

Near-Group Categories

Jacob A. Siehler

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Mathematics

Frank Quinn, Chair
Edward Green
Peter Haskell
Peter Linnell
Mark Shimozone

April 18, 2003
Blacksburg, Virginia

Keywords: monoidal categories, braided categories, quantum field theory
Copyright 2003, Jacob A. Siehler

Near-Group Categories

Jacob A. Siehler

(ABSTRACT)

We consider the possibility of semisimple tensor categories whose fusion rule includes exactly one noninvertible simple object, so-called *near-group* categories. Data describing the fusion rule is reduced to an abelian group G and a nonnegative integer k . Conditions are given, in terms of G and k , for the existence or nonexistence of coherent associative structures for such fusion rules (ie, solutions to MacLane's pentagon equation). An explicit construction of matrix solutions to the pentagon equations is given for the cases where we establish existence, and classification of the distinct solutions is carried out partially. Many of these associative structures also support (braided) commutative and tortile structures and we indicate when the additional structures are possible. Small examples are presented in detail suitable for use in computational applications.

Acknowledgements

Thanks to

Frank Quinn
for his guidance, friendship, and apparently inexhaustible patience,
my professors at Virginia Tech and at Frostburg State,
and the faculty of the Budapest Semesters in Mathematics program.

I would have been quite lost without them steering me in the right direction.

Dedicated to

The memory of my mother, Julia Siehler.

CONTENTS

Chapter I. Introduction and summary of results	1
1.1 A little history	1
1.2 Near-group categories	1
1.3 Summary of results	2
Chapter II. Braidings for the $k = 0$ categories	6
2.1 Notation for commutativities	6
2.2 Extracting the invariants	6
2.3 Realizing the parameters	7
2.4 Proofs for 1.3.2 and 1.3.3	7
2.5 An example	11
2.6 The ground ring	12
Chapter III. Monoidal structures for the $k > 0$ categories	13
3.1 Notation for associativities	13
3.2 Examples for small k	16
3.3 Pentagon equations and proof for Theorem 1.3.5	19
3.4 Further reductions of pentagon equations	23
3.5 Groups which support a permutation π	38
3.6 The trivial-group case	40
Chapter IV. Additional structures for the $k > 0$ categories	43
4.1 Commutativity and hexagon equations	43
4.2 Examples of braidings	51
4.3 Twist	54
References	55

INTRODUCTION AND SURVEY OF RESULTS

1.1 A little history

The roots of this paper go back, approximately, to the 1959 paper [St] in which Stasheff develops a series of homotopy obstructions to the problem of rectifying an H -space structure into an associative H -space structure. To start the problem, we assume that the two possible iterated multiplications for a three-fold product are not equal, but homotopic, and we have chosen homotopies to do the job. These homotopies determine a map of S^1 , decomposed as a polyhedron with five vertices, and the first obstruction is extending this map across a disc. The vertices of the pentagon correspond to the five possible parenthesisations of a four-fold product. The remaining obstructions are also extension problems from a sphere (presented as a polyhedron) across a ball. If all the obstructions vanish, the given H -space is equivalent (as an H -space) to an H -space which is strictly associative. The proof of all this is a generalization of the Milnor construction of the classifying space for a topological group.

A categorical analog of Stasheff's problem is as follows: H -space gets replaced with *monoidal category*; that is, a category with a bifunctorial product. These are also known as tensor categories. See [Mac] for precise definitions. Associative-up-to-homotopy gets replaced with associative-up-to-natural-isomorphism; choosing homotopies gets replaced with choosing specific associativity isomorphisms. The question is whether the category thus equipped is equivalent to a monoidal category in which the associativity isomorphisms are in fact identity maps. But here, MacLane's coherence theorem [Mac] says that for categories only the first-level obstruction matters. If the pentagonal diagram corresponding to four-fold products commutes, then the product is equivalent to an associative one.

MacLane also proves [Mac] a similar coherence theorem involving commutativity isomorphisms, under the assumption that the commuting isomorphisms "square" to the identity. With this hypothesis, we call the categories *symmetric-commutative*. In this setting the theorem requires that a certain hexagonal diagram (involving the various parenthesisations and permutations of three-fold products) commutes.

Subsequently quite a lot of coherence theorems have been proven for extra structures on monoidal categories. From a topological point of view, the most significant of these are as follows: The 1993 paper [JS] proves a coherence theorem for categories with commutativity that doesn't square to the identity. These are called *braided-commutative* categories; the terminology comes from the fact that the topological category of braids is the free braided-commutative category generated by one object. That paper is actually a revised version of work that originally appeared in 1985. Subsequently, in 1994, [Sh] defines *tortile* categories by adding a few axioms to braided categories, and proves a coherence theorem which says that tortile categories bear the same relationship to the category of framed tangles as braided categories do to the category of braids.

Connections between structured categories and low-dimensional topology became strengthened as categories became the preferred language for (topological) quantum field theory. I simply defer to two excellent references on this matter; Quinn [Q] gives a careful treatment of the use of symmetric-commutative categories for field-theory invariants of 2-complexes (and so presentations

of groups); Turaev's book [T] is a reference for the process by which one can produce field theory invariants of 3-manifolds from tortile categories under a strong nondegeneracy condition called modularity. With modularity added to the axioms of a tortile category, it is possible to generate invariants of framed links that are stable under Kirby calculus moves.

The purpose of the present paper is not to introduce new axioms or coherence theorems, but to provide some tractable examples of categories that do and do not satisfy the various axioms; there is not much structure theory available for monoidal categories in general and it seems that a good source of examples may help the development of such a theory. When we restrict our attention to *semisimple* categories (explained below), the various axioms (pentagon, hexagon, and so on) translate into large matrix equations for which we must find solutions. They may be intractable to solve in general, but here we introduce a class of categories where the equations can be solved.

1.2 Near-group categories

The scope of the present paper is limited to finite semisimple monoidal categories with duality.

Finite semisimple means: our categories have a "ground ring" R , and hom sets in the category are free R -modules; that is, there is a finite set of simple objects s_i with

$$\mathrm{hom}(s_i, s_j) \cong \begin{cases} R, & i = j \\ 0, & i \neq j \end{cases}$$

and every object in the category is (isomorphic to) a direct sum of simple objects.

Monoidal means: there is a (bifunctorial) tensor product $\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$. We assume the existence of a unit object (ϵ) for our tensor product (so that tensoring on either side by ϵ is naturally isomorphic to the identity). For objects a, b, c there are natural associativity morphisms $\alpha_{a,b,c} : (a \otimes b) \otimes c \rightarrow a \otimes (b \otimes c)$, and these satisfy the pentagon axiom.

Duality means: every object x has a dual object x^* . Moreover, there exist "pairing" and "copairing" morphisms $\lambda_x : x^* \otimes x \rightarrow \epsilon$ and $\Lambda_x : \epsilon \rightarrow x \otimes x^*$ which satisfy the identities:

$$(\mathrm{id}_x \otimes \lambda_x)(\alpha_{x,x^*,x})(\Lambda_x \otimes \mathrm{id}_x) = \mathrm{id}_x$$

and

$$(\lambda_x \otimes \mathrm{id}_{x^*})(\alpha_{x^*,x,x^*})^{-1}(\mathrm{id}_{x^*} \otimes \Lambda_x) = \mathrm{id}_{x^*}$$

A consequence of this hypothesis is the existence of adjunction isomorphisms $\mathrm{hom}(x \otimes y, z) \cong \mathrm{hom}(x, z \otimes y^*)$ and $\mathrm{hom}(x, y \otimes z) \cong \mathrm{hom}(y^* \otimes x, z)$. As a special case, simples s_i and s_j have

$$\mathrm{hom}(\epsilon, s_i \otimes s_j) \cong \begin{cases} R, & s_j = s_i^* \\ 0, & \text{otherwise} \end{cases}$$

Categories in which every simple has a multiplicative inverse (so $g \otimes g^{-1} \cong \epsilon$) have been studied carefully, and called variously Θ -categories ([FK]) or *group-categories* [Q2]. Note that the multiplicative inverse is the same object as the dual. Complete information is available about the classification of categorical structures on group-categories and the interpretation of their field theories (in [Q2]). The classification is possible in one sense because all the structural equations are 1-dimensional and there is no noncommutative matrix arithmetic involved in their solutions.

In the present paper we would like to advance to studying a slightly more complicated sort of multiplication, in which there is (up to isomorphism) a single noninvertible simple object. For a category with such a multiplication we introduce the term *near-group category*. The noninvertible

simple object we will call m . The invertible simple objects comprise a group G under tensor product; invertibility of the group elements implies

$$g \otimes m \cong m \otimes g \cong m$$

for any invertible g . Moreover, the duality assumption implies

$$m \otimes m \cong G \oplus k \cdot m$$

that is, $m \otimes m$ splits as one summand of each invertible type, and some number k of m -summands (possibly $k = 0$). We see that the multiplication table (or *fusion rule*) for a near-group category is described by giving the group G and the integer k ; we will refer to categories with the *near-group fusion rule* (G, k) .

The first question of interest is which (G, k) actually occur as fusion rules of near-group categories; the primary issue is the existence of coherent associativity, but we also want to investigate which G and k admit the additional layers of structure we have indicated in the preceding section.

1.3 Summary of results

There is a significant difference between the fusion rules with $k = 0$ and those with $k > 0$. For the $k = 0$ categories, Tambara and Yamagami [TY] have already classified the monoidal structures. Their result is:

1.3.1 Theorem (Tambara-Yamagami). *Monoidal near-group categories with fusion rule $(G, 0)$ correspond to pairs (χ, τ) where χ is a nondegenerate, symmetric R -valued bicharacter of G , and τ is a square root of $1/|G|$*

Notice in this case ($k = 0$), there are no constraints on the group; any abelian group may occur as the group of invertibles in a near-group category with $k = 0$ (provided that the $|G|$ is invertible and has a square root in the ground ring).

Our main result in this case is the following theorem, which gives necessary and sufficient conditions under which these categories admit a balanced (tortile) braided structure, and parametrizes the distinct braidings.

1.3.2 Theorem. *Suppose G is a finite abelian group, \mathcal{C} is a monoidal near-group category with fusion rule $(G, 0)$, and R contains roots of unity of order $8|G|$. Then*

- (1) \mathcal{C} admits a braiding if and only if G is an elementary abelian 2-group; that is, every element has order 2.
- (2) The nonequivalent braidings on \mathcal{C} are in one-to-one correspondence with $(n + 1)$ -tuples $(\delta_1, \dots, \delta_n, \Delta)$, where $\Delta = \pm 1$ and $\delta_i = \pm 1$ for all i , and n is the rank of G .
- (3) Each braiding of \mathcal{C} has exactly two choices of twist morphisms compatible with it.

Explicit computation of the commutativities further establishes

1.3.3 Corollary. *In any braiding of \mathcal{C} ,*

- (1) *the group subcategory generated by invertibles is symmetric commutative.*
- (2) *a basis can be chosen so that every commuting isomorphism is multiplication by an $8|G|$ -th root of unity.*

In 2.5 we give a simple example to show that that the order condition of 1.3.3(2) is sharp, and 2.6 contains some additional comments about the conditions on the ground ring R .

For the case when $k > 0$, we give the following results. Regarding monoidal structures:

1.3.4 Theorem (Order control). *If the near-group fusion rule (G, k) admits a monoidal structure then $|G| \leq k + 1$.*

1.3.5 Theorem (Existence). *In the maximal case $|G| = k + 1$ the near-group fusion rule (G, k) admits a monoidal structure iff G is the multiplicative group of a finite field (ie, cyclic of order $p^\alpha - 1$ for prime p).*

Note in this case ($k > 0$), there are very constraints on which groups may appear, in contrast with the $k = 0$ case.

To prove necessity in 1.3.5, we examine in detail (3.3 and 3.4) the pentagon equations in the category; we find that G must support some special structure (3.3.2) and we show (3.5) that only the specified groups support this structure.

We give two different proofs of sufficiency. In 3.3.1 a finite group is constructed whose category of representations has the given fusion rule. Representation categories are symmetric monoidal, so this also shows if there is any monoidal category then there is a symmetric one. The other proof of sufficiency is in 3.4.18. This uses the analysis of the pentagon equations carried out in 3.3 and 3.4 to directly exhibit solutions of the matrix equations. This approach gives information about the whole set of categories, including some that do not admit braidings. There is a “simplest” standard solution; analysis of hexagon equations in 4.1 verifies that this solution additionally admits a symmetric commuting structure. It seems likely that this is the representation category exhibited earlier, but this has not been verified.

The analysis of the pentagon equations enables small cases to be worked out completely.

1.3.6 Theorem. *The first three maximal-order cases have the following structure.*

<i>fusion</i>	<i>field</i>	<i>monoidal str</i>	<i>braidings</i>	<i>balance</i>	<i>symmetric</i>
$(\mathbb{Z}/2, 1)$	F_3	3, indexed by $\xi, \xi^3 = 1$	$\xi = 1, 3$ indexed by $\psi^3 = 1$ $\xi \neq 1$ not braided	$\psi = 1$ bal. $\psi \neq 1$ not	$\psi = 1$ symmetric
$(\mathbb{Z}/3, 2)$	F_{2^2}	2, indexed by $\xi = \pm 1$	$\xi = 1, 4$ indexed by $\psi(1), \psi(2) = \pm 1$ $\xi \neq 1$ not braided	all balanced	$\psi(1) = \psi(2)$ sym $\psi(1) = -\psi(2)$ not
$(\mathbb{Z}/4, 3)$	F_5	unique monoidal str	unique braiding	balanced	symmetric

The primes 2 and 3 play special roles in the analysis, so the complexity of the first two cases probably is representative of the fusion rules corresponding to finite fields of characteristic 2 or 3. Larger primes may have simpler behavior, though the complete uniqueness seen in the F_5 case is probably too simple.

At the other extreme from the maximal-order case we have:

1.3.7 Theorem. *Assume that the characteristic of the ground ring R is not equal to 2. Then, in the minimal case $|G| = 1$, the near-group fusion rule (G, k) does not admit a monoidal structure if $k \equiv 2$ or $3 \pmod{4}$*

Remark. A stronger result is obtained in [O] for the case where the ground ring has characteristic zero, but the present proof works also for positive odd characteristic.

We prove this in 3.6. When G is small there is less symmetry to exploit and the pentagon equations become much more difficult; nonexistence theorems are easier than constructions. For $k = 1$ and $|G| = 1$ it is not difficult to solve (the unique characteristic 5 solution is given in [Q];

this lifts to two distinct solutions in characteristic 0). But the next possible trivial-group case, $k = 4$, so far seems to be intractable.

4.1 reduces the hexagon equations and gives a standard construction of commutativity data. 4.2 then gives the braidings possible for the example categories from 3.2, and this includes nonsymmetric braidings on the standard monoidal structures; it turns out that the more exotic monoidal structures exhibited in 3.2 do not support braidings.

4.3 gives a brief note on the possibility of adding twist morphisms to the braided near-group categories studied in sections 4.2 (producing tortile categories).

BRAIDINGS FOR THE $k = 0$ CATEGORIES

In this chapter we introduce some notation for the commuting isomorphisms in a near-group categories with $k = 0$ fusion rules, show how to compute the classifying invariant $(\delta_1, \dots, \delta_n, \Delta)$, and prove the classification theorem 1.3.2 and its corollary 1.3.3. Also we give an example to show that the hypotheses of the theorem are sharp and include some remarks on the necessity of roots of unity in the ground ring R .

2.1 Notation

In a near-group category there are four different kinds of commutes to consider, and we use notation that recognizes their different roles. For $g, h \in G$, the commuting isomorphisms are:

$$\begin{aligned} gh &\rightarrow hg && \text{is multiplication by } \sigma_0(g, h) \\ gm &\rightarrow mg && \text{is multiplication by } \sigma_1(g) \\ mg &\rightarrow gm && \text{is multiplication by } \sigma_2(g) \\ mm &\rightarrow mm && \text{is multiplication by } \sigma_3(g) \text{ on the } g \text{ summand} \end{aligned}$$

2.2 Extracting the invariants

We first want to clarify the result of [TY] cited in 1.1.1. Saying that χ is a bicharacter of G means that $\chi(ab, c) = \chi(a, c)\chi(b, c)$ and $\chi(a, bc) = \chi(a, b)\chi(a, c)$; this is just a bilinear form written multiplicatively. The technique of [TY] is to establish that for each pair (χ, τ) there is a choice of basis, called a *normal basis*, so that the associativities in the category have the following form: for $a, b, c \in G$,

$$\begin{aligned} \alpha_{a,b,c} &= 1 \\ \alpha_{a,b,m} &= \alpha_{m,a,b} = 1 \\ \alpha_{a,m,b} &= \chi(a, b) \\ \alpha_{a,m,m} &= \alpha_{m,m,a} = \oplus_b \mathbf{1}_b \\ \alpha_{m,a,m} &= \oplus_b \chi(a, b) \\ \alpha_{m,m,m} &= (\tau\chi(a, b)^{-1})_{a,b} \end{aligned}$$

and moreover,

$$\alpha_{m,m,m}^{-1} = (\tau\chi(a, b))_{a,b}$$

Now, to obtain the $(\delta_1, \dots, \delta_n, \Delta)$ describing the commutativity, fix generators g_1 through g_n for G and choose a normal basis for the parameters χ and τ describing the associative structure. Then the δ_i and Δ parameters are computed by taking

$$\delta_i = \frac{\sigma_1(g_i)}{\sqrt{\chi(g_i, g_i)}}$$

and

$$\Delta = \frac{\sigma_3(\epsilon)}{\sqrt{\tau \sum_{g \in G} \sigma_1(g)}}$$

It is not obvious that these invariants are ± 1 -valued; this will follow from our examination of the hexagon equations below.

2.3 Realizing the parameters

[TY] gives the construction to realize the parameters χ and τ describing the associative structure. We assume we have that construction in hand and fix a normal basis for it. Realizing the braiding parameters $(\delta_1, \dots, \delta_n, \Delta)$ means explicitly giving the values of the σ functions.

1. Commuting group elements. Set

$$\sigma_0(g, h) = \chi(g, h)$$

2. Commuting a group element with the noninvertible. First, for the generators g_i , set

$$\sigma_1(g_i) = \sigma_2(g_i) = \delta_i \sqrt{\chi(g_i, g_i)}$$

Any other element g in the group can be written uniquely as a product of generators with each generator appearing at most once (generators have order 2). Say $g = h_1 h_2 \cdots h_k$ is the expression for g as a product of generators. Set

$$\sigma_1(g) = \sigma_2(g) = \prod_{i=1}^k \left(\sigma_1(h_i) \prod_{i < j \leq k} \chi(h_i, h_j) \right)$$

3. Commuting the noninvertible with itself. This also goes in two steps. First, set

$$\sigma_3(\epsilon) = \Delta \cdot \sqrt{\tau \sum_{g \in G} \sigma_1(g)}$$

Then, for any other $g \in G$, set

$$\sigma_3(g) = \sigma_3(\epsilon) \sigma_1(g) \chi(g, g)$$

Comparing these definitions to the procedure above for extracting invariants, it is clear that the σ 's we have defined do realize the parameters $(\delta_1, \dots, \delta_n, \Delta)$.

Note. We see from the formulas that the commutativity inside the group category is entirely determined by the associativity parameters; all the “new” information concerns the behavior of the noninvertible.

2.4. Proofs of results for $k = 0$ categories.

2.4.1 The hexagon restraints. The results of the theorem come directly from the hexagon axioms. If we let a, b, c stand for group elements, there are eight types of three-term products to consider: $abc, abm, amb, mab, mma, mam, amm,$ and mmm . Using a normal basis, we can express

associativities in terms of χ and τ , and write out the standard hexagon equations corresponding to the eight three-term products:

$$\begin{aligned}
\sigma_0(a, b)\sigma_0(a, c) &= \sigma_0(a, bc) \\
\sigma_0(a, b) &= \chi(b, a) \\
\sigma_0(a, b)\sigma_1(a) &= \sigma_1(a)\chi(a, b) \\
\sigma_2(ab) &= \sigma_2(b)\chi(a, b)\sigma_2(a) \\
\sigma_2(a)\sigma_3(ba^{-1}) &= \chi(a, b)\sigma_3(b) \\
\sigma_3(a^{-1}b)\sigma_2(a) &= \sigma_3(b)\chi(a, b) \\
\sigma_0(a, a^{-1}b) &= \sigma_1(a)\chi(a, b)\sigma_1(a) \\
\sigma_3(a)\tau\chi(a, b)^{-1}\sigma_3(b) &= \sum_{c \in G} \tau\chi(a, c)^{-1}\tau\sigma_2(c)\chi(c, b)^{-1}
\end{aligned}$$

The hexagon for mmm actually gives the matrix equation $AS_2A = S_3AS_3$, where $A = \alpha_{m,m,m} = (\chi(a, b))_{a,b}$, $S_2 = \oplus_a \sigma_2(a)$ and $S_3 = \oplus_a \sigma_3(a)$. The final equation in the list above corresponds to the (a, b) -th entry of the matrix equation.

