University of California
Santa Barbara

Congruence subgroups from quantum representations of mapping class groups

A dissertation submitted in partial satisfaction
of the requirements for the degree

Doctor of Philosophy
in
Mathematics

by

Joseph J. Ricci

Committee in charge:

Professor Zhenghan Wang, Chair
Professor Darren Long
Professor Jon McCammond

June 2018

The Dissertation of Joseph J. Ricci is approved.

Professor Darren Long

Professor Jon McCammond

Professor Zhenghan Wang, Committee Chair

June 2018

Congruence subgroups from quantum representations of mapping class groups

by

Joseph J. Ricci

Acknowledgements

I would like to thank my advisor Zhenghan Wang for his endless insight and optimism. I could not be more gracious for his input and guidance throughout working on this thesis and my time at UCSB.

I would like to thank Darren Long and Jon McCammond, the other members of my committee. I am honored and humbled to have been a student of such brilliant mathematicians.

I would like to thank my mathematical siblings Colleen Delaney and Wade Bloomquist. Also, a special thanks is due to my friends Micheal Dougherty, and Steve Trettel.
I would like to thank the UCSB Mathematics Department for its support (financial and otherwise) over the last five years and particularly Medina Price for being the most supportive person in the world.

I would like to thanks my family for their unending encouragement since I was a child. Lastly, and perhaps most importantly, I want to thank my two best girls, Bella and Tereza, for always putting a smile on my face after a long day and for sticking with me these past few years.

Joseph Ricci

ricci@math.ucsb.edu
math.ucsb.edu/~ricci

RESEARCH INTERESTS

Quantum topology and algebra, modular tensor categories.

EDUCATION

Ph.D., Mathematics
University of California, Santa Barbara, CA, Expected June 2018
Thesis Advisor: Zhenghan Wang
Thesis Title: *Congruence subgroups from quantum representations of mapping class groups.*

M.A., Mathematics
University of California, Santa Barbara, CA, June 2015

M.A., Mathematics
State University of New York at Buffalo, Buffalo, NY, May 2013

B.S. with Honors, Mathematics
State University of New York at Buffalo, Buffalo, NY, February 2012
Thesis Advisor: David Hemmer
Thesis Title: *Decomposing induced characters of the centralizer of an n-cycle in the symmetric group on $2n$ elements.*

PUBLICATIONS

"Congruence subgroups from representations of the three-strand braid group." Journal of Algebra, Vol 487, 1 October 2017, 93-117.

"Decomposing induced characters of the centralizer of an n-cycle in the symmetric group on $2n$ elements." Involve, Vol. 6 (2013), No. 2, 221-232.

TEACHING EXPERIENCE

At UCSB:

Teaching Assistant

- Differential Equations (Winter 2016)
- Vector Calculus I (Winter 2016)
- Calculus II (Fall 2013, Winter 2014, Fall 2014, Summer 2015, Fall 2015, Summer 2016, Fall 2016, Winter 2017)
- Linear Algebra (Spring 2014)
- Transition to Higher Mathematics (Winter 2015)

Instructor

- Differential Equations (Summer 2014)

At SUNY Buffalo:

Teaching Assistant

- Calculus I (Fall 2011, Fall 2012)
- Calculus II (Spring 2012, Summer 2012, Fall 2012)
- Linear Algebra (Summer 2012)
- Abstract Algebra (Spring 2013)

Instructor

- Calculus for Social Sciences II (Summer 2013)

HONORS AND AWARDS

RTG Fellowship in Geometry-Topology (NSF, UCSB, Spring 2016)
Nominated for Outstanding Teaching Assistant Award (UCSB, 2014)
Hazel and John Wilson Scholarship (SUNY Buffalo Dept. of Math, 2011)

TALKS GIVEN

Invited and Research Talks

- *Non-congruence subgroups from weakly integral anyons* (AMS Sectional Meeting, UI-Bloomington, Indiana, 2017)
- *Congruence subgroups from low-dimensional representations of the braid group* (Knots in Hellas, Ancient Olympia, 2016)

Local Seminar Talks

- *Where does the group go?* (UCSB Quantum Topology Seminar, 2016)
- *Egyptian fractions, Kellogg's qquation, and finite group representations* (UCSB Discrete Geometry Seminar, 2015)
- *Classifying Local Representations of the Braid Group* (UCSB Discrete Geometry Seminar, 2015)
- *Represenations of the Braid Group* (UCSB Discrete Geometry Seminar, 2014)
- *Young Tableaux and Representations of the Symmetric Group* (UCSB Discrete Geometry Seminar, 2014)
- *Hopf Algebras and Monoidal Categories* (UCSB Graduate Category Theory Seminar, 2014)
- *Braid Groups* (UCSB Graduate Algebra Seminar, 2014)
- *Quandles* (UCSB Graduate Algebra Seminar, 2013)

CONFERENCES ATTENDED

- West Coast Lie Theory Workshop, San Diego, CA (2017)
- American Mathematical Society Section Meeting, Bloomington, IN (2017)
- Knots in Hellas 2016, Ancient Olympia, Greece (2016)
- UCB/UCSB Algebra Day, Berkeley, CA (2015)
- Graduate Geometry and Topology Conference, Syracuse, NY (2013)

Abstract

Congruence subgroups from quantum representations of mapping class groups

by

Joseph J. Ricci

Ng and Schauenburg proved that the kernel of a $(2+1)$-dimensional topological quantum field theory representation of $\mathrm{SL}(2,\mathbb{Z})$ is a congruence subgroup. Motivated by their result, we explore when the kernel of an irreducible representation of the braid group B_3 with finite image enjoys a congruence subgroup property. In particular, we show that in dimensions two and three, when the projective order of the image of the braid generator σ_1 is between 2 and 5 the kernel projects onto a congruence subgroup of $\mathrm{PSL}(2,\mathbb{Z})$ and compute its level. However, for each odd integer r equal to at least 5, we construct a pair of non-congruence subgroups associated with three-dimensional representations. Our techniques use classification results of low dimensional braid group representations and the Fricke-Wohlfarht theorem in number theory, as well as Tim Hsu's work on generating sets for the principal congruence subgroups of $\mathrm{PSL}(2,\mathbb{Z})$.

Contents

Chapter 1

Introduction

The double cover $\mathrm{SL}(2,\mathbb{Z})$ of the modular group $\mathrm{PSL}(2,\mathbb{Z})$ naturally occurs in quantum topology as the mapping class group of the torus. Let $\Sigma_{g,n}$ be the orientable genus g surface with n punctures and denote by $\mathrm{Mod}(\Sigma_{g,n})$ its mapping class group. A (2+1)-dimensional topological quantum field theory (TQFT) or equivalently a modular tensor category affords a projective representation of $\mathrm{Mod}(\Sigma_{g,n})$ which we refer to as a quantum representation. An amazing theorem of Ng and Schauenburg [NS10] says that the kernel of a quantum representation of $\mathrm{SL}(2,\mathbb{Z})$ is always a congruence subgroup. The modular group is also disguised as the three-strand braid group B_3 through the central extension:

$$1 \to \langle (\sigma_1\sigma_2)^3 \rangle \to B_3 \to \mathrm{PSL}(2,\mathbb{Z}) \to 1.$$

Each simple object of the modular tensor category $\mathcal{C}$ associated to a $(2+1)$-TQFT gives rise to a representation of B_3. Are there versions of the Ng-Schauenburg congruence kernel theorem for those braid group representations? We initiate a systematical investigation of this problem and find that a naive generalization does not hold.

To pass from a quantum representation of B_3 to one of the modular group $\mathrm{PSL}(2, \mathbb{Z})$, we consider only irreducible representations $\rho_X : B_3 \to \mathrm{GL}(d, \mathbb{C})$ associated to a simple object X of a modular tensor category $\mathcal{C}$. Then the generator $(\sigma_1\sigma_2)^3$ of the center of B_3 acts by a scalar of finite order. By tensoring ρ_X with a root of unity, we obtain a representation of the modular group $\overline{\rho}_X : \mathrm{PSL}(2, \mathbb{Z}) \to \mathrm{GL}(d, \mathbb{C})$. According to the property F conjecture, the representations ρ_X should have finite images if the squared quantum dimension d_X^2 of X is an integer. So, to generalize the Ng-Schauenburg result, it makes sense to look at simple objects with Property F. For the Ising anyon σ, the kernel is indeed a congruence subgroup, but the kernel for the anyon denoted as G in $D(S_3)$ is not [CHW15]. Therefore, when a Property F anyon has a congruence subgroup property is more subtle. In this paper we systematically explore the low dimensional irreducible representations of B_3 with finite images, and determine when the kernel is a congruence subgroup.

In addition to the intrinsic mathematical interest, this research has potential application in physics. Topological quantum computation relies on braiding anyons and so unitary representations of braid groups arise naturally here. The matrices contained in the image of a B_3 representation can also be used as quantum gates for topological quantum computations. Therefore, the congruence property of B_3 representations might even find application to quantum information processing [Wan10]. Whether the kernel is a congruence or non-congruence subgroup may relate to some interesting properties of the associated gate set.

Another motivation of this research is to study the vector-valued modular forms (VVMF) associated to congruence subgroups (see [Gan14] and the references therein). VVMFs provide deep insight for the study of TQFTs and conformal field theories (CFTs). Since the general VVMF theory applies also to non-congruence subgroups, TQFT representations of B_3 provide interesting test ground of the theory and conversely, VVMF could provide deep insight into the study of the TQFT representations of B_3 even in the non-congruence case.

Our main results essentially come in two varieties. First, for two or three-dimensional representations of B_3 with finite image such that the projective order of σ_1 is less than 5, we are able to prove that the kernel is always a congruence subgroup. On the other hand, we provide a construction for non-congruence subgroups associated to three-dimensional representations of B_3. In fact, for any odd integer r equal to 5 or more, we can construct representations such that σ_1 maps to an element of order $2r$ and the kernel is a non-congruence subgroup. Therefore, the uniformity exhibited in the Ng-Schauenburg theorem does not extend to quantum representation of B_3.

Let us summarize the structure of this work. In chapter 2, we introduce the machinery required to define the our so-called quantum representations. In the case of quantum representations of the braid group, our construction admits a pictorial description of the representations compatible with the definition of the braid group as a group of braid diagrams with the operation of stacking. Two formulations are provided; one using categorical language and one using $6j$ symbols.

In chapter 3, the language of congruence subgroups of the modular group is introduced. To every finite index subgroup of the modular we can associate an integer called the geometric level. It turns out that the geometric level is a central ingredient in proving our main results. In this chapter we also prove the Fricke-Wohlfahrt theorem and, combined with the work of Hsu, we establish a criterion for determining when a finite index subgroup of the modular group is a congruence subgroup which requires only checking a few equalities. This is easily programmed by a computer, for instance.

In chapter 4, we record the results of Rowell, Tuba, and Wenzl which will important tools for our classification. Then we are able to prove our main results. First, we explore representations in dimension two. After a series of reductions, we find there are only a small number of equivalence classes of representations that satisfy the conditions we are interested in and show each one has a kernel that projects onto a congruence subgroup of $\mathrm{PSL}(2,\mathbb{Z})$. The story is similar in dimension three for those representations mapping σ_1 to a matrix of projective order less than 6, but fails to persist for all irreducibles.

In chapter 5, we explore our results within the context of the Property F conjecture. Whenever X is a Property F anyon, the kernels of the afforded representations of B_3 are either congruence or non-congruence subgroups. Therefore we can classify anyons as either congruence or non-congruence type.

In chapter 6, we provide some directions in which to take this work and some potential areas of application. It could be interesting to understand the role of the congruence property of a representation when it is the multiplier of a vector-valued modular form. Another option could be to explore vector-valued modular forms which are invariant in some sense with respect to a finite index subgroup of the modular group and understand how the congruence property fits into this theory.

Chapter 2

Quantum representations of mapping class groups

In this chapter we will define the notion of a fusion category, which can be regarded as the quantum version of a finite group. There are several equivalent ways of defining a fusion category. One approach is using categorical language, which is elegant but leaves calculations difficult. Another approach is using 6j symbols which naturally allows for explicit calculations. This is analogous to defining a connection in differential geometry either coordinate-free or with Christoffel symbols. Since we have application to quantum computation in mind we will go the route of $6j$ symbols. We will see that a braided $6j$ fusion system (and therefore equivalently a braided fusion category) amounts to a collection of complex numbers that determine the matrix entries to certain representations of the braid groups, regarded as the mapping class group of the marked disc. Our goal will be to keep track of this data diagrammatically using objects called fusion trees. If the braiding additionally satisfies a certain non-degeneracy condition, the data of the fusion system also defines representations of the mapping class groups surfaces with genus.

2.1 6j fusion systems

A $6j$ fusion system axiomatizes the numerical data that goes along with the categorical definition of a fusion category. First, we will define a label set, which behaves similar to a group.

Definition 2.1.1 *A* **label set** *is a finite set L together with a distinguished element 1 and an involution $(-)^* : L \to L$ such that $1^* = 1$. Elements of L are called* **labels** *and 1 is called the* **trivial label***. The map $(-)^*$ is called the* **duality***.*

A fusion rule is the generalization of the binary product that is a part of a group structure. However, a fusion rule allows us to combine two elements of a label set and outputs a sum of a labels rather than a single label.

Definition 2.1.2 *Denote by $\mathbb{N}^L$ the set of functions from L to $\mathbb{N}$. A function $-\otimes- : L \times L \to \mathbb{N}^L$ is called a* **fusion rule** *if it satisfies the following conditions. First let us make some notation. Given two labels a and b, formally write $a \otimes b = \oplus N_{ab}^c c$ where $N_{ab}^c = (a \otimes b)(c)$. When no confusion can arise, we will write ab instead of $a \otimes b$. Using this notation, $-\otimes-$ is a fusion rule if for all $a, b, c, d \in L$:*

(i) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$, *that is,*

$$\sum_{x \in L} N_{ab}^x N_{xc}^d = \sum_{x \in L} N_{bc}^x N_{ax}^d$$

(ii) $N_{a1}^c = N_{1a}^c = \delta_{ca}$.

(iii) $N_{ab}^1 = N_{ba}^1 = \delta_{ba^*}$.

A fusion rule is called **multiplicity-free** *if $N_{ab}^c \in \{0, 1\}$ for all $a, b, c \in L$. We will be primarily discussing multiplicity-free fusion rules (and will emphasize those which are not when they arise).*

A triple of labels (a, b, c) is **admissible** if $N_{ab}^{c} \neq 0$. An **automorphism** of a fusion rule is a permutation α of L satisfying

$$N_{\alpha(x)\alpha(y)}^{\alpha(z)} = N_{xy}^{z}$$

for all $x, y, z \in L$.

Example 2.1.3 *Every finite group G gives rise to a label set and fusion rule by setting $L = G$, the trivial label to be the group identity, $g^* = g^{-1}$, and $g \otimes h = gh$. Such systems arise via the representation category of a finite abelian group.*

Example 2.1.4 *This example is due to Tambara and Yamagami [see [TY98]]. Given a finite group G, let m be some symbol not appearing as an element of G. Then we get a fusion rule on the label set $L = G \sqcup \{ m \}$ given by*

$$g \otimes h = gh, \quad m \otimes g = g \otimes m = m, \quad m \otimes m = \oplus_{g \in G} g$$

for $g, h \in G$.

Example 2.1.5 *When $G = \mathbb{Z}_2$ in the example above, the resulting fusion rule is called the Ising fusion rule. The 3 elements of the label set are usually denoted $\{ 1, \sigma, \psi \}$ in the literature where 1 is the trivial label. The fusion rules take the form*

$$\sigma \otimes \sigma = 1 \oplus \psi, \quad \psi \otimes \psi = 1, \quad \sigma \otimes \psi = \psi \otimes \sigma = \sigma.$$

Although quite simple, this fusion rule is quite important. It is closely related to the Chern-Simmons-Witten $\mathrm{SU}(2)$-TQFT at level 2 or equivalently the purification of $\mathrm{Rep}\, U_q\mathfrak{sl}_2\,\mathbb{C}$ where q is an appropriate choice of 16th root of unity. It *arises as a Temperley-Lieb-Jones algebroid with Kauffman variable* $A = ie^{-\pi i/16}$ *[see [Wan10]].*

Example 2.1.6 *For this example, we must first give a few definitions. Let* H *be a* $\mathbb{C}$*-algebra. Then* $H \otimes H$ *inherits a natural algebra structure, as do the higher tensor powers of* H*. An algebra homomorphism* $\Delta : H \to H \otimes H$ *is called a comultiplication. For an element* x *of* H*, we will write* $\Delta(x) = \sum_{(x)} x' \otimes x''$ *(this is called Sweedler notation). An algebra homomorphism* $\varepsilon : H \to \mathbb{C}$ *is called a counit and can also be viewed as a one-dimensional representation of* H*. Let* H *be an algebra,* Δ *a comultiplication,* ε *a counit,* $\Phi = \sum_i x_i \otimes y_i \otimes z_i$ *an invertible element of* $H \otimes H \otimes H$*, and* ℓ, r *invertible elements of* H*. Then the tuple* $(H, \Delta, \varepsilon, \Phi, \ell, r)$ *is a* ***quasi-bialgebra*** *if for all* $x \in H$*:*

(i) $(\mathrm{id} \otimes \Delta)(\Delta(x)) = \Phi((\Delta \otimes \mathrm{id})(\Delta(x)))\Phi^{-1}$,

(ii) $(\varepsilon \otimes \mathrm{id})(\Delta(x)) = \ell^{-1} a \ell, \quad (\mathrm{id} \otimes \varepsilon)(\Delta(x)) = rar^{-1}$,

(iii) $(\mathrm{id} \otimes \mathrm{id} \otimes \Delta)(\Phi)(\Delta \otimes \mathrm{id} \otimes \mathrm{id})(\Phi) = \Phi_{234}(\mathrm{id} \otimes \Delta \otimes \mathrm{id})(\Phi)\Phi_{123}$,

(iv) $(\mathrm{id} \otimes \varepsilon \otimes \mathrm{id})(\Phi) = r \otimes \ell^{-1}$

where $\Phi_{123} = \Phi \otimes 1$ *and* $\Phi_{234} = 1 \otimes \Phi$*. This is reminiscent of the definition of bialgebra with the generalization that the comultiplication is not coassociative. Instead, it is replace by the associator conditions involving* Φ*. The element* Φ *is sometimes called the Drinfeld associator of* H*. Suppose further* S *is an anti-automorphism of* H *and there are elements* a *and* b *in* H *such that for all* $x \in H$

$$\sum_{(x)} S(x')ax'' = \varepsilon(x)a, \quad \sum_{(x)} x'bS(x'') = \varepsilon(x)b$$

and

$$\sum_i x_i b S(y_i) a z_i = 1, \quad \sum_i S(\bar{x}_i) a \bar{y}_i b S(\bar{z}_i) = 1,$$

where $\Phi^{-1} = \sum_i \bar{x}_i \otimes \bar{y}_i \otimes \bar{z}_i$. *Then we call the tuple* $(H, \Delta, \varepsilon, \Phi, \ell, r, S, a, b)$ *a* ***quasi-Hopf algebra****. Again, the definition here is similar to a traditional Hopf algebra but it slightly more general. When the structure maps of a quasi-bialgebra or quasi-Hopf algebra is clear or not explicitly needed we will just refer to it by the underlying algebra. Let* H *be a semisimple quasi-Hopf algebra with finitely many isomorphism classes of irreducible representations, say represented by* $V_1, \ldots, V_n$ *where* V_1 *is the trivial representation induced by the counit of* H*. When* V *and* W *are representations of* H*, the comultiplication and antipode of* H *turn* $V \otimes W$ *and* V^* *into representations of* H *too. Since* H *is semisimple, we know that there are non-negative integers* $N_{i,j}^k$ *so that for all* i *and* j *we can write* $V_i \otimes V_j \cong \oplus_k V_k^{\oplus N_{i,k}^k}$*. Then we can obtain a label set and fusion rule by taking* $L = \{1, \ldots, n\}$*, the trivial label to be 1, and the fusion rule* $i \otimes j = \oplus_k N_{i,j}^k k$*. The duality is determined by taking the dual representation of* V_i*. In this case a triple* (i, j, k) *is admissible if and only if an isomorphic copy of* V_k *appears in the decomposition of* $V_i \otimes V_j$ *into its irreducible summands.*

One way to produce a lot of examples of quasi-Hopf algebras is using the quantum double construction, due to Drinfeld ([Dri90]). Let G *be a finite group. There is a quasi-Hopf algebra denoted* $D(G)$*, whose underlying algebra structure is that of* $\mathbb{C}[G] \otimes \mathbb{C}[G]^*$*. In particular, a basis of* $D(G)$ *can identified with tensors of the form* $g \otimes \delta_h$ *where* $g \in G$ *and* $\delta_h(k) = \delta_{h,k}$*. The quasi-Hopf alegbra structure of* $D(G)$ *is well known, as it its representation theory. In particular,* $D(G)$ *is semisimple and its irreducible representations are parameterized by pairs* (C_g, Π)

where C_g is the conjugacy class of some $g \in G$ and Π is an irreducible representation of the centralizer of g.

In their paper [[CHW15]], the authors examined the case of $G = S_3$, the symmetric group on three elements. The conjugacy classes of S_3 are $C_e = \{ e \}$, $C_{(12)} = \{ (12), (13), (23) \}$, and $C_{(123)} = \{ (123), (132) \}$ and the respective centralizers of interest are isomorphic to S_3, $\mathbb{Z}_2$, and $\mathbb{Z}_3$ respectively. The three irreducible representations of $D(S_3)$ corresponding to S_3 are labelled A, B, C where A is the trivial representation, and B and C correspond to sign and 2-dimensional representations. Continuing, the letters D and E are used for the two irreps 1 and -1 coming from $\mathbb{Z}_2$ and finally F, G, H are used to label the three irreducibles corresponding to the trivial, $e^{2\pi i/3}$ and $e^{4\pi i/3}$ representations of $\mathbb{Z}_3$. Thus, we get a label set $L = \{ A, B, C, D, E, F, G, H \}$. The fusion rules are listed below.

$\otimes$	A	B	C	D	E	F	G	H
A	A	B	C	D	E	F	G	H
B	B	A	C	E	D	F	G	H
C	C	C	$A \oplus B \oplus C$	$D \oplus E$	$D \oplus E$	$G \oplus H$	$F \oplus H$	$F \oplus G$
D	D	E	$D \oplus E$	$A \oplus C \oplus F \oplus G \oplus H$	$B \oplus C \oplus F \oplus G \oplus H$	$D \oplus E$	$D \oplus E$	$D \oplus E$
E	E	D	$D \oplus E$	$B \oplus C \oplus F \oplus G \oplus H$	$A \oplus C \oplus F \oplus G \oplus H$	$D \oplus E$	$D \oplus E$	$D \oplus E$
F	F	F	$G \oplus H$	$D \oplus E$	$D \oplus E$	$A \oplus B \oplus F$	$H \oplus C$	$G \oplus C$
G	G	G	$F \oplus H$	$D \oplus E$	$D \oplus E$	$H \oplus C$	$A \oplus B \oplus G$	$F \oplus C$
H	H	H	$F \oplus G$	$D \oplus E$	$D \oplus E$	$G \oplus C$	$F \oplus C$	$A \oplus B \oplus H$

We will be interested in this example throughout this work and refer back to it from time to time.

