*ISSN 1472-2739 (on-line) 1472-2747 (printed)* **719**

*Algebraic & Geometric Topology*
Volume 3 (2003) 719–775
Published: 3 August 2003

# Near-group categories

Jacob Siehler

**Abstract** We consider the possibility of semisimple tensor categories whose fusion rule includes exactly one noninvertible simple object. Conditions are given for the existence or nonexistence of coherent associative structures for such fusion rules, and an explicit construction of matrix solutions to the pentagon equations in the cases where we establish existence. Many of these also support (braided) commutative and tortile structures and we indicate when this is possible. Small examples are presented in detail.

**AMS Classification** 18D10

**Keywords** Monoidal categories, braided categories

## 1 Introduction and results

The term *near-group categories* is introduced to describe a specific class of finite semisimple monoidal categories with duality. For the purposes of the present paper:

*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

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

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

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

*Duality* means: every object $x$ has a dual object $x^*$. Moreover, there exist "pairing" and "copairing" morphisms $\lambda_x\colon x^* \otimes x \to \epsilon$ and $\Lambda_x\colon \epsilon \to x \otimes x^*$ 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 $\hom(x \otimes y, z) \cong \hom(x, z \otimes y^*)$ and $\hom(x, y \otimes z) \cong \hom(y^* \otimes x, z)$. As a special case, simples $s_i$ and $s_j$ have

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

Categories in which every simple has a multiplicative inverse (so $g \otimes g^{-1} \cong \epsilon$) have been studied carefully, and called variously $\Theta$*–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 non-commutative 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. The case where $k = 0$ is dealt with in [TY] and [S], so the present paper is concerned only with near-group fusion rules having $k \geq 1$.

The main results on monoidal structures are:

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

**1.2 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 $p^\alpha - 1$).*

To prove necessity, we examine in detail (sections 4 and 5) the pentagon equations in the category; we find that $G$ must support some special structure (4.2) and we show (6.1) that only the specified groups support this structure.

We give two different proofs of sufficiency. In 4.1 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 5.18. This uses the analysis of the pentagon equations carried out in sections 4 and 5 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 sections 8 and 9 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 Theorem** *The first three maximal-order cases have the following structure:*

| *Fusion* | $(\mathbb{Z}/2,1)$ | $(\mathbb{Z}/3,2)$ | $(\mathbb{Z}/4,3)$ |
|---|---|---|---|
| *Field* | $F_3$ | $F_{2^2}$ | $F_5$ |
| *Monoidal structures* | *3, indexed by $\xi$ where $\xi^3 = 1$* | *2, indexed by $\xi = \pm 1$* | *unique monoidal structure* |
| *Braidings* | *$\xi = 1$: 3, indexed by $\psi^3 = 1$*<br>*$\xi \neq 1$: not braided* | *$\xi = 1$: 4, indexed by $\psi(1), \psi(2) = \pm 1$*<br>*$\xi \neq 1$: not braided* | *unique braiding* |
| *Balance* | *$\psi = 1$: balanced*<br>*$\psi \neq 1$: not balanced* | *all balanced* | *balanced* |
| *Symmetry* | *$\psi = 1$: symmetric* | *$\psi(1) = \psi(2)$: symmetric*<br>*$\psi(1) = -\psi(2)$: not symmetric* | *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:

**1.4 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 $3 \bmod 4$*

**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 section 7. 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.

Section 8 reduces the hexagon equations and gives a standard construction of commutativity data. Section 9 then gives the braidings possible for the example categories from section 3, and this includes nonsymmetric braidings on the standard monoidal structures; it turns out that the more exotic monoidal structures exhibited in section 3 do not support braidings.

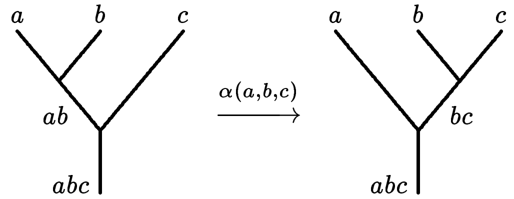
Section 10 gives a brief note on the possibility of adding twist morphisms to the braided near-group categories studied in sections 8 and 9 (producing "tortile categories").

## 2 Notation for associativities

In section 3 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 associativitities 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 $G$.

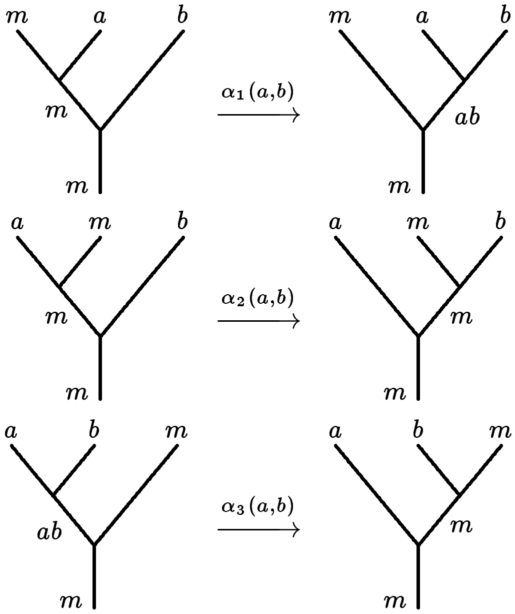
### 2.1 Associativities involving a product of three group elements

These we denote by a function $\alpha$ depending on three group variables.



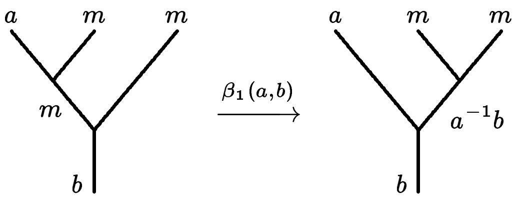

### 2.2 Associativities involving two group elements and one $m$

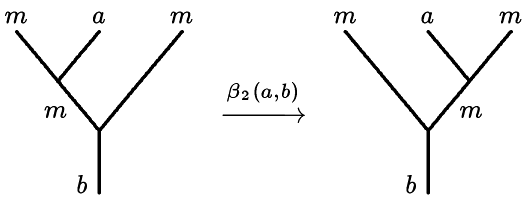
These we think of as a function of the two group elements, denoted by $\alpha$'s with a subscript to indiciate the position of the $m$:

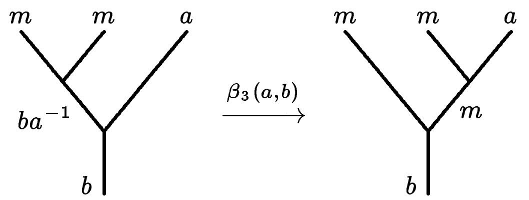



### 2.3 Associativities involving two $m$'s and one group element

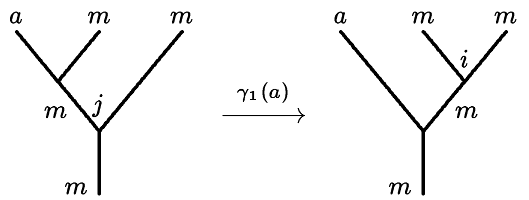
Such a product has both group summands and $m$ summands in it. We will use $\beta$'s to denote the associativity on the group summands:

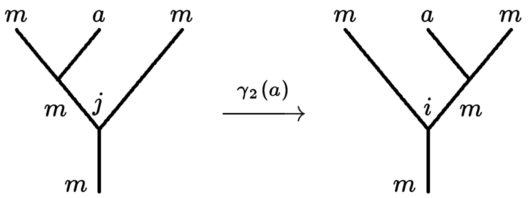


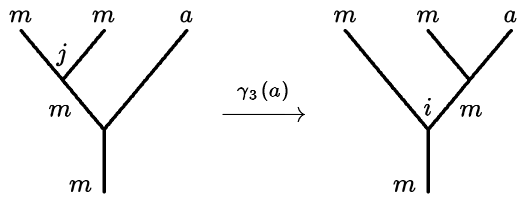



For the same kind of product, $\gamma$'s will denote the the associativity on the $m$ summands. These will take values in $k \times k$ matrices (rows indexed by $i = 1 \dots k$, columns indexed by $j = 1 \dots k$):

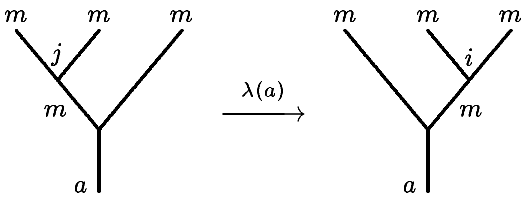


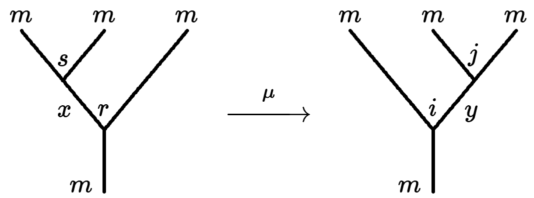




### 2.4 Associativities for a threefold product of $m$'s

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



Finally, $\mu$ stands for associativity on the $m$ summands; $\mu$ 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 $r,s=1\dots k$ when $x=m$. Similarly on the right:




## 3 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 section 5.18. The matrix construction is best explained using a permutation $\pi$ 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.

