AUTOMORPHISMS OF THE DOUBLES OF PURELY NON-ABELIAN FINITE GROUPS

MARC KEILBERG

Abstract. Using a recent classification of \( \text{End}(D(G)) \), we determine a number of properties for \( \text{Aut}(D(G)) \), where \( D(G) \) is the Drinfel’d double of a finite group \( G \). Furthermore, we completely describe \( \text{Aut}(D(G)) \) for all purely non-abelian finite groups \( G \). A description of the action of \( \text{Aut}(D(G)) \) on \( \text{Rep}(D(G)) \) is also given. We are also able to produce a simple proof that \( D(G) \cong D(H) \) if and only if \( G \cong H \), for \( G \) and \( H \) finite groups.

Contents

Introduction 1
Acknowledgments 4
1. Preliminaries 4
2. Essential properties of \( p \) and \( u \) 6
3. Flippable Homomorphisms 11
4. Some subgroups of \( \text{Aut}(D(G)) \) 14
5. Main Result 19
6. Restriction to group-likes 23
7. Exact factorizations and semidirect products for \( \text{Aut}(D(G)) \) 26
8. Action on modules 32
References 36

Introduction

The aim of this paper is to investigate the structure of Hopf automorphisms of \( D(G) \), where \( D(G) \) is the Drinfeld double of a finite group \( G \). We will be able to give a complete description when \( G \) is purely non-abelian, meaning that \( G \) has no non-trivial abelian direct factors. The original motivation for this came from [8], where it was observed that the automorphisms of a semisimple Hopf algebra \( H \) permute its irreducible characters in a way that preserves all higher Frobenius-Schur indicators [10]. This provides the ability to reduce the number of indicator computations actually performed, provided one has a reasonably
robust and efficient way of computing the automorphisms and their action on irreducible modules. Precise computation of indicator values has remained a difficult problem, relying on either computers or especially well-behaved groups [8, 11, 12, 17, 18]. Some advances in this direction were made in [14], which provides an integrality test, but it remains unclear how to predict integrality with complete certainty, or how to predict negative indicators— in particular modules $V \cong V^*$ with a skew-symmetric form [19]— even when integrality is assured.

Automorphisms of Hopf algebras and quantum groups have been studied in several other works, including [2, 3, 4, 5]. Radford [22] showed that Aut($H$) is finite over a field of characteristic zero when $H$ is semisimple, as well as in finite characteristic with certain additional assumptions. Recently, Sage and Vega [24] used Aut($H$) to give a new, extended notion of higher Frobenius-Schur indicators [16], and applied their methods to $H_8$. In [2], a classification of bicrossed products of Hopf algebras and their morphisms is provided. The automorphisms of the quantum groups $H_{4n,\omega}$ were completely determined by these methods, in particular. This classification of morphisms plays a central role in our investigations of Aut($\mathcal{D}(G)$).

All groups will be finite, and we work over an algebraically closed field $\mathbb{C}$ of characteristic zero, unless otherwise indicated. We use $\delta_{x,y}$ as the Kronecker delta symbol. All homomorphisms and automorphisms are of Hopf algebras or groups, as appropriate, unless otherwise noted. We denote the $\mathbb{C}$-linear dual of a group $G$ by $\mathbb{C}G$, with dual basis $\{e_g\}_{g \in G}$. We denote the group-like elements of $\mathbb{C}G$ by $\hat{G}$, which we identify with the usual group of irreducible linear characters. We identify Hom($G, \hat{G}$) with the group of $\mathbb{C}$-bilinear bicharacters $G \times G \to \mathbb{C}^*$ in the usual way. We denote all identity elements and trivial subgroups by 1 when there can be no confusion, with the exception of $\hat{G}$ and $\mathbb{C}G$, whose identities we write as $\varepsilon$. When $K$ is a normal subgroup of $G$, we write $K \triangleleft G$.

We denote the conjugation actions of $G$ on itself and its dual both by $\mapsto$: $x \mapsto e_g = e_{g^{-1}x}$ and $x \mapsto g = xgx^{-1} = g^x$. Given any group homomorphism $f$, we denote its linear dual by $f^*$. The assumptions on the base field are made to assure that $\hat{A} \cong A$ for any abelian group $A$. This can be relaxed to any field where this isomorphism holds for all abelian subgroups of $G$, and in principle our results can be modified to work in an arbitrary field, provided one takes extra care concerning the potential failure of these isomorphisms.

The paper is organized as follows. In Section 1 we cover all of the preliminary results and definitions needed, in particular giving a quick
review of the main result we need from [2]. This result describes morphism $D(G) \to D(H)$ via a quadruplet of morphisms $(p, u, r, v)$, which can be equivalently interpreted as a description in terms of $2 \times 2$ matrices of morphisms satisfying certain compatibility relations. In Section 2 we establish many important properties of $p$ and $u$ that will be used throughout the paper. In section 3 we introduce a special kind of homomorphism $D(G) \to D(H)$, and show that all elements of $\text{Aut}(D(G))$ are of this type. This establishes a certain symmetry between the morphisms $u$ and $v$, providing easy proofs for some key results. In Section 4 we introduce a number of useful subgroups of $\text{Aut}(D(G))$. Section 5 contains the main result, which can be stated as:

**Theorem.** Let $G$ be a finite group. Then $\text{Aut}(D(G))$ has subgroups $S, T, U, V$ with $S \cong \text{End}(Z(G))$, $T \cong \text{Hom}(G, \hat{G})$, $U \cong \text{Aut}_{c}(G) = C_{\text{Aut}(G)}(\text{Inn}(G))$, and $V \cong \text{Aut}(G)$, all of which intersect each other trivially. Moreover, $\text{Aut}(D(G))$ is generated by these subgroups if and only if $G$ is purely non-abelian.

As a special case, if $Z(G) = 1$ then $\text{Aut}(D(G)) \cong \text{Aut}(G) \times \text{Hom}(G, \hat{G})$, where the action is $v^w = v^r w$.

In the last part, $v \in \text{Aut}(G)$ gives the automorphism

$$e_g \# h \mapsto e_{v(g)} \# v(h),$$

as noted by Courter [8]; and $r \in \text{Hom}(G, \hat{G})$ gives the automorphism

$$e_g \# h \mapsto r(h)e_g \# h.$$  

If we write $r(g) = \sum \omega(g, x)e_x$, with $\omega$ a bicharacter, then this is equivalent to $e_g \# h \mapsto \omega(h, g)e_g \# h$. The Theorem can be viewed as analogous to the description of the automorphisms of the direct products of groups given by Bidwell et al. [7]. Indeed, it can be proven from that description, but we do not take that approach here since it is less direct. In Section 6 we consider the restriction of automorphisms to the group-like elements and describe the kernel of this restriction. In Section 7 we determine when certain subgroups are normal, as well as when they have complements, including the kernel of the restriction. This provides a number of different ways to write $\text{Aut}(D(G))$ with exact factorizations or even semidirect products for certain types of groups. We conclude the paper in Section 8 with a discussion on the basic properties of the induced action of a class of morphisms on the categories of representations. This includes the action of the automorphisms of $D(G)$ on the category $\text{Rep}(D(G))$. This provides the necessary details on how to use automorphisms to reduce the number
of simple modules to consider when computing all indicators for this category.

ACKNOWLEDGMENTS

The author would like to thank S. Montgomery, G. Mason, and P. Schauenburg for their many conversations and suggestions.

1. Preliminaries

Our reference for the theory of Hopf algebras is [20]. We use Sweedler summation notation for the comultiplication: \( \Delta(h) = h_{(1)} \otimes h_{(2)} \). For the wide ranging uses and constructions of the Drinfeld double, we also refer the reader to [9]. Here, we take the following definition of \( D(G) \) over a field \( \mathbb{k} \), where \( G \) is a finite group. As a coalgebra, \( D(G) \) is \( (\mathbb{k}^G)^{\text{cop}} \otimes kG \) with the usual tensor product coalgebra structure. We denote a simple tensor of \( D(G) \) by \( e_g \), some \( g, h \in G \). Letting \( \varepsilon = \sum_{g \in G} e_g \), the identity of \( D(G) \) is \( \varepsilon \# 1 \). We will also use \( \varepsilon \) as the counit of \( kG \). The multiplication is given by having \( G \) act on \( \mathbb{k}^G \) by conjugation:

\[
(e_g \# g')(e_h \# h') = \delta_{g,g'} e_{g'h'}.
\]

We denote the functional on \( \mathbb{k}^G \) given by evaluation at \( g \in G \) by \( \text{ev}_g \).

We begin by stating the main result from [2] that we need here.

**Theorem 1.1.** [2, Corollaries 2.3-2.4] Let \( G, H \) be finite groups. Then there exists a bijection between the set of all morphisms of Hopf algebras \( \psi : D(G) \to D(H) \) and the set of all quadruples \( (p, u, r, v) \) where \( u: \mathbb{k}^G \to \mathbb{k}^H \), \( r: \mathbb{k}G \to \mathbb{k}^H \) are unitary coalgebra maps, and \( p: \mathbb{k}^G \to \mathbb{k}H, v: : G \to H \) are morphisms of Hopf algebras satisfying the following compatibility conditions:

\[
\begin{align*}
(1.1) & \quad u(a_{(1)}) \otimes p(a_{(2)}) = u(a_{(2)}) \otimes p(a_{(1)}) \\
(1.2) & \quad u(ab) = u(a_{(1)}) (p(a_{(2)}) \to u(b)) \\
(1.3) & \quad r(hg) = r(h) (v(h) \to r(g)) \\
(1.4) & \quad r(h) (v(h) \to u(b)) = u(h \to b_{(1)}) (p(h \to b_{(2)}) \to r(h)) \\
(1.5) & \quad v(h)p(b)v(h)^{-1} = p(h \to b)
\end{align*}
\]

for all \( a, b \in \mathbb{k}^G \) and \( g, h \in G \).

Under the above bijection the morphism of Hopf algebras \( \psi : D(G) \to D(H) \) corresponding to \( (p, u, r, v) \) is given by:

\[
\begin{align*}
(1.6) & \quad \psi(a \# g) = u(a_{(1)}) (p(a_{(2)}) \to r(g)) \# p(a_{(3)}) v(g)
\end{align*}
\]

for all \( a \in \mathbb{k}^G \) and \( g \in G \).
Proof. We give only the definitions of $u, r, p, v$ for clarity. Full details of the proof can be found in [2].

\begin{align*}
(1.7) \quad u(a) &= ((\text{id} \otimes \epsilon_H) \circ \psi)(a \#_1 G) \\
(1.8) \quad p(a) &= ((\text{ev}_{1_H} \otimes \text{id}) \circ \psi)(a \#_1 G) \\
(1.9) \quad r(g) &= ((\text{id} \otimes \epsilon_H) \circ \psi)(\epsilon_G \# g) \\
(1.10) \quad v(g) &= ((\text{ev}_{1_H} \otimes \text{id}) \circ \psi)(\epsilon_G \# g).
\end{align*}

The first relation is the definition for $u, p$ to cocommutate. Since group algebras are cocommutative, we also have that $r, v$ cocommute trivially, and that $u, r$ trivially have commuting images. Equation (1.5) expresses the commutation relation between the images of $v$ and $p$.

It is convenient to think of $\psi = (p, u, r, v)$ as a matrix

\begin{equation}
\begin{pmatrix}
  u & r \\
p & v
\end{pmatrix},
\end{equation}

with evaluations performed on the right. We may multiply two such matrices together, where, as is standard [6, 7], addition is the convolution product—and thus subtraction indicates the antipode—and multiplication is composition. It is a straightforward exercise to verify that the relations in the Theorem are precisely what is needed to make such a matrix a morphism of Hopf algebras, and for matrix multiplication to correspond to composition of morphisms. Thus the Theorem can be interpreted as describing $\text{Hom}(\mathcal{D}(G), \mathcal{D}(H))$ as matrices of morphisms satisfying the given relations.

This paper is concerned with improving and understanding the above description, especially for isomorphisms. We can immediately show that there is more structure to $r$ than was originally noticed, resulting in several simplifications.

**Corollary 1.2.** The morphism $r$ is a morphism of Hopf algebras, and is thus uniquely determined by a group homomorphism $r \in \text{Hom}(G, \hat{H})$. Equation (1.3) is then a consequence of this, and may be omitted. Furthermore, equation (1.4) simplifies to

\begin{equation}
v(h) \mapsto u(b) = u(h \mapsto b)
\end{equation}

and we may instead write

\begin{equation}
\psi(a \# g) = u(a_{(1)})r(g)\# p(a_{(2)})v(g),
\end{equation}

for all $a \in k^G_{\text{cop}}$ and $g \in G$. 
Proof. Since \( r \) is a morphism of unitary coalgebras, it must map group-likes to group-likes, and so \( r(g) \in \hat{H} \) for all \( g \in G \). Then for any \( y \in H \), \( y \rightarrow r(g) = r(g) \), and so the \( H \)-action is trivial on the image of \( r \). Thus equation (1.3) simplifies to \( r(gh) = r(g)r(h) \) for all \( g, h \in G \). Therefore \( r \) is also an algebra, and thus Hopf, morphism. Equation (1.13) follows similarly. \( \square \)

Since we now know that \( p \), \( r \) and \( v \) are morphisms of Hopf algebras, the question naturally arises as to whether or not \( u \) is also a morphism of Hopf algebras. We suspect this is always true, but we prove it only for a special case that includes the automorphisms in Corollary 2.2. Whenever this is the case, we can identify \( u^* \) with a group homomorphism \( \alpha : H \rightarrow G \). It can easily be seen that \( u \) Hopf implies (1.2), leaving us with just three non-trivial compatibility conditions in this case.

The goal now will be to describe \( \text{Aut}(\mathcal{D}(G)) \) for as many finite groups as possible. The simplest case is, of course, when \( G \) is abelian. For then \( \mathcal{D}(G) \cong \mathbb{k}(G \times G) \), and so \( \text{Aut}(\mathcal{D}(G)) \cong \text{Aut}(G \times G) \), which can be computed by classical methods [25]. We will see in Corollary 2.6 and example 2.7 that, in this case, there are automorphisms \( (p, u, r, v) \) where both \( u, v \) are not isomorphisms. Indeed, there are also automorphisms \( (p, u, r, v) \) where changing \( r \) can fail to yield an automorphism. Such behaviors complicate the description of \( \text{Aut}(\mathcal{D}(G)) \). As such, one suspects that abelian direct factors are the precise cause of such behavior in general, and that a description of \( \text{Aut}(\mathcal{D}(G)) \) for purely non-abelian groups should be more readily attainable. We will prove this in Theorem 2.12; see also Corollary 2.6 and Theorem 5.15.

