AN ABSTRACT OF THE THESIS OF

Scott Garten for the Master of Arts in Mathematics presented on July 29, 1977.

Title: The Wreath Product

Abstract approved: Marion P. Emerson

This thesis deals with a topic in abstract algebra, the wreath product. The wreath product is a special type of permutation group which acts on ordered pairs. An example is given to illustrate the algebraic structure of the wreath product. Methods of performing the operation of composition of mappings as defined for the wreath product are demonstrated. Theorems concerned with the structure of wreath products are developed.

The importance of the concept of wreath products lies in their use in constructing certain types of subgroups of symmetric groups. These subgroups are the Sylow p-subgroups of symmetric groups. The method of constructing Sylow p-subgroups with wreath products is developed. Computation of the number of Sylow 3-subgroups of the symmetric group on thirteen elements is performed. Similar computations for symmetric groups on 12, 14, and 15 elements are shown.

One chapter is devoted to investigating which wreath products have the same internal structure; that is, which are isomorphic. Theorems demonstrating isomorphisms between certain wreath products

with the same number of elements, that is, the same order, are developed, and conclusions for wreath products of order less than 100 are derived from these theorems.

Some minor results of the study are presented in Chapter VI.

THE WREATH PRODUCT

A Thesis

Presented to

the faculty of the Department of Mathematics

Emporia State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

---

by

Scott Garten

July 1977

Marion P Emerson

Approved for the Major Department

Lowell E Durst

Approved for the Graduate Council

6

ACKNOWLEDGMENT

I wish to express my gratitude to Dr. Marion Emerson, without whose encouragement and assistance this Thesis would never have been written.

Table of Contents

List of Tables

Chapter I: Introduction

The wreath product is a special form of permutation group. Understanding the nature of the wreath product facilitates comprehension of certain types of subgroups of the symmetric groups. It is the intention of this thesis to present the concept of the wreath product in a manner that a reader with only a basic knowledge of abstract algebra can understand. It is assumed that the reader has had a course in abstract algebra.

This thesis deals with finite groups.

Some remarks concerning notation and statements of useful theorems (without proof) are in order. Since the topic at hand is permutation groups, the reader is reminded that a permutation group G is a set of one-to-one mappings (permutations) of elements of some set A onto the same set A.

The notation indicating the action of a mapping (permutation) on an element of a set will for the most part be exponential. If a is an element of set A and g is a mapping, a^g is the element to which g maps a.

Permutations are often given in cyclic notation. For instance, (123) is a permutation which maps 1 to 2, 2 to 3, and 3 to 1. It is a mapping of $\{1,2,3\}$ to itself. $1^{(123)} = 2$, $2^{(123)} = 3$, and $3^{(123)} = 1$.

A group G which is generated by a finite set of elements a_1, $a_2, \ldots, a_n$ is designated $\langle a_1,a_2, \ldots, a_n\rangle$. Thus $G = \langle a_1,a_2,\ldots,a_n\rangle$.

A permutation group on a set of n elements consisting of all $n!$ possible one-to-one onto mappings of the set to itself is the symmetric group on n, designated S_n.

The number of elements of a set A is denoted by $|A|$. The number of elements in a group G, the order of the group, is designated similarly, $|G|$.

The identity element of a permutation group is designated as (1).

The theorems which the reader will find helpful are listed along with definitions of appropriate concepts.

1.) Definition of homomorphism: A mapping of the elements of a group G to those of a group H is called a homomorphism if and only if $g_1 \to h_1$ and $g_2 \to h_2$ implies $g_1 g_2 \to h_1 h_2$.

2.) Definition of isomorphism: A one-to-one homomorphism of G onto H is an isomorphism.

The reader is reminded that identities are mapped to identities, and inverses are taken to inverses by homomorphisms.

3.) Cayley's Theorem: Every group G is isomorphic to a permutation group of its own elements.

4.) LaGrange's Theorem: If H is a subgroup of G, then $|H|$ divides $|G|$.