There are some obvious redundancies among the hexagon equations; eliminating these and simplifying the remaining ones yields the following reduced set of equations, equivalent to the original eight:

$$\sigma_0(a, b) = \chi(a, b) \tag{1}$$

$$\sigma_2(ab) = \sigma_2(a)\sigma_2(b)\chi(a, b) \tag{2}$$

$$\sigma_2(a)\sigma_3(ba^{-1}) = \chi(a, b)\sigma_3(b) \tag{3}$$

$$\sigma_1(a)^2 = \chi(a^{-1}, a) \tag{4}$$

$$\tau \sum_c \chi(ab, c)^{-1}\sigma_2(c) = \chi(a, b)^{-1}\sigma_3(a)\sigma_3(b) \tag{5}$$

Computing the inverse hexagons amounts to inverting associativities and reversing commutativities, producing:

$$\sigma_0(b, a) = \chi(a, b)^{-1} \tag{6}$$

$$\sigma_1(ab) = \sigma_1(a)\sigma_1(b)\chi(a, b)^{-1} \tag{7}$$

$$\sigma_1(a)\sigma_3(ba^{-1}) = \chi(a, b)^{-1}\sigma_3(b) \tag{8}$$

$$\sigma_2(a)^2 = \chi(a, a) \tag{9}$$

$$\tau \sum_c \chi(ab, c)\sigma_1(c) = \chi(a, b)\sigma_3(a)\sigma_3(b) \tag{10}$$

2.4.2 Proof of 1.3.2(1). Equations (1) and (6) together with the fact that χ is symmetric imply that $\chi(a, b) = \chi(a, b)^{-1}$ for every $a, b \in G$; that is, χ is ± 1 -valued. But χ is also nondegenerate. If $|a| = 2n + 1$, then $\chi(a, b)^{2n+1} = \chi(1, b) = 1$ for every b . So $\chi(a, b) = 1$ for every b , contradicting nondegeneracy. If $|a| = 2n$ for $n > 1$ then $a^2 \neq 1$ but $\chi(a^2, b) = 1$ for every b , also contradicting nondegeneracy. This shows that every element in G has order 2, as claimed.

2.4.3 Note. Since group elements are self-inverse, we will now drop the inverse signs from group elements whenever they appear. Likewise, we replace χ^{-1} with χ wherever it appears.

2.4.4 Proof of Corollary 1.3.3(1). For invertibles g and h ,

$$\sigma_0(g, h)\sigma_0(h, g) = \chi(g, h)\chi(h, g) = \chi(g, h)^2 = 1.$$

2.4.5 Proof of 1.3.2(2).

1. The invariant $(\delta_1, \dots, \delta_n, \Delta)$ is well-defined. We have to show that our definition is independent of the choice of normal basis that was made. For any group element a , let a_l and a_r be the basis for $\text{hom}(m, am)$ and $\text{hom}(m, ma)$, respectively, in some normal basis; let a'_l and a'_r play the same role in some other normal basis. With respect to any normal basis (by definition), the association $(ma)m \rightarrow m(am)$ is represented by the identity on the 1 summand. That implies that there is some k in the ground ring so that $a'_l = ka_l$ and $a'_r = ka_r$; it follows that the commuting isomorphism $\sigma_1(a) : am \rightarrow ma$ is represented the same with respect to either normal basis, so setting $\delta_i = \sigma_1(g_i)/\sqrt{\chi(g_i, g_i)}$ is well-defined.

It is clear that $\sigma_3(\epsilon)$ doesn't depend on the choice of basis of $\text{hom}(1, mm)$; together with the preceding argument, this is enough to establish that the invariant Δ is well-defined.

2. Giving $(\delta_1, \dots, \delta_n, \Delta)$ determines the commutativity. We have already noted that σ_0 is totally determined by the associative structure. Equations (3) and (8) together imply that $\sigma_1 \equiv \sigma_2$. Equations (2) and (7) say that σ_1 and σ_2 are determined by their values on the generators g_1, \dots, g_n for G ; finally, (4) and (9) say that $\sigma_1(g_i) = \sigma_2(g_i)$ is determined, up to a sign, by the value of $\chi(g_i, g_i)$. Therefore, giving the δ_i to specify those signs is enough to determine σ_1 and σ_2 .

Equation (3) says that σ_3 is determined by its value on any one group element. For instance, specifying $\sigma_3(\epsilon)$ is enough to describe σ_3 entirely. But evaluating (5) for the special case $a = b = 1$, we get

$$\sigma_3(\epsilon)^2 = \tau \sum_{c \in G} \sigma_1(c)$$

So $\sigma_3(\epsilon)$ is in fact determined up to a sign, and giving Δ to specify that sign is enough to determine σ_3 , completing the description of all the commutativities.

3. Every $(\delta_1, \dots, \delta_n, \Delta)$ can be realized. Define the σ functions according to the construction given in 2.3. We have to show that all the hexagon equations are satisfied. Clearly, equations (1) and (6) are satisfied.

Next, we will verify (2) and (7); since the construction defines σ_1 and σ_2 to be equal, and since we can drop inverses, it suffices to check that (2) is satisfied. For a generator g_i ,

$$\sigma_2(g_i)^2 = \left(\delta_i \sqrt{\chi(g_i, g_i)} \right)^2 = \chi(g_i, g_i)$$

so (2) is satisfied on generators. For any element $g = h_1 h_2 \cdots h_k$ expressed as a product of generators,

$$\begin{aligned} \sigma_2(g)^2 &= \left(\prod_{i=1}^k \left(\sigma_2(h_i) \prod_{i < j \leq k} \chi(h_i, h_j) \right) \right)^2 \\ &= \prod_{i=1}^k \sigma_2(h_i)^2 \quad \text{since } \chi^2 = 1 \\ &= \prod_{i=1}^k \chi(h_i, h_i) \end{aligned}$$

Working from the other end,

$$\begin{aligned}
\chi(g, g) &= \chi(h_1 h_2 \cdots h_k, h_1 h_2 \cdots h_k) \\
&= \prod_{1 \leq i, j \leq k} \chi(h_i, h_j) \\
&= \prod_{i=1}^k \chi(h_i, h_i) \quad \text{since } \chi(h_i, h_j) \chi(h_j, h_i) = 1 \text{ when } i \neq j
\end{aligned}$$

This establishes that $\sigma_2(g)^2 = \chi(g, g)$ for every $g \in G$, so equations (2) and (7) are satisfied.

To show that (3) and (8) are satisfied, it suffices to check one or the other; we show that (8) holds (remember that we can drop inverses):

$$\begin{aligned}
\sigma_1(a) \sigma_3(ab) &= \sigma_1(a) \sigma_3(\epsilon) \sigma_1(ab) \chi(ab, ab) \\
&= \sigma_1(a) \sigma_3(\epsilon) \sigma_1(a) \sigma_1(b) \chi(a, b) \chi(ab, ab) \\
&= \sigma_1(a)^2 \sigma_3(\epsilon) \sigma_1(b) \chi(a, b) \chi(a, a) \chi(b, b) \\
&= \chi(a, a)^2 \chi(a, b) \sigma_3(\epsilon) \sigma_1(b) \chi(b, b) \\
&= \chi(a, b) \sigma_3(b)
\end{aligned}$$

Finally we check that (10) is satisfied; (5) is identical. This is another computation directly from the definitions:

$$\begin{aligned}
\chi(a, b) \sigma_3(a) \sigma_3(b) &= \chi(a, b) \chi(a, a) \chi(b, b) \sigma_1(a) \sigma_1(b) \sigma_3(\epsilon)^2 \\
&= \chi(a, b) \chi(a, a) \chi(b, b) \sigma_1(a) \sigma_1(b) \tau \sum_c \sigma_1(c) \\
&= \tau \sum_c \chi(a, a) \chi(b, b) \sigma_1(ab) \sigma_1(c) \\
&= \tau \sum_c \chi(a, a) \chi(b, b) \chi(ab, c) \sigma_1(abc) \\
&= \tau \sum_c \chi(ab, abc) \sigma_1(abc) = \tau \sum_c \chi(ab, c) \sigma_1(c)
\end{aligned}$$

which shows that (10) and (5) are satisfied and completes the verification that the construction gives a commutativity satisfying all the hexagon equations.

2.4.6 Proof of 1.3.2(3). The balance axiom requires that we produce automorphisms θ_s for each simple object s satisfying $\theta_{rs} = \theta_r \theta_s \sigma(r, s) \sigma(s, r)$. Here, that means that for all $g, h \in G$, we must have

$$\begin{aligned}
\theta_{gh} &= \theta_g \theta_h \sigma_0(h, g) \sigma_0(g, h) \\
\theta_m &= \theta_g \theta_m \sigma_1(g) \sigma_2(g) \\
\text{and } \theta_g &= \theta_m^2 \sigma_3(g)^2
\end{aligned}$$

We know that commutativity in the group subcategory is symmetric, and with respect to a normal basis we know that $\sigma_1 = \sigma_2$. So we can give a slightly simplified statement of the requirements:

$$\theta_{gh} = \theta_g \theta_h \tag{11}$$

$$\theta_g = \sigma_1(g)^2 \tag{12}$$

$$\theta_g = \theta_m^2 \sigma_3(g)^2 \tag{13}$$

Strictly speaking, equation (12) should be $\theta_g = \sigma_1(g)^{-2}$, but $\sigma_1(g)^2 = \chi(g, g) = \pm 1$, so dropping the inverse is harmless. To show that the category is balanced we define

$$\begin{aligned}\theta_g &:= \sigma_1(g)^2 \\ \text{and } \theta_m &:= \pm 1/\sigma_3(\epsilon)\end{aligned}$$

and check that these satisfy the axioms. Equation (12) is obviously satisfied. We check (11):

$$\theta_{gh} = \sigma_1(gh)^2 = (\sigma_1(g)\sigma_1(h)\chi(g, h))^2 = \sigma_1(g)^2\sigma_1(h)^2 = \theta_g\theta_h$$

and (13):

$$\begin{aligned}\theta_m^2\sigma_3(g)^2 &= \frac{1}{\sigma_3(\epsilon)^2}(\sigma_3(\epsilon)\sigma_1(g)\chi(g, g))^2 \\ &= \sigma_1(g)^2 = \theta_g\end{aligned}$$

This shows that there are two choices of twist morphisms which balance the commutativity; conversely, it is obvious that we had to define the twist morphisms as we did, so these are the only two possibilities, concluding the proof of Theorem 1.

2.4.7 Proof of Corollary 1.3.3(2). Assume that the σ functions are defined according to the construction in 2.3. We want to show that they take values in the roots of unity. First, $\sigma_0(g, h) = \chi(g, h)$ so σ_0 is ± 1 -valued. Also, $\sigma_1(g)^2 = \sigma_2(g)^2 = \chi(g, g)$ so σ_1 and σ_2 take values that are at most 4th roots of unity.

Now, recall from 3.1 that the hexagon for mmm can be expressed as the matrix equation $AS_2A = S_3AS_3$. Pass to determinants; $A^2 = I$, so $\det A = \pm 1$, and

$$\begin{aligned}\det A \det S_1 &= \det S_3^2 \\ \pm \prod_g \sigma_1(g) &= \prod_g \sigma_3(g)^2 \\ \pm \prod_g \sigma_1(g) &= \prod_g \sigma_3(\epsilon)^2 \sigma_1(g)^2 \chi(g, g)^2 \\ \sigma_3(\epsilon)^{2|G|} &= \pm \prod_g \sigma_1(g)^{-1}\end{aligned}$$

so $\sigma_3(\epsilon)^{8|G|} = 1$. For any other $g \in G$, $\sigma_3(g) = \sigma_3(\epsilon)\sigma_1(g)\chi(g, g)$, so $\sigma_3(g)^{8|G|} = 1$, completing the proof.

2.5 An example

If we let $G = \langle g \rangle$ be the cyclic 2-group, we obtain examples showing that the bounds of Corollary 1.3(2) are best possible without additional hypotheses. There is only one nondegenerate bicharacter χ on G ; monoidal structures are given by $\tau = \pm(1/\sqrt{2})$, and braidings are given by pairs (δ, Δ) of ± 1 's. If we leave the parameters generic, we can compute the interesting commutativities (I stands for a primitive 4th root of 1):

$$\begin{aligned}\sigma_1(\epsilon) &= \sigma_2(\epsilon) = 1 \\ \sigma_1(g) &= \sigma_2(g) = \delta I \\ \sigma_3(\epsilon) &= \Delta \sqrt{\tau(1 + \delta I)} \\ \sigma_3(g) &= \Delta \delta I \sqrt{\tau(1 + \delta I)}\end{aligned}$$

In this case, regardless of the parameters, it is easily verified that $\sigma_3(\epsilon)$ and $\sigma_3(g)$ are primitive 16th roots of unity.

2.6 The ground ring

Theorem 1.3.2 says that if R has enough roots of unity, then every $(\delta_1, \dots, \delta_n, \Delta)$ can be realized as a braiding over R . In general, if R does not have enough roots of unity, some of these will be impossible to realize. The example from 2.5 should be sufficiently cautionary: there, none of the parameter sets can be realized unless the exact hypotheses of theorem 1.3.2 are satisfied. On the other hand, the explicit formulas we have for the associativities and commutativities show that a lack of roots of unity is essentially the only obstruction to realizing the braidings.

We note that near-group categories are never defined over the integers; this is ruled out just by the monoidal structure, since τ is never integral, yet it necessarily appears in the associativity of the noninvertible. We also point out that the bicharacter χ has an important effect on what roots of unity are required. If $\chi(g, g) = -1$ for any $g \in G$, then at least 4th roots of unity are unavoidable in realizing the braidings (this is because $\sigma_1(g)^2 = \chi(g, g)$). Conversely, if $\chi(g, g) = +1$ for every g , then we can refine the proof of 1.3.2(2) to show that we need only $4|G|$ -th roots of unity to realize all the braidings.

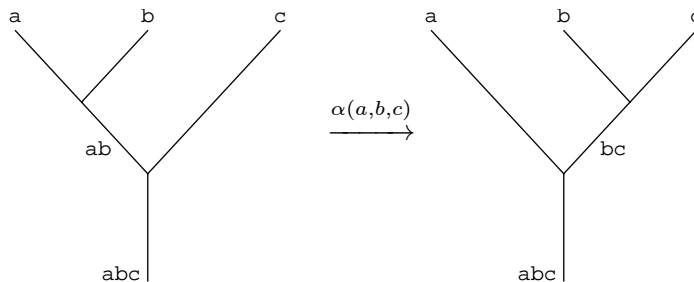
MONOIDAL STRUCTURES FOR THE $k > 0$ CATEGORIES

This chapter contains analysis of the pentagon equations in near-group categories with fusion rule (G, k) where $k > 0$, that is, those categories in which $m \otimes m$ contains some copies of the noninvertible simple m . We will introduce some notation for associativity maps, give the examples promised in 1.3.6, and carry out the proofs of theorems 1.3.4, 1.3.5, and 1.3.7.

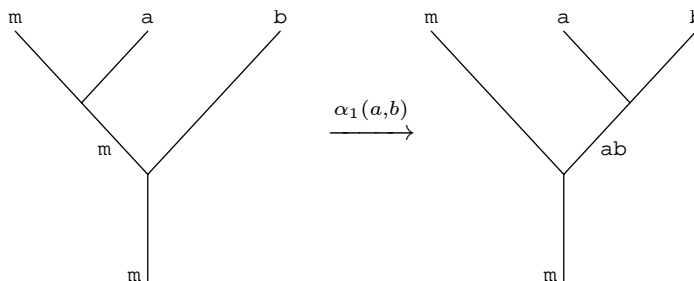
3.1 Notation for associativities

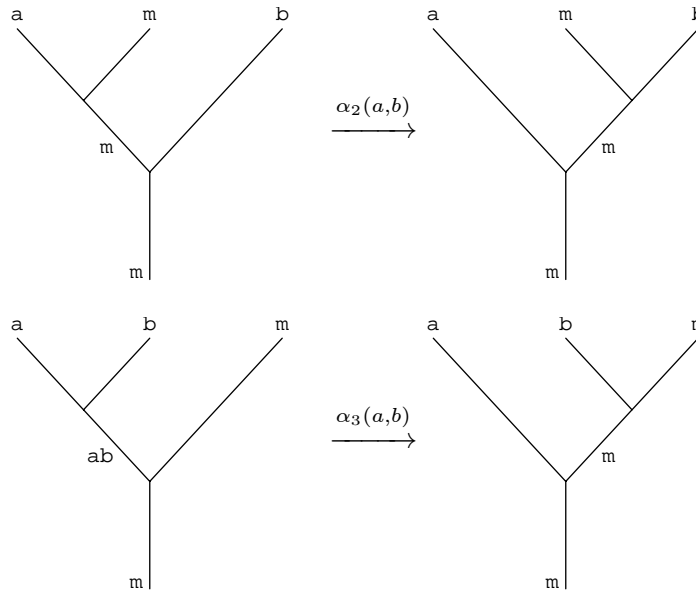
In 3.2 we will give examples and complete data for categories with small values of k . Before doing that we need to introduce notation used to present the many different associativities in the category; this scheme is an extension of the notation used in [TY], and in later sections this notation is used extensively in proofs and calculations. Throughout this section, let a, b, c stand for arbitrary elements of G .

3.1.1 Associativities involving a product of three group elements. These we denote by a function α depending on three group variables.

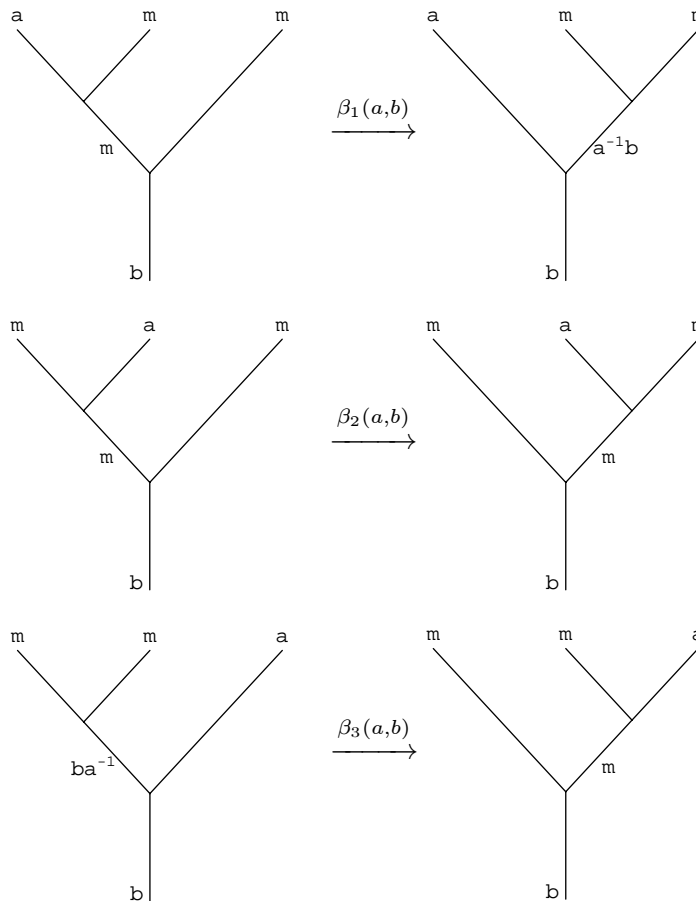


3.1.2 Associativities involving two group elements and one m . These we think of as a function of the two group elements, denoted by α 's with a subscript to indicate the position of the m :



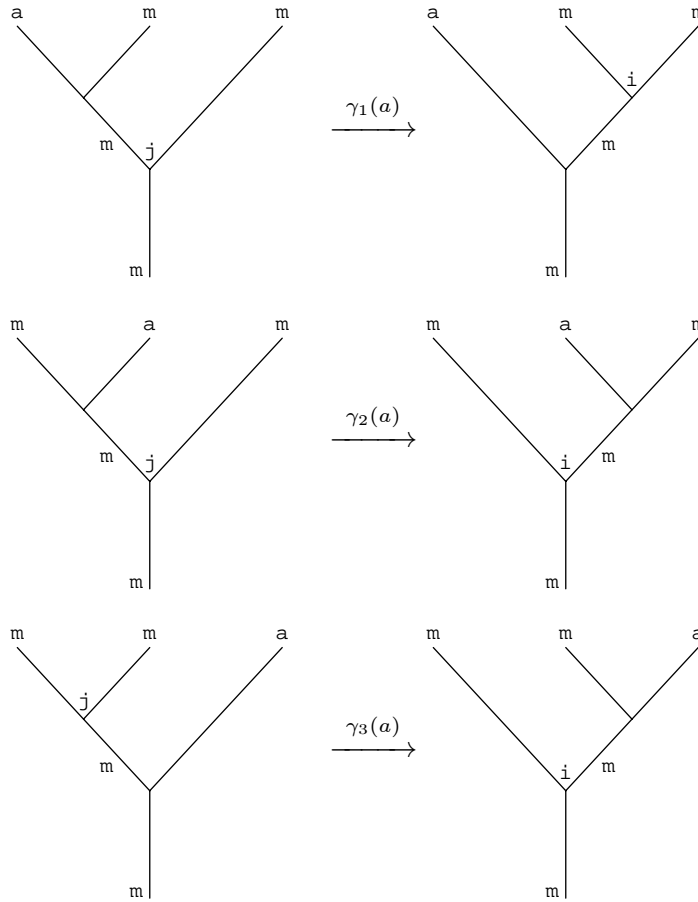


3.1.3 Associativities involving two m 's and one group element. Such a product has both group summands and m summands in it. We will use β 's to denote the associativity on the group summands:

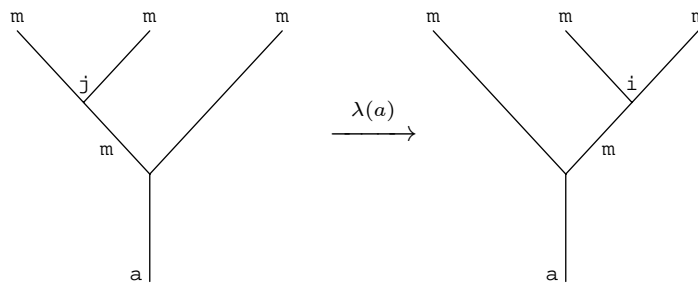


while γ 's will denote the the associativity on the m summands. These will take values in $k \times k$

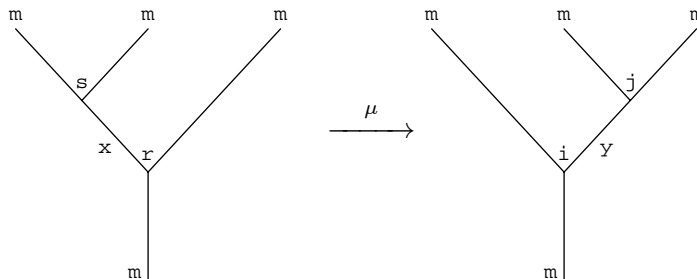
matrices (rows indexed by $i = 1..k$, columns indexed by $j = 1..k$):



3.1.4 Associativities for a threefold product of m 's. Such a product has both group summands and m summands. We will use λ to denote associativity on the group summands. The λ 's will be $k \times k$ matrices:



Finally, μ stands for associativity on the m summands; μ will be a $(k^2 + |G|) \times (k^2 + |G|)$ matrix: on the left, there are $|G|$ basis elements as x runs over G , and k^2 indexed by $r, s = 1..k$ when $x = m$. Similarly on the right:



3.2 Examples and results for small k

In this section we would like to present, for certain groups G and small values of k , the complete classification of monoidal categories with fusion rule (G, k) by giving explicit associativity matrices. The purpose is to make numerical data conveniently available in the small cases and to illustrate the construction given in 3.4.18. The matrix construction is best explained using a permutation π which acts on the nonidentity elements of the group; this satisfies some characterizing identities which are set out in 4.2 but are not important for the present purpose.