2. Essential properties of \( p \) and \( u \)

To discern the properties of \( \text{Aut}(\mathcal{D}(G)) \), we need to explore the consequences the compatibilities have on the exact form the components of a morphism can take. We will begin our investigation with \( p \), starting with the following simple and useful observation.

**Theorem 2.1.** Let \( p : \mathbb{k}^G \rightarrow \mathbb{k}H \) be a morphism of Hopf algebras. Then \( p \) is uniquely determined by a group isomorphism \( \hat{A} \xrightarrow{f} B \), where \( A, B \) are abelian subgroups of \( G, H \) respectively. In this case, \( p \) is given by the obvious imbedding of \( \mathbb{k}^A \rightarrow \mathbb{k}^G \), and setting \( p(e_g) = 0 \) whenever \( g \notin A \), and \( p(\chi) = f(\chi) \) for \( \chi \in \hat{A} \).

Furthermore, if \( v \in \text{Hom}(G, H) \) satisfies equation (1.5), then also \( A \leq G \), and \( B \) is closed under conjugation by elements of \( v(G) \) (ie.,
$B^{v(G)} = B$). In addition, $v$ maps $C_G(A)$ to $C_H(B)$. In particular, $C_H(v(A)) \subseteq C_H(B)$, with equality whenever $v$ is an isomorphism.

**Proof.** Since $k^G$ is a commutative Hopf algebra, we must have that $\text{Im}(p)$ is a commutative Hopf sub-algebra of $kH$. Therefore, there exists an abelian subgroup $B \subseteq H$ such that $\text{Im}(p) = kB$, and we may decompose $p$ as the composition

$$(k^G)^{\text{cop}} \to kB \hookrightarrow kH.$$ 

Now the dual morphism $p^*: k^H \to kG^\text{cop}$ is also a morphism of Hopf algebras, and $kG^\text{cop}$ is naturally isomorphic to $kG$, so there is an abelian subgroup $A \subseteq G$ such that $\text{Im}(p^*) = kA$. We can thus decompose $p^*$ as the composition

$$k^H \hookrightarrow kB \to kA \hookrightarrow kG^\text{cop}.$$ 

Dualizing again we have the following decomposition of $p$:

$$(k^G)^{\text{cop}} \to kA \cong kA \xrightarrow{f} kB \hookrightarrow kH.$$ 

All maps are morphisms of Hopf algebras, so $f$ restricts to a group homomorphism $\rho: A \to B$. By construction, $f$, and therefore $\rho$, are bijections. The choice of isomorphism $k^A \cong kA$ affects the composition, but for a given $p$ changing this isomorphism is equivalent to a change in the isomorphism $f$ (equiv. $\rho$).

That (1.5) implies $A \subseteq G$ and $B^{v(G)} = B$ is clear.

Now let $g \in C_G(A)$, and $a \in k^A$, $b \in B$ such that $p(a) = b$. Then $b = p(a) = p(g \leftarrow a) = p(a)^{v(g)} = b^{v(g)}$. Since $p$ surjects onto $B$, we conclude that $v$ maps $C_G(A)$ to $C_H(B)$. The remaining claims are clear. □

In the subsequent, whenever discussing $p$ or any morphism $(p, u, r, v) \in \text{Hom}(D(G), D(H))$, any use of the letters $A, B$ refer to precisely those subgroups in the preceding Lemma. These subgroups will be used frequently, so whenever convenient we shall invoke and use them without further mention. Note that since $A, B$ are abelian they are contained in their centralizers.

**Corollary 2.2.** Let $(p, u, r, v) \in \text{Hom}(D(G), D(H))$. If $B \leq Z(H)$, then $u$ is a morphism of Hopf algebras.

**Proof.** Apply equations (1.2) and (1.12). □

As remarked before, note that whenever $u$ is Hopf then we may identify $u^*$ with a group homomorphism. We do so in the subsequent without further mention.
Lemma 2.3. Let $\psi = (p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))$. Then the following all hold.

i) $\text{Im}(u^*) \subseteq C_{\mathbb{k}G}(\mathbb{k}A)$.

ii) If $\mathbb{k}A\text{Im}(u^*) = \mathbb{k}G$, then $A \leq Z(G)$.

iii) If the images of $p, v$ commute, then $A \leq Z(G)$.

iv) If $A \leq Z(G)$ and $H = B\text{Im}(v)$, then $B \leq Z(H)$.

v) If $A \leq Z(G)$ and $H = Z(H)\text{Im}(v)$, then $B \leq Z(H)$.

vi) If $\psi$ is surjective, then $B\text{Im}(v) = H$.

vii) If $\psi$ is injective, then $\mathbb{k}A\text{Im}(u^*) = \mathbb{k}G$ and $A \leq Z(G)$.

Proof. For the first statement, note that $u, p$ cocommute is equivalent to $u^*, p^*$ having commuting images. Since $\text{Im}(p^*) = \mathbb{k}A$, the claim follows. The second part then follows.

The third part is similar. Explicitly, if $p, v$ commute, then equation (1.5) becomes $p(e_g) = p(e_{gx^{-1}})$ for all $x, g \in G$. Since $p(e_g) \neq 0 \iff g \in A$ and $p$ is an isomorphism $\mathbb{k}A \rightarrow \mathbb{k}B$, we conclude that $A \leq Z(G)$, as desired.

For the fourth part, we have

$$H = Bv(G) = Bv(C_G(A)) \subseteq BC_H(B) = C_H(B),$$

and thus $B \leq Z(H)$ as claimed. The fifth part is similar, using that $Z(H) \leq C_H(B)$.

The surjectivity statement is an obvious consequence of equation (1.13). Indeed, also from that equation, in order for $\psi(e_g \neq g') \neq 0$ for all $g, g' \in G$, we must have that $\mathbb{k}A\text{Im}(u^*) = \mathbb{k}G$. Applying the previous parts completes the proof. □

The following is then an easy corollary. Since it is essential for the rest of the paper, we mark it as a Theorem.

Theorem 2.4. Let $(p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))$. If $(p, u, r, v)$ is an isomorphism then both $A, B$ are central, and $u$ is a morphism of Hopf algebras.

Indeed, we have the following characterization of isomorphisms between $\mathcal{D}(G)$ and $\mathcal{D}(H)$.

Theorem 2.5. For finite groups $G, H$, we have $\mathcal{D}(G) \cong \mathcal{D}(H) \iff G \cong H$.

Proof. Sufficiency is clear. For necessity, first note that any morphism of Hopf algebras sends group-like elements to group-likes. Thus any isomorphism $\mathcal{D}(G) \cong \mathcal{D}(H)$ restricts to a group isomorphism $\hat{G} \times G \cong \hat{H} \times H$. Since the groups are isomorphic, their character groups are isomorphic: $\hat{G}^2 \cong \hat{H}^2$. By [23, Exercise 6.32], we conclude that $\hat{G} \cong \hat{H}$.
and so $\hat{G} \times G \cong \hat{G} \times H$. We may then apply Exercise 6.33 to conclude that $G \cong H$, as desired. □

In particular, we may focus on $\text{Aut}(\mathcal{D}(G))$ without loss of generality.

**Corollary 2.6.** Let $G$ be a finite group. Then the following are equivalent.

i) $G$ is abelian.

ii) There exists $(p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ with $v \equiv 1$ (the trivial morphism).

iii) There exists $(p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ with $u(e_g) = \delta_{1,g} \varepsilon$ (the trivial morphism).

**Proof.** That (ii) and (iii) imply (i) are a consequence of the Lemma.

On the other hand, if $G$ is abelian, then taking $v, u$ trivial and $p, r$ isomorphisms, we find that $(p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$. □

**Example 2.7.** Indeed, not only does $G$ abelian allow for $u, v$ to have kernels, it also causes bijectivity to be sensitive to the choice of bicharacter. Namely, for $G$ any abelian group, let $(p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ be as in the proof of the Corollary. If we replaced $r$ with any map which was not an isomorphism, then the new endomorphism is clearly not an automorphism. It is not necessary that $p, r$ be isomorphisms for this to occur, in general.

In both the Corollary and example, the reasons for the existence of such automorphisms are precisely the same as why the description of $\text{Aut}(G \times G)$ depends on whether $G$ has abelian factors or not. See [6, 7] for details.

The following will be useful for describing some subgroups of $\text{Aut}(\mathcal{D}(G))$ in Section 4.

**Lemma 2.8.** Let $G$ be a finite group, and let $\psi = (p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$. If either $p$ or $r$ is trivial, then both $u, v$ are isomorphisms.

In particular, if $Z(G) = 1$, then $p$ is always trivial and thus $u, v$ are always isomorphisms.

**Proof.** Consider the case $r$ trivial: $
\begin{pmatrix}
u & 0 \\
p & v
\end{pmatrix} \in \text{Aut}(\mathcal{D}(G))$. Then for every $n \in \mathbb{N}$ we have

$$
\begin{pmatrix}
u & 0 \\
p & v
\end{pmatrix}^n = \begin{pmatrix}
u^n & 0 \\
* & v^n
\end{pmatrix},
$$

where $*$ denotes some morphism. By assumptions, the morphism in question has finite order, so for some $n \in \mathbb{N}$ we have $u^n = \text{id}$ and
\( v^n = \text{id}. \) Therefore, \( u, v \) are isomorphisms. The case where \( p \) is trivial is similar. \( \square \)

We desire an alternative description of equation (1.12). To this end, recall the following definition.

**Definition 2.9.** Let \( H \) be a Hopf algebra with antipode \( S \). We say that an algebra morphism \( f : H \to H \) is normal if \( Sf \ast \text{id} \) is an algebra morphism.

Note that, since \( f \ast ((Sf) \ast \text{id}) = \text{id} \), the definitions are symmetric: \( Sf \ast \text{id} \) and \( f \ast \text{id} \) are simultaneously normal. It is a routine verification that normality is equivalent to saying \( f(a_1bS(a_2)) = a_1f(b)S(a_2) \). The definition of normality here agrees with the definition used for group homomorphisms [23].

We can then provide the following equivalent characterization of equation (1.12).

**Lemma 2.10.** Let \( G, H \) be finite groups, \( u : \mathbb{k}G^{\text{cop}} \to \mathbb{k}H^{\text{cop}} \) a coalgebra morphism, and \( v : \mathbb{k}G \to \mathbb{k}H \) an algebra morphism. Then \( u, v \) satisfy equation (1.12) if and only if \( u \ast v \) is a normal morphism of algebras.

**Proof.** First note that \( u(\lambda \gamma \to \epsilon) = v(\lambda \gamma) \to u(\epsilon) \forall \lambda, \gamma \in G \equiv u^*(v(\lambda \gamma) \to h) = \lambda \gamma \to u^*(h) \forall h \in H, \lambda, \gamma \in G. \) Since \( u^* \), and thus \( u^*v \) are algebra maps, we then have

\[
u^*(v(\lambda \gamma) \to h) = \lambda \gamma \to u^*(h) \iff u^*v(\lambda \gamma)u^*(h)u^*(\lambda^{-1}) = xu^*(h)x^{-1} = xu^*(h)x^{-1} \iff u^*v(x^{-1})xu^*(h)(u^*v(x^{-1})x)^{-1} = u^*(h).
\]

Then the latter holding for all \( h \) is equivalent to \( S(u^*v) \ast \text{id}(x) = u^*v(x^{-1})x \in C_{\mathbb{k}G}(\text{Im}(u^*)) \). This being true for all \( x \) is in turn equivalent to \( S(u^*v) \ast \text{id} \) being a morphism of algebras. This completes the proof. \( \square \)

Of course, whenever \( u \) is a morphism of Hopf algebras, then \( u^* \) is identified with a group homomorphism, and the statement of the Lemma is then that \( u^* \circ v \) is a normal group homomorphism. When \( u, v \) are also isomorphisms, the condition can be further phrased in group theoretic terms.

**Definition 2.11.** \( \text{Aut}_c(G) = \{ \phi \in \text{Aut}(G) \mid \phi(g)g^{-1} \in Z(G) \} \) is a normal subgroup of \( \text{Aut}(G) \), called the central automorphism group.

\( \text{Aut}_c(G) \) can be equivalently characterized as the centralizer of \( \text{Inn}(G) \) in \( \text{Aut}(G) \). It can also be characterized as the normal automorphisms of \( G \). Therefore, when \( u^*, v \in \text{Aut}(G) \) the lemma can be stated as saying \( u^* \circ v \in \text{Aut}_c(G) \).
Lemma 2.8 gave some conditions that forced \(u, v\) to be isomorphisms for \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\). The theory of normal group endomorphisms allows us to show that \(u, v\) are always isomorphisms for any purely non-abelian group. We will see later that this is, in fact, a characterization of purely non-abelian groups.

**Theorem 2.12.** Let \(G\) be a finite group and \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\).

Then \(\ker(u^*)\) and \(\ker(v)\) are contained in an abelian direct factor of \(G\). In particular, if \(G\) is purely non-abelian then \(u, v\) are isomorphisms for all \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\).

**Proof.** Let \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\), and denote its inverse by \((p', u', r', v')\).

Then

\[
\begin{pmatrix}
  u' & r' \\
  p' & v'
\end{pmatrix}
\begin{pmatrix}
  u & r \\
  p & v
\end{pmatrix}
= \begin{pmatrix}
  u'u + r'p & u'r + r'v \\
  p'u + v'p & p'r + v'v
\end{pmatrix}
= \begin{pmatrix}
  1 & 0 \\
  0 & 1
\end{pmatrix}.
\]

In particular, \(p'r + v'v = \text{id}\). Thus for all \(g \in \ker(v)\) we have \(p'r(v) = v\). Since \(\text{Im}(p')\) is a central group algebra, \(p'v\) is clearly a normal endomorphism of \(G\) with abelian image. So by Fitting’s Lemma we conclude that \(G = \text{Im}((p'v)^n) \times \ker((p'v)^n)\) for all sufficiently large \(n \in \mathbb{N}\). Since \(\ker(v) \subseteq \text{Im}((p'v)^n)\) and \(\text{Im}((p'v)^n)\) is abelian, we conclude that \(\ker(v)\) is contained in an abelian direct factor of \(G\), as desired. A similar argument applies to \(u^*\) after dualizing the upper-left entries. The remaining claim is by definition.