The label set and fusion rule correspond to the isomorphism classes of simple objects and tensor product of a fusion category. Another ingredient is the associativity of the tensor product which is captured below.

Definition 2.1.7 *Let L be a label set with a fixed fusion rule. A sextuple of labels (a,b,c,d,n,m) is* **admissible** *if (a,b,m), (m,c,d), (b,c,n), and (a,n,d) are all admissible. Given a function $F : L^6 \to \mathbb{C}$, we write $F^{abc}_{d;nm}$ for $F(a,b,c,d,n,m)$ and F^{abc}_{d} for the matrix with (n,m)-entry $F^{abc}_{d;nm}$ where the indices n and m range over all labels making (a,b,c,d,n,m) admissible. We say F is a* **6j symbol system** *if:*

(i) F satisfies the admissibility condition:

(1) If (a,b,c,d,n,m) is not admissible, then $F^{abc}_{d;nm} = 0$.

(2) Each matrix F^{abc}_{d} is invertible.

(ii) F satisfies the pentagon axiom: for all a, b, c, d, e, f, p, q, $m \in L$, we have

$$\sum_{n\in L} F^{bcd}_{q;pn} F^{and}_{f;qe} F^{abc}_{e;nm} = F^{abp}_{f;qm} F^{mcd}_{f;pe}.$$

We also call the numbers $\{ F^{abc}_{d;nm} \}$ the F-symbols. Below we distinguish those 6j symbol systems satisfying additional axioms corresponding to the unit and rigidity axioms in a fusion category. Let $G^{abc}_{d} = (F^{abc}_{d})^{-1}$ and $G^{abc}_{d;nm}$ be the (n,m)-entry of G^{abc}_{d}.

Definition 2.1.8 *A $6j$ symbol system is a* **6j fusion system** *if:*

(i) F satisfies the triangle axiom: $F^{abc}_{d} = I$ whenever $1 \in \{ a,b,c \}$.

(ii) F satisfies the rigidity axiom: for any $a \in L$, we have $F^{aa^*a}_{a;11} = G^{a^*aa^*}_{a^*;11}$.

Example 2.1.9 *Let G be a finite group considered as a fusion rule. Then the $6j$ fusion systems of G are exactly the 3-cocycles $f : G \times G \times G \to \mathbb{C}$. Note that if (a,b,c,d,n,m) is admissible then necessary $d = abc$, $m = ab$, and $n = bc$. So then $f(a,b,c,d,n,m) = F^{a,b,c}_{d;n,m} = F^{a,b,c}_{abc,bc,ab} = f(a,b,c)$ is really just a function of* *the first three arguments. Then, if* a, b, c, d, e, f, p, q, $m \in G$ *and both sides of*

$$\sum_{n \in L} F^{bcd}_{q;pn} F^{and}_{f;qe} F^{abc}_{e;nm} = F^{abp}_{f;qm} F^{mcd}_{f;pe}$$

are non-zero, then this forces $e = abc, f = abcd, n = bc, m = ab, p = cd,$ *and* $q = bcd$ *so that the equality reduces to*

$$f(b,c,d)f(a,bc,d)f(a,b,c) = f(a,b,cd)f(ab,c,d)$$

which is exaclty the 3-cocycle condition.

Example 2.1.10 *Let* H *be a quasi-bialgebra and let* Φ *be the Drinfeld associator of* H*. For any three* H*-modules* $U, V,$ *and* W*, the action of* Φ *induces a* H*-module isomorphism*

$$F_{U,V,W} : (U \otimes V) \otimes W \to U \otimes (V \otimes W)$$

given by $F_{U,V,W}((u \otimes v) \otimes w) = \Phi \cdot (u \otimes (v \otimes w))$*. Then for all* H*-modules* X*, the map* $F_{U,V,W}$ *induces a linear map*

$$F^{UVW}_X : \mathrm{Hom}(X, U \otimes (V \otimes W)) \to \mathrm{Hom}(X, (U \otimes V) \otimes W)$$

from which the $F-$*symbols can be determined. Axioms in the definition of quasi-bialgebra guarantees the resulting coefficients satisfy the pentagon and definition of* $6j$ *fusion system.*

The two definitions below explain what it means for two 6j fusion systems to be the same.

Definition 2.1.11 *Let* L *be a label set with a fixed fusion rule. Two 6j fusion systems* F *and* $\widetilde{F}$ *are* **gauge equivalent** *if there is a function* $f : L^3 \to \mathbb{C}$ *mapping* (a,b,c) *to* f^{ab}_c *such that:*

(i) $f^{ab}_c \neq 0$ *if* (a,b,c) *is admissible.*

(ii) $f^{1a}_a = f^{a1}_a = 1$ *for all* $a \in L$.

(iii) f *satisfies the rectangle axiom: for all* $a,b,c,d,n,m \in L$,

$$f^{bc}_n f^{an}_d F^{abc}_{d;nm} = \widetilde{F}^{abc}_{d;nm} f^{ab}_m f^{mc}_d.$$

Definition 2.1.12 *Two 6j fusion systems are* **equivalent** *if they are gauge equivalent up to an automorphism of the label set.*

Example 2.1.13 *Let* G *be a finite group, viewed as a label set as in Example 2.1.3. Then* $6j$ *fusion systems with this fusion rule are in bijection with the set of orbits* $H^3(G,\mathbb{C})/\operatorname{Aut}(G)$. *If* $G \cong \mathbb{Z}_n$, *then* $H^3(G,\mathbb{C}) \cong G$. *A generating 3-cocyle is given by*

$$h(x,y,z) = e^{2\pi i\bar{x}(\bar{y}+\bar{z}-\overline{y+z})/n^2}$$

where $\bar{a}$ *is the residue of* a *modulo* n. *The cocycle* h *corresponds to the* $6j$ *symbols* $h(x,y,z) = F^{x,y,z}_{xyz,yz,xy}$. *For* $m = 3$, *the cocycles* h *and* h^2 *differ by the nontrivial automorphism of* $\mathbb{Z}_3$. *Therefore there are just two inequivalent fusion systems with fusion rule given by* $\mathbb{Z}_3$.

As we said before, a fusion category is the quantum analog of a finite group. A braided fusion category is then the analog of an abelian group, where the braiding corresponds to a commutativity condition.

Definition 2.1.14 *A* **braiding** *on a 6j symbol system with label set* L *is a function* $R : L^3 \to \mathbb{C}$ *mapping* (a,b,c) *to* R^{ab}_c *such that:*

(i) $R^{ab}_c \neq 0$ *if* (a,b,c) *is admissible.*

(ii) R satisfies the hexagon axiom: for all $a, b, c, d, e, m \in L$,

$$(R^{ca}_e)^{\pm 1} F^{bac}_{d;em} (R^{ba}_m)^{\pm 1} = \sum_{n \in L} F^{bca}_{d;en} (R^{na}_d)^{\pm 1} F^{abc}_{d,nm}.$$

A 6j fusion system together with a choice of braiding R is called a **braided 6j fusion system***.*

We also call the numbers $\{ R^{ab}_c \}$ the R-symbols. The next two definitions are the version of pivotality and sphericality for $6j$ fusion systems, accounting for the compatible twist.

Definition 2.1.15 *A 6j fusion system is* **pivotal** *if there is a choice of roots of unity t_a for each label $a \in L$ satisfying the pivotal axioms:*

(i) $t_1 = 1$.

(ii) $t_{a^*} = t_a^{-1}$.

(iii) $t_a^{-1} t_b^{-1} t_c = F^{abc^*}_{1;a^*c} F^{bc^*a}_{1;a^*a} F^{c^*ab}_{1;b^*b}$ *for all admissible triples (a, b, c).*

The numbers $\{ t_a \}$ are called the **pivotal coefficients***. A 6j fusion system together with a choice of pivotal coefficients is called a* **pivotal 6j fusion system***. We say a pivotal 6j fusion system is a* **spherical 6j fusion system** *if $t_a \in \{ -1, 1 \}$ for all $a \in L$.*

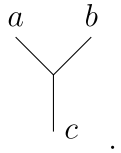
Definition 2.1.16 *A braided 6j fusion system together with a choice of spherical coefficients is called a* ***ribbon 6j fusion system****.*

2.2 Braid group representations from braided $6j$ fusion systems

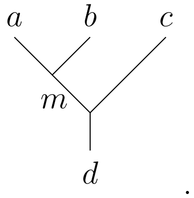
The axioms for the data of a braided $6j$ fusion system provide exactly the conditions required to define a collection of representations of the braid groups. The fusion rules for a $6j$ fusion system can be expressed diagrammatically and the F-symbols and R-symbols relate diagrams to each other. We will see that the pentagon and hexagon axioms are far from arbitrary conditions, but rather provide exactly the coherence that our we would hope our diagrammatic choices exhibit.

2.2.1 Fusion trees

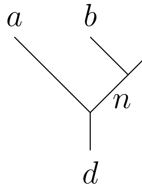
Let $(L, \otimes, F, R)$ be a (multiplicity-free) braided $6j$ fusion system and let $\mathcal{C}$ be a corresponding fusion category. Whenever N_{ab}^c is nonzero, there is a one-dimensional vector space $\mathrm{Hom}(X_c, X_a \otimes X_b)$ for some simple objects X_a, X_b, and X_c corresponding to the labels a, b, c. We can express this pictorially in a **fusion tree** as shown below (we think of the tree as representing a map $X_c \to X_a \otimes X_b$):



We can also draw fusion trees for starting choices of more than two labels, corresponding to maps from a simple object into a higher-fold tensor product. If (a, b, m) and (m, c, d) are both admissible then we can draw the fusion tree

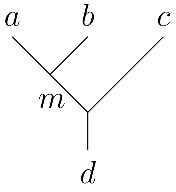


Notice that we chose to have the vertex on the left fork on the tree. However, since the objects $(X_a \otimes X_b) \otimes X_c$ and $X_a \otimes (X_b \otimes X_c)$ are isomorphic, there is an isomorphism between $\mathrm{Hom}(X_d, (X_a \otimes X_b) \otimes X_c)$ and $\mathrm{Hom}(X_d, X_a \otimes (X_b \otimes X_c))$. Hence there are change of basis coefficients from fusion trees of the above form to those of the form

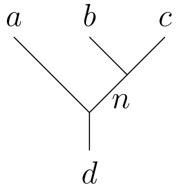


.

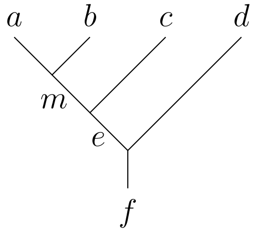
These coefficients are exactly the $6j$ symbols. We express the change of basis as



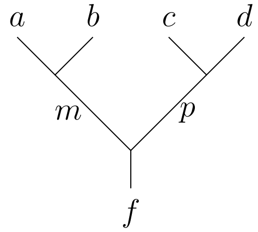
$$= \sum_{n} F^{abc}_{d;nm}$$



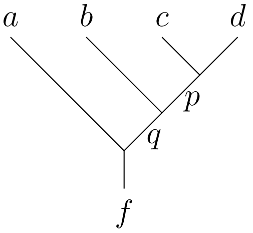
and call this relation an $F-$move (because the coefficients are collected in the so-called F-matrix). We can extend this relation to any fusion trees with more than three top labels. However, we must immediately address a consistency question that arises from our choice above. If we have a fusion tree with four labels at the top then there are multiple ways to apply series of F-moves to arrive two expressions involving the same fusion trees, we would expect that these agree. Fortunately, the pentagon axiom will give us exactly the consistency that we need. Let us demonstrate this. First, we can apply two F-moves to write



$$= \sum_{p} F^{mcd}_{f;pe}$$

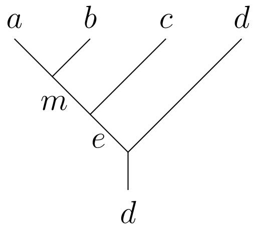


$$= \sum_{p,q} F^{abp}_{f;qm} F^{mcd}_{f;pe} \tag{2.1}$$

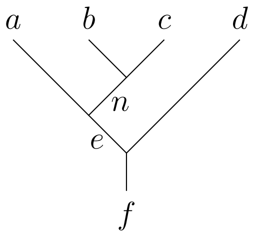


.

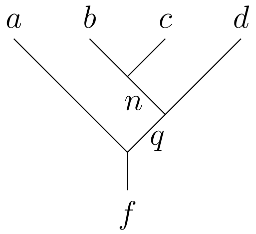
On the other hand, we can apply three F-moves to arrive at fusion trees of the same shape as those above. This yields the expansion



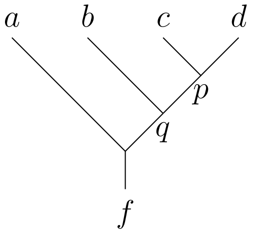
$$= \sum_{n} F^{abc}_{e;nm}$$



$$= \sum_{n,q} F^{and}_{f;qe} F^{abc}_{e;nm}$$



$$= \sum_{n,q,p} F^{bcd}_{q;pn} F^{and}_{f;qe} F^{abc}_{e;nm}$$

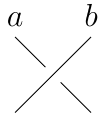


and this should agree with 2.1. Accordingly, for each choice of labels $a, b, c, d, e, f, m, p, q$ we must have

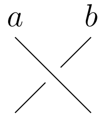
$$\sum_{n \in L} F^{bcd}_{q;pn} F^{and}_{f;qe} F^{abc}_{e;nm} = F^{abp}_{f;qm} F^{mcd}_{f;pe}$$

which is exactly the pentagon axiom for a $6j$ fusion system. Therefore the diagrammatic choices we have made are a natural way to visualize the hom-spaces in a fusion category and the data and axioms of a $6j$ fusion system. It is a theorem of Mac Lane that the pentagon axiom is enough to guarantee that any two series of F-moves can be applied to a fusion tree with more than four labels on the top and the results will be consistent.

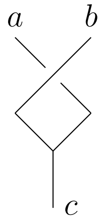
Now we will incorporate the braiding into these diagrams. Naturally,



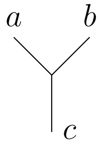
represents a map from $X_b \otimes X_a$ to $X_a \otimes X_b$ with its inverse



and so

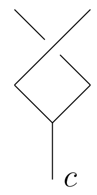


is another fusion tree for the labels (a, b, c). Since we are working with only multiplicity-free fusion rules, the above tree must be a multiple of

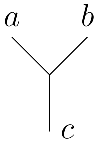


.

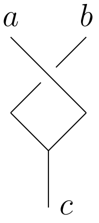
Indeed, the correct choice is



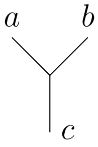
$= R_c^{ab}$



and

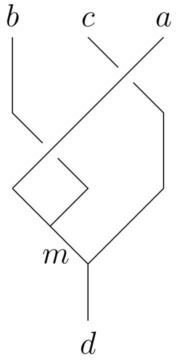


$$= (R_c^{ba})^{-1}$$

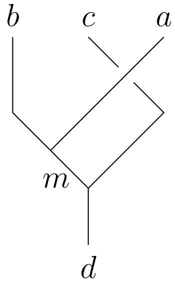


where R_c^{ab} is the $R-$symbol determined by the braiding.

Consider now the different ways of resolving a fusion tree with three nodes at the top with braidings applied first to the two leftmost nodes and then to the two rightmost nodes. On one hand we can first apply an $R-$move to write



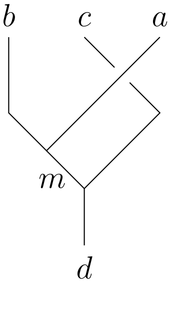
$$= R_m^{ba}$$



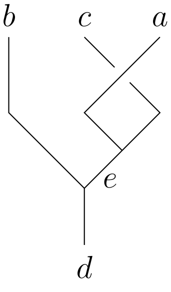
.

Then an $F-$move and another $R-$move give

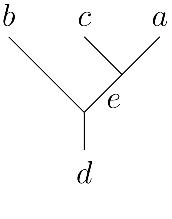
$$R_m^{ba}$$



$$= \sum_{e \in L} F^{bac}_{d;em} R^{ba}_m$$

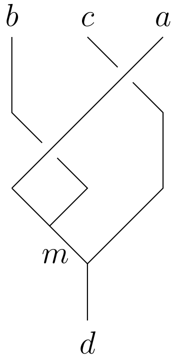


$$= \sum_{e \in L} R_e^{ca} F^{bac}_{d;em} R^{ba}_m$$

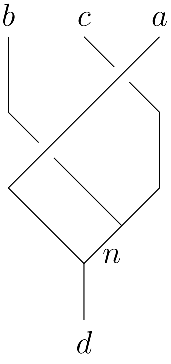


.

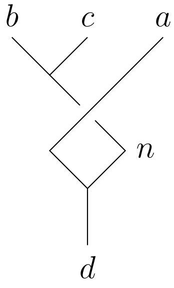
On the other hand, we can first apply an $F-$move and then isotope the fusion tree. Indeed,



$$= \sum_{n \in L} F^{abc}_{d;nm}$$

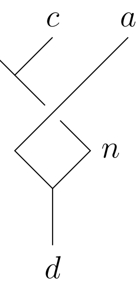


$$= \sum_{n \in L} F^{abc}_{d;nm}$$

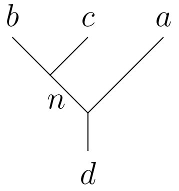


We can then resolve these trees using an $R-$move followed by an $F-$move to write

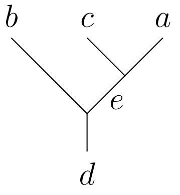
$$\sum_{n \in L} F^{abc}_{d;nm}$$



$$= \sum_{n \in L} R^{na}_{d} F^{abc}_{d;nm}$$



$$= \sum_{n,e \in L} F^{bca}_{d,en} R^{na}_{d} F^{abc}_{d;nm}$$



Then for all labels $a, b, c, d, e, m \in L$ we must have

$$R^{ca}_{e} F^{bac}_{d;em} R^{ba}_{m} = \sum_{n \in L} F^{bca}_{d,en} R^{na}_{d} F^{abc}_{d;nm}.$$

By exchanging the braiding for its inverse in the previous calculations, we are able to derive

$$(R^{ca}_{e})^{-1} F^{bac}_{d;em} (R^{ba}_{m})^{-1} = \sum_{n \in L} F^{bca}_{d,en} (R^{na}_{d})^{-1} F^{abc}_{d;nm}.$$

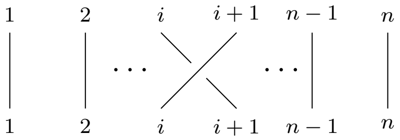
so if we combine these two equations we have exactly the hexagon axiom for the braiding. Accordingly, this tells us are can move and resolve crossings in the diagrams in different orders as shown in the resolutions above and the resulting calculations will agree. We will now show that the hexagon axiom will further imply that the braid relation for the braid group holds and so the fusion trees are actually bases for vector spaces admitting braid group representations whose coefficients are given by braiding and $6j$ symbols.

2.2.2 The braid group

First introduced by Artin ([Art47]), the braid groups are well-studied an ubiquitous in various areas of mathematics and physics. Let us give the algebraic and geometric definition. For each natural number n, the braid group on n-strands B_n is given by the famous presentation

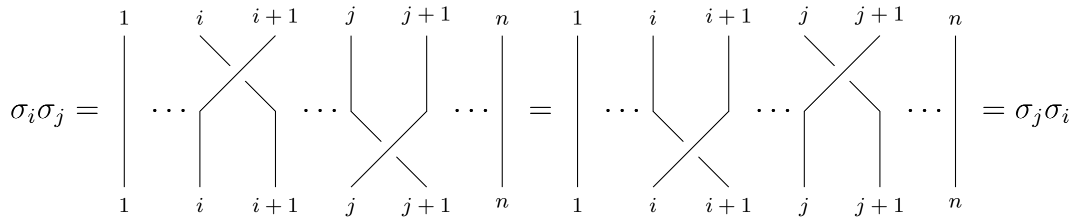
$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| > 1,\, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \rangle.$$

The elements of B_n can also be described visually via the identification

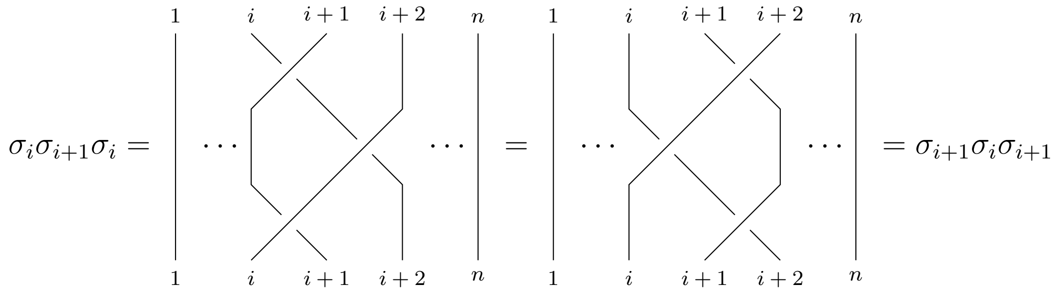
$\sigma_i =$ 

and then the group multiplication corresponds to stacking diagrams from the bottom up. Therefore if σ and τ are two braids then $\sigma\tau$ is the braid with τ at the bottom followed by stacking σ on top of this diagram and then resizing.

The first relation in the above presentation is often called far commutativity and the second is called the braid relation. Far commutativity can be visualized as



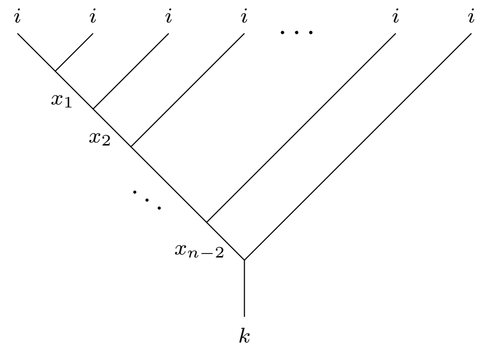
which shows that we can move crossing past each other when they do not interact with the same strands. The braid relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ then translates to the equation


$\sigma_i\sigma_{i+1}\sigma_i =$
$= \sigma_{i+1}\sigma_i\sigma_{i+1}$
1
i
$i+1$
$i+2$
n
$\cdots$

involving isotopy of three strands.

