The Automorphism Group of the Wreath Product of Finite Groups

Kenneth G. Hummel

Western Michigan University

Follow this and additional works at: https://scholarworks.wmich.edu/dissertations

Part of the Mathematics Commons

Recommended Citation

https://scholarworks.wmich.edu/dissertations/2917

This Dissertation-Open Access is brought to you for free and open access by the Graduate College at ScholarWorks at WMU. It has been accepted for inclusion in Dissertations by an authorized administrator of ScholarWorks at WMU. For more information, please contact maira.bundza@wmich.edu.
THE AUTOMORPHISM GROUP OF THE WREATH PRODUCT
OF FINITE GROUPS

by

Kenneth G. Hummel

A Dissertation
Submitted to the
Faculty of The Graduate College
in partial fulfillment
of the
Degree of Doctor of Philosophy

Western Michigan University
Kalamazoo, Michigan
August 1974
ACKNOWLEDGEMENTS

Since it is impossible to list everyone who has helped, one way or another, along the road to completion of this dissertation, I choose to mention here, since the choice is mine, only the following people.

I thank Joe Buckley, under whose able guidance and direction this thesis was developed; my wife Darla and my children, Lacinda and Melinda, who bore graciously both the good moods and bad which I alternately thrust upon them during the period of my work at Western Michigan University; and lastly, the mathematics faculty and department for their support, intellectual, moral, and financial.

Kenneth G. Hummel
INFORMATION TO USERS

This material was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again -- beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

5. PLEASE NOTE: Some pages may have indistinct print. Filmed as received.

Xerox University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
HUMMEL, Kenneth G., 1943-
THE AUTOMORPHISM GROUP OF THE WREATH PRODUCT
OF FINITE GROUPS.

Western Michigan University, Ph.D., 1974
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td></td>
</tr>
<tr>
<td>PRELIMINARIES</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Definitions and Notation</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td></td>
</tr>
<tr>
<td>THE AUTOMORPHISM GROUP OF THE WREATH PRODUCT</td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Aut(A Wr B) as a Split Extension</td>
<td>7</td>
</tr>
<tr>
<td>The Subgroup H of Aut(A Wr B)</td>
<td>16</td>
</tr>
<tr>
<td>III</td>
<td></td>
</tr>
<tr>
<td>THE AUTOMORPHISM GROUP OF THE WREATH PRODUCT OF TWO P-GROUPS</td>
<td>41</td>
</tr>
<tr>
<td>Introduction</td>
<td>41</td>
</tr>
<tr>
<td>The Subgroup H</td>
<td>42</td>
</tr>
<tr>
<td>Some Results on the Structure of Aut(A wr B)</td>
<td>53</td>
</tr>
<tr>
<td>IV</td>
<td></td>
</tr>
<tr>
<td>THE CONJECTURE</td>
<td>58</td>
</tr>
<tr>
<td>&quot;</td>
<td>58</td>
</tr>
<tr>
<td>Introduction</td>
<td>58</td>
</tr>
<tr>
<td>G as a Central Product</td>
<td>58</td>
</tr>
<tr>
<td>G as a Wreath Product</td>
<td>64</td>
</tr>
</tbody>
</table>

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
An important concept in group theory is that of the automorphism group of a group. It has been shown that the automorphism group of the standard wreath product $W$ of a group $A$ by a group $B$ is, except in a few cases, a splitting extension of $A^*H_1$ by $B^*$, where $A^*$ and $B^*$ are isomorphic to the automorphism groups of $A$ and $B$ respectively, $I_1$ is a particular subgroup of the group of inner automorphisms of $W$, and $H$, although somewhat described, is really the "unknown ingredient" of $\text{Aut } W$. In this thesis the subgroup $H$ of $\text{Aut } W$ is described when the group $A$ is purely non-abelian, abelian, or cyclic, and when both $A$ and $B$ are $p$-groups. Some of these descriptions yield formulas for the order of $H$, $o(H)$, (hence for $o(\text{Aut } W)$) and methods whereby all the automorphisms of $W$ may be constructed. Furthermore, when both $A$ and $B$ are $p$-groups, a Sylow $p$-subgroup of $\text{Aut } W$ is described as a splitting extension. A similar result is obtained for $\text{Out } W$.

The conjecture that $o(G)$ divides $o(\text{Aut } G)$ when $G$ is a non-cyclic $p$-group of order greater than $p^2$ is investigated when $G$ is a central product and also when
G is a wreath product. Both investigations yield new classes of groups for which the conjecture is true. Furthermore, the central product work shows that the general conjecture will be established if it can be proven for a smaller class of groups.
CHAPTER I

PRELIMINARIES

Introduction

Most branches of mathematics introduce new and important concepts into their fields of study when they define "products of" and "operations on" particular objects in their realm. In analysis, for example, products of functions, spaces, and measures are important concepts as well as operations such as differentiation, integration, and summation. In graph theory there is the cartesian product of graphs and operations such as complement and converse. This thesis is concerned primarily with the standard wreath product of groups (which is again a group) and the operation "Aut" which assigns to each group $G$ another group, denoted by $\text{Aut} \, G$, consisting of all the automorphisms of $G$.

Chapters II and III investigate the automorphism group of the standard wreath product, the combination of these two important group theoretic ideas. A description of this automorphism group has been given by Houghton [9], but his description contains a subgroup $H$ about which little was known. Let $W$ be the standard wreath product of a group $A$ by a group $B$. Chapter II contains a more detailed description of the subgroup $H$ of $\text{Aut} \, W$ when

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
A is purely non-abelian, abelian, or cyclic. Chapter III is an investigation of Aut W when both A and B are finite p-groups. In this case a formula for the order of H, o(H), and hence for o(Aut W) is determined. Furthermore, the proof is constructive and yields a method whereby all the automorphisms in H and hence in Aut W may be realized from certain homomorphisms.

Chapter IV investigates the conjecture that o(G) divides o(Aut G) when G is a non-cyclic p-group of order greater than p^2. The conjecture is shown to be true whenever G is the central product of non-trivial proper subgroups A and K, where A is abelian and o(K) divides o(Aut K). This result extends the classes of groups for which the conjecture is known to be true and also shows that if the conjecture can be proven for a particular class of p-groups, then it is true for all p-groups under consideration. Also in this chapter, results from Chapters II and III are used to yield theorems giving conditions on the p-groups A and B under which the conjecture is true for W = A wr B. Examples of these conditions are: o(A) divides o(Aut A) and o(B) ≥ o(Z(A)), where Z(A) is the center of A. Furthermore, it is shown that the conjecture is true for the standard wreath product of any two non-trivial p-groups A and B if a weaker statement is true for all non-abelian indecomposable p-groups G.
Definitions and Notation

If $A$ and $B$ are non-trivial groups, the wreath product of $A$ by $B$ is defined as follows. Let $F_1$ be the group of functions from $B$ into $A$ with multiplication of $f, g \in F_1$ defined by $fg(x) = f(x)g(x)$ for all $x \in B$. $F_1$ is the unrestricted direct product of isomorphic copies of $A$, there being one copy of $A$ for each element $b$ in $B$. The subgroup $F_2$ of $F_1$ consisting of all functions with finite support is the corresponding restricted direct product. A function from $B$ into $A$ is said to have finite support if its value is trivial at all but a finite number of elements of $B$. Both of these groups will be denoted by $F$ and the distinction made when necessary. If $f \in F$ and $b \in B$, then $f^b \in F$ is defined by $f^b(x) = f(xb^{-1})$ for all $x \in B$. The group of automorphisms of $F$ defined by $f \rightarrow f^b$ for all $f \in F$ is isomorphic to $B$ and will be identified with $B$. The wreath product of $A$ by $B$ is defined as the splitting extension of $F$ by $B$; i.e., it is generated by $B$ and $F$ with the relations $b^{-1}fb = f^b$ for all $b \in B$ and $f \in F$. If $F$ is unrestricted the wreath product of $A$ by $B$ will be denoted $W = A \text{Wr} B$. The notation $A \text{wr} B$ will be used when $F$ is restricted. $F$ will be referred to as the base group of $W$. The subgroup of $F$ consisting of all constant functions will be
called the diagonal subgroup and denoted by D.

For any group $G$, $Z(G)$ will denote the center of $G$. In the case $W = A \wr B$, $P$ will denote that subgroup of $F$ defined by $P = \{ f \in Z(F) : \prod_{x \in B} f(x) = 1 \}$, where 1 is the identity element of $A$. It is noted that $P$ is the direct product of $o(B) - 1$ isomorphic copies of $Z(A)$.

A group $G$ will be called indecomposable if it cannot be expressed as a direct product of two non-trivial subgroups. For any group $G$, $\text{Aut}_G$ will denote the group of automorphisms of $G$ and $\text{Aut}_c(G)$ will be used to denote that subgroup of $\text{Aut}_G$ consisting of all the central automorphisms of $G$. A central automorphism of $G$ is an automorphism $f$ of $G$ that has the property; $g^{-1}f(g) \in Z(G)$ for all $g \in G$. Let $G$ be a group and $g \in G$. $i_g$ will denote the inner automorphism of $G$ defined by $i_g(h) = g^{-1}hg$ for all $h \in G$ and $\text{Inn}_G$ will denote that subgroup of $\text{Aut}_G$ consisting of all the inner automorphisms of $G$. $\text{Out}_G$ will denote the group of outer automorphisms of $G$. If $H$ is a subgroup of $G$ (denoted by $H \leq G$), then $\text{Aut}_H$ consists of those automorphisms of $G$ which leave $H$ invariant. If $H \leq G$, then $H$ is characteristic in $G$ ($H \text{ char } G$) if and only if $\text{Aut}_H = \text{Aut}_G$. For any two groups $G$ and $K$, $\text{Hom}(G,K)$ is the set of all homomorphisms from $G$ into $K$. If $K \leq G$ and $f$ is any map defined on $G$, then $f|_K$ is the restriction.
of \( f \) to \( K \). A group \( G \) is said to be **purely non-abelian** if it has no non-trivial abelian direct factors.

The fact that two groups \( G \) and \( K \) are isomorphic will be denoted by \( G \cong K \). The Frattini subgroup of a group \( G \) is the intersection of all maximal subgroups of \( G \). The notation \( \Phi(G) \) will be used for this group and the usual convention that \( \Phi(G) = G \) if \( G \) has no maximal subgroup is adopted.

Other definitions and notations will appear in the text of this thesis when they are needed.
CHAPTER II

THE AUTOMORPHISM GROUP OF THE WREATH PRODUCT

Introduction

The wreath product of two groups is playing an increasingly significant role in group theory. Like other "products" of groups (e.g., direct, central, and semi-direct) it is a method whereby a third group may be constructed from two other groups. The third group or child may, as is the situation in real life, have either great or little "resemblance" to its parents. In the case of the so-called "standard wreath product" of groups, the child does "inherit" many important characteristics from its parents. These traits have been exploited at various times by Neumann [12], Houghton [9], Neumann and Neumann [11], and others to ascertain important new information about the standard wreath product and its corresponding automorphism group. Some of these results have been collected at the beginning of this chapter so that this thesis might be a more complete entity in and of itself. In some cases the theorems are restated and proofs which are more in the flavor of the rest of the thesis are given.

It is in this chapter that some new descriptions of the subgroup $H$ of $\text{Aut}(A \wr B)$ are obtained. The most
striking new result is contained in Theorem 2.13. Working from the hypotheses that $A$ is a purely non-abelian finite group and that $B$ is a finite group, a one-to-one map of $H$ onto a set $R$ is obtained. Furthermore, the proof is constructive and thereby yields a method by which all the automorphisms of $W$ in $H$ may be constructed from elements of $R$. A formula for $o(H)$, obtained from a formula for the cardinality of $R$, is given as a corollary.

$\text{Aut}(A \text{ Wr } B)$ as a Split Extension

The initial theorem stated in this section is due to Neumann [12, p. 368]. The result is significant in its own right, essential to later work in this chapter, and rather startling. The proof is fairly long and complex. It is omitted since the result and not the technique of proof is the important factor in this thesis.

**Definition.** If $A$ is a dihedral group whose normal abelian subgroup $K$ of index two contains unique square roots of all its elements, then $A$ is a special dihedral group.

**Theorem 2.1.** The base group in a (restricted or unrestricted) standard wreath product of a group $A$ by a group $B$ is a characteristic subgroup except when $B$ has order two and $A$ is a special dihedral group. In this case the base group $F$ admits a subgroup of index two in
the automorphism group of the wreath product. In other words, \( \text{Aut}_F W = \{ \alpha \in \text{Aut} W : \alpha(F) = F \} \) is a subgroup of index two in \( \text{Aut} W \).

The next two lemmas are also basic background for later results and were first given by Peter Neumann's parents, B.H. Neumann and Hanna Neumann [11, Pp. 474-6]. The proofs are routine in nature and are omitted.

**Lemma 2.2.** If \( \alpha \in \text{Aut} A \), then \( \alpha^* \) defined by
\[
(bf)^{\alpha^*} = bf^{\alpha^*}
\]
for all \( b \in B \) and \( f \in F \), where
\[
(f^{\alpha^*}(x))^{\alpha} = (f(x))^{\alpha}
\]
for all \( x \in B \) is an automorphism of \( W = A \wr B \). Furthermore, the group \( A^* \) of all such automorphisms is isomorphic to \( \text{Aut} A \).

A similar result for the automorphisms of \( B \) is given by

**Lemma 2.3.** If \( \beta \in \text{Aut} B \), then \( \beta^* \) defined by
\[
(bf)^{\beta^*} = b^{\beta}f^\beta^{\ast}
\]
for all \( b \in B \) and \( f \in F \), where
\[
f^{\beta^\ast}(x) = f(x^{\beta^{-1}})
\]
for all \( x \in B \) is an automorphism of \( W = A \wr B \). Furthermore, the group \( B^* \) of all such automorphisms is isomorphic to \( \text{Aut} B \).

It is also noted at this point that the groups \( A^* \) and \( B^* \) commute elementwise.

The next theorem is due to Houghton [9, p. 309], but is restated somewhat to better fit its role in this thesis.
Before stating this theorem it is convenient to introduce some notation and definitions which will be used repeatedly throughout this chapter and the next. Let $W = A \wr B$. $I_1$ will denote the subgroup of $\text{Aut} W$ consisting of those inner automorphisms corresponding to conjugation by elements of the base group $F$. $K$ will be used to denote the subgroup of $\text{Aut}_F W$ consisting of those automorphisms which leave $B$ elementwise fixed. The subgroups $A^*$ and $B^*$ of $\text{Aut} W$ are as defined in Lemmas 2.2 and 2.3 respectively. Finally, $H$ is the subgroup of $K$ consisting of those automorphisms which leave the diagonal elementwise fixed.

**Theorem 2.4.** Let $W = A \wr B$. Then except when $B$ is of order two and $A$ is a special dihedral group

(a) $\text{Aut} W$ is a splitting extension of $K I_1$ by $B^*$,

(b) $K$ is a splitting extension of $H$ by $A^*$,

and (c) the subgroups $A^* H I_1$, $H I_1 B^*$, $H I_1$ and $I_1$ are all normal in $\text{Aut} W$.

In the exceptional case (a) through (c) hold with $\text{Aut} W$ replaced by $\text{Aut}_F W$ a subgroup of index two.

**Proof:** By the result of Neumann which is stated as Theorem 2.1 in this thesis, $\text{Aut}_F W = \text{Aut} W$ except when $B$ is of order two and $A$ is a special dihedral group. Hence both cases of the theorem can be proven simultaneously by showing that (a) through (c) hold with
Aut \( W \) replaced by \( \text{Aut}_F W \) for any choice of the groups \( A \) and \( B \).

(a) \( \text{Aut}_F W \) is a splitting extension of \( KI_1 \) by \( B^* \).

It is first noted that an element \( w \in W \) can be expressed uniquely in the form \( w = xg \) where \( x \in B \) and \( g \in F \), that \( F \) is a normal subgroup of \( W \) and \( \frac{W}{F} \cong B \). If \( \alpha \in \text{Aut}_F W \), then \( \alpha \) induces an automorphism \( u(\alpha) \) of \( \frac{W}{F} \) defined by \( u(\alpha)(wF) = \alpha(w)F \) for all \( wF \in \frac{W}{F} \). If \( \rho \in \text{Aut} \frac{W}{F} \) then for each \( b \in B \) there exists a unique \( x \in B \) such that \( \rho(bF) = xF \). Hence the map \( r(\rho) : B \to B \) defined by \( r(\rho)(b) = x \) for all \( b \in B \) where \( \rho(bF) = xF \) is an automorphism of \( B \). Consider the map \( t = r \circ u \) taking \( \text{Aut}_F W \) into \( \text{Aut} B \). Note that if \( \alpha \in \text{Aut}_F W \), then \( t(\alpha)(b) = x \) for all \( b \in B \) where \( \alpha(b) = xg \) in canonical form. If \( s : \text{Aut} B \to \text{Aut}_F W \) is the homomorphism defined in Lemma 2.3, then \( t \circ s(\beta) = t(\beta^*) = \beta \) and \( \text{Aut}_F W \) is a splitting extension of \( \ker t \) by \( \text{Aut} B \cong B^* \).