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

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

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

Let $\chi$ 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, $\mu$:

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

**Note** The construction in 5.18 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 Example 2 $k = 2, G = \mathbb{Z}/3\mathbb{Z} = \{\epsilon, g, g^2\}$

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

Let $\chi_1$ and $\chi_2$ 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 $\mu$:

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

**Note** The construction in 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.

### 3.3 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 $\pi$ is a nontrivial permutation, and is really the best illustration of the construction in 5.18.

Take $\pi$ to be the 3–cycle $\begin{pmatrix} g & g^1 & g^3 \end{pmatrix}$.

Let $\chi_1, \chi_2$, and $\chi_3$ 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 $\mu$ is given in four submatrices: the upper left "$M$ submatrix" corresponding to $x, y \in G$:

$$\begin{array}{cc}
x = & \begin{array}{cccc} \epsilon & g & g^2 & g^3 \end{array} \\
\begin{array}{c} y = \epsilon \\ g \\ g^2 \\ g^3 \end{array} & \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}
\end{array}$$

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

$$\begin{array}{r|ccccccccc}
(r,s) = & (1,1) & (1,2) & (1,3) & (2,1) & (2,2) & (2,3) & (3,1) & (3,2) & (3,3) \\
\hline
y=\epsilon & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 \\
g & 0 & 0 & \frac{1}{4}\chi_3(g^3) & 0 & \frac{1}{4}\chi_1(g^3) & 0 & \frac{1}{4}\chi_2(g^3) & 0 & 0 \\
g^2 & 0 & 0 & \frac{1}{4}\chi_3(g^2) & 0 & \frac{1}{4}\chi_1(g^2) & 0 & \frac{1}{4}\chi_2(g^2) & 0 & 0 \\
g^3 & 0 & 0 & \frac{1}{4}\chi_3(g) & 0 & \frac{1}{4}\chi_1(g) & 0 & \frac{1}{4}\chi_2(g) & 0 & 0
\end{array}$$

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

$$\begin{array}{r|cccc}
x = & \epsilon & g & g^2 & g^3 \\
\hline
(i,j) = (1,1) & 0 & 0 & 0 & 0 \\
(1,2) & 1 & \chi_1(g^3) & \chi_1(g^2) & \chi_1(g) \\
(1,3) & 0 & 0 & 0 & 0 \\
(2,1) & 1 & \chi_2(g^3) & \chi_2(g^2) & \chi_2(g) \\
(2,2) & 0 & 0 & 0 & 0 \\
(2,3) & 0 & 0 & 0 & 0 \\
(3,1) & 0 & 0 & 0 & 0 \\
(3,2) & 0 & 0 & 0 & 0 \\
(3,3) & 1 & \chi_3(g^3) & \chi_3(g^2) & \chi_3(g)
\end{array}$$

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: $\alpha$ and $\beta$ associativities are trivial; the $\gamma$'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 $\pi$.

Moreover, the large associator $\mu$ is predictably organized. The $M$ submatrix is constant. The $C$ submatrix has one nonzero row in each block (ie, one nonzero row for each $i = 1, 2, \ldots, k$), 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, $\pi$ can be viewed as acting on $\chi_1, \chi_2, \chi_3$ 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.

# 4 Pentagon equations and proof of Theorem 1.2

## 4.1 Proof of theorem 1.2: sufficiency

For each finite field $F_{p^\alpha}$, 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 $p^\alpha$ elements, and $F^*_{p^\alpha}$ for the multiplicative group. Let $\mathcal{G}$ be the semidirect product $F^+_{p^\alpha} \ltimes F^*_{p^\alpha}$ 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 $p^\alpha$.

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 1.2 follows. ◻

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

We will later (5.18) 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:

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

(i) $\pi^3 = id$

(ii) $\pi(x)^{-1} = \pi^{-1}(x^{-1})$

(iii) $\pi(st) = \pi(t)\pi\left[\pi(s)^{-1}\pi(t^{-1})\right]$ *(for all* $s \neq t^{-1}$*)*

Once we have established the intermediate theorem, we analyze (6.1) which groups $G$ support the structure of such a permutation $\pi$, completing the "only if" portion of Theorem 1.2. It is interesting to note that the factorization property (iii) on the permutation $\pi$ 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 $\hom(m, mm)$ 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 $\beta_3$ 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 $\hom(m, mm)$. 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 $a \otimes b \otimes c \otimes d$.

**4.3 Proposition** $\gamma_1$, $\gamma_2$, *and* $\gamma_3$ *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:

$$\gamma_3(b)\gamma_3(a) = \gamma_3(ab) \tag{1}$$
$$\gamma_1(b)\gamma_1(a) = \gamma_1(ab) \tag{2}$$
$$\gamma_2(b)\gamma_2(a) = \gamma_2(ab) \tag{3}$$

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

$$\gamma_3(b)\alpha_2(a,b)\gamma_1(a) = \gamma_1(a)\gamma_3(b) \tag{4}$$
$$\alpha_2(a,b)\gamma_3(b)\gamma_2(a) = \gamma_2(a)\gamma_3(b) \tag{5}$$
$$\gamma_2(b)\gamma_1(a)\alpha_2(a,b) = \gamma_1(a)\gamma_2(b) \tag{6}$$

□

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

**Proof** We choose basis of $\hom(m, mm)$ to split the representation $\gamma_1$ into $k$ linear summands, diagonalizing all $\gamma_1$ matrices. Now, equation (6) 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 $\alpha_2$ 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. □

**4.5 Proposition** *The representations $\gamma_1$, $\gamma_2^{-1}$, and $\gamma_3$ are all conjugate, and $\lambda(\epsilon)$ is an intertwiner carrying $\gamma_3$ to $\gamma_1$ to $\gamma_2^{-1}$ back to $\gamma_3$.*

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

$$\lambda(hg) = \gamma_3(g)\lambda(h) \tag{7}$$
$$\lambda(hg) = \lambda(h)\gamma_1(g) \tag{8}$$
$$\gamma_2(g)\lambda(h)\gamma_3(g) = \lambda(h)\beta_2(g,h) \tag{9}$$
$$\gamma_1(g)\lambda(h)\gamma_2(g) = \lambda(h)\beta_2(g,h) \tag{10}$$

By (7) with $h = \epsilon$, for any $g$ we have $\lambda(g) = \gamma_3(g)\lambda(\epsilon)$.

Now substitute into (8) with $h = \epsilon$ again to get $\gamma_1(g) = \lambda(\epsilon)^{-1}\gamma_3(g)\lambda(\epsilon)$, so $\lambda(\epsilon)$ carries $\gamma_3$ to $\gamma_1$. Take $h = \epsilon$ in the remaining equations to complete the remaining claims. □

**Notation for the associator $\mu$**

Recall from section 2.4 that $\mu$ 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 2.4. On the left, there are $|G|$ basis elements indexed by the elements of $G$, and $k^2$ elements indexed by pairs $(r,s)$ with $1 \le r,s \le k$. So think of the columns of $\mu$ as labeled either by a group element $g$ or a pair of indices $(r,s)$.