2.2.3 An action of braids on fusion trees

One of the main features of fusion trees and braided $6j$ fusion systems is the ability to recover braid group representations from all of the data of the $F-$ and $R-$ symbols. In particular, denote by $V_{i,n,k}$ the vector space spanned by trees with$n$ nodes on top labeled by i and lone node on bottom labelled k. We claim that whenever this vector space is nonzero, then the data of the $6j$ fusion system is exactly the matrix entries of a collection of representations of the n-strand braid group B_n on this vector space with respect to the bases of admissibly labelled fusion trees. Suppose $V_{i,n,k}$ has dimension m. Then a basis of $V_{i,n,k}$ consists of m fusion trees of form

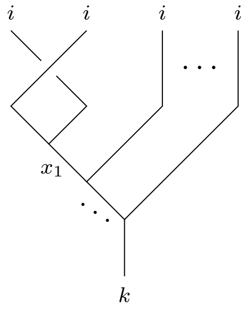


.

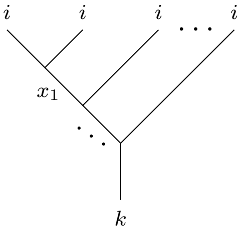
for interior labels $x_1, x_2, \dots, x_{n-2}$ such that each trivalent vertex is admissible. Let us denote this tree by $Y_{x_1,\dots,x_{n-2}}$.

Let us now define a collection of linear maps. For $j = 1, \dots, n-1$, let $T_j : V_{i,n,k} \to V_{i,n,k}$ determined by applying the braiding to the j and $j+1$ leaves of the fusion trees $Y_{x_1,\dots,x_{n-2}}$. There are two scenarios. The map determined by T_1 is necessarily diagonal in the basis of admissibly labelled trees with vertices on the left. Observe that

$$T_1(Y_{x_1,\dots,x_{n-2}}) =$$

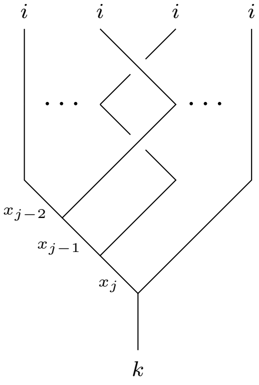


$$= R^{ii}_{x_1}$$



$$= R^{ii}_{x_1} Y_{x_1,\dots,x_{n-2}}.$$

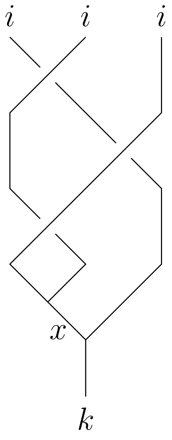
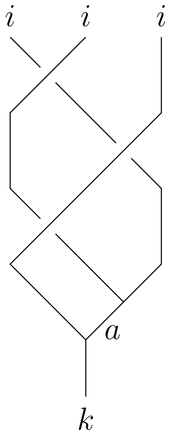
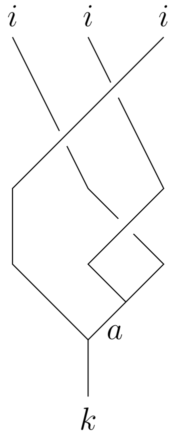
For $j > 1$, the maps T_j are determined by resolving the braiding on inner strands using $F-$ and $R-$moves. We will explicitly calculate the coefficients shortly. Each T_j is invertible and is determined by apply the inverse braiding the j and $j+1$ leaves of the fusion tree. Indeed, let G_j be the linear map determined by stacking the inverse braiding on the j and $j+1$ ends. Then

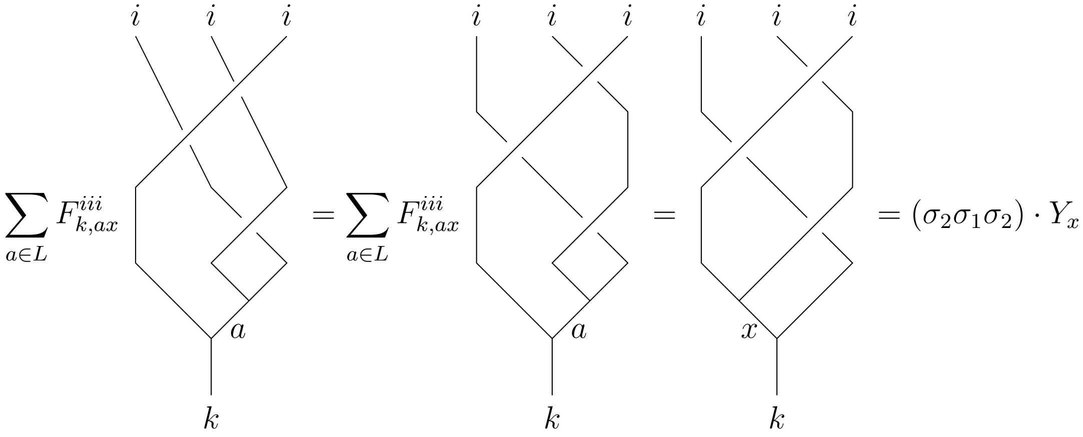
$G_j(T_j(Y_{x_1,\dots,x_{n-2}})) =$  $= Y_{x_1,\dots,x_{n-2}}$

and so $G_j = T_j^{-1}$. If we define a function $\rho_{i,n,k} : B_n \to \mathrm{GL}(V_{i,n,k})$ by $\rho_{i,n,k}(\sigma_j) = T_j$ then we claim this gives a representation. Let us first prove this for the case of $n = 3$.

Lemma 2.2.1 *Suppose $V_{i,3,k}$ is nonzero. Then $\rho_{i,3,k} : B_3 \to \mathrm{GL}(V_{i,3,k})$ is a group representation.*

Proof: It is just a matter of showing that the braid relation holds for the stacking action.

$(\sigma_1\sigma_2\sigma_1) \cdot Y_x =$  $= \sum_{a \in L} F^{iii}_{k,ax}$  $= \sum_{a \in L} F^{iii}_{k,ax}$  where the second equality follows from the hexagon axiom. Then


$\sum_{a\in L} F^{iii}_{k,ax}$
$= \sum_{a\in L} F^{iii}_{k,ax}$
$=$
$= (\sigma_2\sigma_1\sigma_2) \cdot Y_x$
i
a
x
k

and hence $(\sigma_1\sigma_2\sigma_1)\cdot Y_x = (\sigma_2\sigma_1\sigma_2)\cdot Y_x$ which shows that $\rho_{i,3,k}$ is a representation.

■

We can use this lemma to handle the general case.

Proposition 2.2.2 *Let $n \geq 3$ and suppose $V_{i,n,k}$ is nonzero. Then $\rho_{i,n,k} : B_n \to \mathrm{GL}(V_{i,n,k})$ is a group representation.*

Proof: Write $\rho = \rho_{i,n,k}$. If $|j-k| > 1$ then is it clear that $\rho(\sigma_j\sigma_k) = \rho(\sigma_k\sigma_j)$ since we can slide the crossings past each other as they involve disjoint pairs of strands. Any pair σ_j, σ_{j+1} generates a copy of B_3 so the braid relation holds by applying Lemma 2.2.1 locally to the $j, j+1$, and $j+2$ leaves of the fusion trees.

■

These representations arising from $6j$ fusion systems are what we will call ***quantum representations*** of the braid group. The final result we will record in this section tells us the coefficients for the action of each σ_j with respect to the basis of admissibly labelled trees.

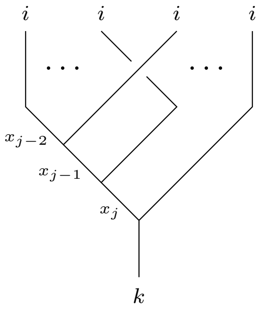
Lemma 2.2.3 *Suppose $V_{i,n,k}$ is nonzero. Then*

$$\sigma_j \cdot Y_{x_1,\ldots,x_{n-2}} = \begin{cases} R^{ii}_{x_1} Y_{x_1,\ldots,x_{n-2}} & \textit{if } j = 1 \\ \sum_{z,w\in L} G^{x_{j-2}ii}_{x_j;wz} R^{ii}_{z} F^{x_{j-2}ii}_{x_j;zx_{j-1}} Y_{x_1,\ldots,x_{j-2},w,x_j,\ldots,x_{n-2}} & \textit{if } j > 1 \end{cases}$$

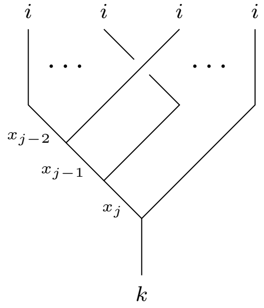
where $x_0 = i$.

Proof: The stacking action can be visualized with the diagrams below, where x_{j-1} denotes the interior label for $j = 1, \ldots, n$ and $x_0 = i$.

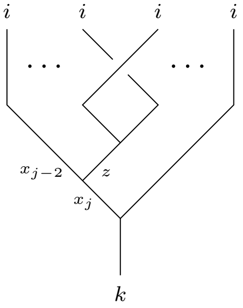
$$\sigma_j \cdot Y_{x_1,\ldots,x_{n-1}} =$$



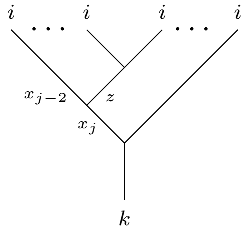
and we can use $F-$ and $R-$ moves to resolve this diagram and write down a formula for the coefficents of the action of σ_j on $Y_{x_1,\ldots x_n}$. Indeed,



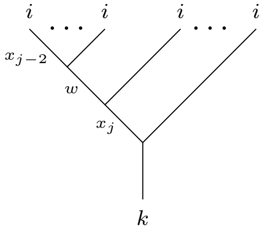
$= \sum_{z \in L} F^{x_{j-2}ii}_{x_j;zx_{j-1}}$



$= \sum_{z \in L} R^{ii}_z F^{x_{j-2}ii}_{x_j;zx_{j-1}}$



$= \sum_{z,w \in L} G^{x_{j-2}ii}_{x_j;wz} R^{ii}_z F^{x_{j-2}ii}_{x_j;zx_{j-1}}$



.

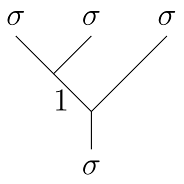
■

Example 2.2.4 *Recall the Ising fusion rule from the beginning of the section. The label set is* $\{ 1, \sigma, \psi \}$ *and the fusion rules are*

$$\sigma \otimes \sigma = 1 \oplus \psi, \quad \psi \oplus \psi = 1, \quad \sigma \otimes \psi = \psi \otimes \sigma = \sigma.$$

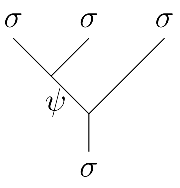
Observe that the vector space $V_{\sigma,3,\sigma}$ *is two-dimensional and admits basis vectors*

$Y_1 =$



and

$Y_\psi =$



.

The action of σ_1 on these vectors is diagonally by the $R-$symbols, i.e.

$$\rho_{\sigma,3,\sigma}(\sigma_1) = \begin{pmatrix} R_1^{\sigma\sigma} & 0 \\ 0 & R_\psi^{\sigma\sigma} \end{pmatrix} = \begin{pmatrix} e^{-\pi i/8} & 0 \\ 0 & e^{3\pi i/8} \end{pmatrix}.$$

The matrix $F_\sigma^{\sigma\sigma\sigma}$ allows us to compute the action of σ_2. We can choose $F_\sigma^{\sigma\sigma\sigma}$ to be of the form

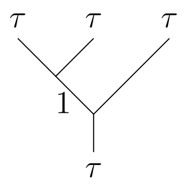
$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

so therefore

$$\rho_{\sigma,3,\sigma}(\sigma_2) = (F_\sigma^{\sigma\sigma\sigma})^{-1}\begin{pmatrix} e^{-\pi i/8} & 0 \\ 0 & e^{3\pi i/8} \end{pmatrix} F_\sigma^{\sigma\sigma\sigma} = \frac{1}{2}\begin{pmatrix} e^{-\pi i/8} + e^{3\pi i/8} & e^{-\pi i/8} - e^{3\pi i/8} \\ e^{-\pi i/8} - e^{3\pi i/8} & e^{-\pi i/8} + e^{3\pi i/8} \end{pmatrix}$$

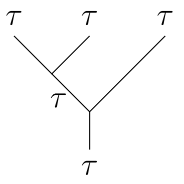
Example 2.2.5 *The Fibonacci theory is the fusion system with label set $L = \{1, \tau\}$ together with the fusion rule $\tau \otimes \tau = 1 \oplus \tau$. Then $V_{\tau,3,\tau}$ has basis*

$Y_1 =$



and

$Y_\tau =$



.

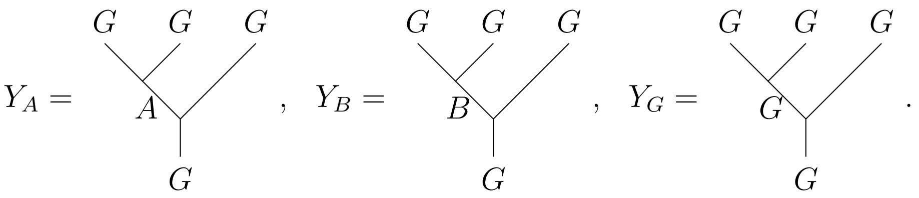
The representation $\rho_{\tau,3,\tau}$ *is determined by* $R_1^{\tau\tau} = e^{-4\pi i/5}$, $R_\tau^{\tau\tau} = e^{3\pi i/5}$ *and*

$$F_\tau^{\tau\tau\tau} = \begin{pmatrix} \phi^{-1} & \phi^{-1/2} \\ \phi^{-1/2} & -\phi^{-1} \end{pmatrix}$$

where $\phi = \frac{1+\sqrt{5}}{2}$ *is the golden ratio. One reason for interest in this representation is that it is known (see [FLW00]) that the image of* $\rho_{\tau,3\tau}$ *is a universal gate set for quantum computation.*

Another example comes from the $D(S_3)$ fusion system described before.

Example 2.2.6 *Recall the labels* A, B, G *of* $D(S_3)$*, presented in Example 2.1.6 and consider the vector space* $V_{G,3,G}$*. The fusion rules* $G \otimes G = A \oplus B \oplus G$*,* $G \otimes A = G$*, and* $G \otimes B = G$ *imply that* $V_{G,3,G}$ *is three-dimensional with basis vectors*



The R- and F- symbols for $D(S_3)$ *were determined in [CHW15]. They have been chosen so that the representations derived therein are unitary. We have* $R_A^{GG} = e^{4\pi i/3}$, $R_B^{GG} = -e^{4\pi i/3}$, *and* $R_G^{GG} = e^{2\pi i/3}$*. Also,*

$$F_G^{GGG} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{\sqrt{2}} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

from which the representation can be computed.

2.3 Categorical perspective

For completeness, we include the categorical definitions that go along side the vocabulary of a $6j$ fusion system introduced in the previous sections. We will assume basic familiarity with categories, functors, and natural transformations. For a category $\mathcal{C}$ and objects A and B of $\mathcal{C}$, denote by $\mathcal{C}(A,B)$ the set of morphisms from A to B.

Definition 2.3.1 *Let k be a field. We say a category $\mathcal{C}$ is* **k-linear** *if for each pair of objects A, B in $\mathcal{C}$, the hom-space $\mathcal{C}(A,B)$ is a k-vector space. An object A of $\mathcal{C}$ is said to be* **simple** *if $\mathcal{C}(A,A)$ is a one-dimensional k-vector space.*

We will only consider $\mathbb{C}$ −linear categories.

2.3.1 Monoidal and fusion categories

The starting point for all of the categorical structures that we will consider is a discussion of monoidal categories. All of the more complicated structures will have an underlying monoidal structure.

Definition 2.3.2 *A* **monoidal category** *is a category $\mathcal{C}$ together with a bifunctor*

$$-\otimes - : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

called a **tensor product***, an object I of $\mathcal{C}$ called the* **unit object***, and natural families of isomorphisms*

$$\alpha_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$$

$$\rho_A : A \otimes I \to A \quad \lambda_A : I \otimes A \to A$$

called respectively the **associator***, the* **right unitor** *and the* **left unitor***, such that the diagrams*

$$\begin{tikzcd}
 & ((A \otimes B) \otimes C) \otimes D \arrow[dl, "\alpha_{A,B,C} \otimes 1_D"'] \arrow[dr, "\alpha_{A \otimes B,C,D}"] & \\
(A \otimes (B \otimes C)) \otimes D \arrow[d, "\alpha_{A,B \otimes C,D}"'] & & (A \otimes B) \otimes (C \otimes D) \arrow[d, "\alpha_{A,B,C \otimes D}"] \\
A \otimes ((B \otimes C) \otimes D) \arrow[rr, "1_A \otimes \alpha_{B,C,D}"] & & A \otimes (B \otimes (C \otimes D))
\end{tikzcd}$$

and

$$\begin{tikzcd}
(A \otimes I) \otimes B \arrow[rr, "\alpha_{A,I,B}"] \arrow[dr, "\rho_A \otimes 1_B"'] & & A \otimes (I \otimes B) \arrow[dl, "1_A \otimes \lambda_B"] \\
 & A \otimes B &
\end{tikzcd}$$

commute.

The term **tensor category** *is reserved for those linear monoidal categories. One way to simplify the investigation of monoidal categories is to consider those wherein the associators and unitors are all trivial.*

When consider maps between monoidal categories, we want functors that also transport the monoidal structure from one category to another. We can never have true equality in categories; the correct addition to include is a natural transformation between the two monoidal structures in the target category. We give the full definition below.

Definition 2.3.3 *Let $\mathcal{C}$ be a monoidal category with associators α, left unitor λ and right unitor ρ. We say $\mathcal{C}$ is* ***strict*** *in the case that α, λ, and ρ are all equal to the identity natural transformation.*

Definition 2.3.4 *Let $\mathcal{C}$ and $\mathcal{D}$ be monoidal categories with respective unit objects $I_{\mathcal{C}}$ and $I_{\mathcal{D}}$. A* ***monoidal functor*** *is a functor $F : \mathcal{C} \to \mathcal{D}$ together with a natural transformation $f_{A,B} : F(A) \otimes F(B) \to F(A \otimes B)$ and morphism $f : I_{\mathcal{D}} \to F(I_{\mathcal{C}})$ such that for all objects A, B, C of $\mathcal{C}$ the diagrams*

$$\begin{tikzcd}
(F(A) \otimes F(B)) \otimes F(C) \arrow[rr, "\alpha_{F(A),F(B),F(C)}"] \arrow[d, "f_{A,B} \otimes \mathrm{id}_{F(C)}"] & & F(A) \otimes (F(B) \otimes F(C)) \arrow[d, "\mathrm{id}_{F(A)} \otimes f_{B,C}"] \\
F(A \otimes B) \otimes F(C) \arrow[d, "f_{A \otimes B,C}"] & & F(A) \otimes F(B \otimes C) \arrow[d, "f_{A,B \otimes C}"] \\
F((A \otimes B) \otimes C) \arrow[rr, "F(\alpha_{A,B,C})"] & & F(A \otimes (B \otimes C))
\end{tikzcd}$$

$$\begin{tikzcd}
F(A) \otimes I_{\mathcal{D}} \arrow[r, "\mathrm{id}_{F(A)} \otimes f"] \arrow[d, "\rho_{F(A)}"] & F(A) \otimes F(I_{\mathcal{C}}) \arrow[d, "f_{A,I_{\mathcal{C}}}"] \\
F(A) & F(A \otimes I_{\mathcal{C}}) \arrow[l, "F(\rho_A)"']
\end{tikzcd}$$

and

$$\begin{tikzcd}
I_{\mathcal{D}} \otimes F(B) \arrow[r, "f \otimes \mathrm{id}_{F(B)}"] \arrow[d, "\lambda_{F(B)}"] & F(I_{\mathcal{C}}) \otimes F(B) \arrow[d, "f_{I_{\mathcal{C}},B}"] \\
F(B) & F(I_{\mathcal{C}} \otimes B) \arrow[l, "F(\lambda_B)"']
\end{tikzcd}$$

commute. A monoidal functor is called a ***monoidal equivalence*** *if the underlying functor F is an equivalence of categories. In this case we say that $\mathcal{C}$ and $\mathcal{D}$ are* ***monoidally equivalent****.*

The following theorem allows us to simplify many discussions as we can speak only of those strict categories but then transport the results back to the non-strict case. This is due to MacLane.

Theorem 2.3.5 ([Lan78]) *Every monoidal category is canonically monoidally equivalent to a strict monoidal category.*

So far, it should be clear that we are generalizing the structure exhibited by, say, the category of representations of some group or algebra. In this case, another piece to include is the corresponding dual objects. The formal definition is provided next.

Definition 2.3.6 *Let $\mathcal{C}$ be a monoidal category and let A be an object of $\mathcal{C}$. A* **left dual** *for A is an object A^* of $\mathcal{C}$ together with morphisms*

$$e_A : A^* \otimes A \to I, \quad d_A : I \to A \otimes A^*$$

such that the diagrams

$$\begin{tikzcd}
A \arrow[r, "\lambda_A^{-1}"] \arrow[rrrrr, bend right, "1_A"'] & I \otimes A \arrow[r, "d_A \otimes 1_A"] & (A \otimes A^*) \otimes A \arrow[r, "\alpha_{A,A^*,A}"] & A \otimes (A^* \otimes A) \arrow[r, "1_A \otimes e_A"] & A \otimes I \arrow[r, "\rho_A"] & A
\end{tikzcd}$$

and

$$\begin{tikzcd}
A^* \arrow[r, "\rho_{A^*}^{-1}"] \arrow[rrrrr, bend right, "1_{A^*}"'] & A^* \otimes I \arrow[r, "1_{A^*} \otimes d_A"] & A^* \otimes (A \otimes A^*) \arrow[r, "\alpha^{-1}_{A^*,A,A^*}"] & (A^* \otimes A) \otimes A^* \arrow[r, "e_A \otimes 1_{A^*}"] & I \otimes A^* \arrow[r, "\lambda_{A^*}^{-1}"] & A^*
\end{tikzcd}$$

commute. In this case, we also say A is a **right dual** *for A^*. An object A is called* **left (resp. right) rigid** *if it has a left (resp. right) dual. We say A is* **rigid** *if it has both a left and right dual. A monoidal category $\mathcal{C}$ is* **left (resp. right) rigid** *if every object of $\mathcal{C}$ is left (resp. right) rigid and $\mathcal{C}$ is* **rigid** *if every object of $\mathcal{C}$ is rigid.*

Continuing with the motivating example of the category of representations of a finite group, recall that this category is semisimple and has finitely many isoclasses of simple objects. This idea is incorporated into the following definition, which is the ultimate goal of this section.

Definition 2.3.7 *A* **fusion category (over a field k)** *is a rigid semisimple k-linear monoidal category, with only finitely many isomorphism classes of simple objects, such that the unit object is simple.*

Before moving on to the next section, we connect the definitions here back to the beginning of this chapter. Plainly, we want to express that fusion categories are the same as 6j fusion systems, up to the appropriate caveats.