The proof of (a) will be complete if \( \ker t = KI_1 \).

First observe that \( \alpha \in \text{Aut}_F W \) is in \( \ker t \) if and only if \( \alpha(b) = b \) (mod \( F \)) for all \( b \in B \). Since \( K \leq \text{Aut}_F W \) and elements of \( K \) leave \( B \) fixed elementwise, it is clear that \( KI_1 \leq \ker t \). To show the other inclusion let \( \alpha \in \ker t \). For each \( b \in B \) there exists an element \( g_b \) in \( F \) such that \( \alpha(b) = bg_b \). Define \( g \in F \) by \( g(b) = [g_b(b)]^{-1} \) for all \( b \in B \). Note that for all \( x,y \in B \), \( \alpha(xy) = xyg_{xy} \) and \( \alpha(xy) = xyg_{xy} = xyg_{xy}^y \).
Hence $g_{xy} = g_y^x$ for all $x, y \in B$. A special case is $g_{x}^{-1} = g^{-1}_x$ for all $x \in B$. It follows that

$$[(g^{-1})_b^bg]_g(x) = [g(xb^{-1})]^{-1}_g [g_b(x)]^{-1}_g(x)$$

$$= g^{-1}_x(xb^{-1})_b g_b(x) [g_x(x)]^{-1}_g(x)$$

$$= g_b^{-1}_x(x) g_b g [g_x(x)]^{-1}_g(x)$$

$$= g_b(x) g_b^{-1}_x(x) g_b g [g_x(x)]^{-1}_g(x)$$

$$= g_b(x) [g_b(x)]^{-1}_g(x) g_b [g_x(x)]^{-1}_g(x) = 1$$

for all $x \in B$. Hence $(i_\alpha \circ \alpha)(b) = i_\alpha(gbg) = g^{-1}_b g = b$ for all $b \in B$, where $i_\alpha$ is the inner automorphism of $W$ corresponding to conjugation by $g$.

Therefore $i_\alpha \circ \alpha$ is in $K$ and $\alpha \in I_1K$. A routine argument shows that $I_1$ is normal in $\text{Aut}_F W$. Hence $I_1K = KI_1$ and $\ker \tau \subseteq KI_1$ which completes the proof of (a).

(b) $K$ is a splitting extension of $H$ by $A^*$. Let $d \in D$ and $\rho \in K$, then $\rho(d) = \rho(d^b) = \rho(b^{-1}db) = b^{-1}_b \rho(d)b = \rho(d)^b_b$ for all $b \in B$. But $g \in F$ satisfies $g^b = g$ for all $b \in B$ if and only if $g \in D$. Hence for all $\rho \in K$, $\rho(D) = D$. Consider the map $v:K \to \text{Aut A}$ defined by $v(\rho) = \rho|D$ for $\rho \in K$. This can be considered as a map into $\text{Aut A}$ since $D \cong A$ and hence $\text{Aut D} \cong \text{Aut A}$. If $s:\text{Aut A} \to K$ is the homomorphism defined in Lemma 2.2 it is a simple matter to observe that $v \circ s$ is the identity on $\text{Aut A}$. Hence $K$ is a
splitting extension of \( \ker v \) by \( \Aut A = A^* \). But \( p \in \ker v \) if and only if \( p|D \) is the identity on \( D \). Hence \( \ker v = H \), those automorphisms of \( W \) in \( K \) which leave the diagonal elementwise fixed.

(c) \( A^*H_1, H_1B^*, H_1 \) and \( I_1 \) are normal in \( \Aut_F W \). These normalities are routine computations and are left to the reader. #

The next theorem is also a result of Houghton and begins to give some insight into the nature of the subgroup \( H \). Although the theorem is actually a statement about \( K \) it is recalled that \( H \leq K \).

**Theorem 2.5.** The group \( K \) is isomorphic to the group of those automorphisms of the base group which commute with the inner automorphisms of \( W \) induced by elements of \( B \).

**Proof:** Let \( p \in K, b \in B, \) and \( f \in F \). It is clear that \( p(f^b) = p(b^{-1}fb) = b^{-1}p(f)b = p(f)^b \) and hence \( p \) commutes with \( i_b \) for all \( p \in K, b \in B \). Conversely, if \( \alpha \in \Aut F \) commutes with \( i_b \) for all \( b \in B \), then \( \alpha \) can be extended to an automorphism \( \gamma \) of \( W \) which fixes \( B \) elementwise. Define \( \gamma : W \to W \) by \( \gamma(bf) = b\alpha(f) \) for all \( b \in B \) and \( f \in F \). #

The previous work has been presented to serve the reader as basic background information. The rest of this
chapter will be devoted mainly to new results. Before proceeding with the new results it is convenient to make the identification suggested by Theorem 2.5, i.e., the subgroup \( H \) of \( \text{Aut} \ W \) will be identified with the subgroup of \( \text{Aut} \ F \) consisting of those automorphisms of \( F \) which commute with the inner automorphisms of \( W \) induced by elements of \( B \) and which also fix the diagonal element-wise. This identification will be seen to be notationally useful in some of the following work.

The next lemma will be quite useful in obtaining a description of the subgroup \( H \) when \( A \) is purely non-abelian. It is also of some interest in its own right as it shows that the subgroup \( H \) always contains a subgroup \( J(B) \) which is isomorphic to \( B \).

**Lemma 2.6.** If \( b \in B \), then \( j_b: F \to F \), defined by 
\[
j_b(f) = f^{(b)} \quad \text{for all } f \in F, \quad \text{where } f^{(b)}(x) = f(b^{-1}x)
\]
for all \( x \in B \), is in \( H \). Furthermore, \( J(B) = \{ j_b : b \in B \} \) is isomorphic to \( B \).

**Proof:** If \( f \) and \( g \) are in \( F \) and \( b \in B \), then 
\[
(fg)^{(b)}(x) = fg(b^{-1}x) = f(b^{-1}x)g(b^{-1}x) = f^{(b)}(x)g^{(b)}(x)
\]
for all \( x \in B \). Hence \( j_b \in \text{Hom}(F,F) \) for all \( b \in B \).

To show that \( j_b \) is one-to-one suppose that \( j_b(f) = j_b(g) \) for some \( f \) and \( g \) in \( F \). It follows that 
\[
f^{(b)}(x) = g^{(b)}(x) \quad \text{for all } x \in B \quad \text{and hence } \quad f(b^{-1}x) = g(b^{-1}x)
\]
for all \( x \in B \). Therefore \( f = g \) and \( j_b \) is one-to-one.
for all $b$ in $B$. Finally to show that $j_b$ is an isomorphism of $F$ it remains to show that $j_b$ is onto. But if $f$ is in $F$, then $f(b^{-1})$ is in $F$ and $j_b(f(b^{-1})) = [f(b^{-1})]_b = f$. To finish the proof that $J(B) \leq H$ it is necessary to show

(i) $j_b \circ i_x = i_x \circ j_b$ for all $b, x \in B$

and (ii) $j_b|_D$ is the identity on $D$ for all $b \in B$, where $i_x$ is the inner automorphism of $W$ corresponding to conjugation by $x \in B$.

Proof of (i): If $f \in F$ and $b, x \in B$, then $j_b \circ i_x(f) = (f^x)(b)$. But for all $y \in B$, $(f^x)(b)(y) = (f^x)(b^{-1}y) = f(b^{-1}yx^{-1}) = f(b)(yx^{-1}) = (f(b))^x(y)$. Hence $j_b \circ i_x(f) = (f^x)(b) = (f(b))^x = i_x \circ j_b(f)$ and (i) is established.

Proof of (ii): If $d \in D$ and $b \in B$, then $j_b(d) = d^b$. But $d^b(y) = d(b^{-1}y) = d(y)$ for all $y \in B$. Hence $j_b(d) = d^b = d$. It is left to show that $J(B) = B$. If $f \in F$ and $x, y \in B$, then $f(xy)(b) = f((xy)^{-1}b) = f(y^{-1}x^{-1}b) = f(y)(x^{-1}b) = [f(y)]_x(b)$ for all $b \in B$. Hence $j_{xy}(f) = f(xy) = [f(y)]_x(b) = j_x(f)(y) = j_x \circ j_y(f)$ for all $f \in F$ and $x, y \in B$. In other words $j_{xy} = j_x \circ j_y$

for all $x, y \in B$ and $t : B \to J(B)$ defined by $t(b) = j_b$ for all $b \in B$ is a homomorphism. It is immediate from the definition of $t$ that it is onto. Next let $x, y \in B$ and suppose that $j_x = j_y$. It follows that $j_x(f) = j_y(f)$ for all $f \in F$ and hence that $f(x)(b) = f(y)(b)$ for all
f in F and b in B. In other words \( f(x^{-1}b) = f(y^{-1}b) \) for all \( f \in F, b \in B \). In particular \( f(e) = f(y^{-1}x) \) for all \( f \in F \). Since A is non-trivial this is only possible if \( y^{-1}x = e \). Hence \( j_x = j_y \) implies that \( x = y \) and \( t \) is one-to-one. #

Throughout the rest of this chapter A and B will denote finite non-trivial groups. Hence the wreath product of A by B is written \( W = A \operatorname{wr} B \).

The following theorem emphasizes the importance of being able to obtain a formula for the order of H.

**Theorem 2.7.** Let A and B be finite non-trivial groups and \( W = A \operatorname{wr} B \). If

\[
X = |W| \cdot |H| \cdot |\operatorname{Aut} A| \cdot |\operatorname{Aut} B| / |A| \cdot |B|
\]

then the order of \( \operatorname{Aut} W \) is given by

\[
|\operatorname{Aut} W| = \begin{cases} X, & \text{if } F \text{ char } G \\ 2X, & \text{otherwise.} \end{cases}
\]

**Proof:** It is sufficient to show that the order of \( KI_1B^* \) is \( X \). Since \( KI_1B^* \) is a splitting extension of \( KI_1 \) by \( B^* \cong \operatorname{Aut} B \) it follows that \( |KI_1B^*| = |KI_1| \cdot |B^*| = |KI_1| \cdot |\operatorname{Aut} B| \) and attention is shifted to the group \( KI_1 \). If \( f \in F \), then \( i_f \) is in \( K \cap I_1 \) if and only if \( i_f(b) = b \) for all \( b \in B \). Now \( i_f(b) = f^{-1}bf = b \) for all \( b \in B \) if and only if \( f = f^b \) for all \( b \in B \). But \( f = f^b \) for all \( b \in B \) if and only if \( f \in D \). Hence it follows that \( K \cap I_1 = [i_f : f \in D] \cong D/Z(D) \cong A/Z(A) \).
Therefore \[ |KI_1| = |K| \cdot |I_1| / |K \cap I_1| = |K| \cdot |I_1| = |Z(A)| / |A|. \]

If \( f, g \in F \), then \( i_f = i_g \) if and only if \( g^{-1}f \in Z(W) = Z(D) \cong Z(A). \) Hence \[ |I_1| = |F| / |Z(A)| = |A|^{|B|} / |Z(A)|. \]

Next it is noted that \( |K| = |H| \cdot |A^*| = |H| \cdot |\text{Aut } A| \), since \( K \) is a splitting extension of \( H \) by \( A^* = \text{Aut } A. \) Combining the above results it is seen that \[ |KI_1B^*| = |KI_1| \cdot |\text{Aut } B| = |K| \cdot |I_1| \cdot |Z(A)| \cdot |\text{Aut } B| / |A| = |H| \cdot |\text{Aut } A| \cdot |A|^{|B|} \cdot |\text{Aut } B| / |A| = |W| \cdot |H| \cdot |\text{Aut } A| \cdot |\text{Aut } B| / |A| \cdot |B| = X. \]

The Subgroup \( H \) of \( \text{Aut } W \)

Since \( H \) has already been identified with a subgroup of the automorphism group of \( F \), and since \( F \) can be viewed as the direct product of \( o(B) \) isomorphic copies of the group \( A \), it is both natural and notationally useful to make the following further identification. Let \( f \in F \), \( B = \{b_1, \ldots, b_n\} \) and suppose \( f(b_i) = a_i \) where \( a_i \in A \) for all \( i = 1, 2, \ldots, n \). Identify \( f \) with \( \prod_{i=1}^{n} (a_i)^{b_i} \). It is noted, for further clarity, that under this identification each element \( a \) in \( A \) has been identified with the function \( f \) in \( F \) which assumes the value \( a \) at the identity element of \( B \) and is trivial elsewhere. Hence the use of \( a^b \) to denote that function in \( F \) which assumes the value \( a \in A \) at \( b \in B \) and is
trivial elsewhere is compatible with the action of \( B \) on \( F \). If \( L \leq A \) and \( b \in B \), then \( L^b \) is the subgroup of \( A^B = F \) consisting of all functions \( f: B \to L \) which are trivial everywhere except, perhaps, at \( b \). Clearly \( L^b \cong L \) for any \( b \in B \).

The following result is an essential ingredient in the proof of a number of later theorems. It is given at this time so that the argument will not have to be repeated each time the result is needed. The proof uses the Remak-Krull-Schmidt Theorem [17, p. 83], one version of which states

**Remak-Krull-Schmidt Theorem.** If a finite group \( G \) has decompositions \( G = A_1 \times \cdots \times A_m = B_1 \times \cdots \times B_n \) where the \( A_i \) and \( B_j \) are indecomposable and non-trivial, then \( m = n \) and there exists a permutation \( \sigma \in S_n \) and a central automorphism \( \psi \) of \( G \) such that \( \psi(A_i) = B_{i\sigma} \).

More precisely, the proof uses the following easy

**Corollary.** If a finite group \( G \) has a decomposition \( G = A_1 \times \cdots \times A_n \) and \( \theta \in \text{Aut } G \) then there exists a permutation \( \sigma \in S_n \) such that \( \theta(A_i) = A_{i\sigma} \) and \( \theta(A_i) \leq A_{i\sigma} Z(G) \).

Also, the identifications given above and the properties of an element in \( H \) are used extensively.
Lemma 2.8. Let $A$ and $B$ be non-trivial finite groups. Let $A = (A_{11} \times \cdots \times A_{1m_1}) \times \cdots \times (A_{r1} \times \cdots \times A_{rm_r})$ where $A_{ij}$ is non-trivial indecomposable for all $i$ and $j$ and $A_{ij} \cong A_{k}$ if and only if $i = k$. Let $e$ denote the identity element of $A$ and $P = \{f \in \mathbb{Z}(F): \prod_{x \in B} [f(x)] = e\}$. If $\varphi \in H$, then for each direct factor $A_{ij}$ of $A$ there exists an element $b \in B$ such that $\varphi(A_{ij}) \subseteq A_{ij}^b \cdot P$. Moreover, for each $a \in A_{ij}$ there exists an $f \in P$ such that $\varphi(a) = a^bf$.

