss sums**:

$$p^\pm = \sum_{a\in \mathrm{Irr}(\mathcal{C})} \theta_a^\pm d_a^2 \tag{II.11}$$

and C is the **charge conjugation matrix** $C_{a,b} = \delta_{a,b^*}$.

When S is invertible, the premodular category is of a particularly nice type known as **modular**. In the modular setting, several additional relations are acquired. For instance, (S, T) furnish a projective representation of $\mathrm{SL}(2, \mathbb{Z})$, and is the source of the nomenclature *modular*. Furthermore, it can be shown that, in the modular setting, one has:

$$SS^\dagger = D^2 \mathbb{I}, \quad \text{and} \quad p^+ p^- = D^2 \tag{II.12}$$

This projective representation can be lifted to a linear one. This allows one to bring the representation theory of the modular group to bear on the study of modular categories. Such analysis will be reviewed in Section III.2 and it will have important number theoretical consequences.

Exploring further, we see that the braiding and the pivotal structure endow the fusion matrices with the following symmetries [BKi]:

$$\begin{gathered} N_{a,b}^{c} = N_{ba}^{c} = N_{a,c^*}^{b^*} = N_{a^*,b^*}^{c^*} \\ N_{a,b^*}^{0} = 1, \quad N_{a^*} = N_a^T, \quad N_a N_b = N_b N_a. \end{gathered} \tag{II.13}$$

The S-matrix and fusion matrices are strongly related. Indeed, the S-matrix is known to simultaneously diagonalize the fusion matrices. In the premodular setting, this manifests itself through the following relation [BKi]:

$$S_{a,j} S_{b,j} = S_{0,j} \sum_{c} N_{a,b}^{c} S_{c,j} \tag{II.14}$$

While in the modular setting, the invertibility of the S-matrix allows one to solve this relation for the fusion matrices producing the famed **Verlinde formula**:

$$N_{a,b}^{c} = \frac{1}{D^2} \sum_{j} \frac{S_{a,j} S_{b,j} S_{c^*,j}}{S_{0,j}} \tag{II.15}$$

Furthermore, it follows that the columns of the S-matrix are eigenvectors of the fusion matrices and the normalized columns produce eigenvalues. Indeed, $\frac{S_{a,b}}{d_b}$ is an eigenvalue of N_a [RSW]. To put it another way, the normalized columns of the S-matrix are characters of the Grothendieck ring. Some implications of this fact will be explored in Section II.5.

Further exploring the implications of the premodular axioms through the graphical calculus, one finds that the S-matrix can be recovered from the fusion matrices, the dimensions, and the twists through the **balancing relation**[BKi]:

$$S_{a,b} = \theta_a^{-1} \theta_b^{-1} \sum_{c \in \operatorname{Irr}(\mathcal{C})} N_{a^*,b}^{c} \theta_c d_c \tag{II.16}$$

While each piece of premodular datum is useful in its own right, the invertibility of the S-matrix is a powerful condition which suggests a clean stratification of premodular categories.

Definition II.3.6. A premodular category, $\mathcal{C}$, is **symmetric** if $S_{a,b} = d_a d_b$ for all $a, b \in \operatorname{Irr}(\mathcal{C})$; it is **modular** if S is invertible, and it is **properly premodular** otherwise.

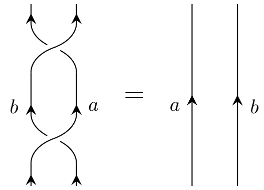
As we will see below, symmetric categories are, in some sense, completely degenerate and are described by finite groups, while modular categories are completely nondegenerate. The properly premodular categories fill in the gap between these two extremes. A construction due to Müger provides a means to discuss this stratification through the braiding. This gives rise to a useful premodular subcategory known as the *Müger center*.

II.4 Center Constructions

Given that properly premodular categories interpolate between the completely degenerate symmetric categories and the non-degenerate modular categories, one might like to have a measure of how close a properly premodular category is to one extreme or another. Since the S-matrix determines the type of properly premodular category one is dealing with and the S-matrix serves to measure the degeneracy of the braiding, one can attempt to capture the degeneracy of a premodular category more exactly through the braiding. Indeed, such analysis leads to [Brug1]:

Proposition II.4.1. *If there is an object in the category, say X_a, such that $M_{a,b} = \mathrm{Id}_{X_a \otimes X_b}$ for all $X_b \in \mathrm{Irr}(\mathcal{C})$, then the the a-th column of the S-matrix will be given by $S_{a,b} = d_a d_b$, that is it is a multiple of the first, and hence the matrix is degenerate.*

Objects X_a, as in this proposition, are called **transparent** or **central**, with the nomenclature arising from the graphical calculus where such an object satisfies:



A study of such objects was undertaken in [Brug1; M4] where it was found that such behavior is the only way for a premodular category to fail to be modular. This led Müger to define a premodular subcategory to isolate the transparent objects in a premodular category.

Definition II.4.2. If $\mathcal{C}$ is a premodular category, then its **Müger center**, $\mathcal{C}'$, is the full premodular subcategory of $\mathcal{C}$ generated by the transparent objects of $\mathcal{C}$.

The Müger center allows one to stratify premodular categories without reference to the S-matrix. In fact, it follows immediately from the definition that:

Proposition II.4.3. *If $\mathcal{C}$ is a premodular category then:*

(i) $\mathcal{C}$ is symmetric if and only if $\mathcal{C} = \mathcal{C}'$.

(ii) $\mathcal{C}$ is modular if and only if $\mathcal{C}' =$ Vec.

(iii) $\mathcal{C}$ is properly premodular otherwise.

Symmetric categories were studied by Deligne, Doplicher, and Roberts [D1; DR1]. Due to these works, symmetric categories were the first class of premodular categories to be completely classified. The result essentially says that all symmetric categories arise from finite groups. To make the statement precise, we need the following definition [ENO2].

Definition II.4.4. A symmetric fusion category $\mathcal{C}$ is **Tannakian** if it is equivalent to $\mathrm{Rep}\,(G)$ as a symmetric fusion category for some finite group G. Similarly, a symmetric fusion category $\mathcal{C}$ is **super-Tannakian** if there is a finite group G and a central element $u \in G$ of order 2 such that $\mathcal{C}$ is equivalent to the category of representations of G on super-vector spaces with u acting by parity.

This definition allows for a succinct statement of Deligne's classification [D1].

Theorem II.4.5. *If $\mathcal{C}$ is a symmetric fusion category, then it is super-Tannakian. In particular, any symmetric category is Grothendieck equivalent to* $\operatorname{Rep}(G)$ *for some finite group G.*

This result gave hope that premodular categories could be understood in some general way, perhaps in terms of groups. However, the methods used to understand symmetric categories are inadequate in the general premodular setting and relatively little progress has been made. Moreover, until [BNRW1] it was unknown whether or not there were even finitely many modular categories of fixed rank, let alone premodular categories. Nonetheless, there is a great deal of theory governing modular categories and comparatively little known about premodular categories. Furthermore, there is a well-known center construction allowing one to generate a modular category from a premodular one [M2]. This construction allows one to associate to any spherical fusion category[10] $\mathcal{C}$, a modular category $\mathcal{Z}(\mathcal{C})$, called the **Drinfeld center** or **double**.[11] The explicit construction is quite involved and will take us too far afield. However, the interested reader can find details in [M2; JS1].

It can be shown that a premodular category $\mathcal{C}$ always embeds into its Drinfeld center. This shows that a complete understanding of the Drinfeld center would allow one to understand the premodular category in terms of a modular category. Furthermore, there are several tantalizing results about the center such as $\dim \mathcal{Z}(\mathcal{C}) = \dim \mathcal{C}^2$. Such results suggest that it may be possible to understand the Drinfeld center. As previously mentioned, the large volume of literature on modular categories makes this an attractive prospect. However, except in limited cases [O2], this has not been possible. Often, the fusion rules and rank of the double wildly differ from those of the original category and, in fact, there is no known bound on the rank of the double strictly in terms of the rank of the initial category. For these reasons, the Drinfeld center has been of limited practical use in classification, but it still remains a powerful theoretical tool and its existence is worth mentioning.

While these center constructions provide theoretical tools for studying premodular categories, they are of limited practical use. However, in the course of studying premodular categories, many arithmetic properties have surfaced which provide more practically applicable tools. The connections between number theory and these categories begin to manifest themselves through the dimensions defined in the previous sections.

[10] Braided is not required.

[11] This terminology arises from the connection between this categorical center constructon and the Drinfeld center construction for Hopf algebras as discussed in Section II.7. This categorical construction can be traced back to Joyal and Street [JS1], where they defined the double fo a monoidal category.

II.5 Dimensions

We have already seen that there is a connection between the dimensions and the S-matrix, as well as several algebraic relations amongst the premodular datum. It is natural to ask if the above discussion exhausts the relations present amongst these matrices and in fact it does not. For instance, it can be shown [HR1] that the columns of the S-matrix are projectively characters of the Grothendieck ring. That is to say, one can define a character ψ_a of the Grothendieck ring by $\psi_a\left(X_b\right) = S_{a,b}/d_a$. In the modular setting, the S-matrix is projectively unitary; this implies that the characters are orthogonal [HR1]:

$$\sum_a \psi_b\left(X_a\right)\overline{\psi_c\left(X_a\right)} = \delta_{bc}D^2/d_b^2 \tag{II.17}$$

This shows that when S is invertible, it diagonalizes the fusion matrices. Moreover, it immediately follows that d_a is necessarily an eigenvalue of N_a.

Since N_a is a nonnegative integer matrix for any a, it is subject to the Frobenius-Perron theorem and, consequently, has a largest positive real eigenvalue. Such an eigenvalue has significance when studying braided fusion categories and is known as the **Frobenius-Perron dimension** of X_a, or **FP-dimension** for short, and is denoted by $\operatorname{FPdim}\left(X_a\right)$. This leads to two "dimensions" associated with a simple object in a premodular category. Furthermore, both of these dimensions recover the dimensions of representations in a representation category, and are both eigenvalues of N_a. In light of this, one might wonder whether or not these two numbers are in fact equal. Sadly, in general, they are not. However, the categorical dimension of a category depends on the spherical structure and often it is possible to select a spherical structure such that $d_a = \operatorname{FPdim}\left(X_a\right)$. A necessary condition for this to be possible is that $D^2 = \operatorname{FPdim}\left(\mathcal{C}\right)$. When this condition is satisfied, one says that the category is **pseudo-unitary**. It can further be shown that all other spherical structures in the pseudo-unitary setting can only cause the categorical dimension to differ from the FP-dimensions by at worst a sign [BNRW1]:

Lemma II.5.1. *If $\mathcal{C}$ is pseudo-unitary, then $d_a = \pm\operatorname{FPdim}\left(X_a\right)$.*

Proof. Note that if $d_a \neq \pm\operatorname{FPdim}\left(X_a\right)$, then $d_a^2 < \operatorname{FPdim}\left(X_a\right)$ for some a. On the other hand, for all b we have $d_a^2 \leq \operatorname{FPdim}\left(X_a\right)^2$ by definition of the FP-dimension. Consequently, $D^2 = \sum\limits_b d_b^2 < \sum\limits_b \operatorname{FPdim}\left(X_b\right) = \operatorname{FPdim}\left(\mathcal{C}\right)$. This contradicts pseudo-unitarity ($D^2 = \operatorname{FPdim}\left(\mathcal{C}\right)$). □

Furthermore, it is known that, in the modular setting even if the category is not pseudo-unitary, one can still locate the FP-dimensions in the S-matrix.

Proposition II.5.2. *If $\mathcal{C}$ is a rank r modular category with modular datum (N, S, T), then $\exists b \in \operatorname{Irr}\left(\mathcal{C}\right)$ such that $S_{a,b} = d_b\operatorname{FPdim}\left(X_a\right)$.*

Proof. We know that the columns of the S-matrix are characters of the Grothendieck ring of $\mathcal{C}$ [HR1]. Since these characters are orthogonal, we know by the invertibility of the S-matrix that the r columns must be linearly independent. Since there are r characters and FPdim is a character, we know that some column of S must be proportional to FPdim. Since $\operatorname{FPdim}(\mathbb{I}) = 1$, we can conclude that the proportionality constant must be the categorical dimension appearing in the first row, i.e. $S_{0,a} = d_a$. □

The existence of two dimensions appearing as eigenvalues of the fusion matrices prompted Parsa Bonderson to ask [PCo1]:

Question II.5.3. *Can all of the eigenvalues appear as dimensions?*

Eric Rowell [RCo1] showed that the answer to this question is negative. In particular, he shows that the FP-dimensions can fail to appear as categorical dimensions for the quantum group $\mathrm{SO}\left(2k+1\right)_{t/2}$ with t odd *viz.* type B with $q = e^{\pi i/\ell}$ and ℓ odd. However, this prompted him to conjecture [RCo1]:

Conjecture II.5.4. *The only eigenvalues that can appear as dimensions are in the orbit of the label* 0*, up to sign.*

Here, the notion of *orbit of the label 0* is related to the Galois theory, which will be discussed in Section III.1. We will not address this conjecture any further in this work, but we find it to be an interesting question.

In a pseudo-unitary premodular category, the dimensions coincide and are positive real algebraic integers, and, in the setting of representation categories, these algebraic integers are rational. In the general setting, stranger things can happen. While the categorical and Frobenius-Perron dimension are always algebraic integers, they need not be rational and the categorical dimensions need not be positive. Nonetheless, there are stringent divisibility conditions that must be satisfied [EG1, Lemma 1.2; ENO1, Proposition 8.15; ENO1, Proposition 8.22].

Proposition II.5.5. *If $\mathcal{C}$ is a premodular category and $\mathcal{D}$ is a fusion subcategory, then:*

(i) $d_a \mid D^2$

(ii) $\operatorname{FPdim}(\mathcal{D}) \mid \operatorname{FPdim}(\mathcal{C})$ *in* $\overline{\mathbb{Z}}$.[12]

(iii) $D^2 \mid \operatorname{FPdim}(\mathcal{C})$ *in* $\overline{\mathbb{Z}}$.

Moreover, if $\mathcal{C}$ is modular, then $d_a^2 \mid D^2$ for all $X_a \in \operatorname{Irr}(\mathcal{C})$.

Remark II.5.6. Part (ii) of this result only requires that $\mathcal{C}$ is a fusion category and $\mathcal{D}$ is a full tensor subcategory. However, as is noted in [ENO1, Remark 8.18], it is not known if (ii) holds when FP-dimensions are replaced by global dimensions. Furthermore, if categorical dimensions are replaced by FP-dimensions, then the analogous statement to (i) is known as **Kaplansky's sixth conjecture for fusion categories**, and the veracity of the statement is unknown.

[12] The ring of algebraic integers.

While a powerful tool, these divisibility conditions are particularly pronounced in small subrings of $\overline{\mathbb{Z}}$. Thus, it is particularly natural to stratify fusion categories based on their dimensions.

Definition II.5.7. A braided fusion category is

(i) **pointed** if $\mathrm{FPdim}\left(X_a\right) = 1$ for all $X_a \in \mathrm{Irr}\left(\mathcal{C}\right)$

(ii) **integral** if $\mathrm{FPdim}\left(X_a\right) \in \mathbb{Z}$ for all $X_a \in \mathrm{Irr}\left(\mathcal{C}\right)$

(iii) **weakly integral** if $\mathrm{FPdim}\left(\mathcal{C}\right) := \sum\limits_{a \in \mathrm{Irr}(\mathcal{C})} \mathrm{FPdim}\left(X_a\right)^2$ is a rational integer.

It has been shown [ENO1] that:

Proposition II.5.8. *If $\mathcal{C}$ is a braided fusion category, then*

pointed $\implies$ integral $\implies$ weakly integral $\implies$ pseudo-unitary.

Remark II.5.9. All implications in Proposition II.5.8 are strict in that there are examples where each of the converse implication is violated.

- Fib is pseudo-unitary, but not weakly integral [RSW].
- Ising is weakly integral, but not integral [RSW].
- $\mathrm{Rep}\left(D\left(\mathfrak{S}_3\right)\right)$ is integral, but not pointed.[13]

Furthermore, an object X in $\mathcal{C}$ is said to be **invertible** if $\mathrm{FPdim}\left(X\right) = 1$.

This stratification is quite important for the study of premodular categories as weaker dimension axioms lead to more complicated categories. For instance, a class of pointed categories that are quite easy to understand arise from vector spaces.

Example II.5.10. *If G is a finite group and $\omega \in Z^3\left(G, \mathbb{K}^\times\right)$ is a 3-cocylce, then the fusion category $\mathit{Vec}_{G,\omega}$ has:*

- *Objects: G-graded $\mathbb{K}$-vector spaces.*
- *Simple objects: V_g, 1-dimensional $\mathbb{K}$-vector spaces concentrated in the g-component (evaluation modules).*
- *Tensor product: $V_g \otimes V_h = V_{gh}$*
- *Duals: $V_g^* = V_{g^{-1}}$.*
- *Associativity $\alpha_{V_g,V_h,V_k} = \omega\left(g,h,k\right)\mathrm{Id}$.*

This category is braided if and only if G is abelian.

In fact, it has been shown that these are all of the pointed categories [ENO1].

[13] Here, $D\left(\mathfrak{S}_3\right)$ is the double of the group $\mathfrak{S}_3$, see Section II.7.

Proposition II.5.11. *If $\mathcal{C}$ is a pointed fusion category over a field $\mathbb{K}$, then it is of the form $Vec_{G,\omega}$ for some finite group G and some 3-cocycle $\omega \in Z^3\left(G, \mathbb{K}^\times\right)$.*

Beyond pointed categories, integral are the next most well understood type. In fact, they can all be understood in terms of quasi-Hopf algebras [ENO1]

Proposition II.5.12 (Theorem 8.33 *loc. cit.*)**.** *Let $\mathcal{C}$ be a fusion category. Then $\mathcal{C}$ is integral if and only if $\mathcal{C}$ is the representation category of a finite dimensional quasi-Hopf algebra.*

Despite this result, integral fusion categories are still poorly understood and the classification of integral modular categories is still an active area of research, cf. Section V.1 and Section V.2.

While premodular categories can be studied based upon these dimension conditions, such conditions can also be used to generate subcategories. Indeed, if $\mathcal{C}$ is a fusion category, then there are two natural subcategories that can be constructed. The **integral subcategory**, $\mathcal{C}_{\text{int}}$, is the full fusion subcategory of $\mathcal{C}$ generated by the simple integral objects. This category in turn contains the **pointed subcategory**, $\mathcal{C}_{\text{pt}}$, the full fusion subcategory generated by the invertible objects. In the modular setting, the invertible objects are incredibly important. Indeed, the simple invertible objects can be used to enumerate the number of pivotal structures, while the self-dual invertible objects count the number of spherical structures [BNRW1]. Additionally, the invertible objects determine a grading of the category, as we will see in the next section.

II.6 Gradings and G-Extensions

It is common in commutative algebra to study graded objects. This allows one to understand more complicated objects in terms of simpler ones. The prototypical example is the ring of polynomials $\mathbb{K}[x]$. This ring is graded by degree, and so much of the information about the ring is gleaned by understanding the behavior of degree 1 polynomials (the 0 and 1 graded pieces). Since braided fusion categories can be viewed as axiomatizations of certain rings (fusion rings), it is reasonable to assume that, under certain circumstances, the categories themselves should be graded in some meaningful way. This led to a study in [GN2], where such a structure on fusion categories was uncovered. In the modular setting, the results are particularly powerful and the finest possible grading can be understood in terms of the pointed subcategory.

Definition II.6.1. If $\mathcal{C}$ is a fusion category, then a **grading** is a finite group G and a map $\deg : \text{Obj}\left(\mathcal{C}\right) \to G$ such that: if X, Y, and Z are objects of $\mathcal{C}$ such that Z is a subobject of $X \otimes Y$, then $\deg Z = \deg X \cdot \deg Y$. If G is the trivial group, then the grading is said to be **trivial** and if this map is surjective, then the grading is **faithful** and that $\mathcal{C}$ is called a G**-extension** of $\mathcal{C}_e$, the trivial component.

Such a grading allows the category to be decomposed as $\mathcal{C} = \bigoplus_{g\in G} \mathcal{C}_g$. The $\mathcal{C}_g$ are full additive subcategories called **components** and are generated by objects of degree g in $\mathcal{C}$. This grading greatly restricts the fusion rules admissible in the category. Indeed, if X and Y are objects of degree g and h respectively, then $X \otimes Y$ is an object in $\mathcal{C}_{gh}$, i.e. $\mathcal{C}_g \otimes \mathcal{C}_h$ is contained in $\mathcal{C}_{gh}$. In the event that the grading is faithful and $\mathcal{C}$ is premodular, the components must be equi-dimensional, that is to say [DGNO1]:

Proposition II.6.2. *If $\mathcal{C}$ is a premodular category which is faithfully graded by a finite group G, then $\dim \mathcal{C}_g = \dim \mathcal{C} / |G|$ for all $g \in G$.*

It can be shown that the set of gradings depends functorially upon the group G [DGNO1]. In particular, there should be a notion of universality. This was explored in [GN2] where they showed that a universal grading always exists and is faithful. The universal grading group is typically denoted by $U_{\mathcal{C}}$ and the trivial component under the universal grading is the *adjoint subcategory*, $\mathcal{C}_{\text{ad}}$. The adjoint subcategory can be defined independent from the universal grading as follows.

Definition II.6.3. If $\mathcal{C}$ is a fusion category, then the **adjoint subcategory**, $\mathcal{C}_{\text{ad}}$, is the full fusion subcategory generated by subobjects of $X \otimes X^*$ as X ranges over the objects of $\mathcal{C}$.

Remark II.6.4. The adjoint subcategory derives its name from the theory of Hopf algebras. Indeed, if H is a semisimple Hopf algebra, then $\operatorname{Rep}(H)$ is a fusion category and $\operatorname{Rep}(H)_{\text{ad}}$ is generated by subrepresentations of the adjoint representation of H [GN2, Remark 3.1].

The universal grading group, adjoint subcategory, pointed subcategory, and Müger center are tightly knit in the modular setting. Indeed, we have [DGNO1]

Proposition II.6.5. *If $\mathcal{C}$ is a modular category, then the universal grading group is isomorphic to the group of isomorphism classes of simple invertible objects in $\mathcal{C}$.*

Remark II.6.6. By abuse of notation, one often says that *the universal grading group is given by $\mathcal{C}_{pt}$.*

The relationship between the pointed subcategory, the adjoint subcategory, and the Müger center can be made explicit [DGNO1]:

Proposition II.6.7. *If $\mathcal{C}$ is a modular category, then:*

(i) $(\mathcal{C}_{\text{pt}})' = \mathcal{C}_{\text{ad}}$

(ii) $(\mathcal{C}_{\text{ad}})' = \mathcal{C}_{\text{pt}}$

(iii) $(\mathcal{C}_{\text{pt}})_{\text{ad}} = \mathit{Vec}$

(iv) $\mathcal{C}' = \mathit{Vec}$

While for a modular category, $\mathcal{C}$, $\mathcal{C}_{\text{pt}}$ and $\mathcal{C}_{\text{ad}}$ are related through the universal grading and the Müger center, and $(\mathcal{C}_{\text{pt}})_{\text{ad}} = \mathcal{C}' = \text{Vec}$, it does not follow that $\mathcal{C}_{\text{ad}} = \text{Vec}$. However, in the event that one can obtain Vec by repeatedly taking adjoint subcategories one says that $\mathcal{C}$ is *nilpotent*. Formally,

Definition II.6.8. Let $\mathcal{C}$ be a modular category and recursively define $\mathcal{C}^{(n)}$ by $\mathcal{C}^{(1)} = \mathcal{C}_{\text{ad}}$ and $\mathcal{C}^{(n)} = \left(\mathcal{C}^{(n-1)}\right)_{\text{ad}}$. If $\exists m$ such that $\mathcal{C}^{(m)} = \text{Vec}$, then $\mathcal{C}$ is **nilpotent**.

Nilpotent and pointed categories comprise some of the simplest known fusion categories. In the following section, we will consider an extended example of so-called group-theoretical categories. Often, nilpotency can be used to reduce the study of certain integral modular categories to the study of group-theoretical categories, e.g. [DGNO2, Corollary 6.7].

II.7 Extended Example: Group Theoretical Categories

Before beginning our discussion of arithmetic properties of modular categories, an extended example is in order. Here, we will treat braided-fusion categories which can be constructed from finite groups known as **group-theoretical** categories. These categories provide an important class of integral categories. However, it has been shown that not all integral fusion categories are group-theoretical [JL1; N3]

In order to properly treat group-theoretical categories we must first consider a simpler construction–the twisted quantum double $D^{\omega}(G)$ of a finite group G. Our construction of this category parallels [BKi; NN1; ERW1].

The twisted quantum double is a quasitriangular, quasi-Hopf algebra constructed from a finite group through its group algebra and its function algebra. The representations of this quasi-Hopf algebra form a modular category (commonly also called the twisted quantum double).

Throughout this section, G will be a finite group and $\omega \in Z^3(G, \mathbb{K}^{\times})$ a 3-cocycle. For simplicity, we will further assume that $\mathbb{K}$ is an algebraically closed field of characteristic 0. We will begin by considering the Drinfeld double, the twisted Drinfeld double will then be obtained by twisting the (co)multiplication by the 3-cocycle ω.

We first note that the group algebra $\mathbb{K}[G]$ can be given the structure of a Hopf algebra. In order to see this, we recall that a $\mathbb{K}$-basis of $\mathbb{K}[G]$ is given by the elements of the group G. Thus to describe a Hopf structure it suffices to define the (co)multiplication, (co)unit, and antipode on this basis. This can be done as follows:

$$\begin{aligned} \text{multiplication} \quad & g \otimes h \mapsto gh \\ \text{unit} \quad & e \quad \text{(the unit in } G\text{)} \\ \text{comultiplication} \quad & \Delta(g) = g \otimes g \\ \text{counit} \quad & \epsilon(g) = 1 \\ \text{antipode} \quad & S(g) = g^{-1} \end{aligned}$$

Note that this Hopf algebra is cocommutative, but it is only commutative when G is as well.

Given a Hopf algebra, one can always form the dual Hopf algebra. In this setting, the dual Hopf algebra to $\mathbb{K}[G]$ is the function algebra $\mathrm{Fun}(G)$. This Hopf algebra has a $\mathbb{K}$-basis given by indicator functions on G:

$$\delta_g(h) = \begin{cases} 1 & g = h \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, the Hopf structure of $\mathrm{Fun}(G)$ is explicitly given by:

$$\begin{aligned} \text{multiplication} \quad & \delta_g \delta_h = \delta_{g,h}\delta_g \\ \text{unit} \quad & 1 = \sum_{g\in G} \delta_g \\ \text{comultiplication} \quad & \Delta(\delta_g) = \sum_{hk=g} \delta_h \otimes \delta_k \\ \text{counit} \quad & \epsilon(\delta_g) = \delta_{g,e} \\ \text{antipode} \quad & \gamma(\delta_g) = \delta_{g^{-1}} \end{aligned}$$

Remark II.7.1. The representations of $\mathbb{K}[G]$ are given by representations of G, while the representations of $\mathrm{Fun}(G)$ are given by G-graded vector spaces [BKi].

The **quantum double** of G is a Hopf algebra, $D(G)$, obtained from $\mathbb{K}[G]$ and $\mathrm{Fun}(G)$. As a vector space, $D(G)$ is given by $\mathrm{Fun}(G) \otimes_{\mathbb{K}} \mathbb{K}[G]$, while its Hopf algebra structure is given by [BKi]:

$$\begin{aligned} \text{multiplication} \quad & (\delta_{g_1} \otimes h_1)(\delta_{g_2} \otimes h_2) = \delta_{g_1 h_1, h_1 g_2}(\delta_{g_1} \otimes h_1 h_2) \\ \text{unit} \quad & 1 = \sum_{g\in G} \delta_g \otimes e \\ \text{comultiplication} \quad & \Delta(\delta_g \otimes h) = \sum_{g_1 g_2 = g} (\delta_{g_1} \otimes h) \otimes (\delta_{g_2} \otimes h) \\ \text{counit} \quad & \epsilon(\delta_g \otimes h) = \delta_{g,e} \\ \text{antipode} \quad & \gamma(\delta_g \otimes h) = \delta_{h^{-1}g^{-1}h} \otimes h^{-1} \end{aligned}$$

Remark II.7.2. The astute reader may notice that $D(G)$ is simply a semidirect product of the group algebra $\mathbb{K}[G]$ with the function algebra $\mathrm{Fun}(G)$, that is $D^{\omega}(G) = \mathrm{Fun}(G) \rtimes \mathbb{K}[G]$ where $h\delta_g h^{-1} = \delta_{hgh^{-1}}$.

Remark II.7.3. The Hopf algebra $D(G)$ is quasi-triangular with R-matrix given by:

$$R = \sum_{g\in G} (\delta_g \otimes e) \otimes (1 \otimes g)$$

One can use the 3-cocycle ω to *twist* the multiplication and comultiplication. This is done by defining:

$$\begin{aligned}\theta_k(g,h) &:= \frac{\omega(k,g,h)\,\omega\left(h,h^{-1}g^{-1}kgh\right)}{\omega\left(g,h,g^{-1}kg,h\right)}\\ \gamma_g(k,h) &:= \frac{\omega(k,h,g)\,\omega\left(g,g^{-1}kg,g^{-1}hg\right)}{\omega\left(k,g,g^{-1}hg\right)}\end{aligned}$$

the twisted (co)multiplication are then given by [ERW1]:

$$\text{multiplication}\quad \left(\delta_{g_1}\otimes h_1\right)\left(\delta_{g_2}\otimes h_2\right) = \theta_{g_1}\left(h_1,h_2\right)\delta_{g_1,h_1g_2h_1^{-1}}\delta_{g_1}\otimes\left(h_1h_2\right) \tag{II.18}$$

$$\text{comultiplication}\quad \Delta\left(\delta_g\otimes h\right) = \sum_{\substack{k,\ell\in G\\ k\ell=g}}\gamma_h(k,\ell)\left(\delta_k\otimes h\right)\otimes\left(\delta_g\otimes h\right) \tag{II.19}$$

The **twisted quantum double** of G is the quasi-Hopf algebra $D^{\omega}(G)$ whose underlying vector space, unit, counit, and anitpode are the same as $D(G)$, but has the twisted (co)multiplication defined in equation (II.18).