The parametrization on the right is similar so $\mu$ 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 $1 \le i,j,r,s \le k$, entries in $\mu$ 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 $\mu$ into submatrices $M$, $R$, $C$, and $N$ as follows:

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

Think of $\mu$ 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

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

**Remaining pentagons for products with three $m$'s**

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

Pentagon $mmmg/m$:

$$\mu[a,b]\alpha_2(b,g) = \mu[g^{-1}a,b]\alpha_1(g^{-1}a,g)\beta_3(g) \tag{11$M$}$$

$$r_a = \beta_3(g)r_{g^{-1}a}\left(\gamma_3(g)^{-1}\otimes \mathrm{ID}_k\right) \tag{11$R$}$$

$$\alpha_2(a,g)c_a = \left(\gamma_3(g)\otimes\gamma_3(g)\right)c_a \tag{11$C$}$$

$$\left(\gamma_3(g)\otimes\gamma_3(g)\right)N = N\left(\gamma_3(g)\otimes \mathrm{ID}_k\right) \tag{11$N$}$$

Pentagon $mmgm/m$:

$$\mu[a,b]\beta_2(g,a)\beta_3(g) = \mu[a,bg^{-1}] \tag{12M}$$
$$r_a\left(\gamma_2(g)\otimes\gamma_3(g)^{-1}\right) = \beta_2(g,a)r_a \tag{12R}$$
$$c_{g^{-1}a} = \beta_3(g)\left(\mathrm{ID}_k\otimes\gamma_2(g)\right)c_a \tag{12C}$$
$$\left(\mathrm{ID}_k\otimes\gamma_2(g)\right)N = N\left(\gamma_2(g)\otimes\gamma_3(g)^{-1}\right) \tag{12N}$$

Pentagon $mgmm/m$:

$$\mu[a,b]\beta_2(g,b) = \mu\left[g^{-1}a,b\right] \tag{13M}$$
$$r_{g^{-1}a} = r_a\left(\mathrm{ID}_k\otimes\gamma_2(g)\right) \tag{13R}$$
$$\left(\gamma_2(g)^{-1}\otimes\gamma_1(g)\right)c_a = \beta_2(g,a)c_a \tag{13C}$$
$$\left(\gamma_2(g)\otimes\gamma_1(g)^{-1}\right)N = N\left(\mathrm{ID}_k\otimes\gamma 2(g)\right) \tag{13N}$$

Pentagon $gmmm/m$:

$$\mu\left[a,g^{-1}b\right] = \mu[a,b]\alpha_2(g,b) \tag{14M}$$
$$r_a\left(\gamma_1(g)\otimes\gamma_1(g)\right) = \alpha_2(g,a)r_a \tag{14R}$$
$$c_{g^{-1}a} = \left(\gamma_1(g)\otimes\mathrm{ID}_k\right)c_a \tag{14C}$$
$$N\left(\gamma_1(g)\otimes\gamma_1(g)\right) = \left(\gamma_1(g)\otimes\mathrm{ID}_k\right)N \tag{14N}$$

**4.6 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 (13M) to get $\mu[g,\epsilon]=\mu[\epsilon,\epsilon]$ for all $g\in G$. By (14M), $\mu[g,h^{-1}h] = \mu[g,^{-1}h]\alpha_2(h,h)$; the claim follows. □

### 4.7 Proof of order-control theorem 1.1

By lemma 4.6, the $1\times|G|$ row vector $m_a = \big(\mu(a,b)\big)_b$ is actually independent of $a$ so we will write $\vec{m}$ for this common value.

Equation (11R) implies that $r_g = \beta_3(g)r_\epsilon\left(\gamma_3(g)^{-1}\otimes\mathrm{ID}_k\right)$ for all $g\in G$.

Thus the first $|G|$ rows of $\mu$ look like

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

Since $\mu$ 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 $|G| \leq k+1$. □

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

**Proof** Similar to lemma 4.6, equations (11M) and (12M) 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 4.4, 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 $\alpha_2$ is bimultiplicative.) Now, let $g = \epsilon$ in the above. □

# 5 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 result.

**5.1 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) *$\gamma_1, \gamma_2^{-1}$ and $\gamma_3$ 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 $i = 1 \ldots k$, then the $\chi_i$ 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 $\gamma_1$, $\gamma_2^{-1}$, and $\gamma_3$ are conjugate representations; it remains to show that all three can be simultaneously be diagonalized. Define $\theta$ on $G \times G \times G$ by

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

Equations (4) through (6) and $\alpha_2$ vanishing imply that $\theta$ is a homomorphism; we can therefore choose basis of $\hom(m, m \otimes m)$ so that $\theta$ splits as linear representations. Then of course $\gamma_1(g) = \theta(g, \epsilon, \epsilon)$ is diagonal for all $g$; similarly $\gamma_2$ and $\gamma_3$.

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

Claim (iv) follows from linear independence in the proof of theorem 1.1. □

**5.2 Corollary** *With respect to the basis given in 5.1, there is a permutation $\pi$ of order 3 in $S_k$ and constants $\xi(j)$ such that*

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

**Proof** Follows from 4.5 and 5.1 (iv). □

### 5.3 Remark

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

### Notation

By the numbering indicated in 5.1 (iv) we can think of an index $i$ in $\{1, 2, \dots, k\}$ as corresponding to one of the $k$ nontrivial characters of $G$. If we let $\chi_\epsilon$ 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 $\chi's$, there is an equivalent description using entries in $\gamma_1$ matrices: For $r, s \in \{1, 2, \dots, k\}$,

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

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 $\pi$ from 5.2 as acting on the nonidentity elements of $G$.

Precisely the same characters appear in the representation $\gamma_3$ although their order of appearence on the diagonal is permuted by the $\pi$ of lemma 5.2. We introduce an analogous operation $\circ$ on $\{\epsilon, 1, 2, \ldots, k\}$ by

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

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 $\pi$: If $r \circ s \neq \epsilon$, then

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

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:

**5.4 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 (14N), $N[(i,j);(r,s)]$ must be zero for all $(i,j)$. Linear independence of the columns of $\mu$ implies that $r_g[(r,s)] \neq 0$ for some $g \in G$, but (11R) 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 (14R),

$$r_g[(r,s)] = \gamma_1(g)_r \gamma_1(g)_s r_g[(r,s)]$$

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 (11N) and (11C) instead of (14N) and (14C). $\square$

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 $c_g[(i, i^{\circ -1})]$.

**5.5 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 (14N) implies $r*s=i$.

Conversely, suppose $r*s=i$ and $i\circ j=r$. By 5.4, $r_g[(r,s)]=0$ for all $g\in G$, so linear independence of the columns of $\mu$ 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 $N[(i,j);(r,s)]$. □

### 5.6 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 5.1(i). We write $N[-;(r,s)]$ for the entire $(r,s)$ column of $N$, and $N[(i,j);-]$ for the $(i,j)$ row.

$$\sum_{c\in G}\mu[a,c]\mu[c,b] + r_a\,(\lambda(g)\otimes \mathrm{ID}_k)\,c_b = \delta_{a,b^{-1}g} \tag{15$M$}$$

$$\sum_{c\in G}\mu[a,c]r_c[(r,s)] + r_a\,(\lambda(g)\otimes \mathrm{ID}_k)\,N[-;(r,s)] = 0 \tag{15$R$}$$

$$\sum_{c\in G}c_c[(i,j)]\mu[c,b] + N[(i,j);-]\,(\lambda(g)\otimes \mathrm{ID}_k)\,c_b = 0 \tag{15$C$}$$

$$\sum_{c\in G}c_c[(i,j)]r_c[(r,s)] + N[(i,j);-]\,(\lambda(g)\otimes \mathrm{ID}_k)\,N[-;(r,s)] = \lambda(g)[i,s]\lambda(g)[j,r] \tag{15$N$}$$

**5.7 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 (11R) and (14C). □

**5.8 Proposition** *The permutation $\pi$ from 5.2 satisfies $\pi(x^{-1}) * \pi^{-1}(x) = \epsilon$ (for any index $x$, $1\leq x\leq k$.)*

**Proof** In equation (15R) 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 5.7. Therefore,

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

by orthogonality of characters. So (15R) reduces to

$$r_a\left(\lambda(g) \otimes \mathrm{ID}_k\right) N[-;(r,s)] = 0$$

and in particular, for $g = a = \epsilon$,

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

By 5.5 this yields no useful information if $r * s = \epsilon$ so assume $r * s \neq \epsilon$. By 5.5, 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 $\pi$ manages to "line up" that nonzero entry from $N$ with one of the nonzero entries in $r_\epsilon$. But we know where the nonzero entries in $r_\epsilon$ live by 5.4. So if (15R) 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 (15R) 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,

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

□

**5.9 Proposition** *The permutation $\pi$ satisfies $\pi(s * t) = \pi(t) * \pi\left[\pi(s)^{-1} * \pi(t^{-1})\right]$ (for all $s \neq t^{-1}$)*

**Proof** Consider (15$N$) 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,

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

But for the lefthand side of (15$N$) to be nonzero, it must be that $i = \pi(r*s)*x$; since we have chosen $i = \pi(s)$, the following relation appears:

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

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. □

### 5.10 Proof of intermediate theorem 4.2

The results in 5.2, 5.8, and 5.9 establish Theorem 4.2: If a monoidal structure exists, then we can extract a permutation $\pi$ satisfying the three indicated properties. $\square$

In section 6 we will complete Theorem 1.2 by identifying which groups support such a $\pi$ 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 5.18.