**Remark.** An alternative proof can be given using the methods of Section 6. This method also relies on the theory of normal group endomorphisms, however, so the above proof is more direct.

This result will allow us to completely describe the elements of \(\text{Aut}(\mathcal{D}(G))\) for purely non-abelian groups in Theorem 5.7.

### 3. Flippable Homomorphisms

**Definition 3.1.** Let \(G, H\) be finite groups and \(\psi = (p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))\). We say that \(\psi\) is flippable if \(\phi = (p^*, v^*, r^*, u^*) \in \text{Hom}(\mathcal{D}(H), \mathcal{D}(G))\). In this case we call \((p^*, v^*, r^*, u^*)\) the flip of \(\psi\).

**Remark.** The taking of duals still gives morphisms with the proper domain and range, after using that \(G\) is naturally isomorphic to \(G^{\text{op}}\). Indeed, the description of \(\text{Hom}(\mathcal{D}(G), \mathcal{D}(H))\) can have all co-opposites removed entirely. Also observe that any flippable morphism necessarily has \(u\) a morphism of Hopf algebras, since \(u^*\) must necessarily be Hopf for \(\phi\) to be a morphism of Hopf algebras.
We use the obvious nomenclature derived from the definition. For example, the act of taking the flip will be called flipping, etc. Clearly the flip of a flippable morphism is itself flippable. The primary use for flippable morphisms in this paper is that proving general properties about \( v \) for a collection of flippable morphisms, which is also closed under flipping, automatically lets one deduce the same properties for \( u^* \). The following lemma uses flipping to prove facts about \( A, B \).

**Lemma 3.2.** Let \( G, H \) be finite groups, and suppose \( \psi = (p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H)) \) is flippable. Then the images of \( p \) and \( v \) commute. Moreover, \( A, B \leq Z(G) \).

**Proof.** Since \( (p^*, v^*, r^*, u^*) \in \text{Hom}(\mathcal{D}(H), \mathcal{D}(G)) \), we know that \( p^* \) and \( v^* \) cocommute by (1.1). The dual statement to this is that the images of \( p \) and \( v \) commute. That \( A \leq Z(G) \) then follows from Lemma 2.3. By flipping, we obtain that \( B \leq Z(H) \). \( \square \)

In particular, when viewed as matrices the flippable morphisms have cocommuting columns and commuting rows.

**Proposition 3.3.** Let \( G \) be a finite group and let \( \text{End}_f(\mathcal{D}(G)) \) denote the set of all flippable endomorphisms of \( \mathcal{D}(G) \). Then \( \text{End}_f(\mathcal{D}(G)) \) is a submonoid of \( \text{End}(\mathcal{D}(G)) \), and flipping is an anti-isomorphism of monoids of order at most two.

**Proof.** Let \( \phi, \psi \in \text{End}_f(\mathcal{D}(G)) \), and write

\[
\psi = \begin{pmatrix} u_1 & r_1 \\ p_1 & v_1 \end{pmatrix}, \\
\phi = \begin{pmatrix} u_2 & r_2 \\ p_2 & v_2 \end{pmatrix}.
\]

Denote the flips of \( \phi, \psi \) by \( F(\phi), F(\psi) \) respectively. By definition \( F(F(\phi)) = \phi \), which gives the order statement and bijectivity.

Now observe that

\[
(3.1) \quad \phi \circ \psi = \begin{pmatrix} u_2u_1 + r_2p_1 & u_2r_1 + r_2v_1 \\ p_2u_1 + v_2p_1 & p_2r_1 + v_2v_1 \end{pmatrix},
\]

\[
(3.2) \quad F(\psi) \circ F(\phi) = \begin{pmatrix} v_1^*v_2^* + r_1^*p_2^* & v_1^*r_2^* + r_1^*u_2^* \\ p_1^*v_2^* + u_1^*p_2^* & p_1^*r_2^* + u_1^*u_2^* \end{pmatrix}.
\]

Since the columns of \( \psi \) cocommute, and the rows of \( \phi \) commute, we conclude that \((u_2u_1 + r_2p_1)^* = (p_2^* + u_1^*)^* \), and similarly for the other entries of (3.1). Subsequently, we conclude that \( F(\phi \circ \psi) = F(\psi) \circ F(\phi) \), and that \( \phi \circ \psi \in \text{End}_f(\mathcal{D}(G)) \). Since the identity map is clearly flippable, and is its own flip, this shows that \( \text{End}_f(\mathcal{D}(G)) \)
is a submonoid, and that \( F \) is an anti-morphism of monoids. This completes the proof. \( \square \)

We now wish to show that every automorphism of \( \mathcal{D}(G) \) is flippable, and that their flips are again automorphisms. We need the following lemma. The proof given is thanks to A. Caranti.

**Lemma 3.4.** Let \( G, H \) be groups (not necessarily finite). Let \( v : G \to H \) and \( w : H \to G \) be group homomorphisms. Suppose \( Z(H) \operatorname{Im}(v) = H \) and \( Z(G) \operatorname{Im}(w) = G \). Then the following hold:

i) \( C_G(\operatorname{Im}(w)) = Z(G) \)

ii) \( C_H(\operatorname{Im}(v)) = Z(H) \)

iii) \( v(Z(G)) \subseteq Z(H) \)

iv) \( w(Z(H)) \subseteq Z(G) \)

v) The following are equivalent:
   (a) \( w \circ v \) is a normal group homomorphism.
   (b) \( v \circ w \) is a normal group homomorphism.

Indeed, if any of the two equivalent conditions hold, then also \( \operatorname{ker}(v) \subseteq Z(G) \) and \( \operatorname{ker}(w) \subseteq Z(H) \).

**Proof.** First, note that since \( G = Z(G) \operatorname{Im}(w) \) we have

\[
Z(G) = C_G(G) = C_G(Z(G) \operatorname{Im}(w)) = C_G(\operatorname{Im}(w)).
\]

Similarly, \( Z(H) = C_H(\operatorname{Im}(v)) \).

Now for any \( g \in Z(G) \), we have \( v(g) \in Z(\operatorname{Im}(v)) \). Since \( H = Z(H) \operatorname{Im}(v) \), we have that \( Z(\operatorname{Im}(v)) \leq Z(H) \). Thus \( v(Z(G)) \leq Z(H) \).

Similarly, \( w(Z(H)) \leq Z(G) \).

We now need to prove the equivalence part. By symmetry, we need only prove that (a)\( \Rightarrow \) (b). So suppose that (a) is true. Let \( h \in H \) be arbitrary, and write \( h = bv(g) \) for some \( b \in Z(G) \) and \( g \in G \). For simplicity of notation, write \( v(g) = g^v \), and similarly for other group homomorphisms. Then

\[
h^{uv}h^{-1} = (bg^v)^{uv}(bg^v)^{-1} = b^{uv}b^{-1}(g^{uv}g^{-1})^v \in Z(H),
\]

which is (b) by definition. Here we used that \( b^{uv} \in Z(H) \) by (iii) and (iv); and that \( g^{uv}g^{-1} \in Z(G) \) by assumptions, and then again applying (iii).

The remaining claims about \( \operatorname{ker}(v) \) and \( \operatorname{ker}(w) \) are then obvious. \( \square \)

**Theorem 3.5.** Every element of \( \operatorname{Aut}(\mathcal{D}(G)) \) is flippable. Moreover, the flip of an automorphism is itself an automorphism, and flipping is an anti-isomorphism of \( \operatorname{Aut}(\mathcal{D}(G)) \).
Proof. By Theorem 2.4 and Lemma 2.3, the preceding lemma applies to any \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\), with \(w = u^*\). The lemma is precisely what is needed for \((p^*, v^*, r^*, u^*) \in \text{End}(\mathcal{D}(G))\). Let \(F\) denote the flip map. Since \(F\) is a monoidal anti-isomorphism of \(\text{End}_f(\mathcal{D}(G))\), it follows that \(F((p, u, r, v)^{-1}) = F((p, u, r, v))^{-1}\), and in particular that \(F\) restricts to an anti-isomorphism \(\text{Aut}(\mathcal{D}(G)) \rightarrow \text{Aut}(\mathcal{D}(G))\). \(\Box\)

Remark. Lemma 3.4 can also be used to show other homomorphisms are flippable, such as all morphisms when \(G, H\) are abelian. Automorphisms are just the simplest ones for which it can be verified the Lemma applies to in general.

In general, flipping is not the same as inverting. However, any group anti-isomorphism can be expressed as the composition of the inversion map and a group isomorphism. This group isomorphism is simply the map \(\psi \mapsto F(\psi^{-1})\).

Since all automorphisms are flippable, and flippable morphisms satisfy some of the basic requirements to be a bijection, we suspect there is a nice invertibility test that can be phrased in terms of flipping. In general, flippable morphisms need not be invertible, as can easily be demonstrated by considering the endomorphisms of \(\mathcal{D}(\mathbb{Z}_2)\). We suspect the following to be true.

**Conjecture 3.6.** \(\psi \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))\) is invertible if and only if it is flippable and it sends the integral of \(\mathcal{D}(G)\) to the integral of \(\mathcal{D}(H)\).

It is easy to verify that in order to preserve integrals, we must have \(B \text{Im}(v) = H\), and from being flippable we know \(A, B\) are central.

If the conjecture were false, then there would exist finite groups \(G, H\) and a non-bijective, flippable homomorphism \(\psi : \mathcal{D}(G) \rightarrow \mathcal{D}(H)\) such that the induced functor \(\text{Rep}(\mathcal{D}(H)) \rightarrow \text{Rep}(\mathcal{D}(G))\) preserves all higher Frobenius-Schur indicators \[16\]. Of special interest would be the case \(G = H\). Moreover, the induced functor for flippable homomorphisms tends to take a rather nice form, as will be described in Section 8.

4. **Some subgroups of \(\text{Aut}(\mathcal{D}(G))\)**

The goal of this section is to introduce several subgroups of \(\text{Aut}(\mathcal{D}(G))\). We will use these in the subsequent sections to determine the membership and structure of \(\text{Aut}(\mathcal{D}(G))\) for purely non-abelian groups.

**Definition 4.1.** Let \(G\) be a finite group, and set \(\Lambda(G) = \{(p, \text{id}, 1, \text{id}) \in \text{Aut}(\mathcal{D}(G))\}\).
The choice of notation comes from the original description of morphisms $D(G) \to D(H)$ given by Agore et al. [2]. There, $p$ was written as $p(e_g) = \sum_{h \in H} \lambda(g, h)h$.

**Proposition 4.2.** $\Lambda(G)$ is an abelian subgroup of $\text{Aut}(D(G))$, and $\Lambda(G) \cong \text{End}(Z(G))$ as groups.

**Proof.** We claim that $(p, \text{id}, 1, \text{id}) \in \text{Aut}(D(G)) \iff A, B \leq Z(G)$.

Suppose that $(p, \text{id}, 1, \text{id}) \in \text{Aut}(D(G))$. Since the morphism is flippable, $p$ commutes and cocommutes with identity maps. Thus $A$ and $B$ are central.

On the other hand, suppose that $p$ is determined by $A, B \leq Z(G)$. It is easy to verify that $(p, \text{id}, 1, \text{id}) \in \text{End}(D(G))$. In matrix notation, we observe that
\[
\begin{pmatrix}
1 & 0 \\
p & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
-p & 1
\end{pmatrix}
= \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}.
\]

This means that $(p, \text{id}, 1, \text{id})$ is invertible with inverse $(Sp, \text{id}, 1, \text{id})$. That $Sp$ is a morphism of Hopf algebras, and subsequently that $(Sp, \text{id}, 1, \text{id}) \in \text{End}(D(G))$ is guaranteed by the assumption that $A, B \leq Z(G)$.

This proves the claim. It remains to show that $\Lambda(G)$ is an abelian group and to exhibit the desired isomorphism.

Let $(p_1, \text{id}, 1, \text{id}), (p_2, \text{id}, 1, \text{id}) \in \Lambda(G)$. Then the composition is
\[
\begin{pmatrix}
1 & 0 \\
p_1 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
p_2 & 1
\end{pmatrix}
= \begin{pmatrix}
1 & 0 \\
p_1 + p_2 & 1
\end{pmatrix}.
\]

Equivalently, $(p_1, \text{id}, 1, \text{id}) \circ (p_2, \text{id}, 1, \text{id}) = (p_1 \ast p_2, \text{id}, 1, \text{id})$. It follows that $\Lambda(G)$ is a subgroup of $\text{Aut}(D(G))$. As previously noted, $p_1$ and $p_2$ commute and cocommute with identity maps. Therefore they convolution commute: $p_1 \ast p_2 = p_2 \ast p_1$. Therefore $\Lambda(G)$ is abelian.

The claim in fact shows that $\Lambda(G)$ depends only on $Z(G)$, and in particular $\Lambda(G) \cong \Lambda(Z(G))$. So we may suppose that $G$ is abelian. Then a morphism of Hopf algebras $p: k^G \to k^G$ is exactly a group homomorphism $\widehat{G} \to G$. Fixing an isomorphism $\widehat{G} \cong G$, any group homomorphism $\widehat{G} \to G$ is equivalent to a group homomorphism $G \to \widehat{G}$, as well as equivalent to a group homomorphism $G \to G$. It is easy to see that these in fact give group isomorphisms.

We conclude that
\[
\Lambda(G) \cong \text{Hom}(\widehat{Z(G)}, Z(G)) \cong \text{Hom}(Z(G), \widehat{Z(G)}) \cong \text{End}(Z(G))
\]
for all finite groups $G$. This completes the proof.
Proposition 4.3. [8, Proposition 2.3.5] Let $G$ be a finite group. Then $\text{Aut}(G)$ embeds as a subgroup of $\text{Aut}(\mathcal{D}(G))$, where $\sigma \in \text{Aut}(G)$ is sent to the automorphism defined by $e_g \# h \mapsto e_{\sigma(g)} \# \sigma(h)$. Equivalently, $\sigma \mapsto \begin{pmatrix} (\sigma^{-1})^* & 0 \\ 0 & \sigma \end{pmatrix}$.