Just as in the untwisted case, $D^{\omega}(G)$ is quasi-triangular, but its R-matrix is modified by the 3-cocycle [ERW1]:

$$\begin{aligned}R &= \sum_{g\in G}\delta_g\otimes g\\ R^{-1} &= \sum_{g,h\in G}\theta_{ghg^{-1}}\left(g,g^{-1}\right)^{-1}\left(\delta_g\otimes e\right)\otimes\left(\delta_h\otimes g^{-1}\right)\end{aligned}$$

The representation category of a twisted Drinfeld double has been shown to form a modular category [BKi; Tu1]. Furthermore, the rank of the category, S-matrix, and T-matrix can be explicitly determined in terms of conjugacy classes of G and irreducible representations of the centralizers of such conjugacy classes. To do this we follow [NN1]. They first observe that if $g\in G$, then $\theta_g\mid_{C_G(g)}$ is a normalized 2-cocycle. The irreducible objects of $\operatorname{Rep}\left(D^{\omega}(G)\right)$ are in bijection with:

$$\Gamma = \left\{\left([g],\chi\right)\mid \overline{g}\text{ distinct conjugacy classes of }G\text{ and }\chi\text{ an irreducible }\theta_g\text{-character of }C_G(g)\right\}$$

Here, $[g]$ denotes the conjugacy class of g in G.

Remark II.7.4. Recall that if β is a 2-cocycle of a group G, then a **β-representation** is a map $\tilde{\rho}: G\to \mathrm{GL}(V)$ for some vector space V, which satisfies $\tilde{\rho}(g)\tilde{\rho}(h) = \beta(g,h)\tilde{\rho}(gh)$. An **(irreducible) β-character** is defined to be the trace of an (irreducible) β-representation [CGR1].

Remark II.7.5. If $\omega = 1$, then the simple objects of $\operatorname{Rep}\left(D^{\omega}(G)\right)$ are in bijection with

$$\Gamma = \left\{\left([g],\chi\right)\mid [g]\text{ distinct conjugacy classes of }G\text{ and }\chi\text{ an irreducible character of }C_G(g)\right\}$$

The S-matrix, T-matrix, and dimensions of $D^{\omega}(G)$ are then given by [NN1]:

$$S\left(\left(g,\chi\right),\left(h,\chi'\right)\right)=\sum_{k\in[g],\ell\in[h]\cap C_G(k)}\overline{\left(\frac{\theta_g\left(x,\ell\right)\theta_g\left(x\ell,x^{-1}\right)\theta_h\left(y,k\right)\theta_h\left(yk,y^{-1}\right)}{\theta_g\left(x,x^{-1}\right)\theta_h\left(y,y^{-1}\right)}\right)}\overline{\chi}\left(x\ell x^{-1}\right)$$
$$\times\overline{\chi'}\left(yky^{-1}\right)$$

$$\theta\left(g,\chi\right)=\frac{\chi\left(g\right)}{\deg\chi}$$
$$d\left(a,\chi\right)=\left|[g]\right|\deg\chi=\frac{|G|}{\left|C_G\left(g\right)\right|}\deg\chi$$

where x and y are defined by $k=x^{-1}gx$ and $\ell=y^{-1}hy$.

Remark II.7.6. In the setting that $\omega=1$, these formulas are simplified to read [NN1]:

$$S\left(\left(g,\chi\right),\left(h,\chi'\right)\right)=\frac{|G|}{\left|C_G\left(g\right)\right|\left|C_G\left(h\right)\right|}\sum_{k\in G(g,h)}\overline{\chi}\left(khk^{-1}\right)\overline{\chi'}\left(k^{-1}gk\right)$$
$$\theta\left(g,\chi\right)=\frac{\chi\left(g\right)}{\deg\chi}$$
$$d\left(g,\chi\right)=\left|[g]\right|\deg\chi=\frac{|G|}{\left|C_G\left(g\right)\right|}\deg\chi$$

where $G\left(g,h\right)=\left\{k\in G\mid gkhk^{-1}=khk^{-1}g\right\}$.

Since the twisted quantum doubles are always modular, they provide a limited source of braided fusion categories. However, recall that if $\mathcal{C}$ is a spherical fusion category, then its Drinfeld center $\mathcal{Z}\left(\mathcal{C}\right)$ is always a modular category [ENO1]. This leads to the notion of group-theoretical fusion categories.

Definition II.7.7. A spherical fusion category $\mathcal{C}$ is said to be **group-theoretical** if $\mathcal{Z}\left(\mathcal{C}\right)$ is braided monoidally equivalent to $D^{\omega}\left(G\right)$ for a finite group G and a 3-cocycle $\omega\in Z^3\left(G,\mathbb{K}^{\times}\right)$.

The Drinfeld double construction of braided fusion categories is still not very well understood and so it is surprising that group-theoretical fusion categories can be completely characterized by finite group data [ENO1]. In order to see how this is done, we follow [ENO1] and let G be a finite group with a subgroup H, a 3-cocycle $\omega\in Z^3\left(G,\mathbb{C}^{\times}\right)$ and a 2-cochain $\psi\in C^2\left(H,\mathbb{C}^{\times}\right)$ with $d\psi=\omega\mid_H$. We now take the category of G-graded vector spaces with associativity defined by ω, $\mathrm{Vec}_{G,\omega}$, and form the subcategory $\mathrm{Vec}_{G,\omega}\left(H\right)$ of H-graded objects in $\mathrm{Vec}_{G,\omega}$. Finally, we define the twisted group algebra $A=\mathbb{C}_{\psi}\left[H\right]$, which can be seen to be an associative algebra in $\mathrm{Vec}_{G,\omega}\left(H\right)$ [O5]. Group-theoretical categories, $\mathcal{C}\left(G,H,\omega,\psi\right)$ are exactly the categories of A-bimodules in $\mathrm{Vec}_{G,\omega}$ [ENO1; O5].

Group-theoretical categories are well understood [ENO1] and constitute a class of completely classified braided fusion categories. In fact, an entire classification program paralleling the rank classification discussed in this dissertation revolves around classifying integral modular categories whose dimensions have a specified prime factorization structure. Often, this classification results in the statement that such categories are group-theoretical. For instance, it has been shown that:

Theorem II.7.8. *If $\mathcal{C}$ is an integral fusion category, then $\mathcal{C}$ is group-theoretical if:*

(i) $\mathrm{FPdim}\,(\mathcal{C}) = p^n$ *[DGNO2, Corollary 6.8]*

(ii) $\mathrm{FPdim}\,(\mathcal{C}) = pq$ *[EGO, Theorem 6.3]*

(iii) $\mathrm{FPdim}\,(\mathcal{C}) = pqr$ *[ENO2, Theorem 9.2]*

Similarly, if $\mathcal{C}$ is an integral modular category, then $\mathcal{C}$ is group-theoretical if:

(i) $\mathrm{FPdim}\,(\mathcal{C}) = pq^3$ *[NR1, Proposition 4.12]*

(ii) $\mathrm{FPdim}\,(\mathcal{C}) = pq^4$ *[AIM1]*

(iii) $\mathrm{FPdim}\,(\mathcal{C}) = p^2q^2$ *for* $p, q > 2$ *[AIM1].*

where p, q, and r are distinct primes.

However, not all integral braided fusion categories are group-theoretical. For instance, the smallest non-group-theoretical integral modular category is in dimension 36 and arises from quantum groups [AIM1].

CHAPTER III

ARITHMETIC PROPERTIES OF MODULAR CATEGORIES

III.1 Galois Theory

As previously mentioned, modular categories enjoy a wide variety of arithmetic properties. Central to the study of such properties are the Galois symmetries of the category. These symmetries were first observed in the context of rational conformal field theories (RCFT) in [BG] and have since been expounded upon in [RSW; G1; DLN1]. In this section, we will give a brief account of the salient features, but a more complete analysis can be found in [RSW].

To properly discuss the Galois symmetries, we must first introduce some notation. As discussed in Chapter II, the columns of the S-matrix are eigenvalues of the fusion matrices and hence obey integral polynomials; in particular, they are algebraic integers. We thus have a number field $\mathbb{Q}(S)$, which is the field obtained by adjoining the elements of the S-matrix to $\mathbb{Q}$, that is, it is the smallest number field over which S is defined. This notation will be used for other matrices in this report, that is for any matrix M, the field $\mathbb{Q}(M)$ will be the field obtained by adjoining the elements of M to $\mathbb{Q}$. The fields $\mathbb{Q}(S)$ and $\mathbb{Q}(T)$ have a particularly restrictive structure:

Theorem III.1.1. *If $\mathcal{C}$ is a modular category with S-matrix, S, and T-matrix, T, then:*

(i) (de Boer-Goeree Theorem): $\mathbb{Q}(S)$ is abelian and Galois over $\mathbb{Q}$.

(ii) $\mathbb{Q}(T)$ is a cyclotomic field isomorphic to $\mathbb{Q}\left(\zeta_{\mathrm{ord}(T)}\right)$ and is a Galois extension of $\mathbb{Q}(S)$ [NS3].

The Galois structure of $\mathbb{Q}(S)$ can be exploited to study modular categories. Furthermore, this structure may provide a means to produce new modular categories from old ones. Indeed, the relations of Chapter II are algebraic in nature and hence, an element $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ can be applied. This suggests that one can apply an element σ of the absolute Galois group to the data describing a modular category $\mathcal{C}$ to produce a new modular category $\sigma(\mathcal{C})$. If $\sigma(\mathcal{C})$ exists as a modular category it is called a **Galois conjugate** of $\mathcal{C}$. Furthermore, the orbit of $\mathcal{C}$ under $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ is called a **Galois orbit** of $\mathcal{C}$. However, existence of Galois conjugate categories is a deep open question related to the realizability of a modular category given (N, S, T, R, F) satisfying the relations of the previous section. Furthermore, it is not even clear what field σ needs to permute. Indeed, the following is still an open question:

Question III.1.2. *If $\mathcal{C}$ is a modular category, can F be renormalized such that its entries reside in $\mathbb{Q}(T)$? If not, can one quantify the failure?*

Clearly from the definition of modular datum, we know that the Galois conjugate of modular datum is again modular datum. This observation allows us to speak of the Galois orbit and Galois conjugates of (pre)modular datum.

Despite these unanswered questions, Galois theory provides a very powerful tool for studying modular categories. For brevity in the following discussions, for a modular category $\mathcal{C}$, we define the **Galois group of $\mathcal{C}$** by $\mathrm{Gal}(\mathcal{C}) := \mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. By definition, this group acts by field automorphism on $\mathbb{Q}(S)$, but can also be seen to act by permutation on the set $\mathrm{Irr}(\mathcal{C})$ [RSW]. For this reason, we will abuse notation and refer to $\mathrm{Gal}(\mathcal{C})$ as an automorphism group and a subgroup of a symmetric group. Furthermore, the action of $\mathrm{Gal}(\mathcal{C})$ must permute normalized columns of the S-matrix. This permutation action can be made explicit [RSW, Theorem 2.7]:

Theorem III.1.3. *If $\mathcal{C}$ is a rank r modular category with modular datum (N_a, S, T) and Galois group G, then:*

(i) $\mathrm{Gal}(\mathcal{C})$ *embeds as an abelian subgroup of* $\mathfrak{S}_r$*.*

(ii) For any $\sigma \in G$, $P_\sigma = d_{\sigma(0)} S^{-1} \sigma(S)$ is a signed permutation matrix.

(iii) For each $\sigma \in G$, there are $\epsilon_{a,\sigma} = \pm 1$ such that

$$\begin{aligned}\sigma(S_{a,b}) &= \frac{\epsilon_{\sigma(b),\sigma} S_{a,\sigma(b)}}{d_{\sigma(0)}}\\ S_{a,b} &= \epsilon_{\sigma(a),\sigma}\epsilon_{b,\sigma} S_{\sigma(a),\sigma^{-1}(b)}\\ \epsilon_{\sigma^{-1}(a),\sigma^{-1}} &= \epsilon_{\sigma(0),\sigma}\epsilon_{0,\sigma}\epsilon_{a,\sigma}\end{aligned}$$

(iv) If r is even, then $\prod_{a=0}^{r-1} \epsilon_{a,\sigma} = (-1)^\sigma$. If r is odd, then $D \in \mathbb{Q}(S)$, and $\sigma(D) = \frac{\epsilon_\sigma D}{d_{\sigma(0)}}$ where $\epsilon_\sigma = \pm 1$ and $\prod_{a=0}^{r-1} \epsilon_{a,\sigma} = \epsilon_\sigma (-1)^\sigma$

This permutation action has many implications, many of which are explored in [RSW]. This group action and analysis when coupled with the dimensions as discussed in Section II.5 begins to hint at the arithmetic structure of the category. For instance, the Galois theory can often be exploited to understand the dimensions.

Proposition III.1.4. *If $\mathcal{C}$ is a modular category, then 0 is fixed by $\mathrm{Gal}(\mathcal{C})$ if and only if $\mathcal{C}$ is integral.*

Proof. First note that if $\mathcal{C}$ is integral, then $S_{0a} \in \mathbb{Z}$ for all a by Lemma II.5.1 and Proposition II.5.8. The result then follows from the fact that the permutation action arises from σ permuting the characters of the Grothendieck ring of $\mathcal{C}$, of which $\psi_0(X_a) = S_{0,a}$ is one.

Conversely, suppose that $\mathrm{Gal}(\mathcal{C})$ fixes 0, then it must fix $S_{0,b}$ for each b by Theorem III.1.3. Consequently, $S_{0,b} = d_b \in \mathbb{Q}$. On the other hand, d_b is an algebraic integer and hence d_a, $D^2 \in \mathbb{Z}$ for all a. By Proposition II.5.2, we know that there is a label a such that $S_{b,a} = d_a \,\mathrm{FPdim}(X_b)$. In particular, equation (II.17) gives $D^2 = d_a^2 \sum_b \mathrm{FPdim}(X_b)^2$, and thus $\mathrm{FPdim}(\mathcal{C}) = \frac{D^2}{d_a^2}$ is a rational algebraic integer. Consequently, $\mathcal{C}$ is weakly integral and, in particular, pseudo-unitary by Proposition II.5.8. Therefore, $d_a = \pm \operatorname{FPdim}(X_a)$ by Lemma II.5.1. □

Proposition III.1.5. *If $\mathcal{C}$ is a modular category and $\sigma \in \operatorname{Gal}(\mathcal{C})$, then $d_{\sigma(a)}$ is a unit in $\mathbb{Q}(S)$.*

Proof. First note that $\sigma\left(D^2\right) = \sum_{a\in\operatorname{Irr}(\mathcal{C})} \sigma\left(d_a\right)^2 = \sum_{a\in\operatorname{Irr}(\mathcal{C})} \frac{1}{d_{\sigma(0)}^2} S_{0,\sigma(a)}^2 = \frac{1}{d_{\sigma(0)}^2} D^2$. Taking the norm of both sides gives $N_{\mathbb{Q}(S)/\mathbb{Q}}\left(D^2\right) N_{\mathbb{Q}(S)/\mathbb{Q}}\left(d_{\sigma(0)}\right)^2 = N_{\mathbb{Q}(S)/\mathbb{Q}}\left(D^2\right)$ whence $N_{\mathbb{Q}(S)/\mathbb{Q}}\left(d_{\sigma(0)}\right) = \pm 1$. Since $d_{\sigma(0)} \in \mathbb{Q}(S)$, we can conclude that it is a unit in $\mathbb{Q}(S)$. □

These Galois techniques have been heavily exploited and were the main tool used in the classification of rank 4 and 5 modular categories [RSW; BNRW1]. For instance, it is often possible to exclude a modular category based on the cycle structure of its Galois group (not to be confused with its isomorphism class). For instance, it is shown in [BNRW1] that:

Proposition III.1.6. *Let $\mathcal{C}$ be a modular category of odd rank r, then:*

(i) If $r > 3$, then $(0\ 1)(2\ \ldots\ r-1) \notin \operatorname{Gal}(\mathcal{C})$.

(ii) If $\mathcal{C}$ is self-dual, then $(0\ 1\ \ldots\ r-3)(r-2\ r-1) \notin \operatorname{Gal}(\mathcal{C})$.

These techniques can be applied to produce the following tantalizing result.

Proposition III.1.7. *If $\mathcal{C}$ is an odd rank modular category and $\operatorname{Gal}(\mathcal{C}) = \langle(01)\rangle$, then $D^2 = \epsilon_\sigma d_1 N(D)$, and $d_a^2 = \epsilon_{a,\sigma} d_1 N(d_a)$ for $a > 1$, where $N(-)$ is the norm of $\mathbb{Q}(S)$ over $\mathbb{Q}$.*

Proof. Since $\mathcal{C}$ is odd rank, Theorem III.1.3 implies that $D \in \operatorname{Gal}(\mathcal{C})$. Furthermore, if $\sigma = (01) \in \operatorname{Gal}(\mathcal{C})$, then $\sigma(D) = \epsilon_\sigma D/d_1$. In particular, $D^2 = \epsilon_\sigma d_1 N(D)$. Similarly, $\sigma(d_a) = \epsilon_{a,\sigma} d_a/d_1$. Thus, $d_a^2 = \epsilon_{a,\sigma} d_1 N(d_a)$. □

This result tells us that, in the setting of this proposition, D^2 differs from an integer by at worse a unit in $\mathbb{Q}(S)$ and motivates the following conjecture.

Conjecture III.1.8. *If $\mathcal{C}$ is an odd rank modular category and $\operatorname{Gal}(\mathcal{C}) = \langle(01)\rangle$, then $\mathcal{C}$ is weakly-integral.*

Sadly, the techniques involved in analyzing the cycle structure of Galois groups are largely *ad hoc* and a more systematic approach is highly desirable. This can be accomplished through the classification of the fields $\mathbb{Q}(S)$ and isomorphism classes of Galois groups $\operatorname{Gal}(\mathcal{C})$. We will see in Section III.3 that there are strong primality conditions that must be satisfied by modular categories (resp. modular datum), which make such a classification possible and eliminate infinite sequences of possible categories (resp. modular datum). However, the Galois theory presented thus far is insufficient for such an undertaking. In fact, the key result follows from analyzing the representations of $\operatorname{SL}(2,\mathbb{Z})$ formed by the pair (S,T). This allows one to understand the extension $\mathbb{Q}(S) \subset \mathbb{Q}(T)$ and to gain insights into the field $\mathbb{Q}(S)$.

III.2 Representation Theory of $\mathrm{SL}(2,\mathbb{Z})$

The modular group is a widely studied group with important applications in complex analysis, where it describes the fractional linear transformations of the upper half plane, and in number theory, where it is describes the symmetries of elliptic functions. Geometrically, the modular group can be seen to describe the mapping class group of the torus. It is this last interpretation that we are most interested in. In this setting, it has presentation:

$$\mathrm{SL}(2,\mathbb{Z}) = \langle \mathfrak{s}, \mathfrak{t} \mid \mathfrak{s}^4 = 1,\ (\mathfrak{s}\mathfrak{t})^3 = \mathfrak{s}^2 \rangle$$

This abstract group can be realized as a matrix group by taking $\mathfrak{s} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\mathfrak{t} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Geometrically, $\mathfrak{s}$ flips the meridian and longitudinal cycles of a torus and $\mathfrak{t}$ twists the longitudinal direction (Dehn twist).

Given the topological nature of modular categories, in particular their relationship to TQFT and 3-manifold invariants [BKi; Tu1], it is unsurprising that the categories have a geometric flavor and are related to the modular group. In fact, it has been shown that every rank r modular category $\mathcal{C}$ generates a projective representation of the modular group:

$$\begin{aligned} \overline{\rho}_{\mathcal{C}} : \mathrm{SL}(2,\mathbb{Z}) &\to \mathrm{PGL}(r,\mathbb{K}) \\ \mathfrak{s} \mapsto \eta(S), &\quad \mathfrak{t} \mapsto \eta(T) \end{aligned}$$

where $\eta : \mathrm{GL}(r,\mathbb{K}) \to \mathrm{PGL}(r,\mathbb{K})$ is the natural surjection.

It has been shown that many of the algebraic relations of modular categories can be reinterpreted in terms of the mapping class group of the torus, e.g., the diagonalization of the fusion matrices by the S-matrix [Wal2]. While interesting, we will be more interested in the algebraic implications of this representation.

The connection between modular categories and modular representations has long been known. In [Eh1], certain classes of modular representations have been classified. These modular representations provide the building blocks for the modular datum, and, indeed, one can attempt to study modular categories in this way. However, there is a great deal of ambiguity. For instance, modular categories depend on the exact S- and T-matrix, not just their $\mathrm{GL}(r,\mathbb{K}^{\times})$-orbit, and in [Eh1], it is essentially only these orbits that are classified. In Chapter IV, we will see that there are only finitely many modular categories of fixed rank up to equivalence and so, modular categories constitute a measure zero set in the orbits of $\mathrm{SL}(2,\mathbb{Z})$ representations. Nonetheless, the theory of modular representations is very powerful and provides insights into the algebraic properties of modular categories and the number fields discussed in the previous section. Such an analysis was taken up in [NS3] where Ng and Schauenburg laid to rest the question:

Question III.2.1. *Is the kernel of a modular representation associated with a modular category always a congruence subgroup of* $\mathrm{SL}(2,\mathbb{Z})$*, i.e., does it contain a principal congruence subgroup* $\Gamma(N)$ *of* $\mathrm{SL}(2,\mathbb{Z})$*?*[1]

In [NS3, Theorem 6.8], it was shown that

Theorem III.2.2. *If* $\mathcal{C}$ *is a modular category over* $\mathbb{K}$ *with* $\mathrm{ord}(T) = N$*, then the kernel of the projective modular representation* $\overline{\rho}_{\mathcal{C}}$ *is a congruence subgroup of level* N*.*

This result spawned a great deal of research. In particular, the implications of this result for the number fields $\mathbb{Q}(S)$ and $\mathbb{Q}(T)$ were explored in [DLN1]. In the course of their work, they noted that one could define a **lift** of the projective representation $\overline{\rho}_{\mathcal{C}}$ to a linear one, that is find a linear representation ρ such that the following diagram commutes:

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

They further showed that all such liftings are all of the form:

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

where $\zeta \in \mathbb{K}$ is a 6-th root of the **anomaly** $\alpha = p^+/p^-$ and $x \in \mathbb{K}$ is a 12-th root of unity [DLN1, Section 1.3].

For notational simplicity, we will follow [DLN1] and define $s = \rho_x^\zeta(\mathfrak{s})$ and $t = \rho_x^\zeta(\mathfrak{t})$ for some x and ζ as above. A great deal of the structure of the S- and T-matrices is captured by s and t. For instance, the characters of the Grothendieck ring of $\mathcal{C}$ are still obtained through quotients of the s-matrix: $\psi_a(X_b) = \frac{s_{b,a}}{s_{0,a}}$. However, this renormalization of the S- and T-matrices has several advantages. For instance, it simplifies the Galois action of Theorem III.1.3 to:

$$\sigma(s_{a,b}) = \epsilon_{a,\sigma} s_{\sigma(a),b} = \epsilon_{b,\sigma} s_{a,\sigma(b)}$$

for all a, b and all $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}_{\mathrm{ab}})$, where $\mathbb{Q}_{\mathrm{ab}} = \cup_{n\in\mathbb{N}} \mathbb{Q}(\zeta_n)$. Just as in Theorem III.1.3, one can use the s-matrix to define a signed permutation matrix capturing the action of σ:

$$G_\sigma = \sigma(s)\, s^{-1} = \sigma\left(s^{-1}\right) s$$

[1] A **principal congruence subgroup** $\Gamma(N)$ is the kernel of the homomorphism $\mathrm{SL}(n,\mathbb{Z}) \to \mathrm{SL}(n,\mathbb{Z}/N\mathbb{Z})$.

Under these conventions, it was shown [DLN1, Theorem 1] that the congruence subgroup results of [NS3] and the Galois symmetries of [RSW] are related:

Theorem III.2.3. *Let $\mathcal{C}$ be a rank r modular category with* $\operatorname{ord}(T) = N$ *and* $\rho : \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{GL}(r,\mathbb{K})$ *be a (linear) modular representation of $\mathcal{C}$. Set $s = \rho(\mathfrak{s})$ and $t = \rho(\mathfrak{t})$, then:*

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

(ii) ρ is $\mathbb{Q}(\zeta_n)$-rational, i.e. $\operatorname{im}(\rho) \subset \mathrm{GL}(r,\mathbb{Q}(\zeta_n))$.

(iii) For $\sigma \in$ $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, *$G_\sigma = \sigma(s)s^{-1}$ is a signed permutation matrix, and*

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

for all $\mathfrak{g} \in \mathrm{SL}(2,\mathbb{Z})$.

(iv) Let k be an integer relatively prime to n with inverse ℓ modulo n, then for any automorphism σ_k of $\mathbb{Q}(\zeta_n)$ defined by $\zeta_n = e^{2\pi i/n} \mapsto \zeta_n^k = e^{2\pi k i/n}$, we have

$$G_{\sigma_k} = t^k s t^\ell s t^k s^{-1}$$

An immediate corollary to part (ii) of this theorem is that $\mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q}(s))$ is an elementary abelian 2-group. However, a stronger result was shown [DLN1, Proposition 6.5(iii)]:

Proposition III.2.4. *If $\mathcal{C}$ is a modular category, ρ is a modular representation with $s = \rho(\mathfrak{s})$ and $t = \rho(\mathfrak{t})$, and* $n = \operatorname{ord}(t)$, *then* $\mathrm{Gal}\left(\mathbb{Q}(t)/\mathbb{Q}\left(\frac{s_{a,b}}{s_{0,b}} \mid a,b \in \mathrm{Irr}(\mathcal{C})\right)\right)$ *is an elementary abelian 2-group.*

While this statement seems concerned with linear representations, it is actually tying together the fields $\mathbb{Q}(S)$, $\mathbb{Q}(s)$, $\mathbb{Q}(T)$, and $\mathbb{Q}(t)$. Indeed, $S_{0,0} = T_{0,0} = 1$ and so $\mathbb{Q}(S) \subset \mathbb{Q}(s)$ and $\mathbb{Q}(T) \subset \mathbb{Q}(t)$. Furthermore, s is related to S through a re-scaling and so $\mathbb{Q}\left(\frac{s_{a,b}}{s_{0,b}} \mid a,b \in \mathrm{Irr}(\mathcal{C})\right) = \mathbb{Q}(S)$. Thus, we have the following partial lattice of fields:

$$\begin{tikzcd}
& \mathbb{Q}(t) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(T) \arrow[dr, dash] & & \mathbb{Q}(s) \arrow[dl, dash] \\
& \mathbb{Q}(S) &
\end{tikzcd} \tag{III.1}$$

In particular, Proposition III.2.4 is telling us that all of these extensions are Galois and the relative Galois groups are elementary abelian 2-groups. Of course, this result is concerned with the algebraic structures of the modular datum of a modular category and so by definition must hold for all modular datum. For future use, we collect this result:

Corollary III.2.5. *If (N,S,T) is rank r modular datum and $\rho_x^\zeta : \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{GL}(r,\mathbb{K})$ is an associated linear modular representation with $s = \rho_x^\zeta(\mathfrak{s})$, $t = \rho_x^\zeta(\mathfrak{t})$, then $\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q}(S))$, $\mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q}(S))$, and $\mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q}(s))$ are elementary abelian 2-groups. Moreover, $\mathrm{Gal}(\mathbb{Q}(s)/\mathbb{Q}(S))$ has order 1 or 2.*

Proof. All but the last statement follows immediately from Proposition III.2.4, the Fundamental Theorem of Galois Theory, and the partial lattice III.1. The fact that $\mathrm{Gal}(\mathbb{Q}(s)/\mathbb{Q}(S))$ has order 1 or 2 follows from the observation that $\mathbb{Q}(s)$ is obtained from adjoining $\frac{\zeta^3}{x^3 p^+}$ to $\mathbb{Q}(S)$. Indeed, from definition of ζ, x, and p^+ one can see that $\frac{\zeta^3}{x^3 p^+}$ is a choice of square-root of D^2, i.e. it satisfies $y^2 - D^2$. □

This 2-group structure is quite restrictive and allows one to study the fields defined by s, S, t, and T. For instance, it has long been known that $\mathrm{ord}(T)$ can be bounded in terms of the rank of $\mathcal{C}$ [Ban2, Proposition 6]. To this author's knowledge, an explicit bound was never determined. However, the 2-group structure discussed in the previous corollary allows one to make such a bound explicit.

Proposition III.2.6. *If $\mathcal{C}$ is a modular category of rank r with modular datum (N,S,T), then $\mathrm{ord}(T) \leq 2^{2r/3+8}3^{2r/3}$.*

Proof. It is known, [BG1], that the abelian subgroup of $\mathfrak{S}_r$ of maximal order is:

$$G \cong \begin{cases} (\mathbb{Z}/3\mathbb{Z})^k & r = 3k \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^k & r = 3k+2 \\ (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^{k-1} \text{ or } (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^{k-1} & r = 3k+1 \end{cases}$$

in particular $|G| \leq 3^{r/3}$.

On the other hand, we know that $[\mathbb{Q}(T) : \mathbb{Q}(S)] \leq 2^m$ where m is bounded above by one more than the number of prime factors of $\mathrm{ord}(T)$. The Fundamental Theorem of Galois Theory can be utilized to the relate m to $\mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q})$. To do this, we note that

$$\mathrm{Gal}(\mathbb{Q}(S)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q}) / \mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q}(S))$$

In particular, the structure of $\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(T)/\mathbb{Q}(S))$ ensures that at least $m-3$ (non-trivial) cyclic factors survive in the quotient (the three possible exceptions correspond to primes 2 and 3 in $\mathrm{ord}(T)$) In particular the structure of the maximal abelian subgroup of $\mathfrak{S}_r$ ensures that $m - 3 <= r/3 + 1$. In particular:

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

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

Of course, this proof only relies on the fact that $\operatorname{Gal}(\mathbb{Q}(S)/\mathbb{Q})$ can be viewed as a subgroup of $\mathfrak{S}_r$ and that $\operatorname{Gal}\left(\mathbb{Q}\left(\zeta_{\operatorname{ord}(T)}\right)/\mathbb{Q}(S)\right)$ is an elementary abelian 2-group. So a similar statement can be made for $\operatorname{ord}(t)$. In fact, an entire program of studying the arithmetic properties of the fields $\mathbb{Q}(S)$, $\mathbb{Q}(s)$, $\mathbb{Q}(T)$, $\mathbb{Q}(t)$ can be instituted without reference to the underlying modular category. This will be done in the following section where it will be shown that $\mathbb{Q}(S)$ and $\mathbb{Q}(s)$ can largely be understood in terms of $\mathbb{Q}(T)$ or $\mathbb{Q}(t)$. This will be done through purely number theoretic considerations by studying a class of fields inspired by the above discussion.