Theorem 2.3.8 ([Yam02, ENO05])

(i) There is a bijection between 6j fusion systems up to equivalence and fusion categories over $\mathbb{C}$ up to $\mathbb{C}$-linear monoidal equivalence.

(ii) (Ocneanu rigidity) There are only finite many equivalence classes of fusion categories with a given fusion rule.

2.3.2 Ribbon and premodular categories

In the next few sections, we will describe some of the addition structures and properties that monoidal and fusion categories can have, culminating with the definition of a modular tensor category. The first thing to discuss is braidings for monoidal categories, which is a sort of commutativity condition on the tensor product in the monoidal category.

Definition 2.3.9 *Let $\mathcal{C}$ be a monoidal category. A* **braiding** *for $\mathcal{C}$ is a natural family of isomorphism*

$$c_{A,B} : A \otimes B \to B \otimes A$$

such that the diagrams

$$\begin{tikzcd}
 & (A \otimes B) \otimes C \arrow[dl, "c_{A,B} \otimes 1_C"'] \arrow[dr, "\alpha_{A,B,C}"] & \\
(B \otimes A) \otimes C \arrow[d, "\alpha_{B,A,C}"'] & & A \otimes (B \otimes C) \arrow[d, "c_{A,B\otimes C}"] \\
B \otimes (A \otimes C) \arrow[dr, "1_B \otimes c_{A,C}"'] & & (B \otimes C) \otimes A \arrow[dl, "\alpha_{B,C,A}"] \\
 & B \otimes (C \otimes A) &
\end{tikzcd}$$

and

$$\begin{tikzcd}
 & A \otimes (B \otimes C) \arrow[dl, "1_A \otimes c_{B,C}"'] \arrow[dr, "\alpha^{-1}_{A,B,C}"] & \\
A \otimes (C \otimes B) \arrow[d, "\alpha^{-1}_{A,C,B}"'] & & (A \otimes B) \otimes C \arrow[d, "c_{A\otimes B,C}"] \\
(A \otimes C) \otimes B \arrow[dr, "c_{A,C} \otimes 1_B"'] & & C \otimes (A \otimes B) \arrow[dl, "\alpha^{-1}_{C,A,B}"] \\
 & (C \otimes A) \otimes B. &
\end{tikzcd}$$

commute. A **braided monoidal category** *is a monoidal category together with a chosen braiding.*

Let $\mathcal{C}$ be a braided fusion category. For each object X of $\mathcal{C}$ and natural number n, the hexagon axioms for the braiding imply that there is a group homomorphism $\rho_{X,n}$:

$B_n \to \mathrm{End}(X^{\otimes n})$ where $\rho_{X,n}(\sigma_i) = \mathrm{id}_X^{\otimes i-1} \otimes c_{X,X} \otimes \mathrm{id}_X^{\otimes n-i-1}$ (suppressing associators). Then whenever Y is another object of $\mathcal{C}$ such that $\mathrm{Hom}(Y, X^{\otimes n})$ is nonzero, there is a representation $\rho_{X,n,Y} : B_n \to \mathrm{GL}(\mathrm{Hom}(Y, X^{\otimes n}))$ determined by

$$\rho_{X,n,Y}(\sigma_i) = \Big(f \mapsto \rho_{X,n}(\sigma_i) \circ f\Big)$$

In this way, a braided fusion category provides a wealth of representations of the braid groups. Under the correspondence between braided $6j$ fusion systems and and braided fusion cateogries, these are the same quantum representations defined in the earlier sections.

To get from braided categories to modular categories, we need an another structure, called a twist, which satisfies a certain compatibility condition with the braiding.

Definition 2.3.10 *Let $\mathcal{C}$ be a braided monoidal category. A* **twist** *for $\mathcal{C}$ is a natural family of isomorphisms*

$$\theta_A : A \to A$$

such that $\theta_{A\otimes B} = c_{B,A} \circ (\theta_A \otimes \theta_B) \circ c_{A,B}$. A braided monoidal category with a chosen twist is called a **balanced monoidal category***.*

The next definition generalizes the transpose map on dual vector spaces induced by a linear map.

Definition 2.3.11 *Let $\mathcal{C}$ is a left rigid monoidal category and let A and B be objects of $\mathcal{C}$. To each morphism $f : A \to B$ we can assign a morphism $f^* : B^* \to A^*$ given by the composition $f^* = \lambda_{A^*}(e_B \otimes 1_{A^*})(1_{B^*} \otimes f \otimes 1_{A^*})\alpha^{-1}_{B^*,A,A^*}(1_{B^*} \otimes d_A)\rho^{-1}_{B^*}$. The morphism f^* is called the* ***dual morphism*** **of** ***f*.**

Definition 2.3.12 *Let $\mathcal{C}$ be a balanced rigid monoidal category with twist θ. We say $\mathcal{C}$ is a* **ribbon category** *if*

$$\theta_{A^*} = \theta_A^*$$

for all objects A of $\mathcal{C}$.

Definition 2.3.13 *We call a ribbon fusion category a* **premodular category***.*

2.4 Modular categories and quantum representations

Definition 2.4.1 *For a premodular category $\mathcal{C}$ with braiding c and twist θ, we can define a* ***trace*** *for morphisms $f : A \to A$. Indeed, the composition*

$$I \xrightarrow{d_A} A \otimes A^* \xrightarrow{(\theta_A f)\otimes 1} A \otimes A^* \xrightarrow{c_{A,A^*}} A^* \otimes A \xrightarrow{e_A} I.$$

gives an elements of $\mathcal{C}(I, I)$ and since I is simple, this composition must be of equal to $\operatorname{tr}(f)\operatorname{id}_I$ for some scalar $\operatorname{tr}(f) \in \mathbb{C}$. For an object A of $\mathcal{C}$ we define the ***quantum dimension*** *of an object A, denoted $\dim A$, to be $\operatorname{tr}(\operatorname{id}_A)$. Let $\operatorname{Irr}(\mathcal{C})$ be a complete set of isomorphism classes of simple objects of $\mathcal{C}$. Then we can define the* ***global quantum dimension*** *of $\mathcal{C}$, denoted by $\dim \mathcal{C}$ where*

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

Definition 2.4.2 *Let $\mathcal{C}$ be a premodular category with braiding c and twist θ and let $\{X_0 = I, X_1, \ldots, X_n\}$ be a complete set of isomorphism classes of simple objects of $\mathcal{C}$. Define $s_{i,j}$ to be the scalar $\operatorname{tr}(c_{X_j,X_i} \circ c_{X_i,X_j})$. Since the vector spaces $\operatorname{End}(X_i)$ are one-dimensional, there are scalars θ_i so that $\theta_{X_i} = \theta_i \operatorname{id}_{X_i}$ for all $i = 0, \ldots, n$. Then we can define*

$$\mathbf{s} = (s_{i,j}) \qquad \mathbf{t} = (\theta_i \delta_{i,j})$$

for $i, j = 0, \ldots n$. These are respectively called the $S-$matrix and $T-$matrix of $\mathcal{C}$. A premodular category is called **modular** *if* $\mathbf{s}$ *is invertible.*

Proposition 2.4.3 *In a modular category $\mathcal{C}$ with $S-$matrix* $\mathbf{s}$ *and $T-$matrix* $\mathbf{t}$*,*

$$\mathbf{s}^2 = (\dim(\mathcal{C}))\mathbf{e}, \quad \mathbf{e}^2 = I, \quad (\mathbf{st})^3 = p_{\mathcal{C}}^{+}\mathbf{s}^2, \quad \mathbf{et} = \mathbf{te}$$

where $p_{\mathcal{C}}^{\pm} = \sum_i \theta_i^{\pm} \dim(X_i)$ and $\mathbf{e} = (\delta_{i,j^*})$. In particular, $\mathbf{s}$ *and* $\mathbf{t}$ *define a projective representation of the mapping class group of the torus.*

We call these representations defined above **quantum representations**. We have so far demonstrated that we can define representations of the mapping class group of the n-times punctured disc as well as the torus. It is natural to wonder if we can define representations for the mapping class group of any surface. It turns out that in a modular category, the projective representations of the mapping class group of the torus can be extended to any surface with genus greater than one. Quantum representations of mapping class groups has received considerable attention (see [And06, FK06, Fun99, LW05, FWW02, BW18, Blo18]). We will be focusing on quantum representations of the three-strand braid group, although similar problems could be formulated for other mapping class groups.

Chapter 3

A congruence subgroup problem for quantum representations

Our main goal throughout this work is to explain a construction of congruence and non-congruence subgroups associated to representation of the three-strand braid group, especially quantum representations. In this section, we introduce the vocabulary for finite index and congruence subgroups of the special linear groups. The fact that the three-strand braid group admits $\mathrm{SL}(2,\mathbb{Z})$ as a quotient will then be the bridge between braid group representations and congruence subgroups.

3.1 Finite index subgroups of the special linear groups

Let N be a positive integer at least equal to two and denote by $\mathrm{SL}(N,\mathbb{Z})$ the group of $N \times N$ matrices with integer entries and determinant equal to one. This is a normal subgroup of $\mathrm{GL}(N,\mathbb{Z})$ as it is the kernel of the homomorphism

$$\begin{aligned}\mathrm{GL}(N,\mathbb{Z}) &\to \mathbb{Z}\\ A &\mapsto \det A.\end{aligned}$$

One way of understanding an infinite discrete group like $\mathrm{SL}(N,\mathbb{Z})$ is to understand its finite quotients or more generally its finite index subgroups. There are obvious candidates for finite index subgroups of $\mathrm{SL}(N,\mathbb{Z})$. For each positive integer d, denote by $\mathrm{SL}(N,d)$ the finite group $\mathrm{SL}(N,\mathbb{Z}/d\mathbb{Z})$. There is a surjective homomorphism

$$r_d : \mathrm{SL}(N,\mathbb{Z}) \to \mathrm{SL}(N,d)$$

which is induced by the reduction mod d homomorphism $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$. As $\mathrm{SL}(N,d)$ is a finite group, we can construct a finite index subgroup of $\mathrm{SL}(N,\mathbb{Z})$ by pulling back a subgroup of $\mathrm{SL}(N,d)$ along r_d. The simplest example would be to look at the preimage of the identity i.e. the kernel of r_d. These have a special name.

Definition 3.1.1 *Let $r_d : \mathrm{SL}(N,\mathbb{Z}) \to \mathrm{SL}(N,d)$ be the homomorphism induced by reducing entries modulo d. The kernel of this map is called the* **principal congruence subgroup of level** *d.*

We see that the finite index subgroups G of $\mathrm{SL}(N,\mathbb{Z})$ fall into two classes - those which arise as the preimage of a subgroup of $\mathrm{SL}(N,d)$ and those which do not. In the former case, G must contain the principal congruence subgroup of some level.

Definition 3.1.2 *A finite index subgroup G of $\mathrm{SL}(N,\mathbb{Z})$ is called a* **congruence subgroup** *if G contains a principal congruence subgroup. The minimal integer d such that G contains the principal congruence subgroup of level d is called the* **level** *of G. If G*

does not contain any principal congruence subgroups then G is called a **non-congruence subgroup**.

It is natural to wonder to what extent congruence subgroups account for the finite index subgroups of $\mathrm{SL}(N, \mathbb{Z})$. It turns out that this was answered by Bass, Serre, and Lazard and separately by Mennicke.

Theorem 3.1.3 ([BSL64, Men65]) *Every finite index subgroup of* $\mathrm{SL}(N, \mathbb{Z})$ *is a congruence subgroup if and only if N is greater than two.*

In particular, we see that $\mathrm{SL}(2, \mathbb{Z})$ is the only special linear group which admits non-congruence subgroups. For all other values of N, the only finite index subgroups of $\mathrm{SL}(N, \mathbb{Z})$ arise via the construction outlined above.

3.2 $\mathrm{SL}(2, \mathbb{Z})$

Let us narrow our attention to the case of $\mathrm{SL}(2, \mathbb{Z})$ and the congruence subgroup problem. The group $\mathrm{SL}(2, \mathbb{Z})$ is ubiquitous in mathematics, appearing in numerous areas including number theory, hyperbolic geometry, and topology. Abstractly, $\mathrm{SL}(2, \mathbb{Z})$ has the presentation

$$\mathrm{SL}(2, \mathbb{Z}) = \langle x, y \mid x^2 = (xy)^3,\, x^4 = 1 \rangle \tag{3.1}$$

given by an amalgamated free product of $\mathbb{Z}_4$ and $\mathbb{Z}_6$. This presentation can be realized using the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

by setting $x = S$ and $y = ST$. Another set of generators (although for a different presentation) is given by T and the matrix

$$U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

and the two generators are related by the equation $TST = U$ or $S = T^{-1}UT^{-1}$. The subgroup $\{ I, -I \}$ of $\mathrm{SL}(2, \mathbb{Z})$ is a normal subgroup and quotient group is called $\mathrm{PSL}(2, \mathbb{Z})$. When no confusion arises we will denote the projective image of a matrix A by the same letter. In particular, we can identity the matrices S and T above with elements of $\mathrm{PSL}(2, \mathbb{Z})$ as well. There is a well known isomorphism (see [Alp93])

$$\mathbb{Z}_2 * \mathbb{Z}_3 \cong \mathrm{PSL}(2, \mathbb{Z})$$

which maps the order two generator of $\mathbb{Z}_2 * \mathbb{Z}_3$ to S and the order 3 generator to ST.

Historically (although not uniformly), the group $\mathrm{PSL}(2, \mathbb{Z})$ is often denoted Γ, and we will use this abbreviation. Let us write $q : \mathrm{SL}(2, \mathbb{Z}) \to \Gamma$ for the quotient map. We shall introduce some special notation for the principal congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$ and Γ. Denote by $\widetilde{\Gamma}(d)$ the principal congruence subgroup of level d of $\mathrm{SL}(2, \mathbb{Z})$ and $\Gamma(d)$ the principal congruence subgroup of level d of Γ (its preimage under the quotient map q).

Example 3.2.1 *In this example we show that* $\widetilde{\Gamma}(2) = \langle T^2, U^2, -I \rangle$. *Since*

$$T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

and

$$U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

it is clear that $\langle T^2, U^2, -I \rangle \subseteq \widetilde{\Gamma}(2)$*. Now we need to establish the other inclusion. This can be done essentially using the division algorithm. Suppose*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is an element of $\widetilde{\Gamma}(2)$*. First, if* $c = 0$ *then* A *is necessarily of the form*

$$\begin{pmatrix} \pm 1 & 2m \\ 0 & \pm 1 \end{pmatrix}$$

since $\det A = 1$ *and* $A \equiv I \mod 2$*. Then* $A = \pm T^{2m}$ *is an element of* $\langle T^2, U^2, -I \rangle$*. Similarly, if* $b = 0$ *then* $A = \pm U^{2n}$ *for some* n *and so again* $A \in \langle T^2, U^2, -I \rangle$*. So assume that neither* $b = 0$ *nor* $c = 0$*. Since* a *is odd and* c *is even and nonzero, we know that either* $|a| > |c|$ *or* $|a| < |c|$*. If* $|a| > |c|$*, we can write* $a = 2kc + r$ *for some* r *such that* $|r| < |c|$*. Then*

$$T^{-2k}A = \begin{pmatrix} 1 & -2k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - 2kc & b - 2kd \\ c & d \end{pmatrix} = \begin{pmatrix} r & b - 2kd \\ c & d \end{pmatrix}$$

and now $|r| < |c|$*. Then write* $c = 2\ell r + s$ *where* $|s| < |r|$ *so that*

$$U^{-2\ell}T^{-2k}A = \begin{pmatrix} r & b - 2kd \\ s & d - 2\ell r \end{pmatrix}$$

and again the bottom left entry is of smaller absolute value than the upper left entry. Continuing this way, we can multiply by appropriate even powers of T and U until we arrive at a remainder of 0. Since each term in the product is an element of $\widetilde{\Gamma}(2)$, we know that the 0 cannot be in the top left entry. Therefore we arrive at a matrix of the form

$$\begin{pmatrix} \pm 1 & 2m \\ 0 & \pm 1 \end{pmatrix}$$

which we have already considered. Thus we see that any element of $\widetilde{\Gamma}(2)$ can be written as a product of $-I$ and powers of T^2 and U^2.

Theorem 3.1.3 tells us that $\mathrm{SL}(2,\mathbb{Z})$ is the only special linear group which exhibits finite-index subgroups not arising as preimages of subgroups of $\mathrm{SL}(2,d)$ for some d. In fact, more is true. If we let $n(r)$ be the number of index r subgroups of $\mathrm{SL}(2,\mathbb{Z})$ and $n_c(r)$ the number of those that are congruence subgroups, then

$$\frac{n_c(r)}{n(r)} \to 0$$

as $r \to \infty$. So it is the non-congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$ which account for nearly all of its finite index subgroups, (see [Sto84]).

Now, this leads to a natural problem: given a finite index subgroup of $\mathrm{SL}(2,\mathbb{Z})$, determine whether it is a congruence subgroup. This is sometimes referred to as the **congruence subgroup problem**. We often pass back and forth between $\mathrm{SL}(2,\mathbb{Z})$ and $\mathrm{PSL}(2,\mathbb{Z})$ and in general there is no harm here.

Proposition 3.2.2 *If G is a finite index subgroup of $\mathrm{SL}(2,\mathbb{Z})$ and $q : \mathrm{SL}(2,\mathbb{Z}) \to \Gamma$ is* *the quotient map then G is a congruence subgroup of* $\mathrm{SL}(2,\mathbb{Z})$ *if and only if* $q(G)$ *is a congruence subgroup of* $\mathrm{PSL}(2,\mathbb{Z})$.

Proof: Suppose $\widetilde{\Gamma}(d) \subseteq G \subseteq \mathrm{SL}(2,\mathbb{Z})$. Then $q(\widetilde{\Gamma}(d)) \subseteq q(G) \subseteq \Gamma$. But $q(\widetilde{\Gamma}(d)) = \Gamma(d)$ so $q(G)$ is a congruence subgroup of Γ.Conversely, if $\overline{G}$ is a subgroup of Γ then let G be the corresponding subgroup of $\mathrm{SL}(2,\mathbb{Z})$ so that $q(G) = \overline{G}$. If $q(\Gamma(d)) \subseteq \overline{G}$ then taking the preimage under q we see $\widetilde{\Gamma}(d) \subseteq G$.

■

3.2.1 A family of non-congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$

The purpose of this section is to give an example of an infinite family of non-congruence subgroups of $\mathrm{SL}(2.\mathbb{Z})$ and Γ. This family is interesting because its construction is similar to the one we will provide at the end of the next chapter. Both families arise as kernels of homomorphisms and are in that way a bit mysterious. The example here arises as the kernels of the quotient maps from $\mathrm{SL}(2,\mathbb{Z})$ to the alternating groups A_n. This is our starting point.

Theorem 3.2.3 ([DW71]) *For $n \geq 3$, the alternating groups A_n are generated by an element or order two and an element of order three.*

In particular, since Γ is isomorphic to the free product $\mathbb{Z}_2 * \mathbb{Z}_3$, we can realize these alternating groups as quotients of Γ and therefore of $\mathrm{SL}(2,\mathbb{Z})$. Denote the kernel of the quotient map $\mathrm{SL}(2,\mathbb{Z}) \to A_n$ by K_n. This is a family of finite index subgroups of $\mathrm{SL}(2,\mathbb{Z})$ and we claim that each of these is a non-congruence subgroup. First, we need the following lemmas.

Lemma 3.2.4 *Let $H = G_1 \times \cdots \times G_m$ where each G_i is a finite group. If S is a simple group quotient of H then S is a simple quotient of one of the G_i.*

Proof: Since S is a simple quotient of H, there is a composition series of H with S as a composition factor. Also, if we let $H_i = G_1 \times \cdots \times G_i \times 1 \times \cdots \times 1$, then

$$1 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = H$$

is a normal series for H with factors $H_i/H_{i-1} \cong G_i$ for $i = 1, \ldots, m$. Therefore, by the Jordan-Hölder theorem, there is some i so that S is a composition factor of G_i. Equivalently, S is a simple quotient of G_i. ■

Next we need to identify the composition factors of $\mathrm{SL}(2, p^r)$.

Lemma 3.2.5 *Let p be a prime and $r \geq 1$ an integer. If C is a composition factor of $\mathrm{SL}(2, p^r)$ then C is isomorphic to one of the following:*

(i) a cyclic group.

(ii) $\mathrm{PSL}(2, p)$.

Proof: There is a surjective map $\mathrm{SL}(2, p^r) \to \mathrm{SL}(2, p)$ given by reducing entries $\mod p$. The kernel K_{p^r} of this map is known to be a $p-$group, whose composition factors are all cyclic of order p. Therefore the composition factors of $\mathrm{SL}(2, p^r)$ are cyclic of order p together with the composition factors of $\mathrm{SL}(2, p)$. First consider when p is less than 5. There are isomorphisms $\mathrm{SL}(2, 2) \cong S_3$ and $\mathrm{SL}(2, 3) \cong A_4$, which are both solvable and hence their composition factors are all cyclic groups. Now for p at least 5, recall that the quotient $\mathrm{SL}(2, p)/\{\, I, -I \,\}$ is the simple group $\mathrm{PSL}(2, p)$. Hence the composition factors are cyclic of order 2 and $\mathrm{PSL}(2, p)$. ■

Lemma 3.2.6 *Let n be a positive integer and p a prime. The solutions to*

$$n! = (p-1)p(p+1)$$

are

- $n = 3$, $p = 2$,
- $n = 4$, $p = 3$, *or*
- $n = p = 5$.

Proof: When $n < p$ there are no solutions since then $n!$ is not divisible by p. When $n = p$, we can reduce the equation to

$$(p-2)! = p + 1$$

and the only prime solution is $p = 5$. This gives the solution $n = p = 5$. If $n = p + 1$ then we can reduce the equation to

$$(p-2)! = 1$$

so $p = 2$ or $p = 3$ giving the other two solutions above. When $n > p + 1$ we claim there are no solutions. We can divide $n!$ by $(p-1)p(p+1)$ and the result will be an integer greater than one, so there can be no solutions. ■

We can bring these three lemmas together to prove the following proposition which essentially proves our examples are non-congruence subgroups.

Proposition 3.2.7 *For any $n \geq 6$, the alternating group A_n is not a quotient of* $\mathrm{SL}(2, d)$ *for any $d \geq 2$.*

Proof: Suppose A_n is a quotient of $\mathrm{SL}(2, d)$. If we write $d = p_1^{r_1} \cdots p_m^{r_m}$ then the Chinese Remainder Theorem implies

$$\mathrm{SL}(2, d) \cong \mathrm{SL}(2, p_1^{r_1}) \times \cdots \times \mathrm{SL}(2, p_m^{r_m})$$

and since A_n is simple for $n \geq 5$, by by 3.2.4 there is some i so that A_n is a (simple) quotient of $\mathrm{SL}(2, p_i^{r_i})$. Then A_n is a composition factor of $\mathrm{SL}(2, p_i^{r_i})$. Certainly A_n is not cyclic so by 3.2.5 there must be an isomorphism $A_n \cong \mathrm{PSL}(2, p_i)$. Then considering orders,

$$\frac{n!}{2} = \frac{(p_i^2 - 1)p_i}{2}$$

so by 3.2.6 we see $n \leq 5$. This is a contradiction and so we se that A_n is not a quotient of $\mathrm{SL}(2, d)$. ■

Finally, we can prove that each of the K_n are non-congruence subgroups.