The order of an element a of a group G is the smallest positive integer n such that $a^n = (1)$. Since $\langle a\rangle$ is a subgroup of G, and

$|\langle a\rangle| = n$, the order of an element of a group G must divide the order of the group G.

5.) Definition of conjugates: Two elements s and s' of a group G are conjugate if and only if for some $x \in G$, $x^{-1}sx = s'$.

6.) Definition of conjugate sets: Two sets of elements S and S' are conjugate if for some fixed $x \in G$, $x^{-1}Sx = S'$.

7.) Theorems concerning conjugate sets:

(a) If S and S' are conjugate sets, they contain the same number of elements.

(b) Any set conjugate to a subgroup is also a subgroup.

(c) Two conjugate subgroups are isomorphic. The operation of conjugation is an isomorphism.

8.) Definition of normal subgroups: A subgroup H of a group G is a normal subgroup if $x^{-1}Hx = H$ for all $x \in G$. A normal subgroup H of G is sometimes called a self-conjugate subgroup.

9.) Definition of coset: Given a group G and a subgroup H. The set of elements hx, all $h \in H$, $x \in G$, x fixed, is called a right coset of H, and is designated Hx. Similarly, the set of elements xh, all $h \in H$, is called a left coset xH of H.

10.) Theorems on cosets:

(a) for H a subgroup of G, all $x,y \in G$, either $Hx \cap Hy = \emptyset$ or $Hx = Hy$.

(b) $|xH| = |H|$ and $|Hx| = |H|$

11.) Definition of a factor group: If H is a normal subgroup in G, the factor group G/H consists of all distinct right cosets of H. The operation in G/H is defined as $(Hx_i)(Hx_j) = Hx_ix_j$.

$|G/H| = \frac{|G|}{|H|}$

H is the identity element in G/H.

12.) The First Theorem on Homomorphisms: In the homomorphism $G \to H$, the set T of elements of G mapped onto the identity of H is a normal subgroup of G. T is called the kernel of the homomorphism.

13.) The Second Theorem on Homomorphisms: Given a group G and a normal subgroup T; then if $H = G/T$, there is a homomorphism $G \to H$ whose kernel is T. This homomorphism is given by $g \to Tx_i$ if $g \in Tx_i$ in G.

14.) The Third Theorem on Homomorphisms: If $G \to K$ is a homomorphism of G onto K and T is the kernel of the homomorphism, then K is isomorphic to G/T, $(K \simeq G/T)$.

15.) Definition of Direct Product: The direct product of groups $A_1, A_2, \ldots, A_n$, designated $(A_1 x A_2 x \ldots x A_n)$ is the set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$ for $a_i \in A_i$. The product of $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ is defined by

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

The direct product is a group.

16.) A theorem concerning direct products: A group G is isomorphic to the direct product of subgroups A_i for i = 1, 2,..., n, if

(a) every A_i is a normal subgroup of G;

(b) $A_j \cap (\underset{i \neq j}{\cup} A_i) = \langle 1 \rangle$, the identity subgroup for all j = 1, 2,..., n.

(c) $G = \cup A_i$ for i = 1, 2,..., n.

If this isomorphism is satisfied, G, is called the direct product of the A_i's, equating (1, 1,..., a_i,..., 1) to a_i.

17.) A preliminary to the Sylow Theorems:

If the order of a group G is divisible by a prime p, then G contains an element of order p.

18.) The first Sylow Theorem: If G is of order $n = p^m s$, where p does not divide s, p a prime, then G contains subgroups of order p^i, for i = 1, 2,..., m, and each subgroup of order p^i, i = 1, 2,..., m-1 is a normal subgroup of at least one subgroup of order p^{i+1}.

19.) Definition of p-group: A group P is a p-group if every element of P has order a power of a prime p.

20.) Definition of Sylow p-subgroup: A subgroup S of a group G is a Sylow p-subgroup of G if it is a p-group and is not contained in any larger p-group which is a subgroup of G.