III.3 Applications of Number Theory to Modular Categories

As was discussed in the previous sections, modular categories possess a Galois symmetry, which, when coupled with the $\operatorname{SL}(2,\mathbb{Z})$ structures underlying these categories, gives rise to interesting relations between the number fields one can construct from the category. For instance, it was shown in the previous section that $\mathbb{Q}(t)$ and is a cyclotomic field which is Galois over both $\mathbb{Q}(S)$ and $\mathbb{Q}(s)$, moreover the relative Galois groups are elementary abelian 2-groups. This structure allowed us to bound $\operatorname{ord}(T)$ and $\operatorname{ord}(t)$ strictly in terms of the rank of the category. In this section, we will examine a class of number fields which are inspired by these categories. This will allow us to determine primality conditions on modular categories, as well as restrict the fields and Galois groups that need to be considered. The reader not familiar with the number theoretic constructions of this section is encouraged to refer to Appendix A and references therein.

Given an abelian number field, $\mathbb{K}$, the Kronecker-Weber Theorem asserts that there is a cyclotomic extension $\mathbb{Q}(\zeta_m)$ containing $\mathbb{K}$. In particular, there is a minimal integer $\mathfrak{f}(\mathbb{K})$, such that $\mathbb{K} \subset \mathbb{Q}\left(\zeta_{\mathfrak{f}(\mathbb{K})}\right)$, called the **conductor** of $\mathbb{K}$.[2]

Remark III.3.1. When the field under consideration is clear from context, we will simply refer to the conductor as $\mathfrak{f}$ rather than $\mathfrak{f}(\mathbb{K})$.

Much of the information about a number field can be captured through studying its conductor. For instance, the prime divisors of the conductor and the discriminant of a number field must coincide. Since $\mathbb{Q}(\zeta_{\mathfrak{f}})$ is cyclotomic, there is a large volume of literature which can be brought to bear to produce interesting results on a number field $\mathbb{K}$ provided something is known about the extension $\mathbb{K} \subset \mathbb{Q}(\zeta_{\mathfrak{f}})$. On the other hand, it is known that if $\mathcal{C}$ is a modular category with S- and T-matrices, (S,T), and associated level n modular representation (s,t), then one can form a partial lattice of fields (III.1). As discussed in the previous section, properties of this lattice have been studied in [DLN1]. Much of their analysis is quite general and motivates studying *modularly admissible* number fields. A pair of number fields $(\mathbb{K},\mathbb{L})$ is said to be **modularly admissible** if $\mathbb{K} \subset \mathbb{L}$ with

[2] This classical notion of the conductor has been generalized in the context of class field theory in ideal theoretic language. While we will not need the full power of class field theory here, we retained the common symbol, $\mathfrak{f}$, for the conductor arising from that subject.

$\mathbb{L}$ a cyclotomic field and $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is an elementary abelian 2-group. Furthermore, an abelian number field, $\mathbb{K}$, will be said to be modularly admissible if $(\mathbb{K}, \mathbb{Q}(\zeta_{\mathfrak{f}}))$ is modularly admissible. It is clear from the discussion thus far that such fields arise in the context of modular categories. In particular, both $\mathbb{Q}(s)$ and $\mathbb{Q}(S)$ are modularly admissible by [DLN1].

In the language of modularly admissible fields, a portion of [DLN1, Proposition 6.5] can be recast to read:

Proposition III.3.2. *If $(\mathbb{K}, \mathbb{L})$ is modularly admissible and $\mathfrak{f}$ is the conductor of $\mathbb{K}$, then:*

(i) If $\mathbb{L} = \mathbb{Q}(\zeta_n)$, then $n = a\mathfrak{f}$ where $a \mid 24$ and $\gcd(a, \mathfrak{f}) \mid 2$.

(ii) $[\mathbb{L} : \mathbb{Q}(\zeta_{\mathfrak{f}})] \leq 8$ and $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\zeta_{\mathfrak{f}}))$ is an elementary abelian 2-group.

Remark III.3.3. Many of these results can be recovered through the elementary abelian 2-group condition of modularly admissible fields, ramification theory, and cyclotomic reciprocity [B4].

This result can be used to study modularly admissible fields, $\mathbb{K}$, of "small degree," that is satisfying $[\mathbb{K} : \mathbb{Q}] = p^n$ for some prime p and some integer n. Such analysis leads to conditions on the structure of the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ as well as interesting conditions on the prime p. Since modular categories always produce a modularly admissible field, $\mathbb{Q}(S)$, these primality conditions can be used to inform the study of modular categories.

Of particular importance when studying modularly admissible fields is the isomorphism provided by the Fundamental Theorem of Galois Theory:

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \,/\, \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \tag{III.2}$$

and the following isomorphism due to the Chinese Remainder Theorem:

Proposition III.3.4. *If $n = 2^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ where p_j are distinct odd primes, then*

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \begin{cases} (\mathbb{Z}/\varphi(p_2^{a_2})\mathbb{Z}) \times \cdots \times (\mathbb{Z}/\varphi(p_m^{a_m})\mathbb{Z}) & \text{if } a_1 = 0 \text{ or } 1 \\ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/\varphi(p_2^{a_2})\mathbb{Z}) \cdots \times (\mathbb{Z}/\varphi(p_m^{a_m})\mathbb{Z}) & \text{if } a_1 = 2 \\ (\mathbb{Z}/2\mathbb{Z}) \times \left(\mathbb{Z}/2^{a_1-2}\mathbb{Z}\right) \times (\mathbb{Z}/\varphi(p_2^{a_2})\mathbb{Z}) \times \cdots \times (\mathbb{Z}/\varphi(p_m^{a_m})\mathbb{Z}) & \text{if } a_1 \geq 3 \end{cases}$$

For uniformity of notation, it will be assumed that $\mathbb{L} = \mathbb{Q}(\zeta_n)$ and that $n = 2^a 3^b p_1^{a_1} \cdots p_m^{a_m}$ where $3 < p_j < p_{j+1}$ are prime and a, b are potentially zero. Furthermore, let k be defined by $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}/2\mathbb{Z})^k$.

Proposition III.3.4 immediately implies that each odd prime factor of n can account for at most 1 factor of $\mathbb{Z}/2\mathbb{Z}$ in the inclusion $(\mathbb{Z}/2\mathbb{Z})^k \hookrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ and that at most two copies can be accounted for depending on the value of a. This observation can be formally collected as follows:

Corollary III.3.5. *If $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with n and k as above, then there exists $b_j, d = 0, 1$ and $c \leq \max(0, a-1)$ such that*

$$[\mathbb{K} : \mathbb{Q}] = \frac{\varphi(2^a)}{2^c} \frac{\varphi(3^b)}{2^d} \frac{\varphi(p_1^{a_1})}{2^{b_1}} \cdots \frac{\varphi(p_m^{a_m})}{2^{b_m}}$$

in particular $k \leq \begin{cases} n-1 & \textit{if } a = 0,1 \\ n & \textit{if } a = 2 \\ n+1 & \textit{if } a \geq 3 \end{cases}$

These results can be used to restrict the structure of n given $[\mathbb{K} : \mathbb{Q}]$. For instance [RCo1]:

Proposition III.3.6. *If $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with n as above and $[\mathbb{K} : \mathbb{Q}]$ odd, then $p_j \equiv 3 \mod 4$.*

Proof. If $p^\ell \mid n$, then $(\mathbb{Z}/n\mathbb{Z})^\times$ has a direct factor of $\mathbb{Z}/\varphi(p^\ell)\mathbb{Z}$. Furthermore, $\varphi(p^\ell) = p^\ell - p^{\ell-1}$. Reduction modulo 4 shows that $p \not\equiv 1 \mod 4$. In particular, $\mathbb{Z}/4\mathbb{Z}$ appears as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. □

However, more refined statements can be made when the factorization of $[\mathbb{K} : \mathbb{Q}]$ is known. In particular, if $[\mathbb{K} : \mathbb{Q}] = p^h$ for some prime p, we know that $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ has a primary decomposition of the form $\mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_\ell}\mathbb{Z}$. The fact that $(\mathbb{K}, \mathbb{L})$ is modularly admissible constrains the structure of this group further. For instance, the values of r_j are intimately connected to the prime factorization of n.

Corollary III.3.7. *If $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with n and k as above, and $[\mathbb{K} : \mathbb{Q}] = p^h$ for some prime p, then:*

(i) If $p > 3$, then $a_j = 1$, $2^a 3^b \mid 24$, and there exists $r_j > 0$ such that $p_j = 2p^{r_j} + 1$ and $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_m}\mathbb{Z}$.

(ii) If $p = 3$, then $a_j = 1$, $0 \leq a \leq 3$, and there exists $r_j > 0$ and $r \geq 0$ such that $p_j = 2 \times 3^{r_j} + 1$; $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/3^r\mathbb{Z} \times \mathbb{Z}/3^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/3^{r_m}\mathbb{Z}$; and $b = \begin{cases} r+1 & r > 0 \\ 0,1 & r = 0 \end{cases}$.

(iii) If $p = 2$, then $a_j = 1$, $0 \leq \mu \leq 2$, $b = 0, 1$, and there exists $r_j > 0$, $0 \leq \mu \leq 2$, and $r \geq 0$, such that $p_j = 2^{r_j} + 1$ or $2^{r_j+1} + 1$; $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^\mu \times \mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2^{r_1}\mathbb{Z} \times \cdots \mathbb{Z}/2^{r_m}\mathbb{Z}$; and $a = \begin{cases} r+2 \textit{ or } r+3 & \textit{if } r \neq 0 \\ 0,1,2 & \textit{otherwise} \end{cases}$.

Proof. The proof proceeds in cases, first by analyzing $p > 3$ and then slightly modifying the argument in the $p = 2$ and 3 cases to account for the presence of $(\mathbb{Z}/2^a 3^b\mathbb{Z})^\times$ in $(\mathbb{Z}/n\mathbb{Z})^\times$.

<u>Case 1</u> $p > 3$: In this setting, take $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{r_\ell}\mathbb{Z}$ and note that the Fundamental Theorem of Galois Theory implies that $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times / (\mathbb{Z}/2\mathbb{Z})^k$.

Applying Corollary III.3.5, we see that $m = \ell$ and $\mathbb{Z}/p^{r_j} \cong \left(\mathbb{Z}/p_j^{a_j}\right)^\times / (\mathbb{Z}/2\mathbb{Z})$ as $p \nmid \varphi\left(2^a 3^b\right)$. In particular,

$$2p^{r_j} = p_j^{a_j - 1}(p_j - 1) \tag{III.3}$$

Consequently, if $a_j > 1$, then $p = p_j$ and $\exists \nu$ such that $2p^\nu = p - 1$, a contradiction for $\nu \neq 0$. Thus, $\nu = 0$ and $p = 3$, a further contradiction. Thus, we have $a_j = 1$ and $2p^{r_j} + 1 = p_j$.

Combining Corollary III.3.5 with Proposition III.3.4 allows one to conclude that $\varphi\left(2^a 3^b\right) \mid 24$, any larger and there would be an extraneous 2-group or 3-group factor.

Case 2 $p = 3$: In this setting we select r such that $3^r \mid\mid \varphi\left(2^a 3^b\right)$ in particular, $b = r + 1$ if $r \neq 0$ and 0 or 1 otherwise. Taking $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/3^r\mathbb{Z} \times \mathbb{Z}/3^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/3^{r_\ell}\mathbb{Z}$, Corollary III.3.5 then implies that each factor $\mathbb{Z}/3^{r_j}\mathbb{Z}$ must be isomorphic to $\left(\mathbb{Z}/p_j^{a_j}\right)^\times / (\mathbb{Z}/2\mathbb{Z})$ for some j. The argument is then completely analogous to the argument presented in the previous case.

Case 3 $p = 2$: In this case, Proposition III.3.4 implies that the factor of $2^a 3^b$ can give rise to $(\mathbb{Z}/2\mathbb{Z})^\mu \times (\mathbb{Z}/2^r\mathbb{Z})$ in the primary decomposition of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ and written in the proposition statement. Here, $(\mathbb{Z}/2\mathbb{Z})^\mu$ can acquire one factor from $\left(\mathbb{Z}/3^b\mathbb{Z}\right)^\times$ and one factor from $(\mathbb{Z}/2^a\mathbb{Z})^\times$ and so $0 \leq \mu \leq 2$. Of course, here, we are allowing $r = 1$ as a possibility. Consequently, the factor $(\mathbb{Z}/2^r\mathbb{Z})$ must be given by $\left(\mathbb{Z}/2^{a-2}\mathbb{Z}\right)$ or $\left(\mathbb{Z}/2^{a-2}\mathbb{Z}\right)/(\mathbb{Z}/2\mathbb{Z})$. Thus, $r = a - 2$ or $a - 3$. In particular, $a = r + 2$ or $r + 3$ if $r \neq 0$ and $a \leq 2$ for $r = 0$.

The remainder of this case proceeds just as above except now that $p_j - 1 = 2^{r_j}$ or $2^{r_j + 1}$. □

This result can be used to determine stringent conditions on p, the divisors of n, and the primary decomposition of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ in the setting that $[\mathbb{K} : \mathbb{Q}] = p^h$. Due to the special properties of 2 and 3, these cases must be treated separately. The case of $p > 3$ will be taken first and it requires the following lemma:

Lemma III.3.8. *If p and $2p^\beta + 1$ are primes larger than 3, then p and $2p^\beta + 1$ are congruent to 2 modulo 3 and β is odd.*

Proof. We proceed by cases based on the congruence class of p modulo 3. Since $p > 3$ is prime, we know that $p \not\equiv 0 \mod 3$. If $p \equiv 1 \mod 3$, then direct calculation reveals that $2p^\beta + 1 \equiv 0 \mod 3$. Primality of $2p^\beta + 1$ implies that $2p^\beta + 1 = 3$, a contradiction. Thus, $p \equiv 2 \mod 3$ and hence $2p^\beta + 1 \equiv (-1)^{\beta+1} + 1 \mod 3$. Thus β is odd lest we contradict the primality of $2p^\beta + 1$. □

Coupled with the above results, this lemma implies the following conditions on p and on the primary decomposition of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$:

Proposition III.3.9. *If $p > 3$ is prime and $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with $[\mathbb{K} : \mathbb{Q}] = p^h$, then:*

(i) $p \equiv 2 \mod 3$

(ii) There is a strict odd partition of h, $(r_1, \ldots, r_m)$, such that $2p^{r_j}+1$ is prime and the elementary divisors of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ *are* p^{r_j}.

(iii) $n = 2^a 3^b (2p^{r_1}+1)\cdots(2p^{r_m}+1)$ *where* $2^a 3^b \mid 24$.

Proof. As usual, let $n = 2^a 3^b p_1^{a_1}\cdots p_m^{a_m}$ and let $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}/p^{r_1}) \times \cdots (\mathbb{Z}/p^{r_\ell})$ be the primary decomposition ordered such that $r_j \leq r_{j+1}$. Then Corollary III.3.7 part (i) implies that $m = \ell$, $a_j = 1$, $p_j = 2p^{r_j}+1$ and $2^a 3^b \mid 24$. Since p_j is a prime factor of n, $r_j > 0$, and $p > 3$, Lemma III.3.8 implies that $p \equiv 2 \mod 3$ and that r_j is odd. Finally, by hypothesis $p_i \neq p_j$ for $i \neq j$ and so $r_i \neq r_j$ for $i \neq j$. Thus $(r_1, \ldots, r_\ell)$ form a strict odd partition of h. □

Remark III.3.10. The condition that $2p^r+1$ is prime can be quite strong depending on p and r. For instance, if $r = 1$ (p and $2p+1$ are prime), then one says that p is a **Sophie Germain prime**.[3] It has been conjectured, but is as yet unproven, that there are infinitely many Sophie Germain primes. Certainly, there are many examples of such primes, indeed the first few are:

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, \ldots$$

The sequence has been cataloged in [OEIS, A005384].

Corollary III.3.11. *If $p > 3$ is prime, $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with $[\mathbb{K} : \mathbb{Q}] = p^h$, and $\mathbb{Z}/p\mathbb{Z}$ appears in the primary decomposition of* $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$*, then p is a Sophie Germain prime.*

This result indicates that the infinitude of Sophie Germain primes can be answered through a study of modular categories.

Proposition III.3.12. *If $\{\mathcal{C}_j\}$ is an infinite sequence of modular categories such that* $\mathrm{Gal}(\mathcal{C}_j) \cong \mathbb{Z}/p_j\mathbb{Z}$ *with p_j prime and $p_j < p_{j+1}$, then there are infinitely many Sophie Germain primes.*

Proof. By [DLN1, Proposition 6.5], we know that $\mathbb{Q}(S)$ is modularly admissible and so the result follows by Corollary III.3.11. □

Due to Proposition III.3.9, the problem of understanding the possible isomorphism class of Galois groups $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ for modularly admissible fields $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ satisfying $[\mathbb{K} : \mathbb{Q}] = p^h$ with $p > 3$ prime can be greatly simplified through a combinatorial study of strict odd partitions of h. Such studies are common in combinatorics and it is well-known that the number of strict odd partitions of h, S_h, has generating function:

$$\sum_{h=0}^{\infty} S_h x^h = \prod_{j=0}^{\infty} \left(1 + x^{2j+1}\right) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 + 2x^8 + 2x^9 + \cdots$$

[3] If $2p+1$ is prime, but no restrictions are placed on p, then $2p+1$ is said to be a **safe prime**. This terminology arises from cryptography. Clearly, every Sophie Germain prime is safe, but the converse is false.

The sequence $\{S_h\}$ has been cataloged at [OEIS, A000700], and can be applied to produce the following result:

Proposition III.3.13. *If $p > 3$ is prime and $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with $[\mathbb{K} : \mathbb{Q}] = p^h$, then $p \equiv 2 \mod 3$. Furthermore, if $h \leq 7$, then $h \neq 2$ and:*

(i) If $h = 1$, 3, 5, or 7, then $2p^h + 1$ is prime, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/p^h\mathbb{Z}$, and $n = A\left(2p^h + 1\right)$ where $A \mid 24$.

(ii) If $h = 4$, or 6, then p is Sophie Germain, $2p^{h-1} + 1$ is prime, $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{h-1}\mathbb{Z}$, and $n = A(2p + 1)\left(2p^{h-1} + 1\right)$ where $A \mid 24$.

Proof. The claim that $h \neq 2$ follows immediately from the fact that there is no strict odd partition of 2. For $h \leq 7$ and $h \neq 2$, there is a unique strict odd partition of h depending on the parity of h: for h odd, the partition is (h) and, for h even, the partition is $(h - 1, 1)$. The result then follows from Proposition III.3.9 and Corollary III.3.11. □

Most of this analysis can be extended to the $p = 2$ and 3 cases, though some minor modifications are required due to the fact that $\left(\mathbb{Z}/2^a3^b\mathbb{Z}\right)^\times$ have factors of $\mathbb{Z}/2\mathbb{Z}$. Sadly, primes of the form $2 \times 3^r + 1$ are not well studied and so nothing beyond part (ii) of Corollary III.3.7 can be said in the case that $p = 3$.

In the $p = 2$ setting, things are much more interesting, in part due to the extensive studies done on primes of the form $2^a + 1$. In particular, the following two classical results can be used to induce strong conditions on modularly admissible fields of degree 2.

Lemma III.3.14. *If $2^c + 1$ is a prime > 3, then $\exists \ell$ such that $c = 2^\ell$.*

Proof. This statement is proved by contraposition and so it is assumed that c is not a power of 2. Consequently, c must split as $c = rs$ with s odd. Direct calculation reveals that $2^{rs} + 1 = (2^r - 1)\sum_{\ell=0}^{s-1} 2^\ell$, in particular, $2^{rs} + 1$ has a non-trivial factor. □

Lemma III.3.15. *If $2^c + 1$ is prime for $c > 2$, then neither $2^{c+1} + 1$ nor $2^{c-1} + 1$ are prime.*

Proof. From Lemma III.3.14, we know that if $2^c + 1$ is prime then $c = 2^\ell$ for some ℓ in particular, $c \equiv 0 \mod 2$. However, if $2^{c\pm1}+1$ is prime then $c\pm1 \equiv 0 \mod 2$ by Lemma III.3.14, a contradiction. □

Remark III.3.16. Numbers of the form $2^{2^c} + 1$ are called **Fermat numbers** and in the case that they are prime, they are called **Fermat primes**. The first five Fermat numbers are Fermat primes. Due to the quick growth of the numbers Fermat conjectured, but admitted that he could not prove, that all Fermat numbers are Fermat primes. However, it was later discovered that not all fermat numbers are prime, e.g. $2^{2^5} + 1$. This prompted Eisentein in 1844 to ask if there are infinitely many Fermat primes. Today it is widely believed that there are not, and in fact, many mathematicians believe that the only Fermat primes are the five known Fermat primes:[4] $3, 5, 17, 257, 65537$ [OEIS, A019434].

Fermat primes naturally arise when studying modularly admissible fields.

Proposition III.3.17. *If $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible with $[\mathbb{K} : \mathbb{Q}] = 2^h$, then there is a partition $(\mu, r, r_1, \ldots, r_m)$ of h, such that $0 \leq \mu \leq 2$ and:*

(i) $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{\mu} \times (\mathbb{Z}/2^r\mathbb{Z}) \times G$.

(ii) $0 < r_j < r_{j+1}$*, the elementary divisors of G are 2^{r_j}, and either $2^{r_j} + 1$ or $2^{r_j+1} + 1$ is a Fermat prime. In particular, $r_j = 2^{\ell_j}$ or $r_j = 2^{\ell_j} - 1$ for some $\ell_j \in \mathbb{N}$.*

(iii) $n = 2^a 3^b p_1 \cdots p_m$ *where* $p_j = 2^{r_j}+1$ *or* $2^{r_j+1}+1$, $b = 0, 1$, *and* $a = \begin{cases} r+2 \text{ or } r+3 & \text{if } r \neq 0 \\ 0, 1, 2 & \text{otherwise} \end{cases}$

Proof. This result follows by combining Corollary III.3.7, Lemma III.3.14, and Lemma III.3.15. □

One might wonder if such a study generalizes to modularly admissible fields with multiple prime factors. And, in fact it does. For instance, the above analysis *mutatis mutandis* gives the following result in degree 6.

Proposition III.3.18. *If $(\mathbb{K}, \mathbb{Q}(\zeta_n))$ is modularly admissible and $[\mathbb{K} : \mathbb{Q}] = 6$, then $n \mid 5040$ or 312.*

Remark III.3.19. In the general $[\mathbb{K} : \mathbb{Q}] = pq$ situation, there is a proliferation of cases, and while we find it interesting to ask what primality conditions arise and what the conductor of $\mathbb{K}$ can be, we will not address this problem further in this work.

The primality conditions arising in this section indicate that modularly admissible number fields are highly restricted and that a classification of such fields may be possible. Owing to special properties of the number 2, one can characterize all 2-Kummer (multi-quadratic) extensions of $\mathbb{Q}$ which are modularly admissible.

Proposition III.3.20. *If $\mathbb{K} = \mathbb{Q}\left(\sqrt{a_1}, \ldots, \sqrt{a_m}\right)$ is modularly admissible and the a_j are square-free integers, then $0 \leq m \leq 4$, and $a_j \in \{-1, \pm 2, \pm 3, 5, \pm 6\}$.*

Proof. Letting $\mathfrak{g}_j$ denote the conductor of $\mathbb{Q}\left(\sqrt{a_j}\right)$ and $\mathfrak{f}$ denote the conductor of $\mathbb{K}$, the Fundamental Theorem of Galois Theory produces the short exact sequence:

$$0 \to \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\mathfrak{f}}\right)/\mathbb{K}\right) \to \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\mathfrak{f}}\right)/\mathbb{Q}\right) \to \mathrm{Gal}\left(\mathbb{K}/\mathbb{Q}\right) \to 0$$

[4] There is a great deal of numeric evidence to suggest this, for instance, $2^{2^k} + 1$ is known to be composite for $5 \leq n \leq 32$.

Since $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\mathfrak{f}}\right)/\mathbb{K}\right)$ and $\mathrm{Gal}\left(\mathbb{K}/\mathbb{Q}\right)$ are elementary abelian 2-groups, one can conclude that the exponent of $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\mathfrak{f}}\right)/\mathbb{Q}\right)$ is 2 or 4. In particular, Proposition III.3.4 implies that $\mathfrak{f} \mid 120$. However, $\mathbb{Q}\left(\zeta_{\mathfrak{g}_j}\right)$ is a cyclotomic subfield of $\mathbb{Q}\left(\zeta_{\mathfrak{f}}\right)$, and so $\mathfrak{g}_j \mid 120$.

On the other hand, the prime divisors of the conductor and the discriminant of a number field must coincide. Consequently, the well-known discriminant formula for a quadratic field implies that the prime divisors of a_j are 2, 3, and 5. Since a_j is square-free, there are 16 possibilities. This finite list can be iterated through and the above result follows by computing $\mathfrak{f}$ in each case and demanding that $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{\mathfrak{f}}\right)/\mathbb{K}\right)$ is an elementary abelian 2-group. □

Remark III.3.21. While this greatly restricts the number of 2-Kummer extension of $\mathbb{Q}$ that can appear when studying modular categories, it is unknown if this bound is sharp. Indeed, the modular categories Fib, Ising, $\mathbb{Z}/3\mathbb{Z}-MTC$, $\mathbb{Z}/4\mathbb{Z}-MTC$, $\mathcal{C}\left(A_1, q=e^{\pi i/6}, \ell=6\right)$, and $D^{\omega}\left(QD16\right)$ realize the fields $\mathbb{Q}\left(\sqrt{5}\right)$, $\mathbb{Q}\left(\sqrt{-3}\right)$, $\mathbb{Q}\left(i\right)$, $\mathbb{Q}\left(\sqrt{3}\right)$, and $\mathbb{Q}\left(\sqrt{-2}\right)$ respectively through $\mathbb{Q}\left(S\right)$. However, we are not aware of a modular category satisfying $\mathbb{Q}\left(S\right)=\mathbb{Q}\left(\sqrt{\pm 6}\right)$ and so it is an open question as to whether or not the 2-Kummer fields: $\mathbb{Q}\left(\sqrt{\pm 6}\right)$, $\mathbb{Q}\left(\sqrt{5},\sqrt{6}\right)$, $\mathbb{Q}\left(\sqrt{6},\sqrt{-1}\right)$, and $\mathbb{Q}\left(\sqrt{-1},\sqrt{5},\sqrt{6}\right)$ are realized through $\mathbb{Q}\left(S\right)$ for some modular category.

Proposition III.3.2 and III.3.20 can be combined to produce the following corollary:

Corollary III.3.22. *If $\mathcal{C}$ is a modular category with S-matrix, S, and level n modular representation (s,t), such that $\mathbb{Q}\left(S\right)$ (resp. $\mathbb{Q}\left(s\right)$) is a 2-Kummer extension of $\mathbb{Q}$, then*

$$n \in \{3,4,5,6,8,10,12,15,16,20,24,30,40,48,60,80,120,240\}.$$

Furthermore, if $n \in \{3,4,6,8,12,24\}$, then $\mathbb{Q}\left(S\right)$ (resp. $\mathbb{Q}\left(s\right)$) is 2-Kummer.

To study modularly admissible fields $(\mathbb{K}, \mathbb{Q}\left(\zeta_n\right))$ satisfying $[\mathbb{K}:\mathbb{Q}]=p^h$, but which are not 2-Kummer extensions of $\mathbb{Q}$, one applies Proposition III.3.9, Proposition III.3.17, and part (ii) of Corollary III.3.7 to determine the possibilities for n and then performs an exhaustive search of subfields of $\mathbb{Q}\left(\zeta_n\right)$ for those that are modularly admissible. In the case that $p=3$, some general theory regarding the discriminant of cubic fields can be applied to ease the computation [HSW1], but, in general, the discriminants of number fields of prime power degree are poorly understood. Analysis can easily be performed on a desktop computer for $[\mathbb{K}:\mathbb{Q}]=3,4$, and 5, but as the degree increases the combinatorial explosion of cases quickly becomes overwhelming.

Proposition III.3.23. *If $(\mathbb{K}, \mathbb{Q}\left(\zeta_n\right))$ is a degree 3 modularly admissible field, then exactly one of the following is true:*

(i) $\mathbb{K}$ is the splitting field of $x^3-21x-7$, its conductor is 7, and $7 \mid n \mid 168$.

(ii) $\mathbb{K}$ is the splitting field of x^3-3x-1, its conductor is 9, and $9 \mid n \mid 72$.

Proposition III.3.24. *If $(\mathbb{K}, \mathbb{Q}\left(\zeta_n\right))$ is a degree 4 modularly admissible field, then either $\mathbb{K}$ is a 2-Kummer extension of $\mathbb{Q}$ or it is one of the fields given in Table III.1.*

Defining polynomial of $\mathbb{K}$	Conductor	Possible n
$x^4+x^3+x^2+x+1$	5	$20,40,60,120$
$x^4+2x^3-16x^2-32x+16$	15	$60,120$
x^4-4x^2+2	16	$16,32,48,96$
x^4+4x^2+2	16	$16,48$
x^4-5x^2+5	20	$20,40,60,120$
x^4-10x^2+20	40	$40,120$
x^4+10x^2+20	40	$40,120$
x^4-12x^2+18	48	48
x^4+12x^2+18	48	48
x^4+15x^2+45	60	$60,120$
x^4-30x^2+180	120	120
x^4+30x^2+180	120	120

Table III.1: Modularly admissible fields with Galois group $\mathbb{Z}/4\mathbb{Z}$.

Proposition III.3.25. *If $(\mathbb{K},\mathbb{Q}(\zeta_n))$ is a degree 5 modularly admissible field, then $\mathbb{K}$ is the splitting field of $x^5+x^4-4x^3-3x^2+3x+1$, its conductor is 11, and $11 \mid n \mid 264$.*

These results can be applied to modular categories and provide particularly powerful techniques when considering (weakly) integral modular categories as will be demonstrated in Section V.2.

CHAPTER IV

RANK FINITENESS AND THE CAUCHY THEOREM

Despite the work done on the classification of modular categories it has been an open question as to whether or not this was a computationally feasible problem since 2003. The feasibility comes in the guise of a finiteness conjecture due to Wang [W1]:

Conjecture IV.0.26. *There are finitely many modular categories of fixed rank r, up to equivalence.*

Prior to the work [BNRW1], this conjecture had only been resolved in certain restricted cases. For instance, it was shown [ENO1, Proposition 8.38] that there are finitely many weakly integral fusion categories through a classical number theoretic argument due to Landau [L1].