Proof: Recalling that $A_{ij}^b = \{a^b : a \in A_{ij}\}$ it is seen that $F = \prod_{x \in B} \prod_{i=1}^{r} \prod_{j=1}^{m_i} A_{ij}^x$. Since $\varphi \in H$ it follows that $\varphi(F) = \prod_{x \in B} \prod_{i=1}^{r} \prod_{j=1}^{m_i} \varphi(A_{ij}^x) = \prod_{x \in B} \prod_{i=1}^{r} \prod_{j=1}^{m_i} \varphi(A_{ij})^x = F$. Fix $i$ and $j$, then it follows from the Corollary to the Remak-Krull-Schmidt Theorem that $\varphi(A_{ij}) \subseteq A_{ik}^b \mathbb{Z}(F)$ for some $k = 1, 2, \ldots, m_i$ and some $b \in B$. Let $a \in A_{ij} \subseteq F$. There exists a $c \in A_{ik} \subseteq F$ and an $f \in \mathbb{Z}(F)$ such that $\varphi(a) = c^bf$. But $\varphi \in H$ and hence $\varphi(a^x) = \varphi(a)^x = c^bx^xf^x$. Furthermore, $\varphi|D$ is the identity on $D$ and so $\prod_{x \in B} [a^x] = \varphi(\prod_{x \in B} [a^x]) = \prod_{x \in B} [\varphi(a)^x] = \prod_{x \in B} [c^bx^x] \cdot \prod_{x \in B} [f^x]$. Evaluating at the identity element $e$ of $B$ it is seen that $a = cz$, where $z = \prod_{x \in B} [f^x(e)] \in \mathbb{Z}(A)$. Hence $c = az^{-1}$ and $\varphi(a) = c^bf = a^b(z^{-1})^bf = a^bg$ where $g = (z^{-1})^bf \in \mathbb{Z}(F)$. A review of what has been shown to this point shows that the proof will be complete if the
function \( g \in Z(F) \) which depends on \( a \in A_i \) and is
given by \( \varphi(a) = a^bg \) can be shown to be more precisely in
\( P \subseteq Z(F) \). Recalling that \( \varphi(a^x) = \varphi(a)^x \) for all \( x \in B \)
and that \( \varphi|_\mathcal{D} \) is the identity on \( \mathcal{D} \) it is seen that
\[
\prod_{x \in \mathcal{B}} [a^x] = \varphi(\prod_{x \in \mathcal{B}} [a^x]) = \prod_{x \in \mathcal{B}} [\varphi(a^x)]
\]
\[
= \prod_{x \in \mathcal{B}} [\varphi(a)^x] = \prod_{x \in \mathcal{B}} [a^{bx_i}]. \prod_{x \in \mathcal{B}} [g^x].
\]
But \( \prod_{x \in \mathcal{B}} [a^x] = \prod_{x \in \mathcal{B}} [a^{bx_i}] \) and hence \( \prod_{x \in \mathcal{B}} [g^x] = 1 \), the iden-
tity of \( F \). If \( e \) is the identity of \( A \) and \( y \in B \), then
\( e = \prod_{x \in \mathcal{B}} [g^x(y)] = \prod_{x \in \mathcal{B}} [g(y^{-1}x)] = \prod_{x \in \mathcal{B}} [g(x)] \). Hence \( g \in P \)
and the proof is complete. #

In trying to describe the subgroup \( H \) of \( \text{Aut} W \) a
typical difficulty is encountered, i.e., to obtain more
and more detailed descriptions of \( H \) it is necessary to
place more and more restrictions on the groups \( A \) and \( B \).
The trick, obviously, is to balance one against the
other. The initial theorems in this chapter placed no re-
strictions on \( A \) and \( B \) and provided some information
about \( H \). More information about \( H \) has been acquired
by assuming the groups \( A \) and \( B \) to be finite. In the
next lemma and theorem it is further assumed that \( A \) is
non-abelian indecomposable. As expected, even more de-
tailed information about \( H \) is obtained.

**Lemma 2.9.** If \( A \) is a non-abelian indecomposable group
and \( B = \{b_1, b_2, \ldots, b_n\} \), then \( \sigma: \text{Hom}(A, P) \to A_c(F) \cap H \)

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
defined by
\[ [\sigma(t)] \left( \prod_{i=1}^{n} (a_i b_i) \right) = \prod_{i=1}^{n} [t(a_i) b_i] \]
for all \( t \in \text{Hom}(A,P) \) and \( \prod_{i=1}^{n} (a_i b_i) \in F \) is a one-to-one map of \( \text{Hom}(A,P) \) onto \( \text{Ac}(F) \cap H \).

**Proof:** If \( t \in \text{Hom}(A,P) \), then \( t^*: F \to P \) defined by
\[ t^* \left( \prod_{i=1}^{n} (a_i b_i) \right) = \prod_{i=1}^{n} [t(a_i) b_i] \]
for all \( \prod_{i=1}^{n} (a_i b_i) \in F \)
is an extension of \( t \) to a homomorphism of \( F \) into
\( P \leq Z(F) \) which commutes with the inner automorphisms of \( W \) corresponding to conjugation by elements of \( B \). Now \( A \) is non-abelian indecomposable and hence \( F \) is purely non-abelian. It follows by a result of Adney and Yen [1, p. 137] that \( \sigma(t): F \to F \) defined by
\[ [\sigma(t)](g) = gt^*(g) \]
for all \( g \in F \) is a central automorphism of \( F \). It is clear that \( \sigma(t) \) commutes with \( i_b \) for all \( b \in B \) and hence to show that \( \sigma(t) \) is in fact in \( H \) it is necessary to show that \( \sigma(t)|D \) is the identity on \( D \). If \( d \in D \) and \( d(b) = a \) for all \( b \in B \), then \( \sigma(t)(d) = d \prod_{i=1}^{n} [t(a_i) b_i] = d \) since \( t(a) \in P \) implies that
\[ \prod_{i=1}^{n} [t(a_i) b_i] \]
is the identity of \( F \). It has been established thus far that \( \sigma \) is, indeed, a map of \( \text{Hom}(A,P) \) into \( \text{Ac}(F) \cap H \). It is next shown that \( \sigma \) is one-to-one. If \( t \) and \( u \) are in \( \text{Hom}(A,P) \) and \( \sigma(t) = \sigma(u) \) then
\[ \sigma(t)(a) = \sigma(u)(a) \]
for all \( a \in A \). But then \( at(a) = au(a) \).
for all \( a \in A \) and \( t = u \). Hence \( \sigma \) is one-to-one. To show that \( \sigma \) is onto let \( \varphi \in A_{C}(F) \cap H \); since 
\( \varphi \in A_{C}(F) \), for each \( a \in A \) there exists a \( g \in Z(F) \)
such that \( \varphi(a) = ag \) and in fact, \( g \in P \) since \( \varphi|D \) is
the identity on \( D \). It follows that \( t:A \to P \) defined by
\[ t(a) = a^{-1} \varphi(a) \] is in \( \text{Hom}(A,P) \). Since an automorphism
of \( F \) in \( H \) is completely determined by its action on
\( A, \sigma(t) = \varphi \) and \( \sigma \) is onto. This completes the proof. 

The subgroup \( J(B) \) of \( H \) described in Lemma 2.6
plays an important role in the description of \( H \) when \( A \)
is non-abelian indecomposable. This is seen in

**Theorem 2.10.** If \( A \) is a non-abelian indecomposable
finite group and \( B \) is a finite group, then \( H \) is a
splitting extension of \( A_{C}(F) \cap H \) by \( J(B) \). Moreover,
if \( B \) is abelian, then \( H = (A_{C}(F) \cap H) \times J(B) \).

**Proof:** If \( \varphi \in H \) there exists a unique \( b \in B \) such that
for each \( a \in A, \varphi(a) = abf \) for some \( f \in P \). It is
noted that the existence of a \( b \in B \) is given by
Lemma 2.8 and its uniqueness by the fact that \( A \) is non-
abelian. Consider the map \( t:H \to J(B) \) defined by
\[ t(\varphi) = j_{b} \] where \( b \) is the unique element of \( B \) associ-
ated with \( \varphi \) as determined above. It is noted that
\( g \in P \) if and only if \( g \in Z(F) \) and \( \prod_{x \in B}[g^{x}] = 1 \). Hence
for all \( \varphi \in H, \varphi(P) = P \). Now let \( \varphi_{1} \) and \( \varphi_{2} \) be in \( H 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
and let \( x \) and \( y \) be the associated elements of \( B \) for \( \varphi_1 \) and \( \varphi_2 \) respectively. Let \( a \in A \), \( \varphi_1(a) = a^x g \), and \( \varphi_2(a) = a^y f \) where \( f \) and \( g \) are in \( P \). It follows that

\[
\varphi_1 \circ \varphi_2(a) = \varphi_1(a^y f) = a^x g \varphi_1(f) = a^{xy} g \varphi_1(f) = a^{xy} h,
\]

where \( h = g^{y} \varphi_1(f) \in P \). Hence \( t(\varphi_1 \circ \varphi_2) = j_x \circ j_y = t(\varphi_1) \circ t(\varphi_2) \) and \( t \) is a homomorphism. Now \( j_b(a) = a^b \) for all \( a \in A \) and hence \( t(j_b) = j_b \). If \( s: J(B) \to H \) is the inclusion map then \( t \circ s \) is the identity on \( J(B) \) and \( H \) is a splitting extension of \( \ker t \) by \( J(B) \). Now \( \varphi \in \ker t \) if and only if \( t(\varphi) = j_e \) and hence \( \ker t = A_c(F) \cap H \).

If \( B \) is abelian \( j_b = i_b \) for all \( b \in B \) and hence \( \ker t = A_c(F) \cap H \). It follows that when \( B \) is abelian

\[
H = (A_c(F) \cap H) \times J(B).
\]

Since \( P \leq Z(F) \), it follows that \( \text{Hom}(A, P) \) is a group for any choice of the group \( A \). Recalling that \( P = \{ f \in Z(F) : \prod_{x \in B} [f(x)] = e \} \), where \( e \) is the identity of \( A \) it is clear that \( \text{Hom}(A, P) \) is isomorphic to the direct product of \( o(B) - 1 \) copies of \( \text{Hom}(A, Z(A)) \). When combined with Lemma 2.9 and Theorem 2.10, this observation yields the following immediate result.

**Corollary 2.10.1.** If \( A \) is a non-abelian indecomposable group and \( o(B) = n \), then \( o(H) = n \cdot o(\text{Hom}(A, Z(A)))^{n-1} \).

A slight digression from the investigation of \( H \) is appropriate at this time. It deals with the wreath power
of a group and hence begins with the following definition.

**Definition.** Let $A$ be a finite group. The $n$th wreath power of $A$ is defined recursively by $^1A = A$ and $^{n}A = (^{n-1}A) \wr A$ for all $n \geq 2$.

This digression is appropriate at this time since $^{n}A$ is non-abelian indecomposable for $n \geq 2$, where $A$ is any finite group. This result follows from Theorem 7.1 in Neumann [12, p. 356] which characterizes those standard wreath products which are indecomposable. Combining this result with another result of Neumann (which will be given in the proof of Theorem 2.11) and using Corollary 2.10.1 and Theorem 2.7 which deal with the orders of $H$ and $\text{Aut } W$ respectively it is possible to obtain

**Theorem 2.11.** Let $A$ be an arbitrary finite group and let $H_n$ denote the subgroup $H$ of $\text{Aut } (^nA)$ for all $n \geq 2$. Then if $|A| = m$:

(a) $|H_n| = m \cdot |\text{Hom}(A/A', Z(A))|^{(n-1)(m-1)}$ for $n \geq 3$, where $A'$ denotes the derived (commutator) subgroup of $A$ and (b) $|\text{Aut } (^nA)| = |^{n}A| \cdot \prod_{k=2}^{n} |H_k| \cdot |\text{Aut } A|^{n/|A|} n$ for all $n \geq 2$, except when $A \cong C_2$ in which case the denominator is $|A|^{n-1}$.

**Proof:** As has been noted a consequence of Neumann's work is that $^{n}A$ is non-abelian indecomposable for all $n \geq 2$.

(a) A further consequence of Neumann's work [12, p. 350]
is that $nA/(nA)' \cong n^{-1}A/(n^{-1}A)' \times (A/A')$ for all $n \geq 2$.

A simple induction argument yields $nA/(nA)' = \prod_{i=1}^{n} (A/A')$ for each $n \geq 1$. Furthermore it is a simple matter to show that $Z(nA) = Z((n^{-1}A) \wr A) \cong Z(D)$ for all $n \geq 2$.

But $Z(D) \cong Z(n^{-1}A)$ and hence $Z(nA) \cong Z(A)$ for all $n \geq 1$. Combining these three results with Corollary 2.10.1 yields $|H_n| = |A| \cdot |\operatorname{Hom}(n^{-1}A,Z(n^{-1}A))|^{m-1}$

$$= |A| \cdot |\operatorname{Hom}(n^{-1}A,Z(A))|^{m-1}$$

$$= m \cdot |\operatorname{Hom}(n^{-1}A/(n^{-1}A)',Z(A))|^{m-1}$$

$$= m \cdot |\operatorname{Hom}((A/A'),Z(A))|^{(n-1)(m-1)}$$

for all $n \geq 3$. It is noted that the relationship $|\operatorname{Hom}(A,Z(A))| = |\operatorname{Hom}((A/A'),Z(A))|$ has also been used.

(b) The proof is by induction on $n$.

$n = 2$: This is Theorem 2.7 with $A = B$.

The induction step: Since $C_2 \wr C_2$ is not a "special dihedral" group, it follows from Theorem 2.7 that if $n \geq 3$, then

$$|\operatorname{Aut}(nA)| = |nA| \cdot |H_n| \cdot |\operatorname{Aut}(n^{-1}A)| \cdot |\operatorname{Aut}A|/|A| \cdot |n^{-1}A|$$

for all groups $A$. Applying the induction hypothesis yields $|\operatorname{Aut}(nA)| =

$$|nA| \cdot |H_n| \cdot [|n^{-1}A| \cdot \prod_{k=2}^{n-1} |H_k| \cdot |\operatorname{Aut}A|^{n-1}/|A|^{n-1}] \cdot |\operatorname{Aut}A|/$$

($|A| \cdot |n^{-1}A|$) except when $A = C_2$ in which case the quantity in brackets has denominator $|A|^{n-2}$. A simple algebraic manipulation gives the desired expression for $|\operatorname{Aut}(nA)|$ and completes the induction. #
For those who wish a perhaps more descriptive formula in terms of the group $A$, it is pointed out that a standard induction argument will yield

$$|n_A| = m^1 + m^2 + \ldots + m^{n-1},$$

where $m = |A|$.

The next lemma will be used in the proof of Theorem 2.13 and again in the proof of Theorem 3.2. The lemma "roughly" stated says: If $A_j$ is a non-trivial indecomposable direct factor of the group $A$ and if $\overline{\varphi}$ is a homomorphism which acts on $A_j$ like an element of $H$ would act, then $\overline{\varphi}$ can be extended to a map $\varphi$ in $\text{Hom}(F,F)$ which is "almost" in the subgroup $H$ of $\text{Aut}(A \wr B)$. This lemma would, of course, be even more significant if the word "almost" could be removed from the above statement. One way to do that is to impose further restrictions on the group $A$ or on both of the groups $A$ and $B$. This is exactly what the hypotheses of Theorems 2.13 and 3.2 do and hence why Lemma 2.12 plays such an important role in the proofs of these theorems.

The precise statement of Lemma 2.12 is:

**Lemma 2.12.** Let $A$ and $B$ be finite groups. Let

$$A = \bigotimes_{j=1}^{s} [A_j]$$

where $A_j$ is non-trivial indecomposable for all $j = 1, 2, \ldots, s$ and let $B = \{b_1, b_2, \ldots, b_n\}$. Fix $i \in \{1, 2, \ldots, s\}$ and let $C = \bigotimes_{x \in B, j \neq i} [A_j^x]$, $L = \bigotimes_{x \in B, j = i} [A_j^x]$. (Note that $F = C \times L$.) Fix $b \in B$ and
let \( \varphi \in \text{Hom}(A, A) \) have the property that for each
\( a \in A \), \( \varphi(a) = a^b h \) for some \( h \) in \( P \) depending on \( a \).

Letting \( f \in C \) and \( g = \prod \limits_{k=1}^{n} ([a_k]b_k) \in L \) define \( \varphi : F \to F \)
by \( \varphi(f \prod \limits_{k=1}^{n} ([a_k]b_k)) = f \prod \limits_{k=1}^{n} [\varphi(a_k)b_k] \). Then \( \varphi \) has the
following properties:

(a) \( \varphi \in \text{Hom}(F,F) \)
(b) \( \varphi | A = \varphi \)
(c) \( \varphi | C \) is the identity map on \( C \)
(d) \( \varphi \in H \) if and only if \( \varphi \) is one-to-one or onto.

**Proof:** First note that \( [\varphi(a_k)b_k] = a_k^{b_k} h_k \) where
\( \varphi(a_k) = a_k^{h_k} \) with \( h_k \in P \leq Z(F) \). But \( bb_k = bb_s \) if
and only if \( k = s \). Hence any two factors in the product
given in the definition of \( \varphi \) commute and the product is
unambiguous. It is now possible to proceed with the proof
of (a) through (d).