In particular, we identify $\text{Aut}(G)$ as a subgroup of $\text{Aut}(\mathcal{D}(G))$ via the image of this embedding.

Proposition 4.4. For any $r \in \text{Hom}(G, \hat{G})$, 
\[
\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \in \text{Aut}(\mathcal{D}(G)).
\]

In particular, this gives an embedding $\text{Hom}(G, \hat{G}) \hookrightarrow \text{Aut}(\mathcal{D}(G))$, sending $r \in \text{Hom}(G, \hat{G})$ to the map $e_g \# h \mapsto r(h)e_g \# h$.

Proof. Given $r \in \text{Hom}(G, \hat{G})$, we see the desired matrix is trivially an element of $\text{End}(\mathcal{D}(G))$. If $r$ has order $n$, we can easily see that the matrix also has order $n$, so that the matrix is an element of $\text{Aut}(\mathcal{D}(G))$ as claimed. It is another simple check that the claimed embedding is actually an injective group homomorphism. \qed

We identify $\text{Hom}(G, \hat{G})$ with the image of this embedding.

Remark. If we write $r(h) = \sum \omega(h, x)e_x$, where $\omega$ is some bicharacter, then the description of the map is $e_g \# h \mapsto \omega(h, g)e_g \# h$.

As $\text{Aut}_c(G)$ is a subgroup of $\text{Aut}(G)$, it can be viewed as a subgroup of $\text{Aut}(\mathcal{D}(G))$ through the embedded copy of $\text{Aut}(G)$. However, in light of Lemma 2.10 there are additional copies of $\text{Aut}_c(G)$.

Proposition 4.5. For any $w \in \text{Aut}_c(G)$ we have 
\[
\begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}, \begin{pmatrix} (w^{-1})^* & 0 \\ 0 & 1 \end{pmatrix} \in \text{Aut}(\mathcal{D}(G)).
\]

In particular, these give two distinct, injective group homomorphisms $\text{Aut}_c(G) \to \text{Aut}(\mathcal{D}(G))$ whose images intersect trivially.

Indeed, the embeddings also intersect trivially with the usual embedding of $\text{Aut}(G)$, and corresponding sub-embedding of $\text{Aut}_c(G)$. The second embedding will be the one we use in the subsequent. So when we refer to $\text{Aut}_c(G)$ as a subgroup of $\text{Aut}(\mathcal{D}(G))$, it will be to this second embedding. To help avoid potential confusion with these three
distinct copies of $\text{Aut}_c(G)$, we will prefer, whenever possible, to consider the subgroup generated by $\text{Aut}(G)$ and either of the embeddings of $\text{Aut}_c(G)$ above instead.

**Definition 4.6.** Let $G$ be any group (not necessarily finite). We define $\text{SpAut}_c(G)$, the split central automorphism group of $G$, by

$$\text{SpAut}_c(G) = \{(w, v) \in \text{Aut}(G) \times \text{Aut}(G) : w^{-1} \circ v \in \text{Aut}_c(G)\}.$$  

The binary operation is inherited from $\text{Aut}(G) \times \text{Aut}(G)$.

It may not be immediately clear that this is actually a subgroup, so we justify the terminology with the following result.

**Lemma 4.7.** $\text{SpAut}_c(G)$ is a subgroup of $\text{Aut}(G) \times \text{Aut}(G)$. Furthermore, $\text{SpAut}_c(G) \cong \text{Aut}_c(G) \rtimes \text{Aut}(G)$ with the usual conjugation action.

**Proof.** We note that $(\text{id}, \text{id}) \in \text{SpAut}_c(G)$, and this element serves as a two-sided identity. Now suppose $(\alpha, v) \in \text{SpAut}_c(G)$. The inverse of this element would be $(\alpha^{-1}, v^{-1})$, so we must show this is an element of $\text{SpAut}_c(G)$. Since $\text{Aut}_c(G)$ is a normal subgroup of $\text{Aut}(G)$, we have that

$$(\alpha, v) \in \text{SpAut}_c(G) \iff \alpha^{-1}v \in \text{Aut}_c(G)$$

$$\iff v \in \alpha \text{Aut}_c(G)$$

$$\iff v \in \text{Aut}_c(G)\alpha$$

$$\iff v \in (\alpha^{-1}\text{Aut}_c(G))^{-1}$$

$$\iff v^{-1} \in \alpha^{-1}\text{Aut}_c(G)$$

$$\iff (\alpha^{-1}, v^{-1}) \in \text{SpAut}_c(G).$$

which establishes that $\text{SpAut}_c(G)$ is closed under inversion. If also $(\beta, w) \in \text{SpAut}_c(G)$, then we may write $v(g) = \alpha(g)z(g)$ and $\beta^{-1}(w(g)) = gz'(g)$ for some $z, z' \in \text{Hom}(G, Z(G))$; we note that $z, z'$ are homomorphisms, which follows from $Z(G)$ being abelian. We then have

$$(\alpha \circ \beta)^{-1} \circ (v \circ w)(g) = \beta^{-1} \circ \alpha^{-1} \circ v \circ w(g)$$

$$= \beta^{-1}\alpha^{-1} \circ \alpha \ast z \circ w(g)$$

$$= \beta^{-1}(\alpha^{-1}(\alpha(w(g))z(w(g))))$$

$$= \beta^{-1}(w(g)\alpha^{-1}(z(w(g))))$$

$$= \beta^{-1}(w(g))\alpha^{-1}(z(w(g)))$$

$$= gz'(g)\beta^{-1}(\alpha^{-1}(z(w(g)))].$$
Since $Z(G)$ char $G$, we conclude that $\beta^{-1}(\alpha^{-1}(z(w(g)))) \in Z(G)$ for all $g$, and therefore that $(\alpha \circ \beta, v \circ w) \in \text{SpAut}_c(G)$, as desired.

Consider $H = \{(w,1) \in \text{SpAut}_c(G)\}$ and $K = \{(v,v) \in \text{SpAut}_c(G)\}$. By definition we have $H \cong \text{Aut}_c(G)$ and $K \cong \text{Aut}(G)$. Furthermore, it is equally clear that $H \trianglelefteq \text{SpAut}_c(G)$, $H \cap K = 1$, and $\text{SpAut}_c(G) = HK$. Thus $\text{SpAut}_c(G) \cong \text{Aut}_c(G) \rtimes \text{Aut}(G)$, as desired.

This complete the proof. □

We view $\text{Aut}(G)$ as a subgroup of $\text{SpAut}_c(G)$ via the embedding $v \mapsto (v,v)$. Since there will be many semidirect products involved in our investigation of $\text{Aut}(D(G))$, and $\text{Aut}(D(G))$ has many natural copies of $\text{Aut}_c(G)$, for clarity of presentation we prefer to use $\text{SpAut}_c(G)$ rather than $\text{Aut}_c(G) \rtimes \text{Aut}(G)$ to denote this group. We use the latter only for specific examples. Whenever $\text{Aut}_c(G) = 1$, such as when $Z(G) = 1$, we clearly have $\text{SpAut}_c(G) \cong \text{Aut}(G)$.

**Proposition 4.8.** Let $G$ be a finite group. For any $(w,v) \in \text{SpAut}_c(G)$,

$$
\begin{pmatrix}
(w^{-1})^* & 0 \\
0 & v
\end{pmatrix} \in \text{Aut}(D(G)).
$$

In particular, this gives an embedding $\text{SpAut}_c(G) \hookrightarrow \text{Aut}(D(G))$. Explicitly, $(w,v)$ corresponds to the isomorphism $e_g # h \mapsto e_{w(g)} # v(h) = (w^{-1})^*(e_g) # v(h)$.

**Proof.** Such a matrix is easily verified to give an element of $\text{End}(D(G))$. Moreover, it also clear that its inverse is the matrix corresponding to $(w^{-1}, v^{-1}) = (w,v)^{-1}$, and so the matrix is in $\text{Aut}(D(G))$. It is equally clear that this gives an injective group homomorphism. □

It should be noted that the embedded copy of $\text{Aut}(G)$ in $\text{SpAut}_c(G)$ is mapped to the usual embedding of $\text{Aut}(G)$ into $\text{Aut}(D(G))$. So the copy of $\text{SpAut}_c(G)$ is naturally viewed as a generalization of this embedding. Indeed, it is clear that this copy of $\text{SpAut}_c(G)$ contains both of the embeddings from Proposition 4.5 and moreover that it is generated by $\text{Aut}(G)$ and either one of these copies of $\text{Aut}_c(G)$. As usual, we identify $\text{SpAut}_c(G)$ with the image of this embedding.

If we combine Propositions 4.4 and 4.8, we get a subgroup containing, and generated by, both $\text{Hom}(G, \hat{G})$ and $\text{SpAut}_c(G)$.

**Theorem 4.9.** Let $G$ be a finite group.

Then the elements of $\text{Aut}(D(G))$ of the form

$$
\begin{pmatrix}
u & r \\
0 & v
\end{pmatrix}
$$

are in $\text{SpAut}_c(G)$. Further, $\text{SpAut}_c(G)$ is naturally identified with $\text{Aut}(D(G))$.
form a subgroup isomorphic to $\text{SpAut}_c(G) \ltimes \text{Hom}(G, \hat{G})$, where the action of $\text{SpAut}_c(G)$ on $\text{Hom}(G, \hat{G})$ is given by $r^{(w,v)} = w^r v$.

Explicitly, $((w, v), r) \in \text{SpAut}_c(G) \ltimes \text{Hom}(G, \hat{G})$ corresponds to the isomorphism $e_g \# h \mapsto r(h)e_{w^{-1}(g)}\#v(h)$.

Proof. Note that by Lemma 2.8 we are guaranteed that $u, v$ are isomorphisms, and $u^* \circ v \in \text{Aut}_c(G)$. Given this, the rest of the proof is another straightforward verification using the matrix form for elements of $\text{Aut}(\mathcal{D}(G))$, and the preceding results. In particular, we can write

$$
\begin{pmatrix}
  u & r \\
  0 & v 
\end{pmatrix} =
\begin{pmatrix}
  1 & rv^{-1} \\
  0 & 1 
\end{pmatrix}
\begin{pmatrix}
  u & 0 \\
  0 & v 
\end{pmatrix}
= \begin{pmatrix}
  u & 0 \\
  0 & v 
\end{pmatrix}
\begin{pmatrix}
  1 & u^{-1}r \\
  0 & 1 
\end{pmatrix},
$$

from which it follows that

$$
\begin{pmatrix}
  u^{-1} & 0 \\
  0 & v^{-1} 
\end{pmatrix}
\begin{pmatrix}
  1 & r \\
  0 & 1 
\end{pmatrix}
\begin{pmatrix}
  u & 0 \\
  0 & v 
\end{pmatrix} = \begin{pmatrix}
  1 & u^{-1}rv \\
  0 & 1 
\end{pmatrix}.
$$

□

Note that $\text{SpAut}_c(G) \ltimes \text{Hom}(G, \hat{G})$ is a proper subgroup whenever $Z(G) \neq 1$, since then it intersects trivially with the non-trivial subgroup $\Lambda(G)$. On the other hand, $\text{SpAut}_c(G) \ltimes \text{Hom}(G, \hat{G}) \cong \text{Aut}(G) \ltimes \text{Hom}(G, \hat{G})$ and $\Lambda(G) = 1$ whenever $Z(G) = 1$.

5. Main Result

We can now proceed to establish the main result of the paper, which characterizes all elements of $\text{Aut}(\mathcal{D}(G))$ for $G$ purely non-abelian, and provides a decomposition into a product of subgroups. First, we need a few preliminary results. The first concerns the obvious subgroup of $\text{Aut}(\mathcal{D}(G))$ when $G$ is a direct product.

**Proposition 5.1.** Let $G = H \times K$, with $H, K$ finite groups. Then $\text{Aut}(\mathcal{D}(H)) \times \text{Aut}(\mathcal{D}(K))$ is (isomorphic to) a subgroup of $\text{Aut}(\mathcal{D}(G))$.

Proof. Given

$$
f = (p_H, u_H, r_H, v_H) \in \text{Aut}(\mathcal{D}(H)),
g = (p_K, u_K, r_K, v_K) \in \text{Aut}(\mathcal{D}(K)),
$$

then clearly $f \otimes g = (p_H \otimes p_K, u_H \otimes u_K, r_H \otimes r_K, v_H \otimes v_K) \in \text{Aut}(\mathcal{D}(G))$. This is precisely the automorphism of $\mathcal{D}(G)$ which restricts to $f$ on $\mathcal{D}(H)$ and restricts to $g$ on $\mathcal{D}(K)$. □
By Corollary 2.6, example 2.7, and Theorem 2.12 we then have the following two corollaries.

**Corollary 5.2.** $G$ is purely non-abelian if and only if $u, v$ are isomorphisms for all $(p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$.

**Corollary 5.3.** If $G$ has an abelian direct factor, then the following all hold:

i) $\exists (p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ with $\ker(v) \neq 1$.

ii) $\exists (p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ with $\ker(u^*) \neq 1$.

iii) $\exists (p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ and $r' \in \text{Hom}(G, \hat{G})$ such that $(p, u, r', v) \notin \text{Aut}(\mathcal{D}(G))$.

iv) $\exists (p, u, r, v) \in \text{Aut}(\mathcal{D}(G))$ with any two, or all three, of the above properties.

We previously defined the subgroup $\Lambda(G)$ in Definition 4.1. We will need the following lemma.

**Lemma 5.4.** Let $\begin{pmatrix} u & r \\ p & v \end{pmatrix} \in \text{Aut}(\mathcal{D}(G))$. If $u$ is invertible, then we may write

$$\begin{pmatrix} u & r \\ p & v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ pu^{-1} & 1 \end{pmatrix} \begin{pmatrix} u & r \\ 0 & -pu^{-1}r + v \end{pmatrix}.$$ 

Here the left matrix is in $\Lambda(G)$, and the right is in $\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G})$.