Corollary 3.2.8 *For any $n \geq 6$, the kernel K_n does not contain any of the subgroups $\Gamma(d)$. Therefore, K_n is a non-congruence subgroup.*

Proof: If K_n contains $\Gamma(d)$ then we can denote by $\overline{K_n}$ the quotient $K_n/\Gamma(d)$ and write

$$A_n \cong \mathrm{SL}(2, \mathbb{Z})/K_n \cong (\mathrm{SL}(2, \mathbb{Z})/\Gamma(d))/(K_n/\Gamma(d)) \cong \mathrm{SL}(2, d)/\overline{K_n}$$

which shows that A_n is a quotient of $\mathrm{SL}(2, d)$, contradicting 3.2.7. ■

So we have arrived at our family of non-congruence subgroups.

3.3 The geometric level of a finite index subgroup and the Fricke-Wohlfahrt theorem

Proposition 3.2.2 tells us that solving the congruence subgroup problem in $\mathrm{SL}(2,\mathbb{Z})$ or Γ are equivalent problems. With this in mind we will work primarily in Γ. In the beginning of this chapter we associated to each congruence subgroup G a number called its level which is the minimal integer d such that $\Gamma(d)$ is a subgroup of G. More generally, given any finite index subgroup G of Γ, we can associate to it an integer called its geometric level. Recall that T denotes the image of the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

in Γ. Now Γ permutes the cosets of G, acting by left multiplication. If G is a finite index then this action corresponds to a permutation representation on a finite set and therefore induced a homomorphism to a finite symmetric group. The geometric level of G is the order of T under this homomorphism.

Definition 3.3.1 *Let G be a subgroup of Γ with finite index μ and let $p : \Gamma \to S_\mu$ be the coset representation afforded by G, where S_μ is the symmetric group on μ elements. Define the* **geometric level** *of G, denoted $\mathrm{geolevel}(G)$ to be the order of the element $p(T)$ in S_μ.*

The following lemma will be of use.

Lemma 3.3.2 *Let G be a finite index subgroup of Γ. Then*

$$\mathrm{geolevel}(G) = \min\left\{\, k \geq 1 \;\middle|\; \langle\langle T^N \rangle\rangle \subseteq G \,\right\}.$$

In particular, if $G = \ker \varphi$ *for some homomorphism* φ *then* $\operatorname{geolevel}(G)$ *equals the order of* $\varphi(T)$.

Proof: Let $\operatorname{geolevel}(G) = d$. Then T^d acts trivially on the $G-$cosets of Γ so we have $T^d gG = gG$ for all $g \in G$. Then $g^{-1}T^d g \in G$ for all g and so $\langle\langle T^d \rangle\rangle \subseteq G$. We claim that d is minimal. Suppose k is the smallest positive integer for which $\langle\langle T^k \rangle\rangle \subseteq G$. Then given $g \in G$, write $g^{-1}T^k g = x \in G$ and observe that $T^k gG = gxG = gG$ so $T^k \in \ker p$. Since k is the smallest integer for which this is true, it must be that $k = d$. Therefore, we see that

$$\operatorname{geolevel}(G) = d = \min \left\{ k \geq 1 \;\middle|\; \langle\langle T^k \rangle\rangle \subseteq G \right\}.$$

If further G is normal so that $G = \ker \varphi$ for some homomorphism φ then

$$\operatorname{geolevel}(G) = d = \min \left\{ k \geq 1 \;\middle|\; T^k \in \ker \varphi \right\} = |\varphi(T)|.$$

■

Our goal will be to prove that when G is a congruence subgroup then $\operatorname{geolevel}(G) = \operatorname{level}(G)$. Lemma 3.3.3 will be our first step.

Lemma 3.3.3 *Suppose* G *is a congruence subgroup. Then* $\operatorname{geolevel}(G) \leq \operatorname{level}(G)$.

Proof: Let $n = \operatorname{level}(G)$ and $d = \operatorname{geolevel}(G)$. Since $\Gamma(n) \subseteq G$ and $\Gamma(n)$ is normal, we see that $\langle\langle T^n \rangle\rangle \subseteq G$. But since $\operatorname{geolevel}(G) = m$, we know m is the least integer for which this is true. Therefore $m \leq n$. ■

It is a nontrivial theorem due to Fricke and Wohlfahrt that when G is a congruence subgroup, then its level and geometric level agree. The following lemmas are a series of reductions that will allow us to ultimately prove the Fricke-Wohlfahrt theorem.

Lemma 3.3.4 *Let k and n be positive integers and suppose $A \in \Gamma(k)$. If the off-diagonal entries of A are divisible by n then $AB \in \Gamma(n)$ for some $B \in \langle\langle T^k \rangle\rangle$.*

Proof: Let $A \in \Gamma$ such that the off-diagonal entries of A are divisible by n. Define a function $\Phi : \Gamma \to \Gamma$ by

$$\Phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & ad-1 \\ 1-ad & d(2-ad) \end{pmatrix}.$$

Note that if $V = TU^{-1}T^3U^{-1}T$ then

$$\Phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ST^{d-1}S)^{-1}(VT^{a-1}V^{-1})T^{d-1}$$

hence $\Phi(A)$ is an element of $\langle\langle T^k \rangle\rangle$ since $a-1 = d-1 = 0 \mod k$. As both b and c are divisible by n and $ad - bc = 1$, we have $ad = 1 \mod n$ and so $A = \Phi(A)$ mod n. Equivalently, $A\Phi(A)^{-1} \in \Gamma(n)$. Thus we can take $B = \Phi(A)^{-1}$. ■

Lemma 3.3.5 *Let k and n be positive integers and suppose $A \in \Gamma(k)$. If the diagonal entires of A are relatively prime to n then there is a matrix $C \in \langle\langle T^k \rangle\rangle$ so that the off diagonal entries of CA are divisible by n.*

Proof: Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $\gcd(a, n) = 1$. Then a is a unit mod n say with inverse a'. We can write

$c = m\widetilde{c}$ and let $p = -a'\widetilde{c}$. Then

$$(ST^mS)^{-p}A = \begin{pmatrix} 1 & 0 \\ mp & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c+amp & d+bmp \end{pmatrix}$$

and $c + amp = m(\widetilde{c} - a'a\widetilde{c})$ is congruent to 0 mod n. Let $\widetilde{d} = d + bmp$. Taking the determinant of $(ST^mS)^{-p}A$, we see that $\widetilde{d}$ is relatively prime to n. Therefore we can also choose ℓ so that $b + \widetilde{d}m\ell = 0$ mod n. In this case,

$$T^{m\ell}(ST^mS)^{-p}A = \begin{pmatrix} 1 & m\ell \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c+amp & \widetilde{d} \end{pmatrix} = \begin{pmatrix} * & b+\widetilde{d}m\ell \\ c+amp & \widetilde{d} \end{pmatrix}$$

has both off diagonal entries congruent to 0 mod n. Take $C = T^{m\ell}(ST^mS)^{-p}$.

■

Lemma 3.3.6 *Let k and n be positive integers. For any $A \in \Gamma(k)$ there is $M \in \langle\langle T^k \rangle\rangle$ so that the diagonal entries of AM are relatively prime to n.*

Proof: If the diagonal entries of A are already relatively prime to n are done. Otherwise, $\gcd(a, n) \neq 1$ or $\gcd(d, n) \neq 1$. Suppose first that $\gcd(a, n) \neq 1$. Since $ad - bc = 1$ we know $\gcd(a, b) = 1$. Then since $a = 1$ mod k, we also have $\gcd(a, bk) = 1$. Recall Dirichlet's theorem on primes in arithmetic progressions: Suppose r and s are relatively prime integers. Then

$$\{\, r + st \mid t \in \mathbb{Z} \,\}$$

contains infinitely many prime numbers. In particular, taking $r = a$ and $s = bk$ we can choose an integer p so that $a + bkp$ is a prime number larger than n.

Then

$$A(ST^kS)^{-p} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ mp & 1 \end{pmatrix} = \begin{pmatrix} a+bkp & b \\ c+dkp & d \end{pmatrix}$$

has upper left entry relatively prime to n. If further $\gcd(d,n)=1$ then $A(ST^kS)^{-p}$ has diagonal entires relatively prime to n and we are done, taking $M=(ST^kS)^{-p}$. Otherwise, let $\widetilde{a} = a+bmk$, let $\widetilde{c} = c+dmk$ and note that $\widetilde{a}d - b\widetilde{c} = 1$ so $\gcd(\widetilde{c},d)=1$. As $\gcd(d,k)=1$, just as above we can choose ℓ so that $d+\widetilde{c}k\ell$ is a prime number larger than n. Then

$$A(ST^kS)^{-p}T^{m\ell} = \begin{pmatrix} \widetilde{a} & b \\ \widetilde{c} & d \end{pmatrix} \begin{pmatrix} 1 & m\ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \widetilde{a} & * \\ \widetilde{c} & d+\widetilde{c}kp \end{pmatrix}$$

and $A(ST^kS)^{-p}T^{m\ell}$ has diagonal entries relatively prime to n. Hence we can set $M=(ST^kS)^{-p}T^{m\ell}$. ■

These three lemmas together imply the following:

Lemma 3.3.7 *Let k and n be positive integers. Then $\Gamma(k) \subseteq \langle\langle T^k\rangle\rangle\Gamma(n)\langle\langle T^k\rangle\rangle$.*

Proof: Let $A \in \Gamma(k)$. Then by 3.3.6, there is some $M \in \langle\langle T^k\rangle\rangle$ so that AM has diagonal entries relatively prime to n. Lemma 3.3.5 tells us we can choose $C \in \langle\langle T^k\rangle\rangle$ so that CAM has off-diagonal entires divisible by n. Lastly, Lemma 3.3.4 implies $CAMB \in \Gamma(n)$ for some $B \in \langle\langle T^k\rangle\rangle$. Rearranging, we see $A \in \langle\langle T^k\rangle\rangle\Gamma(n)\langle\langle T^k\rangle\rangle$. ■

The Fricke-Wohlfahrt now follows as a corollary of the previous Lemma.

Theorem 3.3.8 (Fricke-Wohlfahrt theorem) *Suppose G is a congruence subgroup of Γ. Then the level of G equals the geometric level of G.*

Proof: Let $d = \text{geolevel}(G)$ and $n = \text{level}(G)$. Then $\Gamma(n) \subseteq G$ and $\langle\langle T^d \rangle\rangle \subseteq G$. By Lemma 3.3.7, $\Gamma(d) \subseteq \langle\langle T^d \rangle\rangle \Gamma(n) \langle\langle T^d \rangle\rangle$, therefore $\Gamma(d) \subseteq G$. Since $\text{level}(G) = n$, it must be that $d \geq n$. However, by Lemma 3.3.3 we know that $n \leq d$, so it must be that $d = n$. ■

Our main use of the Fricke-Wohlfahrt theorem is Corollary 3.3.9, which gives us a way to decide whether G is a congruence subgroup as long as we can compute its geometric level. In the cases we will be considering, G will be the kernel of a representation and so the geometric level of G will be the order of the image of T under the representation.

Corollary 3.3.9 *Suppose G is a finite index subgroup of Γ with geometric level d. If $\Gamma(d) \not\subseteq G$ then G is non-congruence subgroup.*

3.3.1 Generators for $\Gamma(d)$

Corollary 3.3.9 can actually be put to practical use. If S is a generating set for $\Gamma(d)$ then it is enough to check if $S \subseteq G$. Later, we will be interested exclusively in the case that $G = \ker \rho$ for a finite-dimensional representation ρ with finite image and so it would be sufficient to check whether the elements of S are sent to the identity under ρ. Fortunately, in [Hsu96], Tim Hsu was able to construct reasonably small normal generating sets for all the principal congruence subgroups of Γ and we record his results below.

Proposition 3.3.10 *Let d be an integer greater than one. Write $d = ek$ where e is a power of two and k is odd and let G_d be the corresponding set of elements corresponding to d listed below. Then in any of the above cases, $\Gamma(d) = \langle\langle G_d \rangle\rangle$.*

(i) (d is odd) If $e = 1$ then let $t(d)$ be the multiplicative inverse of 2 mod d and

$$G_d = \left\{ T^d,\ (U^2 T^{-t(d)})^3 \right\}.$$

(ii) (d is a power of two) If $k = 1$ then let $f(d)$ be the multiplicative inverse of 5 mod d and set $P_d = T^{20}U^{f(d)}T^{-4}U^{-1}$. Then

$$G_d = \left\{ T^d,\, (P_d U^5 T U^{-1} T)^3,\, (TU^{-1}T)^{-1} P_d (TU^{-1}T) P_d \right\}.$$

(iii) (d even, not a power of two) If $e > 1$ and $k > 1$ then let a be the unique integer mod d so that

$$\begin{aligned} a &= 0 \mod e \\ a &= 1 \mod k \end{aligned}$$

and let b be the unique integer mod d so that

$$\begin{aligned} b &= 0 \mod k \\ b &= 1 \mod e. \end{aligned}$$

Write $t(d)$ for the multiplicative inverse of 2 mod k and $f(d)$ for the multiplicative inverse of 5 mod e,let

$$\begin{aligned} x &= T^a & \qquad z &= T^b \\ y &= U^a & \qquad w &= U^b, \end{aligned}$$

and $p_d = z^{20}w^{f(d)}z^{-4}w^{-1}$. Then G_d is given by

$$\Big\{ T^d,\, [x, w],\, (xy^{-1}x)^4,\, (xy^{-1}x)^2(x^{-1}y)^3,\, (xy^{-1}x)^2(x^{t(d)}y^{-2})^3,$$

$$(zw^{-1}z)^2(p_d w^5 zw^{-1}z)^{-3},\ (zw^{-1}z)^{-1}p_d(zw^{-1}z)p_d,\ w^{25}p_d w^{-1}p_d^{-1}\Big\}.$$

We can combine this with Corollary 3.3.9 to get the following result. This will be a central tool for our main results.

Corollary 3.3.11 *Let H be a finite group. Suppose $\varphi : \Gamma \to H$ is a homomorphism and let d be the order of $\varphi(T)$. Then $\ker\varphi$ is a congruence subgroup if and only if $G_d \subseteq \ker\varphi$. In this case, $\mathrm{level}(\ker\varphi) = d$.*

Proof: By 3.3.2, $\ker\varphi$ has geometric level equal to the order of d. If $\ker\varphi$ is a congruence subgroup then $\mathrm{level}(\ker\varphi) = d$ by the Fricke-Wohlfahrt theorem and we must have $\Gamma(d) \subseteq \ker\varphi$. So clearly $G_d \subseteq \ker\varphi$. Now suppose $G_d \subseteq \ker\varphi$. Then since $\ker\varphi$ is normal, we see $\langle\langle G_d\rangle\rangle \subseteq \ker\varphi$ as well. In particular, $\ker\varphi$ contains $\Gamma(d)$, so $\ker\varphi$ is a congruence subgroup of level at most d. If $\ker\varphi$ contains $\Gamma(k)$ for some $k < d$ then $T^k \in \ker\varphi$, which contradicts d being the order of $\varphi(T)$. ■

3.4 The Ng-Schauenburg theorem for quantum representations and our main problem

The bridge between this and the previous chapter is the Ng-Schauenburg theorem, presented below. It establishes a connection between quantum representations of $\mathrm{SL}(2,\mathbb{Z})$ and congruence subgroups.

Theorem 3.4.1 ([NS10]) *Let $\mathcal{C}$ be a modular category and $\rho_{\mathcal{C}}$ the quantum representation of $\mathrm{SL}(2,\mathbb{Z})$ associated to $\mathcal{C}$. Then the kernel of the $\rho_{\mathcal{C}}$ is a congruence subgroup.*

This provides us with motivation for our main problem. We know from Chapter 2 that given any modular tensor category $\mathcal{C}$ we can associated to every surface a projective representation of its mapping class group. If we replace the torus by the n-times punctures disc, we obtain the quantum representations of B_n discussed in Chapter 2. Recall that $B_3/Z(B_3) \cong \Gamma$, so we can associate to subgroups of B_3 the same congruence or non-congruence property of subgroups of Γ. In particular, given an irreducible quantum representation of B_3 with finite image, we can first replace it by a representation that factors through the quotient map π. This is because the center acts by some scalar by Schur's Lemma and so we can scale this away. In this case we end up with a finite representation of Γ and so it makes sense to ask whether or not the kernel of this induced representation is a congruence subgroup. Is there a way to compute the level or geometric level in terms of the data of the representation. The corollary at the end of the previous section gives us the first step towards answering these questions. Let G_d be the set of generators of $\Gamma(d)$ in Hsu's theorem.

Theorem 3.4.2 *Let $\rho : B_3 \to \mathrm{GL}(n, \mathbb{C})$ be a representation with finite image that factors through π and let d be the order of $\rho(\sigma_1)$. Then $\pi(\ker \rho)$ is a congruence subgroup of Γ if and only if $\pi^{-1}(G_d) \subseteq \ker \rho$.*

Proof: Since ρ factors through π, there is an induced representation $\bar{\rho}$ of Γ, which also has finite image. Then by 3.3.11, we see that $\pi(\ker \rho) = \ker \bar{\rho}$ is a congruence subgroup if and only $G_d \subseteq \ker \bar{\rho}$ where d is the order of $\bar{\rho}(T)$. But $\rho(\sigma_1) = \bar{\rho}(\pi(\sigma_1))$, so taking preimages, the result follows. ■

We now have a systematic approach to deciding whether or not a (quantum or otherwise) representation of B_3 gives rise to a congruence subgroup via the kernel of a possibly scaled version of the representation. The next step, which is carried out in Chapter 4, is to parametrize the space of two or three dimensional irreducible representations of

B_3 with finite image and for those which factor through π, decide whether the induced kernel is a congruence subgroup. We can specialize Hsu's work to the case of a matrix representation. Since the representations we will be concerned with have finite image, the image of the generators T and U must have finite projective order and finite order. So while they may seem quite specific, the two hypotheses in subsequent proposition are actually quite generic to our situation.

Proposition 3.4.3 *Let H be a finite group and $\rho : \Gamma \to H$ a homomorphism and write $\rho(T) = A$ and $\rho(U) = B^{-1}$. Suppose A^r is central and the order of A is an even composite integer d that is not a power of 2 and let $G_d, a, b, t(d), f(d), x, y, z, w, p_d$ be an in 3.3.10.*

(i) If d divides 24, a is a multiple of r, $12a$ is a multiple of d, $3at(d)$ is a multiple of d and $\rho(p_d)$ is a central element of order at most 2, then $\ker\rho$ *is a congruence subgroup of level d if $\rho((zw^{-1}z)^2) = \rho(p_d(w^5zw^{-1}z)^3)$.*

(ii) If b is a multiple of r, $12b$ is a multiple of d, and $(17 - f(d))b$ is a multiple of d then $\ker\rho$ *is a congruence subgroup of level d if $\rho((xy^{-1}x)^2) = \rho((y^2x^{-t(d)})^3)$.*

Proof: Let us consider each case separately. Note that A and B have the same order since they are conjugate. According to 3.3.11, we know that $\ker\rho$ is a congruence subgroup if and only if $G_d \subseteq \ker\rho$. Then we must show that each element of

$$\Big\{T^d,\ [x,w],\ (xy^{-1}x)^4,\ (xy^{-1}x)^2(x^{-1}y)^3,\ (xy^{-1}x)^2(x^{t(d)}y^{-2})^3,\\ (zw^{-1}z)^2(p_dw^5zw^{-1}z)^{-3},\ (zw^{-1}z)^{-1}p_d(zw^{-1}z)p_d,\ w^{25}p_dw^{-1}p_d^{-1}\Big\}.$$

is mapped to the identity under ρ. Since A has order d, we see that $\rho(T^d)$ is the identity, so we need only be concerned with the elements above other than

T^d. First let us suppose the hypotheses of (i). As a is a multiple of r, the element $\rho(x) = A^a$ is central so that $[x, w] \in \ker \rho$. Next, we can compute $\rho((xy^{-1}x)^4) = A^{12a}$ which must be the identity since $12a$ is a multiple of d. Also $\rho((xy^{-1}x)^2(x^{-1}y)^3) = A^{6a}A^{-6a}$ is the identity and $\rho((xy^{-1}x)^2(x^{t(d)}y^{-2})^3) = A^{12a+3at(d)} = A^{3at(d)}$ but since $3at(d)$ is a mutliple of d, we know this is trivial. We can compute $\rho((zw^{-1}z)^{-1}p_d(zw^{-1}z)p_d)$ is the identity since $\rho(p_d)$ is central and of order at most 2. Finally, since d divides 24, we know that $\rho(w^25p_dw^{-1}p_d^{-1}) = \rho(w^{24}) = B^{-24b} = (B^{24})^{-b}$ is the identity since B^{24} is. Hence, we can conclude $\ker \rho$ is a congruence subgroup of level d if $\rho((zw^{-1}z)^2) = \rho(p_6(w^5zw^{-1}z)^3)$, since then $G_d \subseteq \ker \rho$.