(a) Let \( h_1 \) and \( h_2 \) be in \( F \) and express them uniquely
in the form \( h_1 = f_1 g_1 \), \( h_2 = f_2 g_2 \) where \( f_1, f_2 \in C \) and
\( g_1 = \prod \limits_{k=1}^{n} ([a_k]b_k) \), \( g_2 = \prod \limits_{k=1}^{n} ([c_k]b_k) \in L \). If \( \varphi \) and \( \varphi \)
are as in the hypotheses, then since \( g_1 g_2 = \prod \limits_{k=1}^{n} ([a_k c_k]b_k) \)
it follows that
\[
\varphi(h_1 h_2) = \varphi(f_1 g_1 f_2 g_2) = \varphi(f_1 f_2 g_1 g_2) = \prod \limits_{k=1}^{n} [\varphi(a_k)c_k b_k] = \prod \limits_{k=1}^{n} [\varphi(a_k)b_k c_k b_k].
\]
Now if \( 1 \leq m, r \leq n \), then \( \overline{\varphi}(a_m)^{bm} \equiv a_m^{bm} \pmod{p} \) and 
\( \overline{\varphi}(c_r)^{br} \equiv c_r^{br} \pmod{p} \). But \( P \leq Z(F) \) and hence
\( \overline{\varphi}(a_m)^{bm} \) commutes with \( \overline{\varphi}(c_r)^{br} \) whenever \( m \neq r \). It follows that
\[
\prod_{k=1}^{n} [\overline{\varphi}(a_k)^{b_k} \cdot \overline{\varphi}(c_k)^{b_k}] = \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k} \cdot \prod_{k=1}^{n} \overline{\varphi}(c_k)^{b_k}
\]
and therefore
\[
\varphi(h_1 h_2) = f_1 f_2 \cdot \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k} \cdot \prod_{k=1}^{n} \overline{\varphi}(c_k)^{b_k} = \varphi(h_1) \cdot \varphi(h_2)
\]
But also, \( \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k} \in LP \). Hence
\[
\varphi(h_1 h_2) = f_1 \cdot \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k} \cdot f_2 \cdot \prod_{k=1}^{n} \overline{\varphi}(c_k)^{b_k} = \varphi(h_1) \cdot \varphi(h_2)
\]
and \( \varphi \in \text{Hom}(F,F) \).

(b) and (c) are clear from the definition of \( \varphi \) and no proofs will be given.

(d) It is sufficient to show (i) \( i_x \circ \varphi = \varphi \circ i_x \) for all \( x \in B \) and (ii) \( \varphi|D \) is the identity map on \( D \). To show (i), let \( h \in F, x \in B \). Since \( h = f \cdot \prod_{k=1}^{n} (a_k)^{b_k} \)
where \( f \in C \) and \( a_k \in A_i \) for all \( k = 1,2,\ldots,n \) it follows that
\[
\varphi \circ i_x(h) = \varphi(h^x) = \varphi(f^x \cdot \prod_{k=1}^{n} (a_k)^{b_k x}) = f^x \cdot \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k x}
\]
\[
= [f \cdot \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k}]^x = i_x(f \cdot \prod_{k=1}^{n} \overline{\varphi}(a_k)^{b_k}) = i_x \circ \varphi(h)
\]
Hence \( i_x \circ \varphi = \varphi \circ i_x \) for all \( x \in B \).

To show (ii) it is first recalled that if \( h \in P \), then 
\( \prod_{k=1}^{n} (h)^{b_k} = 1 \), the identity of \( F \). Now if \( d \in D \), then \( d = fg \) where \( f \in D \cap C \) and \( g \) has constant value \( a \in A_i \). Since \( \overline{\varphi}(a) = a^{ih} \) for some \( h \in P \) it follows
that \( \varphi(d) = \varphi(fg) = f \varphi(g) = f \cdot \prod_{x \in B} [\varphi(a)]^x \)
\[ = f \cdot \prod_{x \in B} [a^b]^x \cdot \prod_{x \in B} [h^x] = f \cdot \prod_{x \in B} [a^b] \]
\[ = f \cdot \prod_{y \in B} [a^y] = fg = d. \]
Hence (ii) is established and the proof is complete. #

Now that Lemma 2.12 is in hand it is possible to give a reasonably complete description of \( H \) in the case that \( A \) is a purely non-abelian finite group. The description is contained in the following theorem and its first corollary.

**Theorem 2.13.** Let \( A \) be a purely non-abelian finite group and \( B \) a group of order \( n \). Let \( A = A_1 \times \cdots \times A_s \) where \( A_k \) is a non-trivial indecomposable group for each \( k = 1, 2, \ldots, s \) and let \( R = \prod_{k=1}^s [B \times \text{Hom}(A_k, P)] \). If \( \varphi \in H \) then

(a) for each \( k = 1, 2, \ldots, s \) there exists a unique \( b \in B \) such that \( \varphi(A_k) \leq A_k^b \cdot P \). Furthermore, the map \( \gamma: A_k \to P \) defined by \( \gamma(a) = a^{-1}[\varphi \circ \rho(a)] \) for all \( a \in A_k \) is in \( \text{Hom}(A_k, P) \). Hence each \( \varphi \in H \) determines in this way an element of \( R \).

(b) The map \( t:H \to R \) defined in (a) is a one-to-one map of \( H \) onto \( R \).

**Proof:** (a) Let \( k \) be arbitrary but fixed. Since \( A \) is purely non-abelian, \( A_k \) is non-abelian. As was mentioned in the proof of Theorem 2.10, Lemma 2.8 combined
with the fact that $A_k$ is non-abelian gives the existence of a unique $b \in B$ such that $\varphi(A_k) \leq A_k^b : P$. Since $\varphi \in H$ and $\varphi(a) = a^b f$ for each $a \in A_k$, where $f \in P$, it follows that $\gamma(a) = f^{b^{-1}}$ and it is straightforward that $\gamma$ as defined is in $\text{Hom}(A_k,P)$. Hence given $\varphi \in H$, a pair $(b,\gamma)$ where $b \in B$, $\gamma \in \text{Hom}(A_k,P)$ is obtained for each $k = 1,2,\ldots,s$.

(b) Let $\varphi \in H$ and let $(b,\gamma)$ be the $k$-th pair in $t(\varphi)$. Then for $a \in A_k$, $\varphi(a) = a^b f = a^b \gamma(a)^b$ and the pair $(b,\gamma)$ determines $\varphi$ on $A_k$. Consequently, the $s$ pairs in $t(\varphi)$ determine $\varphi$ on $A$. But an element of $H$ is completely determined by its action on $A$. Hence $t$ is one-to-one.

It remains to show that the map $t$ is onto $R$. Let $r \in R$, then the following construction will produce an $\varphi \in H$ such that $t(\varphi) = r$. For clarity, the proof is broken into two steps.

**Step 1:** Let $b \in B$ and $\gamma \in \text{Hom}(A_k,P)$. Step 1 shows how to construct a $\varphi \in H$ such that $t(\varphi)$ has the ordered pair $(b,\gamma)$ in the $k$-th position and has the ordered pair $(e,v_j)$ in all other positions, where $e$ is the identity of $B$ and $v_j$ is the homomorphism mapping everything in $A_j$ onto the identity of $F$. The construction proceeds as follows:

Define $u \in \text{Hom}(A_k,A_k^b : P)$ by $u(a) = a^b \gamma(a)^b$ for all $a \in A_k$. The map $u$ is a homomorphism since $\gamma$ is a
homomorphism and the image of $\gamma$ is in $P \leq Z(F)$. Now by Lemma 2.12 $u$ can be extended to a homomorphism $\varphi$ of $F$ into $F$ such that $\varphi|A_k = u$ and $\varphi|C$ is the identity on $C = \chi \times A_j^x$ where the product is over all $x \in B$ and all $j = 1, 2, \ldots, s$ such that $j \neq k$. Since

$$a^{-1}[\varphi^j \gamma_j (a)] = a^{-1}[\varphi(a) b^{-1}] = a^{-1}[\varphi(a)] b^{-1}$$

$$= a^{-1}[u(a) b^{-1}] = a^{-1}[a \gamma(a) b] b^{-1} = \gamma(a)$$

for all $a \in A_k$, it is clear that if $\varphi$ is in $H$, then $t(\varphi)$ is the desired $s$-tuple. Hence by Lemma 2.12 (d) it remains to show that $\varphi$ as defined is one-to-one or onto. It is shown that $\varphi$ is onto. Clearly $C \leq \text{im} \varphi$ and it is sufficient to show that $\chi_{x \in B}(A_k^x) \leq \text{im} \varphi$. It is first necessary to obtain a different description of $\chi_{x \in B}(A_k^x)$ as a set. Define $P_j$ by $P_j = \{ f \in P : f(B) \subseteq Z(A_j) \}$ for all $j = 1, 2, \ldots, s$. Then $P$ can be regarded as the direct product of the subgroups $P_j$, where $j = 1, 2, \ldots, s$. Hence if $M = \chi[P_j]$ where the product is over all $j = 1, 2, \ldots, s$ such that $j \neq k$, then $P = M \times P_k$ and any element in $P$ can be expressed uniquely in the form $gh$ where $g \in M$, $h \in P_k$. It follows that $\sigma : A_k \rightarrow P_k$ defined by $\sigma = \delta \circ \gamma$, where $\delta$ is the projection of $P$ onto $P_k$ is in $\text{Hom}(A_k, P_k)$. By Lemma 2.9, $\sigma$ gives rise to an automorphism of $A_k \wr B$ which is in the subgroup $H$ of $\text{Aut}(A_k \wr B)$. This result is exploited to yield the description.
With this different description of \( X_k \) as a set, it is now possible to show that \( \varphi \) is indeed onto and hence in \( H \).

Let \( f \in X_k \), \( f(x) = a_x \in A_k \) for each \( x \) in \( B \) and \( \gamma(a_x) = g_x h_x \) where \( g_x \in M \leq Z(F) \) and \( h_x \in P_k \).

Then (1) since \( g_x^{-1} \in M \leq C \) and \( \varphi|C \) is the identity on \( C \) it follows that \( \varphi(g) = g \) where \( g = \prod_{x \in B} (g_x^{-1})^x \);

(2) \( \varphi(a_x) = u(a_x) = a_x^b \cdot \gamma(a_x)^b \);

(3) \( f = \prod_{x \in B} (a_x^x) \); and

(4) \( h_x = \sigma(a_x) = \sigma(f(x)) \) for all \( x \in B \).

Hence

\[
\varphi(\bar{g} \cdot \prod_{x \in B} [a_x^{b-1}]) = \bar{g} \cdot \varphi(\prod_{x \in B} [a_x^{b-1}]) = \bar{g} \cdot \prod_{x \in B} [\varphi(a_x)^{b-1}] = \bar{g} \cdot \prod_{x \in B} [g_x h_x] = f \cdot \prod_{x \in B} [\sigma(f(x))]^x.
\]

It is concluded that \( \varphi \) is onto. Hence \( \varphi \) is in \( H \).

**Step 2:** Since \( r \in R \), \( r = \sum_{k=1}^{s} (b_k \cdot \gamma_k) \) where \( b_k \in B \)

and \( \gamma_k \in \text{Hom}(A_k, P) \) for all \( k = 1, 2, \ldots, s \). Define for each positive integer \( n < s \) the set
\[ R_n = \{ r \in R : b_k = e \text{ and } \gamma_k = \nu_k \text{ for all } k \text{ such that } n < k \leq s \} \text{ and let } R_s = R. \] The proof that \( t \) is onto will be by induction on \( m \). The statement to be proved by induction is: If \( A \) is the direct product of \( s \) non-abelian indecomposable factors and \( m \) is an integer such that \( 1 \leq m \leq s \), then for each \( r \in R_m \) there exists a \( \varphi \in H \) such that \( t(\varphi) = r \). It is noted that Step 1 with \( k = 1 \) anchors the induction. Now let \( s > 1 \) and let \( m \) be a positive integer such that \( 2 \leq m \leq s \). (If \( s = 1 \) there is nothing more to show.) Let \( r \in R_m \) and denote by \( (b_k, \gamma_k) \) the \( k^{th} \) ordered pair of \( r \). Hence \( b_k = e \) and \( \gamma_k = \nu_k \) for all \( k > m \). Let \( r_1 \) be the element of \( R_{m-1} \) which agrees with \( r \) on the first \( m-1 \) ordered pairs. By the induction hypothesis there exists an \( \varphi_1 \in H \) such that \( t(\varphi_1) = r_1 \). Since \( \gamma_m \in \text{Hom}(A_m, P) \) and \( \varphi_1(P) = P \) it follows that \( \varphi_1^{-1}\gamma_m \in \text{Hom}(A_m, P) \). Construct as in Step 1 a \( \varphi_2 \) in \( H \) such that the \( m^{th} \) ordered pair of \( t(\varphi_2) \) is \( (b_m, \varphi_1^{-1}\gamma_m) \) and all other ordered pairs are \( (e, \nu_k) \). Clearly \( \varphi = \varphi_1 \circ \varphi_2 \) is in \( H \). Furthermore, if \( a \in A_k \) for some \( k = 1, 2, \ldots, s \), then

\[
\varphi(a) = \varphi_1 \circ \varphi_2(a) = \begin{cases} 
\varphi_1(a) & \text{if } k \neq m \\
\varphi_1[a^m(\varphi_1^{-1}\gamma_m(a))^{b_m}] & \text{if } k = m \\
\nu_k(a)^{b_k} & \text{if } k < m \\
a & \text{if } k > m \\
\varphi_1(a^m) \cdot \gamma_m(a)^{b_m} = a^m \cdot \gamma_m(a)^{b_m} & \text{if } k = m.
\end{cases}
\]

Hence \( t(\varphi) = r \) and the proof is complete. #
Recalling that $\text{Hom}(A_k, P)$ is isomorphic to the direct product of $|B| - 1 = n - 1$ isomorphic copies of $\text{Hom}(A_k, Z(A))$ yields the following rather explicit formula for $|H|$. 

**Corollary 2.13.1.** Under the hypotheses of Theorem 2.13, 

$$|H| = |B|^s \prod_{k=1}^s |\text{Hom}(A_k, Z(A))|^{n-1},$$

where $n = |B|$. 

**Remark.** If desired, the above corollary can be combined with Theorem 2.7 on the order of $\text{Aut} W$ to give a formula for $|\text{Aut} W|$ whenever the group $A$ is purely non-abelian.

The next two corollaries provide examples of the type of results which may be extracted from Theorem 2.13 by considering various special cases.

**Corollary 2.13.2.** Let $A$ be any finite group such that $Z(A) = \{e\}$ and let $B$ be any finite group. Let $A = A_1 \times \cdots \times A_s$ where $A_k$ is non-trivial indecomposable for all $k = 1, 2, \ldots, s$. Then $H$ is the direct product of $s$ copies of $J(B) \cong B$.

**Proof:** Since $Z(A) = \{e\}$ it follows that $P = \{1\}$ and hence $R$ is isomorphic to $\prod_{k=1}^s [B]$. Furthermore, an examination of the proof of Theorem 2.13 will show that the map $t : H \to R$ is an isomorphism of groups when $Z(A) = \{e\}$. The connection with $J(B)$ is emphasized since
if \( t(\varphi) = (b_1, b_2, \ldots, b_s) \), then \( \varphi|_{A_k^B} = j_{b_k}|_{A_k^B} \) for all \( k = 1, 2, \ldots, s \) where \( A_k^B = \{ f \in F : f(B) \subseteq A_k \} \). 

Next recall that Theorem 2.11 dealt with the order of the subgroup \( H \) and the order of \( \text{Aut} W \) when \( W \) was the wreath power of a group \( A \). It is now possible to give a more complete result in the case that \( A \) is a purely non-abelian group. This result is

**Corollary 2.13.3.** Let \( A \) be a purely non-abelian finite group. If \( A = A_1 \times \cdots \times A_s \) where \( A_k \) is non-trivial indecomposable for all \( k = 1, 2, \ldots, s \), then \( |\text{Aut}(nA)| = |nA| \cdot |A|^{s-2} \cdot \prod_{k=1}^{s} |\text{Hom}(A_k, Z(A))| \cdot |A|^{-1} \cdot |\text{Aut} A|^n \) for all \( n \geq 2 \).

**Proof:** Corollary 2.13.1 with \( A = B \) yields

\( |H_2| = |A|^s \cdot \prod_{k=1}^{s} |\text{Hom}(A_k, Z(A))| \cdot |A|^{-1} \). The remainder of the proof is a straightforward calculation using the formulas given in Theorem 2.11 and is omitted.