3.2.1 Example 1. $k = 1, G = \mathbb{Z}/2\mathbb{Z} = \{\epsilon, g\}$.

Here there is only one nonidentity element in G so of course π is the trivial permutation.

In fact, there are three distinct monoidal structures possible for this fusion rule, classified by a choice of ξ with $\xi^3 = 1$ (of course in characteristic 3 these collapse to a single solution).

Let χ be the nontrivial character of G , that is, $\chi(\epsilon) = 1, \chi(g) = -1$.

Let a, b, c represent arbitrary elements of G . With a good choice of basis, the associativities are as follows:

$$\begin{aligned} \alpha(a, b, c) &\equiv (1) \\ \alpha_1(a, b) = \alpha_2(a, b) = \alpha_3(a, b) &\equiv (1) \\ \beta_1(a, b) = \beta_2(a, b) = \beta_3(a, b) &\equiv (1) \\ \gamma_1(a) = \gamma_2(a) = \gamma_3(a) &= (\chi(a)) \\ \lambda(a) &= (\xi\chi(a)) \end{aligned}$$

and finally, μ :

$$\begin{array}{c} x = \epsilon \quad x = g \quad x = m \\ y = \epsilon \\ y = g \\ y = m \end{array} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2\xi} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2\xi} \\ 1 & -1 & 0 \end{pmatrix}$$

Note: the construction in 3.4.18 corresponds to $\xi = 1$, which is also the structure of the category of representations of the group S_3 , in characteristic prime to 6.

3.2.2 Example 2. $k = 2, G = \mathbb{Z}/3\mathbb{Z} = \{\epsilon, g, g^2\}$.

In this case take π to be the identity permutation on $\{g, g^2\}$.

Let χ_1 and χ_2 be the two nontrivial characters of G .

There are two distinct monoidal structures for this fusion rule, corresponding to a choice of $\xi = \pm 1$, and with a good choice of bases the associativity data is as follows:

$$\begin{aligned}
\alpha(a, b, c) &\equiv (1) \\
\alpha_1(a, b) = \alpha_2(a, b) = \alpha_3(a, b) &\equiv (1) \\
\beta_1(a, b) = \beta_2(a, b) = \beta_3(a, b) &\equiv (1) \\
\gamma_1(a) = \gamma_2(a^{-1}) = \gamma_3(a) &= \begin{pmatrix} \chi_1(a) & 0 \\ 0 & \chi_2(a) \end{pmatrix} \\
\lambda(a) &= \begin{pmatrix} \xi\chi_1(a) & 0 \\ 0 & \xi\chi_2(a) \end{pmatrix}
\end{aligned}$$

and μ :

$$(i, j) = \begin{pmatrix} y = \epsilon \\ g \\ g^2 \\ (1, 1) \\ (1, 2) \\ (2, 1) \\ (2, 2) \end{pmatrix} \begin{pmatrix} x = \epsilon & g & g^2 & (r, s) = (1, 1) & (1, 2) & (2, 1) & (2, 2) \\ \xi/3 & \xi/3 & \xi/3 & 0 & \xi/3 & 1/3 & 0 \\ \xi/3 & \xi/3 & \xi/3 & 0 & (\xi/3)\chi_1(g^2) & (1/3)\chi_2(g^2) & 0 \\ \xi/3 & \xi/3 & \xi/3 & 0 & (\xi/3)\chi_1(g) & (1/3)\chi_2(g) & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \xi \\ 1 & \chi_1(g^2) & \chi_1(g) & 0 & 0 & 0 & 0 \\ \xi & \xi\chi_2(g^2) & \xi\chi_2(g) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Note: The construction in 3.4.18 corresponds to $\xi = +1$, and this is also the structure in the category of representations of the group A_4 in characteristic prime to 12.

3.2.3 Example 3. $k = 3, G = \mathbb{Z}/4\mathbb{Z} = \{\epsilon, g, g^2, g^3\}$.

The data for this example is lengthy, but this is the smallest available example where π is a nontrivial permutation, and is really the best illustration of the construction in 3.4.18. Take π to be the 3-cycle $(g \ g^2 \ g^3)$.

Let χ_1, χ_2 , and χ_3 be the nontrivial characters of G , with $\chi_2(g^2) = 1$.

There is a unique monoidal structure for this fusion rule, and with a good choice of bases the associativity data is as follows:

$$\begin{aligned}
\alpha(a, b, c) &\equiv (1) \\
\alpha_1(a, b) = \alpha_2(a, b) = \alpha_3(a, b) &\equiv (1) \\
\beta_1(a, b) = \beta_2(a, b) = \beta_3(a, b) &\equiv (1) \\
\gamma_1(a) &= \begin{pmatrix} \chi_1(a) & 0 & 0 \\ 0 & \chi_2(a) & 0 \\ 0 & 0 & \chi_3(a) \end{pmatrix} \\
\lambda(\epsilon) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\
\gamma_2(a) &= \lambda(\epsilon)^{-1}\gamma_1(a^{-1})\lambda(\epsilon) \\
\gamma_3(a) &= \lambda(\epsilon)^{-1}\gamma_2(a^{-1})\lambda(\epsilon) \\
\lambda(a) &= \lambda(\epsilon)\gamma_1(a)
\end{aligned}$$

and the large associator μ is given in four submatrices: the upper left “ M submatrix” corre-

sponding to $x, y \in G$:

$$y = \begin{matrix} \epsilon \\ g \\ g^2 \\ g^3 \end{matrix} \begin{pmatrix} x = \epsilon & g & g^2 & g^3 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

the lower left “ C submatrix”, corresponding to $x \in G, y = m$:

$$(i, j) = \begin{matrix} (1, 1) \\ (1, 2) \\ (1, 3) \\ \\ (2, 1) \\ (2, 2) \\ (2, 3) \\ \\ (3, 1) \\ (3, 2) \\ (3, 3) \end{matrix} \begin{pmatrix} x = \epsilon & g & g^2 & g^3 \\ 0 & 0 & 0 & 0 \\ 1 & \chi_1(g^3) & \chi_1(g^2) & \chi_1(g) \\ 0 & 0 & 0 & 0 \\ \\ 1 & \chi_2(g^3) & \chi_2(g^2) & \chi_2(g) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & \chi_3(g^3) & \chi_3(g^2) & \chi_3(g) \end{pmatrix}$$

the upper right “ R submatrix”, corresponding to $x = m, y \in G$:

$$(r, s) = \begin{matrix} (1, 1) & (1, 2) & (1, 3) & & (2, 1) & (2, 2) & (2, 3) & & (3, 1) & (3, 2) & (3, 3) \\ y = \epsilon & \begin{pmatrix} 0 & 0 & 1/4 & & 0 & 1/4 & 0 & & 1/4 & 0 & 0 \\ g & \begin{pmatrix} 0 & 0 & \frac{1}{4}\chi_3(g^3) & & 0 & \frac{1}{4}\chi_1(g^3) & 0 & & \frac{1}{4}\chi_2(g^3) & 0 & 0 \\ g^2 & \begin{pmatrix} 0 & 0 & \frac{1}{4}\chi_3(g^2) & & 0 & \frac{1}{4}\chi_1(g^2) & 0 & & \frac{1}{4}\chi_2(g^2) & 0 & 0 \\ g^3 & \begin{pmatrix} 0 & 0 & \frac{1}{4}\chi_3(g) & & 0 & \frac{1}{4}\chi_1(g) & 0 & & \frac{1}{4}\chi_2(g) & 0 & 0 \end{pmatrix} \end{pmatrix} \end{pmatrix} \end{matrix}$$

and the lower right “ N submatrix” corresponding to $x = y = m$, with columns indexed by (r, s) and rows indexed by (i, j) in the same (lexicographic) order they appear in the previous two submatrices:

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

This example illustrates the most important structural features of the solutions in the maximal group case, ie, in the setting of theorem 1.2: α and β associativities are trivial; the γ 's are k -dimensional representations of G built out of the nontrivial characters of G ; the shape of the $\lambda(\epsilon)$ matrix comes from the permutation π .

Moreover, the large associator μ is predictably organized. The M submatrix is constant. The C submatrix has one nonzero row in each block (ie, one nonzero row for each $i = 1, 2, \dots, k$), and the columns are simply related by characters of G . The R submatrix is organized much like C .

Finally, if we identify G with its dual group of characters, π can be viewed as acting on χ_1, χ_2, χ_3 as the 3-cycle $(\chi_1 \chi_2 \chi_3)$. This is the key to understanding the N submatrix: a nonzero entry occurs in row (i, j) , column (r, s) if and only if $\chi_r \chi_s = \chi_i$ and $\pi^{-1}(\chi_i) \pi^{-1}(\chi_j) = \pi^{-1}(\chi_r)$.

Elaborating these observations and turning them into theorems will be the work of the next two sections.

3.3. Pentagon equations and proof of Theorem 1.3.5

3.3.1. Proof of Theorem 1.3.5, sufficiency. For each finite field F_{p^α} , we construct a nonabelian group whose category of representations is a near-group category in which the group of invertibles is isomorphic to the multiplicative group of the field.

Write $F_{p^\alpha}^+$ for the additive group of the field with p^α elements, and $F_{p^\alpha}^*$ for the multiplicative group. Let \mathcal{G} be the semidirect product $F_{p^\alpha}^+ \rtimes F_{p^\alpha}^*$ with the obvious action.

It's easy to verify:

1. $[\mathcal{G}, \mathcal{G}] = F_{p^\alpha}^+$
2. G has one conjugacy class containing the identity, one conjugacy class consisting of the nonidentity elements in $F_{p^\alpha}^+$, and $(p^\alpha - 2)$ classes each of order p^α .

It follows that in the semisimple setting, \mathcal{G} has $(p^\alpha - 1)$ linear representations comprising a cyclic group $\mathbb{Z}_{p^\alpha - 1}$, together with a single, noninvertible, $(p^\alpha - 1)$ -dimensional representation m . By dimension, $m \otimes m$ contains $(p^\alpha - 2)$ copies of m , so the category of representations of \mathcal{G} has near-group fusion rule $(\mathbb{Z}_{p^\alpha - 1}, p^\alpha - 2)$, and the “if” of Theorem 1.3.5 follows. \square

Remark. The group \mathcal{G} is none other than the affine group of the field F_{p^α} . The presentation as a semidirect product is just convenient for counting its representations.

We will later (3.4.18) show explicitly how to build associativity matrices that solve the pentagon equations for these fusion rules. That point of view emerges from the analysis of the pentagon equations we carry out in this and the following section. Our goal is to prove the following intermediate theorem:

3.3.2. Intermediate Theorem. *If the near-group fusion rule (G, k) supports a monoidal structure, and $|G| = k + 1$, then there is a permutation π on the nonidentity elements of G with the following three properties:*

- i) $\pi^3 = id$
- ii) $\pi(x)^{-1} = \pi^{-1}(x^{-1})$
- iii) $\pi(st) = \pi(t)\pi[\pi(s)^{-1}\pi(t^{-1})]$ (for all $s \neq t^{-1}$)

Once we have established the intermediate theorem, we analyze (3.5) which groups G support the structure of such a permutation π , completing the “only if” portion of Theorem 1.3.5. It is interesting to note that the factorization property (iii) on the permutation π is similar to the property studied by [KR] (particularly, their Proposition 2) where they produce solutions to the pentagon equations from “symmetrically factorizable groups.”

Pentagon equations. Assume we have a near-group category with fusion rule (G, k) .

Equations (1)-(11) of [TY] hold verbatim in this setting; consequently after fixing bases for all hom sets except $\text{hom}(m, mm)$ we may assume:

- $\alpha \equiv \alpha_1 \equiv \alpha_3 \equiv 1$
- $\beta_1 \equiv 1$
- $\beta_2 \equiv \alpha_2$ are symmetric and bimultiplicative

$$\beta_3(a, b) = \beta_3(a, \epsilon)$$

Since β_3 is independent of the second variable, we will abbreviate $\beta_3(a, b)$ to simply $\beta_3(a)$.

We proceed by examining remaining pentagon equations and looking for a good choice of basis for $\text{hom}(m, mm)$. In what follows we will refer to “the pentagon $abcd/x$ ”, meaning the content of the pentagon equation for the x summands in the product $a \otimes b \otimes c \otimes d$.

3.3.3 Proposition. $\gamma_1, \gamma_2,$ and γ_3 are representations of G .

Proof: For $a, b \in G$, this is precisely the content of the pentagons $mmab/m$, $abmm/m$, and $mabm/m$, respectively:

$$\gamma_3(b)\gamma_3(a) = \gamma_3(ab) \quad (14)$$

$$\gamma_1(b)\gamma_1(a) = \gamma_1(ab) \quad (15)$$

$$\gamma_2(b)\gamma_2(a) = \gamma_2(ab) \quad (16)$$

Pentagons $ammb/m$, $mamb/m$, and $ambm/m$ are commutator relationships among the γ representations:

$$\gamma_3(b)\alpha_2(a, b)\gamma_1(a) = \gamma_1(a)\gamma_3(b) \quad (17)$$

$$\alpha_2(a, b)\gamma_3(b)\gamma_2(a) = \gamma_2(a)\gamma_3(b) \quad (18)$$

$$\gamma_2(b)\gamma_1(a)\alpha_2(a, b) = \gamma_1(a)\gamma_2(b) \quad (19)$$

3.3.4 Proposition. $\alpha_2(a, b)$ is an r -th root of unity where $r \mid \gcd(k, |G|)$.

Proof: We choose basis of $\text{hom}(m, mm)$ to split the representation γ_1 into k linear summands, diagonalizing all γ_1 matrices. Now, equation (19) says

$$\gamma_2(b)^{-1}\gamma_1(a)\gamma_2(b) = \alpha_2(a, b)\gamma_1(a)$$

The right hand side is of course diagonal; the left hand side is therefore diagonal and has the same eigenvalues as $\gamma_1(a)$. Multiplication by $\alpha_2(a, b)$ simply permutes those eigenvalues.

Since α_2 is multiplicative in each factor we know $\alpha_2(a, b)$ is an r -th root of unity for some r which divides $|G|$. But by the above observation the k eigenvalues of $\gamma_1(a)$ break up into n orbits each of size r ; we obtain $k = nr$ and so r divides k as well. \square

3.3.5 Proposition. The representations $\gamma_1, \gamma_2^{-1},$ and γ_3 are all conjugate, and $\lambda(\epsilon)$ is an intertwiner carrying γ_3 to γ_1 to γ_2^{-1} back to γ_3 .

Proof: The pentagons for $mmmg/hg$, $gmmm/hg$, $mmgm/h$, and $mgmm/h$ give the following equations respectively:

$$\lambda(hg) = \gamma_3(g)\lambda(h) \quad (20)$$

$$\lambda(hg) = \lambda(h)\gamma_1(g) \quad (21)$$

$$\gamma_2(g)\lambda(h)\gamma_3(g) = \lambda(h)\beta_2(g, h) \quad (22)$$

$$\gamma_1(g)\lambda(h)\gamma_2(g) = \lambda(h)\beta_2(g, h) \quad (23)$$

By (20) with $h = \epsilon$, for any g we have $\lambda(g) = \gamma_3(g)\lambda(\epsilon)$.

Now substitute into (21) with $h = \epsilon$ again to get $\gamma_1(g) = \lambda(\epsilon)^{-1}\gamma_3(g)\lambda(\epsilon)$, so $\lambda(\epsilon)$ carries γ_3 to γ_1 . Take $h = \epsilon$ in the remaining equations to complete the remaining claims. \square

Notation for the associator μ .

Recall from 3.1 that μ is the associator for the threefold product of m 's, on its m summands. We think of it concretely as a matrix with respect to the standard bases indicated by the trees in 3.1. On the left, there are $|G|$ basis elements indexed by the elements of G , and k^2 elements indexed by pairs (r, s) with $1 \leq r, s \leq k$. So think of the columns of μ as labeled either by a group element g or a pair of indices (r, s) .

The parametrization on the right is similar so μ also has $|G|$ rows labeled by group elements and k^2 rows labeled by pairs of indices (i, j) .

If $g, h \in G$, and $1 \leq i, j, r, s \leq k$, entries in μ might be described as $\mu[g, h]$, $\mu[g; (r, s)]$, $\mu[(i, j); g]$ or $\mu[(i, j); (r, s)]$. It will be useful to break up μ into submatrices M , R , C , and N as follows:

$$\begin{aligned} M_{|G| \times |G|} &:= (\mu[g, h])_{g, h} \\ R_{|G| \times k^2} &:= (\mu[g; (r, s)])_{g, (r, s)} \\ C_{k^2 \times |G|} &:= (\mu[(i, j); g])_{(i, j), g} \\ N_{k^2 \times k^2} &:= (\mu[(i, j); (r, s)])_{(i, j), (r, s)} \end{aligned}$$

Think of μ assembled from these pieces as

$$\mu = \begin{pmatrix} M & R \\ C & N \end{pmatrix}$$

It will also be convenient to talk about isolated rows from R and columns from C , so define

$$\begin{aligned} r_g &= \text{the } g\text{th row of } R \\ \text{and } c_g &= \text{the } g\text{th column of } C \end{aligned}$$

Remaining pentagons for products with three m 's.

The pentagons mmm/m , $mmgm/m$, $mgmm/m$, and $gmmm/m$ are information about symmetries inside of the big associator μ . Each one of the four pentagons can be split into four statements, about the M , R , C , and N parts of μ . The next 16 equations are to hold for all a, b , and g in G .

Pentagon mmm/m :

$$\mu[a, b]\alpha_2(b, g) = \mu[g^{-1}a, b]\alpha_1(g^{-1}a, g)\beta_3(g) \quad (24M)$$

$$r_a = \beta_3(g)r_{g^{-1}a}(\gamma_3(g)^{-1} \otimes \text{ID}_k) \quad (24R)$$

$$\alpha_2(a, g)c_a = (\gamma_3(g) \otimes \gamma_3(g))c_a \quad (24C)$$

$$(\gamma_3(g) \otimes \gamma_3(g))N = N(\gamma_3(g) \otimes \text{ID}_k) \quad (24N)$$

Pentagon $mmgm/m$:

$$\mu[a, b]\beta_2(g, a)\beta_3(g) = \mu[a, bg^{-1}] \quad (25M)$$

$$r_a(\gamma_2(g) \otimes \gamma_3(g)^{-1}) = \beta_2(g, a)r_a \quad (25R)$$

$$c_{g^{-1}a} = \beta_3(g)(\text{ID}_k \otimes \gamma_2(g))c_a \quad (25C)$$

$$(\text{ID}_k \otimes \gamma_2(g))N = N(\gamma_2(g) \otimes \gamma_3(g)^{-1}) \quad (25N)$$

Pentagon $mgmm/m$:

$$\mu[a, b]\beta_2(g, b) = \mu[g^{-1}a, b] \quad (26M)$$

$$r_{g^{-1}a} = r_a (\text{ID}_k \otimes \gamma_2(g)) \quad (26R)$$

$$(\gamma_2(g)^{-1} \otimes \gamma_1(g)) c_a = \beta_2(g, a) c_a \quad (26C)$$

$$(\gamma_2(g) \otimes \gamma_1(g)^{-1}) N = N (\text{ID}_k \otimes \gamma_2(g)) \quad (26N)$$

Pentagon $gmmm/m$:

$$\mu[a, g^{-1}b] = \mu[a, b]\alpha_2(g, b) \quad (27M)$$

$$r_a (\gamma_1(g) \otimes \gamma_1(g)) = \alpha_2(g, a) r_a \quad (27R)$$

$$c_{g^{-1}a} = (\gamma_1(g) \otimes \text{ID}_k) c_a \quad (27C)$$

$$N (\gamma_1(g) \otimes \gamma_1(g)) = (\gamma_1(g) \otimes \text{ID}_k) N \quad (27N)$$

3.3.6 Lemma. For all $g, h \in G$, $\mu[g, h] = \mu[\epsilon, \epsilon]\alpha_2(h, h)^{-1}$.

Proof: Take $a = g$ and $b = \epsilon$ in (26M) to get $\mu[g, \epsilon] = \mu[\epsilon, \epsilon]$ for all $g \in G$. By (27M), $\mu[g, h^{-1}h] = \mu[g, \epsilon]\alpha_2(h, h)$; the claim follows. \square

3.3.7 Proof of order-control theorem 1.3.4. By 3.3.6, the $1 \times |G|$ row vector $m_a = (\mu(a, b))_b$ is actually independent of a so we will write \vec{m} for this common value.

Equation (24R) implies that $r_g = \beta_3(g)r_\epsilon (\gamma_3(g)^{-1} \otimes \text{ID}_k)$ for all $g \in G$.