On the other hand, if $v$ is invertible, then

$$\begin{pmatrix} u & r \\ p & v \end{pmatrix} = \begin{pmatrix} u - rv^{-1}p & r \\ 0 & v^{-1}p \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v^{-1}p & 1 \end{pmatrix},$$

and this is again a product of automorphisms, this time with an element of $\Lambda(G)$ on the right and an element of $\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G})$ on the left.

**Proof.** Simply multiply out the matrices and use Proposition 4.2 to obtain the products. We need only justify that the second matrices are in $\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G})$. To this end, note that for either such matrix we have 0 in the bottom left corner, and thus they have $A = B = 1$. Since the matrix gives an isomorphism, by Lemma 2.3 we conclude that the diagonal terms are isomorphisms. This completes the proof.

**Remark.** An alternative characterization of the lemma is that any automorphism $(p, u, r, v)$ with either $u$ or $v$ an isomorphism lies in the subgroup generated by $\Lambda(G)$ and $\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G})$. 
Example 5.5. In general, it need not be true that $u, v$ are always simultaneously isomorphisms. Indeed, for $G = \mathbb{Z}_2$, denote its non-trivial bicharacter by $\text{sgn}$, and the unique isomorphism $\hat{G} \to G$ by $p$. Then the following is in $\text{Aut}(\mathcal{D}(G))$:

$$\begin{pmatrix} 0 & \text{sgn} \\ p & 1 \end{pmatrix}.$$  

Indeed, $-\text{sgn}p$ is the isomorphism $g \mapsto g^{-1}$.

Corollary 5.6. All elements of $\text{Aut}(\mathcal{D}(G))$ of the form $\begin{pmatrix} u & 0 \\ p & v \end{pmatrix}$ form the subgroup $\Lambda(G) \rtimes \text{SpAut}_c(G)$. Here $(w, v) \in \text{SpAut}_c(G)$ acts on $\Lambda(G)$ from the left by $(w, v).(p, \text{id}, 1, \text{id}) = (vpw^*, \text{id}, 1, \text{id})$.

Proof. By Lemma 2.8, any such morphism has $u, v$ isomorphisms. It is easily verified that such morphisms form a subgroup, and by the Lemma the subgroup is the product of the subgroups $\Lambda(G)$ and $\text{SpAut}_c(G)$. In particular, we have

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & 0 \\ 0 & v^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ vpu^{-1} & 1 \end{pmatrix}.$$  

This completes the proof. \qed

Recall that an (exact) factorization of a group $G$ is given by subgroups $H, K$ such that $G = HK$ and $H \cap K = 1$ \cite{15, 26, 27}. Note that neither subgroup is required to be normal.

Our main result also now follows directly from the Lemma and Theorem 2.12.

Theorem 5.7. Let $G$ be a purely non-abelian finite group. Then we have exact factorizations

$$\text{Aut}(\mathcal{D}(G)) = \Lambda(G)(\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G})) = (\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G}))\Lambda(G).$$

We therefore also have the order formula

$$|\text{Aut}(\mathcal{D}(G))| = |\text{End}(Z(G))| \cdot |\text{Hom}(G, \hat{G})| \cdot |\text{Aut}_c(G)| \cdot |\text{Aut}(G)|.$$

Recall that a group is said to be perfect if $G = G'$, the derived subgroup of $G$.

Corollary 5.8. Suppose $G$ is a perfect group. Then

$$\text{Aut}(\mathcal{D}(G)) \cong \Lambda(G) \rtimes \text{Aut}(G).$$

Here the action is $v.(p, \text{id}, 1, \text{id}) = (vp^*, \text{id}, 1, \text{id})$.  

In particular, $G$ is centerless and perfect $\iff$ $\text{Aut}(\mathcal{D}(G)) \cong \text{Aut}(G)$. This latter isomorphism therefore holds for all non-abelian simple groups.

**Proof.** A perfect group is clearly purely non-abelian. Moreover, since $G = G'$ we have $\text{Hom}(G, \widehat{G}) = 1$. Therefore $\text{Aut}(\mathcal{D}(G)) \cong \Lambda(G) \rtimes \text{SpAut}_c(G)$ by Corollary 5.6. It is well known that, for any group $G$, the members of $\text{Aut}_c(G)$ fix $G'$ elementwise. Thus for $G$ perfect $\text{Aut}_c(G) = 1$ and $\text{SpAut}_c(G) \cong \text{Aut}(G)$. Therefore $\text{Aut}(\mathcal{D}(G)) \cong \Lambda(G) \rtimes \text{Aut}(G)$ as claimed. \hfill $\Box$

**Corollary 5.9.** If $Z(G) = 1$, then $\text{Aut}(\mathcal{D}(G)) \cong \text{Aut}(G) \rtimes \text{Hom}(G, \widehat{G})$.

**Example 5.10.** Consider $S_n$, the symmetric group on $n \geq 3$ symbols. Then

$$\text{Aut}(\mathcal{D}(S_n)) \cong \mathbb{Z}_2 \times \text{Aut}(S_n).$$

**Example 5.11.** For $A_n$, the alternating group on $n \geq 5$ symbols,

$$\text{Aut}(\mathcal{D}(A_n)) \cong \text{Aut}(S_n).$$

**Example 5.12.** For $A_4$ we have $\text{Hom}(A_4, \widehat{A}_4) \cong \mathbb{Z}_3$ and thus

$$\text{Aut}(\mathcal{D}(A_4)) \cong S_4 \rtimes \mathbb{Z}_3,$$

where transpositions act by inversion.

**Example 5.13.** Let $D_{2n}$ be the dihedral group of order $2n$. If $n$ is odd, then $\text{Aut}(\mathcal{D}(D_{2n})) \cong \mathbb{Z}_2 \times \text{Hol}(\mathbb{Z}_n)$, where $\text{Aut}(D_{2n}) \cong \text{Hol}(\mathbb{Z}_n)$ is the holomorph of $\mathbb{Z}_n$. In this case, $|\text{Aut}(\mathcal{D}(D_{2n}))| = 2n\phi(n)$, where $\phi$ is the Euler totient function. When $n$ is even the center is non-trivial, and the description becomes more complicated. Indeed, when $n$ is even and not divisible by 4, $D_{2n} \cong \mathbb{Z}_2 \times D_n$, and so $D_{2n}$ is not purely non-abelian. We leave further details on this to the next section.

**Example 5.14.** For $q \geq 4$ a prime power, $G = \text{SL}(2, q)$ is quasisimple, so in particular perfect, and has $\text{Aut}(G) \cong \text{PGL}(2, q)$, a projective semilinear group. Therefore

$$\text{Aut}(\mathcal{D}(\text{SL}(2, q))) \cong \text{End}(\mathbb{Z}_q) \rtimes \text{PGL}(2, q).$$

When $q$ itself is prime, note that $\text{End}(\mathbb{Z}_q) \cong \mathbb{Z}_q$ and $\text{PGL}(2, q) = \text{PSL}(2, q)$.

We can summarize our results on purely non-abelian groups with the following.

**Theorem 5.15.** Let $G$ be a finite group. Then the following are equivalent.

i) $G$ is purely non-abelian.
ii) Every \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\) has \(u, v\) isomorphisms.

iii) For any \(r' \in \text{Hom}(G, \hat{G})\) and \((p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\), then also \((p, u, r', v) \in \text{Aut}(\mathcal{D}(G))\).

iv) \(\text{Aut}(\mathcal{D}(G)) = \Lambda(G)(\text{SpAut}_c(G) \ltimes \text{Hom}(G, \hat{G}))\) is an exact factorization.

Our next goal is to find a number of normal subgroups of \(\text{Aut}(\mathcal{D}(G))\) and determine when they have complements.

6. Restriction to group-likes

Let \(\Gamma = \Gamma_G = \hat{G} \times G\) be the group-like elements of \(\mathcal{D}(G)\). Since any morphism of Hopf algebras must send group-like elements to group-like elements, there is a natural restriction of \(\text{Hom}(\mathcal{D}(G), \mathcal{D}(H))\) to the group homomorphisms \(\text{Hom}(\Gamma_G, \Gamma_H)\). In particular, this gives a group homomorphism \(\text{Aut}(\mathcal{D}(G)) \rightarrow \text{Aut}(\Gamma)\). This simple observation was used earlier in the proof of Theorem 2.5.

Here and for the remainder of the paper, let \(N\) be the kernel of the restriction \(\text{Aut}(\mathcal{D}(G)) \rightarrow \text{Aut}(\Gamma)\), and identify \(\text{Aut}(\mathcal{D}(G))/N\) with the image. In particular, \(N\) is the normal subgroup of all automorphisms of \(\mathcal{D}(G)\) which fix every element of \(\Gamma\). When \(N = 1\) this means that \(\text{Aut}(\mathcal{D}(G))\) is isomorphic to a subgroup of \(\text{Aut}(\Gamma)\). In this section we describe \(N\) explicitly, and determine when \(N = 1\) holds. In the next section we will determine when \(N\) and certain other subgroups have a complement.

It is helpful to know exactly what the restriction map looks like.

**Lemma 6.1.** Let \(\psi = (p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))\). Then for \(\chi \in \hat{G}\) and \(g \in G\) we have

\[
(6.1) \quad \psi(\chi \# g) = r(g)u(\chi) \# p(\chi)v(g).
\]

Thus the restriction of \(\psi\) gives the group homomorphism

\[
(6.2) \quad (\chi, g) \mapsto (r(g)u(\chi), p(\chi)v(g)),
\]

and this will be an isomorphism whenever \(\psi\) is.

Note that since \(u\) is a unitary coalgebra map, it restricts to a group homomorphism \(\hat{G} \rightarrow \hat{H}\).

In general, however, \(\psi\) need not be an isomorphism for its restriction to be an isomorphism.

**Example 6.2.** If \(G\) is a perfect group, then \(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \text{End}(\mathcal{D}(G))\) is clearly not an isomorphism, but restricts to the identity on \(\Gamma_G = G\).
We now proceed to determine the membership and structure of \(N\).

We have previously defined \(\Lambda(\mathcal{G})\) in Definition 4.1.

**Definition 6.3.** For \(G\) a finite group, define
\[
\Lambda_c(G) = \{(p, u, 1, \text{id}) \in \text{Aut}(\mathcal{D}(G))\}.
\]

Clearly \(\Lambda(G) \subseteq \Lambda_c(G)\). For \((p, u, 1, \text{id}) \in \Lambda_c(G)\) we have \(u^* = u^* \circ \text{id}\) is a normal group endomorphism. In particular, if \(u^* \in \text{Aut}(G)\), then in fact \(u^* \in \text{Aut}_c(G)\). Furthermore, for \(u^* \in \text{Aut}_c(G)\),
\[
(p, u, 1, \text{id}) = (1, u, 1, \text{id}) \circ (p, \text{id}, 1, \text{id})
\]
is a composition of automorphisms by Propositions 4.2 and 4.8 and so is itself an automorphism. It may not be immediately obvious that \(u\) must be an isomorphism for any element of \(\Lambda_c(G)\), however.

**Lemma 6.4.** Every \((p, u, 1, \text{id}) \in \Lambda_c(G)\) has \(u^* \in \text{Aut}_c(G)\). Moreover, \(\Lambda_c(G)\) is the subgroup of \(\text{Aut}(\mathcal{D}(G))\) fixing \(1 \times G \subseteq \Gamma\) element-wise.

**Proof.** Let \((p_1, u_1, 1, \text{id}), (p_2, u_2, 1, \text{id}) \in \Lambda_c(G)\). Then
\[
\begin{pmatrix} u_1 & 0 \\ p_1 & 1 \end{pmatrix} \begin{pmatrix} u_2 & 0 \\ p_2 & 1 \end{pmatrix} = \begin{pmatrix} u_1 u_2 & 0 \\ p_1 u_2 + p_2 & 1 \end{pmatrix}.
\]
Since \((p_1, u_1, 1, \text{id})\) is invertible and has finite order, we see that we must have \(u_1^n = \text{id}\) for some \(n \in \mathbb{N}\). Thus \(u\) must be invertible. This proves the first claim, and the matrix product above then shows that \(\Lambda_c(G)\) is a subgroup.

Now, on the other hand, let \(g \in G\) and \(\psi = (p, u, r, v) \in \text{Aut}(\mathcal{D}(G))\). Then by (6.1),
\[
\psi(\varepsilon \# g) = r(g) \# v(g).
\]
Thus \(\psi\) fixes all of \(G\) if and only if \(r\) is trivial and \(v\) is the identity. So by definition, if and only if \(\psi \in \Lambda_c(G)\). This completes the proof.

**Corollary 6.5.** \(\Lambda_c(G) \cong \text{Aut}_c(G) \rtimes \Lambda(G)\) where \(\text{Aut}_c(G)\) acts on \(\Lambda(G)\) on the right by \((p, 1, 1, \text{id})^w = (p(w^{-1})^*, \text{id}, 1, \text{id})\).

**Proof.** We embed \(\text{Aut}_c(G)\) into \(\Lambda_c(G)\) (and \(\text{Aut}(\mathcal{D}(G))\)) in particular as in Proposition 4.3,
\[
w \mapsto \begin{pmatrix} (w^{-1})^* & 0 \\ 0 & 1 \end{pmatrix}.
\]
Then we compute
\[
\begin{pmatrix} w^* & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} \begin{pmatrix} (w^{-1})^* & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p(w^{-1})^* & 1 \end{pmatrix}.
\]
Theorem 6.7. \(N\) equivalent to \(A\) \(\leq\) \(\Lambda(G)\). Clearly \(\text{Aut}_c(G)\) and \(\Lambda(G)\) intersect trivially, and by Lemma 6.4 we conclude that \(\Lambda_c(G)\) is the product of these subgroups. This completes the proof.

We now consider which elements of \(\Lambda_c(G)\) fix \(\hat{G}\), which by construction gives us the normal subgroup \(N\).

Consider \(\psi \in \Lambda_c(G)\) and let \((\chi, g) \in \Gamma\). Then \(\psi(\chi \# g) = u(\chi) \# p(\chi)g\). Thus \(\psi\) fixes all of \(\Gamma\) if and only if \(p\) is trivial on \(\hat{G}\), and \(u\) is the identity on \(\hat{G}\). Since \(u^* \in \text{Aut}_c(G)\), we see that \(\chi = u(\chi) = \chi \circ u^*\) for all \(\chi \in \hat{G}\) \(\iff u^*(g^{-1})g \in Z(G) \cap G'\) for all \(g \in G\).