The key breakthrough in the general setting is a divisibility result proven in [BNRW1] known as the Cauchy Theorem for Modular Categories:

Theorem IV.0.27 (Cauchy Theorem for Modular Categories)**.** *If $\mathcal{C}$ is a modular category with T-matrix, T, and global dimension D^2, then the prime factors of* $\operatorname{ord}(T)$ *and* D^2 *coincide in* $\mathbb{Q}(T)$.

Remark IV.0.28. This theorem derives its name from its relationship to finite groups. Indeed, this theorem reduces to the classical Cauchy Theorem for finite groups when $\mathcal{C} = \operatorname{Rep}(D(G))$ for a finite group G since, in this, case $\operatorname{ord}(T) = \operatorname{Exp}(G)$ and $D^2 = |G|^2$.

This theorem complements the divisibility discussed in Proposition II.5.5 and fixes the prime divisors of the dimensions in a category in terms of the T-matrix. Restricting the prime divisors of algebraic integers imposes incredibly stringent conditions on the types of numbers that can appear as dimensions. Algebraic numbers with fixed prime divisors are well-known to number theorists and go under the moniker: *$\mathcal{S}$-units.* The general use of $\mathcal{S}$-units in number theory has previously prompted a study of their properties. Of particular interest in this paper is a finiteness result from the 1980's due to Evertse [Ev1]. In [Ev1], Evertse shows that there are finitely many $\mathcal{S}$-units, $\{x_j\}$, up to scaling that satisfy the innocuous equation $0 = x_1 + \cdots + x_r$ subject to certain mild non-degeneracy conditions.

In this chapter, the $\mathcal{S}$-units and the $\mathcal{S}$-unit equation will be introduced. Readers familiar with these concepts should feel free to skip Section IV.1, while for those readers wanting to know more, a more complete accounting of these topics can be found in [We1; Ch1]. With these preliminary concepts covered, Section IV.2 will be devoted to the application of the proof of rank finiteness through the Cauchy Theorem for Modular Categories and the classical theory of $\mathcal{S}$-units.

IV.1 $\mathcal{S}$-units

Broadly speaking, $\mathcal{S}$-units are algebraic numbers with a predefined set of prime divisors. These numbers are a natural generalization of $\mathcal{O}_{\mathbb{K}}^{\times}$. In fact, from an adelic perspective, the ring of integers and unit group are overspecialized and $\mathcal{S}$-units and $\mathcal{S}$-integers are somewhat more natural. $\mathcal{S}$-integers (units) have a very rigid and beautiful theory from the adelic point of view which is introduced in [We1]. This paper will not need the full power of the adele ring and we will restrict our attention to the classical notions of places, absolute values, and divisibility.

The theory of primality in a number field can be studied through equivalence classes of absolute values on the field known as *places.* Places provide a means to study number fields topologically by associating valuations and absolute values to primes in a number field lying over rational primes. Explicitly, one can define a discrete valuation on a number field $\mathbb{K}$, $\operatorname{ord}_{\mathfrak{p}} : \mathbb{K}^{\times} \to \mathbb{Z}$, for each prime ideal $\mathfrak{p}$ by $\operatorname{ord}_{\mathfrak{p}}(\alpha) = k$ where k is defined to be the unique integer such that $(\alpha) = \mathfrak{p}^k \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ is the factorization of the (fractional) ideal (α). The valuation corresponding to $\mathfrak{p}$ allows us to define a **$\mathfrak{p}$-adic absolute value** on $\mathbb{K}$ by

$$|x|_{\mathfrak{p}} = \begin{cases} 0 & \text{if } x = 0 \\ c^{\operatorname{ord}_{\mathfrak{p}}(x)} & \text{if } x \neq 0 \end{cases}$$

for some $c \in (0,1)$.[1] It can be shown that the $\mathfrak{p}$-adic absolute value on $\mathbb{K}$ is non-Archimedean, that is, it satisfies the ultrametric inequality $|x+y|_{\mathfrak{p}} \leq \max\left\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\right\}$. In order to determine Archimedean absolute values, one can utilize the field embeddings $\sigma_j : \mathbb{K} \hookrightarrow \mathbb{C}$. These embeddings will be ordered such that the first r_1 embeddings are real, the next r_2 embeddings are complex and distinct under complex conjugation, and the last r_2 will be given by $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$. These embeddings can be used to pull-back the absolute values from $\mathbb{R}$ and $\mathbb{C}$ respectively:

$$|x|_{\sigma_j} = \begin{cases} |\sigma_j(x)| & \text{if } 1 \leq j \leq r_1 \\ |\sigma_j(x)|^2 & \text{if } r_1 + 1 \leq j \leq r_2 \end{cases}$$

Remark IV.1.1. While there are $r_1 + 2r_2$ field embeddings, only $r_1 + r_2$ distinct absolute values can be formed by pull-back since $|\cdot|_{\sigma_{r_1+j}} = |\cdot|_{\sigma_{r_1+r_2+j}}$. For this reason when considering the Archimedean absolute arising in this way, we will only consider $|\cdot|_{\sigma_j}$ for $1 \leq j \leq r_1 + r_2$.

The Archimedean and the non-Archimedean absolute values can be used to define metric topologies on $\mathbb{K}$, and it is natural to ask if the induced topologies are distinct. When the topologies induced by two absolute values are not distinct, the absolute values are said to be **equivalent** and an equivalence class of absolute values on $\mathbb{K}$ is called a **place**. Furthermore, the set of places on $\mathbb{K}$ will be denoted by $V_{\mathbb{K}}$. A well-known theorem due to Ostrowski says that the above discussion exhausts the places of $\mathbb{K}$ [Ch1]:

Theorem IV.1.2 (Ostrowki)**.** *If $|\cdot|$ is an absolute value on $\mathbb{K}$, then either $|\cdot|$ is Archimedean and equivalent to $|\cdot|_{\sigma_j}$ for some embedding σ_j, or $|\cdot|$ is non-Archimedean and is equivalent to $|\cdot|_{\mathfrak{p}}$ for some finite prime $\mathfrak{p}$. Moreover, $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{q}}$ are inequivalent for $\mathfrak{p} \neq \mathfrak{q}$.*

[1] The exact value of c will not alter the topology induced on the number field by the $\mathfrak{p}$-adic absolute value.

In light of this, we say that a place is **discrete** or **non-Archimedean** if it contains the absolute value $|\cdot|_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$. The place is said to be **real (resp. imaginary) Archimedean** if it contains the absolute value $|\cdot|_{\sigma_j}$ for some real (resp. complex) embedding σ_j. Furthemore, due to the correspondence between non-Archimedean places and finite primes, one often calls the Archimedean places *infinite places* (or *infinite primes*) and the discrete places are often called *finite places* (or *finite primes*).

A study of places quickly reveals that certain choices of representatives of places lead to particularly nice results. In order to discuss these places and distinguished representatives we, introduce the following notation:

- If $v \in V_{\mathbb{K}}$ is a discrete place, then denote the corresponding prime ideal by $\mathfrak{p}_v$.
- For a finite prime $\mathfrak{p}$, denote by $v_{\mathfrak{p}}$ the place containing $|\cdot|_{\mathfrak{p}}$.
- For finite places v, $\operatorname{ord}_v := \operatorname{ord}_{\mathfrak{p}_v}$.
- For an embedding σ_j, denote the corresponding place by v_{σ_j}.
- The set of infinite places will be denoted by $\mathcal{S}_\infty$.

A canonical choice of representatives for each place is then given by:

$$|\cdot|_v = \begin{cases} N_{\mathbb{K}/\mathbb{Q}}\left(\mathfrak{p}_v\right)^{-\operatorname{ord}_v(\cdot)} & v \text{ is finite} \\ \left|\sigma_v\left(\cdot\right)\right| & v \text{ is infinite real} \\ \left|\sigma_v\left(\cdot\right)\right|^2 & v \text{ is infinite complex} \end{cases}$$

Under this normalization, one can show that the famous **product formula** holds [Mi1]:

Theorem IV.1.3 (Product Formula)**.** *If* $\alpha \in \mathbb{K}^\times$*, then* $\displaystyle\prod_{v \in V_{\mathbb{K}}} |\alpha|_v = 1.$

Examination of the finite places reveals that, for any $\alpha \in \mathbb{K}^\times$, there must be at most finitely many places with $|\alpha|_v \neq 1$. Consequently, the product in Theorem IV.1.3 is really finite for any fixed $\alpha \in \mathbb{K}^\times$. So one might ask, *For a finite set of places* $\mathcal{S}$ *containing* $\mathcal{S}_\infty$*, what numbers* $\alpha \in \mathbb{K}^\times$ *satisfy* $\prod_{v\in\mathcal{S}} |\alpha|_v = 1$*?* In the case that $\mathcal{S} = \mathcal{S}_\infty$, our choice of $|\cdot|_v$ reveals that $\prod_{v\in\mathcal{S}_\infty} |\alpha|_v = \left|N_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|$ and so the numbers of interest are simply the units, $\mathcal{O}_{\mathbb{K}}^\times$. By expanding $\mathcal{S}$ to encompass finitely many finite places, numbers with a fixed set of prime divisors are allowed. However, the numbers under consideration always satisfy a norm-like condition: $\prod_{v\in\mathcal{S}} |\alpha|_v = 1$ which inspires their moniker **$\mathcal{S}$-units**. The $\mathcal{S}$-units form a multiplicative group, which by analogy with the unit group, will be denoted by $\mathcal{O}_{\mathbb{K},\mathcal{S}}^\times$ or simply $\mathcal{O}_{\mathcal{S}}^\times$ when the field under consideration is clear.[2]

$\mathcal{S}$-units often appear in number theory and have been widely studied. Of particular interest are

[2] This may seem like a thin reason for calling these numbers "units", however one can actually construct a ring $\mathcal{O}_{\mathbb{K},\mathcal{S}} = \left\{x \in \mathbb{K} \mid \prod_{v\in\mathcal{S}} |x|_v \leq 1\right\}$ called the ring of $\mathcal{S}$-integers, which are themselves a natural notion of an integer ring in the ring of adeles, in this ring the $\mathcal{S}$-units are the multiplicative unit group.

those satisfying the **$\mathcal{S}$-unit equation**

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

for some fixed positive integer n. This equation is said to be a **proper $\mathcal{S}$-unit equation** if one demands:

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

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

Clearly if $(x_0, \ldots, x_n) \in \mathbb{K}^{n+1}$ satisfies a (proper) $\mathcal{S}$-unit equation, then any scalar multiple of this affine point will satisfy the same equation. For this reason, one often studies the $\mathcal{S}$-unit equation projectively, that is searches for projective points $X = [x_0 : \cdots : x_n] \in \mathbb{P}^n\mathbb{K}$ satisfying the (proper) $\mathcal{S}$-unit equation and subject to the condition that there is an affine representative of X, $x = (x_0, \ldots, x_n) \in \left(\mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}\right)^{n+1}$.

Due to the projective and algebraic nature of the (proper) $\mathcal{S}$-unit equation, it is perhaps unsurprising that certain tools from algebraic geometry are employed to study $\mathcal{S}$-units. In particular, the **projective height** is often used

$$H(X) = \prod_{v \in V_{\mathbb{K}}} \max\left(|x_0|_v, \ldots, |x_n|_v\right)$$

where $X = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n\mathbb{K}$. This projective height is an important quantity to number theorists and, in fact it can be shown that there are finitely many projective points in $\mathbb{P}^n\mathbb{K}$ with bounded projective height.

In 1984, Evertse took up a study of $\mathcal{S}$-units through analyzing the projective height [Ev1]. By bounding the projective height, he showed *loc. cit.*:

Theorem IV.1.4. *If $\mathbb{K}$ is a number field, $\mathcal{S}$ a finite set of places of $\mathbb{K}$ containing $\mathcal{S}_\infty$, and n is a fixed positive integer, then there are only finitely many projective points $X = [x_0 : \cdots : x_n] \in \mathbb{P}^n\mathbb{K}$ satisfying the proper $\mathcal{S}$-unit equation:*

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

IV.2 Rank Finiteness and a Classification Algorithm

The goal of this section is to provide a proof of rank finiteness for modular categories through a reduction to Theorem IV.1.4 via the Cauchy Theorem for Modular Categories. Specifically, it will be shown that:

Theorem IV.2.1. *There are only finitely many modular categories of fixed rank r, up to equivalence.*

The first step in this analysis is to reduce the the proof of this theorem to bounding the FP-dimension. While it has long been known that there are finitely many modular categories of bounded FP-dimension (up to equivalence), cf. the proof of [ENO1, Proposition 8.38], we arrive at this result in a new way.

Ocneanu Rigidity (Theorem II.1.39) is a relatively classical result in the field of fusion categories and says that: *there are finitely many fusion categories of fixed fusion ring, up to equivalence.* In particular, if the fusion coefficients of a fusion category can be bounded, one can conclude, by Ocneanu Rigidity, that there are only finitely many fusion categories satisfying said bounds, up to equivalence. Such a bound on the fusion coefficients can be determined in terms of the FP-dimensions through the spectral theory for matrices.

Scholium IV.2.2. *If $\mathcal{C}$ is a rank n fusion category, then for any simple object X_a, we have the inequality:*

$$||N_a||_{max} \leq \mathrm{FPdim}\left(X_a\right) = ||N_a||_2 \leq n\, ||N_a||_{max}$$

where here $||\cdot||_{max}$ is the max-norm on matrices which is given by:

$$||A||_{max} = \max_{i,j} \left\{|a_{ij}|\right\}$$

Proof. Letting $\rho\left(N_a\right)$ denote the spectral radius of N_a, recall that the 2-norm of N_a is given by $||N_a|| = \sqrt{\rho\left(N_a^T N_a\right)}$. Next recalling that N_a is normal, it follows that N_a and N_a^T are simultaneously diagonalizable. In particular, by definition of the spectral radius, we see that $\rho\left(N_a^T N_a\right) \leq \rho\left(N_a^T\right)\rho\left(N_a\right)$. Of course, $N_a^T = N_{a^*}$ and $\rho\left(N_b\right) = \mathrm{FPdim}\left(X_b\right)$ for all b. Therefore, $||N_a||_2 \leq \rho\left(N_a\right) = \mathrm{FPdim}\left(X_a\right)$. On the other hand, it is well-known that $\rho\left(A\right) \leq ||A||_2$ for any complex-valued matrix. It follows that $\rho\left(N_a\right) = ||N_a||_2$. The result then follows by recalling that the 2-norm and the max-norm are related by: $||A||_{max} \leq ||A||_2 \leq \sqrt{mn}\, ||A||_{max}$ for an $m \times n$ matrix A. □

This scholium couples with Ocneanu Rigidity to give the following finiteness result.

Corollary IV.2.3. *There are finitely many fusion categories $\mathcal{C}$ satisfying* $\mathrm{FPdim}\left(\mathcal{C}\right) \leq M$ *for some fixed number M, up to equivalence.*

Proof. From the definition of $\mathrm{FPdim}\left(\mathcal{C}\right)$, we know that $\mathrm{FPdim}\left(X_a\right) \leq \mathrm{FPdim}\left(\mathcal{C}\right)$ and hence the fusion coefficients are bounded above by M by Scholium IV.2.2. Since the fusion coefficients are non-negative integers, the result follows by Ocneanu Rigidity. □

Coupling this result with the Cauchy Theorem for Modular Categories (IV.0.27) and the upper bound on $\operatorname{ord}(T)$ given by Proposition III.2.6, we can reduce the proof of Theorem IV.2.4 to this corollary and Evertse's $\mathcal{S}$-unit finiteness result (Theorem IV.1.4).

Theorem IV.2.4. *There are finitely many modular categories of fixed rank r, up to equivalence.*

Proof. For fixed rank r, Proposition III.2.6 provides an explicit upper bound on $\operatorname{ord}(T)$. For such $\operatorname{ord}(T)$, one may define the finite set of places, $\mathcal{S}$, of $\mathbb{Q}\left(\zeta_{\operatorname{ord}(T)}\right)$ to be those satisfying $\left|\operatorname{ord}(T)\right|_v \neq 1$. The Cauchy Theorem for Modular Categories coupled with [EG1, Lemma 1.2] then implies that D^2 and d_j are $\mathcal{S}$-units for all simple objects X_a. Furthermore, the definition of the global dimension of the category gives rise to the $\mathcal{S}$-unit equation:

$$0 = D^2 - d_0^2 - \cdots - d_{r-1}^2$$

This equation is a proper $\mathcal{S}$-unit equation owing to the fact that d_a^2 is a real positive number for all a. In particular, Theorem IV.1.4 shows that there are finitely many projective solutions to this equation. Recalling that $d_0^2 = 1$ allows us to fix the normalization in the above $\mathcal{S}$-unit equation. In particular, we can conclude that there is a upper bound on D^2 and a lower bound on d_a for all a.

However, $\operatorname{FPdim}(\mathcal{C}) = D^2/d_a^2$ for some simple dimension d_a by Proposition II.5.2. Consequently, the lower bound on d_a and an upper bound on D^2 imply an upper bound on $\operatorname{FPdim}(\mathcal{C})$. The result then follows from Corollary IV.2.3 and the observation that these bounds depend only on the rank. □

This proof not only gives rank finiteness, but it also suggest an algorithm for classifying modular categories of fixed rank. Indeed, it follows from Dirichlet's unit theorem that [We1]:

Theorem IV.2.5. *If $\mathbb{K}$ is a number field and $\mathcal{S}$ is a finite set of places containing $\mathcal{S}_\infty$, then $\mathcal{O}_{\mathbb{K},\mathcal{S}}^\times$ is a finitely generated abelian group with torsion given by the roots of unity in $\mathbb{K}$ and free part of rank $\#\mathcal{S} - 1$.*

A set of generators for the free part of $\mathcal{O}_{\mathbb{K},\mathcal{S}}^\times$ is known as a **system of fundamental $\mathcal{S}$-units** and there are known algorithms for computing such a system, e.g. [C2]. Coupling these observations produces the following classification algorithm:

Algorithm IV.2.6.

(0) Specify the rank, r.

(1) For each integer N with $1 \leq N \leq 2^{2r/3+8}3^{2r/3}$ perform steps 2-9.

(2) Form the set of places, $\mathcal{S}$, of $\mathbb{Q}(\zeta_N)$ consisting of the infinite places and those associated with the prime factors of N.

(3) Determine a fundamental system of $\mathcal{S}$-units, $\epsilon_1, \ldots, \epsilon_{s-1}$.

(4) Solve the exponential Diophantine system:

$$1 = \epsilon_1^{a_{r,1}} \cdots \epsilon_{s-1}^{a_{r,s-1}} - \sum_{j=1}^{r-1} \epsilon_1^{a_{j,1}} \cdots \epsilon_{s-1}^{a_{j,s-1}}, \quad a_{j,k} \in \mathbb{Z} \tag{IV.1}$$

(5) Set $\operatorname{FPdim}(\mathcal{C}) = \epsilon_1^{a_{s,1}} \cdots \epsilon_{s-1}^{a_{s,s-1}}$ and $\operatorname{FPdim}(X_j)^2 = \epsilon_1^{a_{j,1}} \cdots \epsilon_{s-1}^{a_{j,s-1}}$. Verify that these numbers are positive algebraic integers and that $\operatorname{FPdim}(X_j)^2 \mid \operatorname{FPdim}(\mathcal{C})$.

(6) Determine the fusion coefficients $N_{a,b}^c$ satisfying the symmetries II.13 and Scholium IV.2.2.

(7) For each diagonal matrix T or order N with $T_{0,0} = 1$, determine S from N_a and T by equation (II.16).

(8) Verify the algebraic relations of Chapter II for (N, S, T), e.g., equations II.15 and II.10.

(9) Search for realizations.

There are however, several pit-falls. The most obvious being the search for realizations, which still remains a black-art. However, even more fundamentally speaking, the algorithm is very inefficient. Indeed, the known algorithms for computing fundamental systems of $\mathcal{S}$-units rely on computing a shortest vector in a lattice, a problem which is known to be NP-hard.[3] Furthermore, solving equation (IV.1) is very difficult. Finally, even assuming that these obstacles can be overcome, the bound on the number of solutions is currently quadrupally exponential:

Proposition IV.2.7. *For fixed rank r, there are at most*

$$\sum_{m=1}^{2^{2r/3+8}3^{2r/3}} \left(2^{35}r^2\right)^{r^3\left(\varphi(m)^{\log_2(m)}+\varphi(m)/2+1\right)-r/2}$$

possible solutions to the dimension equation:

$$D^2 = 1 + d_1^2 + \cdots + d_{r-1}^2$$

Proof. First note that by [Ev2, Theorem 3], there are at most $\left(2^{35}r^2\right)^{r^3 s - r/2}$ solutions to the proper $\mathcal{S}$-unit equation:

$$x_1 + x_2 + \cdots + x_r = 1$$

subject to $x_j \leq x_{j+1}$, where s is the cardinality of $\mathcal{S}$.

However, s depends on the prime factorization of $\operatorname{ord}(T)$. In particular, if p is a rational prime of $\operatorname{ord}(T)$, and there are at worst $\varphi(\operatorname{ord}(T))$ primes lying over p in $\mathbb{Q}\left(\zeta_{\operatorname{ord}(T)}\right)$. Thus there are at most $\operatorname{ord}(T)^{\omega(\operatorname{ord}(T))}$ finite places in $\mathcal{S}$, where $\omega(m)$ is defined to be the number of rational prime divisors

[3] Preliminary analysis reveals that computing a fundamental system of $\mathcal{S}$-units may reside in BQP [B3; Ha1; HM1; SV1].

of m. Elementary analysis reveals that $\omega\left(m\right) \leq \log_2\left(m\right)$ and so $s \leq \varphi\left(\operatorname{ord}\left(T\right)\right)^{\log_2\left(\operatorname{ord}\left(T\right)\right)} + r_1 + r_2$ where r_1 is the number of distinct real field embeddings of $\mathbb{K}$ into $\mathbb{C}$, and r_2 is the number of conjugate pair complex field embeddings. However, it is well-known that a non-trivial cyclotomic field has no real embeddings. In particular, $r_2 = \varphi\left(\operatorname{ord}\left(T\right)\right)/2$ and $s \leq \varphi\left(\operatorname{ord}\left(T\right)\right)^{\log_2 \operatorname{ord}\left(T\right)} + \varphi\left(\operatorname{ord}\left(T\right)\right)/2 + 1$. Combining these two results reveals that an upper bound on the number of possible dimension tuples $\left(\operatorname{FPdim}\left(\mathcal{C}\right), 1, \operatorname{FPdim}\left(X_1\right)^2, \ldots, \operatorname{FPdim}\left(X_{r-1}\right)^2\right)$ for a rank r modular category with T-matrix of order $\operatorname{ord}\left(T\right)$ is $\left(2^{35}r^2\right)^{r^3\left(\varphi(\operatorname{ord}(T))^{\log_2(\operatorname{ord}(T))} + \varphi(\operatorname{ord}(T))/2+1\right) - r/2}$. The result then follows by summing over all possible values of $\operatorname{ord}\left(T\right)$ as determined by Proposition III.2.6. □

It is interesting to ask whether or not this bound is necessary asymptotically. It is a widely held belief that modular categories are "sparse", a belief which is borne out in small rank, e.g., compare the 2 actual solutions in rank 2 with the theoretical bound of $\approx 2^{10^{42}}$. However, asymptotic analysis is still lacking and so one might ask:

Question IV.2.8. *Is there an asymptotic bound on the number of modular categories (up to equivalence) in terms of the rank which is better than those implied by Proposition IV.2.7?*

Along similar lines, one might ask

Question IV.2.9. *Is there an explicit upper bound on* $\operatorname{FPdim}\left(\mathcal{C}\right)$ *solely in terms of the rank?*

Remark IV.2.10. This question seems tractable as the analysis of Evertse shows that the projective height of $\left[-\operatorname{FPdim}\left(\mathcal{C}\right) : 1 : \operatorname{FPdim}\left(X_1\right)^2 : \cdots : \operatorname{FPdim}\left(X_{r-1}\right)^2\right]$ can be bounded in terms of field data and hence in terms of $\operatorname{ord}\left(T\right)$. We hope to address this question in future work.

Lastly, one might ask [ECo1]:

Question IV.2.11. *Can* $\left|D^2 - 1\right|$ *be explicitly bounded in terms of the rank?*

Remark IV.2.12. This question can be reduced to the problem of finding a shortest vector as follows.

Fix the rank r and $N = \operatorname{ord}\left(T\right)$. Then defining $\mathcal{S}$ to be the infinite places of $\mathbb{Q}\left(\zeta_N\right)$ together with the finite places dividing N, one can determine a fundamental system of $\mathcal{S}$-units $\epsilon_1, \ldots, \epsilon_{s-1}$ where $s - 1 = \#\mathcal{S}$. Since D^2 is a $\mathcal{S}$-unit, there exist integers a_j such that $D^2 = \epsilon_1^{s_1} \cdots \epsilon_{s-1}^{a_{s-1}}$. One can then define an embedding $\operatorname{Log}_{\mathcal{S}} : \mathbb{K} \to \mathbb{R}^s$ by

$$\operatorname{Log}_{\mathcal{S}}\left(a\right) = \left(\log\left|\alpha\right|_v \mid v \in \mathcal{S}\right)$$

Then $\operatorname{Log}_{\mathcal{S}}\left(\mathcal{O}_{\mathbb{K},\mathcal{S}}^{\times}\right)$ is a lattice in the hyperplane $\left\{x \in \mathbb{R}^s \mid \sum_{j=1}^{s} x_j = 0\right\}$. A shortest vector in this lattice could, in principle, be used to determine a bound on $\left|D^2 - 1\right|$.

While the general shortest vector problem is NP-hard, it may be that the extra structure of the $\mathcal{S}$-units and the cyclotomic field $\mathbb{Q}\left(\zeta_N\right)$ can be brought to bear to make this approach viable.

CHAPTER V
CLASSIFICATION

Theorem IV.2.4 indicates that the classification problem for modular categories is computationally feasible. In light of this, one might attempt to classify modular categories with computer aid. This approach has been explored even prior to Theorem IV.2.4 and in fact, such classification lent a great deal of credence to Wang's Conjecture. Prior to the proof of Theorem IV.2.4, the rank finiteness result was known for integral modular categories and as such a great deal of work went into the classification of these categories. In the integral setting, it has long been known that the number of solutions to the dimension equation is bounded by a doubly exponential sequence known as Sylvester's sequence [BR1]. While quickly growing, this sequence suggests a much lower bound on the number of modular categories in terms of rank than Proposition IV.2.7, and so one might hope that the techniques present in the integral classification may lead to faster techniques in the non-integral setting. In this chapter, we will consider the classification problem for rank at most 7 integral modular categories and rank 6 weakly integral categories. This work illustrates how the number theoretic results presented in Section III.3 can be practically applied. This further suggests that a more delicate analysis of the arithmetic properties of modular categories *viz.* the rank finiteness may lead to an improved algorithm for classification.

In Section V.1, integral classification techniques will be reviewed and applied to classify integral modular categories through rank 6 and partially through rank 11. In Section V.2, the lessons learned in Section III.3 will be applied to provide faster algorithms for classification in the integral setting. This approach is a modification of the one utilized in Section V.1, but extends to the weakly integral setting. These new techniques will be applied to produce a classification of integral modular categories in rank 7 and weakly integral modular categories in rank 6.

V.1 Integral Modular Categories

In this section, the classification techniques for integral modular categories presented in [BR1] will be reviewed. These techniques are relatively straightforward and at their core is a method for determining Egyptian fractions for 1 through bounds dating to the early 1900's [Cu1].

Throughout this section, $\mathcal{C}$ will denote an integral modular category of rank r with categorical dimensions $d_1, \dots, d_r$ ordered in a weakly decreasing fashion with $d_r = \dim(\mathbb{I}) = 1$.[1] Due to the integrality of $\mathcal{C}$ and [EG1, Lemma 1.2], it can be deduced that $D^2/d_a^2 := x_a$ are rational integers

[1] Many of the arguments for the bounds in this section come down to counting and re-indexing in this fashion helps to reduce "fence-post errors".

generating an Egyptian fraction exansion for 1:

$$1 = \sum_{a=1}^{r} \frac{1}{x_a} \tag{V.1}$$

This equation appears in plane tilings and electric circuit calculations and goes under the moniker *Kellogg's Equation*, as its study was documented in 1921 by Kellogg. The work of Kellogg was taken up in 1922 by Curtiss [Cu1] who showed that the x_a can be bounded. In particular, if the results of [Cu1] and [L1] are combined, then under the ordering $x_a \leq x_{a+1}$ and $x_{r-1} = D^2$, it can be shown that the x_a are bounded by:

$$a \leq x_a \leq u_a\,(r-a+1) \quad \text{for all} \quad 1 \leq a \leq r$$

where $u_1 := 1$ and $u_k = u_{k-1}\,(u_{k-1}+1)$. These u_k form a doubly exponential sequence known as **Sylvester's sequence**, which is cataloged at [OEIS]. These bounds can be utilized to determine the possible dimensions of integral modular categories of fixed rank. The naive search algorithm can be further improved by noting that $x_r/x_a = d_a^2$ is a perfect square in $\mathbb{Z}$. This gives rise to the following algorithm for determining x_a [BR1, Algorithm 4.1].

Algorithm V.1.1.

(1) Form the set of pairs $S_2 := \{(x, x \cdot y^2) : 2 \leq x \leq r, 1 \leq y \leq \sqrt{u_r/x}\}$. These are the possible pairs (x_1, x_n).

(2) Having determined S_k for some $2 \leq k \leq r-2$, determine the set S_{k+1} of $(k+1)$-tuples $(j_1, \ldots, j_{k-1}, J, j_k)$ such that

  (a) $(j_1, \ldots, j_k) \in S_k$,

  (b) $\max(j_{k-1}, k) \leq J \leq \min(j_k, u_k(r-k+1))$,

  (c) $\sqrt{j_k/J} \in \mathbb{Z}$ and

  (d) $\frac{1}{J} + \sum_{i=1}^{k} \frac{1}{x_i} \leq 1$.

(3) The solution set S_r is the set of r-tuples $(j_1, \ldots, j_{r-2}, J, j_{r-1})$ where

  (a) $(j_1, \ldots, j_{r-1}) \in S_{r-1}$,

  (b) $\max(j_{r-2}, r-1) \leq J \leq \min(j_{r-1}, 2u_{r-1})$,

  (c) $\sqrt{j_{r-1}/J} \in \mathbb{Z}$ and

  (d) $\frac{1}{J} + \sum_{a=1}^{r-1} \frac{1}{x_a} = 1$.