### 5.11 Identifying primitive data

At this point we have reduced the problem of describing the categorical data to describing the associativities $\lambda(\epsilon)$ and $\mu$. We know the $\alpha$'s and $\beta$'s are trivial and we know that the $\gamma$'s contain all the nontrivial characters. All $\lambda(g)$ are determined once we know $\lambda(\epsilon)$ and the $\gamma$'s. The $\lambda(\epsilon)$ is described by the permutation $\pi$ and the function $\xi$ of 5.2; $\mu$ is described by $M$, $R$, $C$, and $N$ but $M$ is a constant block; all of $C$ can be generated given the function $c_\epsilon$. Likewise $R$ is described by the function $r_e$, 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 $r_\epsilon$ in terms of $c_\epsilon$ thus reducing the problem to specifying three functions $\xi$, $c_\epsilon$, and $N$.

**5.12 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 $r_\epsilon$ 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

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

Write $X$ for the involutive permutation matrix $\left(\delta_{a,b^{-1}}\right)_{a,b\in G}$ 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. □

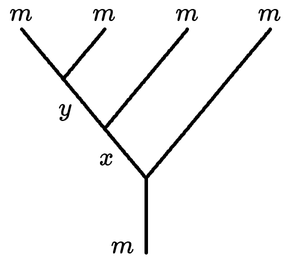
Moreover, examination of the first column on both sides implies $y^2|G|^{-1} = 1$, and we have

**5.13 Corollary** $\mu[\epsilon,\epsilon] = \pm 1/|G|$

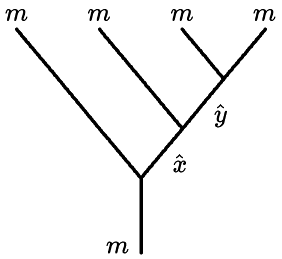
We introduce $\delta := |G|\mu[\epsilon,\epsilon] = \pm 1$ as this will occur frequently in subsequent equations.

### 5.14 The big pentagon: *mmmm/m*

Graphically, the bases for the full left and full right associated product have the form




or




respectively.

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:

$$\begin{array}{c} \\ {\scriptstyle \hat{x}\in G \atop \hat{y}=m} \\ {\scriptstyle \hat{x}=m \atop \hat{y}\in G} \\ \hat{x}=\hat{y}=m \end{array}
\begin{array}{c}
\begin{array}{ccc} {\scriptstyle x\in G \atop y=m} & {\scriptstyle x=m \atop y\in G} & x=y=m \end{array} \\
\left(\begin{array}{ccc}
(16) & (18) & (23) \\
(17) & — & (20),(21) \\
(22) & (18),(19) & (24)
\end{array}\right)
\end{array}$$

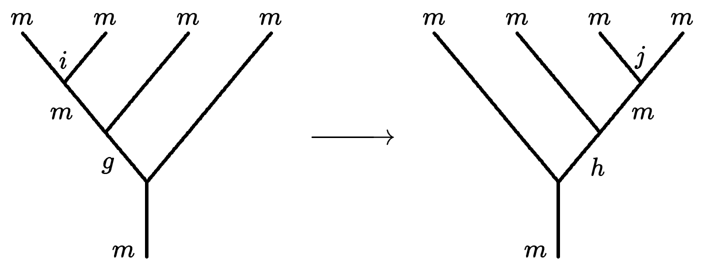
The table indicates which submatrix of the pentagon equation corresponds to which of the following constraints. We have used all reductions available to express these in the minimal number of variables: these are essentially functional equations in the functions $c_\epsilon$, $\xi$, and $N$, and they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

$$\begin{aligned}
c_\epsilon(i)c_\epsilon(\pi^{-1}(i))^{-1} &= \delta\xi(i^{-1})\xi(\pi(i^{-1}))\xi(\pi^{-1}(i)) && (16)\\
\xi(i)c_\epsilon(i) &= \delta\xi(\pi(i^{-1}))c_\epsilon(\pi(i^{-1})) && (17)\\
c_\epsilon(i) &= \delta c_\epsilon(\pi(i)^{-1}) && (18)\\
c_\epsilon(i) &= c_\epsilon(j)N(i*j^{-1},j) \\
&\qquad N(\pi(j)*\pi(i)^{-1},\pi(j)^{-1}) && (19)\\
\xi(i)c_\epsilon(i) &= \delta\xi(\pi(i^{-1}))c_\epsilon(\pi(i^{-1})) && (20)\\
\xi(\pi^{-1}(i)*\pi(j^{-1}))c_\epsilon(\pi^{-1}(i)*\pi(j^{-1})) &= \xi(\pi^{-1}(i))c_\epsilon(\pi^{-1}(i)) \\
&\qquad N(i,i^{-1}*j)N(i^{-1},j) && (21)\\
c_\epsilon(i)N(i,j) &= \xi(j)c_\epsilon(i*j)N(\pi(i*j)^{-1},\pi(j)) && (22)\\
\xi(\pi^{-1}(i))N(i,j)c_\epsilon(\pi^{-1}(i)) &= \xi\left(\pi(\pi^{-1}(j)*\pi(i)\right)\xi\left(\pi^{-1}(i*j))^{-1}\right) \\
&\qquad N(j,(i*j)c_\epsilon(\pi^{-1}(i*j)) && (23)\\
c_\epsilon\left((i*j)^{-1}\right)c_\epsilon(j)^{-1}\xi(j)^{-1} &= N\left(\pi^{-1}(i)*\pi(j),\pi(j)^{-1}\right) \\
&\qquad N\left(\pi^{-1}(i),\pi(j)\right) && (24)
\end{aligned}$$

**Note** The $y, \hat{y} \in G$ piece of the pentagon is automatically satisfied by the properties of the permutation $\pi$, without introducing any new relations. This will be illustrated in section 5.18 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.

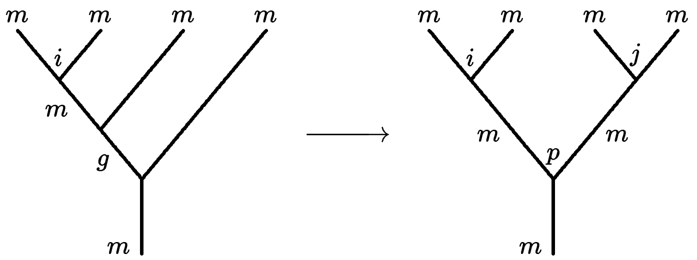
## 5.15 Derivation of equation (16)

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



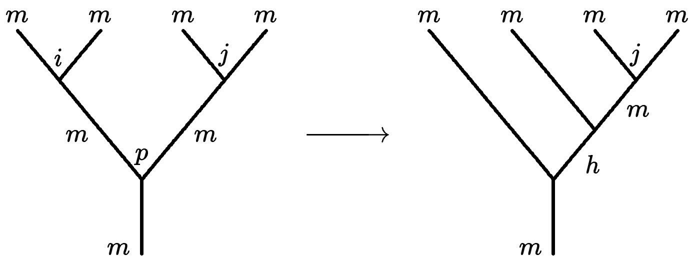
For each $g,h \in G$ we get a $k \times k$ submatrix of coefficients indexed by $i$ and $j$. Using the reductions available it is not difficult to compute these coefficients.