Thus the first $|G|$ rows of μ look like

$$\begin{pmatrix} \vec{m} & r_\epsilon \\ \vec{m} & \beta_3(g_2)r_\epsilon (\gamma_3(g_2)^{-1} \otimes \text{ID}_k) \\ \vec{m} & \beta_3(g_3)r_\epsilon (\gamma_3(g_3)^{-1} \otimes \text{ID}_k) \\ \vdots & \vdots \\ \vec{m} & \beta_3(g_N)r_\epsilon (\gamma_3(g_N)^{-1} \otimes \text{ID}_k) \end{pmatrix}_{|G| \times (|G| + k^2)}$$

Since μ is invertible these are linearly independent. If we write $r_\epsilon = \sum_i u_i \otimes v_i$, it follows that the $|G| \times (k + 1)$ matrix

$$\begin{pmatrix} 1 & \sum_i u_i \\ 1 & \sum_i \beta_3(g_1)u_i \gamma_3(g_1)^{-1} \\ \vdots & \vdots \\ 1 & \sum_i \beta_3(g_N)u_i \gamma_3(g_N)^{-1} u_i \end{pmatrix}$$

has linearly independent rows; hence $|G| \leq k + 1$. \square

3.3.8 Proposition. If $|G| = k + 1$ then $\beta_3(h) = \alpha_2(h, h)$ for all $h \in G$.

Proof: Similar to lemma 3.3.6, equations (24M) and (25M) imply that

$$\mu[g, h] = \mu[\epsilon, \epsilon]\beta_3(g)\beta_3(h)^{-1}\beta_2(h, g)^{-1}$$

for all $g, h \in G$. Equating this with the expression from lemma 3.3.6, we find

$$\mu[\epsilon, \epsilon]\beta_3(g)\beta_3(h)\beta_2(h, g)^{-1} = \mu[\epsilon, \epsilon]\alpha_2(h, h)^{-1}$$

Implicit in the proof of the order control theorem, if $|G| = k + 1$ then $\mu[\epsilon, \epsilon]$ cannot be zero (this would violate linear independence). So we can cancel and rearrange to get

$$\alpha_2(h, hg^{-1}) = \beta_3(h)\beta_3(g)^{-1}$$

(we have also used that $\alpha_2 \equiv \beta_2$ and α_2 is bimultiplicative.) Now, let $g = \epsilon$ in the above. \square

3.4. Further reduction of pentagons when $|G| = k + 1$

We proceed in the maximal-group case; throughout this section, G is a group of order $k + 1$. The results of the previous section are summarized for this special case in the following

3.4.1 Proposition. *In a near-group category with fusion rule (G, k) where $|G| = k + 1$, there exists a choice of bases such that*

- i) $\alpha, \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ are all identically equal to 1.
- ii) γ_1, γ_2^{-1} and γ_3 are conjugate representations of G in diagonal matrices.
- iii) $\mu[a, b]$ is constant (independent of both a and b).
- iv) If we define $\chi_i(g) = \gamma_1(g)_{i,i}$, for $i = 1 \dots k$, then the χ_i are precisely the k nontrivial characters of G .

Proof: All of (i) was proven in the previous section. For $\beta_2, \alpha_2, \beta_3$ vanishing use 4.6 and 4.8.

For (ii), we have already established that γ_1, γ_2^{-1} , and γ_3 are conjugate representations; it remains to show that all three can be simultaneously be diagonalized. Define θ on $G \times G \times G$ by

$$\theta(g, h, k) = \gamma_1(g)\gamma_2(h)\gamma_3(k)$$

Equations (17) through (19) and α_2 vanishing imply that θ is a homomorphism; we can therefore choose basis of $\text{hom}(m, m \otimes m)$ so that θ splits as linear representations. Then of course $\gamma_1(g) = \theta(g, \epsilon, \epsilon)$ is diagonal for all g ; similarly γ_2 and γ_3 .

Claim (iii) follows from 4.6 and $\alpha_2 \equiv 1$

Claim (iv) follows from linear independence in the proof of theorem 1.3.4. \square

3.4.2 Corollary. *With respect to the basis given in 3.4.1, there is a permutation π of order 3 in S_k and constants $\xi(j)$ such that*

$$\lambda(\epsilon) = (\xi(j)\delta_{i,\pi(j)})_{i,j}$$

Proof: Follows from 3.3.5 and 3.4.1(iv). \square

Remark. To make this π an invariant of the category (so it doesn't depend on an ordered basis of $\text{hom}(m, mm)$), we more correctly think of π as a permutation on the set of nontrivial characters of G .

3.4.3 Notation. By the numbering indicated in 3.4.1(iv) we can think of an index $i = 1 \dots k$ as corresponding to one of the k nontrivial characters of G . If we let χ_ϵ stand for the trivial character of G then the set $\{\epsilon, 1, 2, \dots, k\}$ becomes a group under $*$ where we define

$$r * s = i \iff \chi_r \chi_s = \chi_i$$

By the definition of the χ 's, there is an equivalent description using entries in γ_1 matrices: For $r, s \in \{1, 2, \dots, k\}$,

$$\begin{aligned} r * s = i &\iff \gamma_1(g)_r \gamma_1(g)_s = \gamma_1(g)_i \quad \forall g \in G, i \in \{1, 2, \dots, k\} \\ r * s = \epsilon &\iff \gamma_1(g)_r \gamma_1(g)_s = 1 \quad \forall g \in G \end{aligned}$$

If r is an index then r^{-1} will denote the inverse with respect to this $*$ operation.

Of course the group we obtain this way is abstractly isomorphic to G itself and if we choose an isomorphism then we can view the permutation π from 3.4.2 as acting on the nonidentity elements of G .

Precisely the same characters appear in the representation γ_3 although their order of appearance on the diagonal is permuted by the π of lemma 3.4.2. We introduce an analogous operation \circ on $\{\epsilon, 1, 2, \dots, k\}$ by

$$\begin{aligned} r \circ s = i &\iff \gamma_3(g)_r \gamma_3(g)_s = \gamma_3(g)_i \quad \forall g \in G, i \in \{1, 2, \dots, k\} \\ r \circ s = \epsilon &\iff \gamma_3(g)_r \gamma_3(g)_s = 1 \quad \forall g \in G \end{aligned}$$

The inverse of r with respect to \circ will be denoted $r^{\circ-1}$. There is a straightforward translation between the $*$ and \circ operations via π : If $r \circ s \neq \epsilon$, then

$$\begin{aligned} r \circ s &= \pi [\pi^{-1}(r) * \pi^{-1}(s)] \\ \text{and } r^{\circ-1} &= \pi [\pi^{-1}(r)^{-1}] \end{aligned}$$

The \circ operation is therefore not strictly necessary but it eliminates the frequent awkward expressions on the righthand side of the above equations, considerably neatening statements such as the following:

3.4.4 Proposition (R and C structure). *For any g in G ,*

- i) $r_g[(r, s)] = 0 \iff r * s = \epsilon$
- ii) $c_g[(i, j)] = 0 \iff i \circ j = \epsilon$

Proof: For (i), first suppose $r * s = \epsilon$. Then by (27N), $N[(i, j); (r, s)]$ must be zero for all (i, j) . Linear independence of the columns of μ implies that $r_g[(r, s)] \neq 0$ for some $g \in G$, but (24R) says that for any $g, h \in G$, $r_h[(r, s)]$ and $r_g[(r, s)]$ are related via multiplication by a unit. So in fact $r_g[(r, s)] \neq 0$ for all $g \in G$.

Conversely, suppose $r_g[(r, s)] \neq 0$. Then by (27R), $r_g[(r, s)] = \gamma_1(g)_r \gamma_1(g)_s r_g[(r, s)]$ for all $g \in G$. Since $r_g[(r, s)]$ can be cancelled, we see that $\gamma_1(g)_r \gamma_1(g)_s = 1$ for all $g \in G$, which means by definition $r * s = \epsilon$.

Proof of (ii) is similar, using equations (24N) and (24C) instead of (27N) and (127C). \square

The previous result suggests notational shorthand: since for a given r , $r_g[(r, s)]$ is nonzero only for $s = r^{-1}$ we will abbreviate to $r_g(r)$ to refer to this nonzero entry. Similarly, $c_g(i)$ will be short for $c_g[(i, i^{\circ-1})]$.

3.4.5 Proposition (N structure). $N[(i, j); (r, s)] \neq 0 \iff r * s = i$ and $i \circ j = r$.

Proof: First suppose $N[(i, j); (r, s)] \neq 0$. Then for all $g \in G$, (11N) implies

$$\gamma_3(g)_i \gamma_3(g)_j N[(i, j); (r, s)] = \gamma_3(g)_r N[(i, j); (r, s)]$$

and we can cancel the N entry to obtain $\gamma_3(g)_i \gamma_3(g)_j = \gamma_3(g)_r$ for all g , which is the definition of $i \circ j = r$. Similarly, equation (27N) implies $r * s = i$.

Conversely, suppose $r * s = i$ and $i \circ j = r$. By 3.4.4, $r_g[(r, s)] = 0$ for all $g \in G$, so linear independence of the columns of μ implies that $N[(p, q); (r, s)]$ is nonzero for at least one pair of indices (p, q) . But the first half of this proposition implies that the only possible nonzero entry in this column is $N[(i, j); (r, s)]$. \square

3.4.6 The pentagon $mmmm/g$.

This pentagon gives the following equations for all $a, b, g \in G$, for all indices $1 \leq i, j, r, s \leq k$. They have been reduced using the simplifications available from 3.4.1(i). We write $N[-; (r, s)]$ for the entire (r, s) column of N , and $N[(i, j); -]$ for the (i, j) row.

$$\sum_{c \in G} \mu[a, c] \mu[c, b] + r_a (\lambda(g) \otimes \text{ID}_k) c_b = \delta_{a, b^{-1}g} \quad (28M)$$

$$\sum_{c \in G} \mu[a, c] r_c[(r, s)] + r_a (\lambda(g) \otimes \text{ID}_k) N[-; (r, s)] = 0 \quad (28R)$$

$$\sum_{c \in G} c_c[(i, j)] \mu[c, b] + N[(i, j); -] (\lambda(g) \otimes \text{ID}_k) c_b = 0 \quad (28C)$$

$$\sum_{c \in G} c_c[(i, j)] r_c[(r, s)] + N[(i, j); -] (\lambda(g) \otimes \text{ID}_k) N[-; (r, s)] = \lambda(g)[i, s] \lambda(g)[j, r] \quad (28N)$$

3.4.7 Lemma. For any $g \in G$,

i) $r_g[(r, s)] = \gamma_3(g)_r^{-1} r_\epsilon[(r, s)]$

ii) $c_g[(i, j)] = \gamma_1(g)_i^{-1} c_\epsilon[(i, j)]$

Proof: Immediate from (24R) and (27C)

3.5.8 Proposition. The permutation π from 3.4.2 satisfies $\pi(x^{-1}) * \pi^{-1}(x) = \epsilon$ (for any index x , $1 \leq x \leq k$.)

Proof: In equation (28R) the summation in fact vanishes. To see this, fix a, r , and s . Now, $\mu[a, c]$ is constant by 5.1(iii), and $r_c[(r, s)] = r_\epsilon[(r, s)] \gamma_3(c)_r^{-1}$ by 3.4.7. Therefore,

$$\sum_{c \in G} \mu[a, c] r_c[(r, s)] = \mu[\epsilon, \epsilon] r_\epsilon[(r, s)] \sum_c \gamma_3(c)_r^{-1} = 0 \text{ by orthogonality of characters}$$

So (28R) reduces to $r_a (\lambda(g) \otimes \text{ID}_k) N[-; (r, s)] = 0$ and in particular, for $g = a = \epsilon$,

$$r_\epsilon (\lambda(\epsilon) \otimes \text{ID}_k) N[-; (r, s)] = 0$$

By 3.4.5 this yields no useful information if $r * s = \epsilon$ so assume $r * s \neq \epsilon$. By 3.4.5, there is a single nonzero entry in $N[-; (r, s)]$, namely $N[(i, j); (r, s)]$ where $r * s = i$ and $i \circ j = r$. The lefthand side will not be zero if π manages to “line up” that nonzero entry from N with one of the nonzero entries in r_ϵ . But we know where the nonzero entries in r_ϵ live by 3.4.4. So if (28R) is to be satisfied there must not exist any triple of indices r, s, x with $r * s \neq \epsilon$, $\pi(r * s) * x = \epsilon$, and $(r * s) \circ x = r$.

For any index r , there is an s so that $x^{-1} = \pi(r * s)$. So (28R) says $\pi^{-1}(x^{-1}) \circ x \neq r$ for any index r ; by elimination it must be that $\pi^{-1}(x^{-1}) \circ x = \epsilon$. Now,

$$\begin{aligned} \pi^{-1}(x^{-1}) \circ x &= \epsilon \\ \implies \pi^{-2}(x^{-1}) * \pi^{-1}(x) &= \epsilon \\ \implies \pi(x^{-1}) * \pi^{-1}(x) &= \epsilon \quad (\text{since } \pi^3 = \text{id}) \quad \square \end{aligned}$$

3.4.9 Proposition. The permutation π satisfies $\pi(s * t) = \pi(t) * \pi[\pi(s)^{-1} * \pi(t^{-1})]$ (for all $s \neq t^{-1}$)

Proof: Consider (28N) with $r \neq s^{-1}$, $i = \pi(s)$, and $j = \pi(r)$, so that the summation on the left vanishes but the righthand side is nonzero. By the N structure proposition, the only nonzero entry in column (r, s) of N occurs in row $(r * s, x)$ where $x = (r * s)^{\circ^{-1}} \circ r$. Expressed purely in terms of the $*$ operation,

$$x = \pi[\pi^{-1}(r * s)^{-1} * \pi^{-1}(r)]$$

But for the lefthand side of (28N) to be nonzero, it must be that $i = \pi(r * s) * x$; since we have chosen $i = \pi(s)$, the following relation appears:

$$\pi(s) = \pi(r * s) * \pi[\pi^{-1}(r * s)^{-1} * \pi^{-1}(r)] \quad (\forall r \neq s^{-1})$$

The identity claimed in the proposition follows from a change of variable: set $t = (r * s)$ and rewrite. The change of variable is reversible so the two identities are in fact equivalent. \square

3.4.10 Proof of Intermediate Theorem 3.3.2. The results in 3.4.2, 3.4.8, and 3.4.9 establish Theorem 4.2: If a monoidal structure exists, then we can extract a permutation π satisfying the three indicated properties. \square

In 3.5 we will complete Theorem 1.3.5 by identifying which groups support such a π but the remainder of this section will continue the analysis of the pentagon equations so that we can give an explicit matrix solution to the pentagon equations in 3.4.18.

3.4.11 Identifying primitive data. At this point we have reduced the problem of describing the categorical data to describing the associativities $\lambda(\epsilon)$ and μ . We know the α 's and β 's are trivial and we know that the γ 's contain all the nontrivial characters. All $\lambda(g)$ are determined once we know $\lambda(\epsilon)$ and the γ 's. The $\lambda(\epsilon)$ is described by the permutation π and the function ξ of 5.2; μ is described by M , R , C , and N but M is a constant block; all of C can be generated given the function c_ϵ . Likewise R is described by the function r_ϵ , and N by a function of two indices: $N(r, s)$, denoting the single nonzero entry in column (r, s) of N (where $r * s \neq \epsilon$). Our next step is to give a formula for r_ϵ in terms of c_ϵ thus reducing the problem to specifying three functions ξ , c_ϵ , and N .

3.4.12 Proposition. $r_\epsilon(i) = [|G|\xi(\pi^{-1}(i))c_\epsilon(\pi^{-1}(i))]^{-1}$

Proof: The key is to reformulate (15M) as a small matrix equation which essentially allows us to solve for R in terms of C . For $g \in G$, set $r'_g = (r_g(i))_i$, a $1 \times k$ row vector regarded as r_ϵ with all the zeros squeezed out. Similarly, set $c'_g = (c_g(i))_i^T$, a $k \times 1$ column vector. Define

$$R_0 = \begin{pmatrix} y & r'_\epsilon \\ y & r'_1 \\ \vdots & \vdots \\ y & r'_k \end{pmatrix} \quad C_0 = \begin{pmatrix} y & y & \cdots & y \\ c'_\epsilon & c'_1 & \cdots & c'_k \end{pmatrix} \quad \lambda_0 = \begin{pmatrix} 1 & 0 \\ 0 & \lambda(\epsilon) \end{pmatrix}$$

where $y = \sqrt{|G|\mu[\epsilon, \epsilon]^2}$. The three matrices defined above are $(k+1) \times (k+1)$ and invertible by linear independence of characters. For $g = \epsilon$ it is simple to verify that equation (15M) for all $a, b \in G$ is equivalent to the matrix equation

$$R_0 \lambda_0 C_0 = (\delta_{a, b^{-1}})_{a, b \in G}$$

Write X for the involutive permutation matrix $(\delta_{a, b^{-1}})_{a, b \in G}$ and D_0 for a diagonal matrix with $(c_\epsilon(i)c_\epsilon(i^{-1})|G|)^{-1}$ on the diagonal. Character relations let us calculate

$$C_0^{-1} = C_0^T X D_0$$

and so

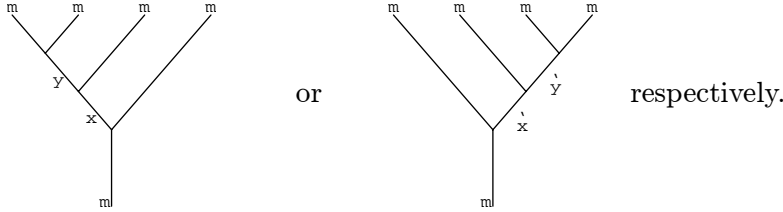
$$R_0 = X C_0^T X D_0 \lambda_0^{-1}$$

Now it is easy to expand the matrix product on the right hand side and obtain the formula claimed. Moreover, examination of the first column on both sides implies $y^2|G|^{-1} = 1$, and we have

3.4.13 Corollary. $\mu[\epsilon, \epsilon] = \pm 1/|G|$

We introduce $\delta := |G|\mu[\epsilon, \epsilon] = \pm 1$ as this will occur frequently in subsequent equations.

3.4.14 The big pentagon: $mmmm/m$. Graphically, the bases for the full left and full right associated product have the form



On the left, for example, there are $k|G|$ basis elements with $x \in G$, $k|G|$ basis elements with $y \in G$, and k^3 with $x = y = m$, for a total of $k^3 + 2k|G|$ elements. Rather than view this pentagon as one large $(k^3 + 2k|G|)$ -dimensional matrix equation, we break it down into several more sensible submatrix equations based on this grouping of basis elements:

$$\begin{array}{c} \hat{x} \in G \\ \hat{y} = m \\ \hat{x} = m \\ \hat{y} \in G \\ \hat{x} = \hat{y} = m \end{array} \begin{pmatrix} \begin{array}{ccc} x \in G & x = m & x = y = m \\ y = m & y \in G & \end{array} \\ \begin{array}{ccc} (29) & (31) & (34) \\ (30) & \text{---} & (33), (34) \\ (35) & (31), (32) & (37) \end{array} \end{pmatrix}$$

The table indicates which submatrix of the pentagon equation corresponds to which of the following constraints. We have used all reductions available to express these in the minimal number of variables: these are essentially functional equations in the functions c_ϵ , ξ , and N , and they are to hold for all indices i, j for which they make sense:

$$c_\epsilon(i) = \delta \xi(i^{-1}) \xi(\pi(i^{-1})) \xi(\pi^{-1}(i)) c_\epsilon(\pi^{-1}(i)) \quad (29)$$

$$\xi(i) c_\epsilon(i) = \delta \xi(\pi(i^{-1})) c_\epsilon(\pi(i^{-1})) \quad (30)$$

$$c_\epsilon(i) = \delta c_\epsilon(\pi(i)^{-1}) \quad (31)$$

$$c_\epsilon(i) = c_\epsilon(j) N(i * j^{-1}, j) N(\pi(j) * \pi(i)^{-1}, \pi(j)^{-1}) \quad (32)$$

$$\xi(i) c_\epsilon(i) = \delta \xi(\pi(i^{-1})) c_\epsilon(\pi(i^{-1})) \quad (33)$$

$$\xi(\pi^{-1}(i) * \pi(j^{-1})) c_\epsilon(\pi^{-1}(i) * \pi(j^{-1})) = \xi(\pi^{-1}(i)) c_\epsilon(\pi^{-1}(i)) N(i, i^{-1} * j) N(i^{-1}, j) \quad (34)$$

$$c_\epsilon(i) N(i, j) = \xi(j) c_\epsilon(i * j) N(\pi(i * j)^{-1}, \pi(j)) \quad (35)$$

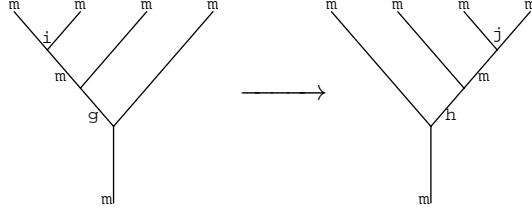
$$\begin{aligned} \xi(\pi^{-1}(i)) N(i, j) c_\epsilon(\pi^{-1}(i)) &= \xi(\pi(\pi^{-1}(j) * \pi(i))) \xi(\pi^{-1}(i * j))^{-1} \\ & \quad N(j, (i * j) c_\epsilon(\pi^{-1}(i * j))) \end{aligned} \quad (36)$$

$$c_\epsilon((i * j)^{-1}) = c_\epsilon(j) \xi(j) N(\pi^{-1}(i), \pi(j)) N(\pi^{-1}(i) * \pi(j), \pi(j)^{-1}) \quad (37)$$

Note: the $y, \hat{y} \in G$ piece of the pentagon is automatically satisfied by the properties of the permutation π , without introducing any new relations. This will be illustrated in 3.4.18 below. In general the process of transcribing the above equations from the abstract pentagon is lengthy but requires no sophistication. We will illustrate the derivation of two of the equations and omit the similar details of the remainder.

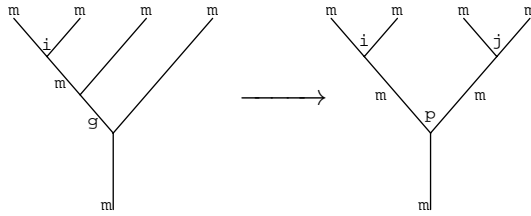
3.4.15 Derivation of equation (29).