For $r = 5$ and $r = 6$, the only solutions are respectively given by:

$$\{(5,5,5,5,5), (2,8,8,8,8)\} \quad \text{and} \quad \{(6,6,6,6,6,6), (3,3,12,12,12,12), (4,4,4,9,9,36)\}$$

These tuples can be analyzed leading to [BR1]:

Theorem V.1.2. *Any integral modular category of rank at most 6 is pointed.*

In rank 7, the bounds are quite large and cannot be overcome on a basic desktop. In Section V.2 this burden will be lessened through the use of number theoretic techniques. However, before discussing these techniques, it is illuminating to examine alternative conditions that can be applied to the category to lessen the bounds on the dimensions.

In order to improve the bounds, one might ask that the category be **maximally non-self dual** (MNSD). A modular category is said to be MNSD if the only self-dual simple object is the trivial object. In particular, MNSD categories only exist in odd rank, $r = 2k + 1$. Since $\dim(X) = \dim(X^*)$, the MNSD condition nearly halves the number of variables in the dimension equation. Indeed, reordering the x_a as defined above, one sees that Kellogg's equation is replaced by:

$$1 = \sum_{a=1}^{k} \frac{2}{x_a} + \frac{1}{x_r} \tag{V.2}$$

While the MNSD condition will clearly reduce the bounds on the x_a, one might wonder how stringent this condition is. In fact, maximal non-self duality is quite a general condition as is seen by [BR1]:

Proposition V.1.3. *Let $\mathcal{C}$ be a modular category of rank r. Then the following are equivalent:*

(i) *$\mathcal{C}$ is maximally non-self dual.*

(ii) $\mathrm{FPdim}(\mathcal{C})$ *is odd and, in particular, an integer.*

(iii) *$\mathcal{C}$ is (monoidally) equivalent to* $\mathrm{Rep}(A)$*, where A is an odd-dimensional semisimple quasi-Hopf algebra.*

Proof. This follows immediately from [HR1, Theorem 2.2], [NS2, Corollary 8.2(ii)], and [DGNO1, Corollary 2.33]. □

Modified versions of Kellogg's equation, such as equation (V.2), were studied in 1921 by Takenouchi [Ta1]. In this paper, Takenouchi provided bounds on the x_a which can be utilized as above to produce a linear improvement to Algorithm V.1.1. In particular, the bounds can be used to show [BR1, Lemma 4.4]:

Lemma V.1.4. *Suppose that $\mathcal{C}$ is an integral modular category of rank r and there exist k integers $p_1 \geq p_2 \geq \cdots \geq p_k$ such that the non-trivial (isomorphism classes of) simple objects can be* *partitioned into k sets $P_1, \ldots, P_k$ such that $X \in P_j$ has $\dim(X) = p_j$, and $|P_j| = \ell$ for all $1 \leq j \leq k$. Then:*

(i) the numbers $x_j := \frac{D^2}{p_j^2}$ for a weakly increasing sequence of integers such that $\sum_{j=1}^{k} \frac{\ell}{x_j} + \frac{1}{x_{k+1}} = 1$, and

(ii) $\ell j \leq x_j \leq (r + \ell - j\ell) \frac{A_j}{\ell}$ for $j \leq k$ and $(k+1) \leq x_{k+1} \leq \frac{A_{k+1}}{\ell}$ where $A_1 := \ell$ and $A_j = A_{j-1}(A_{j-1} + 1)$.

This linear improvement of $r \rightarrow\approx r/\ell$ variables can be applied to coerce a desktop computer into executing Algorithm V.1.1 for rank ≤ 11 for MNSD categories. However, the bounds of Lemma V.1.4 remain doubly exponential and it was found that rank 13 exhausted the memory of typical computers. Nonetheless, in [BR1] we found that:

Theorem V.1.5. *All maximally non-self dual modular categories of rank at most 11 are pointed.*

Remark V.1.6. If G is a finite group of odd order and ω is a 3-cocycle $Z^3(G, \mathbb{C}^\times)$, then it can be shown that $\operatorname{Rep}(D^\omega(G))$ is a maximally non-self dual modular category by Proposition V.1.3 and the constructions of Section II.7. Furthermore, direct search in GAP reveals that the smallest (rank) example of a non-pointed MNSD category of this form is in rank 25 and dimension 441, namely $\operatorname{Rep}(D(\mathbb{Z}/3\mathbb{Z} \ltimes \mathbb{Z}/7\mathbb{Z}))$. This has prompted speculation that this is the smallest non-pointed MNSD modular category.

V.2 Rank 6 Weakly Integral and Rank 7 Integral Modular Categories

In this section, rank 6 weakly integral modular categories and rank 7 integral modular categories will be classified up to Grothendieck equivalence. This is demonstrative of the utility of the number theory techniques discussed in Section III.3 and it is reasonable to believe that the calculations can be extended to produce a classification in higher degree.

The analysis of the weakly-integral and integral modular categories differ very slightly, and the setup in both cases is essentially identical. In either case, Proposition II.5.5 can be applied to the FP-dimension equation to produce the Diophantine system:

$$1 = \sum_{a=1}^{r} \frac{1}{x_a}, \quad x_a \leq x_{a+1} \tag{V.3}$$

where the x_a are related to the dimensions by $\frac{d_a^2}{D^2}$, re-indexed to produce the weakly increasing condition on the x_a.[2]

This Egyptian fraction for 1 was considered in the previous section, where the results of [Cu1] were used to produce the bounds:

$$j \leq x_j \leq (r - j + 1) u_j, \quad u_1 := 1, \quad u_{j+1} := u_j (u_j + 1) \tag{V.4}$$

[2] We retain the indexing from 1 rather than 0 from the previous section for consistency.

As previously discussed, this, in principle, gives a means to solve equation (V.3) through direct computation. However, the double exponential growth of the u_j overwhelms most personal computers for $r \geq 6$. Due to exponential growth, a further stratification is required.

The idea is to stratify by the isomorphism class of $\operatorname{Gal}(\mathcal{C})$. As was discussed in Section III.1, $\operatorname{Gal}(\mathcal{C})$ is an abelian subgroup of $\mathfrak{S}_r$, and, in the integral setting, it must fix 0 by Proposition III.1.4. However, due to our reindexing and reordering of dimensions as in equation (V.3), we should assume that $\mathfrak{S}_r$ permutes $\{1, 2, \ldots, r\}$ and that, in the integral setting, $\operatorname{Gal}(\mathcal{C})$ fixes 7 in $\mathfrak{S}_7$. Thus for the purposes of this section, it suffices to consider abelian subgroups of $\mathfrak{S}_6$. In particular, $\operatorname{Gal}(\mathcal{C})$ belongs to one of the following isomorphism classes:

$$1,\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/7\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/3\mathbb{Z})^2,\ (\mathbb{Z}/2\mathbb{Z})^3$$

In each of these cases, the prime divisors of $\operatorname{ord}(T)$ are essentially fixed *viz.* Propositions III.3.13, III.3.17, III.3.18, and Corollary III.3.7. Coupling these primality conditions with the divisibility results of Proposition II.5.5 and Theorem IV.0.27 shows that the prime divisors of the x_a must also divide $\operatorname{ord}(T)$.

For many of these Galois groups, the number of free parameters in equation (V.3) can be reduced through the following lemma.

Lemma V.2.1. *If $\mathcal{C}$ is a weakly integral modular category and $\sigma \in \operatorname{Gal}(\mathcal{C})$, then $d_{\sigma(a)} = \pm d_a$ for all a.*

Proof. Since $\mathcal{C}$ is weakly integral, there exists $m_a \in \mathbb{N}$ such that $d_a = \sqrt{m_a}$ [ENO1, Proposition 8.27]. Furthermore, $d_{\sigma(0)}$ is a unit in $\mathbb{Q}(S)$ for all $\sigma \in \operatorname{Gal}(\mathcal{C})$ by Proposition III.1.5. Thus, $d_{\sigma(0)} = \pm 1$ and $\sigma(d_a) = \pm d_a$. However, Theorem III.1.3 implies that $\sigma(d_a) = \frac{\pm d_{\sigma(a)}}{d_{\sigma(0)}}$ and hence $d_{\sigma(a)} = \pm d_a$. □

The restriction on the prime divisors of the x_a and the reduction in the number of variables in equation (V.3) due to Lemma V.2.1 makes the integral rank 7 and weakly integral rank 6 cases tractable allowing us to show:

Theorem V.2.2. *If $\mathcal{C}$ is an integral rank 7 modular category, then $\mathcal{C}$ is pointed.*

Theorem V.2.3. *If $\mathcal{C}$ is a weakly integral rank 6 modular category, then it is pointed or Grothendieck equivalent to* $\mathrm{SO}(5)_2$ *or* $\mathrm{Sem} \boxtimes \mathrm{Ising}$.

Corollary V.2.4. $\operatorname{Rep}(D(\mathfrak{S}_3))$ *is the smallest non-pointed integral modular category (rank 8).*

Proof. Apply Theorem V.2.2 and Theorem V.1.2 to conclude that there are no non-pointed integral modular categories of rank ≤ 7. The result then follows by examining $D(\mathfrak{S}_3)$ *viz.* Section II.7 and GAP. □

V.2.1 Rank 7 Integral Modular Categories

In this section, Proposition II.5.5 implies that the condition $\sqrt{\frac{x_7}{x_j}} \in \mathbb{Z}$ should be imposed on equation (V.3) to produce the Diophantine system:

$$1 = \sum_{j=1}^{7} \frac{1}{x_j}, \quad x_j \leq x_{j+1}, \quad \sqrt{\frac{x_7}{x_j}} \in \mathbb{Z} \tag{V.5}$$

Further note that if D^2 is odd, then $\mathcal{C}$ is maximally non-self dual by Proposition V.1.3 and hence is covered by Theorem V.1.5. Thus in this section, D^2, and hence x_7, will be taken to be even. The proof of Theorem V.2.2 now proceeds by examining the possible isomorphism classes of $\mathrm{Gal}\left(\mathcal{C}\right)$.

Lemma V.2.5. *There are no rank 7 integral modular categories* $\mathcal{C}$ *with* $\mathrm{Gal}\left(\mathcal{C}\right) \cong \left(\mathbb{Z}/3\mathbb{Z}\right)^2$.

Proof. In this setting, Lemma V.2.1 reduces the system V.5 to

$$1 = \frac{3}{x_1} + \frac{3}{x_2} + \frac{1}{x_3}, \quad x_j \leq x_{j+1}, \quad \sqrt{\frac{x_3}{x_j}} \in \mathbb{Z} \tag{V.6}$$

This revised Diophantine system is subject to the bounds produced by Lemma V.1.4:

$$3 \leq x_1 \leq 7, \quad 6 \leq x_2 \leq 8, \quad 3 \leq x_3 \leq 10 \tag{V.7}$$

However, the prime divisors of x_j are in the set $\{2,\ 3,\ 7\}$ by part (ii) of Corollary III.3.7. Of course, Theorem III.1.3 implies that $\sqrt{x_3} \in \mathbb{Q}\left(S\right)$ and hence x_3 is a perfect square,[3] in particular, $x_3 = 4$ or 9. Finally, applying Proposition II.5.5, one sees that there exist $a_j, b_j \in \mathbb{N}$ such that $x_j = 2^{2a_j}3^{2b_j}$. Given the bounds V.7 and the condition $x_j \leq x_{j+1}$, we can conclude that $a_1 = a_2 = a_3 = 1$, which violates equation (V.6). □

Lemma V.2.6. *There are no rank 7 integral modular categories satisfying* $\mathrm{Gal}\left(\mathcal{C}\right) \cong \mathbb{Z}/5\mathbb{Z}$.

Proof. In this case, Lemma V.2.1 reduces the Diophantine system V.5 to:

$$1 = \frac{5}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}, \quad x_3 \geq \max\left(x_1, x_2\right), \quad \sqrt{x_3/x_j} \in \mathbb{Z}$$

Once again, Theorem III.1.3 shows that $\sqrt{x_3} \in \mathbb{Q}\left(S\right)$ and hence x_3 is a perfect square. Proposition II.5.5 then implies that x_j is a perfect square for all j.

On the other hand, Lemma V.1.4 may be applied to the system V.5 to produce the bounds $5 \leq x_1 \leq 7$ or $6 \leq x_1 \leq 12$ and $1 \leq x_2 \leq 7$. Coupling this with Proposition III.3.13 shows that x_1 and x_2 have prime divisors are in the set $\{2,\ 3,\ 11\}$. Therefore, $x_1 = 6, 8, 9, 11$. The condition that x_1 is a perfect square implies that $x_1 = 9$ and $x_2 = 4$. This contradicts the integrality of x_3. □

[3] This follows from the fact that $[\mathbb{Q}\left(S\right) : \mathbb{Q}]$ is odd.

Lemma V.2.7. *If $\mathcal{C}$ is a rank 7 integral modular category with* $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}/6\mathbb{Z}$*, then $\mathcal{C}$ is pointed.*

Proof. Here there are two possibilities for the cycle structure of $\mathrm{Gal}(\mathcal{C})$:

$$\langle(1\ 2\ 3\ 4\ 5\ 6)\rangle \quad \text{and} \quad \langle(1\ 2)\,(3\ 4\ 5)\rangle.$$

The first possibility when coupled with Lemma V.2.1 and Lemma V.1.4 leads to the solution $x_j = 7$ and hence $\mathcal{C}$ is pointed. In the second case, Lemma V.2.1 reduces the Diophantine equation V.3 to:

$$1 = \frac{6}{3x_1} + \frac{6}{2x_2} + \frac{6}{6x_3} + \frac{1}{x_4}$$

When rewriting the Diophantine system in this setting, there is no way to ensure that $x_1 \leq x_2 \leq x_3$, only that $x_4 \geq x_j$ for all j. However, this problem can be rectified by defining y_j such that $y_j \leq y_{j+1}$ by $\{y_1, y_2, y_3\} = \{3x_1, 2x_2, 6x_3\}$. This allows Lemma V.1.4 to be applied leading to the bounds:

$$6 \leq 3x_1, 2x_2, 6x_3 \leq 1806, \quad 4 \leq x_4 \leq 543907 \tag{V.8}$$

Proposition III.3.18 says that $x_j = 2^{a_j}3^{b_j}5^{c_j}7^{f_j}$, while equation (V.8) gives bounds on the a_j, b_j, c_j, and f_j. The case that x_4 is odd and hence $\mathcal{C}$ is maximally non-self dual was considered in [BR1]. So we can iterate through the possible values of x_j and retain only solutions satisfying $2 \mid x_4$ and $\sqrt{x_4/x_j} \in \mathbb{Z}$. This leads to the two possible dimension lists:

$$(d_a \mid 1 \leq j \leq 7) = (1, 2, 2, 3, 3, 3, 6) \quad \text{or} \quad (1, 1, 1, 1, 2, 2, 2)$$

The first possibility would give $D^2 = 72 = 2^3 3^2$ and hence violate [ENO2, Proposition 8.2] as it contains only a single invertible object. The second possibility leads to $D^2 = 16$ and hence $\mathrm{ord}(T)$ a power of 2 by Theorem IV.0.27. The Chinese Remainder Theorem then implies that $(\mathbb{Z}/\mathrm{ord}(T)\,\mathbb{Z})^\times$ is a group whose exponent is a power of 2 and thus lacks a quotient isomorphic to $\mathbb{Z}/6\mathbb{Z}$. □

Lemma V.2.8. *There are no rank 7 integral modular categories, $\mathcal{C}$, such that $|\mathrm{Gal}(\mathcal{C})| = 2^k$ for some $k \in \mathbb{N}$ or $|\mathrm{Gal}(\mathcal{C})| = 3$.*

Proof. If $|\mathrm{Gal}(\mathcal{C})| = 2^k$ for some k, then the condition that $\mathrm{Gal}(\mathcal{C})$ is an abelian subgroup of $\mathfrak{S}_6$ implies that $k = 0, 1, 2, 3$. Thus, Proposition III.3.17 allow us to conclude that the prime divisors of x_j are in the set $\{2,\ 3,\ 5,\ 17\}$. In particular, the pointed case ($x_j = 7$) cannot occur.

If $k = 3$, then Lemma V.2.1 forces the Diophantine system V.5 to be the one studied in Theorem V.1.5. There, the only solution was found to be $x_j = 7$, the pointed solution, contradicting the above observation.

So it remains to consider $k = 0, 1, 2$ and $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}/3\mathbb{Z}$. In these cases, Proposition III.3.17 and part (ii) of Corollary III.3.7 show that the prime divisors of the x_j are in the set $\{2,\ 3,\ 5\}$.

Consequently, $x_j = 2^{a_j}3^{b_j}5^{c_j}$ for some a_j, b_j, and c_j. The bounds V.4 can then be applied to produce relatively small bounds on the a_j, b_j and c_j. Finally, the condition $\sqrt{x_7/x_j} \in \mathbb{Z}$ manifests itself as:

$$2 \mid (a_7 - a_j)\,, \quad 2 \mid (b_7 - b_j)\,, \quad \text{and} \quad 2 \mid (c_7 - c_j)$$

Iterating through the possibilities reveals that there is no solution. □

The case that $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}/7\mathbb{Z}$ may be omitted by Proposition III.3.13 and thus Theorem V.2.2 follows.

V.2.2 Rank 6 Weakly Integral Modular Categories

In this setting, Proposition II.5.5 implies that the condition $\frac{x_6}{x_j} \in \mathbb{Z}$ should be imposed on equation (V.3) to produce the Diophantine system:

$$1 = \sum_{j=1}^{6} \frac{1}{x_j}, \quad x_j \leq x_{j+1}, \quad \sqrt{\frac{x_6}{x_j}} \in \mathbb{Z} \tag{V.9}$$

Further note that if D^2 is odd, then $\mathcal{C}$ is maximally non-self dual by Proposition V.1.3 and hence is covered by Theorem V.1.5. Thus, it will be assumed that D^2, and hence x_6, is even.

Just as in the integral case, the analysis now splits based on the isomorphism class of $\mathrm{Gal}(\mathcal{C})$. However, the integral cases were considered in Section V.1, and so only solutions which are non-integral need to be considered. In particular, we may assume that $\mathbb{Q}(S)$ has a degree 2 subfield and thus $\mathrm{Gal}(\mathcal{C})$ has even order.

Lemma V.2.9. *If $\mathcal{C}$ is a rank 6 weakly integral modular category satisfying $\mathrm{Gal}(\mathcal{C}) \cong \mathbb{Z}/6\mathbb{Z}$, then it is integral.*

Proof. Here, there are two possible cycle structures for $\mathrm{Gal}(\mathcal{C})$, they are

$$\langle (1\ 2\ 3\ 4\ 5\ 6) \rangle \quad \text{and} \quad \langle (1\ 2)\,(3\ 4\ 5) \rangle.$$

The 6-cycle leads to a pointed solution and so it suffices to consider the equation:

$$\frac{1}{6} = \frac{1}{3x_1} + \frac{1}{2x_2} + \frac{1}{6x_3}$$

with no imposed order on the x_j. Defining y_j to be integers such that $y_j \leq y_{j+1}$ and $\{y_j\} = \{x_j\}$ and then applying [Ta1] and [L1] as in Lemma V.1.4 produces the bounds:

$$7 \leq y_1 \leq 18, \quad 7 \leq y_2 \leq 84, \quad 7 \leq y_3 \leq 1806$$

Coupling Theorem IV.0.27 with Proposition III.3.18 reveals that the x_j have prime divisors are in the set $\{2,\ 3,\ 5,\ 7\}$. Enumerating this small list of numbers, we find that there are only 18 solutions to the Diophantine system V.9. However, the condition that $[\mathbb{Q}(d_a \mid 1 \leq a \leq 6) : \mathbb{Q}] = 2$ and the required $\mathbb{Z}/2\mathbb{Z}$-grading described in [GN2, Theorem 3.10] eliminate most of the cases leaving only the following possibilities for (d_a):

$$\left(1,1,1,3,2\sqrt{3},2\sqrt{3}\right), \quad \left(1,1,2,2,2,\sqrt{14}\right), \quad \left(1,1,2,\sqrt{2},\sqrt{2},\sqrt{2}\right), \quad \left(1,1,1,3,\sqrt{3},\sqrt{3}\right),$$
$$\left(1,1,1,1,1,\sqrt{5}\right), \quad \left(1,1,1,1,\sqrt{2},\sqrt{2}\right), \quad \left(1,1,2,\sqrt{6},\sqrt{6},\sqrt{6}\right), \quad \text{and} \quad \left(1,1,2,2,2,\sqrt{2}\right).$$

The first, fourth, fifth, and seventh cases can be excluded by examining the universal grading [DGNO1, Proposition 2.3]. In cases three and eight, we can conclude that there is an Ising subcategory by [DGNO1, Corollary B.12]. Consequently, [M4, Theorem 4.2 and Corollary 3.5] imply that the category would be expressible as a Deligne product of modular categories, one of which is the Ising category, a contradiction.

This leaves $\left(1,1,2,2,2,\sqrt{14}\right)$ and $\left(1,1,1,1,\sqrt{2},\sqrt{2}\right)$. In the first case, the fusion rules can be determined and the S-matrix recovered in terms of the T-matrix through the balancing equation II.16. The fusion rules reveal that the category would be self-dual and hence the S-matrix is real. This fact fixes all but one of the twists. The remaining twist must have order dividing 5040 by Proposition III.3.18 which contradicts $S^2 = D^2 C$. □

Lemma V.2.10. *If $\mathcal{C}$ is a rank 6 weakly integral modular category with $|\mathrm{Gal}(\mathcal{C})| = 8$, then $\mathcal{C}$ has dimensions $(d_a) = \left(1,1,2,2,\sqrt{5},\sqrt{5}\right)$ or $\left(1,1,1,1,\sqrt{2},\sqrt{2}\right)$.*

Proof. Since $|\mathrm{Gal}(\mathcal{C})| = 8$, equation (V.9) can be reduced to:

$$\frac{1}{2} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}, \quad x_j \leq x_{j+1}, \quad x_j \mid x_3 \tag{V.10}$$

The analysis of [Ta1] and [L1], as in Lemma V.1.4, can be applied to produce the bounds:

$$2 \leq x_1 \leq 6, \quad 3 \leq x_2 \leq 12, \quad 4 \leq x_3 \leq 42$$

Corollary III.3.17 implies that the prime divisors of the x_j are in the set $\{2,\ 3,\ 5,\ 17\}$. Enumerating the possible values of x_j reveals that there are 6 possibilities which satisfy equation (V.10). However, only two of them can be equi-dimensionally graded such that the trivial component is an integral category given by $\mathcal{C}_{\mathrm{ad}}$ [DGNO1, Proposition 2.3][ENO1, Proposition 8.27]. The result then follows. □

Lemma V.2.11. *If $\mathcal{C}$ is a rank 6 weakly integral modular category with $|\mathrm{Gal}(\mathcal{C})| = 2$, or 4, then $\mathcal{C}$ has dimensions $(d_a) = \left(1,1,2,2,\sqrt{5},\sqrt{5}\right)$ or $\left(1,1,1,1,\sqrt{2},\sqrt{2}\right)$.*

Proof. Here, equation (V.9) must be studied without modification. The bounds V.4 can be computed and coupled with the factorization $x_j = 2^{a_j}3^{b_j}5^{c_j}$ provided by Corollary III.3.17, Proposition II.5.5, and Theorem IV.0.27. The resulting list of tuples (x_j) is relatively small and can be iterated over leading to 953 solutions to equation (V.9).

However, we know that at least two numbers must agree for the solution to be valid by Lemma V.2.1. Further imposing the equi-dimensionality of the universal grading given by [DGNO1, Proposition 2.3], and the fact that the trivial component is $\mathcal{C}_{\text{ad}}$ which is integral by [ENO1, Proposition 8.27] reveals three possibilities.

$$(d_a) = \left(1,1,2,\sqrt{2},\sqrt{2},\sqrt{2}\right), \quad \left(1,1,2,2,\sqrt{5},\sqrt{5}\right), \quad \text{or} \quad \left(1,1,1,1,\sqrt{2},\sqrt{2}\right)$$

The first case must have a non-degenerate Ising subcategory by [DGNO1, Corollary B.12], and so by [M4, Theorem 4.2 and Corollary 3.5], we know that the category would arise as a Deligne product with one factor being an Ising category. This is an impossibility and so the result follows. □

It now remains to identify categories with dimension tuples $\left(1,1,2,2,\sqrt{5},\sqrt{5}\right)$ and $\left(1,1,1,1,\sqrt{2},\sqrt{2}\right)$ up to Grothendieck equivalence.

Lemma V.2.12. *If $\mathcal{C}$ is a weakly integral rank 6 modular category with dimension $\left(1,1,1,1,\sqrt{2},\sqrt{2}\right)$, then it is Grothendieck equivalent to* $\text{Sem} \boxtimes \text{Ising}$.

Proof. It follows from [DGNO1, Proposition 2.3] that the category is universally graded by $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the second case, the objects of dimension $\sqrt{2}$ are self-dual and so by [DGNO1, Corollary B.12] and [M4, Theorem 4.2 and Corollary 3.5], we can conclude that $\mathcal{C}$ is Grothendieck equivalent to $\text{Sem} \boxtimes \text{Ising}$. Thus it remains to consider the case that $\mathcal{C}$ is $\mathbb{Z}/4\mathbb{Z}$ graded.

In this case, the trivial component contains two objects of dimension 2 while components $\mathcal{C}_1$ and $\mathcal{C}_3$ each contain an object of dimension $\sqrt{2}$ and the component $\mathcal{C}_2$ contains two invertible objects. The invertible objects may be labeled by 1, Z_1, Z_2, Z_3 and ordered such that: Z_1 tensor generates $\mathcal{C}_{\text{pt}}$, the trivial component contains 1 and Z_2, and the the component $\mathcal{C}_2$ contains Z_1 and Z_3. Denoting the dimension $\sqrt{2}$ objects by X_1 and X_2, we can determine the fusion rules: $X_1 \otimes X_2 = 1 \oplus Z_2$, and $X_1 \otimes X_1 = X_2 \otimes X_2 = Z_1 \oplus Z_3$ The S-matrix can be computed from theses fusion rules in terms of the T=matrix via equation (II.16). The condition that the resulting matrix be symmetric leads to the condition $\theta_{Z_1} = \theta_{Z_3}$, while [GN2, Lemma 6.1] implies that $\theta_1, \theta_2 = \pm 1$. Computing the $(0,1)$ entry of $S^2 = D^2C$ leads to the equation: $0 = 1 + \theta_1^2 + 4\theta_1 + 2\theta_2$, which implies $\theta_1 = -1$ and $\theta_2 = 1$. However, such twists lead to a degenerate S-matrix. □

Lemma V.2.13. *If $\mathcal{C}$ is a rank 6 weakly integral modular category with dimensions $\left(1,1,2,2,\sqrt{5},\sqrt{5}\right)$, then it is Grothendieck equivalent to* $\text{SO}(5)_2$.

Proof. Just as in the previous lemma, [DGNO1, Proposition 2.3] implies that $\mathcal{C}$ is universally graded by $\mathbb{Z}/2\mathbb{Z}$. Furthermore, [ENO1, Proposition 8.27] implies that the trivial component is integral and given by $\mathcal{C}_{\text{ad}}$. In particular, $\mathcal{C}_{\text{ad}}$ is an integral rank 4 premodular category with objects of dimensions

$(1, 1, 2, 2)$. Such categories are studied in Section VI.2 and it is found in Propositions VI.2.10 and VI.2.1 that $\mathcal{C}_{\text{ad}}$ is Grothendieck equivalent to $(\mathrm{SO}(5))_{ad}$.[4] In fact, the twists and the portion of the S-matrix corresponding to $\mathcal{C}_{ad}$ can be recovered from Proposition VI.2.10 by noting that, in this case, $\mathcal{C}_{\text{ad}}$ cannot be symmetric if the S-matrix of $\mathcal{C}$ is to be invertible. So it remains to determine fusion rules for the two objects of dimension $\sqrt{5}$. To facilitate this process, the invertible objects will be denoted by 1 and Z, the self-dual dimension 2 objects denoted by X_1 and X_2, and the dimension $\sqrt{5}$ objects given by Y_1 and Y_2. To determine the fusion rules involving the Y_j, the two duality cases will be taken in turn.

Case 1 $Y_j = Y_j^*$: Coupling the fusion rules of $\mathcal{C}_{\text{ad}}$ from Proposition VI.2.10 with the complete symmetry of the symbol $N_{i,j}^k$ due to self-duality allows for the fusion rules to be greatly simplified. Dimension count then produces the relations: $\sum\limits_k N_{Y_i,X_j}^k = 2$ and $\sum\limits_k N_{Y_i,Y_j}^k = 3$ which fix the remaining fusion coefficients. The unique fusion ring that arises is that of $\mathrm{SO}(5)_2$ [GK1].

Case 2 $Y_1 = Y_2^*$: Just as in the previous case, dimension count coupled with the fusion symmetries II.13, and the fusion ring of $\mathcal{C}_{\text{ad}}$ allows us to exactly determine the fusion ring of $\mathcal{C}$. An application of the balancing relation (II.16) then determines the S-matrix in terms of the T-matrix. It follows from Proposition VI.2.10 that θ_1, θ_Z, θ_{X_1}, and θ_{X_2} are fixed up to a primitive 5-th root of unity. Coupling [GN1, Lemma 6.1] with the relation $S^2 = D^2 C$ reveals that $\theta_{Y_1} = -\theta_{Y_2}$ is a primitive 8-th root of unity. However, this is incompatible with the relation $(ST)^3 = p^+ S^2$. □

[4] This is Grothendieck equivalent to $\mathrm{Rep}(D_{10})$ and so the fusion rules of $\mathcal{C}_{ad}$ can be recovered from finite group data.