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




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

and the second step is

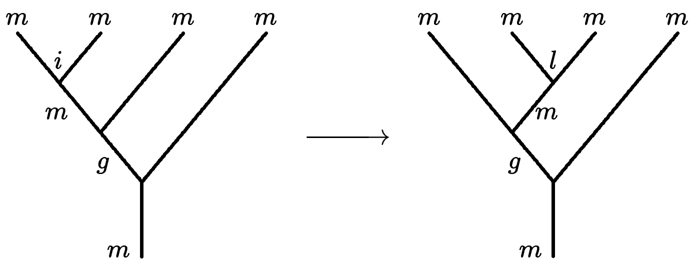



$$(m{\to}mm)_p \otimes (m{\to}mm)_i \otimes (m{\to}mm)_j$$
$$\overset{\alpha}{\longmapsto} r_h[p,i](m{\to}mh)\otimes(h{\to}mm)\otimes(m{\to}mm)_j + \text{irrelevant terms}$$

Therefore the $(j,i)$ coefficient is $\sum_p c_g[p,j]r_h[p,i]$. By 5.4 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

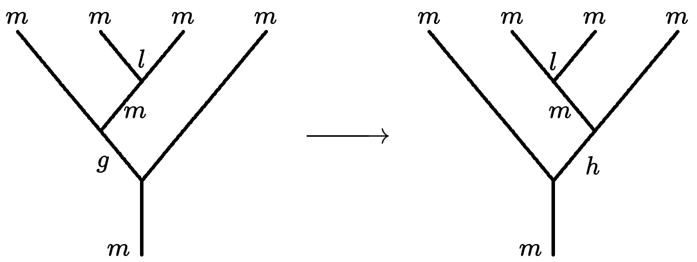
$$\left(c_g(i^{-1})r_g(i^{-1})\delta_{j,\pi^{-1}(i)}\right)_{j,i}$$

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



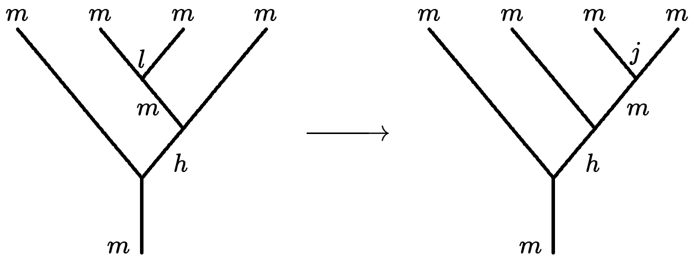
$$
\begin{aligned}
&(m\to gm)\otimes(g\to mm)\otimes(m\to mm)_i \\
&\qquad \xmapsto{\alpha} \sum_l \lambda(g)[l,i](m\to gm)\otimes(g\to mm)\otimes(m\to mm)_l
\end{aligned}
$$

From here,




$$
\begin{aligned}
&(m\to gm)\otimes(g\to mm)\otimes(m\to mm)_l \\
&\qquad \xmapsto{\alpha} \mu[h,g](m\to mh)\otimes(h\to mm)(m\to mm)_l + \text{irrelevant terms}
\end{aligned}
$$

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




$$
\begin{aligned}
&(m\to mh)\otimes(h\to mm)(m\to mm)_l \\
&\qquad \xmapsto{\alpha} \lambda(h)[j,l](m\to mh)\otimes(h\to mm)\otimes(m\to mm)_j + \text{irrelevant terms}
\end{aligned}
$$

so the submatrix from this path is

$$
\begin{aligned}
&\mu[\epsilon,\epsilon]\lambda(h)\lambda(g) \\
&\qquad = \mu[\epsilon,\epsilon]\lambda(\epsilon)\gamma_1(h)\lambda(\epsilon)\gamma_1(g) \quad \text{by 4.5}
\end{aligned}
$$

and the requirement of the pentagon equation is that

$$
\mu[\epsilon,\epsilon]\lambda(\epsilon)\gamma_1(h)\lambda(\epsilon)\gamma_1(g) = \left(c_g(i^{-1})r_h(i^{-1})\delta_{j,\pi^{-1}(i)}\right)_{j,i} \tag{16'}
$$

**Claim** (16′) *for arbitrary $g$ and $h$ follows from the case $g=h=\epsilon$*

**Proof** The matrix product on the left is

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

So (16′) can be written as

$$\mu[\epsilon,\epsilon]\xi(i)\xi(\pi(i))\chi_i(g)\chi_{\pi(i)}(h) = c_g(i^{-1})r_h(i^{-1}) \quad \forall i \tag{16''}$$

But $c_g(i^{-1}) = c_\epsilon(i^{-1})\chi_i(g)$ by $(14C)$. 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. □

Now 5.12 replaces the $r_\epsilon$ with an equivalent expression in $c_\epsilon$,

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

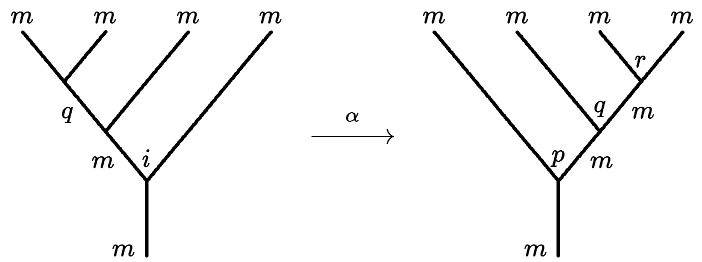
Rearrange:

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

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

### 5.16 Derivation of equations (18) and (19)

Graphically, we are interested in the following basis elements:




Following the two-step path in the pentagon, first

$$(m{\to}mm)_i \otimes (m{\to}gm) \otimes (g{\to}mm)$$
$$\qquad \xmapsto{\alpha} \gamma_1(g)[r,i](m{\to}gm) \otimes (g{\to}mm) \otimes (m{\to}mm)_r + \text{irrelevant terms}$$

and then

$$(m{\to}gm) \otimes (g{\to}mm) \otimes (g{\to}mm)_r$$
$$\qquad \xmapsto{\alpha} \mu[(p,q);g](m{\to}mm)_p \otimes (m{\to}mm)_q \otimes (m{\to}mm)_r + \text{irrelevant terms}$$

So the total coefficient from this path is simply

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

Following the three-step path, first

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

then

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

and

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

while

$$\begin{aligned}(m{\to}mm)_i&\otimes(m{\to}mm)_j\otimes(m{\to}mm)_l\\ &\overset{\alpha}{\longmapsto}\sum_s\mu[(p,s);(i,j)](m{\to}mm)_p\otimes(m{\to}mm)_s\otimes(m{\to}mm)_l+\text{irrel. terms}\end{aligned}$$

and

$$\begin{aligned}(m{\to}mm)_p&\otimes(m{\to}mm)_s\otimes(m{\to}mm)_l\\ &\overset{\alpha}{\longmapsto}\mu[(q,r);(s,l)](m{\to}mm)_p\otimes(m{\to}mm)_q\otimes(m{\to}mm)_r+\text{irrelevant terms}\end{aligned}$$

So the total coefficient from this path is

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

and the requirement of the pentagon is that

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

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 (14C) and (12C) to replace the $c_g$ and $c_h$ terms with expressions in $c_\epsilon$:

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

If $r \neq i$ the lefthand side vanishes since $\gamma_1$ 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 $q = i^{\circ -1}$, so the only requirement here is

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

which is precisely equation (18).