As the table indicates, this equation is supposed to come from the following piece of the pentagon:



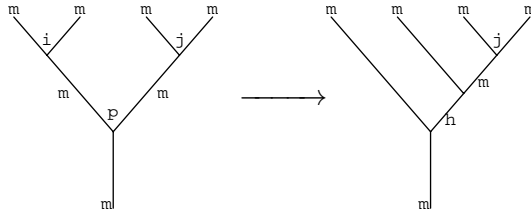
For each $g, h \in G$ we get a $k \times k$ submatrix of coefficients indexed by i and j . Using the reductions available it is not difficult to compute these coefficients.

Following the two-step path in the pentagon, the first step is



$$(m \rightarrow gm) \otimes (g \rightarrow mm) \otimes (m \rightarrow mm)_i \xrightarrow{\alpha} \sum_p c_g[p, j] (m \rightarrow mm)_p \otimes (m \rightarrow mm)_i \otimes (m \rightarrow mm)_j + \text{irrelevant terms}$$

and the second step is

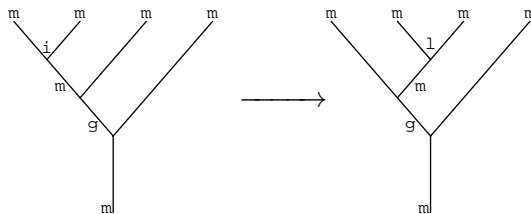


$$(m \rightarrow mm)_p \otimes (m \rightarrow mm)_i \otimes (m \rightarrow mm)_j \xrightarrow{\alpha} r_h[p, i] (m \rightarrow mh) \otimes (h \rightarrow mm) \otimes (m \rightarrow mm)_j + \text{irrelevant terms}$$

Therefore the (j, i) coefficient is $\sum_p c_g[p, j] r_h[p, i]$. By 3.4.4 this sum will be zero unless there is an index $p = j^{\circ-1} = i^{-1}$ which happens iff $j = \pi^{-1}(i)$, in which case the coefficient is $c_g(i^{-1}) r_h(i^{-1})$, and so the submatrix here is

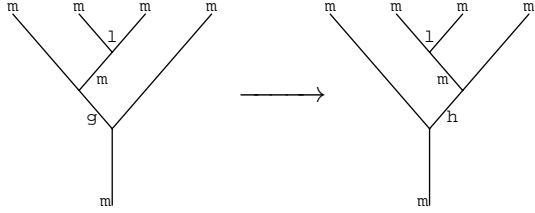
$$\left(c_g(i^{-1}) r_h(i^{-1}) \delta_{j, \pi^{-1}(i)} \right)_{j, i}$$

Now we follow the three-step path in the pentagon; the first step is



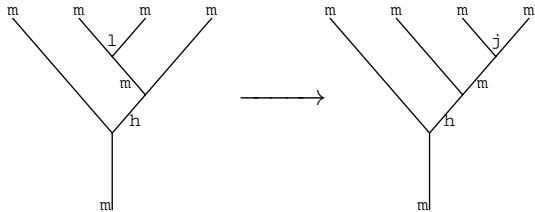
$$(m \rightarrow gm) \otimes (g \rightarrow mm) \otimes (m \rightarrow mm)_i \\ \xrightarrow{\alpha} \sum_l \lambda(g)[l, i] (m \rightarrow gm) \otimes (g \rightarrow mm) \otimes (m \rightarrow mm)_l$$

From here,



$$(m \rightarrow gm) \otimes (g \rightarrow mm) \otimes (m \rightarrow mm)_l \\ \xrightarrow{\alpha} \mu[h, g] (m \rightarrow mh) \otimes (h \rightarrow mm) (m \rightarrow mm)_l + \text{irrelevant terms}$$

Note that $\mu[h, g] = \mu[\epsilon, \epsilon]$, independent of h and g . In the third association,



$$(m \rightarrow mh) \otimes (h \rightarrow mm) (m \rightarrow mm)_l \\ \xrightarrow{\alpha} \lambda(h)[j, l] (m \rightarrow mh) \otimes (h \rightarrow mm) \otimes (m \rightarrow mm)_j + \text{irrelevant terms}$$

so the submatrix from this path is

$$\mu[\epsilon, \epsilon] \lambda(h) \lambda(g) \\ = \mu[\epsilon, \epsilon] \lambda(\epsilon) \gamma_1(h) \lambda(\epsilon) \gamma_1(g) \quad \text{by 3.3.5}$$

and the requirement of the pentagon equation is that

$$\mu[\epsilon, \epsilon] \lambda(\epsilon) \gamma_1(h) \lambda(\epsilon) \gamma_1(g) = \left(c_g(i^{-1}) r_h(i^{-1}) \delta_{j, \pi^{-1}(i)} \right)_{j, i} \quad (29')$$

Claim. (29') for arbitrary g and h follows from the case $g = h = \epsilon$

Proof: The matrix product on the left is

$$\left(\mu[\epsilon, \epsilon] \chi_i(g) \xi(i) \chi_{\pi(i)}(h) \xi(\pi(i)) \delta_{j, \pi^{-1}(i)} \right)_{j, i}$$

So 16' can be written as

$$\mu[\epsilon, \epsilon] \xi(i) \xi(\pi(i)) \chi_i(g) \chi_{\pi(i)}(h) = c_g(i^{-1}) r_h(i^{-1}) \quad \forall i \quad (29'')$$

But $c_g(i^{-1}) = c_\epsilon(i^{-1}) \chi_i(g)$ by (27C). Similarly $r_h(i^{-1}) = r_\epsilon(i^{-1}) \chi_{\pi(i)}(h)$. All terms involving g and h in fact cancel, so the general case reduces to

$$\mu[\epsilon, \epsilon]\xi(i)\xi(\pi(i)) = c_\epsilon(i^{-1})r_\epsilon(i^{-1})$$

as claimed. \square

Now 5.12 replaces the r_ϵ with an equivalent expression in c_ϵ ,

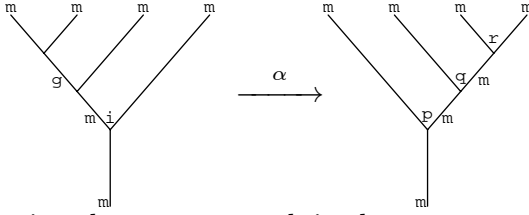
$$\mu[\epsilon, \epsilon]\xi(i)\xi(\pi(i)) = c_\epsilon(i^{-1}) (|G|\xi(\pi^{-1}(i^{-1}))c_\epsilon(\pi^{-1}(i^{-1})))^{-1}$$

Rearrange:

$$c_\epsilon(i^{-1}) = \delta\xi(i)\xi(\pi(i))\xi(\pi^{-1}(i^{-1}))c_\epsilon(\pi^{-1}(i^{-1}))$$

and we have shown that this piece of the pentagon is precisely equation (16) (after a final change of variable $i \mapsto i^{-1}$).

3.4.16 Derivation of equations (31) and (32). Graphically, we're interested in the following basis elements:



Following the two-step path in the pentagon, first

$$\begin{aligned} (m \rightarrow mm)_i \otimes (m \rightarrow gm) \otimes (g \rightarrow mm) \\ \xrightarrow{\alpha} \gamma_1(g)[r, i](m \rightarrow gm) \otimes (g \rightarrow mm) \otimes (m \rightarrow mm)_r + \text{irrelevant terms} \end{aligned}$$

and then

$$\begin{aligned} (m \rightarrow gm) \otimes (g \rightarrow mm) \otimes (g \rightarrow mm)_r \\ \xrightarrow{\alpha} \mu[(p, q); g](m \rightarrow mm)_p \otimes (m \rightarrow mm)_q \otimes (m \rightarrow mm)_r + \text{irrelevant terms} \end{aligned}$$

So the total coefficient from this path is simply

$$\mu[(p, q); g]\gamma_1(g)[r, i]$$

Following the three-step path, first

$$\begin{aligned} (m \rightarrow mm)_i \otimes (m \rightarrow gm) \otimes (g \rightarrow mm) \\ \xrightarrow{\alpha} \sum_{h \in G} \mu[h; g](m \rightarrow mm)_i \otimes (m \rightarrow mh) \otimes (h \rightarrow mm) \\ + \sum_{j, l} \mu[(j, l); g](m \rightarrow mm)_i \otimes (m \rightarrow mm)_j \otimes (m \rightarrow mm)_l \end{aligned}$$

then

$$\begin{aligned} (m \rightarrow mm)_i \otimes (m \rightarrow mh) \otimes (h \rightarrow mm) \\ \xrightarrow{\alpha} \gamma_2(h)[p, i](m \rightarrow mm)_p \otimes (m \rightarrow hm) \otimes (h \rightarrow mm) \end{aligned}$$

and

$$\begin{aligned} (m \rightarrow mm)_p \otimes (m \rightarrow hm) \otimes (h \rightarrow mm) \\ \xrightarrow{\alpha} \mu[(q, r); h](m \rightarrow mm)_p \otimes (m \rightarrow mm)_q \otimes (m \rightarrow mm)_r + \text{irrelevant terms} \end{aligned}$$

while

$$(m \rightarrow mm)_i \otimes (m \rightarrow mm)_j \otimes (m \rightarrow mm)_l \\ \xrightarrow{\alpha} \sum_s \mu[(p, s); (i, j)](m \rightarrow mm)_p \otimes (m \rightarrow mm)_s \otimes (m \rightarrow mm)_l + \text{irrelevant terms}$$

and

$$(m \rightarrow mm)_p \otimes (m \rightarrow mm)_s \otimes (m \rightarrow mm)_l \\ \xrightarrow{\alpha} \mu[(q, r); (s, l)](m \rightarrow mm)_p \otimes (m \rightarrow mm)_q \otimes (m \rightarrow mm)_r + \text{irrelevant terms}$$

So the total coefficient from this path is

$$\sum_{h \in G} \mu[(q, r); h] \gamma_2(h)[p, i] \mu[h; g] \\ + \sum_{j, l, s} \mu[(q, r); (s, l)] \mu[(p, s); (i, j)] \mu[(j, l); g]$$

and the requirement of the pentagon is that

$$\mu[(p, q); g] \gamma_1(g)[r, i] = \sum_{h \in G} \mu[(q, r); h] \gamma_2(h)[p, i] \mu[h; g] \\ + \sum_{j, l, s} \mu[(q, r); (s, l)] \mu[(p, s); (i, j)] \mu[(j, l); g]$$

We will handle this in two cases.

Case I, $i = p$. In this case, the second summation on the righthand side vanishes, by the N structure theorem (because $i * j \neq i = p$). Again, $\mu[g, h] = \mu[\epsilon, \epsilon]$ independent of g and h , so we are left with

$$c_g(i, q) \gamma_1(g)[r, i] = \mu[\epsilon, \epsilon] \sum_h c_h(q, r) \gamma_2(h)[i, i]$$

Now we can use (27C) and (25C) to replace the c_g and c_h terms with expressions in c_ϵ :

$$c_\epsilon(i, q) \gamma_1(g^{-1})[i, i] \gamma_1(g)[r, i] = \mu[\epsilon, \epsilon] \sum_h c_\epsilon(q, r) \gamma_2(h^{-1})[r, r] \gamma_2(h)[i, i]$$

If $r \neq i$ the lefthand side vanishes since γ_1 is diagonalized, and the righthand side vanishes by orthogonality of characters. So we can reduce to

$$c_\epsilon(i, q) = \mu[\epsilon, \epsilon] |G| c_\epsilon(q, i)$$

and both vanish by the C structure theorem unless $q = i^{o-1}$, so the only requirement here is

$$c_\epsilon(i) = \delta c_\epsilon(i^{o-1}) \text{ for all } i$$

which is precisely equation (31).

Case II, $i \neq p$. In this case the first summation vanishes because γ_2 is diagonalized, and we are left with

$$c_g(p, q) \gamma_1(g)[r, i] = \sum_{j, l, s} \mu[(q, r); (s, l)] \mu[(p, s); (i, j)] \mu[(j, l); g] \quad (38)$$

Note that for many choices of indices p, q, i, r the equation will be satisfied without introducing any new constraints since both sides vanish. We need to identify precisely when this happens. Fix indices p, q, i, r .

By the C -structure theorem and diagonalization of γ_1 , the lefthand side is nonzero iff

$$p = q^{\circ-1} \text{ and } r = i \quad (39)$$

By the C - and N -structure theorems, the righthand side is nonzero iff there exist indices s, l satisfying

$$q \circ r = s \quad (40i)$$

$$s * j^{\circ-1} = q \quad (41ii)$$

$$p \circ s = i \quad (42iii)$$

$$i * j = p \quad (43iv)$$

Claim: The conditions of (39) are equivalent to the conditions of (40).

Proof: Assume (39), guaranteeing the lefthand side is nonzero. In order to satisfy (40iii) and (40iv) we must take

$$j = p * i^{-1} \text{ and } s = p^{\circ-1} \circ i$$

This s and j clearly satisfy (40i); with a little more work we verify that (40ii) also holds:

$$\begin{aligned} s * j^{\circ-1} &= (p^{\circ-1} \circ i) * (p * i^{-1})^{\circ-1} \\ &= \pi(\pi(p^{-1}) * \pi^{-1}(i)) * \pi(p * i^{-1})^{-1} \\ &= \pi(p)^{-1} \quad \text{using 5.9} \\ &= p^{\circ-1} = q \end{aligned}$$

as required. Conversely, suppose the conditions of (40) are satisfied. Then we simply repeat the above calculation to show that $q = p^{\circ-1}$. It follows from (40i) and (40iii) that $i = r$, so both conditions of (39) are satisfied. \square

Therefore in considering the requirements of (38) we only need the case $p = q^{\circ-1}$ and $r = i$, reducing to

$$c_g(p)\gamma_1(g)[i, i] = N[p^{\circ-1} \circ i, (p^{\circ-1} \circ i)^{-1} * p^{\circ-1}]N[i, i^{-1} * p]c_g(p * i^{-1})$$

Using (27C) and cancelling γ 's, this reduces further to

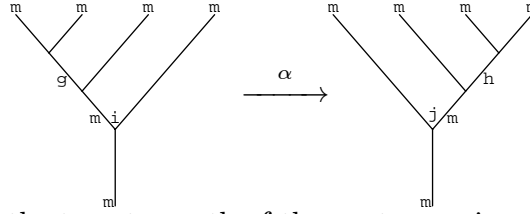
$$c_\epsilon(p) = N[p^{\circ-1} \circ i, (p^{\circ-1} \circ i)^{-1} * p^{\circ-1}]N[i, i^{-1} * p]c_\epsilon(p * i^{-1})$$

which, after a change of variable, is precisely equation (32), and we have completed showing that equations (31) and (32) completely describe the requirements of this piece of the pentagon. \square

Derivation of the remaining equations in the list is very similar to the examples we have worked. The $y, \hat{y} \in G$ equation is a little different; we have claimed it is automatically satisfied by the properties of π already established, and we will now prove that.

3.4.17 The $y, \hat{y} \in G$ piece of the pentagon.

Here we consider the following entries in the pentagon:



It is easy to verify that the two-step path of the pentagon gives zero coefficient for this entry. Walking through the three-step path as we did for previous pieces gives a total coefficient of

$$\sum_{a \in G} \mu[\epsilon, \epsilon]^2 \gamma_2(a)[i, j] + \sum_{p, q, l} \mu[h; (l, q)] \mu[(j, l); (i, p)] \mu[(p, q); g]$$

Now the first sum (over $a \in G$) is always vanishing, so the requirement of the pentagon is that

$$\sum_{p, q, l} r_h(l, q) \mu[(j, l); (i, p)] c_g(p, q) = 0$$

for all i and j . If $i = j$ the $\mu[(j, l); (i, p)]$ is always zero by the N -structure theorem and the sum vanishes. If $i \neq j$, there could be at most one nonzero term; by the N - and C -structure theorems this would occur for

$$\begin{aligned} l &= j^{\circ-1} \circ i \\ p &= i^{-1} * j \\ \text{and } q &= p^{\circ-1} \end{aligned}$$

But then

$$\begin{aligned} l * q &= (j^{\circ-1} \circ i) * (i^{-1} * j)^{\circ-1} \\ &= \pi [\pi(j^{-1}) * \pi^{-1}(i)] * \pi [i^{-1} * j]^{-1} \\ &= \pi(j)^{-1} \quad \text{by 3.4.9} \\ &\neq \epsilon \end{aligned}$$

so by the R -structure theorem $r_h(l, q) = 0$ and in fact every term of the summation is zero without imposing any further conditions. \square

3.4.18 Constructing matrix solutions to the pentagon equations.

Suppose we are given near-group fusion rule (G, k) , $|G| = k + 1$, and we are given a permutation π on $G \setminus \epsilon$ satisfying the three conditions of Theorem 4.2. Guided by the preceding analysis, we give a set of associativity matrices and prove that they satisfy all pentagon equations.

Using the notation established earlier, set

$$\alpha, \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \equiv 1$$

Let χ_1, \dots, χ_k be the nontrivial characters of G , and choose an identification of G with its dual group of characters so that π can be regarded as permuting the characters. For indices i, j, r write $i * j = r$ provided $\chi_i \chi_j = \chi_r$; write $i \circ j = \epsilon$ provided $\chi_i \chi_j = \chi_\epsilon$, the trivial character. Let i^{-1} stand for the inverse of i with respect to this operation.

Write $i \circ j = r$ provided $\pi^{-1}(i) * \pi^{-1}(j) = \pi^{-1}(r)$, and let $i^{\circ-1}$ denote the inverse with respect to this operation. As indicated before, $i^{\circ-1} = \pi(i)^{-1}$.

Now we can make the following definitions:

$$\begin{aligned}\lambda(\epsilon) &= (\delta_{i, \pi(j)})_{i,j} \\ \gamma_1(g) &= \begin{pmatrix} \chi_1(g) & & & \\ & \chi_2(g) & & \\ & & \ddots & \\ & & & \chi_k(g) \end{pmatrix} \\ \gamma_2(g) &= \lambda(\epsilon)^{-1} \gamma_1(g^{-1}) \lambda(\epsilon) \\ \gamma_3(g) &= \lambda(\epsilon)^{-1} \gamma_2(g^{-1}) \lambda(\epsilon) \\ \lambda(g) &= \gamma_3(g) \lambda(\epsilon) \quad \text{for arbitrary } g \in G\end{aligned}$$

Note that with these definitions, all $\gamma_2(g)$ and $\gamma_3(g)$ are diagonal, and

$$\begin{aligned}\gamma_2(g)[i, i] &= \chi_{\pi(i)^{-1}}(g) \\ \text{and } \gamma_3(g)[i, i] &= \chi_{\pi^{-1}(i)}(g)\end{aligned}$$

At this point we have defined all associativities except μ and it clear that pentagon equations (14)-(23) of this paper are satisfied, as well as (1)-(11) of [TY] (together, these account for all four-term products involving two m 's or fewer). The only associativity left to define is μ .

For $g, h \in G$ and $i, j, r, s \in \{1, 2, \dots, k\}$, define

$$\begin{aligned}\mu[g, h] &= |G|^{-1} \\ \mu[(i, j); g] &= \chi_i(g^{-1}) \delta_{i, j \circ^{-1}} \\ \mu[g; (r, s)] &= (|G| \chi_{\pi^{-1}(r)}(g))^{-1} \delta_{r, s^{-1}} \\ \mu[(i, j); (r, s)] &= \delta_{r, i \circ j} \delta_{i, r * s}\end{aligned}$$

Equations (24M-27M) are clearly satisfied by construction.

(27C) is clearly satisfied by construction. For (26C), check: $((\gamma_2(g)^{-1} \otimes \gamma_1(g)) c_g)[(i, j)] = \chi_{\pi(i)}(g) \chi_j(g) c_g(i, j)$, so if $j \neq i \circ^{-1} = \pi(i)^{-1}$ then $c_g(i, j) = 0$ and (26C) is satisfied; if $j = i \circ^{-1}$ then $\chi_{\pi(i)}(g) \chi_j(g) = 1$ and (26C) is still satisfied. Verifying (25C) and (24C) is similar.

(24R) is clearly satisfied by construction.

Check that (25R) is satisfied: for $a, g \in G$,

$$\begin{aligned}r_a(\gamma_2(g) \otimes \gamma_3(g)^{-1}) &= r_a \\ \iff r_\epsilon[r, s] \chi_{\pi(r)^{-1}}(g) \chi_{\pi^{-1}(s)^{-1}}(g) &= r_\epsilon[r, s] \quad \forall r, s\end{aligned}$$

If $r \neq s^{-1}$ then $r_\epsilon(r, s) = 0$, and (25R) is satisfied. If $r = s^{-1}$ then by property (ii) of π , $\pi(r)^{-1} * \pi^{-1}(s)^{-1} = \epsilon$, so $\chi_{\pi(r)^{-1}}(g) \chi_{\pi^{-1}(s)^{-1}}(g) = 1$, and (12R) is satisfied.

Check that (26R) is satisfied: This is trivial for $r \neq s^{-1}$, so assume $r = s^{-1}$. By property (ii) of π , then, $\pi(s) = \pi^{-1}(r)^{-1}$, so for any $a, g \in G$,

$$\begin{aligned}(r_a(\text{ID}_k \otimes \gamma_2(g)))[r, s] &= (|G| \chi_{\pi^{-1}(r)}(a) \mu[(\pi^{-1}(r), s); \epsilon])^{-1} \chi_{\pi(s)^{-1}}(g) \\ &= (|G| \chi_{\pi^{-1}(r)}(a) \chi_{\pi(s)}(g) \mu[(\pi^{-1}(r), s); \epsilon])^{-1} [r, s] \\ &= (|G| \chi_{\pi^{-1}(r)}(g^{-1} a) \mu[(\pi^{-1}(r), s); \epsilon])^{-1} \\ &= r_{g^{-1} a}\end{aligned}$$

so (26R) is satisfied. Checking (27R) is similar to (25R), so details are omitted.