CHAPTER VI

PREMODULAR CATEGORIES

Since their inception, there has been considerable interest in modular categories, partly owing to their applicability in mathematics, computer science, and physics. However, premodular, braided fusion, and fusion categories have received less attention than their modular brethren. This may be in part due to the difficulties inherent in studying these categories. Indeed, much of the arithmetic theory present in the modular setting is absent. For instance, it is known that if $\mathcal{C}$ is a premodular category, then:

- d_a need not reside in $\mathbb{Q}(T)$ (Ng-Schauenburg Theorem) as is evidenced by $(\mathrm{SU}(2)_6)_{\mathrm{ad}}$.
- $\mathrm{Gal}(\mathbb{Q}(s)/\mathbb{Q})$ need not act by signed permutation on s as is seen by $\mathrm{Fib} \boxtimes \mathrm{Rep}(\mathbb{Z}/2\mathbb{Z})$.
- The universal grading group need not be isomorphic to the group of isomorphism classes in $\mathcal{C}_{pt}$, as can be seen by $(\mathrm{SU}(2)_6)_{\mathrm{ad}}$.
- Examining $(\mathrm{SU}(2)_4)_{\mathrm{ad}}$ or $\mathrm{Rep}(\mathfrak{S}_3)$, we see that d_a^2 need not divide D^2.

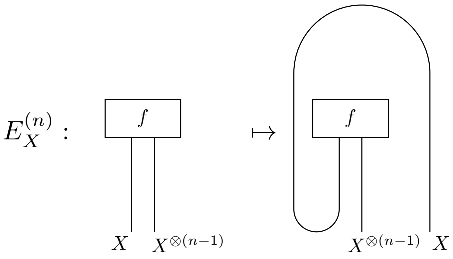
Despite these shortcomings, some work has been done. In [O2] and [O4], Ostrik studied and classified rank 2 fusion categories and rank 3 premodular categories (up to Grothendieck equivalence). In the rank 2 setting, he computed the Drinfeld center and then applied modular techniques. This approach is cumbersome and impractical in higher rank. Indeed, it is known that the rank of the Drinfeld center can grow exponentially in the rank of $\mathcal{C}$ [Eti2] and there is very little theory controlling the structure of modular datum of $\mathcal{Z}(\mathcal{C})$ strictly in terms of the modular datum of $\mathcal{C}$. In the rank 3 setting, the techniques employed by Ostrik were largely *ad hoc*, but hinted at an arithmetic structure underlying premodular categories.

In this chapter, we will discuss the classification of rank 4 premodular categories up to Grothendieck equivalence. Our approach will largely rely on *ad hoc* number theoretic analysis, modularization, and the second Frobenius-Schur indicator. In particular, an explicit formula for this indicator is found for premodular categories and its formula suggests a generalization of the Ng-Schauenburg Theorem to the premodular setting.

It should be noted that, while we obtain a classification of rank 4 premodular categories up to Grothendieck equivalence, the general rank finiteness question for premodular categories is still open. Of course, bounding the rank of $\mathcal{Z}(\mathcal{C})$ in terms of the rank of $\mathcal{C}$ would allow one to determine rank finiteness for premodular categories from Theorem IV.2.4. However, at the time of this writing such a bound is lacking in the general case.

Despite this apparent failure of modular techniques in the premodular setting, work in the field suggests that there is still a rich arithmetic structure. For instance, generalizations of the Ng-Schauenburg Theorem and Cauchy Theorem can be determined in the premodular setting. However, in order to do this one must remove the focus from the T-matrix and instead consider the so-called *Frobenius-Schur indicators.*

In classical representation theory, the second Frobenius-Schur indicator of an irreducible representation of a finite group is a number that can be computed from the character, which indicates if it is real, complex, or quaternionic. Higher indicators can also be computed and provide useful invariants of the representation. Given that fusion categories axiomatize the representation theory, it is perhaps unsurprising that the Frobenius-Schur indicators can be generalized to the context of braided fusion categories. These indicators were first studied in the context of modular categories in [Ban1], and later generalized to spherical fusion categories in [NS1; NS2]. The n^{th} indicator is defined by $\nu_n(X) := \mathrm{Tr}\left(E_X^{(n)}\right)$ where $E_X^{(n)}$ is the linear map graphically defined by:



It can be shown that there is a minimal integer number $\mathrm{FSExp}(\mathcal{C})$ called the **Frobenius-Schur exponent** of $\mathcal{C}$, defined by $d_a = \nu_{\mathrm{FSExp}(\mathcal{C})}(X_a)$ for all $X_a \in \mathrm{Irr}(\mathcal{C})$ [NS2]. In the modular setting, it is know that the Frobenius-Schur exponent coincides with the order of the T-matrix. However, in the premodular setting the Frobenius-Schur exponent seems to play a more fundamental role than $\mathrm{ord}(T)$. Indeed, while it is not true that $d_a \in \mathbb{Q}(T)$ in the premodular setting, it is known that [NS2]:

Proposition VI.0.14. *If $\mathcal{C}$ is a premodular category, then $d_a \in \mathbb{Q}\left(\zeta_{\mathrm{FSExp}(\mathcal{C})}\right)$ for all $a \in \mathrm{Irr}(\mathcal{C})$.*

Moreover, the Frobenius-Schur exponent allows one to generalize the Cauchy Theorem for Modular Categories to the spherical fusion setting.

Proposition VI.0.15. *If $\mathcal{C}$ is a spherical fusion category, then D^2 and $\mathrm{FSExp}(\mathcal{C})$ have the same prime divisors (when viewed as principal ideals) in $\mathbb{Q}\left(\zeta_{\mathrm{FSExp}(\mathcal{C})}\right)$.*

Proof. It is known that $\mathrm{FSExp}(\mathcal{C}) = \mathrm{ord}\left(T_{\mathcal{Z}(\mathcal{C})}\right)$ and $\dim \mathcal{Z}(\mathcal{C}) = \dim \mathcal{C}^2$ [NS2]. Thus, the result follows immediately from Theorem IV.0.27. □

In principle, this result can be utilized to examine rank finiteness in the premodular setting, just as in the modular setting.

Corollary VI.0.16. *Let $\mathcal{C}$ be a premodular category with Frobenius-Schur exponent N, and define $\mathcal{S} = \mathcal{S}_\infty \cup \mathcal{S}_{fin}$ where $\mathcal{S}_\infty$ are the infinite primes of $\mathbb{Q}(\zeta_N)$ and $\mathcal{S}_{fin}$ are the finite primes of $\mathbb{Q}(\zeta_N)$ which divide N. Then D^2 and the d_a are $\mathcal{S}$-units in $\mathbb{Q}(\zeta_N)$ for any simple object X_j in $\mathcal{C}$.*

Proof. Since $d_a \mid D^2$ by Proposition II.5.5, the result follows from Proposition VI.0.15. $\square$

Thus, if we can bound $\operatorname{FSExp}(\mathcal{C})$ in terms of the rank for a premodular category $\mathcal{C}$, then rank finiteness will immediately follow as in Section IV.2, that is we have:

Proposition VI.0.17. *If there is a function f such that for any rank r spherical fusion category $\mathcal{C}$ we have $\operatorname{FSExp}(\mathcal{C}) \leq f(r)$, then there are finitely many spherical fusion categories of fixed rank r.*

Proof. The proof proceeds just as in Section IV.2. $\square$

Such a bound follows immediately if one can bound the rank of $\mathcal{Z}(\mathcal{C})$ in terms of the rank of $\mathcal{C}$. Of course, $\mathcal{Z}(\mathcal{C})$ is not always the only modular category associated with a premodular category $\mathcal{C}$. Indeed, it was shown in [Brug1, Corollary 3.5] that if $\mathcal{C}'$ is integral and does not contain sVec, then $\mathcal{C}$ admits a minimal modularization (a special case of de-equivariantization). In particular, a more tractable problem than the rank finiteness for premodular categories may be the following [WalCo1]:

Question VI.0.18. *Are there finitely many modularizable premodular categories of fixed rank r (up to equivalence)?*

Given that the objects in the (de)equivariantization can be explicitly described in terms of group data and the simple objects of $\mathcal{C}$ [DGNO1], it seems reasonable that one should be able to bound the rank of the modularization of a premodular category and deduce rank finiteness. This would essentially reduce the rank finiteness question for premodular categories to the case that the category contains sVec or $\mathcal{C}' \not\subset \mathcal{C}_{\text{int}}$.

Given the vital role played by the Frobenius-Schur indicator in (pre)modular categories, an explicit formula in terms of the (pre)modular datum is highly desirable. In the next section we will consider such a formula. However, it will require understanding the braiding of the Müger center and thus will not be strictly expressible in terms of the premodular datum. Nonetheless, the formula that we derive will have important integrality consequences that can be used to complete the rank 4 classification of (pre)modular categories up to Grothendieck equivalence.

VI.1 Frobenius-Schur Indicators

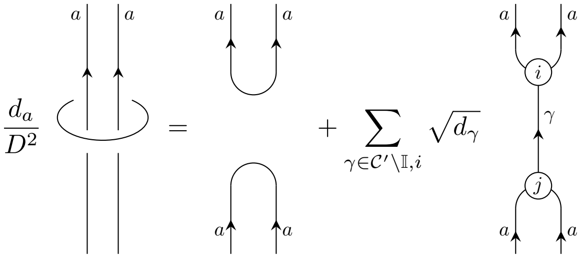
In the modular setting, the Frobenius-Schur indicators provide a powerful tool for studying and classifying categories. Indeed, these indicators were central to the proof of the Cauchy Theorem for Modular Categories and hence rank finiteness [BNRW1]. As was discussed above, the Frobenius-Schur indicators allow one to compute the Frobenius-Schur exponent for a premodular category, which in many ways is the correct generalization of $\operatorname{ord}(T)$. While these indicators are defined in the premodular setting, there is currently no explicit formula for the n-th indicator in terms of the premodular datum. In this section, we will determine the following formula for the second Frobenius-Schur indicator of a self-dual simple object in a premodular category.

$$\nu_2\left(X_a\right)=\frac{1}{D^2}\sum_{b,c}N_{b,c}^{a}d_b d_c\left(\frac{\theta_b}{\theta_c}\right)^2-\theta_a\sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I}}d_\gamma\operatorname{Tr}\left(R_\gamma^{aa}\right). \tag{VI.1}$$

This formula recovers the modular one [NS2] when the Müger center is trivial However, in the general premodular setting, it requires knowledge of the R-matrices. While this somewhat limits the direct usefulness of this formula, it can still be applied to determine integral conditions that must be satisfied by the premodular datum. In Section VI.2, this will allow us to complete the classification of rank 4 premodular categories up to Grothendieck equivalence.

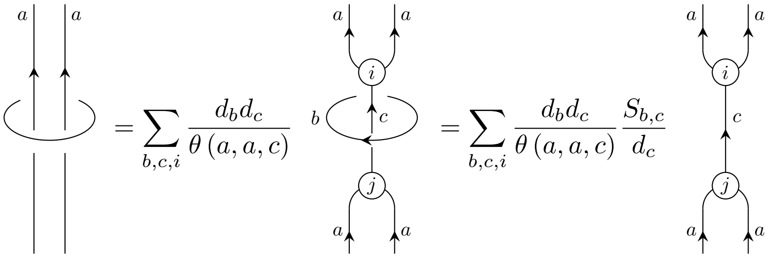
In order to derive equation (VI.1), we proceed as in the modular setting by following Ng and Schauenburg [NS2]. Inspection of their proof reveals that modularity is only utilized when invoking [BKi, Corollary 3.1.11]. However, this result of [BKi] does not completely fail in the premodular setting.

Proposition VI.1.1. *If $\mathcal{C}$ is premodular and X_a is self-dual, then*

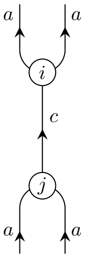

$\frac{d_a}{D^2}$
a
a
$=$
a
a
a
a
$+\sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I},i}\sqrt{d_\gamma}$
a
a
i
γ
j
a
a

where here the unlabeled circle is given by equation (II.7).

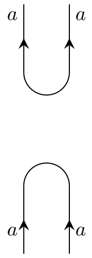
Proof. Applying equation (II.6) and [BKi, Lemma 3.1.4] we have


a
a
$=\sum_{b,c,i}\frac{d_b d_c}{\theta\left(a,a,c\right)}$
a
a
i
b
c
j
a
a
$=\sum_{b,c,i}\frac{d_b d_c}{\theta\left(a,a,c\right)}\frac{S_{b,c}}{d_c}$
a
a
i
c
j
a
a

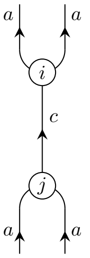
$= \sum_{c,i} \frac{\left(S^2\right)_{0,c}}{\theta\left(a,a,c\right)}$



$=$



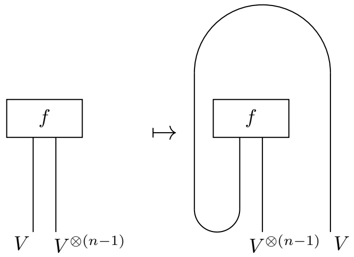
$+ \sum_{c\neq 0,i} \frac{\left(S^2\right)_{0,c}}{\theta\left(a,a,c\right)}$



Since the columns of the S-matrix are eigenvectors of the fusion matrices, we know that $\left(S^2\right)_{\gamma,0} = d_\gamma D^2$ if $X_\gamma \in \mathcal{C}'$, and 0 otherwise; this observation gives the desired result. □

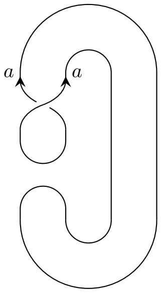
The proof of equation (VI.1) now proceeds exactly as in [NS2; W2]. Indeed, recall that the n-th Frobenius-Schur indicator is defined by $\nu_n\left(X\right) = \mathrm{Tr}\left(E_X^{(n)}\right)$, where $E_X^{(n)}$ is given by

E_X^n :



Just as in [NS2; W1], we can utilize appropriately chosen bases for our fusion and splitting spaces, e.g. II.4, so that if X_a is self-dual, its second Frobenius-Schur indicator can be graphically expressed as:

$\nu_2\left(X_a\right) = \frac{\theta_a}{d_a}$



(VI.2)

Remark VI.1.2. The factor of $\frac{1}{d_a}$ is due to a renormalization of the basis elements of $\mathrm{Hom}_{\mathcal{C}}\left(X \otimes X, \mathbb{I}\right)$ and $\mathrm{Hom}_{\mathcal{C}}\left(\mathbb{I}, X \otimes X\right)$ to have norm 1.

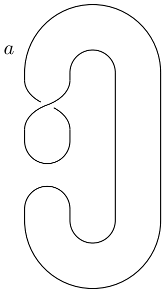
Since the second Frobenius-Schur indicator for a non-self dual object is zero [NS2], there is no loss of generality in taking $\nu_2\left(X_a\right) = 0$ for X_a non-self dual and deriving only a formula for $X_a = X_a^*$.

Theorem VI.1.3. *If $\mathcal{C}$ is a premodular category and X_a is a simple self-dual object, then*

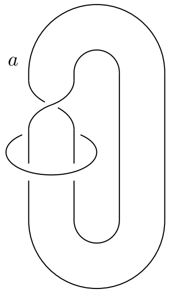
$$\nu_2\left(X_a\right) = \frac{1}{D^2}\sum_{b,c} N^a_{b,c} d_b d_c \left(\frac{\theta_b}{\theta_c}\right)^2 - \theta_a \sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I}} d_\gamma \operatorname{Tr}\left(R^{aa}_\gamma\right).$$

Proof. The proof proceeds by applying Proposition VI.1.1 to equation (VI.2) and then making use of the graphical calculus. To simplify notation, we observe that, since X_a is self-dual, the arrow on the ribbon corresponding to this object can be safely removed.

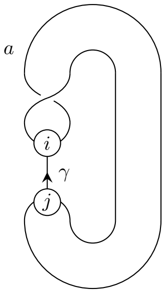
$$\nu_2\left(X_a\right) = \frac{\theta_a}{d_a}$$



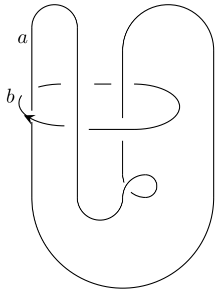
$$= \frac{\theta_a}{d_a}\frac{d_a}{D^2}$$



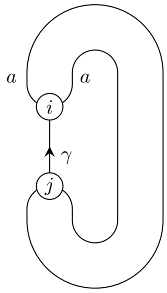
$$- \frac{\theta_a}{d_a}\sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I},i,j}\sqrt{d_\gamma}$$



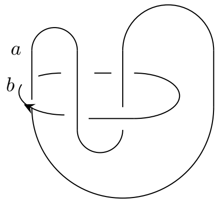
$$= \frac{\theta_a}{D^2}\sum_b d_b$$



$$- \frac{\theta_a}{d_a}\sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I},i,j}\sqrt{d_\gamma}R^{aa}_{\gamma,i}$$

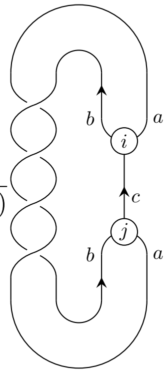


$$= \frac{\theta_a^2}{D^2}\sum_b d_b$$



$$- \frac{\theta_a}{d_a}\sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I},i,j}\sqrt{d_\gamma}R^{aa}_{\gamma,i}\theta\left(a,a,\gamma\right)\delta_{ij}$$

$$= \frac{\theta_a^2}{D^2}\sum_{b,c,i,j}\frac{d_b d_c}{\theta\left(a,b,c\right)}$$



$$- \theta_a \sum_{\gamma\in\mathcal{C}'\setminus\mathbb{I}} d_\gamma \operatorname{Tr}\left(R^{aa}_\gamma\right)$$

$$= \frac{\theta_a^2}{D^2} \sum_{b,c,i,j} \frac{d_b d_c \left(R^{ab}_{c,i} R^{ba}_{c,i}\right)^2}{\theta\left(a,b,c\right)} \theta\left(a,b,c\right) \delta_{ij} - \theta_a \sum_{\gamma \in \mathcal{C}' \setminus \mathbb{I}} d_\gamma \operatorname{Tr}\left(R^{aa}_\gamma\right)$$
$$= \frac{\theta_a^2}{D^2} \sum_{b,c,i} d_b d_c \left(R^{ab}_{c,i} R^{ba}_{c,i}\right)^2 - \theta_a \sum_{\gamma \in \mathcal{C}' \setminus \mathbb{I}} d_\gamma \operatorname{Tr}\left(R^{aa}_\gamma\right)$$

Applying equation (216) of Appendix E in [K1] and noting that $\left(S^2\right)_{\gamma,0} = d_\gamma D^2$ for $X_\gamma \in \mathcal{C}'$ gives:

$$\nu_2\left(X_a\right) = \frac{\theta_a^2}{D^2} \sum_{b,c,i} d_b d_c \left(\frac{\theta_c}{\theta_a \theta_b}\right)^2 - \theta_a \sum_{\gamma \in \mathcal{C}' \setminus \mathbb{I}} d_\gamma \operatorname{Tr}\left(R^{aa}_\gamma\right).$$

Making use of equation (II.13), we have: $N^c_{a,b} = N^c_{b,a} = N^a_{b,c^*} = N^a_{c^*,b}$. However, $\theta_{b^*} = \theta_b$ and $d_{b^*} = d_b$, so

$$\nu_2\left(X_a\right) = \frac{1}{D^2} \sum_{b,c} N^a_{b,c^*} d_b d_{c^*} \left(\frac{\theta_{c^*}}{\theta_b}\right)^2 - \theta_a \sum_{\gamma \in \mathcal{C}' \setminus \mathbb{I}} d_\gamma \operatorname{Tr}\left(R^{aa}_\gamma\right).$$

Reindexing the first sum gives the desired result. □

Since the R-matrices appear in this indicator, it is of limited computational use. However, one can show that the two sums of Theorem VI.1.3 are both rational integers. To do this, we first recall that the Müger center of $\mathcal{C}$ is a premodular subcategory of $\mathcal{C}$. In particular, its fusion rules and twists descend from $\mathcal{C}$. Moreover, $R_{W,V} \circ R_{V,W} = id_{V \otimes W}$ on $\mathcal{C}'$ by its definition. So applying [NS1, Proposition 6.1], we can deduce that if $X_\gamma \in \mathcal{C}'$, then $\theta_\gamma = \pm 1$. However, $\theta_a R^{a,a}_{c,i} = \pm\sqrt{\theta_c}$ and so, if $X_\gamma \in \mathcal{C}'$, we conclude that $\theta_a R^{a,a}_{\gamma,i} \in \{\pm 1, \pm i\}$, which leads to the following corollary.

Corollary VI.1.4. *If $\mathcal{C}$ is premodular and $X_a \in \mathcal{C}$ simple, then*

$$\frac{1}{D^2} \sum_{b,c} N^a_{b,c} d_b d_c \left(\frac{\theta_b}{\theta_c}\right)^2$$

is real and if X_a is self-dual, then it is a rational integer.

Proof. Applying [NS1], we know that $\nu_2\left(X_a\right) \in \{-1, 0, 1\}$. Coupling this observation with the afore mentioned fact that $\theta_a R^{a,a}_{\gamma,i} \in \{\pm 1, \pm i\}$ for $X_\gamma \in \mathcal{C}'$, we can conclude that for X_a self-dual:

$$\frac{1}{D^2} \sum_{b,c} N^a_{b,c} d_b d_c \left(\frac{\theta_b}{\theta_c}\right)^2 \in \mathbb{Z}\left[i\right].$$

However, $N_{b,c}^{a}=N_{c,b}^{a}$, $d_b\in\mathbb{R}$, and $\overline{\theta_b}=\theta_b^{-1}$ for all a,b,c. So for any a, we have that

$$\frac{1}{D^2}\sum_{b,c}N_{a,b}^{c}d_bd_c\left(\frac{\theta_c}{\theta_b}\right)^2$$

is invariant under complex conjugation.

Consequently, if X_a is self-dual, then $\frac{1}{D^2}\sum_{b,c}N_{b,c}^{a}d_bd_c\left(\frac{\theta_b}{\theta_c}\right)^2\in\mathbb{Z}\left[i\right]\cap\mathbb{R}=\mathbb{Z}$. □

Remark VI.1.5. In the modular setting, it is known that the second Frobenius-Schur indicator is computed by:

$$\frac{1}{D^2}\sum_{b,c}N_{b,c}^{a}d_bd_c\left(\frac{\theta_b}{\theta_c}\right)^2$$

and in particular, this value takes on values ±1 or 0 [NS2]. This corollary indicates that this fact is only mildly weaker in the premodular setting, that is say that the formula for 2nd Frobenius-Schur indicator in the modular setting still produces a rational integer in the premodular setting when a is self-dual.

Examination of Theorem VI.1.3 reveals that $R_c^{a,a}$ enters into the formula for the second indicator. Since the R-matrices involve square roots of the twists, we know that $R_c^{a,b}$ is a $2N^{\text{th}}$ root of unity where $N=\operatorname{ord}\left(T\right)$. Coupling this observation with the definition of the Frobenius-Schur exponent motivates the following conjecture.

Conjecture VI.1.6. *If $\mathcal{C}$ is premodular, X_a is a simple object and $N=\operatorname{ord}\left(T\right)$, then $d_a\in\mathbb{Z}\left[\zeta_{2N}\right]$.*

This result is reminiscent of the Ng-Schauenburg Theorem for modular categories, which tells us that for any simple object X_a, $d_a\in\mathbb{Z}\left[\zeta_N\right]$ where $N=\operatorname{ord}\left(T\right)$ [NS1]. One might wonder if this theorem holds in the premodular setting despite the appearance of the R-matrices. However, examination of the premodular category $\mathcal{C}\left(sl\left(2\right),8\right)_{a,d}$ reveals that the Ng-Schauenburg Theorem fails, but that Conjecture VI.1.6 holds. Preliminary results indicate that more complicated combinations of the R-matrices may appear in higher indicators, so more work is needed before the techniques of Ng and Schauenburg can be applied to Conjecture VI.1.6. However, this conjecture has been verified for premodular categories of rank <5. Since the Ng-Schauenburg Theorem holds in the premodular setting when $\operatorname{ord}\left(T\right)$ is replaced by $\operatorname{FSExp}\left(\mathcal{C}\right)$, one could rephrase this conjecture in the following way:

Conjecture VI.1.7. *If $\mathcal{C}$ is a premodular category, then $\operatorname{FSExp}\left(\mathcal{C}\right)=\operatorname{ord}\left(T\right)$ or $2\operatorname{ord}\left(T\right)$.*

Theoretical questions aside, the Frobenius-Schur indicators have practical importance. In particular, the integrality condition provided by Corollary VI.1.4 is a very powerful tool and in the next section, we will utilize it to complete the rank 4 classification of premodular categories up to Grothendieck equivalence.

VI.2 Classification

In this section, we will classify rank 4 premodular datum. In particular, we will determine all rank 4 premodular categories up to Grothendieck equivalence. As discussed above, many of the standard modular techniques fail in the premodular setting, most notably the Galois symmetry. However, in a premodular category which is not modular, there is necessarily a symmetric subcategory. Symmetric categories have been classified by Deligne, cf. Theorem II.4.5. Thus, we are able to easily determine many of the fusion coefficients for non-modular premodular categories. This is most pronounced in the setting that $\mathcal{C}$ is actually a symmetric category where Deligne's classification *loc. cit.* immediately gives the following:

Proposition VI.2.1. *If $\mathcal{C}$ is a rank 4 symmetric category, then it is Grothendieck equivalent to* $\operatorname{Rep}(G)$ *where G is $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_{10}, or $\mathfrak{A}_4$.*

Proof. Due to [D1], we know that a rank 4 symmetric category is Grothendieck equivalent to $\operatorname{Rep}(G)$ for some finite group with 4 irreducible representations and hence, 4 conjugacy classes. Thus, we may couple the class equation with [Cu1] to deduce that $|G| \leq 42$. The result then follows by examining this finite collection of groups in GAP. □

Next, we consider modular categories. We recall that much of the classification has been completed in [RSW]. The omissions will be filled in and the classification completed in the following result.[1]

Proposition VI.2.2. *If $\mathcal{C}$ is a rank 4 modular category, then it is Galois conjugate to a modular category from [RSW][2] or has S–matrix*

$$\begin{pmatrix} 1 & -1 & \overline{\tau} & \tau \\ -1 & 1 & -\tau & -\overline{\tau} \\ \overline{\tau} & -\tau & -1 & -1 \\ \tau & -\overline{\tau} & -1 & -1 \end{pmatrix},$$

where $\tau = \frac{1+\sqrt{5}}{2}$ is the golden mean and $\overline{\tau} = \frac{1-\sqrt{5}}{2}$ is its Galois conjugate.

Proof. By [RSW], the only case left to examine is when the Galois group is $\langle (0\ 1)\,(2\ 3) \rangle$ and $\mathcal{C}$ is not pseudo-unitary. Applying the standard Galois techniques present in [RSW] leads to:

$$S = \begin{pmatrix} 1 & d_1 & d_2 & d_3 \\ d_1 & \epsilon_0 & \epsilon_3 d_3 & \epsilon_0\epsilon_3 d_2 \\ d_2 & \epsilon_3 d_3 & s_{22} & s_{23} \\ d_3 & \epsilon_0\epsilon_3 d_2 & s_{23} & \epsilon_0 s_{22} \end{pmatrix}.$$

where $\epsilon_j = \pm 1$. Taking the cases $\epsilon_0 = \pm 1$ separately, we have.

Case 1: $\epsilon_0 = 1$.

[1] The author would like to thank Eric Rowell for suggesting this approach.

[2] Here, we allow for a non-standard choice of spherical structure, e.g., $S = \left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$ is the S-matrix corresponding to the Semion category with the non-standard spherical structure.

Orthogonality of the first two columns of S gives $d_1 = -\epsilon_3 d_2 d_3$. Applying our Galois element to this equation implies that $\epsilon_3 = -1$. Next, orthogonality of the last two columns gives us that $S_{2,3}S_{2,2} = -d_2 d_3$. This coupled with the orthogonality of the second and the fourth columns gives $S_{2,2} = -1$ or $S_{2,2} = d_3^2$. We now examine these two subcases separately.

Case 1.1: $S_{2,2} = d_3^2$

Applying the orthogonality of the first and the fourth columns of the S–matrix, we find that $d_3 = \pm d_2$, we can apply the Verlinde formula and this relation to compute $N_{1,1}^3 = d_3 - \frac{1}{d_3}$ and so $d_3 = \frac{n\pm\sqrt{4+n^2}}{2}$ for some $n \in \mathbb{N}$. Examining the remaining $N_{1,a}^b$, we find that either $n = 0$ or $d_2 = d_3$. However, if $n = 0$, we have $d_a = \pm 1$ for all a. Since rank 4 pointed modular categories have been classified, we may assume $d_2 = d_3$. Under this assumption the S–matrix takes the form

$$S = \begin{pmatrix} 1 & d_3^2 & d_3 & d_3 \\ d_3^2 & 1 & -d_3 & -d_3 \\ d_3 & -d_3 & d_3^2 & -1 \\ d_3 & -d_3 & -1 & d_3^2 \end{pmatrix}.$$

Applying the balancing relation–equation (II.16)– and the Verlinde formula, we find $-1 = S_{2,3} = \frac{\left(n\pm\sqrt{4+n^2}\right)^2\theta_1}{4\theta_2\theta_3}$, where θ_a are the twists. Taking the modulus of both sides and recalling that $|\theta_a| = 1$ gives the equation $4 = \left(n \pm \sqrt{4+n^2}\right)^2$, whose only solution over $\mathbb{N}$ is $n = 0$ and so we have that $\mathcal{C}$ is pointed.

Case 1.2: $S_{2,2} = -1$

In this case, we apply the Verlinde formula to compute $N_{1,1}^2$ and $N_{1,1}^3$ which leads to $d_2 = \frac{1}{2}\left(n \pm \sqrt{4+n^2}\right)$ and $d_3 = \frac{1}{2}\left(m \pm \sqrt{4+m^2}\right)$ for some $m, n \in \mathbb{N}$. The balancing equation for $S_{2,2}$, $S_{2,3}$, and $S_{3,3}$ gives that $\theta_1 = \theta_2\theta_3$ and that

$$d_2 = \pm\sqrt{\frac{-1+\theta_2-\theta_2^2}{\theta_2}}, \quad d_3 = \pm\sqrt{\frac{-1+\theta_3-\theta_3^2}{\theta_3}}$$

Combining these results produces a degree 4 integral polynomial which must be satisfied by the roots of unity θ_2 and θ_3. Applying the inverse Euler (totient) phi function, we see that θ_2, θ_3 are $\pm i$ or primitive 5th roots of unity and so $d_2, d_3 \in \{\pm 1, \pm\tau, \pm\overline{\tau}\}$ where τ is the golden mean $\frac{1}{2}\left(1+\sqrt{5}\right)$ and $\overline{\tau}$ is its Galois conjugate. This leads to 48 (S, T) combinations. Twelve of the S–matrices are distinct with half of them Galois conjugate to the other half. Of these remaining six, two can be removed by relabeling. Thus, we have the following four S–matrices and their Galois conjugates:

$$\begin{pmatrix} 1 & -1 & \overline{\tau} & \tau \\ -1 & 1 & -\tau & -\overline{\tau} \\ \overline{\tau} & -\tau & -1 & -1 \\ \tau & -\overline{\tau} & -1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & -1 & -\tau & \tau \\ -1 & -1 & -\tau & -\tau \\ -\tau & -\tau & 1 & 1 \\ \tau & -\tau & 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & \tau & \tau \\ 1 & -1 & -\tau & \tau \\ \tau & -\tau & 1 & -1 \\ \tau & \tau & -1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & \tau^2 & \tau & \tau \\ \tau^2 & 1 & -\tau & -\tau \\ \tau & -\tau & -1 & \tau^2 \\ \tau & -\tau & \tau^2 & -1 \end{pmatrix}.$$

The second matrix corresponds to Sem $\boxtimes$ Fib where Sem is given the the non-standard spherical structure, i.e., has S-matrix $\left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$. The last two matrices are pseudo-unitary and hence appear in [RSW]. This leaves only the first S-matrix which corresponds to Fib $\boxtimes\overline{\text{Fib}}$.