**Case II** $i \neq p$ In this case the first summation vanishes because $\gamma_2$ is diagonalized, and we are left with

$$c_g(p,q)\gamma_1(g)[r,i] = \sum_{j,l,s}\mu[(q,r);(s,l)]\mu[(p,s);(i,j)]\mu[(j,l);g] \tag{25}$$

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 $\gamma_1$, the lefthand side is nonzero iff

$$p = q^{\circ -1} \text{ and } r = i \tag{26}$$

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

$$q \circ r = s \tag{27i}$$
$$s * j^{\circ -1} = q \tag{27ii}$$
$$p \circ s = i \tag{27iii}$$
$$i * j = p \tag{27iv}$$

**Claim:** The conditions of (26) are equivalent to the conditions of (27).

**Proof** Assume (26), guaranteeing the lefthand side is nonzero. In order to satisfy (27iii) and (27iv) we must take

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

This $s$ and $j$ clearly satisfy (27i); with a little more work we verify that (27ii) 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, supppose the conditions of (27) are satisfied. Then we simply repeat the above calculation to show that $q = p^{\circ-1}$. It follows from (27i) and (27iii) that $i = r$, so both conditions of (26) are satisified. □

Therefore in considering the requirements of (25) 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 (14C) and cancelling $\gamma$'s, this reduces further to

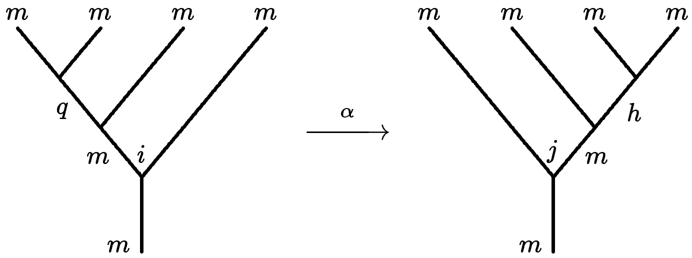
$$c_\epsilon(p) = N[p^{\circ-1} \circ i, (p^{\circ-1} \circ i)^{-1} * p^{\circ-1})]N[i, i^{-1} * p]c_\epsilon(p * i^{-1})$$

which, after a change of variable, is precisely equation (19), and we have completed showing that equations (18) and (19) completely describe the requirements of this piece of the pentagon. □

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 $\pi$ already established, and we will now prove that.

### 5.17 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

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

But then

$$\begin{aligned} l * q &= (j^{\circ-1}\circ i) * (i^{-1} * j)^{\circ-1} \\ &= \pi\left[\pi(j^{-1}) * \pi^{-1}(i)\right] * \pi\left[i^{-1} * j\right]^{-1} \\ &= \pi(j)^{-1} \quad \text{by 5.9} \\ &\neq \epsilon \end{aligned}$$

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. □

### 5.18 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 $\pi$ 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 $\chi_1,\ldots,\chi_k$ be the nontrivial characters of $G$, and choose an identification of $G$ with its dual group of characters so that $\pi$ can be regarded as permuting the characters.

For indices $i, j, r$ write $i * j = r$ provided $\chi_i \chi_j = \chi_r$; write $i * j = \epsilon$ 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:

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

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

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

At this point we have defined all associativities except $\mu$ and it clear that pentagon equations (1)–(10) 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 $\mu$.

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

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

Equations (11M–14M) are clearly satisfied by construction.

(14C) is clearly satisfied by construction. For (13C), check:

$$\left(\left(\gamma_2(g)^{-1} \otimes \gamma_1(g)\right) c_g\right)[(i,j)] = \chi_{\pi(i)}(g)\chi_j(g)c_g(i,j)$$

so if $j \neq i^{\circ -1} = \pi(i)^{-1}$ then $c_g(i,j) = 0$ and (13C) is satisfied; if $j = i^{\circ -1}$ then $\chi_{\pi(i)}(g)\chi_j(g) = 1$ and (13C) is still satisfied. Verifying (12C) and (11C) is similar.

(11R) is clearly satisfied by construction.

Check that (12R) is satisfied: for $a, g \in G$,

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

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

Check that (13R) is satisfied: This is trivial for $r \neq s^{-1}$, so assume $r = s^{-1}$. By property (ii) of $\pi$, then, $\pi(s) = \pi^{-1}(r)^{-1}$, so for any $a, g \in G$,

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

so (13R) is satisfied. Checking (14R) is similar to (12R), so details are omitted.

(11N) 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 (11N) is satisfied; if $i \circ j = r$ then $\chi_{\pi^{-1}(i)}\chi_{\pi^{-1}(j)} = \chi_{\pi^{-1}(r)}$ so (11N) is satisfied in that case as well.

(12N) 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 $\pi$ to massage this expression:

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

therefore

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

therefore in this case $\chi_{\pi(j)^{-1}} = \chi_{\pi(r)^{-1}}\chi_{\pi^{-1}(s)^{-1}}$ and equation (12N) is satisfied.

Checking (13N) is similar to (12N) and checking (14N) is similar to (11N) so details are omitted.

Check for (15M): by construction,

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

and

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

So we can compute

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

whence

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

and

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

so (15M) is satisfied.

Verifications of (15C) and (15R) are similar and easy. We will check that (15C) 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

$$N[(i,j);-]\,(\lambda(g) \otimes \mathrm{ID}_k))\,c_b = 0$$

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 (15C) 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:

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

so the $\delta$ kills off every summand where $N[(i,j);(r,s)]$ is nonzero. That completes the check that (15C) is satisfied and (15R) is obviously very similar.

Checking (15N): Recall this equation requires that

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

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:

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

Second calculation: By construction $N[(i,j);-]\,(\lambda(g) \otimes \mathrm{ID}_k)\, N[-;(r,s)]$ 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 $r \neq s^{-1}$. For any indices $p$ and $q$,

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

Therefore,

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

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

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

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 $s$:

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

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

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

Now we will proceed to verify equality in (15N). 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 (15N) 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 (15N) 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 (15N), all terms in the summation are zero, whereas by second calculation the term involving $N$'s gives precisely $\chi_{r*s}(g)$, so (15N) 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)** Suppose $i \neq j^{\circ -1}$ or $r \neq s^{-1}$. In this case every term of the summation is clearly zero.

**Case II, part (ii)** Suppose $i = j^{\circ -1}$ 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 (15N).

This completes the verification of (15N) 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 (16)–(24). However, our construction makes the functions $c_\epsilon$, $\xi$, and $N$ which we use to express those equations all identically 1, giving a trivial solution to equations (16)–(24). With this observation we complete the verification that all pentagon equations in the category are satisfied and we have constructed a coherent monoidal structure. □

The example data for $k = 1, 2, 3$ in section 3 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.

## 6 Groups that support a $\pi$

In this section we characterize the groups and permutations satisfying the hypotheses of Theorem 4.2. For reference: the hypotheses are that $\pi$ is a permutation on the nonidentity elements of $G$, satisfying

(i) $\pi^3 = \mathrm{id}$

(ii) $\pi(x)^{-1} = \pi^{-1}(x^{-1})$

(iii) $\pi(st) = \pi(t)\pi\big[\pi(s)^{-1}\pi(t^{-1})\big]$ (for all $s \neq t^{-1}$)

The result is:

**6.1 Theorem** *A finite abelian group $G$ admits a permutation $\pi$ 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:

**6.2 Lemma** *Suppose $G, \pi$ 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 $\pi$. Properties (i) and (ii) are also used to simplify. Let $s \neq t^{-1}$ be any nonidentity elements in $G$.

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

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 $\omega$. (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 $\omega = \omega^{-1}$. □

**Note** It may be the case that $\omega = \epsilon$.

Now we can proceed with the main result.

**Proof of 6.1** 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 $G, \pi$ 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:

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

The element $\omega$, 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,

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

On the other (the right) hand,

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

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

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

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

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

and putting it all together we have obtained

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

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. □

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

# 7 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 $\epsilon$ and a noninvertible $m$; the fusion rule is described by $m \otimes m = \epsilon \oplus km$. There are two nontrivial associativity morphisms, $\lambda\colon \hom(\epsilon, (mm)m) \to \hom(\epsilon, m(mm))$ and $\mu\colon \hom(m, (mm)m) \to \hom(m, m(mm))$. These have to satisfy two pentagon equations: $mmmm/\epsilon$ and $mmmm/m$. 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 $mmmm/\epsilon$ pentagon is formulated as a $(k^2+1)\times(k^2+1)$ matrix equation. Write $\mathrm{ID}_k$ for a $k \times k$ identity matrix, and $X_k$ for the matrix which operates on basis $\{e_i \otimes e_j\}_{i,j=1\ldots k}$ by tensor flip: $X_k\colon e_i \otimes e_j \mapsto e_j \otimes e_i$. Write $\lambda'$ for the block matrix $(1) \oplus (\lambda \otimes \mathrm{ID}_k)$. With this notation, the pentagon equation is

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

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

$$M^2L^k = L^{2k}\det(X_k) \tag{25}$$

The $mmmm/m$ 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

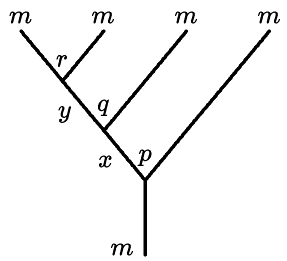
$$P_1 = \begin{pmatrix} 0 & \mathrm{ID}_k & 0 \\ \mathrm{ID}_k & 0 & 0 \\ 0 & 0 & \mathrm{ID}_{k^3} \end{pmatrix}$$