The next three theorems are concerned with the problem of describing the subgroup \( H \) of \( \text{Aut} W \) when \( A \) is abelian or cyclic. Although no definitive results are obtained about the subgroup \( H \), these theorems show that the problem of determining \( H \) in these cases is equivalent to other unsolved problems in group theory.
Theorem 2.14. Let A be a finite abelian group and
B = \{e, b_2, \ldots, b_n\}. Let \( r: H \to \text{Aut } P \) be defined by
\[ r(\varphi) = \varphi|P \] for all \( \varphi \in H \). If \( A = \langle a_1 \rangle \times \cdots \times \langle a_m \rangle \)
where \( |a_i| = (p_i)^{k_i} \), \( p_i \) a prime for each \( i = 1, \ldots, m \)
and if \( S_i(P) \) is the Sylow \( p_i \)-subgroup of \( P \), then
the kernel of \( r \) is isomorphic to \( \prod_{i=1}^{m} [T_i] \), where
\[ T_i = D \cap \Omega_{k_i}(S_i(P)) \] for each \( i = 1, \ldots, m \). Furthermore,
\( \ker r \leq Z(H) \) and the image of \( r \), \( \text{im } r = \{ \varphi \in \text{Aut } P : \varphi(f^b) = \varphi(f)^b \} \) for all \( b \in B, f \in P \) and \( \bigcap_{j=2}^{n} [P_{ij}] \neq \emptyset \)
for all \( i = 1, \ldots, m \), where
\[ P_{ij} = \{ g \in \Omega_{k_i}(S_i(P)) : g^{a_{ij}^{-1}} = (a_{ij}^{b_j})^{-1} \varphi(a_{ij}^{b_j})^{-1} \} \].

Proof: It is trivial that if \( \varphi \in H \), then \( \varphi(P) = P \).
Hence \( r \) is well-defined. By Lemma 2.8, for each
\( a \in A \) there exists a \( b \in B \) and an \( f \in P \) such that
\( \varphi(a) = a^bf. \) But \( A \) is abelian and hence \( a^b^{-1} \in P \). It
can be concluded that for each \( a \in A \) there exists a
\( g \in P \) (let \( g = a^b^{-1}f \)) such that \( \varphi(a) = ag \).

Now if \( \varphi \in \ker r \), then \( \varphi|P \) is the identity on
\( P \) and for each \( i = 1, \ldots, m \) there exists an
\( f_i \in \Omega_{k_i}(S_i(P)) \) such that \( \varphi(a_i) = a_if_i \). Furthermore
since \( a_i^{b_j} \) is in \( P \), \( a_i^{b_j} = \varphi(a_i^{b_j}) = a_i^{b_j}f_i^{b_j}f_i^{-1} \)
for all \( i \) and \( j \). Hence for each \( i \), \( f_i^{b_j}f_i = 1 \) for all
\( j \) and \( f_i \in D \). Therefore \( f_i \in D \cap \Omega_{k_i}(S_i(P)) \) for
all \( i \). Now let \( u: \ker r \to \prod_{i=1}^{m} [T_i] \) be the map which
associates with each \( \varphi \in \ker r \) the ordered \( m \)-tuple of

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
If \( \varphi_1, \varphi_2 \in \ker r \) and 
\[
\varphi_1(a_i) = a_i f_i, \quad \varphi_2(a_i) = a_i g_i, 
\]
then recalling that 
\[
g_i \in D \quad \text{it is seen that} \quad \varphi_1 \varphi_2(a_i) = \varphi_1(a_ig_i) = \varphi_1(a_i)g_i = a_if_ig_i. 
\]
Hence \( u \) is a homomorphism. Also, since \( \varphi \in H \) is completely determined by its action on the \( a_i \) for \( i = 1, \ldots, m \), it follows that \( u \) is one-to-one.

Finally, \( u \) is onto, since if 
\[
(f_1, f_2, \ldots, f_m) \in \times_{i=1}^m [T_i],
\]
the map \( \overline{\varphi} \) defined by \( \overline{\varphi}(a_i) = a_if_i \) can be extended to an element \( \varphi \in \ker r \) such that \( u(\varphi) = (f_1, f_2, \ldots, f_m) \).

Hence \( u \) is an isomorphism of groups.

To see that \( \ker r \leq Z(H) \), let \( \varphi \in \ker r \) and \( \psi \in H \). Suppose that \( \varphi(a_i) = a_if_i \) and \( \psi(a_i) = a_ig_i \) for all \( i = 1, \ldots, m \). It is sufficient to show that 
\[
\varphi \psi(a_i) = \psi \varphi(a_i) \quad \text{for all} \quad i = 1, \ldots, m. 
\]
Noting that 
1. \( \varphi|_P \) is the identity on \( P \), 
2. \( f_i \in T_i \leq D \), and 
3. \( g_i \in \Omega_{k_i}(P) \leq P \) it follows that 
\[
\varphi \psi(a_i) = \varphi(a_ig_i) = \varphi(a_i)g_i = a_if_ig_i = a_ig_if_i = \psi(a_if_i) = \psi \varphi(a_i). 
\]
Hence \( \ker r \leq Z(H) \).

It is obvious that \( \text{im } r \subseteq \{ \psi \in \text{Aut } P : \psi(f)^b = \psi(f)^b \} \) for all \( b \in B \), \( f \in P \) and 
\[
\bigcap_{j=2}^n [P_{ij}] \neq \emptyset \quad \text{for all} \quad i = 1, \ldots, m \} = M. 
\]
The proof of the other inclusion begins by noting that 
\[
\bigcap_{j=2}^n [P_{ij}] \neq \emptyset \quad \text{if and only if} \quad \bigcap_{j=2}^n [P_{ij}] \text{ is a single coset of } T_i \text{ in } \Omega_{k_i}(S_i(P)). 
\]

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
"if" is clear. Fix $i$ and let $g, h \in \bigcap_{j=2}^{n} [P_{ij}]$, then $g_{bj-1} = h_{bj-1}$ for all $j$. Hence $(h^{-1}g)_{bj} = h^{-1}g$ for all $j$ and $h^{-1}g \in D$. Therefore $gT_i = hT_i$ and the "only if" is established. Now since $A$ is abelian it follows that $F = P \times A$ and each element of $F$ can be written canonically in the form $f \cdot \prod_{i=1}^{m} (a_i)^{s_i}$, where $f$ is in $P$ and $s_i$ is an integer for each $i$. Let $\gamma \in M$ and choose any $g_i \in \bigcap_{j=2}^{n} [P_{ij}]$. A routine verification will show that $\gamma^* : F \to F$ defined by $\gamma^*(f \cdot \prod_{i=1}^{m} (a_i)^{s_i}) = \gamma(f) \cdot \prod_{i=1}^{m} (a_i g_i)^{s_i}$ for all $f \cdot \prod_{i=1}^{m} (a_i)^{s_i} \in F$ is in $H$ and that $r(\gamma^*) = \gamma$. Hence $M \subseteq \text{im } r$. Therefore $M = \text{im } r$ and the proof is complete. #

A somewhat "sharper" result can be obtained if $(|A|,|B|) = 1$. Under these conditions it can be shown that:

**Theorem 2.15.** If $A$ and $B$ are finite groups such that $A$ is abelian and $(|A|,|B|) = 1$, then $H = \{ \gamma \in \text{Aut } P : \gamma(f^b) = \gamma(f)^b \text{ for all } b \in B, f \in P \}$. 

**Proof:** Let $r : H \to \text{Aut } P$ be defined by $r(\varphi) = \varphi|_P$ for all $\varphi \in H$. If $d \in D$, then $\prod_{b \in B}[d(b)] = [d(b)]^{|B|}$ and it follows immediately from $(|A|,|B|) = 1$ that $D \cap P = \{1\}$. Hence it is clear from Theorem 2.14 that $\ker r$ is trivial and that $H$ is isomorphic to $\text{im } r$. It is also immediate from Theorem 2.14 that $\text{im } r$ is a
subgroup of
\[ T = \{ \psi \in \text{Aut} \Gamma : \psi(f^b) = \psi(f)^b \text{ for all } b \in B, f \in \Gamma \}. \]

The proof will be complete if it can be shown that 
\[ T \subseteq \text{im } r. \] Let \( \psi \in T \) and let \( i \) be arbitrary but fixed. Let \( \psi(a_i b_j - 1)^j = f_{b_j} = a_i b_j - 1 g_{b_j} \) for each 
\[ j = 2, \ldots, n \] and note that \( \psi(e) = 1. \) Now \( \psi(a_i b_j - 1)^x = \psi((a_i b_j - 1)^x) = \psi(a_i b_j - 1, a_i b_j - 1, \ldots, a_i b_j - 1) \) and hence 
\[ g_{b_j} = g_{b_j} \cdot g_{b_j} \cdot g_{b_j} \cdot g_{b_j} \] 
for all \( j = 2, \ldots, n. \) Let \( t \) and \( s \) be integers such that 
\[ t|A| + s|B| = 1 \] and define 
\[ g = \prod_{j=2}^{n} (g_{b_j} - 1)^s. \] It follows that 
\[ g_{x - 1} = \prod_{j=2}^{n} (g_{b_j} x^s)^{-s} \cdot \prod_{j=2}^{n} (g_{b_j} x^s)^{-s} \cdot \prod_{j=2}^{n} (g_{b_j} x^s)^{-s} \cdot \prod_{j=2}^{n} (g_{b_j} x^s)^{-s} \]
\[ = [\prod_{j=2}^{n} (g_{b_j} x^s)]^{-s} \cdot [g_{b_j} x^s]^{|B|-1} \]
\[ = g_{b_j} x^s [g_{b_j} x^s]^{|B|-1} = g_{b_j} x^s |B| = g_{x^s} \text{ for all } x \in B. \]

Hence \( g \in \prod_{j=2}^{n} \left[ p_{ij} \right]. \) But \( i \) was arbitrary and it follows from Theorem 2.14 that \( \psi \in \text{im } r. \) Therefore 
\[ T \subseteq \text{im } r \] and the proof is complete. #

The final theorem of this chapter is concerned with the problem of describing the subgroup \( H \) of \( \text{Aut}(A \wr B) \) when \( A \) is a finite cyclic group and \( B \) is an arbitrary finite group. It is noted that if \( A = \langle a \rangle \) \( |a| = m \) and \( B = \{ b_1, b_2, \ldots, b_n \} \), then \( F \) is isomorphic to the group ring \( \mathbb{Z}_m[B] \) where \( \mathbb{Z}_m \) is the ring of integers modulo \( m. \) The map \( u : F \to \mathbb{Z}_m[B] \) defined by

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
It is this isomorphism which is exploited to yield

**Theorem 2.16.** Let $A = \langle a \rangle$ where $|a| = m$ and $B = \{b_1, b_2, \ldots, b_n\}$. Let $\epsilon: \mathbb{Z}_m[B] \to \mathbb{Z}_m$ be defined by $\epsilon(\sum j_i b_i) = \sum j_i \pmod{m}$ and let $I = \ker \epsilon$. If $M = \{1 + Q : Q \in I \text{ and } 1 + Q \text{ is a unit in } \mathbb{Z}_m[B]\}$, a subgroup of the multiplicative group of units of the ring $\mathbb{Z}_m[B]$, then $t: H \to M$ defined by $t(\varphi) = u(\varphi(a))$ is an isomorphism of groups.

**Proof:** Since $A$ is abelian, if $\varphi \in H$ there exists an element $g = \prod_{i=1}^n (a^{j_i})^{b_i} \in P$ such that $\varphi(a) = ag = \prod_{i=1}^n (a^{j_i})^{b_i}$ and $\sum_{i=1}^n (j_i) \equiv 0 \pmod{m}$. Now $v = u \circ \varphi \circ u^{-1}$ is an automorphism of $\mathbb{Z}_m[B]$ and $v(1) = 1 + Q$ where $Q = \sum_{i=1}^n (j_i b_i) \in I$. Furthermore $v(R) = (1 + Q)R$ for all $R \in \mathbb{Z}_m[B]$. Clearly $v^n(1) = (1 + Q)^n$ for all $n \geq 1$. Hence since $v$ is in $\text{Aut}(\mathbb{Z}_m[B])$ there exists a positive integer $k$ such that $v^k$ is the identity on $\mathbb{Z}_m[B]$ and $1 = v^k(1) = (1 + Q)^k$. Therefore $1 + Q$ is in $M$ and the map $t$ defined by $t(\varphi) = u(\varphi(a)) = 1 + Q$ for all $\varphi \in H$ is into $M$.

Next let $\varphi_1$ and $\varphi_2$ be in $H$ and suppose $u \circ \varphi_1 \circ u^{-1}(1) = 1 + Q$, $u \circ \varphi_2 \circ u^{-1}(1) = 1 + R$, then

$$u \circ \varphi_1 \circ \varphi_2 \circ u^{-1}(1) = u \circ \varphi_1 \circ u^{-1}[u \circ \varphi_2 \circ u^{-1}(1)]$$
\[ = u_o \varphi_1 \circ u^{-1}(1 + R) = (1 + Q) \cdot (1 + R) \cdot \]

Hence \( t(\varphi_1 \circ \varphi_2) = u(\varphi_1 \circ \varphi_2(a)) = u \circ \varphi_1 \circ \varphi_2 \circ u^{-1}(1) \)

\[ = (1 + Q) \cdot (1 + R) \]

\[ = [u \circ \varphi_1 \circ u^{-1}(1)] \cdot [u \circ \varphi_2 \circ u^{-1}(1)] \]

\[ = u(\varphi_1(a)) \cdot u(\varphi_2(a)) \]

\[ = t(\varphi_1) \cdot t(\varphi_2) \quad \text{and} \quad t \text{ is a homomorphism.} \]

It is immediate that \( \ker t \) is trivial and hence \( t \) is one-to-one.

Now let \( 1 + Q \in M \) and define \( v : \mathbb{Z}_m[B] \to \mathbb{Z}_m[B] \) by \( v(R) = (1 + Q)R \) for all \( R \in \mathbb{Z}_m[B] \). Note the following properties of \( v \); (1) \( v(R + S) = v(R) + v(S) \),

(2) \( v(Rb) = (1 + Q)(Rb) = [(1 + Q)R]b = v(R)b \),

(3) \( v(kN) = (1 + Q)(kN) = kN + Q(kN) \), \( k \in \mathbb{Z}_m \),

where \( N = \sum_{i=1}^{n} (b_i) \) (note if \( Q \in I \), then \( Q(kN) = 0 \)), and

(4) if \( (1 + Q)^{-1} = S \), then \( v(SR) = R \) for all \( R \) in \( \mathbb{Z}_m[B] \). Now consider the map \( u^{-1} \circ v \circ u : F \to F \). Properties (1) through (4) translate into the following properties of \( \varphi = u^{-1} \circ v \circ u \); (1) \( \varphi \) is a homomorphism,

(2) \( \varphi(f^b) = \varphi(f)^b \) for all \( b \in B \), \( f \in F \), (3) \( \varphi|D \) is the identity on \( D \), and (4) \( \varphi \) is onto (hence one-to-one). Hence \( \varphi = u^{-1} \circ v \circ u \in H \) and since \( t(\varphi) = u(\varphi(a)) = u[u^{-1} \circ v \circ u(a)] = v \circ u(a) = v(1) = 1 + Q \), the map \( t \) is onto.

Combining the above results about \( t \) yields the desired result. #
CHAPTER III

THE AUTOMORPHISM GROUP OF THE WREATH PRODUCT
OF TWO P-GROUPS

Introduction

The study of finite p-groups is an important branch of group theory. In the case that $G$ is a nilpotent group, for example, it is well known that $G$ is the direct product of its Sylow p-subgroups. Even when $G$ is an arbitrary finite group, knowing the structure of the Sylow p-subgroups often reveals information about the structure of $G$. For example, if $G$ is a finite group whose Sylow p-subgroups are all cyclic, then $G$ has a normal subgroup $N$ such that $(G/N)$ and $N$ are both cyclic.

Throughout this chapter $A$ and $B$ will denote finite non-trivial p-groups. It is noted that if $A$ and $B$ are finite groups, then $W = A \text{ wr } B$ is a p-group if and only if $A$ and $B$ are both p-groups. Hence all finite p-groups which are also standard wreath products can be constructed by choosing the p-groups $A$ and $B$ properly.

The most striking result of this chapter is Theorem 3.2. It gives a one-to-one map of $H$ onto a set $R$ in a manner similar to that of Theorem 2.13. The proof
yields a method whereby all the elements of $H$ can be constructed and a corollary gives the order of $H$ by determining the cardinality of the set $R$.

The Subgroup $H$

The first result of this chapter could possibly have been given as a corollary to Theorem 2.16. On the other hand, this result will play an important role in the proof of Theorem 3.2 and therefore could be called a lemma. However, since it gives a rather complete description of the subgroup $H$ of Aut($A \wr B$) when $A$ is a finite cyclic $p$-group and $B$ is a finite $p$-group, it has been decided that its most appropriate position is that of a theorem in this chapter.

Some of the notation of Theorem 2.16 is reviewed in the hypotheses of the theorem for the convenience of the reader.