Now let us consider the second scenario described above. Since b is a multiple of r, we know that A^b is central in H. Then $\rho(p_d) = \rho(z^{20}w^{f(d)}z^{-4}w^{-1}) = A^{(17-f(d))b}$ which must be the identity since $(17 - f(d))b$ is a multiple of d. Therefore $p_d \in \ker \rho$ so that $\rho((zw^{-1}z)^{-1}p_d(zw^{-1}z)p_d)$ is the identity. We can then compute $\rho((zw^{-1}z)^2(p_dw^5zw^{-1}z)^{-3}) = A^{12b}$ and this is the identity since $12b$ divides d. This also implies $\rho(w^{25}p_dw^{-1}p_d) = \rho(w^{24}) = B^{-24b}$ is the identity. As b is a multiple of r, we know that $\rho(w) = A^b$ is central in H, so then $[x, w] \in \ker \rho$. Again because $12b$ divides d we know that $\rho((xy^{-1}x)^4) = A^{-12b}(ABA)^4$ is trivial. Lastly, $\rho((xy^{-1}x)^2) = A^{6b}(ABA)^2 = A^{6b}$ and $\rho((y^{-1}x)^3) = A^{-6b}(BA)^3 = A^{6b}$ so that $(xy^{-1}x)^2(x^{-1}y)^3 \in \ker \rho$. Thus, we are able to conclude that $\ker \rho$ is a congruence subgroup of level d if $\rho((xy^{-1}x)^2) = \rho((y^2x^{-t(d)})^3)$. ■

Chapter 4

Congruence subgroups and low-dimensional representations of B_3

This chapter is devoted to presenting the main results in our work in understanding the congruence subgroup problem for quantum representations of B_3. It is broken up into three sections. The first section examines our problem for two-dimensional representations. We are able to show through a series of reductions and lemmas that the space of two-dimensional irreducible representations of B_3 with finite image that factor through the quotient map $\pi : B_3 \to \Gamma$ is parametrized by a finite set. The same holds in dimension three for the subset of representations with the projective order of the image of σ_1 being between 3 and 5. The Tuba and Wenzl classification of low-dimensional representations is our main tool here, together with the work of Rowell and Tuba. Tuba and Wenzl showed that for two and three dimensional irreducible representations ρ of B_3, the equivalence class of ρ is completely determined by the set $\text{spec}(\rho(\sigma_1))$. They also provides us with a standard representative for each equivalence class, which is a function of the eigenvalues of $\rho(\sigma_1)$. Rowell and Tuba provided a condition on the eigenvalues of $\rho(\sigma_1)$ which determined whether the image $\rho(B_3)$ is a finite group. Our parametrization is deduced by combining their results into an algebraic condition on eigenvalues of $\rho(\sigma_1)$ which determine when the representation ρ factors through π and has finite image. We can then apply the corollary to Hsu's theorem (3.3.11) to each representation. In dimension two, we find that all representations have kernels that project onto congruence subgroups of Γ. The same is true for the three dimensional representations with the the projective order of the image of σ_1 between 3 and 5. However, we are able to explicitly provide examples of irreducible three-dimensional representations with finite image that factor through π such that the projective order is any odd integer greater than or equal to 5 and $\pi(\ker \rho)$ is a non-congruence subgroup of Γ. In particular, the Ng-Schauenburg Theorem does not generalize to quantum representations of B_3 under this formulation. Nonetheless, we are still able to classify many representations and construct interesting examples of non-congruence subgroup of Γ. Moreover, we can show that some of our examples arise via quantum representations.

4.1 Two-dimensional representations

Let us first examine the situation for two-dimensional representations. First, we have the following easy proposition.

Proposition 4.1.1 *Let λ_1 and λ_2 be nonzero complex numbers. Then $\rho_{\lambda_1,\lambda_2} : B_3 \to \mathrm{GL}(2,\mathbb{C})$ given by*

$$\rho_{\lambda_1,\lambda_2}(\sigma_1) = \begin{pmatrix} \lambda_1 & \lambda_1 \\ 0 & \lambda_2 \end{pmatrix}, \quad \rho_{\lambda_1,\lambda_2}(\sigma_2) = \begin{pmatrix} \lambda_2 & 0 \\ -\lambda_2 & \lambda_1 \end{pmatrix}$$

defines a representation of B_3*.*

Proof: Let

$$A = \begin{pmatrix} \lambda_1 & \lambda_1 \\ 0 & \lambda_2 \end{pmatrix}$$

and

$$B = \begin{pmatrix} \lambda_2 & 0 \\ -\lambda_2 & \lambda_1 \end{pmatrix}.$$

Then we need to show that $ABA = BAB$. It is an easy calculation to show that

$$ABA = \begin{pmatrix} 0 & \lambda_1^2\lambda_2 \\ -\lambda_1\lambda_2^2 & 0 \end{pmatrix} = BAB$$

so that $\rho_{\lambda_1,\lambda_2}$ does indeed define a representation. ■

We will use the notation $\rho_{\lambda_1,\lambda_2}$ throughout the rest of this work. Tuba and Wenzl were able to classify irreducible representations of B_3 and $\mathrm{SL}(2,\mathbb{Z})$ by the spectrum of the image of the braid generator. In dimension two, their result takes the following form. From the above we can see that $\mathrm{spec}(\rho_{\lambda_1,\lambda_2}(\sigma_1)) = \{\,\lambda_1, \lambda_2\,\}$. The Tuba-Wenzl (TW) classification tells us that in fact irreducible two-dimensional representations are determined by the spectrum of the image of σ_1 and (almost) any two non-zero complex numbers determine an irreducible representation, namely $\rho_{\lambda_1,\lambda_2}$. Moreover, we get a condition on the eigenvalues to ensure that the representation factors through the quotient map π.

Theorem 4.1.2 ([TW01])

(i) Let N_2 *be the zero set of* $\lambda_1^1 + \lambda_1\lambda_2 + \lambda_2^2$*. There is a bijection between conjugacy classes of irreducible* 2*-dimensional representations of* B_3 *and* S_2*-orbits of* $\mathbb{C}^2 \setminus N_2$*.*

(ii) Suppose $\rho : B_3 \to \mathrm{GL}(2, \mathbb{C})$ *is irreducible and* $\mathrm{spec}(\rho(\sigma_1)) = \{ \lambda_1, \lambda_2 \}$*. Then* ρ *is equivalent to* $\rho_{\lambda_1,\lambda_2}$*. Furthermore,* ρ *factors through* π *if and only if* $-(\lambda_1\lambda_2)^3 = 1$*.*

Example 4.1.3 *The representation* $\rho_{1,1} : B_3 \to \mathrm{GL}(2, \mathbb{C})$ *is the composition of the projection*

$$\sigma_1 \mapsto T, \quad \sigma_2 \mapsto U^{-1}$$

followed by the inclusion $\mathrm{SL}(2, \mathbb{Z}) \hookrightarrow \mathrm{GL}(2, \mathbb{C})$*. Observe that*

$$\rho_{1,1}(\sigma_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho_{1,1}(\sigma_2) = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

which are T *and* U^{-1} *respectively.*

Rowell and Tuba provided criteria to determine when the image of an irreducible representation of B_3 is finite from the eigenvalues of σ_1. We provide the version of their results for dimension two below. In this case, the finiteness is guaranteed whenever the projective order of the matrix assigned to σ_1 is between 2 and 5. First, recall the definition of projective order.

Definition 4.1.4 *Let* A *be an* $n \times n$ *matrix with eigenvalues* $\lambda_1, \lambda_2, \ldots, \lambda_n$*. Define the* **projective order** *of* A *to be*

$$\mathrm{po}(A) = \min \left\{ t > 1 \;\middle|\; \lambda_1^t = \cdots = \lambda_n^t \right\}$$

where this is allowed to be infinite. The projective order of a matrix is invariant under scaling. That is, $\mathrm{po}(A) = \mathrm{po}(\theta A)$ *for all* $\theta \in \mathbb{C}^*$*. Equivalently,* $\mathrm{po}(A)$ *can be defined to be the order* A *viewed as an element of* $\mathrm{PGL}(d, \mathbb{C})$*.*

Theorem 4.1.5 (**[RT10]**) *Suppose $\rho : B_3 \to \mathrm{GL}(2, \mathbb{C})$ is an irreducible representation. Write $\mathrm{spec}(\rho(\sigma_1)) = \{\, \lambda_1, \lambda_2 \,\}$. Then $\rho(B_3)$ is finite if and only if λ_1 and λ_2 are distinct roots of unity and $2 \leq \mathrm{po}(\rho(\sigma_1)) \leq 5$.*

Example 4.1.6 *We know that the image of $\rho_{1,1}$ cannot be finite since its image is $\mathrm{SL}(2, \mathbb{Z})$. As $\mathrm{po}(\rho_{1,1}(\sigma_1)) = 1$, this confirms the sharpness of the lower bound above.*

Example 4.1.7 *Let us revisit the representation $\rho_{\sigma,3,\sigma}$ from Example 2.2.4 associated to the Ising fusion rule. We have*

$$\rho_{\sigma,3,\sigma}(\sigma_1) = \begin{pmatrix} e^{-\pi i/8} & 0 \\ 0 & e^{3\pi i/8} \end{pmatrix}, \quad \rho_{\sigma,3,\sigma}(\sigma_2) = \frac{1}{2}\begin{pmatrix} e^{-\pi i/8} + e^{3\pi i/8} & e^{-\pi i/8} - e^{3\pi i/8} \\ e^{-\pi i/8} - e^{3\pi i/8} & e^{-\pi i/8} + e^{3\pi i/8} \end{pmatrix}$$

so that $\mathrm{spec}(\rho_{\sigma,3,\sigma}(\sigma_1)) = \{\, e^{-\pi i/8}, e^{3\pi i/8} \,\}$. Then we see that $\rho_{\sigma,3,\sigma}$ is equivalent to $\rho_{e^{\pi i/8}, e^{3\pi i/8}}$, is irreducible, and has finite image since $\mathrm{po}(\rho_{\sigma,3,\sigma}(\sigma_1)) = 4$.

Example 4.1.8 *Recall the Fibonacci representation $\rho_{\tau,3\tau}$. Since $R_1^{\tau\tau} = e^{4\pi i/5}$ and $R_\tau^{\tau\tau} = e^{3\pi i/5}$, we see that $\mathrm{po}(\rho_{\tau,3,\tau}(\sigma_1)) = 10$. This is consistent with what we should expect since the image of $\rho_{\tau,3\tau}$ is dense in $\mathrm{SU}(2)$ (so certainly not finite).*

If we combine the above result with Theorem 4.1.2 then we can derive an algebraic condition on the eigenvalues of the image of σ_1 under an irreducible representation to determine when the image image is finite and the representation factors through the quotient map $\pi : B_3 \to \Gamma$.

Corollary 4.1.9 *Suppose $\rho : B_3 \to \mathrm{GL}(2, \mathbb{C})$ is an irreducible representation with finite image that factors through π. Then ρ is equivalent to $\rho_{\lambda, e^{2\pi i j/r}\lambda}$ for some r with $2 \leq r \leq 5$,*

$j \in \mathbb{Z}_r^\times$, and some λ such that

$$\lambda^6 + e^{-6\pi ij/r} = 0. \tag{4.1}$$

Proof: Since $\rho(B_3)$ is finite, by 4.1.5, we can write $\operatorname{spec}(\rho(\sigma_1)) = \{\,\lambda, e^{2\pi ij/r}\lambda\,\}$ for some r between 2 and 5 and $j \in \mathbb{Z}_r^\times$. In particular, ρ is equivalent to $\rho_{\lambda, e^{2\pi ij/r}\lambda}$, by the Wenzl classification. Tuba-Wenzl also implies $-(\lambda e^{2\pi ij/r}\lambda)^3 = 1$ since ρ factors through π. Then

$$\lambda^6 + e^{-6\pi ij/r} = 0$$

as claimed. ■

4.1.1 Projective order lemmas

The Tuba-Wenzl classification and the above lemma tell us that for each r between 2 and 5 and $j \in \mathbb{Z}_r^\times$ and each solution to $\lambda^6 + e^{-6\pi ij/r} = 0$, the representations $\rho_{\lambda, e^{2\pi ij/r}\lambda}$ factor through π. Accordingly, there is an irreducible representation $\rho_{r,j,\lambda}$ of Γ so that $\rho_{\lambda, e^{2\pi ij/r}\lambda} = \rho_{r,j,\lambda} \circ \pi$. However, Corollary 4.1.9 does not provide an exact parametrization, as their is some redundancy. Here we give a series of lemmas with the goal of parametrizing the space of (equivalence classes of) irreducible two-dimensional representations of Γ that have finite image. By applying the above results and few more reductions, we are able to show that there are just finitely many options and list them all. These representations are in bijection with a complete list of isomorphism classes of irreducible two-dimensional representations of B_3 with finite image that factor through π, so we will have obtained a complete list of all representations we need to inspect. The strategy is to classify the representations according to the projective order of the image of σ_1. Following Rowell and Tuba, we need only consider projective orders between 2 and 5. Let us start with projective order 2.

Lemma 4.1.10 *Suppose* $\rho : \Gamma \to \mathrm{GL}(2, \mathbb{C})$ *is an irreducible representation with finite image such that* $\mathrm{po}(\rho(T)) = 2$*. Then* ρ *is equivalent to* $\rho_{2,1,\lambda}$ *for some* $\lambda \in \{ 1, e^{2\pi i/6}, e^{4\pi i/6} \}$.

Here we continue with those representations mapping σ_1 to a matrix of projective order 3,4, or 5.

Proof: Let $A = \rho(T)$. Since $\mathrm{po}(A) = 2$, we know that $\mathrm{spec}(A) = \{ \lambda, -\lambda \}$ for some eigenvalue λ of A. By Tuba-Wenzl, we see that $\lambda^6 = 1$ so that λ is a 6th root of unity. If λ is a 6th root of unity, then so is $-\lambda$, hence the only unique cases are $\lambda = 1, e^{2\pi i/6}$, or $e^{4\pi i/6}$. ■

Lemma 4.1.11 *Suppose* $\rho : \Gamma \to \mathrm{GL}(2, \mathbb{C})$ *is an irreducible representation with finite image such that* $\mathrm{po}(\rho(T)) = 3$*. Then* ρ *is equivalent to* $\rho_{3,1,\lambda}$ *for some* $\lambda \in \{ e^{(1+2k)\pi i/6} \mid 0 \leq k \leq 5 \}$.

Proof: Let $A = \rho(T)$ and let $\lambda \in \mathrm{spec}(A)$. Since $\mathrm{po}(A) = 3$, we know that the other eigenvalue of A is either $e^{2\pi i/3}\lambda$ or $e^{4\pi i/3}\lambda$. If it is $e^{4\pi i/3}\lambda$, write $\mu = e^{4\pi i/3}\lambda$, so that $\mathrm{spec}(A)$ can be written $\{ \mu, e^{2\pi i/3}\mu \}$. By the Tuba-Wenzl classification, we see that $\mu^6 + 1 = 0$ so therefore ρ is equivalent to a representation of the form $\rho_{3,1,\lambda}$ where $\lambda \in \{ e^{(1+2k)\pi i/6} \mid 0 \leq k \leq 5 \}$. ■

Lemma 4.1.12 *Suppose* $\rho : \Gamma \to \mathrm{GL}(2, \mathbb{C})$ *is an irreducible representation with finite image such that* $\mathrm{po}(\rho(T)) = 4$*. Then* ρ *is equivalent to* $\rho_{4,1,\lambda}$ *for some* $\lambda \in \{ e^{(3+4k)\pi i/12} \mid 0 \leq k \leq 5 \}$.

Proof: Let $A = \rho(T)$. Similarly to the previous lemma, we can arrange is so that $\mathrm{spec}(A) = \{ \lambda, i\lambda \}$ for some λ satisfying $\lambda^6 + i$ where $\lambda \in \{ e^{(3+4k)\pi i/12} \mid 0 \leq k \leq 5 \}$.

■

Lemma 4.1.13 *Suppose* $\rho : \Gamma \to \mathrm{GL}(2, \mathbb{C})$ *is an irreducible representation with finite image such that* $\mathrm{po}(\rho(T)) = 5$*. Then* ρ *is equivalent to* $\rho_{5,1,\lambda}$ *for some* $\lambda \in \{ e^{(9+10k)\pi i/30} \mid 0 \leq k \leq 5 \}$ *or* $\rho_{5,2,\lambda}$ *for some* $\lambda \in \{ e^{(13+10k)\pi i/30} \mid 0 \leq k \leq 5 \}$.

Proof: Let $A = \rho(T)$. Again applying the technique in the proof of Lemma 4.1.11, we can always arrange it so that spec(A) is of the form $\{\,\lambda, e^{2\pi i/5\lambda}\,\}$ where λ satisfies $\lambda^6 + e^{4\pi i/5} = 0$ or $\{\,\lambda, e^{4\pi i/5}\lambda\,\}$ for some λ such that $\lambda^6 + e^{8\pi i5} = 0$ and these exhaust all possibilities when po$(A) = 5$. Thus ρ is equivalent to $\rho_{5,1,\lambda}$ for some $\lambda \in \{\,e^{(9+10k)\pi i/30} \mid 0 \le k \le 5\,\}$ or $\rho_{5,2,\lambda}$ for some $\lambda \in \{\,e^{(13+10k)\pi i/30} \mid 0 \le k \le 5\,\}$. ■

This in fact completely classifies all two-dimensional irreducible representations of Γ with finite image, which we have summarized below.

Theorem 4.1.14 *Suppose $\rho : \Gamma \to \mathrm{GL}(2,\mathbb{C})$ is an irreducible representation with finite image. Then ρ is equivalent to one of the representations in the conclusions of Lemmas 4.1.10, 4.1.11, 4.1.12, and 4.1.13.*

Proof: Since $\rho \circ \pi$ is an irreducible 2-dimensional representation of B_3 with finite image that factors through π, we can apply Corollary 4.1.9. Then we see $2 \le \mathrm{po}(\rho(T)) \le 5$, so that ρ must be equivalent to one of the representations in the four lemmas above. ■

4.1.2 Congruence kernels for two-dimensional representations

Now that we have a list of all relevant representations in dimension two, we can apply $Hsu's$ work to decide which representations give rise to congruence subgroups. There are essentially three cases: when the order of the image of σ_1 is 2, 8, or even composite but not a power of two. First, recall that $\langle\langle T^2 \rangle\rangle = \Gamma(2)$.

Proposition 4.1.15 *If ρ is equivalent to one of $\rho_{2,1,1}$ then $\rho(T)$ is of order 2 and* $\ker\rho$ *is a congruence subgroup of level equal to the order of 2.*

Proof: If ρ is equivalent to $\rho_{2,1,1}$ then the order of $\rho(T)$ is 2 and so $\ker\rho$ is a congruence subgroup since $\Gamma(2)$ is normally generated by T^2. ■

The other outlying case if when $d = 8$, considered below.

Proposition 4.1.16 *If ρ is equivalent to one of $\rho_{4,1,e^{3\pi i/12}}$ or $\rho_{4,1,e^{15\pi i/12}}$ then the order of $\rho(T)$ is 8 and* $\ker\rho$ *is a congruence subgroup of level equal to the order of 8.*

Proof: If ρ is equivalent to one of $\rho_{4,1,e^{3\pi i/12}}$, or $\rho_{4,1,e^{15\pi i/12}}$ then we can calculate the order of $\rho(T)$ to be 8. Thus, by 3.3.11, we see $\ker\rho$ is a congruence subgroup if (in the notation of 3.3.10) $\{\, (P_8U^5TU^{-1}T)^3,\, (TU^{-1}T)^{-1}P_8(TU^{-1}T)P_8 \,\} \subseteq \ker\rho$. Let us write $A = \rho(T)$ and $B = \rho(U^{-1})$. Then in either case,

$$\rho(P_8) = A^{20}B^{-f(8)}A^{-4}B = B^{1-f(8)} = B^{-4} = -I,$$

so clearly $(TU^{-1}T)^{-1}P_8(TU^{-1}T)P_8 \in \ker\rho$. Finally we can compute

$$\rho((P_8U^5TU^{-1}T)^3) = (B^{-1}ABA)^3 = (AB)^3 = I$$

since ρ is a representation. Thus we see that the kernel of each of the representations above is a congruence subgroup of level 8. ■

The most encompassing case if when d is a composite integer that is not a power of 2. This allows us to apply Proposition 3.4.3.

Proposition 4.1.17 *Suppose $\rho : \Gamma \to$* GL$(2, \mathbb{C})$ *is an irreducible representation with finite image such that the order of $\rho(T)$ is an even composite integer d that is not a power of two. Then* $\ker\rho$ *is a congruence subgroup of level d.*

Proof: By 4.1.14, ρ is equivalent to one of the representations in the conclusions of the four projective order lemmas above. Of those that map T to a matrix of even composite order which is not a power 2, we have recorded the data in the hypothesis and conclusion of 3.4.3. In particular, in each case we see that the kernel of the representation associated to each row is a congruence subgroup of Γ. First, in the notation of Hsu's theorem (3.3.10), we list the data for the representations such that d divides 24, a is a multiple of r, $12a$ is a multiple of d, $3at(d)$ is a multiple of d and $\rho(p_d)$ is a central element of order at most 2, Then, we can compute $\rho((zw^{-1}z)^2)$ and $\rho(p_d(w^5zw^{?1}z)^3)$ and compare the results, as in the conclusion of 3.4.3.

r	j	λ	d	a	$12a$	$t(d)$	$3at(d)$	$\rho(p_d)$	$\rho(zw^{-1}z)^2$	$\rho(p_dw^5zw^{-1}z)^3$
2	1	$e^{2\pi i/6}$	6	4	48	2	24	I	$-I$	$-I$
2	1	$e^{4\pi i/6}$	6	4	48	2	24	I	$-I$	$-I$
4	1	$e^{7\pi i/12}$	24	16	192	2	96	$-I$	I	I
4	1	$e^{11\pi i/12}$	24	16	192	2	96	$-I$	I	I
4	1	$e^{19\pi i/12}$	24	16	192	2	96	$-I$	I	I
4	1	$e^{23\pi i/12}$	24	16	192	2	96	$-I$	I	I

Next we list collect the data for the representations such that b is a multiple of r, $12b$ is a multiple of d, and $(17 - f(d))b$ is a multiple of d. We then compare $\rho((xy^{-1}x)^2)$ and $\rho((y^2x^{-t(d)})^3)$.

r	j	λ	d	b	$12b$	$f(d)$	$(17-f(d))b$	$t(d)$	$\rho(xy^{-1}x)^2$	$\rho(y^2x^{-t(d)})^3$
3	1	$e^{\pi i/6}$	12	9	108	1	144	2	$-I$	$-I$
3	1	$e^{3\pi i/6}$	12	9	108	1	144	2	$-I$	$-I$
3	1	$e^{5\pi i/6}$	12	9	108	1	144	2	$-I$	$-I$
3	1	$e^{7\pi i/6}$	12	9	108	1	144	2	$-I$	$-I$
3	1	$e^{9\pi i/6}$	12	9	108	1	144	2	$-I$	$-I$
3	1	$e^{11\pi i/6}$	12	9	108	1	144	2	$-I$	$-I$
5	1	$e^{9\pi i/30}$	20	5	60	1	80	3	$-I$	$-I$
5	1	$e^{39\pi i/30}$	20	5	60	1	80	3	$-I$	$-I$
5	1	$e^{19\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	1	$e^{29\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	1	$e^{49\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	1	$e^{59\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	2	$e^{3\pi i/30}$	20	5	60	1	80	3	$-I$	$-I$
5	2	$e^{33\pi i/30}$	20	5	60	1	80	3	$-I$	$-I$
5	2	$e^{13\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	2	$e^{23\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	2	$e^{43\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$
5	2	$e^{53\pi i/30}$	60	45	540	1	720	8	$-I$	$-I$

Thus we see each corresponding representation must have a kernel which is a congruence subgroup of level d.

■

We can now piece together the three previous results to prove the following result.

Theorem 4.1.18 *Suppose $\rho : \Gamma \to \mathrm{GL}(2, \mathbb{C})$ is an irreducible representation with finite image and let d be the order of $\rho(T)$. Then $\ker\rho$ is a congruence subgroup of level d.*

Proof: If d is a composite integer that is not a power of 2, then by the above proposition we see that $\ker\rho$ must be a congruence subgroup of level d. The only other cases are when ρ is equivlanent to $\rho_{2,1,1}$ or one of $\rho_{4,1,\pm e^{3\pi i/12}}$ but these representations also have kernels that are congruence subgroup by 4.1.15 and 4.1.16. ■

As a corollary, we obtain our main result for two-dimensional representations of B_3. First we make a definition.