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

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

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

$$\begin{aligned} A &= \lambda \oplus (\mathrm{ID}_k \otimes \mu) \quad \text{and} \\ B &= \mathrm{ID}_k \oplus (\mu \otimes \mathrm{ID}_k) \end{aligned}$$

then the large pentagon $mmmm/m$ 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

$$(LM^k)^2 = M^k (-1)^k (\det X_k)^k \tag{26}$$

**7.1 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 $e_i \otimes e_j - e_j \otimes e_i$, $1 \le i < j \le k$. The dimension will be even, hence $\det X_k = +1$, iff $4|k$ or $4|(k-1)$. □

**7.2 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 25 and 26 reduce to

$$L^2 = M^{-2r}$$
$$M^2 = (-1)L^{2r}$$

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

**Case II** $k \equiv 3 \pmod 4$ In this case equations 25 and 26 reduce to

$$L^2 = M^{-k}$$
$$M^2 = (-1)L^k$$

whence $L^{k^2+4} = -1$. □

**7.3 Lemma** *$\mu[\epsilon, \epsilon]$ is invertible.*

**Proof** This a consequence of duality assumptions (explained in the introduction). We have assumed the existence of a map $\lambda_m$ such that

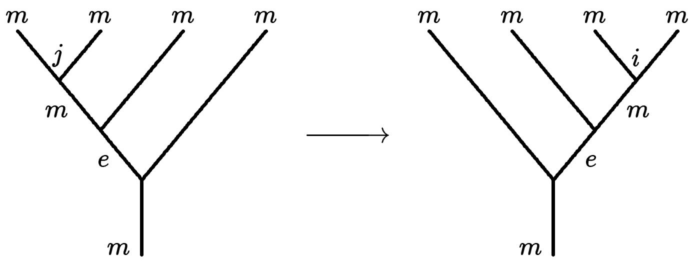
$$m \to \epsilon m \to (mm)m \xrightarrow{\mu} m(mm) \xrightarrow{1\otimes\lambda_m} m\epsilon \to m$$

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

**7.4 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

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

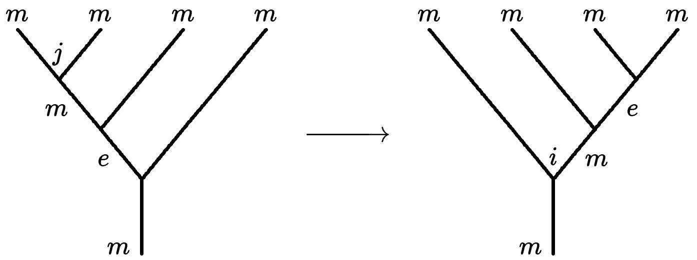
If we define $k \times k$ matrices $\mu_R$ and $\mu_C$ as follows:

$$\mu_R[i, j] = \mu[\epsilon; (i, j)]$$
$$\mu_C[i, j] = \mu[(j, i); \epsilon]$$

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

$$\mu_C \mu_R = \mu[\epsilon, \epsilon]\lambda^2 \tag{27}$$

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




This piece gives us

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

which we can reformulate as a matrix equation:

$$\mu_C^T \mu_R \lambda = \mu[\epsilon, \epsilon]\mathrm{ID}_k \tag{28}$$

By previous proposition, $\mu[\epsilon, \epsilon]$ is invertible. So we can combine (27) and (28), 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. $\square$

### 7.5 Proof of theorem 1.4

By 7.2, 7.4, and the hypothesis that the ground ring $R$ has characteristic other than 2, the pentagon equations admit no solution when $k \equiv 2$ or $3 \pmod 4$. $\square$

## 8 Additional structures I: commutativity

With sections 3 through 5 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 5.18 always admits a (symmetric) commuting structure.

Throughout this section we will assume we are in the setting of theorem 1.2 and have chosen bases so that all the reductions of sections 4 and 5 are in effect.

### 8.1 Notation for commutativity

This is a slight extension of the notation used previously in [S]. For $g, h \in G$, the commuting isomorphisms are:

$gh \to hg$ is multiplication by $\sigma_0(g,h)$
$gm \to mg$ is multiplication by $\sigma_1(g)$
$mg \to gm$ is multiplication by $\sigma_2(g)$
$mm \to mm$ is multiplication by $\sigma_3(g)$ on the $g$ summand

and commutativity on the $m$ summands of $m \otimes m$ is represented by a $k \times k$ matrix $\sigma_4$.

### 8.2 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:

$$\sigma_0(a,c)\sigma_0(a,b) = \sigma_0(a,bc) \tag{$abc/abc$}$$

Hexagons for products with one $m$:

$$\sigma_1(a)\sigma_0(a,b) = \sigma_1(a) \tag{$abm/m$}$$
$$\sigma_0(a,b)\sigma_1(a) = \sigma_1(a) \tag{$amb/m$}$$
$$\sigma_2(b)\sigma_2(a) = \sigma_2(ab) \tag{$mab/m$}$$

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

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

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

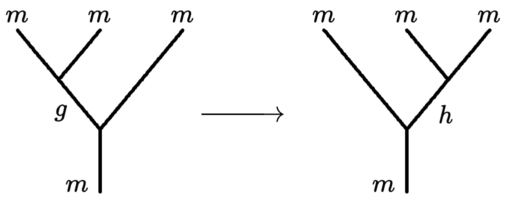
$$\sigma_2(a)\gamma_3(a)\sigma_4 = \gamma_2(a)\sigma_4\gamma_3(a) \tag{$mma/m$}$$
$$\sigma_4\gamma_1(a)\sigma_2(a) = \gamma_1(a)\sigma_4\gamma_2(a) \tag{$mam/m$}$$
$$\sigma_1(a)\gamma_2(a)\sigma_1(a) = \gamma_3(a)\sigma_1(a)\gamma_1(a) \tag{$amm/m$}$$

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

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

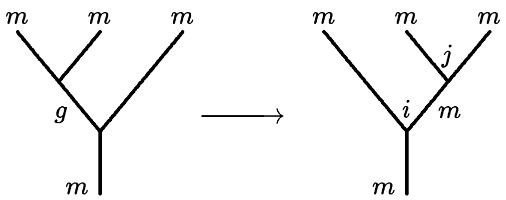
The hexagon for $m$ summands in a product of three $m$'s we break into individual entries in the matrices.

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



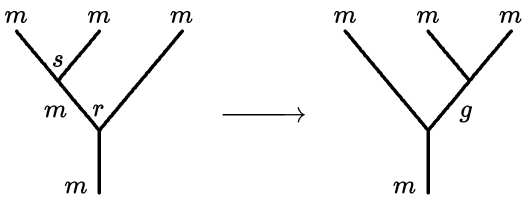

$$\sigma_3(g)\mu[h,g]\sigma_3(h) = \sum_{a\in G}\mu[a,g]\sigma_2(a)\mu[g,a] + \sum_{i,j,p}\mu[(i,j);g]\sigma_4[p,i]\mu[h;(p,j)]$$

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



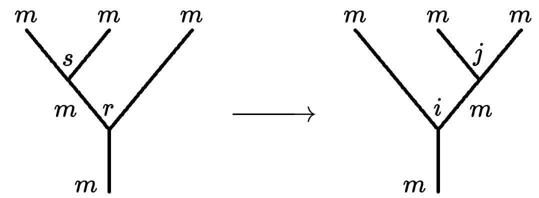

$$\sum_p \sigma_3(g)\mu[(i,p);g]\sigma_4[j,p] = \sum_{a\in G}\mu[a,g]\sigma_2(a)\mu[(i,j);a] + \sum_{r,s,t}\mu[(r,s);g]\sigma_4[t,r]\mu[(i,j);(t,s)]$$

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



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

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




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

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.

### 8.3 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 $\sigma_1, \sigma_2$ must both be equal to a distinguished linear character of $G$. Then $\sigma_3$ is entirely determined up to the value of $\sigma_3(\epsilon)$, and happily, the $\sigma_4$ matrix admits considerable simplification as well.