**Definition 6.6.** Let \(G\) be any group, and define

\[
\text{Aut}_c'(G) = \{\phi \in \text{Aut}_c(G) \mid \phi(g^{-1})g \in Z(G) \cap G' \text{ for all } g \in G\}.
\]

It is easy to show that \(\text{Aut}_c'(G)\) is a normal subgroup of \(\text{Aut}_c(G)\) and also \(\text{Aut}(\hat{G})\). What we have just shown is that \(u^* \in \text{Aut}_c'(G)\).

Furthermore, since \(p\) is given by an isomorphism from \(\hat{A} \to B\), we conclude that \(p\) is trivial on \(\hat{G}\) \(\iff \chi|_A = \varepsilon_A\) for all \(\chi \in \hat{G}\), which is in turn equivalent to \(A \leq G'\). Since necessarily \(A \leq Z(G)\), this is equivalent to \(A \leq Z(G) \cap G'\). Any such \(p\) can be uniquely identified with a member of the group \(\text{Hom}(Z(G) \cap G', Z(G))\) under the identification of \(p\) with an element of \(\text{End}(Z(G))\), and vice versa. Moreover, this respects the group structures.

Combining, we get the desired description of \(N\).

**Theorem 6.7.** \(N \cong \text{Aut}_c'(G) \times \text{Hom}(Z(G) \cap G', Z(G))\). Thus, \(N = 1\) if and only if \(Z(G) \cap G' = 1\). In particular, if \(G\) is abelian or centerless, then \(N = 1\). At the other extreme, \(Z(G) \leq G' \iff N = \Lambda_c(G)\), and the kernel in this case is non-trivial precisely when \(Z(G) \neq 1\).

Recall that a group \(G\) is called a stem group if \(Z(G) \leq G'\) [13]. Note that any stem group is necessarily purely non-abelian. By Lemma 5.4 we get the following.

**Corollary 6.8.** If \(G\) is a stem group, then

\[
\text{Aut}(\mathcal{D}(G))/N \cong \text{Aut}(G) \times \text{Hom}(G, \hat{G}).
\]

In the next section we will show that

\[
\text{Aut}(\mathcal{D}(G)) \cong N \rtimes (\text{Aut}(G) \times \text{Hom}(G, \hat{G}))
\]

precisely when \(G\) is a stem group.

**Example 6.9.** \(N = 1\) for \(D_{2n}\), the dihedral group of order \(2n\), if and only if \(n \not\equiv 0 \mod 4\). On the other hand, \(D_{2n}\) is a stem group whenever \(n\) is divisible by \(4\), and so the corollary applies. See also Examples 5.13 and 7.4.
Example 6.10. It is well known that, for any group, the elements of $\text{Aut}_c(G)$ fix $G'$ elementwise. So let $G$ be a perfect group. Then $G$ is trivially a stem group, $\text{Hom}(G, \hat{G}) = 1$, and we have $N = \Lambda(G) \cong \text{End}(Z(G))$. Therefore $\text{Aut}(\mathcal{D}(G))/N \cong \text{Aut}(G)$. This also follows from Corollary 5.8 which gives a stronger result.

7. Exact factorizations and semidirect products for $\text{Aut}(\mathcal{D}(G))$

We now wish to expand our ability to find exact factorizations for $\text{Aut}(\mathcal{D}(G))$, and to determine when they are semidirect products. These results may be considered as variations on the main theorem.

We have already shown that $\Lambda(G)$ and $\text{SpAut}_c(G)$ give an exact factorization of $\text{Aut}(\mathcal{D}(G))$ if and only if $G$ is purely non-abelian. The next result determines when this is actually a semidirect product.

**Theorem 7.1.** $\Lambda(G)$ is normal in $\text{Aut}(\mathcal{D}(G))$ if and only if $G$ is a stem group. Therefore, $\text{Aut}(\mathcal{D}(G)) \cong \Lambda(G) \rtimes (\text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G}))$ if and only if $G$ is a stem group.

**Proof.** Let $\begin{pmatrix} u & r \\ 0 & v \end{pmatrix} \in \text{SpAut}_c(G) \rtimes \text{Hom}(G, \hat{G}) \subseteq \text{Aut}(\mathcal{D}(G))$. Then its inverse is $\begin{pmatrix} u^{-1} & -u^{-1}rv^{-1} \\ 0 & v^{-1} \end{pmatrix}$. Therefore the conjugate

$$ morphur0v \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} \begin{pmatrix} u^{-1} & -u^{-1}rv^{-1} \\ 0 & v^{-1} \end{pmatrix} $$

is equal to

$$ \begin{pmatrix} 1 + rpu^{-1} & -rpu^{-1}rv^{-1} \\ vpu^{-1} & -vpu^{-1}rv^{-1} + 1 \end{pmatrix}. $$

For this to be an element of $\Lambda(G)$, the diagonal entries must both be 1. So $rpu^{-1} = 0$ and $-vpu^{-1}rv^{-1} = 0$. Since $u, v$ are isomorphisms, this simplifies to $rp = 0$ and $pu^{-1}r = 0$. Note that $rp = 0$ implies that $-rpu^{-1}rv^{-1} = 0$, which is the other condition for $\Lambda(G)$ to be normal. Now $rp = 0$ for all choices of $r, p \Leftrightarrow Z(G) \leq G'$. In other words, $G$ is necessarily a stem group, and therefore also purely non-abelian. So we may suppose that $G$ is a stem group. For any $g \in G$ and $z \in Z(G)$ the coefficient of $e_z$ in $r(g)$ is therefore 1. Since $Z(G) \text{char } G$ and $u^* \in \text{Aut}(G)$, we conclude that $pu^{-1}v = 0$.

This completes the proof. □

We can improve the situation by enlarging our consideration to $\Lambda_c(G)$.
Lemma 7.2. If \( G \) is purely non-abelian, then \( \Lambda_c(G) \) and \( \text{Aut}(G) \rtimes \text{Hom}(G, \hat{G}) \) give an exact factorization of \( \text{Aut}(D(G)) \).

Proof. Suppose \( G \) is purely non-abelian and \( \psi = \begin{pmatrix} u & r \\ p & v \end{pmatrix} \in \text{Aut}(D(G)) \).

We can therefore write
\[
\begin{pmatrix} u & r \\ p & v \end{pmatrix} = \begin{pmatrix} u & 0 \\ p & -pu^{-1}r + v \end{pmatrix} \begin{pmatrix} 1 & u^{-1}r \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ pu^{-1} & 1 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & -pu^{-1}r + v \end{pmatrix} \begin{pmatrix} 1 & u^{-1}r \\ 0 & 1 \end{pmatrix}.
\]

Now, the matrix in the middle may be written as the product
\[
\begin{pmatrix} u(-pu^{-1}r + v)^* & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} ((-pu^{-1}r + v)^{-1})^* & 0 \\ 0 & -pu^{-1}r + v \end{pmatrix}.
\]

We conclude that \( \psi = ST \) with \( S \in \Lambda_c(G) \) and \( T \in \text{Aut}(G) \rtimes \text{Hom}(G, \hat{G}) \) where
\[
S = \begin{pmatrix} 1 & 0 \\ pu^{-1} & 1 \end{pmatrix} \begin{pmatrix} u(-pu^{-1}r + v)^* & 0 \\ 0 & 1 \end{pmatrix},
\]
\[
T = \begin{pmatrix} ((-pu^{-1}r + v)^{-1})^* & 0 \\ 0 & -pu^{-1}r + v \end{pmatrix} \begin{pmatrix} 1 & u^{-1}r \\ 0 & 1 \end{pmatrix}.
\]

Therefore \( \text{Aut}(D(G)) = \Lambda_c(G)(\text{Aut}(G) \rtimes \text{Hom}(G, \hat{G})) \), and clearly
\[
\Lambda_c(G) \cap \text{Aut}(G) \rtimes \text{Hom}(G, \hat{G}) = 1.
\]

So by definition, \( \Lambda_c(G) \) and \( \text{Aut}(G) \rtimes \text{Hom}(G, \hat{G}) \) give an exact factorization. \( \square \)

We subsequently have the following variation of Theorem 7.1.

Theorem 7.3. \( \Lambda_c(G) \) is normal in \( \text{Aut}(D(G)) \) \( \iff \) \( G \) is a stem group. Therefore, \( \text{Aut}(D(G)) \cong \Lambda_c(G) \rtimes (\text{Aut}(G) \rtimes \text{Hom}(G, \hat{G})) \) \( \iff \) \( G \) is a stem group.

Proof. We consider the conjugation action of \( \text{Aut}(G) \rtimes \text{Hom}(G, \hat{G}) \) on \( \Lambda_c(G) \). We can compute that the conjugate
\[
\begin{pmatrix} (v^{-1})^* & r \\ 0 & v \end{pmatrix} \begin{pmatrix} u & 0 \\ p & 1 \end{pmatrix} \begin{pmatrix} v^* & -v^*rv^{-1} \\ 0 & v^{-1} \end{pmatrix}
\]

is equal to
\[
\begin{pmatrix} -(v^{-1})^*uv^* + rv^* \\ vpu^* \\ vpu^* \\ -(v^{-1})^*uv^*rv^{-1} - rv^*rv^{-1} + rv^{-1} \end{pmatrix}.
\]
For this to be an element of $\Lambda_c(G)$, we must have the upper right entry is 0, and the lower right is 1. The last condition is equivalent to $-vpv^*rv^{-1} = 0$, which is equivalent to $pv^*r = 0$. This must hold for all choices of $p, v, r$ for normality to hold. Thus we have $pr = 0$ for all $p, r$ in particular, and as before this implies that $Z(G) \leq G'$. Thus for normality to hold we must have that $G$ is a stem group, and so in particular purely non-abelian.

So we may suppose, then, that $G$ is a stem group, and therefore $pv^*r = 0$ for all choices of $p, v, r$. We need only show that the upper right entry, the bicharacter in the conjugate, is trivial. Since $G$ is a stem group, this bicharacter being trivial is equivalent to $-((v^{-1})^*uv^* + 1)r = 0$. Since $u^* \in \text{Aut}_c(G)$, it follows by normality that $vu^*v^{-1} \in \text{Aut}_c(G)$ as well. Therefore $-((v^{-1})^*uv^* + 1)$ is the dual of a group homomorphism $G \to Z(G)$. Since $G$ is a stem group, it therefore follows that $-((v^{-1})^*uv^* + 1)r = 0$, as desired.

This completes the proof. 

Example 7.4. Consider $G = D_{2n}$ with $4 \mid n$. Then $\hat{G} \cong \mathbb{Z}_2^2$, and subsequently $\text{Hom}(G, \hat{G}) \cong \mathbb{Z}_2^4$. Furthermore, $Z(G) \cong \mathbb{Z}_2$, implying $\Lambda(G) \cong \mathbb{Z}_2$, and it is routine to check that $\text{Aut}_c(G) \cong \mathbb{Z}_2^2$. In particular, $\Lambda_c(G) \cong \mathbb{Z}_2^3$ and $\text{SpAut}_c(G) \cong \mathbb{Z}_2^2 \rtimes \text{Hol}(\mathbb{Z}_n)$. Since $G$ is a stem group, the previous two theorems give us the isomorphisms

$$\text{Aut}(\mathcal{D}(D_{2n})) \cong \mathbb{Z}_2^3 \rtimes (\text{Hol}(\mathbb{Z}_n) \rtimes \mathbb{Z}_2^4)$$

$$\cong \mathbb{Z}_2 \times ((\mathbb{Z}_2^2 \rtimes \text{Hol}(\mathbb{Z}_n)) \rtimes \mathbb{Z}_2^4).$$

See also Examples [5.13] and [6.9]. Note that in this case we have

$$|\text{Aut}(\mathcal{D}(D_{2n}))| = 2^7 n \phi(n),$$

where $\phi$ is the Euler totient function. For $n = 4$ we see that $\text{Aut}(\mathcal{D}(D_8))$ has order $2^{10} = 1024$.

Example 7.5. Let $Q$ be the quaternion group of order 8. The following are all well-known:

$$Q' = Z(Q) \cong \mathbb{Z}_2,$$

$$\hat{Q} \cong \mathbb{Z}_2^2,$$

$$\text{Aut}(Q) \cong S_4,$$

$$\text{Aut}_c(Q) \cong \mathbb{Z}_2^2.$$
Proof. Since the kernel $N$ is normal and is contained in $\Lambda_c(G)$, by Lemma [7.2] it suffices to prove that $N$ has a complement in $\Lambda_c(G)$.

Let $u^*_c \in \text{Aut}_{c'}$ and $p_c$ be such that $(p_c, u_c, 1, \text{id}) \in N$. Then for any $(p, u, 1, \text{id}) \in \Lambda_c(G)$ we may write

\[
\begin{pmatrix}
  u & 0 \\
  1 & p
\end{pmatrix} = \begin{pmatrix}
  u_c & 0 \\
  p_c & 1
\end{pmatrix} \begin{pmatrix}
  u_c^{-1}u & 0 \\
  -p_cu_c^{-1}u + p & 1
\end{pmatrix}.
\]

We consider first the bottom left entries. Since $Z(G)$ and $G'$ are both characteristic in $G$, it follows that $Z(G) \cap G'$ is characteristic in $G$. Therefore we have that $(p_cu_c^{-1}u, 1, \text{id}) \in N$. So for $N$ to have a complement, we conclude that it is necessary for $\text{Hom}(Z(G) \cap G', Z(G))$ to be a direct factor of $\text{End}(Z(G))$. Applying Fitting’s Lemma to the canonical injection, we conclude that $\text{Hom}(Z(G) \cap G', Z(G))$ is a direct factor of $\text{End}(Z(G))$ if and only if $Z(G) \cap G'$ is a direct factor of $Z(G)$.