Definition 4.1.19 *Let $\rho : G \to \mathrm{GL}(d, \mathbb{C})$ be a representation of a group G. Another representation ρ' is called a* **scaling** *of ρ there is some scalar $\theta \in \mathbb{C}^*$ so that for all $g \in G$ we have $\rho'(g) = \theta\rho(g)$. In this case we write $\rho' = \theta\rho$ and we say a representation is* **essentially finite** *if it has a scaling with finite image. Clearly if ρ is irreducible then so is $\theta\rho$ for any θ.*

We have:

Corollary 4.1.20 *Suppose $\rho : B_3 \to \mathrm{GL}(2, \mathbb{C})$ is an irreducible representation with finite image. Then there is a scaling ρ' of ρ factoring through π so that $\pi(\ker \rho')$ is a congruence subgroup of Γ. In this case, $\pi(\ker \rho')$ is of level equal to the order of $\rho'(\sigma_1)$.*

We can also apply our results to fusion systems and quantum representations.

Corollary 4.1.21 *Let $(L, \otimes, F, R)$ be a braided $6j$ fusion system such that the R-symbols are distinct roots of unity. Suppose for some labels i and k in L the map $\rho_{i,3,k}$ is a two-dimensional irreducible representation of B_3. Then there is a scaling ρ of the representation $\rho_{i,3,k}$ of B_3 so that $\pi(\ker \rho)$ is a congruence subgroup equal to the order of $\rho(\sigma_1)$.*

> **Example 4.1.22** *Let us revisit the two-dimensional representations from the Ising fusion system. We have $\mathrm{spec}(\rho_{\sigma,3,\sigma}(\sigma_1)) = \{\, e^{-\pi i/8}, e^{3\pi i/8} \,\}$ and since $-(e^{-\pi i/8} e^{3\pi i/8})^3 = e^{7\pi i/4}$, we see that $\rho_{3,\sigma,3}$ does not factor through π. If θ is a 6^{th} root of $e^{-7\pi i/4}$ then $\theta\rho_{3,\sigma,3}$ does factor through π. For example, take $\theta = e^{\pi i/24}$. Then $\mathrm{spec}(\theta\rho_{3,\sigma,3}) = \{\, e^{23\pi i/12}, ie^{23\pi i/12} \,\}$ so that $\theta\rho_{3,\sigma,3}$ is equivalent to $\rho_{4,1,e^{23\pi i/12}}$. Therefore the kernel of $\theta\rho_{3,\sigma,3}$ is a congruence subgroup of level 24.*

4.2 Three-dimensional representations

The structure of this section mirrors the previous one. We first reduce the problem to studying representations of Γ which we can then lift back to B_3. We start with the three-dimensional version of the TW classification.

Proposition 4.2.1 *Let λ_1, λ_2, and λ_3 be nonzero complex numbers. Then $\rho_{\lambda_1,\lambda_2,\lambda_3} : B_3 \to \mathrm{GL}(3,\mathbb{C})$ given by*

$$\rho_{\lambda_1,\lambda_2,\lambda_3}(\sigma_1) = \begin{pmatrix} \lambda_1 & \lambda_1\lambda_3\lambda_2^{-1} + \lambda_2 & \lambda_2 \\ 0 & \lambda_2 & \lambda_2 \\ 0 & 0 & \lambda_3 \end{pmatrix}, \quad \rho_{\lambda_1,\lambda_2,\lambda_3}(\sigma_2) = \begin{pmatrix} \lambda_3 & 0 & 0 \\ -\lambda_2 & \lambda_2 & 0 \\ \lambda_2 & -\lambda_1\lambda_3\lambda_2^{-1} - \lambda_2 & \lambda_1 \end{pmatrix}$$

defines a representation of B_3.

Proof: This is again a straightforward calculation. Let

$$A = \begin{pmatrix} \lambda_1 & \lambda_1\lambda_3\lambda_2^{-1} + \lambda_2 & \lambda_2 \\ 0 & \lambda_2 & \lambda_2 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

and

$$B = \begin{pmatrix} \lambda_3 & 0 & 0 \\ -\lambda_2 & \lambda_2 & 0 \\ \lambda_2 & -\lambda_1\lambda_3\lambda_2^{-1} - \lambda_2 & \lambda_1 \end{pmatrix}.$$

Then we can compute

$$ABA = (\lambda_1\lambda_2\lambda_3) \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = BAB$$

so indeed $\rho_{\lambda_1,\lambda_2,\lambda_3}$ is a representation. ■

Again we find that the set of eigenvalues of a three-dimensional irreducible representation determines its equivalence class. Also, almost all choices of three non-zero complex numbers produce an irreducible representation and there is a condition on the eigenvalues to ensure the image of the representation is finite.

Theorem 4.2.2 ([TW01])

(i) Let N_3 be the zero set of $\{\, \lambda_j^2 + \lambda_k\lambda_\ell \mid \{\, j,k,l \,\} = \{\, 1,2,3 \,\} \,\}$. Then there is a bijection between conjugacy classes of irreducible 3-dimensional representations of B_3 and S_3-orbits of $\mathbb{C}^3 \setminus N_3$.

(ii) Suppose $\rho : B_3 \to \mathrm{GL}(3,\mathbb{C})$ is irreducible and $\mathrm{spec}(\rho(\sigma_1)) = \{\, \lambda_1, \lambda_2, \lambda_3 \,\}$. Then ρ is equivalent to $\rho_{\lambda_1,\lambda_2,\lambda_3}$. Furthermore, ρ factors through π if and only if $(\lambda_1\lambda_2\lambda_3)^2 = 1$.

The next step is to determine which eigenvalues correspond to representations with finite image. Along with their result in dimension two, Rowell and Tuba also provided a necessarily and sufficient conditions for a three-dimensional irreducible representation to have finite image. Their result eliminates more degree of freedom and so we are able to finally parametrize the space of representations that we are interested in. We will only consider the situations described in (i) and (iii) below. Case (i) is analogous to the scenario for two-dimensional irreducibles but the extra dimension allows for some more freedom, demonstrated in cases (ii) and (iii).

Theorem 4.2.3 ([RT10]) *Suppose $\rho : B_3 \to \mathrm{GL}(3,\mathbb{C})$ is an irreducible representation. Write $\mathrm{spec}(\rho(\sigma_1)) = \{\, \lambda_1, \lambda_2, \lambda_3 \,\}$. Then $\rho(B_3)$ if finite if and only if one of the following occurs:*

(i) λ_1, λ_2, and λ_3 are distinct roots of unity and $3 \le \mathrm{po}(\rho(\sigma_1)) \le 5$.

(ii) $\mathrm{po}(\rho(\sigma_1)) = 7$ *and* $\frac{1}{\lambda_1}\,\mathrm{spec}(\rho(\sigma_1))$ *is Galois conjugate to* $\{\, 1, e^{2\pi i/7}, e^{2\pi ik/7} \,\}$ *for* $k = 3$ *or* $k = 5$*.*

(iii) $\mathrm{po}(\rho(\sigma_1)) > 5$ *and* $\mathrm{spec}(\rho(\sigma_1)) = \{\, \lambda, -\lambda, \mu \,\}$ *for some distinct roots of unity* λ *and* μ*.*

As a corollary we have:

Corollary 4.2.4 *Suppose* $\rho : B_3 \to \mathrm{GL}(3, \mathbb{C})$ *is an irreducible representations with finite image and* $3 \leq \mathrm{po}(\rho(\sigma_1)) \leq 5$*. Then* ρ *is equivalent to* $\rho_{\lambda, e^{2\pi ij/r}\lambda e^{2\pi ik/r}\lambda}$ *where* $r = \mathrm{po}(\rho(\sigma_1))$*,* $j, k \in \mathbb{Z}_r^\times$ *are distinct, and* λ *satisfies*

$$\lambda^6 = e^{-4\pi i(j+k)/r}. \tag{4.2}$$

This gives us an explicit equation to work from to classify three-dimensional irreducible representations with finite image that factor through π.

> **Example 4.2.5** *The three-dimensional representation* $\rho_{G,3,G}$ *associated to the* $D(S_3)$ *fusion system has* $\mathrm{spec}(\rho_{G,3,G}(\sigma_1)) = \{\, \pm e^{4\pi i/3}, e^{2\pi i/3} \,\}$ *so the above theorems tells us that it has finite image and is irreducible.*

4.2.1 More projective order lemmas

According to 4.2.3, we should consider those representations mapping σ_1 to an element of projective order between 3 and 5. Working in the other direction, if we let r be an integer between 3 and 5, let j and k be distinct elements of $\mathbb{Z}_r^\times$, and λ a solution to

$$\lambda^6 = e^{-4\pi i(j+k)/r}$$

then there is an irreducible representation $\rho_{\lambda, e^{2\pi i j/r}\lambda e^{2\pi i k/r}\lambda}$ and $\rho_{\lambda, e^{2\pi i j/r}\lambda e^{2\pi i k/r}\lambda} = \rho_{r,j,k,\lambda} \circ \pi$ where $\rho_{r,j,k,\lambda} : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ is irreducible and has finite image. Thus, we will classify the representations $\rho_{r,j,k,\lambda}$ which then gives us a classification for the corresponding irreducible representations of B_3. We begin with the case of projective order equal to 3.

Lemma 4.2.6 *If* $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ *is an irreducible representation with finite image and* $\mathrm{po}(\rho(T)) = 3$ *then* ρ *is equivalent to* $\rho_{3,1,2,\lambda}$ *where* $\lambda \in \{ 1, e^{2\pi i/6} \}$.

Proof: Let $A = \rho(T)$. Since $\mathrm{po}(A) = 3$ and the eigenvalues of A are distinct, then $\mathrm{spec}(A)$ is necessarily of the form $\{ \lambda, e^{2\pi i/3}\lambda, e^{4\pi i/3}\lambda \}$ where $\lambda^6 = 1$. However, to account for only distinct cases, we can take $\lambda = 1$ or $\lambda = e^{2\pi i/6}$. ■

Here we continue with the case of projective order 4 or 5.

Lemma 4.2.7 *If* $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ *is an irreducible representation with finite image and* $\mathrm{po}(\rho(T)) = 4$ *then* ρ *is equivalent to* $\rho_{4,1,3,\lambda}$ *where* $\lambda \in \{ e^{2\pi i k/6} \mid 0 \le k \le 5 \}$.

Proof: Let $A = \rho(T)$ and let $\mathrm{spec}(A) = \{ \lambda_1, \lambda_2, \lambda_3 \}$. Since $\mathrm{po}(A) = 4$ and each of the λ_i are distinct, we can say without loss of generality that λ_2 must be either $i\lambda_1$ or $-i\lambda_1$. If it is $-i\lambda_1$ then write $\mu = -i\lambda_1$ so that $\lambda_1 = i\mu$. Then, renaming elements, we can say that $\mathrm{spec}(A)$ is of the form $\{ \mu, i\mu, \mu_3 \}$ and μ_3 can be either $-\mu$ or $-i\mu$. If it is $-\mu$, then set $\eta = i\mu$ so that $-\mu = i\eta$ and $\mu = -i\eta$. Thus $\mathrm{spec}(A) = \{ \eta, i\eta, -i\eta \}$ where μ satisfies $\eta^6 = 1$ and therefore, ρ is equivalent to one of the $\rho_{4,1,3,\lambda}$ for some $\lambda \in \{ e^{2\pi i k/6} \mid 0 \le k \le 5 \}$. ■

Lemma 4.2.8 *If* $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ *is an irreducible representation with finite image and* $\mathrm{po}(\rho(T)) = 5$ *then* ρ *is equivalent to* ρ *is equivalent to* $\rho_{5,1,2,\lambda}$ *where* $\lambda \in \{ e^{(4+5k)\pi i/15} \mid 0 \le k \le 5 \}$ *or* $\rho_{5,1,3,\lambda}$ *where* $\lambda \in \{ e^{(2+5k)\pi i/15} \mid 0 \le k \le 5 \}$.

Proof: We can use the same technique as in the proof above so that $\operatorname{spec}(A)$ is of the form $\{\, \lambda, e^{2\pi i/5}\lambda, e^{4\pi i/5}\lambda \,\}$ or $\{\, \lambda, e^{2\pi i/5}\lambda, e^{6\pi i/5}\lambda \,\}$. Applying Corollary 4.2.4, we see that ρ is equivalent to $\rho_{5,1,2,\lambda}$ where $\lambda \in \{\, e^{(4+5k)\pi i/15} \mid 0 \leq k \leq 5 \,\}$ or $\rho_{5,1,3,\lambda}$ where $\lambda \in \{\, e^{(2+5k)\pi i/15} \mid 0 \leq k \leq 5 \,\}$. ■

4.2.2 Congruence kernels for three-dimensional representations of small projective order

According to 3.3.11, whenever ρ is an irreducible representation of Γ with finite image such that the order of $\rho(T)$ is an odd integer d, in order to show that $\ker \rho$ is a congruence subgroup of level d, it is enough to show that $(U^2T^{-t(d)})^3$ is in the kernel of ρ, where $t(d)$ is the multiplicative inverse of 2 modulo d. We shall use this line of reasoning for the three following propositions, which consider the cases of $d = 3, 5$, or 15.

Proposition 4.2.9 *If $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ is equivalent to $\rho_{3,1,2,1}$ then the order of $\rho(T)$ is 3 and $\ker \rho$ is a congruence subgroup of level 3.*

Proof: We need to show that $(U^2T^{-2})^3$ is in the kernel of ρ. Equivalently, we need to show that $(B^{-2}A^{-2})^3$ is the identity, where $A = \rho(T)$ and $B = \rho(U^{-1})$. Since the orders of A and B are both 3, we can rewrite $(B^{-2}A^{-2})^3$ as $(BA)^3$ which is necessarily the identity since ρ is a representation. ■

Proposition 4.2.10 *If $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ is equivalent to $\rho_{5,1,2,e^{8\pi i/5}}$ or $\rho_{5,1,3,e^{4\pi i/5}}$ then the order of $\rho(T)$ is 5 and $\ker \rho$ is a congruence subgroup of level 5.*

Proof: Similar to the above proof, we need only show that $\rho(U^2T^{-3})^3 = (B^3A^2)^3$ is the identity. This can be done explicitly, for example, with Mathematica. ■

Proposition 4.2.11 *If $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ is equivalent to $\rho_{5,1,2,e^{4\pi i/15}}$, $\rho_{5,1,2,e^{14\pi i/15}}$, $\rho_{5,1,3,e^{2\pi i/15}}$, or $\rho_{5,1,3,e^{22\pi i/15}}$ then the order of $\rho(T)$ is 15 and $\ker \rho$ is congruence subgroup of level 15.*

Proof: In each case we are to show that $(U^2T^{-8})^3$ maps to the identity. Let $A = \rho(T)$ and $B = \rho(U^{-1})$. Then $\rho(U^2T^{-8})^3 = (B^{-2}A^{-8})^3 = (B^3A^2)^3$ since A^5 and B^5 are scalar matrices and of order 3. Then, again using Mathematica, we can compute directly that in each case $(B^3A^2)^3$ is the identity. ■

We can apply Proposition 3.4.3 to consider the case where d is an even composite integer that is not a power of 2, which then exhausts the rest of possible representations with projective order between 3 and 5.

Proposition 4.2.12 *Suppose $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ is irreducible with finite image and $3 \leq \mathrm{po}(\rho(\sigma_1)) \leq 5$ and let the order of $\rho(T)$ be an even composite integer d that is not a power of 2. Then $\ker \rho$ is a congruence subgroup of level d.*

Proof: We know that ρ is equivalent to one of the representations in the conclusion of 4.2.6, 4.2.7, and 4.2.8. Of those that map T to a matrix of even composite order which is not a power 2, we have recorded the data in the hypothesis and conclusion of 3.4.3. In particular, in each case we see that the kernel of the representation associated to each row is a congruence subgroup of Γ. First, following our corollary to Hsu's theorem (3.3.10), we list the data for the representations such that d divides 24, a is a multiple of r, $12a$ is a multiple of d, $3at(d)$ is a multiple of d and $\rho(p_d)$ is a central element of order at most 2, Then, we can compute $\rho((zw^{?1}z)^2)$ and $\rho(p_d(w^5zw^{?1}z)^3)$ and compare the results, as in the conclusion of 3.4.3.

r	j	k	λ	d	a	$12a$	$t(d)$	$3at(d)$	$\rho(p_d)$	$\rho(zw^{-1}z)^2$	$\rho(p_dw^5zw^{-1}z)^3$
4	1	3	$e^{2\pi i/6}$	12	4	48	2	24	I	I	I
4	1	3	$e^{4\pi i/6}$	12	4	48	2	24	I	I	I
4	1	3	$e^{8\pi i/6}$	12	4	48	2	24	I	I	I
4	1	3	$e^{10\pi i/6}$	12	4	48	2	24	I	I	I

Next we list collect the data for the representations such that b is a multiple of r, $12b$ is a multiple of d, and $(17 - f(d))b$ is a multiple of d. We then compare $\rho((xy^{-1}x)^2)$ and $\rho((y^2x^{-t(d)})^3)$.

r	j	k	λ	d	b	$12b$	$f(d)$	$(17 - f(d))b$	$t(d)$	$\rho(xy^{-1}x)^2$	$\rho(y^2x^{-t(d)})^3$
3	1	2	$e^{2\pi i/6}$	6	3	36	1	48	2	I	I
5	1	2	$e^{9\pi i/15}$	10	5	60	1	80	3	I	I
5	1	2	$e^{19\pi i/15}$	30	15	180	1	80	8	I	I
5	1	2	$e^{29\pi i/15}$	30	15	180	1	80	8	I	I
5	1	3	$e^{7\pi i/15}$	30	15	180	1	80	8	I	I
5	1	3	$e^{17\pi i/15}$	30	15	180	1	80	8	I	I
5	1	3	$e^{27\pi i/15}$	10	5	60	1	80	3	I	I

Thus we see each corresponding representation must have a kernel which is a congruence subgroup of level d.

■

We can summarize the results of this section so far with the following result.

Theorem 4.2.13 *Suppose $\rho : \Gamma \to \mathrm{GL}(3, \mathbb{C})$ is an irreducible representation with finite image such that $3 \leq \mathrm{po}(\rho(T)) \leq 5$ and let d be the order of $\rho(T)$. Then $\ker \rho$ is a congruence subgroup of level d.*

Proof: If d is a composite integer that is not a power of 2, then by the above proposition we see that $\ker \rho$ must be a congruence subgroup of level d. The other possibility is that ρ is equivalent to one of $\rho_{3,1,2,1}$, $\rho_{5,1,2,e^{8\pi i/5}}$, $\rho_{5,1,2,e^{4\pi i/15}}$, $\rho_{5,1,2,e^{14\pi i/15}}$, $\rho_{5,1,3,e^{4\pi i/5}}$, $\rho_{5,1,3,e^{2\pi i/15}}$, or $\rho_{5,1,3,e^{22\pi/5}}$, all of which have kernels that are congruence subgroups of level equal to the order of the image of T by 4.2.9, 4.2.10, 4.2.11. ■

As a corollary, we obtain our main result concerning three-dimensional representations giving rise to congruence subgroups.

Corollary 4.2.14 *Suppose $\rho : B_3 \to \mathrm{GL}(3, \mathbb{C})$ is an irreducible representation with finite image such that $3 \leq \mathrm{po}(\rho(\sigma_1)) \leq 5$. Then there is a scaling ρ' of ρ factoring through π*

so that $\pi(\ker \rho')$ is a congruence subgroup of Γ. In this case, $\pi(\ker \rho')$ is of level equal to the order of $\rho'(\sigma_1)$.

Again, we can apply this result to fusion systems and quantum representations.

Corollary 4.2.15 *Let $(L, \otimes, F, R)$ be a braided $6j$ fusion system such that the R-symbols are distinct roots of unity. Suppose for some labels i and k in L the vector space $V_{i,3,k}$ is a three-dimensional irreducible representation of B_3 such that σ_1 acts by an element of projective order between 3 and 5. Then there is a scaling ρ of the representation $\rho_{i,3,k}$ of B_3 so that $\pi(\ker \rho)$ is a congruence subgroup equal to the order of $\rho(\sigma_1)$.*

4.3 Non-congruence subgroups from finite braid group representations

This section is devoted to providing a construction for an infinite family of non-congruence subgroups of Γ associated to three-dimensional irreducible representations of B_3. Our strategy for this construction is again a consequence of the TW classification, the finiteness result of Rowell and Tuba, and Hsu's generator theorem. More specifically, we will provide an explicit family of irreducible three-dimensional representations ρ_α, each of which factor through π and whose images are all finite. However, we can show if d_α is the order of $\rho_\alpha(\sigma_1)$ then the generating set G_{d_α} is not contained in the kernel. In fact, we will show that one of the elements of G_{d_α} has an eigenvalue that is not equal to 1. Our first easy lemma is more of an observation about a certain collection of three-dimensional irreducible representations of B_3.

Lemma 4.3.1 *Let $\alpha = e^{2\pi i j/r}$ where r is an odd integer greater than 4 and $j \in \mathbb{Z}_r^\times$. Then the representations $\rho_{\alpha,-\alpha,\alpha^{-2}}$ and $\rho_{\alpha,-\alpha,-\alpha^{-2}}$ of B_3 factor through π and have finite image.*

Proof: Applying the Tuba-Wenzl classification, we see that since $\alpha(-\alpha)(\pm\alpha^{-2}) = \mp 1$, the representations both factor through π. Then we can apply the results from Tuba and Rowell to see that since $\mathrm{spec}(\rho_{\alpha,-\alpha,\pm\alpha^{-2}}(\sigma_1))$ is of the form $\{\, \lambda, -\lambda, \mu \,\}$ for distinct roots of unity λ and μ, the image of both representations must be finite. We can be sure that the spectrums consist of distinct elements since r is odd and at least 5. ■

Now that we know $\rho_{\alpha,-\alpha,\alpha^{-2}}$ and $\rho_{\alpha,-\alpha,-\alpha^{-2}}$ for $\alpha = e^{2\pi ij/r}$ have finite image, we will consider the image of $[\sigma_1^{r+1}, \sigma_2^{-r}]$ under these representations. Recall that $\pi(\sigma_1) = T$ and $\pi(\sigma_2) = U^{-1}$ so that $\pi([\sigma_1^{r+1}, \sigma_2^{-r}] = [T^{r+1}, U^r]$. It will turn out that this is an element of G_{2r} with which we should be concerned.