Case 2: $\epsilon_0 = -1$

By resolving the labeling ambiguity present between the labels 2 and 3, we can take $\epsilon_3 = 1$. There are now two subcases.

Case 2.1: $|d_1| \geq 1$

Following the procedure of [RSW], we find that $d_1 = \frac{1}{2}\left(n \pm \sqrt{n^2+4}\right)$ and $\exists a, b \in \mathbb{Q}$ and $r, s \in \mathbb{Z}$ such that:

$$\begin{aligned} r = 2b + an, &\quad s = bn - 2a, \\ d_2 = ad_1 + b, &\quad d_3 = bd_1 - a, \\ D^2 = \left(1 + d_1^2\right)&\left(1 + a^2 + b^2\right). \end{aligned}$$

Additionally, the techniques of [RSW] lead to $|d_1|^4 \leq 1 + 5|d_1| + 8|d_1|^2 + 5|d_1|^3$. Coupling these results with $|d_1| \geq 1$ gives that $1 \leq |d_1| \leq \psi$, where ψ is a root of $x^4 - 5x^3 - 8x^2 - 5x - 1$, and is approximately given by 6.38048. Thus $-7 < d_1 < 7$. We also find that:

$$r^2 + s^2 \leq \left(n^2 + 4\right) \frac{4|d_1|^3 + 5|d_1|^2 + 4|d_1| + 1}{|d_1|^2\left(1 + |d_1|^2\right)}.$$

Given a bound on d_1, we now have a bound on a sum of squares of integers and hence we can exhaust all possibilities. To do this, we proceed in two subcases:

Case 2.1.1: $n > 0$

The fact that $d_1 = \frac{1}{2}\left(n + \sqrt{n^2+4}\right)$ implies $1 \leq n \leq 6$ and we have the case considered in [RSW]. From there, it follows that $(n, r, s) = (1, -2, -1)$ or $(1, 2, 1)$ and $d_1 = \tau$, $d_3 = \pm\tau$, and $d_2 = \pm 1$. However, these lead to relabelings of the S-matrices from case 1.

Case 2.1.2: $n < 0$

Proceeding as in case 2.1.1, we find that there are 446 possible triples (n, r, s) of which only 24 pass the integrality tests of [RSW]. Applying the Verlinde formula to determine the fusion rules in these cases, we find that all of these either violate the integrality or non-negativity of the fusion coefficients.

Case 2.2: $|d_1| < 1$

Applying our Galois element, we see that $\sigma(d_1) = -\frac{1}{d_1}$. Setting $\delta_i = \sigma(d_i)$, we find modular datum (potentially) coresponding to a category $\hat{\mathcal{C}}$, which is Galois conjugate to $\mathcal{C}$; whence if $\hat{\mathcal{C}}$ does not exist, then neither does $\mathcal{C}$. However, $|\delta_1| > 1$ and, since Galois conjugation preserves all categorical identities used in case 2.1, we see that we must have $\delta_3 = \delta_2\delta_1$, $\delta_2 = \pm 1$ and $\delta_1 = \tau$. However, this is the same conclusion as in case 2.1.1. Ergo, $\mathcal{C}$ must be Galois conjugate to one of the case 2.1.1

results. Since these are conjugate to the categories determined in [RSW], we can conclude that $\mathcal{C}$ has an S–matrix Galois conjugate to one appearing in case 1. □

Having dispensed with the symmetric and modular cases, we find that it is useful to stratify the properly premodular categories by duality and symmetric subcategory. It is known that every properly premodular category has a symmetric subcategory, its Müger center [M4]. Since the rank has been fixed the possible symmetric subcategories can be completely determined.

Proposition VI.2.3. *If $\mathcal{C}$ is a rank 4 non-pointed properly premodular category, then there are four cases:*

(i) $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathfrak{S}_3)$ *and $\mathcal{C}$ is self-dual.*

(ii) $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/3\mathbb{Z})$ *and $X_1^* = X_2$.*

(iii) $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$ *and $\mathcal{C}$ is self-dual.*

(iv) $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$ *and $X_2^* = X_3$.*

Proof. We know from [M4] and comments in the introduction,[3] that since $\mathcal{C}$ is non-symmetric and non-modular, then it must have a nontrivial symmetric subcategory of rank 2 or 3. Rank 3 symmetric subcategories are known to be Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/3\mathbb{Z})$ or $\operatorname{Rep}(\mathfrak{S}_3)$ [O4]. Rank 2 proceeds similarly and leads to categories Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$.

In the rank 3 case, we take X_0, X_1, and X_2 to be representatives of the distinct simple isomorphism classes that generate the symmetric subcategory, while, in rank 2, we take X_0 and X_1 to be the representative generators of $\mathcal{C}'$. The result then follows immediately by standard representation theory. □

Remark VI.2.4. This proposition only provides the fusion rules of the Müger center and does not immediately allow one to conclude that the central objects have twist 1. Nonetheless, knowledge of the fusion rules and dimensions are sufficient for the classification up to Grothendieck equivalence.

Classification of the properly premodular categories now proceeds by cases. The categories with high rank symmetric subcategories are, perhaps not surprisingly, easier to deal with since more of the datum is predetermined. As such, we will proceed through $\operatorname{Rep}(\mathfrak{S}_3)$ and $\operatorname{Rep}(\mathbb{Z}/3\mathbb{Z})$ first and then discuss the $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$ cases.

Proposition VI.2.5. *There is no rank 4 properly premodular category with $\mathcal{C}'$ Grothendieck equivalent to* $\operatorname{Rep}(\mathfrak{S}_3)$*.*

Proof. Applying the known representation theory of $\mathfrak{S}_3$, equation (II.13) and dimension counts, we find

$$N_1 = \begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix} \quad N_2 = \begin{pmatrix} 0&0&1&0\\ 0&0&1&0\\ 1&1&1&0\\ 0&0&0&2 \end{pmatrix} \quad N_3 = \begin{pmatrix} 0&0&0&1\\ 0&0&0&1\\ 0&0&0&2\\ 1&1&2&M \end{pmatrix}$$

[3] In [M4], $\mathcal{Z}_2(\mathcal{C})$ is a canonical full symmetric subcategory of $\mathcal{C}$, i.e. $\mathcal{C}'$.

for some $M \in \mathbb{N}$. Recall that $S_{a,b} = d_a d_b$ for $0 \leq a, b \leq 2$ by [M4, Proposition 2.5]. Coupling this with equation (II.16), we find $\theta_1 = \theta_2 = 1$. Denoting θ_3 by θ, this gives

$$S = \begin{pmatrix} 1 & 1 & 2 & \frac{N \pm \sqrt{24+M^2}}{2} \\ 1 & 1 & 2 & \frac{N \pm \sqrt{24+M^2}}{2} \\ 2 & 2 & 4 & N \pm \sqrt{24+M^2} \\ \frac{N \pm \sqrt{24+M^2}}{2} & \frac{M \pm \sqrt{24+M^2}}{2} & N \pm \sqrt{24+M^2} & \frac{12 + \left(M \pm \sqrt{24+M^2}\right) M\theta}{2\theta^2} \end{pmatrix}.$$

Since $\frac{S_{3,3}}{S_{0,3}}$ must satisfy the characteristic polynomial of N_3, we can deduce that θ must be a primitive root of unity satisfying a degree integral 3 polynomial. Employing the inverse Euler phi function, we find that $\theta = \pm 1$ and $M = 0$. Thus, $d_3 = \pm\sqrt{6}$. Having removed the free parameters from this datum, we are in a position to prove that such a category cannot exist. The Müger center, $\operatorname{Rep}(\mathfrak{S}_3)$, constitutes a Tannakian subcategory of $\mathcal{C}$. By [NNW1] and [DGNO1, Remark 5.10], we can form the de-equivariantization, $\mathcal{C}_{\mathfrak{S}_3}$, which is a braided $\mathfrak{S}_3$-crossed fusion category. However, $\operatorname{FPdim}(\mathcal{C}_{\mathfrak{S}_3}) = \frac{1}{6}\operatorname{FPdim}(\mathcal{C})$, $\dim(\mathcal{C}_{\mathfrak{S}_3}) = \frac{1}{6}\dim(\mathcal{C}) = 2$, and $\operatorname{FPdim}(\mathcal{C}_{\mathfrak{S}_3}) = 2$ [DGNO1]. Thus, $\mathcal{C}_{\mathfrak{S}_3}$ is weakly integral braided $\mathfrak{S}_3$-crossed fusion category and we may apply [ENO1, Corollary 8.30] to deduce that $\mathcal{C}_{\mathfrak{S}_3}$ is equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$ and hence pointed. Consequently, $\mathcal{C}$ is group-theoretical and in particular integral, contradicting $d = \pm\sqrt{6}$ [NNW1; DGNO1]. □

Proposition VI.2.6. *If $\mathcal{C}$ is a non-pointed properly premodular category such that $\langle X_0, X_1, X_2 \rangle = \mathcal{C}'$ is Grothendieck equivalent to* $\operatorname{Rep}(\mathbb{Z}/3\mathbb{Z})$*, then:*

$$S = \begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & 1 & 1 & 3 \\ 1 & 1 & 1 & 3 \\ 3 & 3 & 3 & -3 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$N_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$$

Such premodular datum is realized by $\left(\operatorname{SU}(2)_4\right)_{\text{ad}}$.

Proof. Applying Proposition VI.2.3, we know that $\mathcal{C}$ is self-dual and so applying the representation theory of $\mathbb{Z}/3\mathbb{Z}$ and equation (II.13), we find that the fusion matrices are determined up to $N_{3,3}^3$. Making use of equation (II.16), the fact that $S = S^T$, and the fact that, in a properly premodular category, some column of S is a multiple of the first, one finds that

$$S = \begin{pmatrix} 1 & 1 & 1 & d_3 \\ 1 & 1 & 1 & d_3 \\ 1 & 1 & 1 & d_3 \\ d_3 & d_3 & d_3 & \frac{3 + d_3 N_{3,3}^3 \theta_3}{\theta_3^2} \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \theta_3 \end{pmatrix}.$$

By dimension count, we see that $d_3 = \frac{1}{2}\left(N_{3,3}^3 \pm \sqrt{12 + N_{3,3}^3}\right)$. So it remains to determine $N_{3,3}^3$ and θ_3. For notational brevity, we let $M = N_{3,3}^3$. Applying equation (II.14), we find that

$$\begin{aligned} &(\theta_3 - 1)\left(18\theta_3\left(\theta_3^2 + \theta_3 + 1\right) + \theta_3^2 M^4 + 3\theta_3(\theta_3 + 1)(\theta_3 + 2)M^2 + 18\right) \\ &\quad = \pm(\theta_3 - 1)\left(3\theta_3\left(\theta_3^2 + \theta_3 + 2\right)\sqrt{M^2 + 12}M + \theta_3^2\sqrt{M^2 + 12}M^3\right). \end{aligned} \tag{VI.3}$$

We first note that if $\theta_3 = 1$, then $\mathcal{C} = \mathcal{C}'$ contradicting the non-symmetric assumption. Thus, θ_3 satisfies a degree 6 integral polynomial. However, θ_3 is a root of unity, so we can apply the inverse Euler phi function to determine a list of potential values for θ_3. Combing the possible cases, we find $N_{3,3}^3 \in \{0, 2\}$ and $\theta_3 \in \{\pm i, -1\}$. Applying Corollary VI.1.4 with $a = 3$, we find that only $N_{33}^3 = 2$ gives a rational integer. Evaluating equation (VI.3) at $N_{3,3}^3 = 2$ reveals that $\theta = -1$ is the only solution.[4] □

Having dispensed with the "large" symmetric subcategories, we need to consider the case that $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$. We first consider the non-self-dual case, which can be dealt with by cyclotomic/number theoretic techniques.

Proposition VI.2.7. *There is no rank 4 non-pointed properly premodular category such that* $\langle X_0, X_1 \rangle = \mathcal{C}'$ *is Grothendieck equivalent to* $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$, *and* $X_2^* = X_3$.

Proof. Given the standard representation theory of $\mathbb{Z}/2\mathbb{Z}$ and the equation (II.13), we immediately obtain:

$$N_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & N_{3,2}^1 & N_{3,3}^1 \\ 0 & 0 & N_{3,3}^1 & N_{3,2}^1 \end{pmatrix} \quad N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & N_{3,2}^1 & N_{3,3}^1 \\ 0 & N_{3,3}^1 & N_{3,3}^3 & N_{3,3}^2 \\ 1 & N_{3,2}^1 & N_{3,3}^3 & N_{3,3}^3 \end{pmatrix} \quad N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & N_{3,3}^1 & N_{3,2}^1 \\ 1 & N_{3,2}^1 & N_{3,3}^3 & N_{3,3}^3 \\ 0 & N_{3,3}^1 & N_{3,3}^2 & N_{3,3}^3 \end{pmatrix}.$$

Demanding that the fusion matrices mutually commute reveals that either $N_{3,2}^1$ or $N_{3,3}^1$ is 0 and the other is 1. Hence, the proof bifurcates.

Case 1: $N_{3,2}^1 = 1$ and $N_{3,3}^1 = 0$

Returning to the commutativity of the fusion matrices, we are reduced to one equation:

$$2 = \left(N_{3,3}^2\right)^2 - \left(N_{3,3}^3\right)^2.$$

However, such an equation lacks integer solutions, which can be seen by reduction modulo 4.

Case 2: $N_{3,2}^1 = 0$ and $N_{3,3}^1 = 1$.

In this case, the commutativity of the fusion matrices reveals that $N_{3,3}^2 = N_{3,3}^3$, which we will simply call M. Applying equation (II.16), and dimension count, we can determine the S-matrix to be

$$S = \begin{pmatrix} 1 & M \pm \sqrt{1+M^2} \\ M \pm \sqrt{1+M^2} & \frac{1+2\left(M\pm\sqrt{1+M^2}\right)M\theta}{\theta^2} \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Where $\theta := \theta_2 = \theta_3$ and $\theta_1 = 1$, which follows from the Proposition II.4.1. However, $\frac{S_{2,2}}{S_{0,2}}$ must satisfy the characteristic polynomial of N_2, which factors into two quadratics. Inserting this quotient

[4] If one proceeds without appealing to the Frobenius-Schur indicators then the Tambara-Yamagami with dimensions $1, 1, 1, \sqrt{3}$ appear. This can of course be excluded since such categories do not admit a braiding [S1].

into the factors, we find that θ must satisfy either a degree 4 or degree 8 polynomial over $\mathbb{Z}$. Since θ is a primitive root of unity, we can apply the inverse Euler phi function to bound the degree of the minimal polynomial of θ. Proceeding through all cases, we find that $M = 0$ and $\mathcal{C}$ is pointed. □

While this cyclotomic analysis has been quite fruitful, the remaining properly premodular case proves to be resistant and so other approaches are necessary. We begin by recalling that every fusion category admits a (possibly trivial) grading. Since the category has small rank, the grading possibilities allow for further stratification.

Proposition VI.2.8. *If $\mathcal{C}$ is a self-dual rank 4 non-pointed properly premodular category such that $\langle X_0, X_1\rangle = \mathcal{C}'$ is Grothendieck equivalent to* $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$*, then there are three cases.*

(i) $\mathcal{C}$ admits a universal $\mathbb{Z}/2\mathbb{Z}$-grading

(ii) The universal grading group of $\mathcal{C}$ is trivial and $X_1 \otimes X_2 = X_2$

(iii) The universal grading group of $\mathcal{C}$ is trivial and $X_1 \otimes X_2 = X_3$

Proof. If $\mathcal{C}$ admits a nontrivial universal grading, then it must be by $\mathbb{Z}/2\mathbb{Z}$. On the other hand, if $\mathcal{C}$ does not admit a universal grading, then $\mathcal{C}_{\text{ad}} = \mathcal{C}$ [DGNO1]. Since X_1 generates $\mathcal{C}'$ which is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$, we can conclude that if $\mathcal{C}_{\text{ad}} = \mathcal{C}$, then either $X_1 \otimes X_2 = X_2$ or $X_1 \otimes X_2 = X_3$. □

With this proposition in hand, we again proceed by cases. First, we consider the relatively simple case: $\mathcal{C}$ admits a universal $\mathbb{Z}/2\mathbb{Z}$-grading.

Proposition VI.2.9. *Suppose $\mathcal{C}$ is a self-dual rank 4 non-pointed properly premodular category admitting a universal $\mathbb{Z}/2\mathbb{Z}$-grading such that $\mathcal{C}'$ is Grothendieck equivalent to* $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$*, then $\mathcal{C}$ is a Deligne product of the* Fib *with* $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$ *or* sVec*.*

Proof. Dimension count coupled with the representation theory of $\mathbb{Z}/2\mathbb{Z}$ completely determines the fusion relations up to $N_{2,2}^2$. However, we can apply [O4] to conclude that $N_{2,2}^2 \in \{0, 1\}$. $N_{2,2}^2 = 0$ leaves a pointed category and so we must have $N_{2,2}^2 = 1$, and $d := d_2 = d_3 = \frac{1\pm\sqrt{5}}{2}$. Applying equation (II.16) and Proposition II.4.1, we find that $\theta_1 = \pm 1$, $\theta := \theta_2 = \theta_1\theta_3$, and

$$S = \begin{pmatrix} 1 & 1 & d & d \\ 1 & 1 & d & d \\ d & d & \frac{1+d\theta}{\theta^2} & \frac{1+d\theta}{\theta^2} \\ d & d & \frac{1+d\theta}{\theta^2} & \frac{1+d\theta}{\theta^2} \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \pm 1 & 0 & 0 \\ 0 & 0 & \theta & 0 \\ 0 & 0 & 0 & \pm\theta \end{pmatrix}.$$

Since the normalized columns of the S–matrix are characters of the fusion ring, it must be that $\frac{1+d\theta}{d\theta^2}$ is a simultaneous root of the characteristic polynomials of N_2 and N_3. This gives the desired result. □

Finally, we come to the last two cases where $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$ and the universal grading is trivial. These are by far the most complicated cases. To dispense with the first case, we make use of the minimal modularization [Brug1].

Proposition VI.2.10. *Suppose $\mathcal{C}$ is a self-dual, rank 4, non-pointed, properly premodular category such that $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$, $\mathcal{C}$ has trival universal grading group, and $X_1 \otimes X_2 = X_2$, then*

$$S = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 2 & \frac{2+2\theta}{\theta^3} & \frac{2+2\theta^2}{\theta} \\ 2 & 2 & \frac{2+2\theta^2}{\theta} & \frac{2+2\theta}{\theta^3} \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \theta & 0 \\ 0 & 0 & 0 & \theta^{-1} \end{pmatrix}$$

$$N_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

and θ is a primitive 5^{th} root of unity. Such premodular datum is realized by $(\mathrm{SO}(5)_2)_{\mathrm{ad}}$.

Proof. The representation theory of $\mathbb{Z}/2\mathbb{Z}$, dimension count, and equations (II.13), and (II.16) give:

$$N_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & N_{2,2}^2 & N_{3,2}^2 \\ 0 & 0 & N_{3,2}^2 & N_{3,3}^2 \end{pmatrix} \quad N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & N_{3,2}^2 & N_{3,3}^2 \\ 1 & 1 & N_{3,3}^2 & N_{3,3}^3 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 1 & d_2 & d_3 \\ 1 & 1 & d_2 & d_3 \\ d_2 & d_2 & \frac{2+d_2N_{2,2}^2\theta_2+d_3N_{3,2}^2\theta_3}{\theta_2^2} & \frac{d_2N_{3,2}^2\theta_2+d_3N_{3,3}^2\theta_3}{\theta_2\theta_3} \\ d_3 & d_3 & \frac{d_2N_{3,2}^2\theta_2+d_3N_{3,3}^2\theta_3}{\theta_2\theta_3} & \frac{2+d_2N_{3,3}^2\theta_2+d_3N_{3,3}^3\theta_3}{\theta_3^2} \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \theta_2 & 0 \\ 0 & 0 & 0 & \theta_3 \end{pmatrix}.$$

Applying [Brug1, Proposition 4.2], we can deduce that $\mathcal{C}$ admits a modularization, $\hat{\mathcal{C}}$. We can now apply [Brug1, Proposition 4.4] and the equivalence between Bruguières modularization and the de-equivariantization to deduce that $\hat{\mathcal{C}}$ has rank 5 with simple objects $\mathbb{I}, Y_1, Y_2, Z_1, Z_2$ such that $Y_i^* \in \{Y_1, Y_2\}$ and $Z_i^* \in \{Z_1, Z_2\}$. Applying the rank 5 classification of [BNRW1], we see that there are no non-pointed rank 5 modular categories with $\dim X_1 = \dim X_2$ and $\dim X_2 = \dim X_3$. Consequently, $d_2 = \pm 2$ and $d_3 = \pm 2$. Dimension count then allows us to fix all fusion coefficients except for $N_{3,3}^3$. Applying [NR1, Theorem 4.2], we know that $\mathcal{C}$ is Grothendieck equivalent to $\operatorname{Rep}(D_n)$ and is group-theoretical. This gives $d_2 = d_3 = 2$, and determines the fusion coefficients. Applying equations (II.14) and (II.10), we find $\theta_3 = \theta_2^{-1}$ and that θ_2 is a primitive 5th root of unity. □

The final case requires not only the minimal modularization of Bruguières, but also the second Frobenius-Schur indicators.

Proposition VI.2.11. *Suppose $\mathcal{C}$ is a self-dual rank 4 non-pointed properly premodular category such that $\mathcal{C}'$ is Grothendieck equivalent to $\operatorname{Rep}(\mathbb{Z}/2\mathbb{Z})$, the universal grading group is trivial, and*

$X_1 \otimes X_2 = X_3$, *then*

$$S = \left(\begin{smallmatrix} 1 & 1\pm\sqrt{2} \\ 1\pm\sqrt{2} & -1 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \quad T = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -i \end{smallmatrix}\right) N_2 = \left(\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{smallmatrix}\right) \quad N_3 = \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{smallmatrix}\right).$$

Such premodular datum is realized by $\left(\mathrm{SU}\left(2\right)_6\right)_{\mathrm{ad}}$ *and its conjugates.*

Proof. Applying dimension count, equation (II.13), and the usual representation theory for $\mathbb{Z}/2\mathbb{Z}$, we can determine the fusion rules up to two parameters:

$$N_1 = \left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right) \quad N_2 = \left(\begin{smallmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & N & M \\ 0 & 1 & M & N \end{smallmatrix}\right) \quad N_3 = \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & M & N \\ 1 & 0 & N & M \end{smallmatrix}\right).$$

Furthermore, we can deduce that $M, N \neq 0$ lest we reduce to the fusion rules of Proposition VI.2.9 of a pointed category. Next, we may use equation (II.16), dimension count, and that $S_{a,b} = \lambda S_{a,0}$ for some b and some $\lambda \in \mathbb{C}^{\times}$, to find the S- and T-matrices:

$$S = \begin{pmatrix} 1 & \frac{N+M+\epsilon\sqrt{4+(M+N)^2}}{2} \\ \frac{N+M+\epsilon\sqrt{4+(M+N)^2}}{2} & \frac{2+(N\theta+\delta M\theta)\left(N+M+\epsilon\sqrt{4+(M+N)^2}\right)}{2\theta^2} \end{pmatrix} \otimes \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \quad T = \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & \delta & 0 & 0 \\ 0 & 0 & \theta & 0 \\ 0 & 0 & 0 & \delta\theta \end{smallmatrix}\right),$$

where $\epsilon, \delta = \pm 1$. We treat $\delta = 1$ and $\delta = -1$ in separate cases.

Case 1: $\delta = 1$

Here we can apply [Brug1] to deduce that $\mathcal{C}$ is modularizable. Letting $H : \mathcal{C} \to \hat{\mathcal{C}}$ denote its minimal modularization, we have $X_2 \in \mathcal{C}' X_3$ and so $H\left(X_2\right) \cong H\left(X_3\right)$. Furthermore, $\left|\mathrm{Stab}_{\mathcal{C}'} X\right| = 1$ for all simple X and thus, $\dim H\left(X_2\right) = \dim\left(X_2\right)$. Consequently, the trivial object in $\hat{\mathcal{C}}$ as well as $H\left(X_2\right)$ account for $1 + d^2$ of the dimension of $\hat{\mathcal{C}}$. However, $\dim \hat{\mathcal{C}} = \frac{1}{2}\dim\left(\mathcal{C}\right) = 1 + d^2$ and so $\hat{\mathcal{C}}$ is a rank 2 modular category with simple objects $\mathbb{I}$ and $H\left(X_2\right)$. Such categories have been classified in [RSW] and are Grothendieck equivalent to the Semion and the Fibonacci. In these situations, we find either that $\mathcal{C}$ is pointed or that $M = N = 0$ and so we can exclude the case of $\delta = 1$.

Case 2: $\delta = -1$.

Applying the equations (II.14) and (II.10) further reduces the solution space. Discarding any solutions where either M or N is 0 or $\mathcal{C}$ is symmetric leaves 7 possible families of solutions. One of these families contains a Pythagorean triple with 1 which forces $N < 0$ and hence can be discarded. Two of the other families of solutions have M and N related by:

$$M = \frac{-N\theta^2 \pm \sqrt{-\theta\left(1+\theta^2\right)^2\left(1-\left(1+N^2\right)\theta+\theta^2\right)}}{\theta\left(1+\theta\left(\theta-1\right)\right)}.$$

Since $\theta \neq 0$, this can be arranged into a monic integral degree 6 polynomial θ. Since θ is a root of unity, we can apply the inverse Euler phi function to find a possible list of values for θ.

Direct calculation reveals that none of these roots of unity can satisfy this polynomial in a manner consistent with $M, N > 0$.

The remaining four families can be reduced by resolving a labeling ambiguity to give:

$$S = \begin{pmatrix} 1 & N+\epsilon\sqrt{1+N^2} \\ N+\epsilon\sqrt{1+N^2} & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}$$

$$N_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & N & N \\ 0 & 1 & N & N \end{pmatrix} \quad N_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & N & N \\ 1 & 0 & N & N \end{pmatrix}.$$

Applying Corollary VI.1.4 to X_2, we find that $N \pm \frac{N^2-1}{\sqrt{N^2+1}} \in \mathbb{Z}$. Denoting this integer by L and simplifying, we find:

$$4 = \left(N^2+1\right)\left(3+L^2-2LN\right)$$

However, $N^2+1 \neq 0$ and so, reducing modulo N^2+1, we find that $4 \equiv 0 \mod N^2+1$.

This only occurs for $N \in \{-1, 0, 1\}$. Since $N = 0$ leads to $\mathcal{C}$ being pointed and we know $N \geq 0$, we can conclude that $N = 1$. □

The results of this section can be compiled to give the following theorem.

Theorem VI.2.12. *If $\mathcal{C}$ is a non-pointed rank 4 premodular category, then exactly one of the following is true*

(i) $\mathcal{C}$ is symmetric and is Grothendieck equivalent to $\mathrm{Rep}(G)$ where G is $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_{10}, or $\mathfrak{A}_4$.

(ii) $\mathcal{C}$ is properly premodular and is Grothendieck equivalent to a Galois conjugate of one of the following: $\mathcal{C}\left(\mathrm{SU}(2)_6\right)_{\mathrm{ad}}$, $\mathcal{C}\left(\mathrm{SU}(2)_4\right)_{\mathrm{ad}}$, $\mathcal{C}\left(\mathrm{SO}(5)_2\right)_{\mathrm{ad}}$, $\mathrm{Fib} \boxtimes \mathrm{Rep}(\mathbb{Z}/2\mathbb{Z})$, or $\mathrm{Fib} \boxtimes \mathrm{sVec}$.

(iii) $\mathcal{C}$ is modular and is Galois conjugate to a modular category from [RSW][5] or has S-matrix

$$\begin{pmatrix} 1 & -1 & \overline{\tau} & \tau \\ -1 & 1 & -\tau & -\overline{\tau} \\ \overline{\tau} & -\tau & -1 & -1 \\ \tau & -\overline{\tau} & -1 & -1 \end{pmatrix},$$

where $\tau = \frac{1+\sqrt{5}}{2}$ is the golden mean and $\overline{\tau} = \frac{1-\sqrt{5}}{2}$ is its Galois conjugate.

[5] Here, we allow for a non-standard choice of spherical structure, e.g., $S = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ is the S-matrix corresponding to the Semion category with the non-standard spherical structure.

CHAPTER VII
SUMMARY

In this work, we have seen that (pre)modular categories and braided fusion categories are widely applicable in physics, computer science, and mathematics. Not only do they generalize representation theory and describe the representations of quasi-Hopf algebras, they also lead to link invariants, 3-manifold invariants, and describe $(2+1)$-dimensional topological quantum field theories. This last application has garnered a great deal of interest in recent years as it has led to the development of paradigms for quantum computation, which are fault tolerant at the hardware level. An understanding and classification of (pre)modular categories is thus highly desirable.

In Chapter IV, we laid to rest the 9-year old rank finiteness question known as Wang's Conjecture. Thereby, showing that there are finitely many modular categories of fixed rank up to equivalence. This indicates that the classification of modular categories is a tractable problem. The proof of this conjecture spawned an algorithm for classifying modular categories up to Grothendieck equivalence. While this is the first general algorithm for such classification, it suffers several problems. Indeed, not only does the algorithm rely on NP-algorithms *viz.* the computation of a shortest vector in a lattice, but also the upper bound on the number of solutions determined by the algorithm is quadruply exponential. This is in stark contrast to the near linear progression of equivalence classes of modular categories in low rank. This has prompted several questions:

(i) Is this quadruply exponential bound required asymptotically?