(24N) is satisfied provided

$$\chi_{\pi^{-1}(i)}(g)\chi_{\pi^{-1}(j)}(g)N[(i, j); (r, s)] = \chi_{\pi^{-1}(r)}(g)N[(i, j); (r, s)]$$

for all i, j, r, s . If $i \circ j \neq r$ then both sides are zero, and (24N) is satisfied; if $i \circ j = r$ then $\chi_{\pi^{-1}(i)}\chi_{\pi^{-1}(j)} = \chi_{\pi^{-1}(r)}$ so (24N) is satisfied in that case as well.

(25N) is satisfied provided

$$\chi_{\pi^{-1}(i)}(g)\chi_{\pi^{-1}(j)}(g)N[(i, j); (r, s)] = \chi_{\pi^{-1}(r)}(g)N[(i, j); (r, s)]$$

for all i, j, r, s . If $N[(i, j); (r, s)] = 0$ this is satisfied. If $N[(i, j); (r, s)] \neq 0$ then $r * s = i$ and $i \circ j = r$ so $j = r \circ (r * s)^{\circ-1}$; we use the hypotheses on π to massage this expression:

$$\begin{aligned} j &= r \circ (r * s)^{\circ-1} = \pi(\pi((r * s)^{-1}) * \pi^{-1}(r)) \\ &= \pi(s) * \pi(r * s)^{-1} \end{aligned}$$

therefore

$$\begin{aligned} \pi(j)^{-1} &= \pi(\pi(s) * \pi(r * s)^{-1})^{-1} \\ &= (\pi^{-1}(s) * \pi(r))^{-1} \\ &= \pi(r)^{-1} * \pi^{-1}(s)^{-1} \end{aligned}$$

therefore in this case $\chi_{\pi(j)^{-1}} = \chi_{\pi(r)^{-1}}\chi_{\pi^{-1}(s)^{-1}}$ and equation (25N) is satisfied.

Checking (26N) is similar to (25N) and checking (27N) is similar to (24N) so details are omitted.

Check for (28M): by construction,

$$(\lambda(g) \otimes \text{ID}_k)[(i, j); (r, s)] = \chi_r(g)\delta_{i, \pi(r)}\delta_{j, s}$$

and

$$c_b[(r, s)] = \chi_i(b^{-1})\delta_{i, \pi(j)^{-1}}$$

So we can compute

$$\begin{aligned} (\lambda(g) \otimes \text{ID}_k)[(r, s)] &= \sum_{u, v} \chi_u(g)\delta_{i, \pi(u)}\delta_{j, v}\chi_u(b^{-1})\delta_{u, \pi(v)^{-1}} \\ &= \chi_{\pi^{-1}(r)}(gb^{-1})\delta_{r, s^{-1}} \end{aligned}$$

whence

$$\begin{aligned} r_a(\lambda(g) \otimes \text{ID}_k)c_b &= \sum_{r, s} (|G|\chi_{\pi^{-1}(r)}(a)\delta_{r, s^{-1}})^{-1} (\chi_{\pi^{-1}(r)}(gb^{-1})\delta_{r, s^{-1}}) \\ &= \begin{cases} (|G| - 1)/|G|, & a = gb^{-1} \\ -1/|G|, & a \neq gb^{-1} \end{cases} \end{aligned}$$

and

$$\sum_{c \in G} \mu[a, c]\mu[c, b] + r_a(\lambda(g) \otimes \text{ID}_k)c_b = \delta_{a, b^{-1}g}$$

so (28M) is satisfied.

Verifications of (28C) and (28R) are similar and easy. We will check that (28C) is satisfied, splitting into two cases.

Case I, $i = j^{\circ-1}$. In this case $N[(i, j); (r, s)] = 0$ for all r, s so $N[(i, j); -](\lambda(g) \otimes \text{ID}_k) c_b = 0$. As for the summation, $\sum_{c \in G} c_c[(i, j)\mu[c, b]] = \sum_c \chi_i(c^{-1})(1/|G|) = 0$, so (28C) is satisfied in this case.

Case II, $i \neq j^{\circ-1}$. In this case every term in the summation is zero. The other expression on the left also vanishes:

$$N[(i, j); -](\lambda(g) \otimes \text{ID}_k) c_b = \sum_{r, s} N[(i, j); (r, s)] \chi_{\pi^{-1}(r)}(gb^{-1}) \delta_{r, s^{-1}}$$

so the δ kills off every summand where $N[(i, j); (r, s)]$ is nonzero. That completes the check that (28C) is satisfied and (28R) is obviously very similar.

Checking (28N): Recall this equation requires that

$$\sum_{c \in G} c_c[(i, j)] r_c[(r, s)] + N[(i, j); -](\lambda(g) \otimes \text{ID}_k) N[-; (r, s)] = \lambda(g)[i, s] \lambda(g)[j, r]$$

holds for all $g \in G$ and all indices i, j, r, s . This is the trickiest equation to verify; we will first do a general calculation of both expressions on the lefthand side and then proceed to verify equality in several cases.

First calculation:

$$\begin{aligned} \sum_{c \in G} c_c[(i, j)] r_c[(r, s)] &= \frac{1}{|G|} \sum_c \chi_i(c^{-1}) \chi_{\pi^{-1}(r)}(c^{-1}) \delta_{i, j^{\circ-1}} \delta_{r, s^{-1}} \\ &= \delta_{i, j^{\circ-1}} \delta_{r, s^{-1}} \delta_{i, \pi^{-1}(r)^{-1}} \end{aligned}$$

Second calculation: First of all, note that by construction $N[(i, j); -](\lambda(g) \otimes \text{ID}_k) N[-; (r, s)]$ will certainly be zero if $i = j^{\circ-1}$ or $r = s^{-1}$. Let us calculate the value of this expression assuming that $i \neq j^{\circ-1}$ and $r \neq s^{-1}$. To start, for any indices p and q ,

$$\begin{aligned} ((\lambda(g) \otimes \text{ID}_k) (N[-; (r, s)])) [(p, q)] &= \sum_{u, v} (\lambda(g) \otimes \text{ID}_k) [(p, q); (u, v)] N[(u, v); (r, s)] \\ &= \sum_{u, v} \chi_u(g) \delta_{p, \pi(u)} \delta_{q, v} \delta_{u, r * s} \delta_{v, (r * s)^{\circ-1} \circ r} \\ &= \chi_{r * s}(g) \delta_{q, (r * s)^{\circ-1} \circ r} \delta_{p, \pi(r * s)} \end{aligned}$$

Therefore,

$$\begin{aligned} N[(i, j); -](\lambda(g) \otimes \text{ID}_k) N[-; (r, s)] \\ = \sum_{p, q} \chi_{r * s}(g) \delta_{q, (r * s)^{\circ-1} \circ r} \delta_{p, \pi(r * s)} \delta_{p, i \circ j} \delta_{q, (i \circ j)^{-1} * i} \end{aligned}$$

Now it's clear that the only potentially nonzero term in this sum occurs at the indices

$$\begin{aligned} p &= \pi(r * s) \\ \text{and } q &= (r * s)^{\circ-1} \circ r \end{aligned}$$

That term will actually be nonzero iff $i \circ j = \pi(r * s)$ and $(i \circ j)^{-1} * i = (r * s)^{\circ-1}$. We can now solve for the unique i and j that will make this sum nonzero, for a particular r and s :

$$\begin{aligned}
\pi(r * s)^{-1} * i &= (r * s)^{\circ^{-1}} \circ r \\
&= \pi(\pi((r * s)^{-1}) * \pi^{-1}(r)) \\
&= \pi(r * s)^{-1} * \pi(r^{-1} * r * s) \quad \text{using hypotheses on } \pi \\
&= \pi(r * s)^{-1} * \pi(s)
\end{aligned}$$

hence a nonzero result occurs iff $i = \pi(s)$ and $j = \pi(r)$. Thus the final calculation is

$$N[(i, j); -] (\lambda(g) \otimes \text{ID}_k) N[-; (r, s)] = \begin{cases} 0, & i = j^{\circ^{-1}} \text{ or } r = s^{-1} \\ \chi_{r*s}(g) \delta_{i, \pi(s)} \delta_{j, \pi(r)}, & \text{otherwise} \end{cases}$$

Now we will proceed to verify equality in (28N). First of all, the righthand side is easy to calculate; by construction,

$$\lambda(g)[i, s] \lambda(g)[j, r] = \chi_r(g) \chi_s(g) \delta_{i, \pi(s)} \delta_{j, \pi(r)}$$

From here we proceed in cases:

Case I: When the righthand side is nonzero, ie, $i = \pi(s)$ and $j = \pi(r)$.

Case I, part (i): Assume $r * s = \epsilon$. It follows that $i \circ j = \epsilon$ as well; and on the righthand side of the equation (28N) we have specifically $\chi_r(g) \chi_s(g) = 1$.

On the lefthand side $r * s = \epsilon$ implies the term involving N 's is zero, and by the first calculation above, the summation is 1, so (28N) is satisfied.

Case I, part (ii): Assume $r * s \neq \epsilon$. It follows that $i \circ j \neq \epsilon$ as well. On the lefthand side of equation (28N), all terms in the summation are zero, whereas by second calculation the term involving N 's gives precisely $\chi_{r*s}(g)$, so (28N) is satisfied.

Case II: When the righthand side is zero, ie, $i \neq \pi(s)$ or $j \neq \pi(r)$. Note in this case the term involving N 's on the lefthand side is zero, so we have to check that the summation vanishes.

Case II, part (i): Supposing $i \neq j^{\circ^{-1}}$ or $r \neq s^{-1}$. In this case every term of the summation is clearly zero.

Case II, part (ii): Supposing $i = j^{\circ^{-1}}$ and $r \neq s^{-1}$. In this case it must be that both $i \neq \pi(s)$ and $j \neq \pi(r)$. For suppose $i = \pi(s)$. Then $\pi(s) = j^{\circ^{-1}} = \pi(j)^{-1}$ so $\pi(j) * \pi(s) = \epsilon$ and it follows that $\pi(j) = \pi^{-1}(r)$, or $j = \pi(r)$ contradictory to the hypothesis we are assuming in Case II. Similarly $j = \pi(r)$ forces $i = \pi(s)$, a contradiction. So we suppose both $i \neq \pi(s)$ and $j \neq \pi(r)$. Then $i = j^{\circ^{-1}} = \pi(j)^{-1} \neq \pi^{-1}(r)^{-1}$ so the $\delta_{i, \pi^{-1}(r)^{-1}}$ term in our calculation of the summation kills it, and equality holds in (28N).

This completes the verification of (28N) in all cases; equivalently, the verification of the pentagon equations for the group summands of a fourfold product of m 's. The only remaining pentagon to check is the m summands of fourfold product of m 's, which we have reduced to equations (29)-(37). However, our construction makes the functions c_ϵ , ξ , and N which we use to express those equations all identically 1, giving a trivial solution to equations (29)-(37). With this observation we complete the verification that all pentagon equations in the category are satisfied and we have constructed a coherent monoidal structure. \square

The example data for $k = 1, 2, 3$ in 3.2 shows that this "trivial" solution need not be the only one. Completing the classification for those small values of k ad-hoc is easy but so far a general and useful classification theorem hasn't appeared, so for the present we will be content with the existence theorem.

3.5 Groups that support a π

In this section we characterize the groups and permutations satisfying the hypotheses of Theorem 3.3.2. For reference: the hypotheses are that π is a permutation on the nonidentity elements of G , satisfying

- (i) $\pi^3 = \text{id}$
- (ii) $\pi(x)^{-1} = \pi^{-1}(x^{-1})$
- (iii) $\pi(st) = \pi(t)\pi[\pi(s)^{-1}\pi(t^{-1})]$ (for all $s \neq t^{-1}$)

The result is:

3.5.1 Theorem. *A finite abelian group G admits a permutation π satisfying the above hypotheses if and only if G is the multiplicative group of a field; ie, G is cyclic of order $(p^\alpha - 1)$.*

First we prove the following:

3.5.2 Lemma. *Suppose G, π satisfy the hypotheses. Then there is an element $\omega \in G$ such that $s\pi(s)\pi^{-1}(s) = \omega$ for all $s \neq \epsilon \in G$. Moreover, $\omega^2 = \epsilon$.*

Proof: This is established by iterating the product expansion given by property (iii) of π . Properties (i) and (ii) are also used to simplify. Let $s \neq t^{-1}$ be any nonidentity elements in G .

$$\begin{aligned} \pi(st) &= \pi(t)\pi(\pi(s)^{-1}\pi(t^{-1})) \\ &= \pi(t)s^{-1}\pi(\pi(t)\pi^{-1}(s)) \\ &= \pi(t)s^{-1}\pi^{-1}(t)\pi(s^{-1}t^{-1}) \end{aligned}$$

Since $\pi(st)$ is symmetric in s and t , we have

$$\pi(t)s^{-1}\pi^{-1}(t) = \pi(s)t^{-1}\pi^{-1}(s)$$

or, on rearranging,

$$s\pi(s)\pi^{-1}(s) = t\pi(t)\pi^{-1}(t)$$

Since this holds for arbitrary s and t we conclude that the product $s\pi(s)\pi^{-1}(s)$ is independent of s and we call the common value ω . (The case where G has only two nonidentity elements requires a slightly different argument; in that case it is easy to verify that the only permutation satisfying the hypotheses is the identity permutation, and the present proposition is trivial).

For $\omega^2 = \epsilon$, let $s \neq \epsilon \in G$. By the preceding,

$$\begin{aligned} s\pi(s)\pi^{-1}(s) &= s^{-1}\pi(s^{-1})\pi^{-1}(s^{-1}) \\ &= (s\pi^{-1}(s)\pi(s))^{-1} \end{aligned}$$

hence $\omega = \omega^{-1}$. \square

Note: it may be the case that $\omega = \epsilon$.

Now we can proceed with the main result.

Proof of 3.5.1. First suppose $G = F_{p^\alpha}^*$, the multiplicative group of a field. Then defining $\pi(x) = (1 - x)^{-1}$ for $x \neq 1$ gives a permutation satisfying the hypotheses (easily verified).

For the converse, suppose G, π satisfy the hypotheses. We construct a field F with multiplicative group G as follows: setwise, of course, $F = G \cup \{0\}$. The multiplication extends to F by the obvious rule $0 * x = x * 0 = 0$. The main chore is to define addition. We do this as follows:

$$\begin{aligned} 0 + a &= a + 0 = a \\ a + b &= \pi(\omega ba^{-1})^{-1}a, \quad a, b \neq 0, b \neq \omega a \\ a + b &= 0, \quad b = \omega a \end{aligned}$$

The element ω , apparently, acts as a unary $(-)$ operator, giving additive inverses. We now have to show that F is an abelian group under this addition and that multiplication distributes. We will repeatedly use the lemma to replace expressions of the form $\pi(x)^{-1}$ with $\omega x \pi^{-1}(x)$.

1. Addition is commutative:

$$\begin{aligned} a + b &= \pi(\omega b a^{-1})^{-1} a \\ &= \omega \omega b a^{-1} \pi^{-1}(\omega b a^{-1}) a \\ &= \pi(\omega a b^{-1})^{-1} b \\ &= b + a \end{aligned}$$

2. Addition is associative: If any of a, b, c is 0 then $(a + b) + c = a + (b + c)$ is trivial, so we assume $a, b, c \in G$. Expanding the left-associated expression,

$$\begin{aligned} (a + b) + c &= \pi(\omega c (a + b)^{-1})^{-1} (a + b) \\ &= \pi(\omega c (\pi(\omega b a^{-1})^{-1} a)^{-1})^{-1} \pi(\omega b a^{-1})^{-1} a \\ &= \pi(\omega c \pi(\omega b a^{-1}) a^{-1})^{-1} \pi(\omega b a^{-1})^{-1} a \end{aligned}$$

On the other (the right) hand,

$$\begin{aligned} a + (b + c) &= \pi(\omega (b + c) a^{-1})^{-1} a \\ &= \pi(\omega \pi(\omega c b^{-1})^{-1} b a^{-1})^{-1} a \\ &= \pi(st)^{-1} a \end{aligned}$$

where $s = \pi(\omega c b^{-1})^{-1}$ and $t = \omega b a^{-1}$. Continuing the calculation, we have

$$\begin{aligned} a + (b + c) &= (\pi(t) \pi(\pi(s)^{-1} \pi(t^{-1})))^{-1} a \\ &= \pi(\pi(s)^{-1} \pi(t^{-1}))^{-1} \pi(\omega b a^{-1})^{-1} a \end{aligned}$$

now we evaluate the expression $\pi(s)^{-1} \pi(t^{-1})$:

$$\begin{aligned} \pi(s)^{-1} \pi(t^{-1}) &= \pi(\pi(\omega c b^{-1})^{-1})^{-1} \pi(\omega a b^{-1}) \\ &= \pi(\pi^{-1}(\omega b c^{-1}))^{-1} \pi(\omega a b^{-1}) \\ &= \omega c b^{-1} \pi(\omega a b^{-1}) \\ &= \omega c b^{-1} \omega \omega b a^{-1} \pi(\omega b a^{-1}) \\ &= \omega c \pi(\omega b a^{-1}) a^{-1} \end{aligned}$$

and putting it all together we have obtained

$$a + (b + c) = \pi(\omega c \pi(\omega b a^{-1}) a^{-1})^{-1} \pi(\omega b a^{-1})^{-1} a$$

which agrees with the expression obtained from left association.

At this point we have established that F is an abelian group under $+$, and we need only prove that multiplication distributes. This is easy: if $a, b, c \neq 0$,

$$\begin{aligned} a(b + c) &= a \pi(\omega c b^{-1})^{-1} b \\ &= \pi(\omega a c (ab)^{-1})^{-1} ab \\ &= ab + ac \end{aligned}$$

while if any of a, b, c is 0 the calculation is trivial. Distributivity on the right follows by commutativity of multiplication. So we have F a field with units the group G , as claimed. \square

Note that in the field F we have constructed from G and π , the permutation π can now be expressed by the formula $\pi(x) = (1 - x)^{-1}$ so this is essentially the only example.

3.6. The trivial group case: a nonexistence result

Here we study the case in which our category has only two isomorphism classes of simple objects: the identity ϵ and a noninvertible m ; the fusion rule is described by $m \otimes m = \epsilon \oplus km$. There are two nontrivial associativity morphisms, $\lambda : \text{hom}(\epsilon, (mm)m) \rightarrow \text{hom}(\epsilon, m(mm))$ and $\mu : \text{hom}(m, (mm)m) \rightarrow \text{hom}(m, m(mm))$. These have to satisfy two pentagon equations: $m m m m / \epsilon$ and $m m m m / m$. Element-level descriptions of these equations such as we produced in the nontrivial group case are not particularly helpful since we can't use character relations to deduce large amounts of symmetry. We can, however, extract some information by expressing the pentagons in the large as matrix equations and using determinants.

The $m m m m / \epsilon$ pentagon is formulated as a $(k^2 + 1) \times (k^2 + 1)$ matrix equation. Write X_k for the matrix which operates on basis $\{e_i \otimes e_j\}_{i,j=1..k}$ by tensor flip: $X_k : e_i \otimes e_j \mapsto e_j \otimes e_i$. Write λ' for the block matrix $(1) \oplus (\lambda \otimes \text{ID}_k)$. With this notation, the pentagon equation is

$$\mu \lambda' \mu = \lambda' ((1) \oplus X_k) \lambda'$$

Write $M = \det \mu$ and $L = \det \lambda$. Passing to determinants from the above equation,

$$M^2 L^k = L^{2k} \det(X_k) \quad (38)$$

The $m m m m / m$ pentagon is formulated as a $k^3 + 2k$ dimensional matrix equation. We need some permutation matrices to take care of reordering bases in between steps of the pentagon (as the X_k did in the smaller pentagon). Define

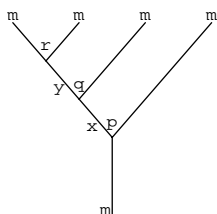
$$P_1 = \begin{pmatrix} 0 & \text{ID}_k & 0 \\ \text{ID}_k & 0 & 0 \\ 0 & 0 & \text{ID}_{k^3} \end{pmatrix}$$

in other words, P_1 exchanges the first block of k basis elements with the second k . Clearly $\det P_1 = (-1)^k$ and $P_1^2 = \text{ID}$. Define

$$P_2 = \text{ID}_{2k} \oplus \overbrace{X_k \oplus \cdots \oplus X_k}^{k \text{ copies}}$$

and note P_2 is also involutory, with $\det P_2 = (\det X_k)^k$.

Finally, let P_3 be the permutation which changes the basis elements



for $\text{hom}(m, (((mm)m)m))$ from (x, y, p, q, r) order to (x, p, y, q, r) order. Now, if we write

$$A = \lambda \oplus (\text{ID}_k \otimes \mu) \quad \text{and}$$

$$B = \text{ID}_k \oplus (\mu \otimes \text{ID}_k)$$

then the large pentagon $m m m m / m$ is expressed as the matrix equation

$$A^{P_3} B^{P_1} A^{P_3} = P_1 B P_2 P_1 B P_1$$

or

$$A^{P_3} B^{P_1} A^{P_3} = B^{P_1} P_1 P_2 B^{P_1}$$

where exponents denote conjugation.

Now $\det A = L^k M$ and $\det B = L^k$ so on passing to determinants from the pentagon, we obtain

$$(LM^k)^2 = M^k (-1)^k (\det X_k)^k \tag{39}$$

3.6.1 Lemma. $\det X_k = \begin{cases} +1, & k \equiv 0 \text{ or } 1 \pmod{4} \\ -1, & k \equiv 2 \text{ or } 3 \pmod{4} \end{cases}$

Proof: The (-1) -eigenspace is spanned by $k(k-1)/2$ vectors of the form $e_i \otimes e_j - e_j \otimes e_i$, $1 \leq i < j \leq k$. The dimension will be even, hence $\det X_k = +1$, iff $4|k$ or $4|(k-1)$. \square

3.6.2 Corollary. *If $k \equiv 2$ or $3 \pmod{4}$ then L is a root of -1 .*

Proof: Case I, $k \equiv 2 \pmod{4}$. Write $k = 2r$, where r odd. Equations (38) and (39) reduce to

$$\begin{aligned} L^2 &= M^{-2r} \\ M^2 &= (-1)L^{2r} \end{aligned}$$

whence $L^{2r^2+2} = -1$.