So suppose that $Z(G) \cap G'$ is a direct factor of $Z(G)$, and write

\[
Z(G) = (Z(G) \cap G') \times C
\]

for some abelian group $C$. Considering now the upper left entries, we see that for $N$ to have a complement we must have that the normal subgroup $\text{Aut}_{c'}(G)$ has a complement in $\text{Aut}_{c'}(G)$. Since $G$ is purely non-abelian, by [1] there is a bijection $\text{Aut}_{c'}(G) \to \text{Hom}(G, Z(G))$ given by $\phi \mapsto (g \mapsto \phi(g)g^{-1})$; letting $S$ denote the inversion map on the group, this is equivalent to $\phi \mapsto \phi \ast S$. For any $\phi \in \text{Aut}_{c'}(G)$ let $z_\phi$ denote the image of $\phi$ under this bijection. Thus $\phi = z_\phi \ast \text{id}$. We have the following identities:

\[
\begin{align}
(7.1) & \quad z_\phi^{-1} = (S \circ z_\phi) \circ \phi^{-1}, \\
(7.2) & \quad z_{\phi \circ \psi} = (z_\phi \circ \psi) \ast z_\psi.
\end{align}
\]
From this it is easy to see that the pre-image of $\text{Hom}(G, C)$ forms a subgroup of $\text{Aut}_c(G)$ which intersects $\text{Aut}_c(G)$ trivially. We need only verify that $\text{Aut}_c(G)$ is the product of these two subgroups. By assumptions, we may uniquely write $z_\phi = z_2 \ast z_1$ with $z_1 \in \text{Hom}(G, Z(G) \cap G')$ and $z_2 \in \text{Hom}(G, C)$. Set $\phi_1 = z_1 \ast \text{id}$ and $\phi_2 = (z_2 \circ \phi_1^{-1}) \ast \text{id}$. Then $\phi = \phi_2 \circ \phi_1$, and $z_{\phi_2} = z_2 \circ \phi_1^{-1} \in \text{Hom}(G, C)$.

This completes the proof. □

Remark. It was essential that we knew $\text{Aut}_c(G)$ was normal. In general, direct factors of $\text{Hom}(G, Z(G))$ can be used to give exact factorizations of $\text{Aut}_c(G)$, but in general it is not necessary that any of the subgroups so produced are normal.

Example 7.7. Define

$$G = \langle x, y, z \mid x^4 = y^4 = z^2 = 1, [x, y] = z, [x, z] = [y, z] = 1 \rangle.$$  

This is a group of order 32, identified in GAP [10] as SmallGroup(32,2).

It is easy to verify that $G$ is purely non-abelian, $Z(G) = \langle x^2, y^2, z \rangle \cong \mathbb{Z}_2^3$ and $G' = \langle z \rangle \cong \mathbb{Z}_2$. Clearly $G' = Z(G) \cap G'$ is a direct factor of $Z(G)$. Therefore the theorem applies, and the kernel $N$ is non-trivial and has a complement in $\text{Aut}(\mathcal{D}(G))$. Note that $G$ is not a stem group, so $\Lambda(G)$ and $\Lambda_c(G)$ are not normal.

Note that the structure, and even membership, of $\text{Aut}(\mathcal{D}(D_{2n}))$ when $n \equiv 2 \mod 4$ is not determined by our results, since then $D_{2n} \cong \mathbb{Z}_2 \times D_n$ is not purely non-abelian. The completion of the general case, which is analogous to the case for groups [6, 7], is left for a future paper. For now, we prove only the following special case.

Proposition 7.8. Let $G = C \times H$, where $C, H$ have no common non-trivial direct factors. Then

$$\text{Aut}(\mathcal{D}(G)) \cong \text{Aut}(\mathcal{D}(C)) \times \text{Aut}(\mathcal{D}(H))$$

if and only if $(|Z(\Gamma_C)|, |Z(\Gamma_H)|) = 1$.

Proof. By Proposition 5.1, $\text{Aut}(\mathcal{D}(C)) \times \text{Aut}(\mathcal{D}(H))$ is always a subgroup, so we need only determine when every automorphism is of this form.

Note that $(|Z(C)||\tilde{C}, |Z(H)||\tilde{H}|) = 1$ is equivalent to the following three conditions all holding:

i) $(|\tilde{C}|, |\tilde{H}|) = 1$;

ii) $(|Z(C)|, |Z(H)|) = 1$;

iii) $(|\tilde{C}|, |Z(H)|) = (|\tilde{H}|, |Z(C)|) = 1$. 
Now we observe that \( \text{Hom}(C \times H, \hat{C} \times \hat{H}) \cong \text{Hom}(C, \hat{C}) \times \text{Hom}(H, \hat{H}) \) \( \Leftrightarrow \) \( (|\hat{H}|, |\hat{K}|) = 1 \), and that \( \text{End}(Z(H) \times Z(C)) \cong \text{End}(Z(H)) \times \text{End}(Z(C)) \Leftrightarrow (|Z(H)|, |Z(C)|) = 1 \).

Suppose that \( \text{Aut}(D(G)) = \text{Aut}(D(C)) \times \text{Aut}(D(H)) \). Then under the imbedding of \( \text{Aut}(G) \hookrightarrow \text{Aut}(D(G)) \), we conclude that \( \text{Aut}(G) = \text{Aut}(C) \times \text{Aut}(H) \). Since \( C, H \) have no common factors, by \([7]\) this holds \( \Leftrightarrow \) both \( \text{Hom}(H, Z(C)) \) and \( \text{Hom}(C, Z(H)) \) are trivial. By properties of the derived subgroup, this is equivalent to \( \text{Hom}(\hat{C}, Z(H)) \) and \( \text{Hom}(\hat{H}, Z(C)) \) both being trivial, which is in turn equivalent to \( (|\hat{H}|, |Z(C)|) = (|\hat{C}|, |Z(H)|) = 1 \).

Combining this with the observations on \( \text{Hom}(G, \hat{G}) \) and \( \text{End}(Z(G)) \), we conclude that \( \text{Aut}(D(G)) = \text{Aut}(D(C)) \times \text{Aut}(D(H)) \) implies that \((|Z(C)||\hat{C}|, |Z(H)||\hat{H}|) = 1 \).

Now suppose that \((|Z(C)||\hat{C}|, |Z(H)||\hat{H}|) = 1 \). It suffices to show that for \((p, u, r, v) \in \text{Aut}(D(G)) \) that all four components split over \( C, H \). We have already observed that this is true for \( p, r \), so we need only prove it is true for \( u, v \). By flipping, we need only prove it is true for \( v \).

Any \( \psi \in \text{Aut}(D(G)) \) restricts to an element of \( \text{Aut}(\Gamma_G) = \text{Aut}(\Gamma_C \times \Gamma_H) \). By the assumptions on \( C, H \) and the orders, we conclude that \( \Gamma_C \) and \( \Gamma_H \) have no common direct factors. Thus by \([7]\) the restriction of \( \psi \) is an element of

\[
\begin{pmatrix}
\text{Aut}(\Gamma_C) & \text{Hom}(\Gamma_H, Z(\Gamma_C)) \\
\text{Hom}(\Gamma_C, Z(\Gamma_H)) & \text{Aut}(\Gamma_H)
\end{pmatrix}
\]

By the order assumptions we conclude that the Hom terms are all trivial. On the other hand, in terms of \((p, u, r, v)\) we compute the off-diagonal terms to be

\[
t(\chi_H, h) = \pi_C(u(\chi_H, \varepsilon))\pi_C(v(h, 1)),
\]

\[
w(\chi_C, c) = \pi_H(u(\varepsilon, \chi_C))\pi_H(v(1, c)),
\]

for all \( \chi_H \in \hat{H}, \chi_C \in \hat{C}, h \in H, c \in C \). Since these maps are trivial, we conclude that the projections involving \( v \) are both trivial. In particular, we conclude that \( v \in \text{End}(C) \times \text{End}(H) \), as desired.

This completes the proof. \( \square \)

**Example 7.9.** The proposition fails to apply to any of the following groups.

i) \( A \times A_4 \) for any abelian group \( A \) with order divisible by 3, since \( \widehat{A_4} \cong \mathbb{Z}_3 \).
ii) $A \times S_n$ for any abelian group $A$ of even order, since $\hat{S}_n \cong \mathbb{Z}_2$. In particular, it fails to apply to $D_{2n} \cong \mathbb{Z}_2 \times D_n$ whenever $n \equiv 2 \mod 4$.

**Example 7.10.** The proposition applies to all of the following groups.

i) $A \times G$, where $A$ is any abelian group and $G$ is any centerless perfect group.

ii) $A \times S_n$ and $A \times D_{2n}$, where $A$ is any abelian group of odd order.

iii) $A \times A_4$ where $A$ is any abelian group with order coprime to 3.

iv) $G \times H$ when $G$ and $H$ have coprime order. This is the case if $G$ is a $p$-group and $H$ a $q$-group for distinct primes $p, q$, for example. If $G$ or $H$ have abelian direct factors then computing the automorphisms of their doubles may itself be non-trivial, however.

### 8. Action on modules

In this section we describe the action of $\text{Aut}(\mathcal{D}(G))$ on the category of representations $\text{Rep}(\mathcal{D}(G))$.

Given algebras $A, B$ and an algebra map $f: A \to B$, we have the induced action $\text{Rep}(B) \to \text{Rep}(A)$ where $V \in \text{Rep}(B)$ is sent to the $A$-module with the same vector space structure and action defined by $a.v = f(a).v$ for all $a \in A, v \in V$. This is an equivalence of tensor categories when $A, B$ are Hopf algebras and $f$ is an isomorphism of Hopf algebras. Modules are identified by their characters as usual, and we use the two interchangeably whenever convenient.

It is well known that the irreducible modules of $\mathcal{D}(G)$ are parametrized by (equivalence classes of) pairs $(s, \eta)$ where $s \in G$, and $\eta$ is an irreducible character of $C_G(s)$. The pair depends only on $\text{class}(s)$, the conjugacy class of $s$ in $G$, and the isomorphism class of $\eta$. See Dijkgraaf et al. [9] for further details. More generally, $\eta$ can be any character of $C_G(s)$, and we obtain a module of $\mathcal{D}(G)$ in the same way: by inducing from $C_G(s)$ up to $G$. As such, we use the notation $(s, \eta)$ to denote any such module, even when $\eta$ is not irreducible. For $(s, \eta)$, the action of $e_g \# h$ is trivial whenever $g \notin \text{class}(s)$. We say that such a module is supported at $\text{class}(s)$, or simply at $s$ when convenient.

The following description of the character of $(s, \chi)$ was proven in [16].

**Lemma 8.1.** Consider a module of $\mathcal{D}(G)$ of the form $(s, \eta)$, with character $\chi$. Let $\text{class}(s)$ be the conjugacy class of $s$ in $G$. For any $y \in \text{class}(s)$ let $y' \in G$ be such that $s^{y'} = y$. If $g \in \text{class}(s)$ and
If $a = \gamma^g$ for some $\gamma \in C_G(s)$, then $\chi(e_g \# a) = \eta(\gamma)$. In all other cases, $\chi(e_g \# a) = 0$.

Let $(p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))$ have $B$ central. Let $s \in H$ and let $\eta$ be any irreducible character of $C_H(s)$. By Schur’s Lemma we may write $\eta(z) = \mu(z)\eta(1)$ for all $z \in Z(H)$, where $\mu$ is some linear character of $Z(H)$. Since $B$ is central, $B \leq C_H(s)$ for every $s \in H$. The restriction of $\mu$ to $B$ is therefore also a linear character of $B$. Define the following value for each such choice of $s, \eta$:

\[ P(\eta) = \frac{1}{\dim \eta} \sum_{a \in A} \eta(p(e_a))a. \]

Note that $P(\eta)$ is in $\mathbb{K}A$ by construction. Indeed, by the previous remarks and properties of $p$ it follows that there is a unique $a' \in A$ such that $\eta(p(e_a)) = \dim \eta \delta_{a,a'}$, so that $P(\eta) \in A$ for all choices of $s, \eta$.

For the remainder of this section we will find it convenient to write the components in terms of their coefficients. We use the original notation from [2]:

\[ p(e_g) = \sum_{h \in H} \lambda(g, h)h, \]
\[ r(g) = \sum_{h \in H} \omega(g, h)e_h. \]

Note that $\omega$ is a bilinear bicharacter. In this notation, the values of $\psi = (p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))$ may be expressed as

\[ \psi(e_g \# h) = \sum_{y \in H, z \in B} \lambda(gu^*(y)^{-1}, z)\omega(h, y)e_y \# zv(h), \]

whenever $u$ is a morphism of Hopf algebras.

Under mild assumptions, the induced map on representations will send a simple module to a (not necessarily simple) module supported on a single conjugacy class.

**Lemma 8.2.** Let $\psi \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))$ have $A, B$ central. Then the induced map $\text{Rep}(\mathcal{D}(H)) \to \text{Rep}(\mathcal{D}(G))$ sends an irreducible module $(s, \eta)$ to a module supported at $P(\eta)u^*(s)$.

**Proof.** Let $\xi$ denote the character of the image module and $\chi$ the character of $(s, \eta)$. Then by definition

\[ \xi(e_g \# h) = \sum_{z \in B} \sum_{y \in H} \lambda(gu^*(y)^{-1}, z)\omega(h, y)\chi(e_y \# zv(h)). \]

By the preceding Lemma, the non-zero terms in the sum require $y \in \text{class}(s)$ and $zv(h) = \gamma^y$ for some $\gamma \in C_H(s)$; note that by centrality...
of $A$ this last condition is equivalent to saying $v(h) = \gamma y'$ for some $\gamma \in C_H(s)$. Therefore we may write
\[ \xi(e_g \# h) = \omega(h, s) \sum_{\substack{y \in \text{class}(s) \\cap \{v(h) = \gamma y'\}}} \left( \sum_{z \in B} \lambda(gu^*(y)^{-1}, z)\mu(z) \right) \eta(\gamma) \]
\[ = \omega(h, s) \sum_{\substack{y \in \text{class}(s) \\cap \{v(h) = \gamma y'\}}} \left( \frac{1}{\dim \eta} \eta(p(e_{gu^*(y)^{-1}})) \right) \eta(\gamma) \]

(8.6)

As previously noted, the term in the parentheses is non-zero, and equal to one, precisely when $gu^*(y)^{-1} = P(\eta)$. Combining, and using the assumption that $A \leq Z(G)$, we have $g \in P(\eta)u^*(\text{class}(s)) \subseteq \text{class}(P(\eta)u^*(s))$. Thus $\xi$ is supported at $P(\eta)u^*(s)$ as claimed. $\square$

In equation (8.6) we see that the summation over $y$ is counting the number of elements $y \in \text{class}(s)$ such that $gu^*(y)^{-1} = P(\eta)$. This number could be something other than 1 in general. Indeed, it may happen that $P(\eta)u^*(\text{class}(s))$ is a proper subset of $\text{class}(P(\eta)u^*(s))$.