(ii) Does rank finiteness provide an explicit upper bound on D^2 solely in terms of the rank?

(iii) Does the proof of rank finiteness provide an explicit bound on $\left|D^2-1\right|$ strictly in terms of the rank?

While we find these questions interesting and hope to address them, they were not considered in this work.

The proof of rank finiteness, as well as previous low rank classification, suggested that modular categories possess strong arithmetic properties and that their study would benefit from a number theoretic treatment. In Sections III.1 and III.2, we reviewed previously known arithmetic properties and some of the consequences of the $\mathrm{SL}\left(2,\mathbb{Z}\right)$-representations associated to modular categories. This prompted the study of modularly admissible fields in Section III.3. There, we found that modularly admissible fields of small degree, in particular prime power degree, are subject to extremely stringent primality conditions. This allowed us to eliminate entire classes of fields from consideration in the study of modular categories. Furthermore, this study suggested that modular categories may be equipped to answer classical number theoretic questions, such as the infinitude of Sophie Germain primes. This section was completed by classifying modularly admissible fields of degree at most 7 as well as all 2-Kummer modularly admissible fields. This classification, in principle, gives powerful techniques. For instance, if one considers only the fields which have class number 1, then the Smith Normal Form may allow one to solve many of the linear Diophantine systems, which arise in the study of modular categories.

In Chapter V, the aforementioned arithmetic properties and primality conditions were applied to the classification of modular categories. In particular, these conditions as well as classical Diophantine analysis allowed us to classify integral modular categories through rank 7, maximally non-self dual modular categories through rank 11, and weakly integral modular categories through rank 6. This is in stark contrast to the quadruply exponential bounds suggested by the classification algorithm IV.2.6. This suggests that more delicate number theoretic analysis can be used to provide improvements to the algorithms IV.2.6 and V.1.1.

Number theoretic analysis proved to be quite useful in the modular setting, and traditionally moving beyond modular categories to premodular categories has been very difficult. This prompted us to ask: *Can the number theoretic techniques used in the modular setting be applied to premodular categories?* In Chapter VI, we found that many of the modular techniques in fact fail in the premodular setting. Nonetheless, we were able to suggest extensions of the modular techniques to the premodular setting. For instance, if $\operatorname{ord}(T)$ is replaced with $\mathrm{FSExp}(\mathcal{C})$, then many of the modular statements, such as the Cauchy Theorem for Modular Categories and the Ng-Schauenburg Theorem, have premodular analogs. This allowed us to suggest approaches to showing rank finiteness in the premodular setting. Moving beyond these theoretical questions, we were able to determine an explicit formula for the 2nd Frobenius-Schur indicator in the premodular setting. This formula requires explicit knowledge of the R-matrices on the Muüger center of the category and so is of limited use. Nonetheless, we were able to apply this formula to determine integrality conditions which must be satisfied by premodular categories. These integrality conditions coupled with *ad hoc* cyclotomic and number theoretic techniques allowed us to complete the classification of rank 4 (pre)modular categories.

Creative applications of number theory allowed us to make great strides in the study of (pre)modular categories. As discussed above, we showed rank finiteness of modular categories, determined stringent primality conditions which must be satisfied by modular categories, and extended the rank classification of (pre)modular categories. This approach is new and the connections between number theory and (pre)modular categories unveiled in this work appear to be deep. Future studies in this direction are warranted and promise to present researchers in both quantum algebra and number theory with new tools, techniques, and directions.

REFERENCES

[AIM1] P. Bruillard et al., *Classification of Integral Modular Categories of Frobenius-Perron Dimension pq^4 and p^2q^2*, In Preparation (2013). arXiv:`1303.4748v1 [math.QA]`.

[At1] M. Atiyah, *Topological Quantum Field Theories*, Publications Mathématiques des l'HÉS **68** (1989), 175–186.

[B3] P. Bruillard, *A Quantum Algorithm for Determining the S-Unit Group*, In Preparation (2012).

[B4] P. Bruillard, *Ramification in Modular Categories*, Unpublished, June 2012.

[Ban1] P. Bantay, *The Frobenius-Schur Indicator in Conformal Field Theory*, Phys. Lett. B **394** (1997), no. 1–2, 87–88. arXiv:`hep-th/9610192v2`.

[Ban2] P. Bantay, *The Kernel of the Modular Representation and the Galois Action in RCFT*, Comm. Math. Phys. **233** (2003), 423–438.

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

[BG1] J. M. Burns and B. Goldsmith, *Maximal Order Abelian Subgroups of Symmetric Groups*, Bull. Lond. Math. Soc. **21** (1980), 70–72.

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

[BNRW1] P. Bruillard, S.-H. Ng, E. C. Rowell, and Z. Wang, *On Modular Categories*, In Preparation (2013).

[BR1] P. Bruillard and E. Rowell, *Modular Categories, Integrality and Egyptian Fractions*, Proc. Amer. Math. Soc. **140** (2012), no. 4, 1141–1150. arXiv:`1012.0814v2 [math.QA]`.

[Brug1] A. Bruguières, *Catégories Prémodulaires, Modularisations et Invariants des Variétés de Dimension 3*, Math. Ann. **316** (2000), 215–236.

[C2] H. Cohen, *Advanced Topics in Computational Number Theory*, ed. by S. Axler, F. W. Gehring, and R. A. Ribet, Graduate Texts in Mathematics, no. 193, Springer-Verlag, New York, NY, 2000.

[CGR1] A. Coste, T. Gannon, and P. Ruelle, *Finite Group Modular Data*, Nuclear Phys. B **581** (2000), no. 3, 679–717. arXiv:`hep-th/0001158`.

[Ch1] N. Childress, *Class Field Theory (Universitext)*, 1st Edition, 2nd Printing, Universitext, Springer Science+Business Media, New York, NY, 2008.

[Cu1] D. R. Curtiss, *On Kellogg's Diophantine Problem*, Amer. Math. Monthly **29** (1922), 380–387.

[D1] P. Deligne, *Catégories Tensorielles*, Mosc. Math. J. **2** (2002), no. 2, 227–248.

[DGNO1] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, *On Braided Fusion Categories I*, Selecta Math. **16** (2010), no. 1, 1–119. arXiv:`0906.0620v3 [math.QA]`.

[DGNO2] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, *Group-Theoretical Properties of Nilpotent Modular Categories*, (2007). arXiv:`0704.0195v2 [math.QA]`.

[DLN1] C. Dong, X. Lin, and S.-H. Ng, *Congruence Property in Conformal Field Theory*, (2012). arXiv:`1201.6644v4 [math.QA]`.

[DR1] S. Doplicher and J. E. Roberts, *A New Duality Theory for Compact Groups*, Invent. Math. **98** (1989), 157–218.

[ECo1] P. Etingof, *Private Communication*, Feb. 2013.

[EG1] P. Etingof and S. Gelaki, *Some Properties of Finite-Dimensional Semisimple Hopf Algebras*, Math. Res. Lett. **5** (1998), no. 1–2, 191–197. arXiv:`q-alg/9712033v1`.

[EGNO1] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik, *Tensor Categories*, 2012, Available at: `http://www-math.mit.edu/~etingof/tenscat1.pdf`.

[EGO] P. Etingof, S. Gelaki, and V. Ostrik, *Classification of Fusion Categories of Dimension pq*, Int. Math. Res. Not. IMRN **57** (2004), 3041–3056. arXiv:`math/0304194v2 [math.QA]`.

[Eh1] W. Eholzer, *On the Classification of Modular Fusion Algebras*, Comm. Math. Phys. **172** (1995), no. 3, 623–659.

[ENO1] P. Etingof, D. Nikshych, and V. Ostrik, *On Fusion Categories*, Ann. of Math. **162** (2005), no. 2, 581–642. arXiv:`math/0203060v10 [math.QA]`.

[ENO2] P. Etingof, D. Nikshych, and V. Ostrik, *Weakly Group-Theoretical and Solvable Fusion Categories*, Adv. Math. **226** (2011), no. 1, 176–205. arXiv:`0809.3031v2 [math.QA]`.

[ERW1] P. Etingof, E. Rowell, and S. Witherspoon, *Braid Representations from Twisted Quantum Doubles of Finite Groups*, Pacific J. Math. **234** (2008), no. 1, 33–42.

[Eti1] P. Etingof, *On Vafa's Theorem for Tensor Categories*, Math. Res. Lett. **9** (2002), 651–657. arXiv:`math/0207007v1 [math.QA]`.

[Eti2] P. Etingof, *On Some Properties of Quantum Doubles of Finite Groups*, (Aug. 2012). arXiv:`1208.4874v1 [math.QA]`.

[Ev1] J.-H. Evertse, *On Sums of S-Units and Linear Recurrences*, Compos. Math. **53** (1984), 225–244.

[Ev2] J.-H. Evertse, *The Number of Solutions of Decomposable Form Equations*, Invent. Math. **122** (1995), 559–601.

[G1] T. Gannon, *Modular Data: The Algebraic Combinatorics of Conformal Field Theory*, J. Algebraic Combin. **22** (2005), no. 2, 211–250.

[GK1] D. Gepner and A. Kapustin, *On the Classifciation of Fusion Rings*, Phys. Lett. B **349** (1995), no. 1–2, 71–75. arXiv:`hep-th/9410089v1`.

[GN1] S. Gelaki and D. Naidu, *Some Properties of Group-Theroetical Categories*, J. Algebra **322** (2009), no. 8, 2631–2641. arXiv:`0709.4326v1 [math.QA]`.

[GN2] S. Gelaki and D. Nikshych, *Nilpotent Fusion Categories*, Adv. Math. **217** (2008), no. 3, 1053–1071. arXiv:`math/0610726v2 [math.QA]`.

[H1] S.-M. Hong, *Classification and Applications of Tensor Categories*, Ph.D. Indiana University, Bloomington, IN, Aug. 2008.

[Ha1] S. Hallgren, *Fast Quantum Algorithms for Computing the Unit Group and Class Group of a Number Field*, In Proceedings of the 37th AMC Symposium on the Theory of Computing (2005).

[HM1] D. Haase and H. Maier, *Quantum Algorithms for Number Fields*, Fortschr. Phys. **54** (2006), no. 8, 866–881.

[HR1] S.-M. Hong and E. Rowell, *On the Classification of the Grothendieck Rings of Non-Self Dual Modular Categories*, J. Algebra **324** (2010), no. 5, 1000–1015. arXiv:`0907.1051v2 [math.QA]`.

[HSW1] J. G. Huard, B. K. Spearman, and K. S. Williams, *A Short Proof of the Formula for the Conductor of an Abelian Cubic Field*, Skr. K. Nor. Vidensk. Selsk. **2** (1994), 3–8.

[JL1] D. Jordan and E. Larson, *On the Classification of Certain Fusion Categories*, J. Noncommut. Geom. **3** (2009), no. 3, 481–499. arXiv:`0812.1603v2 [math.QA]`.

[JS1] A. Joyal and R. Street, *Braided Tensor Categories*, Adv. Math. **102** (1993), no. 1, 20–78.

[K1] A. Kitaev, *Anyons in an Exactly Solved Model and Beyond*, Ann. Physics **321** (2006), no. 1, 2–111. arXiv:`cond-mat/0506438v3`.

[L1] E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante*, Math. Ann. **50** (1903), 671–676.

[M2] M. Müger, *From Subfactors to Categories and Topology II: The Quantum Doubles of Tensor Categories and Subfactors*, J. Pure Appl. Algebra **180** (2003), no. 1–2, 159–219.

[M3] M. Müger, *Tensor Categories: A Selective Guided Tour*, Rev. Un. Mat. Argentina **51** (2010), no. 1, 95–163. arXiv:`0804.3587v3 [math.CT]`.

[M4] M. Müger, *On the Structure of Modular Categories*, Proc. Lond. Math. Soc. **87** (2003), no. 2, 291–308. arXiv:`math/0201017v1 [math.CT]`.

[Mac] S. Mac Lane, *Categories for the Working Mathematician*, Graduate Texts in Mathematics, Springer-Verlag, New York, NY, 1971.

[Mi1] J. S. Milne, *Algebraic Number Theory (v3.03)*, 2011, Available at: `http://www.jmilne.org/math/`.

[Mi2] J. S. Milne, *Class Field Theory (v4.01)*, 2011, Available at: `http://www.jmilne.org/math/`.

[N1] D. Nikshych, *Braided Fusion Categories: A Short Course*, ().

[N2] D. Nikshych, *MATH 961 (Topics in Algebra): Tensor Categories*, 2010, Available at: `http://euclid.unh.edu/~nikshych/TensorCategories.pdf`.

[N3] D. Nikshych, *Non Group-Theoretical Semisimple Hopf Algebras From Group Actions on Fusion Categories*, Selecta Math. **14** (2008), 145–161.

[NC1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, Cambridge CB2 8RU, UK, Jan. 2011.

[NN1] D. Naidu and D. Nikshych, *Lagrangian Subcategories and Braided Tensor Equivalences of Twisted Quantum Doubles of Finite Groups*, Comm. Math. Phys. **279** (2008), no. 3, 845–872. arXiv:`0705.0665v2 [math.QA]`.

[NNW1] D. Naidu, D. Nikshych, and S. Witherspoon, *Fusion Subcategories of Representation Categories of Twisted Quantum Doubles of Finite Groups*, Int. Math. Res. Not. IMRN **22** (2009), 4183–4219.

[NR1] D. Naidu and E. C. Rowell, *A Finiteness Property for Braided Fusion Categories*, Algebr. Represent. Theory **14** (2011), no. 5, 837–855. arXiv:`0903.4157v4 [math.QA]`.

[NS1] S.-H. Ng and P. Schauenburg, *Higher Frobenius-Schur Indicators for Pivotal Categories*, Contemp. Math. **441** (2007). arXiv:`math/0503167v2 [math.QA]`.

[NS2] S.-H. Ng and P. Schauenburg, *Frobenius-Schur Indicators and Exponents of Spherical Categories*, Adv. Math. **211** (2007), no. 1, 34–71. arXiv:`math/0601012v3 [math.QA]`.

[NS3] S.-H. Ng and P. Schauenburg, *Congruence Subgroups and Generalized Frobenius-Schur Indicators*, Comm. Math. Phys. **300** (2010), no. 1, 1–46. arXiv:`0806.2493v3 [math.QA]`.

[O2] V. Ostrik, *On Fusion Categories of Rank 2*, Math. Res. Lett. **10** (2003), no. 2–3, 177–183. arXiv:`math/0203255v1 [math.QA]`.

[O4] V. Ostrik, *Pre-modular Categories of Rank 3*, Mosc. Math. J. **8** (2008), no. 1, 111–118. arXiv:`math/0503564v2 [math.QA]`.

[O5] V. Ostrik, *Module Categories Over the Drinfeld Double of a Finite Group*, Int. Math. Res. Not. IMRN **27** (2003), 1507–1520. arXiv:`math/0202130v2 [math.QA]`.

[OEIS] *Online Encyclopedia of Integer Sequences*, 2013, Available at: `http://oeis.org/`.

[P1] J. Preskill, *Lecture Notes for Physics 219: Quantum Computation*, (June 2004), Available at:
`http://www.theory.caltech.edu/~preskill/ph219/topological.pdf`.

[PCo1] P. Bonderson, *Private Communication*, Oct. 2012.

[RCo1] E. Rowell, *Private Communication*, 2012.

[RR1] N. Read and E. Rezayi, *Beyond Paired Quantum Hall States: Parafermions and Incompressible States in First Excited Landau Level*, Phys. Rev. B **59** (1999), 8804. arXiv:`cond-mat/9809384`.

[RSW] E. Rowell, R. Stong, and Z. Wang, *On Classification of Modular Tensor Categories*, Comm. Math. Phys. **292** (2009), no. 2, 343–389. arXiv:`0712.1377v4 [math.QA]`.

[RW1] E. C. Rowell and Z. Wang, *Localization of Unitary Braid Group Represenations*, Comm. Math. Phys. **311** (2012), no. 3, 595–615. arXiv:`1009.0241v2 [math.RT]`.

[S1] J. A. Siehler, *Braided Near-Group Categories*, (2000). arXiv:`math/0011037v1 [math.QA]`.

[St1] W. Stein, *Introduction to Algebraic Number Theory*, 2005, Available at: `http://modular.math.washington.edu/129-05/notes/129.pdf`.

[SV1] A. Schmidt and U. Vollmer, *Polynomial Time Quantum Algorithm for the Computation of the Unit Group of a Number Field*, In Proceedings of the 37th AMC Symposium on the Theory of Computing (2005), 475–480.

[Ta1] T. Takenouchi, *On an Indeterminate Equation*, Proceedings of the Physico-Mathematical Society of Japan **3** (1921), 78–92.

[TCo1] T. J. Hagge, *Private Communication*, Mar. 2013.

[Tu1] V. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, De Gruyter Studies in Mathematics, no. 18, Walter de Gruyter, Berlin, DE, 1994.

[W1] Z. Wang, *Topological Quantum Computation*, CBMS Regional Conference Series in Mathematics, no. 112, Amer. Mathematical Society, Providence, RI, 2010.

[W2] Z. Wang, *Quantum Computing: A Quantum Group Approach*, (2013). arXiv:`1301.4612v1 [math.QA]`.

[W3] Z. Wang, *Topologization of Electron Liquids with Chern-Simons Theory and Quantum Computation*, Nankai Tracts Math. **10** (2006), 106–120. arXiv:`cond-mat/0601285v1`.

[Wal1] K. Walker, *TQFTs version 1h*, (May 2006).

[Wal2] K. Walker, *On Witten's 3-Manifold Invariants*, Feb. 1991, Available at: `http://canyon23.net/math/1991TQFTNotes.pdf`.

[WalCo1] K. Walker, *Private Communication*, Oct. 2012.

[We1] E. Weiss, *Algebraic Number Theory*, Second (unaltered) Edition, Chelsea Publishing Company, New York, NY, 1976.

[Wi1] F. Wilczek, *Fractional Statistics and Anyon Superconductivity*, World Sci. Publ., Singapore, Dec. 1990.

[WW1] K. Walker and Z. Wang, *(3+1)-TQFTS and Topological Insulators*, (2011). arXiv:`1104.2632v2 [cond-mat.str-el]`.

APPENDIX A
NUMBER THEORY BACKGROUND

In broad strokes, modern number theory attempts to understand generalizations of the rational field $\mathbb{Q}$ called algebraic number fields and generalizations of the ring of integers, $\mathbb{Z}$, in $\mathbb{Q}$. In this section, a brief overview of algebraic number theory will be given. This section is not meant to be comprehensive. A complete accounting can be found in [Mi1; St1; Mi2; Ch1].

An **algebraic number field** is a field $\mathbb{Q}(\theta)$ where θ is algebraic over $\mathbb{Q}$, that is θ satisfies some monic polynomial $f \in \mathbb{Q}[x]$. Algebraic number fields, $\mathbb{K} = \mathbb{Q}(\theta)$, are finite dimensional $\mathbb{Q}$-vector spaces. For algebraic reasons arising from Galois Theory, the dimension of $\mathbb{K}$ as a $\mathbb{Q}$-vector space is denoted $[\mathbb{K} : \mathbb{Q}]$ and is called the **degree** of $\mathbb{K}$ over $\mathbb{Q}$. The smallest degree monic polynomial $f \in \mathbb{Q}[x]$ such that $f(\theta) = 0$ is called the **minimal polynomial** of θ and its degree is $n = [\mathbb{K} : \mathbb{Q}]$. The field is said to be a **cyclotomic extension** if $\theta = \zeta$, a root of unity in $\mathbb{C}$.

Much of the study that has been done for the rationals has revolved around the integers $\mathbb{Z} \subset \mathbb{Q}$. The study of the integers has had a wide range of applications dating back to ancient Greece where Diophantus studied integral solutions to algebraic equations. To this day, this class of equations bears his name and are called **Diophantine equations**. One of the most powerful applications of algebraic number theory is in the study of Diophantine equations over a number field $\mathbb{K}$; that is the study of equations whose solutions are required to be some sort of "integer" in $\mathbb{K}$. This **ring of integers** is denoted by $\mathcal{O}_{\mathbb{K}}$ and consists of all elements $\alpha \in \mathbb{K}$ whose minimal polynomial has coefficients in $\mathbb{Z}$. This naturally generalizes the integers in $\mathbb{Q}$. Indeed, an element $a \in \mathbb{Q}$ is an integer if and only if its minimal polynomial is $f(x) = x - a \in \mathbb{Z}[x]$. Just as $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, so is $\mathbb{K}$ the field of fractions of $\mathcal{O}_{\mathbb{K}}$. Moreover, the presence of a $\mathbb{Q}$–basis of $\mathbb{K}$ allows one to deduce the existence of a $\mathbb{Z}$–basis $\{b_1, \ldots, b_n\}$ of $\mathcal{O}_{\mathbb{K}}$. Typically, the determination of the b_j is a difficult problem, but in the cyclotomic setting one has $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.

A number field $\mathbb{K}$ is a finite dimensional extension of $\mathbb{Q}$ and hence can be viewed as a subfield of $\mathbb{C}$. However, there are often many ways to embed $\mathbb{K}$ into $\mathbb{C}$. In fact, it can be shown that there are $n = [\mathbb{K} : \mathbb{Q}]$ distinct embeddings. Such an embedding is said to be **real** if the image of $\mathbb{K}$ is in $\mathbb{R}$ and is **complex** otherwise. One can easily show that the complex embeddings always arise in conjugate pairs. Throughout this section, r_1 will denote the number of real embeddings of $\mathbb{K}$ and r_2 the number of conjugate pair embeddings. Moreover, these embeddings will be denoted by σ_j and ordered such that the first r_1 embeddings are real, the next r_2 embeddings are distinct (under conjugation) complex embeddings, and the final r_2 embeddings satisfy $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for $1 \leq j \leq r_2$. These embeddings are quite useful and can be used to generate certain functions on $\mathbb{K}$ and $\mathcal{O}_{\mathbb{K}}$. The most common such functions are the **trace** and the **norm** which are are respectively given by:

$$T_{\mathbb{K}/\mathbb{Q}}\left(x\right)=\sum_{j=1}^{n}\sigma_j\left(x\right)\quad\text{and}\quad N_{\mathbb{K}/\mathbb{Q}}\left(x\right)=\prod_{j=1}^{n}\sigma\left(x\right)$$

Remark A.0.13. When the field $\mathbb{K}$ under consideration is clear from context, the norm and trace are often simply denoted by $N\left(\alpha\right)=N_{\mathbb{K}/\mathbb{Q}}\left(\alpha\right)$ and $T\left(\alpha\right)=T_{\mathbb{K}/\mathbb{Q}}\left(\alpha\right)$ respectively.

Since the embeddings σ_j are field homomorphims, it is clear that

$$T_{\mathbb{K}/\mathbb{Q}}\left(x+y\right)=T_{\mathbb{K}/\mathbb{Q}}\left(x\right)+T_{\mathbb{K}/\mathbb{Q}}\left(y\right)\quad\text{and}\quad N_{\mathbb{K}/\mathbb{Q}}\left(xy\right)=N_{\mathbb{K}/\mathbb{Q}}\left(x\right)N_{\mathbb{K}/\mathbb{Q}}\left(y\right)$$

Furthermore, it can be shown that the trace and the norm of an integer in $\mathbb{K}$ are rational integers. This allows us to use the norm to identify the units $\mathcal{O}_{\mathbb{K}}^{\times}$ in the ring $\mathcal{O}_{\mathbb{K}}$. Indeed, these properties immediately imply that $x\in\mathcal{O}_{\mathbb{K}}^{\times}$ if and only if $N_{\mathbb{K}/\mathbb{Q}}\left(x\right)=\pm1$.

The trace can be used to define an invariant of the field $\mathbb{K}$ known as the **discriminant** of $\mathbb{K}$ defined by

$$\Delta_{\mathbb{K}}=\det\left(\sigma_j\left(b_k\right)\right)^2=\det\left(T_{\mathbb{K}/\mathbb{Q}}\left(b_jb_k\right)\right)$$

for an integral basis $\{b_1,\ldots,b_n\}$ of $\mathcal{O}_{\mathbb{K}}$. It can be shown that $\Delta_{\mathbb{K}/\mathbb{Q}}\in\mathbb{Z}$ and that this integer has geometric significance. Indeed, if $\mathcal{O}_{\mathbb{K}}$ is viewed as a lattice under the embedding $\sigma:\mathbb{K}\hookrightarrow\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ given by $\sigma\left(x\right)=\left(\sigma_1\left(x\right),\ldots,\sigma_n\left(x\right)\right)$ then, its co-volume is proportional to $\sqrt{\left|\Delta_{\mathbb{K}/\mathbb{Q}}\right|}$. This makes clear the fact that the discriminant is independent of the integral basis chosen to compute it.

In $\mathbb{Z}$, primes are integers and every integer admits a unique factorization. These two facts can be traced to the statement that $\mathbb{Z}$ is a principal ideal domain and hence, a unique factorization domain. This is not generally true, e.g. $\mathcal{O}_{\mathbb{Q}(\zeta_{23})}$. What is true is that $\mathcal{O}_{\mathbb{K}}$ is a Dedekind domain and hence ideals admit unique factorizations into prime ideals, $\mathfrak{a}=\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_k^{a_k}$. This is analogous to factorization in $\mathbb{Z}$. Indeed, in $\mathbb{Z}$, any integer $m\in\mathbb{Z}$ corresponds to a principal ideal $m\mathbb{Z}$ which can be uniquely factored into prime ideals $\left(p_1\mathbb{Z}\right)^{a_1}\cdots\left(p_k\mathbb{Z}\right)^{a_k}$ where $a_j\in\mathbb{Z}$ and p_j are prime rational integers. However, one can go further, over $\mathbb{Q}$ one has statements such as $\frac{6}{35}=2\times3\times5^{-1}\times7^{-1}$. Due to the lack of unique factorization, such a statement cannot be made in a general number field, $\mathbb{K}$. However, the concept of such a rational factorization can be abstracted to ideals. This leads to the notion of a fractional ideal. Just as an ideal of $\mathbb{K}$ is a $\mathcal{O}_{\mathbb{K}}$-submodule of $\mathcal{O}_{\mathbb{K}}$, a **fractional ideal**, $\mathfrak{a}$, is a $\mathcal{O}_{\mathbb{K}}$-submodule of $\mathbb{K}$ such that $\exists\alpha\in\mathcal{O}_{\mathbb{K}}$ with $\alpha\mathfrak{a}\subset\mathcal{O}_{\mathbb{K}}$. For instance, $\frac{1}{2}\mathbb{Z}$ is a fractional ideal in $\mathbb{Q}$ with $\alpha=2$. The aforementioned factorization of ideals extends to fractional ideals in the obvious way: if $\mathfrak{a}$ is a fractional ideal of $\mathbb{K}$, then $\exists$ prime ideals $\mathfrak{p}_j$ and integers a_j such that $\mathfrak{a}=\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_k^{a_k}$.

It can be shown that prime ideals $\mathfrak{p}$ have finite residue fields $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$. The finiteness of these fields allows one to extend the norm on $\mathbb{K}$ to prime ideals by:

$$N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}) := \#\left(\mathcal{O}_{\mathbb{K}}/\mathfrak{p}\right)$$

This norm can then be extended to arbitrary fractional ideals $\mathfrak{a}$, through the prime factorization $\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_k^{a_k}$, by

$$N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a}) = N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_1)^{a_1}\cdots N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_k)^{a_k}$$

Remark A.0.14. The norm here is viewed as an element of $\mathbb{Q}$, not a fractional ideal. This convention will persist when we extend norms to ideals. Since our base field is $\mathbb{Q}$, there is no loss of generality in doing this. However, some authors will call such a norm the **numeric norm**.

The study of primes and prime factorization in fields is a very rich subject, and is typically explored through ramification theory. We will not need the details of this theory in this work, but many of the results from Section III.3 can be recast in ramification theory. For instance, a great deal of Proposition III.3.2 can be arrived at through such a study. The interested reader is encouraged to consult [Ch1] for an excellent discussion of ramification.

A great deal of effort has gone into the study of cyclotomic fields given their intimate relation with Fermat's Last Theorem. One might hope that the theory of cyclotomic fields can be applied to study other fields. For instance, cyclotomic fields are abelian and if one can realize an abelian extension as a subfield of a cyclotomic field, then it may be possible to apply some of the theory of cyclotomic fields. This leads to the natural question: *If $\mathbb{K}$ is an abelian extension of $\mathbb{Q}$, when is $\mathbb{K}$ contained in a cyclotomic extension of $\mathbb{Q}$ and what features of $\mathbb{K}$ are captured by such an inclusion?* Such questions gave birth to the beautiful subject of Class Field Theory. One of the fundamental results is the Kronecker-Weber theorem which says:

Theorem A.0.15 (Kronecker-Weber)**.** *If $\mathbb{K}$ is an abelian extension of $\mathbb{Q}$, then there exists an integer m such that $\mathbb{K} \subset \mathbb{Q}(\zeta_m)$.*

Class Field Theory goes further and amongst other things, characterizes extensions of $\mathbb{K}$ which are totally unramfied, as well as gives a reciprocity law (Artin Reciprocity) which encompasses many of the previously known laws such as quadratic reciprocity. We will not need the full power and sophistication of Class Field Theory here. However, one notion is quite useful. That is, if $\mathbb{K}$ is an abelian number field, then the Kronecker-Weber theorem guarantees that $\mathbb{K}$ is contained in a cyclotomic extension. Given that such cyclotomic fields exist there is a minimal extension, $\mathbb{Q}(\zeta_k)$ which deserves special attention. The integer k is known as the **conductor** of $\mathbb{K}$ and is typically denoted by $\mathfrak{f}(\mathbb{K})$. Like many classical notions, the conductor has a sophisticated generalization in the context of Class Field Theory, but again this extra level of complexity will not be required. However, we will retain the notation for the conductor, $\mathfrak{f}(\mathbb{K})$, for uniformity. The conductor of the field can be used to capture a lot of information about the field such as the structure of certain prime factorizations and certain character groups. For instance, one can show:

Proposition A.0.16. *If $\mathbb{K}$ is an abelian number field with conductor $\mathfrak{f}(\mathbb{K})$ and discriminant $\Delta(\mathbb{K})$, then a rational prime divides $\mathfrak{f}(\mathbb{K})$ if and only if it divides $\Delta_{\mathbb{K}}$.*