Case II, $k \equiv 3 \pmod{4}$. In this case equations (38) and (39) reduce to

$$\begin{aligned} L^2 &= M^{-k} \\ M^2 &= (-1)L^k \end{aligned}$$

whence $L^{k^2+4} = -1$. \square

3.6.3 Lemma. $\mu[\epsilon, \epsilon]$ is invertible.

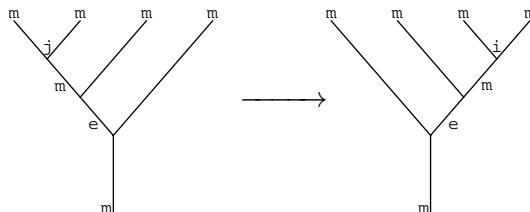
Proof: This a consequence of duality assumptions (see 1.2). We have assumed the existence of a map λ_m such that

$$m \rightarrow \epsilon m \rightarrow (mm)m \xrightarrow{\mu} m(mm) \xrightarrow{1 \otimes \lambda_m} m\epsilon \rightarrow m$$

is equal to the identity on m , which means $\lambda_m \mu[\epsilon, \epsilon] = 1$. \square

3.6.4 Proposition. $L^3 = 1$ (independent of k).

Proof: To prove this we will examine more carefully certain submatrices in the big pentagon. First, consider the $k \times k$ submatrix corresponding to:



Working through both sides of the pentagon, we find this piece gives the equation

$$\sum_p \lambda[p, j] \mu[\epsilon, \epsilon] \lambda[i, p] = \sum_p \mu[(p, i); \epsilon] \mu[\epsilon; (p, j)]$$

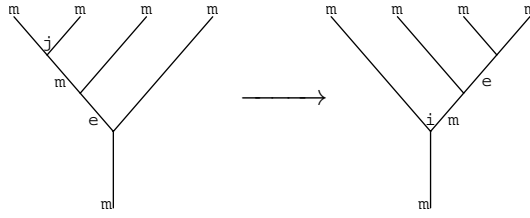
If we define $k \times k$ matrices μ_R and μ_C as follows:

$$\begin{aligned} \mu_R[i, j] &= \mu[\epsilon; (i, j)] \\ \mu_C[i, j] &= \mu[(j, i); \epsilon] \end{aligned}$$

then the above equation can be reformulated as a matrix equation:

$$\mu_C \mu_R = \mu[\epsilon, \epsilon] \lambda^2 \quad (40)$$

Now we consider the $k \times k$ submatrix corresponding to:



This piece gives us

$$\sum_{p, q} \lambda[p, k] \mu[(i, q); \epsilon] \mu[\epsilon; (q, p)] = \mu[\epsilon, \epsilon] \mathbf{ID}_k$$

which we can reformulate as a matrix equation:

$$\mu_C^T \mu_R \lambda = \mu[\epsilon, \epsilon] \mathbf{ID}_k \quad (41)$$

By previous proposition, $\mu[\epsilon, \epsilon]$ is invertible. So we can combine (40) and (41), pass to determinants, and cancel to obtain

$$\det \lambda^2 = (\det \mu_C)(\det \mu_R) = \det \lambda^{-1}$$

or $L^3 = 1$ as claimed. \square

3.6.5 Proof of theorem 1.3.7.

By 3.6.2, 3.6.4, and the hypotheses that the ground ring R has characteristic other than 2, the pentagon equations admit no solution when $k \equiv 2$ or $3 \pmod{4}$. \square

ADDITIONAL STRUCTURES FOR THE $k > 0$ CATEGORIES

4.1 Commutativity and hexagon equations

With 3.2 through 3.4 we have given quite a few examples, and a general construction, of monoidal structures in the maximal-group case. Topological applications (eg, link invariants) generally require at least a commutative structure in addition to the monoidal structures, and that means examining the hexagon equations for coherence of the two structures. In this section we will list the hexagon equations that need to be satisfied, reduce them as much as possible in general, and then show that the general construction of 3.4.18 always admits a (symmetric) commuting structure.

Throughout this section we will assume we are in the setting of theorem 1.3.5 and have chosen bases so that all the reductions of sections 3.3 and 3.4 are in effect.

4.1.1 Notation for commutativity.

As in section 2.1, for $g, h \in G$, the commuting isomorphisms are:

$$\begin{aligned} gh &\rightarrow hg && \text{is multiplication by } \sigma_0(g, h) \\ gm &\rightarrow mg && \text{is multiplication by } \sigma_1(g) \\ mg &\rightarrow gm && \text{is multiplication by } \sigma_2(g) \\ mm &\rightarrow mm && \text{is multiplication by } \sigma_3(g) \text{ on the } g \text{ summand} \end{aligned}$$

Now we also have commutativity on the m summands of $m \otimes m$, represented by a $k \times k$ matrix we call σ_4 .

4.1.2 Unreduced hexagon equations.

The point here is simply to write down a transcription of the hexagon equations using the notation we have developed, without attempting any simplifications. Once we have an entire transcription in hand, we will proceed to analyze and simplify.

We will refer to the xyz/w hexagon meaning the content of the hexagon identity for the w summands in the product xyz . Note that lots of associativities will be invisible since we have chosen bases well.

Let a, b, c stand for arbitrary elements of G .

Hexagons for products with no m 's:

$$\sigma_0(a, c)\sigma_0(a, b) = \sigma_0(a, bc) \qquad (abc/abc)$$

Hexagons for products with one m :

$$\begin{aligned} \sigma_1(a)\sigma_0(a, b) &= \sigma_1(a) && (abm/m) \\ \sigma_0(a, b)\sigma_1(a) &= \sigma_1(a) && (amb/m) \\ \sigma_2(b)\sigma_2(a) &= \sigma_2(ab) && (mab/m) \end{aligned}$$

Hexagons for the group summands of products with two m 's:

$$\begin{aligned}\sigma_2(a)\sigma_3(ba^{-1}) &= \sigma_3(b) && (mma/b) \\ \sigma_3(ba^{-1})\sigma_2(a) &= \sigma_3(b) && (mam/b) \\ \sigma_1(a)^2 &= \sigma(a, ba^{-1}) && (amm/b)\end{aligned}$$

Hexagons for the m summands of products with two m 's:

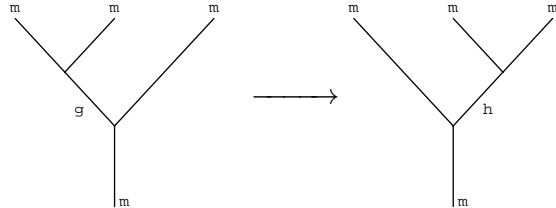
$$\begin{aligned}\sigma_2(a)\gamma_3(a)\sigma_4 &= \gamma_2(a)\sigma_4\gamma_3(a) && (mma/m) \\ \sigma_4\gamma_1(a)\sigma_2(a) &= \gamma_1(a)\sigma_4\gamma_2(a) && (mam/m) \\ \sigma_1(a)\gamma_2(a)\sigma_1(a) &= \gamma_3(a)\sigma_1(a)\gamma_1(a) && (amm/m)\end{aligned}$$

The hexagon for group summands in a product of three m 's:

$$\sigma_4\lambda(g)\sigma_4 = \lambda(g)\sigma_3(g)\lambda(g) \quad (mmm/g)$$

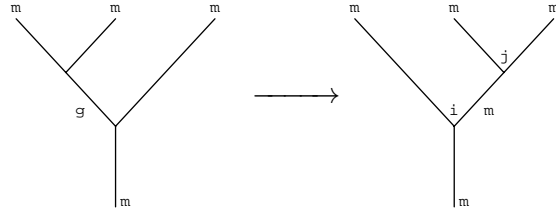
The hexagon for m summands in a product of three m 's we break into individual entries in the matrices.

I. For all $g, h \in G$,



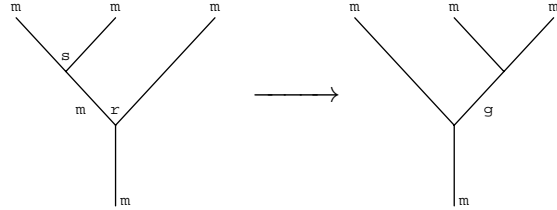
$$\begin{aligned}\sigma_3(g)\mu[h, g]\sigma_3(h) &= \sum_{a \in G} \mu[a, g]\sigma_2(a)\mu[g, a] \\ &+ \sum_{i, j, p} \mu[(i, j); g]\sigma_4[p, i]\mu[h; (p, j)]\end{aligned}$$

II. For all $g \in G, i, j = 1..k$,



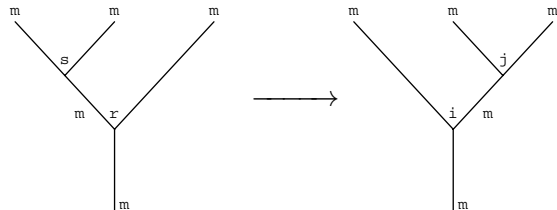
$$\begin{aligned}\sum_p \sigma_3(g)\mu[(i, p); g]\sigma_4[j, p] &= \sum_{a \in G} \mu[a, g]\sigma_2(a)\mu[(i, j); a] \\ &+ \sum_{r, s, t} \mu[(r, s); g]\sigma_4[t, r]\mu[(i, j); (t, s)]\end{aligned}$$

III. For all $g \in G, r, s = 1..k$,



$$\sum_t \sigma_4[t, s] \mu[g; (r, t)] \sigma_3(g) = \sum_{a \in G} \mu[a; (r, s)] \sigma_2(a) \mu[g, a] + \sum_{j, p, q} \mu[(p, q); (r, s)] \sigma_4[j, p] \mu[g; (j, q)]$$

IV. For all $i, j, r, s = 1..k$,



$$\sum_{u, v} \sigma_4[u, s] \mu[(i, v); (r, u)] \sigma_4[j, v] = \sum_{a \in G} \mu[a; (r, s)] \sigma_2(a) \mu[(i, j); a] + \sum_{p, q, t} \mu[(p, q); (r, s)] \sigma_4[t, p] \mu[(i, j); (t, q)]$$

That completes the list of hexagon equations. There are also inverse hexagons to be considered since we do not assume a symmetric commutative structure but we will postpone analysis of the inverse hexagons until we have simplified the standard ones.

4.1.3 Reducing the hexagons.

Quite a lot of reductions are possible in the list of hexagons. To start, $\sigma_0 \equiv 1$ is obvious. We will show that σ_1, σ_2 must both be equal to a distinguished linear character of G . Then σ_3 is entirely determined up to the value of $\sigma_3(\epsilon)$, and happily, the σ_4 matrix admits considerable simplification as well.

4.1.4 Proposition. $\sigma_1 = \sigma_2$

Proof: It's clear from the list of hexagons that $\sigma_0 \equiv 1$ so the present proposition would follow from the amm/b hexagon if we assumed symmetric commutativity. In general, however, it still follows from the mma/b hexagon together with its inverse:

$$\sigma_2(a) = \sigma_3(b) \sigma_3(ba^{-1})^{-1} = \sigma_1(a). \quad \square$$

From the mab/m hexagon it's now clear that σ_1 and σ_2 are linear characters of G . Our next result sharpens that statement. By the results of 3.5, we know there is a unique character χ_ω with $\chi_i \chi_{\pi(i)} \chi_{\pi^{-1}(i)} = \chi_\omega$ for all i ; it satisfies $\chi_\omega^2 = 1$ and is the trivial character (ie, $\omega = \epsilon$) iff $|G|$ is odd.

4.1.5 Proposition. $\sigma_1 = \sigma_2 = \chi_\omega$

Proof: By the amm/b hexagon, $\sigma_1^2 = 1$. Therefore the amm/m hexagon can be reduced to

$$\sigma_1(a) = \gamma_3(a) \gamma_1(a) \gamma_2(a)^{-1}$$

Since γ 's are diagonalized this is equivalent to

$$\sigma_1(a) = \chi_{\pi^{-1}(i)}(a)\chi_i(a)\chi_{\pi(i)}(a)$$

for all a and i . Hence, $\sigma_1 = \chi_\omega$ as claimed. \square

4.1.6 Proposition (σ_4 Structure). *There are invertible constants $\psi(1), \dots, \psi(k)$ such that the matrix σ_4 has the form $\sigma_4 = (\psi(j)\delta_{i,\pi(j^{-1})})_{i,j}$*

Proof: Consider the mma/m hexagon. It now reduces to

$$\chi_\omega(g)\sigma_4[i, j] = \chi_{\pi(i^{-1})}(g)\chi_{\pi^{-1}(i^{-1})}(g)\chi_{\pi^{-1}(j)}(g)\sigma_4[i, j]$$

for all i, j , and g . But that, together with invertibility of σ_4 tells us that $\sigma_4[i, j]$ is nonzero (moreover, invertible) iff $i = \pi(j^{-1})$. \square

Note that the mam/m hexagon is satisfied by precisely the same condition.

4.1.7 Proposition. *All of the mmm/g hexagons are satisfied iff the constants ψ satisfy the identity*

$$\psi(j)\psi(\pi(j)^{-1})\xi(\pi(j^{-1})) = \sigma_3(\epsilon)\xi(j)\xi(\pi(j))$$

for all j .

Proof: This is simply working out the matrix products on both sides. On the left,

$$\sigma_4\lambda(g)\sigma_4 = \left(\psi(j)\psi(\pi(j)^{-1})\xi(\pi(j^{-1}))\chi_{\pi(j^{-1})}(g)\delta_{i,\pi^{-1}(j)} \right)_{i,j}$$

while on the right,

$$\lambda(g)\sigma_3(g)\lambda(g) = \left(\xi(j)\xi(\pi(j))\sigma_3(\epsilon)\chi_\omega(g)\chi_j(g)\chi_{\pi(j)}(g)\delta_{i,\pi^{-1}(j)} \right)_{i,j}$$

All the χ 's cancel and the proposition follows. \square

4.1.8 Reducing the mmm/m hexagon, Part I.

On the lefthand side,

$$\sigma_3(g)\mu[h, g]\sigma_3(h) = \sigma_3(\epsilon)^2\chi_\omega(gh)\mu[\epsilon, \epsilon]$$

On the righthand side, the first summation is

$$\sum_{a \in G} \mu[a, g]\sigma_2(a)\mu[g, a] = (|G|^{-1}) \sum_{a \in G} \chi_\omega(a) = |G|^{-1}\delta_{\omega, \epsilon}$$

The second summation is

$$\sum_{i,j,p} \mu[(i, j); g]\sigma_4[p, i]\mu[h; (p, j)] = \begin{cases} |G|^{-1}\psi(\omega)\xi(\omega)^{-1}\chi_\omega(gh)^{-1}, & \omega \neq \epsilon \\ 0, & \omega = \epsilon \end{cases}$$

In case $|G|$ is odd, $\omega = \epsilon$, the requirement of this piece of the hexagon is simply

$$\sigma_3(\epsilon)^2 = \delta$$

(recall $\delta = |G|\mu[\epsilon, \epsilon] = \pm 1$).

In case $|G|$ is even, $\omega \neq \epsilon$, the requirement of the hexagon is

$$\sigma_3(\epsilon)^2 = \psi(\omega)\xi(\omega)^{-1}$$

In either case this completes the simplification of this piece of the mmm/m hexagon.

4.1.9 Reducing the mmm/m hexagon, Part II.

On the lefthand side,

$$\begin{aligned} \sum_p \sigma_3(g) \mu[(i, p); g] \sigma_4[j, p] &= \sigma_3(g) \sum_p c_\epsilon[(i, p)] \chi_i(g)^{-1} \sigma_4[j, p] \\ &= \sigma_3(\epsilon) \chi_\omega(g) \chi_i(g)^{-1} c_\epsilon(i) \psi(\pi(i)^{-1}) \delta_{i, \pi(j)} \end{aligned}$$

On the right, the first summation is

$$\sum_{a \in G} \mu[a, g] \sigma_2(a) \mu[(i, j); a] = \delta c_\epsilon(i) \delta_{i, \omega} \delta_{i, \pi(j)}$$

The second summation is

$$\sum_{r, s, t} \mu[(r, s); g] \sigma_4[t, r] \mu[(i, j); (t, s)]$$

Note this will be nonzero iff there exist indices r, s , and t satisfying

$$\begin{aligned} r &= s^{\circ-1} = \pi(s)^{-1} \\ t &= \pi(r^{-1}) \\ i \circ j &= t \\ t * s &= i \end{aligned}$$

We can solve for the indices uniquely, in terms of i if they exist:

$$\begin{aligned} \pi^{-1}(s) * s &= i \\ \text{so } \pi(s)^{-1} * \pi(s) * \pi^{-1}(s) * s &= i \\ \text{and } s &= \pi^{-1}(\omega * i^{-1}) \end{aligned}$$

Note that if $i = \omega$ there could be no s filling the requirement and the sum would vanish.

Immediately, $t = \pi(\omega * i^{-1})$ follows. Now from the remaining equation $i \circ j = t$ we discover the condition necessary to get a nonzero sum:

$$\begin{aligned} j &= t \circ i^{\circ-1} = \pi(\pi^{-1}(t) * \pi^{-1}(\pi^{-1}(i^{-1}))) \\ &= \pi(\omega * i^{-1} * \pi(i^{-1})) \\ &= \pi(\omega * i^{-1} * \pi(i^{-1}) * \pi^{-1}(i^{-1}) * \pi^{-1}(i^{-1})^{-1}) \\ &= \pi(\pi(i)) = \pi^{-1}(i) \end{aligned}$$

So a nonzero summation happens precisely when $i = \pi(j)$ and the reduction is

$$\begin{aligned} \sum_{r, s, t} \mu[(r, s); g] \sigma_4[t, r] \mu[(i, j); (t, s)] \\ = c_\epsilon(i) \chi_\omega(g)^{-1} \chi_i(g)^{-1} \psi(\omega * i) N(\pi(\omega i^{-1}), \pi^{-1}(\omega i^{-1})) (1 - \delta_{i, \omega}) \delta_{i, \pi(j)} \end{aligned}$$

The upshot is that for $|G|$ odd, $\omega = \epsilon$, this piece of the hexagon is equivalent to the requirement

$$\sigma_3(\epsilon) \psi(\pi(i)^{-1}) = \psi(i) N(\pi(i^{-1}), \pi^{-1}(i^{-1})), \quad \text{for all } i$$

For $|G|$ even, $\omega \neq \epsilon$, this piece of the hexagon is equivalent to the requirements

$$\begin{aligned} \sigma_3(\epsilon) \psi(\pi^{-1}(\omega)) &= 1 \\ \sigma_3(\epsilon) \psi(\pi(i)^{-1}) &= \psi(\omega * i) N(\pi(\omega * i^{-1}), \pi^{-1}(\omega * i^{-1})), \quad \text{for all } i \neq \omega \end{aligned}$$

4.1.10 Reducing the mmm/m hexagon, Part III.

This is very similar to Part II, so we omit some details. On the left,

$$\sum_t \sigma_4[t, s] \mu[g; (r, t) \sigma_3(g) = \sigma_3(\epsilon) \chi_\omega(g) \psi(s) (|G| \xi(\pi(s)) \chi_{\pi(s)}(g)^{-1} c_\epsilon(\pi(s)))^{-1} \delta_{s, \pi(r)}$$

On the right, the first summation is

$$\sum_{a \in G} \mu[a; (r, s)] \sigma_2(a) \mu[g, a] = \delta (|G| \xi(\omega) c_\epsilon(\omega))^{-1} \delta_{r, s^{-1}} \delta_{\omega, \pi(s)}$$

The second summation is

$$\begin{aligned} & \sum_{j, p, q} \mu[(p, q); (r, s)] \sigma_4[j, p] \mu[g; (j, q)] \\ &= r_g (\pi(r * s)^{-1}) \psi(r * s) N(r, s) \delta_{s, \pi(r)} (1 - \delta_{r, s^{-1}}) \\ &= (|G| \xi(\omega * \pi(s)) \chi_{\omega * \pi(s)}(g)^{-1} c_\epsilon(\omega * \pi(s)))^{-1} \psi(\omega * \pi(s)^{-1}) N(\pi^{-1}(s), s) \delta_{s, \pi(r)} (1 - \delta_{r, s^{-1}}) \end{aligned}$$

So for $|G|$ odd, $\omega = \epsilon$, the requirement of the hexagon is

$$\sigma_3(\epsilon) \psi(s) = \psi(\pi(s)^{-1}) N(\pi^{-1}(s), s), \quad \text{for all } s$$

Note that this is equivalent to the requirement from Part II of the hexagon, under the change of variable $s \rightarrow \pi(i)^{-1}$.

For $|G|$ even, $\omega \neq \epsilon$, this piece of the hexagon is equivalent to the requirements

$$\sigma_3(\epsilon) \psi(\pi^{-1}(\omega)) = 1$$

and

$$\sigma_3(\epsilon) \psi(s) \xi(\omega * \pi(s)) c_\epsilon(\omega * \pi(s)) = \xi(\pi(s)) c_\epsilon(\pi(s)) \psi(\omega * \pi(s)^{-1}) N(\pi^{-1}(s), s)$$

for all $s \neq \pi^{-1}(\omega)$. Note that while the first equation duplicates the result from Part II, the second is a bit more complicated, as it involves ξ 's.