Theorem 3.1. Let $A = \langle a \rangle$ where $|a| = p^m$ and let $B = \{b_1, b_2, \ldots, b_n\}$ be a $p$-group (i.e., $n = p^k$ for some integer $k$). If $\epsilon: \mathbb{Z}_{p^m}[B] \to \mathbb{Z}_{p^m}$ is defined by

$$
\epsilon\left( \sum_{i=1}^{n} [j_i b_i] \right) = \sum_{i=1}^{n} [j_i] \quad \text{for all} \quad \sum_{i=1}^{n} [j_i b_i] \in \mathbb{Z}_{p^m}[B] \quad \text{and} \quad I = \ker \epsilon ,
$$

then

(a) $H = 1 + I$, a subgroup of the multiplicative group of units of $\mathbb{Z}_{p^m}[B]$,

and (b) $\sigma: \text{Hom}(A, P) \to H$ defined by
\[ [\sigma(f)](\prod_{i=1}^{n} (a_{ji})^{bi}) = \prod_{i=1}^{n} [(a \cdot f(a))_{ji}]^{bi} \]
for all \( f \in \text{Hom}(A,P) \) and \( \prod_{i=1}^{n} (a_{ji})^{bi} \) in \( F \) is a one-to-one onto map.

**Proof:**

(a) By Theorem 2.16, \( H = \{ 1 + Q : Q \in I \} \) and \( 1 + Q \) is a multiplicative unit in \( Z_{p^m}[B] \). But if \( B \) is a \( p \)-group, then \( I \) is a nilpotent ideal in \( Z_{p^m}[B] \). It follows that if \( Q \in I \) there exists a positive integer \( k \) such that \( Q^k = 0 \). Therefore,
\[
(1 + Q)(1 - Q + Q^2 - \cdots + Q^{k-1}) = 1 + Q^k = 1
\]
and \( 1 + Q \) is a multiplicative unit in \( Z_{p^m}[B] \). It can be concluded that \( H = 1 + I \). It is noted that the group of units of \( Z_{p^m}[B] \) is a direct product of \( 1 + I \) and \( Z_{p^m} \) where \( Z_{p^m} \) is the group of units of \( Z_{p^m} \). A review of the proof of Theorem 2.16 shows that \( t: (1 + I) \rightarrow H \) defined by \( t(1 + Q) = u^{-1} v o u \) for all \( Q \in I \) where \( v(R) = (1 + Q)R \) for all \( R \in Z_{p^m}[B] \) gives the indicated isomorphism.

(b) If \( f \in \text{Hom}(A,P) \), then \( f \) is completely determined by its action on "a", the generator of \( A \). If \( \tau_1: \text{Hom}(A,P) \rightarrow I \) is defined by \( \tau_1(f) = u(f(a)) \) for all \( f \in \text{Hom}(A,P) \) it is straightforward that \( \tau_1 \) is an isomorphism of groups where \( I \) is considered as an abelian group under addition. Clearly \( \tau_2: I \rightarrow (1 + I) \) defined by \( \tau_2(Q) = 1 + Q \) for all \( Q \in I \) is a one-to-one onto map. It follows that \( \sigma = t \circ \tau_2 \circ \tau_1 : \text{Hom}(A,P) \rightarrow H \) is a one-to-one onto map.
one map of $\text{Hom}(A,P)$ onto $H$. But if $f \in \text{Hom}(A,P)$, then $
abla(f) = t \circ \tau_2 \circ \tau_1(f) = t \circ \tau_2[u(f(a))] = t(1 + u(f(a))) = u^{-1}v_{\circ}u$, where $v(R) = [1 + u(f(a))]R$ for all $R \in \mathbb{Z}^\mu(B)$. Hence

\[\nabla(f)(a) = u^{-1}v_{\circ}u(a) = u^{-1}v(l) = u^{-1}[1 + u(f(a))] = af(a)\]

and therefore, since it has already been established that $\nabla(f) \in H$,

\[\nabla(f)\left(\prod_{i=1}^{n} [a_{ji}]^{bi}\right) = \prod_{i=1}^{n} [\nabla(f)(a)_{ji}]^{bi} = \prod_{i=1}^{n} [(af(a))_{ji}]^{bi}\]

and the proof is complete. 

As has been the practice, whenever possible, a formula is given for the order of $H$.

**Corollary 3.1.1.** If $A$ is a finite cyclic $p$-group and $B$ is a finite $p$-group, then $|H| = |A| |B|^{-1}$.

**Proof:** Since $H \cong 1 + I$, $|H| = |1 + I| = |I| = |P|$. 

The next theorem gives a description of the subgroup $H$ of $\text{Aut}(A \wr B)$ when $A$ and $B$ are any finite $p$-groups.

**Theorem 3.2.** Let $A$ and $B$ be finite $p$-groups. Let $A = C_1 \times \cdots \times C_r \times A_1 \times \cdots \times A_s$ where for $j = 1, \ldots, r$

$C_j = \langle a_j \rangle$ and $|a_j| = p^{x_j}$, $x_j > 0$ and for $k = 1, \ldots, s$, $A_k$ is non-abelian indecomposable. Let

$R = U \times V$ where $U = \times_{j=1}^{r} [\text{Hom}(C_j, P)]$ and $V = \times_{k=1}^{s} [B \times \text{Hom}(A_k, P)]$. Then if $\varphi \in H$,
(a) for each \( j = 1, \ldots, r \), \( \sigma_j : C_j \to P \) defined by
\[
\sigma_j(a_j^n) = (a_j^{-1}[\varphi(a_j)])^n
\]
for all \( n = 1, \ldots, p^x_j \) is in \( \text{Hom}(C_j, P) \) and for each \( k = 1, \ldots, s \) there exists a unique ordered pair \((b_k, \gamma_k)\) where \( b_k \) is that element of \( B \) such that \( \varphi(b_k) \leq A_k^{p_k} \) \( P \) and \( \gamma_k : A_k \to P \) is the element of \( \text{Hom}(A_k, P) \) defined by \( \gamma_k(z) = a_{b_k}^{-1}[\varphi \circ b_k^{-1}(a)] \) for all \( a \in A_k \), and

(b) the map \( t : H \to \mathbb{R} \) which associates with each \( \varphi \in H \) the element \( w \in \mathbb{R} \) as determined in (a) is a one-to-one map of \( H \) onto \( \mathbb{R} \).

**Proof:** This proof follows the pattern of the proof of Theorem 2.13. The fact that each \( \sigma_j \) is a homomorphism follows from the fact that \( a_j \in Z(F) \). The argument that \((b_k, \gamma_k)\) satisfies the required conditions is exactly the same as in the proof of Theorem 2.13. Consequently, the map \( t \) is well-defined.

Also, noting again that \( \varphi \in H \) is completely determined by its action on \( A \), it is straightforward that \( \varphi \) can be recovered if \( t(\varphi) \) is known. It can be concluded that \( t \) is one-to-one.

It remains to show that \( t \) is onto. Again, for convenience, the proof is broken into two steps.

**Step 1.** Let \( b \in B \) and \( \gamma \in \text{Hom}(A_k, P) \) for some fixed \( k \). A few minor notational adjustments in Step 1 of the proof of Theorem 2.13 will show that it is possible to
construct a $\varphi \in H$ such that $t(\varphi)$ has the ordered pair $(b, y)$ in the $(r + k)\text{th}$ position and is trivial in all other positions.

Now if $\sigma_j \in \text{Hom}(C_j, P)$, then $\bar{\sigma}_j : C_j \rightarrow C_j \cdot P$ defined by $\bar{\sigma}_j(a_j^n) = a_j^n \cdot \sigma_j(a_j)^n$ for all $n = 1, \ldots, p^x j$ is in $\text{Hom}(C_j, C_j \cdot P)$. Applying Lemma 2.12 with $b = e$ and $\bar{\varphi} = \bar{\sigma}_j$ yields a map $\varphi_j$ which is in $H$ if and only if $\varphi_j$ is one-to-one or onto. By Lemma 2.12 (c) it is clear that $C = \bigtimes_{i \in B} \bigtimes_{1 \leq i \leq r : i \neq j} \bigtimes_{k=1}^s [A_i^k]$ is a subgroup of $\text{im} \varphi_j$, where $\Lambda = \{1 \leq i \leq r : i \neq j\}$. Hence $\varphi_j$ will be onto if $\bigtimes_{x \in B} [C_j]^x \leq \text{im} \varphi_j$. Define $P_i = \{f \in P : f(B) \subseteq C_i \}$ for all $i = 1, \ldots, r$ and $P_{k+r} = \{f \in P : f(B) \subseteq Z(A_{i_k})\}$ for all $k = 1, \ldots, s$.

Then $P$ can be regarded as the direct product of the subgroups $P_n$, $n = 1, 2, \ldots, s + r$. Hence if $M = \bigtimes_{n \neq j} [P_n]$, then $P = M \times P_j$ and any element in $P$ can be expressed uniquely in the form $gh$ where $g \in M$ and $h \in P_j$. It follows that $\rho : C_j \rightarrow P_j$ defined by $\rho = \delta \circ \sigma_j$ where $\delta$ is the projection of $P$ onto $P_j$ is in $\text{Hom}(C_j, P_j)$.

By Theorem 3.1 (b) $\rho$ gives rise to an automorphism of $C_j \wr B$ which is in the subgroup $H$ of $\text{Aut}(C_j \wr B)$. Hence $\bigtimes_{x \in B} [C_j]^x = \{f \in \bigtimes_{x \in B} [\rho(f(x))]^x : f \in \bigtimes_{x \in B} [C_j]^x\}$. Now let $f \in \bigtimes_{x \in B} [C_j]^x$, $f(x) = a_x \in C_j$ for each $x \in B$ and $\sigma_j(a_x) = g_x h_x$ where $g_x \in M \subseteq Z(F)$ and $h_x \in P_j$. Then (1) since $g_x^{-1} \in M \subseteq C$ and $\varphi_j | C$ is the identity on $C$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
it follows that \( \varphi_j(\bar{g}) = \bar{g} \) where \( \bar{g} = \prod_{x \in B} (g_x^{-1})^x \),
\[
(2) \quad \varphi_j(a_x) = \sigma_j(a_x), \quad (3) \quad f = \prod_{x \in B} [a_x]^x, \quad \text{and}
(4) \quad h_x = \rho(a_x) = \rho(f(x)) \text{ for all } x \in B. \quad \text{Hence}
\]
\[
\varphi_j(\bar{g}f) = \bar{g} \cdot \varphi_j(\prod_{x \in B} [a_x]^x, \prod_{x \in B} [\sigma_j(a_x)]^x) = \bar{g} \cdot \prod_{x \in B} [a_x \cdot \sigma_j(a_x)]^x
\]
\[
= \bar{g} \cdot \prod_{x \in B} [g_x]^x \cdot \prod_{x \in B} [h_x]^x = \bar{g} \cdot \prod_{x \in B} [\rho(f(x))]^x.
\]
It is concluded that \( \varphi_j \) is onto. Hence \( \varphi_j \in H \).

Step 2. Define for each positive integer \( n < r+s \) the set \( R_n = \{ w \in R : \text{all positions } q \text{ of } w \text{ such that } n < q \leq r+s \text{ are trivial} \} \) and let \( R_{r+s} = R \). The proof that \( t \) is onto will be by induction. The statement to be proved is: If \( A \) is the direct product of \( r \) non-trivial cyclic factors and \( s \) non-abelian indecomposable factors and \( m \) is an integer such that \( 1 \leq m \leq r+s \), then for each \( w \in R_m \) there exists a \( \varphi \in H \) such that \( t(\varphi) = w \).

It is first noted that Step 1 with \( j = 1 \) or Step 1 with \( k = 1 \) (if \( r = 0 \)) anchors the induction.

Now let \( r+s > 1 \) (if \( r+s = 1 \) the proof is finished) and let \( m \) be such that \( 2 \leq m \leq r+s \). Let \( w \in R_m \) and let \( w_1 \) be the element of \( R_{m-1} \) which agrees with \( w \) in the first \( m-1 \) positions. By the induction hypothesis there exists a \( \varphi_1 \in H \) such that \( t(\varphi_1) = w_1 \).
case 1: $m \leq r$. Let $\gamma_j$ be the $j^{th}$ position of $w$ for all $j = 1, \ldots, m$. Now $\varphi_1^{-1} \circ \gamma_m \in \text{Hom}(C_m, P)$ and it is possible to construct as in Step 1 a $\varphi_2 \in H$ such that the $m^{th}$ position of $t(\varphi_2)$ is $\varphi_1^{-1} \circ \gamma_m$ and all other positions are trivial. Clearly $\varphi = \varphi_1 \circ \varphi_2 \in H$.

Furthermore,

$$
\varphi(a) = \varphi_1 \circ \varphi_2(a) = \begin{cases}
\varphi_1(a), & \text{if } a \in A_k \text{ or } a \in C_j, j \neq m \\
\varphi_1[a \cdot \varphi_1^{-1} \circ \gamma_m(a)], & \text{if } a \in C_m \\
a \cdot \gamma_j(a), & \text{if } a \in C_j, j < m \\
a, & \text{if } a \in C_j, j \geq m \text{ or } a \in A_k \\
\varphi_1(a) \cdot \gamma_m(a) = a \cdot \gamma_m(a), & \text{if } a \in C_m.
\end{cases}
$$

Hence $t(\varphi) = w$.

case 2: $m > r$. Let $(b_m, \gamma_m)$ be the $m^{th}$ position of $w$. Here $\varphi_1^{-1} \circ \gamma_m \in \text{Hom}(A_{m-r}, P)$ and it is possible to construct as in Step 1 a $\varphi_2 \in H$ such that the $m^{th}$ position of $t(\varphi_2)$ is $(b_m, \varphi_1^{-1} \circ \gamma_m)$ and all other positions are trivial. Clearly $\varphi = \varphi_1 \circ \varphi_2 \in H$ and an argument similar to that in case 1 will show that $t(\varphi) = w$.

Hence in either case $t(\varphi) = w$ and the proof is complete. #

As usual, a formula for $|H|$ is determined from the cardinality of the set $R$. The result here is

**Corollary 3.2.1.** If $A$ and $B$ are finite $p$-groups, then

$$
|H| = \prod_{j=1}^r |\text{Hom}(C_j, Z(A))||B|^{-1} \cdot |B|^S \cdot \prod_{k=1}^S |\text{Hom}(A_k, Z(A))||B|^{-1}
$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
where $A$ has the structure indicated in Theorem 3.2.

**Proof:** $P$ is isomorphic to the direct product of $|B|-1$ isomorphic copies of $Z(A)$. #

Before continuing the list of other corollaries and remarks which can be gleaned from Theorem 3.2, a slight digression seems appropriate.

It is noted that the map $t: H \rightarrow R$ given in Theorem 3.2 exists for any finite groups $A$ and $B$ since its definition did not in any way depend on the fact that $A$ and $B$ were $p$-groups. Furthermore, even in the more general situation $t$ is still one-to-one. It follows that if $A$ and $B$ are finite groups, then $|H| \leq |R|$. A lower bound for $|H|$ can also be obtained. The construction found in Theorem 2.13 can still be used for the non-abelian direct factors of $A$. Hence it can be concluded that $\{(1,1,\ldots,1)\} \times V \subseteq \text{im } t$. Furthermore if $C = \langle a \rangle$ is a direct factor of $A$, then $\sigma: C \rightarrow C \times P$ defined by $\sigma(a^n) = (a^n)^b$ for any fixed $b \in B$ will extend by Lemma 2.12 to an element of $H$. This shows that at least part of $U \times \{(e,v_1),\ldots,(e,v_s)\}$ is always in $\text{im } t$ where $v_k$ is the trivial homomorphism. These observations are condensed into the following remark.

**Remark.** Let $A$ and $B$ be finite groups. If $A = C_1 \times \cdots \times C_r \times A_1 \times \cdots \times A_s$ where $C_j = \langle a_j \rangle$ and...
\[ |a_j| = (p_j)^{x_j} \] for some prime \( p_j \) and integer \( x_j > 0 \) and \( A_k \) is non-abelian indecomposable for each \( k = 1, \cdots, s \), then if \( n = |B| \),

\[
n^{r+s} \prod_{k=1}^{s} |\text{Hom}(A_k, P)| \leq |H| \leq \prod_{j=1}^{r} |\text{Hom}(C_j, P)| \cdot n^s \prod_{k=1}^{s} |\text{Hom}(A_k, P)|.
\]

Furthermore, these bounds are best possible.

**Proof:** The bounds are obtained as mentioned previously. In case both \( A \) and \( B \) are finite \( p \)-groups, Corollary 3.2.1 shows that the upper bound is attained. When \( A \) is purely non-abelian the upper and lower bounds coincide. An examination of \( W = C_3 \wr C_2 \) will show that the bounds given above are \( 2 \leq |H| \leq 3 \) and in fact \( |H| = 2 \). It follows that the given bounds are best possible. #

It is further noted, without proof, that \( |B|^{r+s} \) divides \( |H| \) for any finite groups \( A \) and \( B \) where \( A \) is decomposed as above.