Lemma 4.3.2 *Let $\alpha = e^{2\pi ij/r}$ where r is an odd integer greater than 4 and $j \in \mathbb{Z}_r^\times$. Let ρ be one of $\rho_{\alpha,-\alpha,\alpha^{-2}}$ or $\rho_{\alpha,-\alpha,-\alpha^{-2}}$. Then $e^{-6\pi ij/r} \in \mathrm{spec}(\rho([\sigma_1^{r+1}, \sigma_2^{-r}]))$.*

Proof:

First of all, since r is odd we can write

$$\begin{aligned}\rho([\sigma_1^{r+1}, \sigma_2^{-r}]) &= \rho(\sigma_1)^{r+1}\rho(\sigma_2)^{-r}\rho(\sigma_1)^{-(r+1)}\rho(\sigma_2)^{r} \\ &= \rho(\sigma_1)^{r+1}\rho(\sigma_2)^{-(r-1)}[\rho(\sigma_2)^{-1}\rho(\sigma_1)^2\rho(\sigma_2)]^{-(r+1)/2}\rho(\sigma_2)^{r-1}\end{aligned}$$

and we claim that each of $\rho(\sigma_1)^{r+1}$, , $\rho(\sigma_2)^{r-1}$, and $\rho(\sigma_2)^{-1}\rho(\sigma_1)^2\rho(\sigma_2)$ each have $(0, 0, 1)$ as a left eigenvector. If this is the case, then call the corresponding eigenvalues $\lambda_1, \lambda_2, \lambda_3$. The product $\rho([\sigma_1^{r+1}, \sigma_2^{-r}])$ then has $\lambda_1\lambda_2\lambda_3\lambda_2^{-1} = \lambda_1\lambda_3$ as an eigenvalue.

Now, by construction, the matrix $\rho(\sigma_1)^{r+1}$ is upper triangular with bottom right entry equal to $(\pm\alpha^{-2})^{r+1} = \alpha^{-(2r+2)} = \alpha^{-2}$ since r is odd and $\alpha^r = 1$.

A straightforward calculation shows

$$\rho(\sigma_2)^2 = \begin{pmatrix} \alpha^{-4} & 0 & 0 \\ -\alpha^2 \pm \alpha^{-1} & \alpha^2 & 0 \\ 0 & 0 & \alpha^2 \end{pmatrix}$$

which we note is block diagonal, consisting of one 2×2 block and one 1×1 block. Since $r-1$ is even, we see $\rho(\sigma_2)^{r-1}$ also shares this block form. In particular, $(0,0,1)$ is also a left eigenvector of $\rho(\sigma_2)^{r-1}$. Another calculation yields

$$\rho(\sigma_2)^{-1}\rho(\sigma_1)^2\rho(\sigma_2) = \begin{pmatrix} \alpha^2 & 0 & 0 \\ \alpha^2 \mp \alpha^{-1} & \alpha^{-4} & -\alpha^2 \pm \alpha^{-1} \\ 0 & 0 & \alpha^2 \end{pmatrix}$$

so again $(0,0,1)$ is a left eigenvector of $\rho(\sigma_2)^{-1}\rho(\sigma_1)^2\rho(\sigma_2)$ with corresponding eigenvalue α^2. Accordingly, we can be sure that $\rho([\sigma_1^{r+1}, \sigma_2^{-r}])$ has $(0,0,1)$ as a left eigenvector with corresponding eigenvalue $\alpha^{-2}(\alpha^2)^{-(r+1)/2} = \alpha^{-3}$. ■

Lemma 4.3.3 *Let r be an odd integer. Then the commutator $[T^{r+1}, U^r]$ is an element of $\Gamma(2r)$.*

Proof: This follows from either Hsu's theorem or directly computing elements. Note that since r is odd, $r+1$ is the unique integer taken modulo $2r$ which is congruent to 0 modulo 2 and 1 modulo r. Therefore, Hsu tells us that $[T^{r+1}, U^r]$ is an element of G_{2r}. Of course $G_{2r} \subseteq \Gamma(2r)$. ■

We can now collect the three lemmas above into our main theorems for this section, which tells us about an association between irreducible representations of B_3 and non-congruence subgroups.

Theorem 4.3.4 *Let $\alpha = e^{2\pi ij/r}$ where r is an odd integer greater than 4 and $j \in \mathbb{Z}_r^\times$. If ρ*

is equivalent to one of $\rho_{\alpha,-\alpha,\alpha^{-2}}$ *or* $\rho_{\alpha,-\alpha,-\alpha^{-2}}$ *then* $\pi(\ker\rho)$ *is a non-congruence subgroup of* Γ *with geometric level* $2r$*.*

Proof: We know that ρ has finite image and factors through π. Denote by $\bar{\rho}$ the induced representation of Γ. Since r is odd we can compute the order of $\bar{\rho}(T)$ to be $2r$. Then by 3.3.11, we know that $\ker\bar{\rho}$ is a congruence subgroup if and only if it contains $\Gamma(2r)$. The above lemma tells us that $M_r \in \Gamma(2r)$ but we can compute $\bar{\rho}(M_r) = \rho([\sigma_1^{r+1}, \sigma_2^{-r}])$ which, by Lemma 4.3.2, has $e^{-6\pi ij/r}$ as an eigenvalue. In particular, $\bar{\rho}(M_r)$ cannot be the identity matrix and so $\Gamma(2r)$ is not contained in the kernel of $\bar{\rho}$. Thus we see that $\pi(\ker\rho) = \ker\bar{\rho}$ is a non-congruence subgroup of Γ with geometric level equal to $2r$.

$\blacksquare$

Now we can lift this theorem to B_3.

Theorem 4.3.5 *Let* $\rho : B_3 \to \mathrm{GL}(3,\mathbb{C})$ *be an irreducible representation such that* $\mathrm{spec}(\rho(B_3))$ *is of the form* $\{\, \lambda e^{2\pi ij/r}, -\lambda e^{2\pi ij/r}, \lambda e^{-4\pi ij/r} \,\}$ *or* $\{\, \lambda e^{2\pi ij/r}, -\lambda e^{2\pi ij/r}, -\lambda e^{-4\pi ij/r} \,\}$ *for non-zero complex number* λ*, some odd integer* r *greater than 4 and* $j \in \mathbb{Z}_r^\times$*. Then there is a scaling* $\widetilde{\rho}$ *of* ρ *such that* $\widetilde{\rho}$ *factors through* π *and* $\pi(\ker\widetilde{\rho})$ *is a non-congruence subgroup of* Γ*.*

Proof: Let $\alpha = e^{2\pi ij/r}$. Then the representation $\lambda^{-1}\rho$ is equivalent to $\rho_{\alpha,-\alpha,\alpha^{-2}}$ or $\rho_{\alpha,-\alpha,-\alpha^{-2}}$, which, by the above theorem, has finite image, factors thorugh π, and has a kernel that projects onto a non-congruence subgroup of Γ.

$\blacksquare$

Example 4.3.6 *Let us again return to the representation* $\rho_{G,3,G}$ *determined by the* $D(S_3)$ *data. Recall that* $\mathrm{spec}(\rho_{G,3,G}(\sigma_1)) = \{\, e^{4\pi i/3}, -e^{4\pi i/3}, e^{2\pi i/3} \,\}$*. Rear-*

ranging, we can write

$$\{\, e^{4\pi i/3}, -e^{4\pi i/3}, e^{2\pi i/3} \,\} = e^{-2\pi i/9} \{\, e^{14\pi i/9}, -e^{14\pi i/9}, e^{8\pi i/9} \,\}$$

so that $e^{2\pi i/9}\rho_{G,3,G}$ *is equivalent to* $\rho_{e^{14\pi/9}, -e^{14\pi i/9}, e^{8\pi i/9}}$. *This spectrum is of the form*

$$\{\, \lambda e^{2\pi i j/r}, -\lambda e^{2\pi i j/r}, \lambda e^{-4\pi i j/r} \,\}$$

with $\lambda = e^{-2\pi i/9}, r = 9, j = 7$ *so the kernel of* $e^{2\pi i/9}\rho_{G,3,G}$ *projects onto a non-congruence subgroup of* Γ *of geometric level 18.*

Chapter 5

Congruence anyons

5.1 Property F and the Property F conjecture

Let $\mathcal{C}$ be a strict premodular (or even just braided fusion) category with braiding c and let $\operatorname{Irr}(\mathcal{C}) = \{ X_0 = I, X_1, \ldots, X_n \}$ be a complete set of representatives of simple of objects of $\mathcal{C}$.

Definition 5.1.1 *For each i and j we can write $X_i \otimes X_j \cong \oplus X_k^{\oplus N_{ij}^k}$. Then denote by N_i the matrix with kj entry equal to N_{ij}^k. This is called the* ***fusion matrix*** *of X_i. Each matrix N_i is nonnegative; that is, all of their entries are nonnegative.*

The next theorem is very important in the theory of fusion categories. A proof can be found in [Gan60].

Theorem 5.1.2 (Frobenius-Perron) *Let A be a square matrix with nonnegative entries. Then A has a nonnegative real eigenvalue $\lambda(A)$ such that $|\lambda(A)| \geq \lambda$ for all $\lambda \in \operatorname{spec}(A)$. If A is not nilpotent then $\lambda(A) > 0$.*

This allows us to associate to each simple object in $\mathcal{C}$ a positive number. This gives us a notion of dimension for each object.

Definition 5.1.3 *Let* $\mathrm{Irr}(\mathcal{C}) = \{ X_0 = I, X_1, \ldots, X_n \}$ *be a complete set of representatives of isomorphism classes of simple of objects of a fusion category* $\mathcal{C}$ *with respective fusion matrices* N_i*. For* $X_i \in \mathrm{Irr}(\mathcal{C})$*, let* $\mathrm{FPdim}(X_i) = \lambda(N_i)$*. This is called the* ***Frobenius-Perron dimension*** *of* X_i*. Further define*

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

We say X_i *is* ***integral*** *if* $\mathrm{FPdim}(X_i) \in \mathbb{Z}$ *and we say* X_i *is* ***weakly integral*** *if* $\mathrm{FPdim}(X_i)^2 \in \mathbb{Z}$*. We say* $\mathcal{C}$ *is* ***(weakly) integral*** *if each* X_i *is.*

Proposition 5.1.4 ([EGNO16]) *Let* $\mathcal{C}$ *be a fusion category and let* $\mathrm{Irr}(\mathcal{C})$ *be a complete set of representative of isomorphism class of simple objects of* $\mathcal{C}$*. If* $X \in \mathrm{Irr}(\mathcal{C})$ *then* $\mathrm{FPdim}(X) \geq 1$*.*

In particular, we see that $\mathrm{FPdim}(X)$ is nonzero whenever X is a simple object of a fusion category $\mathcal{C}$. When $\mathcal{C}$ is braided, a fascinating connection between the braid group representations afforded by $\mathcal{C}$ and Frobenius-Perron dimensions has been observed. First, we need another definition.

Definition 5.1.5 *We say an object* X *has* ***Property F*** *if the image of* $\rho_{X,n}$ *is finite for all* n*. If* i *is the label in a braided* $6j$ *fusion system corresponding to the simple object* X *then we say that* i *also has Property* F*.*

Although is has not been proven in general, the following conjecture is true is all known examples. This is perhaps one of the biggest open questions in the theory of fusion categories.

Conjecture 5.1.6 ([NR11]) *Let* X *be an object of a braided fusion category* $\mathcal{C}$*. Then* X *is weakly integral in and only if for each* n *the image of* $\rho_{X,n}$ *is finite.*

In particular, evidence suggests that anyons corresponding to weakly integral simple objects would never be able to provide a universal gate set and hence their braiding alone cannot be used to achieve universal quantum computation. However, it is possible to alter the gate set of a Property F anyon to achieve a universal gate set ([CHW15]).

5.2 Congruence anyons

Here we will define a special class of labels in a braided $6j$ fusion system.

Definition 5.2.1 *Let i be a label with Property F. We say i is* ***congruence type*** *if for all labels k such that $V_{i,n,k}$ is nonzero, the representation $\rho_{i,3,k}$ has the property that any irreducible summand is either one-dimensional or can be scaled to be equivalent to a representation whose kernel projects onto a congruence subgroup of Γ. Otherwise, we say i is of* ***non-congruence type****. If a label is of congruence type then we will call it a* ***congruence anyon****.*

We are able to use our results from the earlier chapters to provide a sufficient condition for a label to be congruence anyon.

Theorem 5.2.2 *Let $(L, \times, F, R)$ be a braided $6j$ fusion system and let $i \in L$ be a Property F label. Suppose for all labels k and all irreducible summands ρ of $\rho_{i,3,k}$ are either:*

(a) one-dimensional,

(b) two-dimensional,

(c) or three-dimensional and $3 \leq \mathrm{po}(\rho(\sigma_1)) \leq 5$.

Then i is congruence type.

Proof: If every irreducible summand of $\rho_{i,3,k}$ satisfies one of the three conditions above, then it follows from the definition of congruence type label and Theorems 4.1.20 and 4.2.14 that i is a congruence type label. ■

Example 5.2.3 *Let $L = \{ 1, \sigma, \psi \}$ be the Ising fusion system. Then*

$$V_{\sigma,3,x} \cong \begin{cases} \mathbb{C}^2 & \textit{if } x = \sigma. \\ 0 & \textit{otherwise.} \end{cases}$$

We know that some scaling of $\rho_{\sigma,3,\sigma}$ is irreducible and its kernel projects onto a congruence subgroup of Γ. Therefore, σ is a congruence anyon.

We can also identify one case where we can be sure that a label is of non-congruence type.

Theorem 5.2.4 *Let $(L, \otimes F, R)$ be a braided $6j$ fusion system and let $i \in L$ be a Property F label. Suppose for some $k \in L$, there is an irreducible summand ρ of $\rho_{i,3,k}$ so that* $\operatorname{spec}(\rho(\sigma_1))$ *is of the form*

$$\lambda \{ e^{2\pi ij/r}, -e^{2\pi ij/r}, e^{-4\pi ij/r} \}$$

or

$$\lambda \{ e^{2\pi ij/r}, -e^{2\pi ij/r}, -e^{-4\pi ij/r} \} .$$

Then i is of non-congruence type.

Proof: If $\operatorname{spec}(\rho(\sigma_1))$ is of one of the above forms, then by Theorem 4.3.5, we see that some scaling of $\ker \rho$ projects onto a non-congruence subgroup of Γ. In particular, i is of non-congruence type. ■

Example 5.2.5 *Consider the label G from the $D(S_3)$ fusion system. We computed* $\operatorname{spec}(\rho_{G,3,G}(\sigma_1)) = e^{-2\pi i/9}\left\{ e^{14\pi i/9}, -e^{14\pi i/9}, e^{8\pi i/9} \right\}$ *and $\rho_{G,3,G}$ is irreducible so we see that G a non-congruence anyon.*

Chapter 6

Further directions and applications

In this last chapter we will discuss some variations on the problem we discussed and somepossible applications in other fields.

6.1 Congruence subgroups of mapping class groups

In chapter 4, we saw that the direct analogue of the Ng-Schauenberg Theorem for B_3 is not true. One remedy for this could be to adjust our notion for congruence subgroups of B_3. This definition relied on being able to pull back congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$ to B_3 and the definition of congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$ rely on its description as a matrix group, rather than as the mapping class group of a surface. Generalizations of congruence subgroups to other mapping class groups are discussed in [Sty18] and [FM11]. Perhaps it would be possible to find "the correct" version of the NS Theorem for the braid groups using the definitions from these other sources.

6.2 Vector-valued modular forms

Representations of Γ are a main ingredient in the theory of vector-valued modular forms. It would be interesting to understand what role of the congruence subgroup property of B_3 discussed in this work plays in the theory of vector-valued modular forms. Let $\mathbb{H}$ be the upper-half plane.

Definition 6.2.1 *Let $\rho : \mathrm{SL}(2, \mathbb{Z}) \to \mathrm{GL}(d, \mathbb{C})$ be a function and $w \in \mathbb{C}$. We call the pair (ρ, w) an* ***admissible multiplier system*** *of rank d if $\rho(I_2)$ is the identity, $e^{-\pi i w}\rho(-I_2)$ is the identity, and the associated automorphy factor $\widetilde{\rho}$ determined by*

$$\widetilde{\rho}_w(\gamma, \tau) = \rho(\gamma)(c\tau + d)^w$$

for $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ and $\tau \in \mathbb{H}$ satisfies

$$\widetilde{\rho}_w(\gamma_1\gamma_2, \tau) = \widetilde{\rho}_w(\gamma_1, \gamma_2 \cdot \tau)\widetilde{\rho}_w(\gamma_2, \tau)$$

for all $\gamma_1, \gamma_2 \in \mathrm{SL}(2\mathbb{Z})$ and $\tau \in \mathbb{H}$. In this case, we call w the ***weight*** *and ρ the* ***multiplier*** *of the system. Equivalently, (ρ, w) is admissible if there exists a representation $\hat{\rho} : B_3 \to \mathrm{GL}(d, \mathbb{C})$ such that $\hat{\rho}(\sigma_1\sigma_2)^3 = e^{\pi i w} I$.*

One can then define a vector-valued modular form for the multiplier system (ρ, w).

Definition 6.2.2 *Let (ρ, w) be an admissible multiplier system of rank d. A function $\mathbb{X} : \mathbb{H} \to \mathbb{C}^d$ is called a* ***vector-valued modular form*** *of weight w with multiplier ρ if*

$$\mathbb{X}(\gamma\tau) = \widetilde{\rho}_w(\gamma, \tau)\mathbb{X}(\tau)$$

for all $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ and $\tau \in \mathbb{H}$ and each component function $\mathbb{X}_i$ is meromorphic on $\mathbb{H}$.

Then there are two ways in which to investigate the connections between VVMF and quantum representations of B_3. We have parametrized possible multipliers for rank 2 and 3 multiplier systems. One could study the different properties of VVMFs associated to multipliers with congruence and non-congruence subgroups as kernels. In another direction, each the representations we considered in this work give rise to finite index subgroups of Γ. Similar to the classical case, there is a theory of vector-valued modular forms for subgroups of Γ and this theory splits naturally into the case of a congruence or non-congruence subgroup.

Bibliography

[Alp93] Roger Alperin. PSL(2,Z) = $Z_2 * Z_3$. *American Mathematical Monthly*, 100(4):385–386, 1993.

[And06] J.E. Andersen. Asymptotic faithfulness of the quantum SU(n) representations of the mapping class groups. *Annals of Mathematics*, 163(1):347–368, 2006.

[Art47] Emil Artin. Theory of braids. *Annals of Mathematics*, 48(1):101–126, 1947.

[Blo18] Wade Bloomquist. Asymptotic faithfulness of quantum sp(4) mapping class group representations. *ArXiv e-prints*, 2018.

[BSL64] H. Bass, J.-P. Serre, and M. Lazard. Sous-groupes d'indice fini dans SL(n, Z). *Bulletin of the American Mathematical Society*, 70:385–392, 1964.

[BW18] Wade Bloomquist and Zhenghan Wang. Comparing skein and quantum group representations and their application to asymptotic faithfulness. *Pure and Applied Mathematics Quarterly*, 2018.

[CHW15] S. X. Cui, S.-M. Hong, and Z. Wang. Universal quantum computation with weakly integral anyons. *Quantum Information Processing*, 14(8):2687–2727, August 2015.

[Dri90] V. Drinfeld. Quasi-hopf algebras. *Leningrad Mathematical Journal*, 1(6):1419–1457, 1990.

[DW71] I.M.S. Dey and James Wiegold. Generators for alternating and symmetric groups. *Journal of the Australian Mathematical Society*, 12(1):63–68, 1971.

[EGNO16] P. Etingof, Shlomo Gelaki, D. Nikshych, and V. Ostrik. *Tensor categories.* American Mathematical Society, 2016.

[ENO05] P. Etingof, D. Nikshych, and V. Ostrik. On fusion categories. *Annals of Mathematics*, 2(162):581–642, 2005.

[FK06] M.H. Freedman and V. Krushkal. On the asymptotics of quantum SU(2) representations of mapping class groups. *Forum Mathematicum*, 18(2):293–304, 2006.

[FLW00] M.H. Freedman, M.J. Larsen, and Z. Wang. A modular functor which is universal for quantum computation. *Communications in Mathematical Physics*, 227(3), 2000.

[FM11] Benson Farb and Dan Margalit. *A primer on mapping class groups.* Princeton University Press, 2011.

[Fun99] L. Funar. On the TQFT representations of the mapping class groups. *Pacific Journal of Mathematics*, 188(2):251–274, 1999.

[FWW02] M.H. Freedman, K. Walker, and Z. Wang. Quantum SU(2) faithfully detects mapping class groups modulo center. *Geometry and Topology*, 6:523–539, 2002.

[Gan60] Feliks Gant. *The theory of matrices.* Chelsea Publishing Company, 1960.

[Gan14] Terry Gannon. *The Theory of Vector-Valued Modular Forms for the Modular Group*, pages 247–286. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. ISBN 978-3-662-43831-2. doi:10.1007/978-3-662-43831-2_9.

[Hsu96] T. Hsu. Identifying congruence subgroups of the modular group. *Proceedings of the American Mathematical Society*, 5(5):1351–1359, 1996.

[Lan78] Saunders Mac Lane. *Categories for the Working Mathematician.* Springer-Verlag New York, 1978.

[LW05] M.J. Larsen and Z. Wang. Density of the SO(3) TQFT representation of mapping class groups. *Communications in Mathematical Physics*, 260(3):641–658, 2005.

[Men65] J. L. Mennicke. Finite factor groups of the unimodular group. *Annals of Mathematics*, 81:31–37, 1965.

[NR11] D. Naidu and E. Rowell. A finiteness property for braided fusion categrories. *Algebras and Representation Theory*, 14(5):837–855, 2011.

[NS10] S.-H. Ng and P. Schauenburg. Congruence subgroups and generalized Frobenius-Schur indicators. *Communications in Mathematical Physics*, 300(1):1–46, 2010.

[RT10] E. Rowell and I. Tuba. Finite linear quotients of B_3 of low dimension. *Journal of Knot Theory and its Ramifications*, 19(5):587–600, 2010.

[Sto84] W. W. Stothers. Level and index in the modular group. *Proceedings of the Royal Society of Edinburgh. Section A.*, 99(1-2):115–126, 1984.

[Sty18] Charalampos Stylianakis. Congruence subgroups of braid groups. *International Journal of Algebra and Computation*, 28(345), 2018.

[TW01] I. Tuba and H. Wenzl. Representations of the braid group B_3 and of SL(2,Z). *Pacific Journal of Mathematics*, 197(2):491–510, 2001.

[TY98] Daisuke Tambara and Shigeru Yamagami. Tensor categories with fusion rules of self-duality for finite abelian groups. *Journal of Algebra*, 209(2):692–707, 1998.

[Wan10] Z. Wang. *Topological quantum computation*, volume 112 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, Providence, RI, 2010.

[Yam02] Shigeru Yamagami. Polygonal presentations of semisimple tensor categories. *Journal of Mathematical Society of Japan*, 54(1):61–88, 2002.