### 8.4 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:

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

From the $mab/m$ hexagon it's now clear that $\sigma_1$ and $\sigma_2$ are linear characters of $G$. Our next result sharpens that statement. By the results of section 7, we know there is a unique character $\chi_\omega$ 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. □

**8.5 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 $\gamma$'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. □

**8.6 Proposition** ($\sigma_4$ Structure) *There are invertible constants $\psi(1), \ldots, \psi(k)$ such that the matrix $\sigma_4$ 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 $\sigma_4$ tells us that $\sigma_4[i,j]$ is nonzero (moreover, invertible) iff $i = \pi(j^{-1})$. □

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

**8.7 Proposition** *All of the $mmm/g$ hexagons are satisified iff the constants $\psi$ 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,

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

while on the right,

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

All the $\chi$'s cancel and the proposition follows. □

### 8.8 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.

### 8.9 Reducing the $mmm/m$ hexagon, part II

On the lefthand side,

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

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:

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

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:

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

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

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

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

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

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

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

## 8.10 Reducing the $mmm/m$ hexagon, part III

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

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

On the right, the first summation is

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

The second summation is

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

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

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

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

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

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

and

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

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 $\xi$'s.

## 8.11 Reducing the $mmm/m$ hexagon, part IV

On the left,

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

On the right, the first summation is

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

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

$$\begin{array}{cc} r = p\circ q & p = r*s \\ t = i\circ j & i = t*q \\ \multicolumn{2}{c}{t = \pi(p^{-1})} \end{array}$$

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

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

but in terms of $i$ and $j$ we must have

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

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 $s$:

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

and the conclusion is

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

Now we can solve for $r$ as well:

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

and so the complete reduction of the second summation is:

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

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

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

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

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

So our final version of the hexagon in this case is

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

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

$$\begin{aligned} \psi(s)\psi & \left(\pi^{-1}(s^{-1} * \pi(r))\right) N(r, \pi(s^{-1})) \\ &= N(r,s)\psi(r*s)N\left(\pi\left((r*s)^{-1}\right), \pi(s) * \pi(r*s)^{-1}\right) \end{aligned}$$

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 section 5, 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:

**8.12 Proposition** *Suppose near-group fusion rule $(G,k)$, $|G| = k+1$, has a monoidal structure described by $\xi, c_\epsilon$, 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) $\sigma_4(g) = \left(\psi(j)\delta_{i,\pi(j^{-1})}\right)_{i,j}$ *where* $\sigma_3(\epsilon)$ *and* $\psi(1),\ldots,\psi(k)$ *are invertible constants.*

**Proof** Summary of results up to this point. □

If we want to construct a braiding, therefore, 8.12 gives a recipe for the commuting maps in terms of constants $\sigma_3(\epsilon)$ and $\psi(1),\ldots,\psi(k)$. The following summarizes the constraints on those constants.

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

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

$$\psi(r)\psi(\pi(r)^{-1})\xi(\pi(r^{-1})) = \sigma_3(\epsilon)\xi(r)\xi(\pi(r)) \tag{29}$$

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

$$\begin{aligned}\psi(r^{-1})\psi(\pi^{-1}(r * \pi(r)))N(r,\pi(r)) \\ = \left(\xi(\pi^{-1}(r)c_\epsilon(\pi^{-1}(r))\right)^{-1} c_\epsilon(r * \pi(r))\end{aligned} \tag{30}$$

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

$$\psi(s)\psi\left(\pi^{-1}(s^{-1} * \pi(r))\right) N(r, \pi(s^{-1})) \\ = N(r,s)\psi(r * s)N\left(\pi\left((r * s)^{-1}\right), \pi(s) * \pi(r * s)^{-1}\right) \quad (31)$$

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

$$\sigma_3(\epsilon)^2 = \delta \quad (32)$$

$$\sigma_3(\epsilon)\psi(\pi(r)^{-1}) = \psi(r)N\left(\pi(r^{-1}), \pi^{-1}(r^{-1})\right) \quad (33)$$

For $|G|$ even,

$$\sigma_3(\epsilon)^2 = \psi(\omega)\xi(\omega)^{-1} \quad (34)$$

$$\sigma_3(\epsilon)\psi(\pi^{-1}(\omega)) = 1 \quad (35)$$

$$\sigma_3(\epsilon)\psi(\pi(r)^{-1}) = \psi(\omega * r)N\left(\pi(\omega * r^{-1}), \pi^{-1}(\omega * r^{-1})\right), \quad \text{for } r \neq \omega \quad (36)$$

$$\sigma_3(\epsilon)\psi(\pi^{-1}(r))\xi\left(\omega * r\right) c_\epsilon\left(\omega * r\right) \\ = \xi\left(r\right) c_\epsilon\left(r\right) \psi\left(\omega * r^{-1}\right) N\left(\pi(r), \pi^{-1}(r)\right), \quad \text{for } r \neq \omega \quad (37)$$

**Proof** Equations (29)–(31) come from 8.7 and 8.11. Equations (32) and (33) come from 8.8 and 8.9. Equations (34)–(37) come from 8.8, 8.9, and 8.10, with minor change of indices to make the present list appear consistent. □

**8.14 Proposition** *The standard monoidal solution constructed in 5.18 admits a symmetric commuting structure.*

**Proof** This is now a triviality. The standard monoidal solution corresponds to taking $\xi, c_\epsilon$, and $N$ all identically equal to 1. Now we can satisfy the constraints listed in 8.3 by setting $\sigma_3(\epsilon) = \psi(1) = \cdots = \psi(k) = 1$ 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 $\sigma_4 = \left(\delta_{i,\pi(j^{-1})}\right)_{i,j}$ 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. □

# 9 Examples of braidings

## 9.1 Example 1 $k = 1, G = \mathbb{Z}/2\mathbb{Z}$

From section 3, there are three monoidal structures, corresponding to a choice of $\xi$ 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:

**9.2 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 7.13 we see that 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 (29), (34), and (35), respectively; none of the remaining equations from 8.13 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 $\chi$ is the nontrivial character of $G$ and $a \in G$. □

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

From section 3 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:

**9.4 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 8.13, and using the monoidal data, we see the requirements of the hexagon axiom are as follows. From equation (29),

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

From equation (30),

$$\psi(2)^2 = 1$$
$$\psi(1)^2\xi = 1$$

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

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

and from (33),

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

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 $a \in G$. □

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

From section 3, this fusion rule has a unique monoidal structure, which is described by taking $\xi, c_\epsilon$, and $N$ all identically 1. As it turns out, the commutative structure is unique as well.

**9.6 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 8.13, and using the monoidal data, we get the following constraints. From (29) with $r = 1, 2, 3$, respectively:

$$\psi(1)\psi(2) = \sigma_3(\epsilon) \qquad \psi(2)\psi(1) = \sigma_3(\epsilon)$$
$$\psi(3)^2 = \sigma_3(\epsilon)$$

From (30) with $r = 1, 2$:

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

From (31) with $(r, s) = (2, 1), (3, 2)$:

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

From (34) and (35),

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

And from (36),

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

Since the monoidal data is trivial, equation (37) is equivalent to (36). 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 $mmm/\epsilon$) 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:

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

where $\chi_\omega$ is the nontrivial order 2 character and $a \in G$. □

## 10 Additional structures II: 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 1.2 (useful for invariants of framed links). We need endomorphisms $\theta_s$ 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:

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

This is simple to work out for the small example categories we have studied in sections 3 and 9, but interesting since it gives a few examples of non-symmetric braidings that do or do not admit braidings. We say a braiding is balanced if there is a $\theta_m$ satisfying the twist equations above.

**10.1 Proposition** (Twist, $k = 1, G = \mathbb{Z}/2\mathbb{Z}$) *In the setting of theorem 9.2, 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 8.2 together with the twist equations above implies $\psi = 1$ immediately. □

**10.2 Proposition** (Twist, $k = 2, G = \mathbb{Z}/3\mathbb{Z}$) *In the setting of theorem 9.4, 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. □

## References

[FK] **J Frolich**, **T Kerler**, *Quantum Groups, Quantum Categories, and quantum field theory*, Springer–Verlag (1993)

[KR] **R M Kashaev**, **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)

[TY] **D Tambara**, **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`

*Department of Mathematics, Virginia Tech*
*Blacksburg, VA 24061-0123, USA*
Email: `jsiehler@math.vt.edu`

Received: 8 November 2002