Clearly we have that $u^*(\text{class}(s)) = \text{class}(u^*(s))$ if and only if for all $g \in \text{class}(u^*(s))$ there exists a unique $y \in \text{class}(s)$ with $g = u^*(y)$. The addition of the central element $P(\eta)$ as above does not change this characterization.

**Lemma 8.3.** Let $G, H$ be finite groups and suppose
\[ (p, u, r, v) \in \text{Hom}(D(G), D(H)) \]
is such that $G = A \text{Im}(u^*)$ and $A \leq Z(G)$. Then
\[ u^*(\text{class}(s)) = \text{class}(u^*(s)) \]
for all $s \in H$.

**Proof.** For any $x \in G$ we may write $x = au^*(h)$ for some $a \in A, h \in H$. Then for any $s \in H$ we have
\[ xu^*(s)x^{-1} = u^*(hsh^{-1}). \]

(8.7)

The result now follows. $\square$

Note that the result is stronger than the observation that $\text{Im}(u^*) \subseteq G$ under the same assumptions.

It is easily checked $(p, u, r, v) \in \text{Hom}(D(G), D(H))$ has $A, B$ central and $v \circ u^*$ normal if and only if $(p, u, r, v)$ is flippable. From this we get the description of the induced action on the representation categories.
Theorem 8.4. Let \((p, u, r, v) \in \text{Hom}(\mathcal{D}(G), \mathcal{D}(H))\) be a flippable homomorphism such that \(A \text{Im}(u^*) = G\). Then the induced map \(\text{Rep}(\mathcal{D}(H)) \to \text{Rep}(\mathcal{D}(G))\) is given by
\[
(s, \eta) \mapsto (P(\eta) u^*(s), r^*(s) \ast (\eta \circ v)).
\]

Proof. By the preceding lemma, note that the assumptions guarantee \(u^*(\text{class}(s)) = \text{class}(u^*(s))\), and that \(P(\eta)\) is defined and central. So for \(g \in \text{class}(P(\eta)u^*(s))\) let \(y_0 \in \text{class}(s)\) be such that \(g = P(\eta)u^*(y_0)\). By Lemma 8.2 the image of \((s, \eta)\) is supported at \(P(\eta)u^*(s)\). We need only verify that the character of the image is equivalent to the one induced from \(r^*(s) \ast (\eta \circ v)\).

First we must justify that \(\eta \circ v\) is a well-defined character of
\[
C_G(P(\eta)u^*(s)) = C_G(u^*(s)).
\]
So suppose that \(u^*(s) = xu^*(s)x^{-1}\) for some \(x \in G\). Applying \(v\) to both sides, we have \(vu^*(x) = v(x)vu^*(s)v(x)^{-1}\). By the assumption that \(v \circ u^*\) is normal, we may write \(vu^*(s) = sc\) for some \(c \in C_H(\text{Im}(v))\). Thus we have \(sc = vu^*(s) = v(x)sv(x)^{-1}c\), or equivalently that \(v(x) \in C_H(s)\). Thus \(v\) maps \(C_G(P(\eta)u^*(s))\) to \(C_H(s)\) and \(\eta \circ v\) is well-defined, as desired.

Now let \(\xi\) be the character of the image, and let \(\beta\) be the character of \((P(\eta) u^*(s), r^*(s) \ast (\eta \circ v))\). By Lemma 8.1
\[
\beta(e_g \# h) = \omega(h, s) \eta(v(t)) = r^*(s)(h) \eta(v(t))
\]
whenever \(g \in \text{class}(P(\eta)u^*(s))\) and \(h = ts\) for some \(t \in C_G(P(\eta)u^*(s)) = C_G(u^*(s))\), and is zero otherwise. On the other hand, by equation 8.6 we have
\[
\xi(e_g \# h) = \omega(h, s) \eta(\gamma) = r^*(s)(h) \eta(\gamma)
\]
whenever \(g \in \text{class}(P(\eta)u^*(s))\) and \(v(h) = \gamma y_0\) for some \(\gamma \in C_H(s)\), and is zero otherwise. So we need only show that the values \(\eta(v(t))\) and \(\eta(\gamma)\) coincide. Indeed, we will show that \(v(t)\) and \(\gamma\) coincide.

So suppose then that we have \(ts' = h\), or equivalently \(t = h^{s'}^{-1}\).
Then \(v(t) = v(h^{s'}^{-1})\). Since \(A \text{Im}(u^*) = G\) and \(A \leq Z(G)\) we may find \(x \in G\) and \(a \in A\) such that \(g' = au^*(x)\). Thus \(h^{s'}^{-1} = h^{u^*(x)^{-1}}\). Since \(v \circ u^*\) is assumed normal, we then have \(v(t) = v(h)^{x^{-1}}\). Now set \(y_0 = s^x\). Then \(gu^*(y_0)^{-1} = gu^*(s^x)^{-1} = g(u^*(s)^{y_0})^{-1} = P(\eta)\). Since there is a unique \(y \in \text{class}(s)\) satisfying \(gu^*(y)^{-1} = P(\eta)\), we conclude that \(y_0\) is this value and that \(y_0^*\) can be taken equal to \(x\). This proves that \(\eta(v(t)) = \eta(\gamma)\), and so completes the proof. 

The theorem applies, in particular, to any element of \(\text{Aut}(\mathcal{D}(G))\). In the case of an automorphism, the image module is necessarily simple.
Such a morphism need not be an isomorphism, however, as demonstrated by \( \begin{pmatrix} 0 & 0 \\ p & 0 \end{pmatrix} \in \text{End}(\mathcal{D}(A)) \), where \( A \) is an abelian group and \( p \) is an isomorphism \( \hat{A} \cong A \).

We note, as an example, that the autoequivalences obtained from the subgroup \( \text{Aut}(G) \rtimes \text{Hom}(G, \hat{G}) \) of \( \text{Aut}(\mathcal{D}(G)) \) include the autoequivalences obtained by lifting the tensor autoequivalences of \( \text{Vec}_G \) through the center construction, as detailed in [21, Example 6.11]. Indeed, the action in the Theorem is, after a few obvious definitions for notation, the matrix action
\[
\begin{pmatrix} v^* & r^* \\ p^* & u^* \end{pmatrix} (\eta, s) = (v^* \eta + r^* s, p^* \eta + u^* s),
\]
where \((\eta, s)\) is the irreducible module \((s, \eta)\) with labels reversed. This is precisely the naively expected action of the flip on the module category.

References

[1] J. E. Adney and Ti Yen. Automorphisms of a \( p \)-group. Illinois J. Math., 9:137–143, 1965. ISSN 0019-2082. URL http://projecteuclid.org/euclid.ijm/1256067587

[2] A. L. Agore, C. G. Bontea, and G. Militaru. Classifying bicrossed products of Hopf algebras. Algebr. Represent. Theory, 17(1):227–264, 2014. ISSN 1386-923X. doi:10.1007/s10468-012-9396-5. URL http://dx.doi.org/10.1007/s10468-012-9396-5

[3] J. Alev and M. Chamarie. Dérivations et automorphismes de quelques algèbres quantiques. Comm. Algebra, 20(6):1787–1802, 1992. ISSN 0092-7872. doi:10.1080/00927879208824431. URL http://dx.doi.org/10.1080/00927879208824431

[4] J. Alev and F. Dumas. Rigidité des plongements des quotients primitifs minimaux de \( U_q(sl(2)) \) dans l’algèbre quantique de Weyl-Hayashi. Nagoya Math. J., 143:119–146, 1996. ISSN 0027-7630. URL http://projecteuclid.org/euclid.nmj/1118771972

[5] Nicolás Andruskiewitsch and François Dumas. On the automorphisms of \( U_q^+(\mathfrak{g}) \). In Quantum groups, volume 12 of IRMA Lect. Math. Theor. Phys., pages 107–133. Eur. Math. Soc., Zürich, 2008. doi:10.4171/047-1/4. URL http://dx.doi.org/10.4171/047-1/4

[6] J. N. S. Bidwell. Automorphisms of direct products of finite groups. II. Arch. Math. (Basel), 91(2):111–121, 2008. ISSN 0003-889X. doi:10.1007/s00013-008-2653-5. URL http://dx.doi.org/10.1007/s00013-008-2653-5
[7] J. N. S. Bidwell, M. J. Curran, and D. J. McCaughan. Automorphisms of direct products of finite groups. *Arch. Math. (Basel)*, 86(6):481–489, 2006. ISSN 0003-889X. doi:10.1007/s00013-005-1547-z URL http://dx.doi.org/10.1007/s00013-005-1547-z

[8] R. Courter. Computing Higher Indicators for the Double of a Symmetric Group. PhD thesis, University of Southern California, 2012. arXiv:1206.6908

[9] R. Dijkgraaf, V. Pasquier, and P. Roche. Quasi Hopf algebras, group cohomology and orbifold models. *Nuclear Phys. B Proc. Suppl.*, 18B:60–72 (1991), 1990. ISSN 0920-5632. doi:10.1016/0920-5632(91)90123-V URL http://dx.doi.org/10.1016/0920-5632(91)90123-V Recent advances in field theory (Annecy-le-Vieux, 1990).

[10] GAP. GAP – Groups, Algorithms, and Programming, Version 4.6.5. The GAP Group, 2013. www.gap-system.org

[11] Christopher Goff, Geoffrey Mason, and Siu-Hung Ng. On the gauge equivalence of twisted quantum doubles of elementary abelian and extra-special 2-groups. *J. Algebra*, 312(2):849–875, 2007. ISSN 0021-8693. doi:10.1016/j.jalgebra.2006.10.022 URL http://dx.doi.org/10.1016/j.jalgebra.2006.10.022

[12] Robert Guralnick and Susan Montgomery. Frobenius-Schur indicators for subgroups and the Drinfel’d double of Weyl groups. *Trans. Amer. Math. Soc.*, 361(7):3611–3632, 2009. ISSN 0002-9947. doi:10.1090/S0002-9947-09-04659-5 URL http://dx.doi.org/10.1090/S0002-9947-09-04659-5

[13] P. Hall. The classification of prime-power groups. *J. Reine Angew. Math.*, 182:130–141, 1940. ISSN 0075-4102.

[14] M. Iovanov, G. Mason, and S. Montgomery. FSZ-groups and Frobenius-Schur Indicators of Quantum Doubles. arxiv.math/1208.4153, 2012.

[15] Noboru Itô. Remarks on factorizable groups. *Acta Sci. Math. Szeged*, 14:83–84, 1951. ISSN 0001-6969.

[16] Yevgenia Kashina, Yorck Sommerhäuser, and Yongchang Zhu. On higher Frobenius-Schur indicators. *Mem. Amer. Math. Soc.*, 181 (855):viii+65, 2006. ISSN 0065-9266. doi:10.1090/memo/0855 URL http://dx.doi.org/10.1090/memo/0855

[17] Marc Keilberg. Higher indicators for some groups and their doubles. *J. Algebra Appl.*, 11(2):1250030, 38, 2012. ISSN 0219-4988. doi:10.1142/S0219498811005543 URL http://dx.doi.org/10.1142/S0219498811005543
Marc Keilberg. Higher Indicators for the Doubles of Some Totally Orthogonal Groups. *Comm. Algebra*, 42(7):2969–2998, 2014. ISSN 0092-7872. doi:10.1080/00927872.2013.775651. URL http://dx.doi.org/10.1080/00927872.2013.775651.

V. Linchenko and S. Montgomery. A Frobenius-Schur theorem for Hopf algebras. *Algebr. Represent. Theory*, 3(4):347–355, 2000. ISSN 1386-923X. doi:10.1023/A:1009949909889. URL http://dx.doi.org/10.1023/A:1009949909889. Special issue dedicated to Klaus Roggenkamp on the occasion of his 60th birthday.

Susan Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993. ISBN 0-8218-0738-2.

Dmitri Nikshych and Brianna Riepel. Categorical Lagrangian Grassmannians and Brauer–Picard groups of pointed fusion categories. *J. Algebra*, 411:191–214, 2014. ISSN 0021-8693. doi:10.1016/j.jalgebra.2014.04.013. URL http://dx.doi.org/10.1016/j.jalgebra.2014.04.013.

David E. Radford. The group of automorphisms of a semisimple Hopf algebra over a field of characteristic 0 is finite. *Amer. J. Math.*, 112(2):331–357, 1990. ISSN 0002-9327. doi:10.2307/2374718. URL http://dx.doi.org/10.2307/2374718.

Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995. ISBN 0-387-94285-8. doi:10.1007/978-1-4612-4176-8. URL http://dx.doi.org/10.1007/978-1-4612-4176-8.

Daniel S. Sage and Maria D. Vega. Twisted Frobenius-Schur indicators for Hopf algebras. *J. Algebra*, 354:136–147, 2012. ISSN 0021-8693. doi:10.1016/j.jalgebra.2011.12.026. URL http://dx.doi.org/10.1016/j.jalgebra.2011.12.026.

K. Shoda. Über die automorphismen einer endlichen abelschen gruppe. *Math. Ann.*, 100(1):674–686, 1928.

Mitsuhiro Takeuchi. Matched pairs of groups and bismash products of Hopf algebras. *Comm. Algebra*, 9(8):841–882, 1981. ISSN 0092-7872. doi:10.1080/00927878108822621. URL http://dx.doi.org/10.1080/00927878108822621.
[27] James Wiegold and Alan G. Williamson. The factorisation of the alternating and symmetric groups. *Math. Z.*, 175(2):171–179, 1980. ISSN 0025-5874. doi:10.1007/BF01674447. URL http://dx.doi.org/10.1007/BF01674447.

Institut de Mathématiques de Bourgogne, Université de Bourgogne,, Faculté des Sciences Mirande, 9 avenue Alain Savary, BP 47870 21078, Dijon Cedex, France

E-mail address: keilberg@usc.edu