The digression having been completed, \( A \) and \( B \) will resume their role as finite \( p \)-groups for the rest of this chapter. Also, as mentioned earlier there are other corollaries and remarks which can be obtained from Theorem 3.2. The next one of these to be considered is a result which was actually first proved by using Lemma 2.8 and a well-known result on \( p' \)-automorphisms of \( p \)-groups. However, it now seems appropriate to include it in this thesis as a corollary to Theorem 3.2.
Corollary 3.2.2. If $A$ and $B$ are finite $p$-groups, then $H$ is a $p$-group.

Proof: Since $A$ is a $p$-group all of the groups of homomorphisms appearing in the formula for $|H|$ given in Corollary 3.2.1 are $p$-groups. #

Combining Theorem 3.2 with Theorem 2.7 on the order of $\text{Aut} W$ yields the next corollary. It is pointed out that Khoroshevskii [10, p. 56] has proved the "if" portion of this corollary for $p$ an odd prime. The author is indebted to Khoroshevskii since it was his paper which suggested Lemma 2.8.

Corollary 3.2.3. If $A$ and $B$ are finite $p$-groups, then $\text{Aut} W$ is a $p$-group if and only if $\text{Aut} A$ and $\text{Aut} B$ are $p$-groups.

The next corollary gives a formula for the order of $\text{Aut} W$ when $A$ and $B$ are both abelian $p$-groups. The formula is complete in the sense that if the abelian groups $A$ and $B$ are known, then $|\text{Hom}(A,A)|$, $|\text{Aut} A|$, and $|\text{Aut} B|$ can be computed from well-known formulas. See, for example, Sanders [15, p. 226].

Corollary 3.2.4. If $A$ and $B$ are finite abelian $p$-groups, then $|H| = |\text{Hom}(A,A)|B|^{-1}$ and hence

$$
|\text{Aut} W| = \begin{cases} 8, & \text{if } A = B = C_2 \\
|A||B|^{-1}|H|\cdot|\text{Aut} A|\cdot|\text{Aut} B|, & \text{otherwise.}
\end{cases}
$$
Returning to the idea of the wreath power of a group $A$, the following three remarks are made. They are all immediate consequences of Theorem 2.11, the corollaries of Theorem 3.2, and some simple algebraic manipulations. Hence no proofs are given.

**Remark 1.** If $A$ is a finite $p$-group, then for $n \geq 2$

$$|\text{Aut}(A^n)| = \begin{cases} 2^{n(n+2)/2} & \text{if } A = C_2 \\ n^n |H_k| \cdot |\text{Aut } A|^n/|A|^n \quad \text{otherwise} \end{cases}$$

where $|H_2|$ is given by Corollary 3.2.1 with $A = B$ and $|H_k| = |A| \cdot |\text{Hom}(A/A', Z(A))| (k-1)(|A|-1)$ for all $k \geq 3$.

**Remark 2.** If $A$ is an abelian $p$-group and $A \neq C_2$ (see Remark 1) then

$$|\text{Aut}(A^n)| = n^n |\text{Hom}(A, A)| (n+1)(|A|-1) \cdot |\text{Aut } A|^n/|A|^2$$

where if $m = |A|$, then

$$n^m = m^1 + m^2 + \cdots + m^{n-1}.$$

A special case of the first two remarks is

**Remark 3.** If $A = C_p$, $p$ an odd prime (for $p = 2$ see Remark 1), then

$$|\text{Aut}(C_p^n)| = n^p |C_p| \cdot p(n+1)(p-1)^n/p^2 \quad \text{for } n \geq 2.$$

It is noted that $nC_p$ is a Sylow $p$-subgroup of $S_{p^n}$, the permutation group on $p^n$ symbols. Hence the above remark gives the order of the automorphism group of that group.
Some Results on the Structure of Aut W

Some information can be obtained about the structure of a Sylow $p$-subgroup of the outer automorphism group of $W$. This information is given in Theorem 3.4 where $A$ and $B$ are finite $p$-groups and in Theorem 3.5 where $B$ is further assumed to be abelian. First however it is convenient to describe a Sylow $p$-subgroup of Aut $W$. The description that will be found to be most useful is given in the following lemma.

**Lemma 3.3.** Let $A$ and $B$ be finite $p$-groups except that if $B = C_2$, then $A \neq C_2$. If $A_p$ and $B_p$ are Sylow $p$-subgroups of Aut $A$ and Aut $B$ respectively, then $A_p^*$ and $B_p^*$ are Sylow $p$-subgroups of $A^*$ and $B^*$ respectively. Furthermore, $Q = A_p^*H_1B_p^*$ is a Sylow $p$-subgroup of Aut $W$ and is a splitting extension of $A_p^*H_1$ by $B_p^*$.

**Proof:** Since Aut $A = A^*$ and Aut $B = B^*$ it is immediate that $A_p^*$ and $B_p^*$ are Sylow $p$-subgroups of $A^*$, $B^*$ respectively.

Now recall that $H_1$ is normal in Aut $W$ and that $A^*$ and $B^*$ commute elementwise. Since $H_1$ is a $p$-group it follows that $H_1 \triangleleft N$ is a normal $p$-subgroup of Aut $W$. Further recalling that Aut $W$ is a splitting extension of $A^*N$ by $B^*$ it is clear that $A_p^*N_{B_p}^*$ is

53
a p-subgroup of Aut W and a splitting extension of 
$A_p^*N$ by $B_p^*$. It remains to show that the index of 
$A_p^*NB_p^*$ in Aut W is relatively prime to $p$. Using 
the fact that Q is a splitting extension it is immediate 
that it is necessary to show that $|A^*N:A_p^*N| = |A^*:A_p^*|$ . 
But N is a normal p-subgroup of Aut W. Therefore 
$A^* \cap N$ is a normal p-subgroup of $A^*$ and hence $A^* \cap N = 
A_p^* \cap N$. A simple order argument yields the desired 
result. #

It is now possible to give information about the 
structure of a Sylow p-subgroup of Out W.

**Theorem 3.4.** Let A and B be finite p-groups except 
that if $B = C_2$, then $A \neq C_2$. If Q is as defined in 
Lemma 3.3, then $R = Q/(\text{Inn W})$ is a Sylow p-subgroup 
of Out W. If $S = A_p^*(\text{Inn W})/(\text{Inn W})$ and 
$T = HB_p^*(\text{Inn W})/(\text{Inn W})$, then R is a splitting exten-
sion of T by S. Furthermore, S is isomorphic to a 
Sylow p-subgroup of Out A and $T \cong B_p^*H/I(B)$ where 
$I(B) = \{i_b \in \text{Inn W} : b \in B\}$.

**Proof:** Since $I_1 \leq \text{Inn W}$ it is immediate that $R = ST$. 
If $t \in S \cap T$, then $t = \alpha^*(\text{Inn W})$ where $\alpha^* \in A_p^*$ and 
$t = h\beta^*(\text{Inn W})$ where $h \in H$, $\beta^* \in B_p^*$. It follows 
that $\alpha^* = h\beta^*i_{xf}$ for some $x \in B$, $f \in F$.

Now if $\alpha^* \in A_p^*$, then $b = \alpha^*(b) = h\beta^*i_{xf}(b)$ for 
all $b \in B$. But $h^{-1}|B$ is the identity on B and
$(\beta^*)^{-1}(b) = \beta^{-1}(b)$ for all $b \in B$. It follows that $
abla_p^{-1}(b) = i_xf(b) = i_{\beta^*}(b^x) \in B$ for all $b \in B$. Hence $f \in F \cap N(B) = D$. Therefore $\beta^{-1}(b) = i_{\beta^*}(b^x) = b^x = i_x(b)$ for all $b \in B$ and $\beta^* = (i_x^{-1})^*$. It is a routine exercise to show that $i_x = i_x \cdot j_x$ for all $x \in B$ where $j_x \in J(B) \leq H$. Also since $f \in D$, $i_xf = i_x^{i_x} = i_x^{i_x}$ and it follows that $h^x \cdot i_xf = h(i_x^{-1}) \cdot i_x^{i_x} = h(i_x^{-1}) \cdot i_x \cdot j_x \cdot i_x^f = hj_x \cdot i_x^f$. Also note that if $f \in D$ and $f(x) = a$ for all $x \in B$, then $i_x = i_x^a$. Combining the above $\alpha^* = h^x \cdot i_xf = hj_x \cdot i_x^a$ and hence $\alpha^* \cdot (i_x^{-1})^* = hj_x \in A^* \cap H = \langle 1 \rangle$. It follows that $\alpha^* = i_x^a \in \text{Inn} W$ and hence $S \cap T = \langle 1 \rangle$.

Since $Hl_1$ is normal in $\text{Aut} W$ and $A^*$, $B^*$ commute elementwise it is straightforward that $T$ is normal in $R$ and hence $R$ is a splitting extension of $T$ by $S$.

Next $A^*_p \preceq A^*_p(\text{Inn} W)$, $\text{Inn} W$ is normal in $A^*_p(\text{Inn} W)$ and $A^*_p \cap \text{Inn} W = (\text{Inn} A)^*$. Hence $S = A^*_p(\text{Inn} W)/(\text{Inn} W) \simeq A^*_p/(\text{Inn} A)^*$ which is a Sylow $p$-subgroup of $\text{Out} A$. Similarly, $H_p^* \preceq H_p^*(\text{Inn} W)$, $\text{Inn} W$ is normal in $H_p^*(\text{Inn} W)$ and $H_p^* \cap \text{Inn} W = I(B)$, hence $T = H_p^*(\text{Inn} W)/(\text{Inn} W) \simeq H_p^*/I(B)$.

If $B$ is abelian a Sylow $p$-subgroup of $\text{Out} W$ can also be viewed as a splitting extension of $A_p^*\text{H}(\text{Inn} W)/(\text{Inn} W)$ by $B_p^*(\text{Inn} W)/(\text{Inn} W)$. It is noted
that this splitting is compatible with the splitting of Aut W. Even more information about the situation when B is abelian is given by the following theorem.

**Theorem 3.5.** Let A and B be finite p-groups with B abelian except that if B = C_2, then A ≠ C_2. If \( A_p^* \) and \( B_p^* \) are Sylow p-subgroups of \( A^* \) and \( B^* \) respectively, \( S = A_p^*(\text{Inn } W)/(\text{Inn } W) \), \( U = H(\text{Inn } W)/(\text{Inn } W) \), and \( V = B_p^*(\text{Inn } W)/(\text{Inn } W) \), then \( Y = A_p^*H(\text{Inn } W)/(\text{Inn } W) \) is a splitting extension of U by S and \( R = A_p^*H(B_p^*H)/(\text{Inn } W) \), a Sylow p-subgroup of \( \text{Out } W \) is a splitting extension of Y by V. Furthermore, S is isomorphic to a Sylow p-subgroup of \( \text{Out } A \), \( U = H/I(B) \), and \( V = B_p^* \).

**Proof:** It is clear that \( Y = US \) and an argument similar to that of Theorem 3.4 will yield \( U \cap S = \{1\} \). (Note that \( J(B) = I(B) \leq H \).) Furthermore, H is normal in \( A^*H \) and it follows that Y is a splitting extension of U by S.

The fact that R is a splitting extension of Y by V follows from (1) \( J(B) = I(B) \leq H \) and (2) \( \text{Aut } W \) is a splitting extension of \( A^*H \) by \( B^* \).

As before, \( S = A_p^*/(\text{Inn } A) \). Also \( H \leq H(\text{Inn } W) \), \( \text{Inn } W \) is normal in \( H(\text{Inn } W) \) and \( H \cap \text{Inn } W = I(B) \). It follows that \( U \simeq H/I(B) \).

Finally, \( B_p^* \leq B_p^*(\text{Inn } W) \), \( \text{Inn } W \) is normal in \( \text{Inn } W \).
$B_p^*(\text{Inn } W)$ and $B_p^* \cap \text{Inn } W = \{1\}$ since $\beta^* = i_{xf}$ leads to the conclusion that $\beta^*(b) = i_f(b) = b(f^{-1})b_f$ for all $b \in B$ and hence that $\beta^* = 1$. It is concluded that $V = B_p^*(\text{Inn } W)/(\text{Inn } W) \simeq B_p^*$. #
CHAPTER IV

THE CONJECTURE "|G| divides |Aut G|

Introduction

The conjecture to be considered in this chapter is:

If G is a non-cyclic p-group of order greater than $p^2$, then $|G|$ divides $|Aut G|$.

There has been some interest in this conjecture in recent years. The conjecture has been established for p-groups of class 2 [5], for p-abelian p-groups [3], and for other classes of p-groups [2], [4]. Inroads into the general conjecture however, have been slight.

The best known result in this direction seems to be a result of Gaschütz [6], [7] (for a very readable account of this see Gruenberg [8, p. 110]) which states: If G is a finite p-group of order greater than p, then $p$ divides $|Out G|$. It is noted that the conjecture states that $|Z(G)|$ divides $|Out G|$.

The results of this chapter will extend the classes of groups for which the conjecture is known to be true. The main results are Theorems 4.3 and 4.5.

G as a Central Product

Otto [11, p. 282] has shown that if a p-group $G = A \times B$ where $A$ is abelian, $B$ is purely non-abelian

58
and \( o(B) | o(Aut B) \), then \( o(G) | o(Aut G) \). A result of this type not only extends the number of groups for which the conjecture is known to be true, but also, and perhaps more importantly, shows that the truth of the overall conjecture depends only on being able to prove it for a smaller class of groups. Otto's result shows that it is sufficient to consider \( p \)-groups with no non-trivial abelian direct factors, i.e., purely non-abelian \( p \)-groups.

The main result of this section is Theorem 4.3. It is noted that Otto's result is a special case of this theorem.

The first result of this chapter is concerned with the ability to extend an automorphism of a particular subgroup of a group to an automorphism of the entire group. The lemma is of some interest in its own right.

**Lemma 4.1.** If \( G = \langle a \rangle H \), \( a \in Z(G) \) and \( H \) is a non-trivial maximal subgroup of the \( p \)-group \( G \), then \( \alpha \in Aut H \) extends to \( \overline{\alpha} \in Aut G \) if and only if \( \alpha(a^p) = a^sp^h \), where \( 0 < s < p \) and \( h \in Z(H) \).

**Proof:** Let \( \alpha \in Aut H \) be extendible to \( \overline{\alpha} \in Aut G \). Noting that each element \( g \in G \) can be expressed uniquely in the form \( g = a^k h \), \( 0 \leq k < p \), \( h \in H \), it is seen that \( \overline{\alpha}(a) = a^sh \), \( 0 \leq s < p \), \( h \in H \). But \( s \neq 0 \), for otherwise \( \overline{\alpha} \) would map \( G \) into \( H \) and not be onto. Also, \( a \in Z(G) \) implies \( \overline{\alpha}(a) = a^sh \in Z(G) \) and so
Conversely, let $a \in \text{Aut} H$ and suppose $a(a^p) = a^{sp} h^p$, $0 < s < p$, $h \in Z(H)$ and define $\overline{a}(g) = \overline{a}(a^kh^p) = a^{sk}h^p a(h')$ for each $g = a^kh^p \in G$. To see that $\overline{a}$ is a homomorphism let $g_1, g_2 \in G$. Then $g_1 = a^{k_1}h_1$, $g_2 = a^{k_2}h_2$ where $0 < k_1, k_2 < p$, $h_1, h_2 \in H$. Let $k_1 + k_2 = k_3 + rp$ where $0 < k_3 < p$ and $r \geq 0$. It follows that $\overline{a}(g_1 g_2) = \overline{a}(a^{k_3} h_1 h_2)
abla = a^{sk_3 h_1 k_3} a^{a^{sp} h^p} a^{a^{sp} h^p} (h_1) (h_2)
abla = a^{s(k_1+k_2)} h_1^{k_1+k_2} a(h_1) a(h_2) = a^{sk_1 h_1 k_1} a(h_1) a^{sk_2 h_2 k_2} a(h_2)
abla = \overline{a}(g_1) \overline{a}(g_2)$. Clearly $\overline{a}$ extends $a$; furthermore $\overline{a}(a^{k_1}h_1) = \overline{a}(a^{k_2}h_2)$ implies $a^{sk_1 h_1 k_1} a(h_1) = a^{sk_2 h_2 k_2} a(h_2)$ and hence $a^{s(k_1-k_2)} \in H$. Therefore $k_1 = k_2$. It follows that $\overline{a}(h_1) = \overline{a}(h_2)$ and hence $h_1 = h_2$. Hence $\overline{a}$ is one-to-one and $\overline{a} \in \text{Aut} G$. #

Theorem 4.3 can be obtained quite easily from the following special case. Before stating the next lemma however it is necessary to make the following definition.