4.1.11 Reducing the mmm/m hexagon, Part IV.

On the left,

$$\begin{aligned} \sum_{u, v} \sigma_4[u, s] \mu[(i, v); (r, u)] \sigma_4[j, v] &= \sigma_4[\pi(s^{-1}), s] \mu[(i, \pi(j^{-1})); (r, \pi(s^{-1}))] \sigma_4[j, \pi(j^{-1})] \\ &= \psi(s) \psi(\pi(j^{-1})) N(r, \pi(s^{-1})) \delta_{i, r * \pi(s^{-1})} \delta_{r, i \circ \pi(j^{-1})} \end{aligned}$$

On the right, the first summation is

$$\begin{aligned} & \sum_{a \in G} \mu[a; (r, s)] \sigma_2(a) \mu[(i, j); a] \\ &= (|G| \xi(\pi^{-1}(r)) c_\epsilon(\pi^{-1}(r)))^{-1} c_\epsilon(i) \sum_a \chi_\omega(a) \chi_i(a)^{-1} \chi_{\pi^{-1}(r)}(a)^{-1} \delta_{r, s^{-1}} \delta_{i, j \circ^{-1}} \\ &= (\xi(\pi^{-1}(r)) c_\epsilon(\pi^{-1}(r)))^{-1} c_\epsilon(i) \delta_{r, s^{-1}} \delta_{i, j \circ^{-1}} \delta_{\omega, i * \pi^{-1}(r)} \end{aligned}$$

Recall the second summation is

$$\sum_{p, q, t} \mu[(p, q); (r, s)] \sigma_4[t, p] \mu[(i, j); (t, q)]$$

As usual, there could be at most one nonzero term in the sum and the game is to find the conditions on i, j, r, s which would permit this. A nonzero sum happens iff there are p, q, t with

$$\begin{aligned} r &= p \circ q & p &= r * s \\ t &= i \circ j & i &= t * q \\ & & t &= \pi(p^{-1}) \end{aligned}$$

In terms of r and s , the magic indices must be

$$\begin{aligned} p &= r * s \\ q &= \pi(s) * \pi(r * s)^{-1} \\ t &= \pi((r * s)^{-1}) \end{aligned}$$

but in terms of i and j we must have

$$\begin{aligned} p &= \pi(i^{-1}) * \pi(j^{-1}) \\ q &= \pi^{-1}(j * \pi(i)) \\ t &= i \circ j = \pi(\pi^{-1}(i) * \pi^{-1}(j)) \end{aligned}$$

So we can determine r and s in terms of i and j if there is to be a nonzero sum. First, we can solve for s :

$$\begin{aligned} \pi(s) &= \pi^{-1}(j * \pi(i)) * \pi(r * s) \\ &= (\pi(j^{-1} * \pi(i)^{-1}))^{-1} * \pi(\pi(i^{-1}) * \pi(j^{-1})) \\ &= (i^{-1} * \pi(\pi(j^{-1})^{-1} * \pi^{-1}(i)))^{-1} * \pi(\pi(i^{-1}) * \pi(j^{-1})) \\ &= i * \pi^{-1}(\pi(j^{-1}) * \pi(i^{-1})) * \pi(\pi(i^{-1}) * \pi(j^{-1})) \\ &= i * \omega * \pi^{-1}(j) * \pi^{-1}(i) \\ &= \omega * \omega * \pi(i)^{-1} * \pi^{-1}(j) \\ &= \pi(i)^{-1} * \pi^{-1}(j) \end{aligned}$$

and the conclusion is

$$s = \pi^{-1}(\pi(i)^{-1} * \pi^{-1}(j)) = \pi(\pi(i) * \pi(j^{-1}))^{-1}$$

Now we can solve for r as well:

$$\begin{aligned} r &= \pi(i^{-1}) * \pi(j^{-1}) * \pi(\pi(i) * \pi(j^{-1})) \\ &= \pi(i^{-1}) * \pi(j^{-1}) * \pi^{-1}(i) * \pi(\pi(j) * i^{-1}) \\ &= \pi(j^{-1}) * \pi^{-1}(j) * \pi(\pi^{-1}(i) * j^{-1}) \\ &= \pi(\pi^{-1}(i) * j^{-1}) \end{aligned}$$

and so the complete reduction of the second summation is:

$$\begin{aligned} \sum_{p,q,t} \mu[(p, q); (r, s)] \sigma_4[t, p] \mu[(i, j); (t, q)] \\ = N(r, s) \psi(r * s) N(\pi((r * s)^{-1}), \pi(s) * \pi(r * s)^{-1}) \\ \delta_{r, \pi(\pi^{-1}(i) * j^{-1})} \delta_{s, \pi^{-1}(\pi(i)^{-1} * \pi^{-1}(j))} (1 - \delta_{r, s^{-1}}) (1 - \delta_{i, j \circ^{-1}}) \end{aligned}$$

Now we can set about extracting practical equations.

Assume the lefthand side is nonzero, ie, $i = r * \pi(s^{-1})$ and $r = i \circ \pi(j^{-1})$.

Case I. $r = s^{-1}$ and $i = j^{\circ-1}$. In this case the second sum on the right vanishes but since we have $i = r * \pi(r) = \omega * \pi(r^{-1})$, the first sum on the right does not vanish, so we get the requirement

$$\psi(s)\psi(\pi(j^{-1}))N(r, \pi(s^{-1})) = (\xi(\pi^{-1}(r))c_\epsilon(\pi^{-1}(r)))^{-1} c_\epsilon(i)$$

This can be rewritten all in terms of r , but it requires some work to express $\pi(j^{-1})$ in terms of r :

$$\begin{aligned} \pi(j^{-1}) &= r \circ (r * \pi(r))^{\circ-1} \\ &= \pi(\pi^{-1}(r) * \pi(r^{-1} * \pi(r)^{-1})) \\ &= (\pi(r * \pi(r)))^{-1} * \pi^{-1}(r) \\ &= \pi^{-1}(r * \pi(r)) \end{aligned}$$

So our final version of the hexagon in this case is

$$\psi(r^{-1})\psi(\pi^{-1}(r * \pi(r)))N(r, \pi(r)) = (\xi(\pi^{-1}(r))c_\epsilon(\pi^{-1}(r)))^{-1} c_\epsilon(r * \pi(r)),$$

for all r .

Case II. $r \neq s^{-1}$ and $i \neq j^{\circ-1}$. In this case the first sum on the right vanishes but it is easy to verify that the second does not. As in the previous case we can solve for $\pi(j^{-1})$ in terms of r and s , namely, $\pi(j^{-1}) = \pi^{-1}(s^{-1} * \pi(r))$. So our final version of the hexagon in this case is

$$\psi(s)\psi(\pi^{-1}(s^{-1} * \pi(r)))N(r, \pi(s^{-1})) = N(r, s)\psi(r * s)N(\pi((r * s)^{-1}), \pi(s) * \pi(r * s)^{-1}),$$

for all $r \neq s^{-1}$.

Case III. $r \neq s^{-1}$ xor $i \neq j^{\circ-1}$. If the lefthand side is nonzero, it is easy to check that this cannot occur.

That takes care of all possibilities when the lefthand side is nonzero. But conversely any conditions under which the righthand side is nonzero give a nonzero lefthand side so we have covered all the nontrivial possibilities, and completed reducing all the hexagon equations. As with the results of the largest pentagon in 3.4, the expressions are awkward but do have the virtue of admitting an obvious trivial solution.

We summarize the work of this section so far in the following:

4.1.12 Proposition. *Suppose near-group fusion rule (G, k) , $|G| = k + 1$, has a monoidal structure described by ξ, c_ϵ , and N . If a braiding is possible, then that braiding has the following structure:*

1. $\sigma_0 \equiv 1$
2. $\sigma_1(g) = \sigma_2(g) = \chi_\omega(g)$ for all $g \in G$.
3. $\sigma_3(g) = \sigma_3(\epsilon)\chi_\omega(g)$ for all g in G
4. $\sigma_4(g) = (\psi(j)\delta_{i, \pi(j^{-1})})_{i,j}$ where $\sigma_3(\epsilon)$ and $\psi(1), \dots, \psi(k)$ are invertible constants.

Proof: Summary of results up to this point. \square

If we want to construct a braiding, therefore, 4.1.12 gives a recipe for the commuting maps in terms of constants $\sigma_3(\epsilon)$ and $\psi(1), \dots, \psi(k)$. The following summarizes the constraints on those constants.

4.1.13 Proposition. *The hexagon axiom is satisfied provided $\sigma_3(\epsilon)$ and $\psi(1), \dots, \psi(k)$ satisfy the following constraints:*

Independent of $|G|$, for all indices r ,

$$\psi(r)\psi(\pi(r)^{-1})\xi(\pi(r^{-1})) = \sigma_3(\epsilon)\xi(r)\xi(\pi(r)) \quad (42)$$

for $r \neq \pi(r)^{-1}$,

$$\psi(r^{-1})\psi(\pi^{-1}(r * \pi(r)))N(r, \pi(r)) = (\xi(\pi^{-1}(r)c_\epsilon(\pi^{-1}(r)))^{-1}c_\epsilon(r * \pi(r))) \quad (43)$$

and for $s \neq \pi(r)$, $s \neq r^{-1}$,

$$\psi(s)\psi(\pi^{-1}(s^{-1} * \pi(r)))N(r, \pi(s^{-1})) = N(r, s)\psi(r * s)N(\pi((r * s)^{-1}), \pi(s) * \pi(r * s)^{-1}) \quad (44)$$

For $|G|$ odd, for all indices r ,

$$\sigma_3(\epsilon)^2 = \delta \quad (45)$$

$$\sigma_3(\epsilon)\psi(\pi(r)^{-1}) = \psi(r)N(\pi(r^{-1}), \pi^{-1}(r^{-1})) \quad (46)$$

For $|G|$ even,

$$\sigma_3(\epsilon)^2 = \psi(\omega)\xi(\omega)^{-1} \quad (47)$$

$$\sigma_3(\epsilon)\psi(\pi^{-1}(\omega)) = 1 \quad (48)$$

$$\sigma_3(\epsilon)\psi(\pi(r)^{-1}) = \psi(\omega * r)N(\pi(\omega * r^{-1}), \pi^{-1}(\omega * r^{-1})), \quad \text{for } r \neq \omega \quad (49)$$

$$\begin{aligned} \sigma_3(\epsilon)\psi(\pi^{-1}(r))\xi(\omega * r)c_\epsilon(\omega * r) \\ = \xi(r)c_\epsilon(r)\psi(\omega * r^{-1})N(\pi(r), \pi^{-1}(r)), \quad \text{for } r \neq \omega \end{aligned} \quad (50)$$

Proof: Equations (42)-(44) come from 4.1.7 and 4.1.11. Equations (45) and (46) come from 4.1.8 and 4.1.9. Equations (47)-(50) come from 4.1.8, 4.1.9, and 4.1.10, with minor change of indices to make the present list appear consistent. \square

4.1.14 Proposition. *The standard monoidal solution constructed in 3.4.18 admits a symmetric commuting structure.*

Proof: This is now a triviality. The standard monoidal solution corresponds to taking ξ, c_ϵ , and N all identically equal to 1. Now we can satisfy the constraints listed in 4.1.13 by setting $\sigma_3(\epsilon) = \psi(1) = \dots = \psi(k) = 1$ as well, obtaining a solution to the hexagon equations. It's easy to check that this is a symmetric structure: $\sigma_0(g, h)\sigma_0(h, g) = 1$ since $\sigma_0 \equiv 1$. Also $\sigma_1(g)\sigma_2(g) = \sigma_2(g)\sigma_1(g) = \chi_\omega(g)^2 = 1$. Similarly, $\sigma_3(g)^2 = \sigma_3(\epsilon)\chi_\omega(g)^2 = 1$, and $\sigma_4 = (\delta_{i, \pi(j^{-1})})_{i, j}$ is self-inverse because the map $j \mapsto \pi(j^{-1})$ is an involution. Since the structure is symmetric we do not need to consider any inverse hexagons. \square

4.2. Examples of braidings

4.2.1 Example 1. $k = 1, G = \mathbb{Z}/2\mathbb{Z}$.

From 3.2, there are three monoidal structures, corresponding to a choice of ξ a cube root of unity. In the language we have developed the monoidal structure is described by $c_\epsilon(1) = 1$, $\xi(1) = \xi$, and there is no N due to a shortage of indices. Braidings, if possible, are described by invertible constants $\sigma_3(\epsilon)$ and $\psi(1)$. The possibilities are given in the following:

4.2.2 Theorem (Braidings, $k = 1, G = \mathbb{Z}/2\mathbb{Z}$). *The $\xi = 1$ structure admits three distinct braidings corresponding to a choice of $\psi = \psi(1)$ with $\psi^3 = 1$. The $\xi \neq 1$ structures do not admit braidings.*

Proof: Referring to proposition 4.1.13 we see the only requirements of the hexagon axiom are:

$$\begin{aligned}\psi^2\xi &= \sigma_3(\epsilon)\xi^2 \\ \sigma_3(\epsilon)^2 &= \psi\xi^{-1} \\ \sigma_3(\epsilon)\psi &= 1\end{aligned}$$

(these come from equations (42), (47), and (48), respectively; none of the remaining equations from 4.1.13 apply in this case). It is easy that these equations are satisfied iff $\psi^3 = \xi$ and $\sigma_3(\epsilon) = \psi^{-1}$. But inverse hexagons will be satisfied iff $\psi^{-3} = \xi$ as well; we conclude that $\xi = 1$ is the only monoidal structure which admits any commutative structure satisfying both the hexagon and inverse hexagon axioms. Of course the $\psi = 1$ structure is symmetric; the other two clearly not.

For reference, then, the complete data for the braidings in this case is:

$$\begin{aligned}\sigma_0 &\equiv (1) \\ \sigma_1(a) &= \sigma_2(a) = (\chi(a)) \\ \sigma_3(a) &= (\psi^{-1}\chi(a)) \\ \sigma_4 &= (\psi)\end{aligned}$$

where χ is the nontrivial character of G and $a \in G$. \square

4.2.3 Example 2. $k = 2, G = \mathbb{Z}/3\mathbb{Z} = \{\epsilon, g, g^2\}$. From 3.2 there are two distinct monoidal structures corresponding to a choice of $\xi = \pm 1$. In the language we have developed, the monoidal structure is described by

$$\begin{aligned}\xi(1) &= \xi(2) = \xi \\ c_\epsilon(1) &= 1, \quad c_\epsilon(2) = \xi \\ N(1, 1) &= 1, \quad N(2, 2) = \xi\end{aligned}$$

Braidings, if possible, are described by $\sigma_3(\epsilon)$, $\psi(1)$, and $\psi(2)$. The possibilities are given in the following:

4.2.4 Theorem (Braidings, $k = 2, G = \mathbb{Z}/3\mathbb{Z}$). *The $\xi = 1$ structure admits four distinct braidings corresponding to a choice of $\psi(1), \psi(2)$ with $\psi(1)^2 = \psi(2)^2 = 1$. The $\xi = -1$ structure does not admit any braiding.*

Proof: Referring to proposition 4.1.13, and using the monoidal data, we see the requirements of the hexagon axiom are as follows. From equation (42),

$$\psi(1)\psi(2)\xi = \sigma_3(\epsilon)$$

From equation (43),

$$\begin{aligned}\psi(2)^2 &= 1 \\ \psi(1)^2\xi &= 1\end{aligned}$$

There are no indices r, s to which (31) applies. From (32),

$$\sigma_3(\epsilon)^2 = \xi$$

and from (46),

$$\begin{aligned}\sigma_3(\epsilon)\psi(2) &= \psi(1)\xi \\ \sigma_3(\epsilon)\psi(1) &= \psi(2)\end{aligned}$$

It's clear that these are satisfied iff we take $\psi(1)^2 = \xi$, $\psi(2)^2 = 1$, and $\sigma_3(\epsilon) = \psi(1)\psi(2)\xi$. For inverse mmm/m hexagon to be satisfied, though, $\sigma_3(\epsilon)$ has to be self-inverse, and so $\xi = +1$ is the only possibility for the monoidal structure. The cases $\psi(1) = \psi(2) = \pm 1$ are symmetric; the $\psi(1) \neq \psi(2)$ cases are not.

For reference, the complete data for the braidings in this case is:

$$\begin{aligned}\sigma_0 &\equiv (1) \\ \sigma_1 &\equiv \sigma_2 \equiv (1) \\ \sigma_3(a) &= (\psi(1)\psi(2)) \\ \sigma_4 &= \begin{pmatrix} 0 & \psi(2) \\ \psi(1) & 0 \end{pmatrix}\end{aligned}$$

where $a \in G$. \square

4.2.5 Example 3. $k = 3, G = \mathbb{Z}/4\mathbb{Z} = \{\epsilon, g, g^2, g^3\}$.

From 3.2, this fusion rule has a unique monoidal structure, which is described by taking ξ, c_ϵ , and N all identically 1. As it turns out, the commutative structure is unique as well.

4.2.6 Theorem (Braidings, $k = 3, G = \mathbb{Z}/4\mathbb{Z}$). *The unique monoidal structure for this fusion rule admits a unique braiding.*

Proof: Referring to proposition 4.1.13, and using the monoidal data, we get the following constraints. From (42) with $r = 1, 2, 3$, respectively:

$$\begin{aligned}\psi(1)\psi(2) &= \sigma_3(\epsilon) & \psi(2)\psi(1) &= \sigma_3(\epsilon) \\ \psi(3)^2 &= \sigma_3(\epsilon)\end{aligned}$$

From (43) with $r = 1, 2$:

$$\psi(3)\psi(2) = 1 \quad \psi(2)\psi(3) = 1$$

From (44) with $(r, s) = (2, 1), (3, 2)$:

$$\psi(1)^2 = \psi(3) \quad \psi(2)^2 = \psi(1)$$

From (47) and (48),

$$\sigma_3(\epsilon)^2 = \psi(2) \quad \sigma_3(\epsilon)\psi(1) = 1$$

And from (49),

$$\sigma_3(\epsilon)\psi(2) = \psi(3) \quad \sigma_3(\epsilon)\psi(3) = \psi(1)$$

Since the monoidal data is trivial, equation (50) is equivalent to (59). It is easy to check that the solutions to these are of the following form: $\psi(2)$ any fifth root of unity; $\psi(1) = \psi(2)^2$; $\psi(3) = \psi(2)^{-1}$; $\sigma_3(\epsilon) = \psi(2)^{-2}$. In other words, the commutativity data is determined by the choice of $\psi(2)$. However, inverse hexagons (consider mmm/ϵ) force the additional requirement

$\psi(1) = \psi(2) = \psi(3)$, so the only braiding comes from $\psi(2) = 1$ (our standard symmetric solution). For reference, the complete data:

$$\begin{aligned}\sigma_0 &\equiv (1) \\ \sigma_1(a) = \sigma_2(a) &= (\chi_\omega(a)) \\ \sigma_3(a) &= (\chi_\omega(a)) \\ \sigma_4 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\end{aligned}$$

where χ_ω is the nontrivial order 2 character and $a \in G$. \square

4.3. Twist.

This is just a brief comment on the possibility of adding twist morphisms to a braided near-group category in the setting of Theorem 1.3.5 (useful for invariants of framed links). We need endomorphisms θ_s for each simple s , which balance the commutative structure in the sense that $\theta_{r \otimes s} = \theta_r \theta_s \sigma(r, s) \sigma(s, r)$ where $\sigma(r, s)$ is used generically to denote commuting r past s . After the simplifications of the braided structure carried out in section 8, it is easy to see that this axiom reduces to the following:

$$\begin{aligned}\theta_g &= 1 \quad \text{for all } g \in G \\ \sigma_3(\epsilon)^2 \theta_m^2 &= 1 \\ \psi(j) \psi(\pi(j^{-1})) &= \theta_m \quad \text{for all } j\end{aligned}$$

This is simple to work out for the small example categories we have studied in 3.2 and 4.2, but interesting since it gives a few examples of non-symmetric braidings that do or do not admit twist. We say a braiding is balanced if there is a θ_m satisfying the twist equations above.

4.3.1 Proposition (Twist, $k = 1, G = \mathbb{Z}/2\mathbb{Z}$). *In the setting of theorem 4.2.2, the $\psi = 1$ structure is balanced. The $\psi \neq 1$ structures are not.*

Proof: The symmetric $\psi = 1$ case has trivial twist morphisms and the braiding data from 4.2.2 together with the twist equations above implies $\psi = 1$ immediately. \square

4.3.2 Proposition (Twist, $k = 2, G = \mathbb{Z}/3\mathbb{Z}$). *In the setting of theorem 4.2.4, all of the braidings are balanced.*

Proof: The symmetric $\psi(1) = \psi(2)$ structures take trivial twist morphisms; taking $\theta_m = -1$ satisfies the nonsymmetric $\psi(1) = -\psi(2)$ structures. \square

References

- [FK] J. Frolich and T. Kerler, *Quantum Groups, Quantum Categories, and quantum field theory*, Springer-Verlag, 1993.
- [JS] A. Joyal and R. Street, *Braided tensor categories*, *Advances in Math.* **102** (1993), 20–78.
- [KR] R. M. Kashaev and N. Reshitikhin, *Symmetrically Factorizable Groups and Set-Theoretical Solutions of the Pentagon Equation*, math.qa/0111171.
- [Mac] S. MacLane, *Categories for the Working Mathematician*, Springer-Verlag, 1971.
- [O] V. Ostrik, *Fusion categories of rank 2*, math.QA/0203255.
- [Q] F. Quinn, *Lectures on Axiomatic Topological Quantum Field Theory*, *Geometry and Quantum Field Theory Volume 1*, IAS/Park City Mathematical Series, American Mathematical Society, 1995.
- [Q2] F. Quinn, *Group categories and their field theories*, *Geometry and Topology Monographs*, vol. 2, 1999, pp. 407–453.
- [T] V.G. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, de Gruyter, 1994.
- [TY] D. Tambara and S. Yamagami, *Tensor Categories with Fusion Rules of Self-Duality for Finite Abelian Groups*, *Journal of Algebra* **209** (1998), 692–707.
- [S] J. Siehler, *Braided Near-group Categories*, math.qa/0011037.
- [Sh] M.C. Shum, *Tortile tensor categories*, *Journal of Pure and Applied Algebra* **93** (1994), 57–110.
- [St] J.D. Stasheff, *Homotopy associativity of H-spaces. I*, *Transactions of the AMS* **108** (1963), 275–292.

Vita

Jacob A. Siehler

Education

2003	PhD Mathematics	Virginia Tech	Blacksburg, VA
2001	MS Mathematics	Virginia Tech	Blacksburg, VA
1997	BA Mathematics	Frostburg St. University	Frostburg, MD
1997	BA Computer Science	Frostburg St. University	Frostburg, MD
1996	Budapest Semesters in Mathematics		