If $G$ is a finite $p$-group, then

$$\Omega_k(G) = \langle \{ g \in G : o(g) \mid p^k \} \rangle .$$

Lemma 4.2. If $G = \langle a \rangle H$, $a \in Z(G)$, $H$ is a non-trivial maximal subgroup of the $p$-group $G$ and $o(H) \mid o(\text{Aut} H)$, then $o(G) \mid o(\text{Aut}_H G) \mid o(\text{Aut} G)$.
Proof: The proof is broken into two cases.

Case 1. $o(a) = p$. This is actually a special case of Otto's result. However, an independent proof is given so that Otto's result might be seen to be a corollary of Theorem 4.3.

It is first noted that every automorphism of $H$ extends to an automorphism of $G$. Hence the restriction map $\theta : \text{Aut}_HG \to \text{Aut}H$ is onto.

Let $\alpha \in \ker \theta$. It follows that $\alpha(a) = a^{s_h}$ where $0 < s < p$ and $h \in \Omega_1(Z(H))$. Conversely, for each $s$ such that $0 < s < p$ and $h \in \Omega_1(Z(H))$ define $\beta : G \to G$ (dependent on the choices of $s$ and $h$) by $\beta(a^{k_h}) = a^{sk_hk_h}$ for all $a^{k_h} \in G$. It is routine that $\beta \in \ker \theta$. Hence $o(\ker \theta) = (p - 1) \cdot o(\Omega_1(Z(H)))$. It can be concluded that $o(\text{Aut}_HG) = o(\ker \theta) \cdot o(\text{Aut}H) = (p - 1) \cdot o(\Omega_1(Z(H))) \cdot o(\text{Aut}H)$. Since $o(H) | o(\text{Aut}H)$ it follows that $o(G) | o(\text{Aut}_HG) | o(\text{Aut}G)$.

Case 2. $o(a) > p$. A restatement of Lemma 4.1 shows that $\alpha \in \text{Aut}H$ extends to $\overline{\alpha} \in \text{Aut}G$ if and only if the induced automorphism $\alpha^* \in \text{Aut}[Z(H)/\xi(Z(H))]$ leaves $\langle a^P \rangle \leq Z(H)/\xi(Z(H))$ invariant. Consider the permutation representation $(\text{Aut}H, X)$; where $X = \{\text{cyclic subgroups of } Z(H)/\xi(Z(H))\}$. Then $E = \{\alpha \in \text{Aut}H : \alpha \text{ is extendable to } \overline{\alpha} \in \text{Aut}G\} = \text{St}(\langle a^P \rangle)$, the stabilizer of $\langle a^P \rangle$.

Now $|\text{Aut}H : E|$ is the order of one orbit and hence $|\text{Aut}H : E| \leq |X| = (p^r - 1)/(p - 1) < p^r$ where
Z(H)/Z(Z(H)) is elementary abelian of rank r. Hence
\[ p^r > (|Aut H|_p)/(|E|_p) \text{ and } (|Aut H|_p)^{p^{r-1}}|E|_p \]
where
\[ |G|_p \] is the highest power of p dividing |G|. Using the hypothesis that \( o(H) | o(Aut H) \) it is seen that \( o(G) | p^r | |E|_p \) and the proof will be complete if
\[ p^r (|E|_p) | o(Aut H) \]. Again consider the restriction map
\( \theta: Aut_H G \to Aut H \) and note that \( im \theta = E \). Let \( \alpha \in \ker \theta \) and suppose that \( \alpha(a) = a^{s_h} \) where \( 0 < s < p \) and \( h \in Z(H) \). Then \( \alpha(a^p) = [\alpha(a)]^p = a^p \) implies
\[ a^{s_h} = a \mod \Omega_1(Z(G)) \]. Clearly, \( \Omega_1(Z(H)) \subseteq \Omega_1(Z(G)) \).
If this inclusion is proper, there exists an element \( a' \in Z(G) \) with \( a' \not\in H \) and \( o(a') = p \). Hence case 1 applies. Therefore without loss of generality
\[ \Omega_1(Z(H)) = \Omega_1(Z(G)) \] and consequently \( a^{s_h} = ah' \) for some \( h' \in \Omega_1(Z(H)) \). Conversely, for each \( h' \in \Omega_1(Z(H)) \) the map \( \overline{\alpha}: G \to G \) defined by \( \overline{\alpha}(a^h) = (ah')^h \) for all \( a^h \in G \) is in \( \ker \theta \). It follows that
\[ o(\ker \theta) = o(\Omega_1(Z(H))) = o(Z(H)/Z(Z(H))) = p^r \]
and hence \( p^r \cdot o(E) = o(Aut_H G) \). This implies
\[ p^r (|E|_p) | o(Aut_H G) \] completing the proof. 

It is now possible to state and prove the main result of this section.

**Theorem 4.3.** If a p-group \( G \) is the central product of non-trivial subgroups \( H \) and \( A \), where \( A \) is abelian and \( o(H) | o(Aut H) \), then \( o(G) | o(Aut G) \).
Proof: Note that $A \leq Z(G)$ and let $|A : H \cap A| = p^n$ where $n \geq 1$. The proof is by induction on $n$.

$n = 1$. Lemma 4.2 gives this result for without loss of generality $A = \langle a \rangle$.

The induction step. Let $n > 1$ and select $A_1 \subset A$ such that $H \cap A < A_1 < A$ and $|A_1 : H \cap A| = p$. Let $H_1 = HA_1$. It follows that $H \cap A_1 = H \cap A$ and $|A_1 : H \cap A_1| = p$. Hence by Lemma 4.2 $o(H_1)|o(Aut H_1)$.

But $G = H_1 A$ and $H_1 \cap A = A_1$. Hence $|A : H_1 \cap A| = p^{n-1}$ and the induction hypothesis yields $o(G)|o(Aut G)$. #

As was noted earlier, Otto's result shows that the truth of the overall conjecture depends on being able to prove it for purely non-abelian $p$-groups. Theorem 4.3 has a similar effect as can be noted from the following remark. The proof of this remark is straightforward and hence is omitted.

Remark. For a finite $p$-group $G$, the following are equivalent:

(i) $G$ is the central product of proper subgroups $A$ and $H$ where $A$ is abelian.

(ii) There exists a maximal subgroup $K$ of $G$ such that $Z(K) < Z(G)$.

(iii) $Z(G) \nsubseteq \mathfrak{z}(G)$.
This section investigates the conjecture "$o(W)$ divides $o(\text{Aut } W)$" when the group $W$ is a standard wreath product of finite $p$-groups. Many of the results of Chapters II and III can be used to shed some light on the conjecture in this case. The first theorem to be stated can be seen to be of the same type as Theorem 4.3. This theorem has a number of consequences, one of them is (fortunately or unfortunately?) that standard wreath products are not the place to look for counterexamples to the conjecture.

**Theorem 4.4.** If $A$ and $B$ are finite $p$-groups, $W = A \text{ wr } B$ and $o(A)|o(\text{Aut } A)$, then $o(W)|o(\text{Aut } W)$.

**Proof:** The proof is in two cases.

**Case 1.** $A = B = C_2$. Here $W = D_8 \cong \text{Aut } D_8$. Clearly, $o(W)|o(\text{Aut } W)$.

**Case 2.** Not both $A$ and $B$ are $C_2$. By Theorem 2.7, $o(\text{Aut } W) = o(W) \cdot o(H) \cdot o(\text{Aut } A) \cdot o(\text{Aut } B)/o(A) \cdot o(B)$. Since $o(A)|o(\text{Aut } A)$ it is sufficient to show that $o(B)$ divides $o(H) \cdot o(\text{Aut } B)$. But Lemma 2.6 shows that $J(B) \leq H$ and $J(B) \cong B$. It follows that $o(B)|o(H)|o(H) \cdot o(\text{Aut } B)$.

An interesting corollary to Theorem 4.4 is

**Corollary 4.4.1.** If $A$ is a finite abelian $p$-group, $B$
is a finite p-group and $W = A \wr B$, then $o(W) | o(\text{Aut} W)$.

\textbf{Proof:} The proof is divided into four cases.

\textbf{case 1.} $A$ non-cyclic and $o(A) > p^2$. It is well known that under these conditions $o(A) | o(\text{Aut} A)$. Hence Theorem 4.4 yields the result in this case.

\textbf{case 2.} $A = C_p \times C_p$. It follows from Corollary 3.2.1 that $|H| = |A||B|^{-1}. |A||B|^{-1}$. A simple algebraic argument will show $|H| = |A|^2(|B|^{-1}) = p^4(|B|^{-1}) \geq p.|B|$. But $H$ is a p-group and hence $p.|B|$ divides $|H|$. Since $p | o(\text{Aut} A)$ it follows that $o(A) \cdot o(B)$ divides $o(H) \cdot o(\text{Aut} A)$. Theorem 2.7 now yields the desired result.

\textbf{case 3.} $A$ cyclic, except if $B = C_2$, then $A \neq C_2$. If $o(A) = p^n$, then $o(\text{Aut} A) = p^{n-1}(p - 1)$. In this case Corollary 3.2.1 gives $|H| = |A||B|^{-1}$ and another algebraic argument will show that $|H| = |A||B|^{-1} \geq p.|B|$. Hence again $o(A) \cdot o(B) | o(H) \cdot o(\text{Aut} A)$ and case 3 can be established.

\textbf{case 4.} $A = B = C_2$. Again $C_2 \wr C_2 = D_8 \approx \text{Aut} D_8$. #

Corollary 3.2.1 again plays an important role in the following theorem.

\textbf{Theorem 4.5.} Let $A$ and $B$ be finite p-groups and let $A = C \times A_1 \times \cdots \times A_s$ where $C$ is abelian and $A_k$ is non-abelian indecomposable for all $k = 1, \cdots, s$. If $W = A \wr B$ and $|A_k|$ divides
\[ |\text{Hom}(A_k, Z(A_k))| \leq |\text{Hom}(A_k, P_k)| \quad \text{which divides} \]
\[ \left| \frac{|\text{Hom}(A_k, Z(A_k))|}{|B|^{-1}} \right| = \left| \frac{|\text{Hom}(A_k, P_k)|}{|\text{Hom}(A_k, Z(A_k))|} \right| \]

\[ \text{Proof:} \quad \text{There are two cases to consider.} \]

**case 1.** \( s = 0 \). If \( s = 0 \), then \( A \) is abelian and Corollary 4.4.1 yields the desired result.

**case 2.** \( s > 0 \). If \( s > 0 \), then

\[ \circ(\text{Aut } W) = \circ(W) \cdot \circ(H) \cdot \circ(\text{Aut } A) \cdot \circ(\text{Aut } B) / \circ(A) \cdot \circ(B) . \]

Define \( P_k = \{ f \in P : f(B) \subseteq Z(A_k) \} \), then

\[ |\text{Hom}(A_k, Z(A_k))| \leq |\text{Hom}(A_k, P_k)| \]

\[ \text{It follows that} \quad \prod_{k=1}^{s} |A_k| \quad \text{divides} \quad \prod_{k=1}^{s} |\text{Hom}(A_k, P_k)| \]

\[ \text{Next suppose without loss of generality that} \quad C = C_1 \times \cdots \times C_r \quad \text{where} \quad C_j \quad \text{is cyclic of order} \quad p^{x_j} \quad \text{and} \quad x_1 \leq x_2 \leq \cdots \leq x_r \]. It is immediate that \( |C| \) divides \( |\text{Hom}(C_r, P)| \). It can be concluded that \( |C| \) divides \( \prod_{j=1}^{r} |\text{Hom}(C_j, P)| \).

Now Corollary 3.2.1 gives the order of \( H \) as

\[ |H| = \prod_{j=1}^{r} |\text{Hom}(C_j, P)| \cdot |B|^s \cdot \prod_{k=1}^{s} |\text{Hom}(A_k, P_k)| . \]

Hence \( \circ(A) \cdot \circ(B) \cdot \circ(H) \cdot \circ(\text{Aut } A) \) and the result follows. \#

Theorem 4.5 can be used to obtain a number of conditions on the \( p \)-groups \( A \) and \( B \) which would guarantee that \( \circ(W) \mid \circ(\text{Aut } W) \). An example of one such condition is given in the following corollary.
Corollary 4.5.1. If $A$ and $B$ are finite $p$-groups and $|B| \geq |Z(A)|$, then $\sigma(W)|\sigma(\text{Aut}W)$.

Proof: If $A$ is abelian there is nothing to show; hence let $A_k$ be a non-abelian indecomposable direct factor of $A$. Since $2^m \geq 2^{m+1} \geq m + 2$ for all integers $m \geq 1$ and all primes $p$, it follows that $(p^2)^{|B|-1} \geq |B| \geq |Z(A)| \geq |Z(A_k)|$. Now $|\text{Hom}(A_k,Z(A_k))| = |\text{Hom}(A_k/A'_k,Z(A'_k))|$ and so $p^2$ divides $|\text{Hom}(A_k,Z(A_k))|$. Therefore $|Z(A_k)| \leq (p^2)^{|B|-1} \leq |\text{Hom}(A_k,Z(A_k))||B|-1$ and it can be concluded that $|Z(A_k)|$ divides $|\text{Hom}(A_k,Z(A_k))||B|-1$. It is immediate that $|A_k|$ divides $|\text{Hom}(A_k,Z(A_k))||B|-1$. $|\text{Aut}A_k|$. Theorem 4.5 now yields the desired result. #

An almost trivial consequence of Corollary 4.5.1 is contained in the following

Remark. If $A$ is a finite non-trivial $p$-group, then $\sigma(A_n)|\sigma(\text{Aut}[A_n])$ for all $n \geq 2$.

Proof: $Z(A_n) \approx Z(A)$ for all $n \geq 1$. Hence $|A| \geq |Z(A_n)|$ for all $n \geq 1$. #

Although the previous theorems, corollaries, and remark have shown that $\sigma(W)|\sigma(\text{Aut}W)$ under many different and varied hypotheses on the finite $p$-groups $A$ and $B$,
no proof has yet been given to show that it is always true. In fact, no proof has yet been found by this author. One possible approach to the more general result is indicated by the following theorem. This theorem shows that the conjecture is true for the wreath product of any two finite p-groups if a weaker result is true for all non-abelian indecomposable p-groups.

**Theorem 4.6.** The following Statements are equivalent.

(i) If A and B are finite non-trivial p-groups and $W = A \text{ wr } B$, then $\sigma(W) | \sigma(\text{Aut } W)$.

(ii) If G is a non-abelian indecomposable p-group, then $\sigma(G) | \sigma(\text{Hom}(G, Z(G)))^{p-1} \cdot \sigma(\text{Aut } G)$.

**Proof:** (i) implies (ii). Let G be a non-abelian indecomposable p-group and consider $W = G \text{ wr } C_p$. Now by Theorem 2.7

$$\sigma(\text{Aut } W) = \sigma(W) \cdot \sigma(H) \cdot \sigma(\text{Aut } G) \cdot \sigma(\text{Aut } C_p) / \sigma(G) \cdot \sigma(C_p)$$

and by Corollary 3.2.1,

$$\sigma(H) = p \cdot \sigma(\text{Hom}(G, P)) = p \cdot \sigma(\text{Hom}(G, Z(G)))^{p-1}.$$ 

It follows that $\sigma(G) | \sigma(\text{Hom}(G, Z(G)))^{p-1} \cdot \sigma(\text{Aut } G)$ since it has been assumed that $\sigma(W) | \sigma(\text{Aut } W)$.

(ii) implies (i). If (ii) is true, then $\sigma(A_k)$ divides $\sigma(\text{Hom}(A_k, Z(A_k)))^{p-1} \cdot \sigma(\text{Aut } A_k)$ for all non-abelian indecomposable direct factors $A_k$ of A. Theorem 4.5 now yields the desired result. #
The thesis is concluded with the following remark. The reader is asked to notice the implications of this remark as it pertains to Theorem 4.6 and Theorem 4.5.

**Remark.** If $G$ is a non-abelian indecomposable finite $p$-group and $\exp(Z(G)) \leq \exp(G/G')$, then

$$o(G) | o(Hom(G, Z(G))) \cdot o(\text{Inn } G) | o(Hom(G, Z(G)))^{p-1} \cdot o(\text{Aut } G).$$

**Proof:** $o(Hom(G, Z(G))) = o(Hom([G/G'], Z(G))) \geq o(Z(G))$ and hence $o(Z(G)) | o(Hom(G, Z(G)))$. The result is now immediate. 

#
BIBLIOGRAPHY


70

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