21.) A corollary to the first Sylow Theorem: Every finite group G of order $n = p^m s$, where $(p,s) = 1$, p a prime, contains a Sylow p-subgroup of order p^m, and every p-group which is a subgroup of G is contained in a Sylow p-subgroup of G.

22.) The Second Sylow Theorem: In a finite group G, the Sylow p-subgroups are conjugate.

23.) The Third Sylow Theorem: The number of Sylow p-subgroups of a finite group G is of the form $1 + kp$ and is a divisor of $|G|$.

The above definitions and theorems are referred to from time to time as they are needed to prove the theorems involving wreath products.

Chapter II: The Wreath Product

As the introduction states, wreath products are permutation groups. They act on sets of ordered pairs. The fashion in which the elements of a wreath product permute the ordered pairs depend upon the components of each ordered pair.

Let G be a permutation group on the set A and H be a permutation group on set B, with $|A| = m$ and $|B| = n$. Without loss of generality, let $A = \{1, 2, \ldots, m\}$ and $B = \{1, 2, 3, \ldots, n\}$.

Allow G^* to be the set of all n-tuples of elements of G. There exist mappings ϕ from the ordered set $B = \{1, 2, \ldots, n\}$ to each element of G^*: $\phi(i)$ is the i^{th} component of the element of G^*. Each of these n-tuples of G^* can be considered to be an element of the direct product of n copies of G, $G_1 X G_2 X \ldots X G_n$. There are $|G|^n$ n-tuples in G^*.

The wreath product of G by H, designated $G \wr H$, is a group of mappings (permutations) on $A \times B$ onto itself. These mappings are represented by $\theta = [g_1, g_2, \ldots, g_n; h]$ where $g_i \in G$ and $h \in H$. The mapping θ on $A \times B$ is defined by

$$(a,i)^{\theta} = (a,i)^{[g_1, g_2, \ldots, g_n; h]} = (a^{\phi(i)}, i^h) = (a^{g_i}, i^h)$$

To prove that $G \wr H$ is a group, first examine closure. For θ_1 and θ_2 elements of $G \wr H$, $\theta_1 \theta_2$ is a product of mappings and is well-defined; that is, $\theta_1 \theta_2 \in G \wr H$. If $\theta_1 = [g_1, g_2, \ldots, g_n; h]$ and $\theta_2 = [p_1, p_2, \ldots, p_n; k]$ then $(a,i)^{\theta_1 \theta_2} = [(a,i)^{\theta_1}]^{\theta_2} = (a^{\phi(i)}, i^h)^{\theta_2} =$

$(a^{g_i}, i^h)\theta_2 = ((a^{g_i})\phi'(i^h), (i^h)^k) = (a^{g_i p_{ih}}, i^{hk}) = (a,i)^{\theta_3}$ for $\Theta_3 =$ $[g_1p_1h, g_2p_2h, \ldots, g_np_nh; hk]$. Since $g_ip_{ih} \in G$ and $hk \in H$, $\Theta_3 \in G \wr H$.

Examining this result closely shows that it is not necessary to consider the action of the elements of $G \wr H$ on $(a,i) \in A \times B$ when computing products of elements of $G \wr H$. Notice that in $\theta_1\theta_2$, h permuted the p_i's in θ_2. In the example which follows this proof, the action of h_i in $\theta_i\theta_j$ on the g_j components of θ_j is demonstrated.

Since composition of mappings is an associative operation, it is seen that for $\theta_i, \theta_j, \theta_k \in G \wr H$, $(\theta_i\theta_j)\theta_k = \theta_i(\theta_j\theta_k)$.

There exists an identity element $I \in G \wr H$. $I = [(1),(1),\ldots,(1);(1)]$. For $\theta \in G \wr H$, $\theta I = I\theta = \theta$ since

$$
\begin{aligned}
&[g_1, g_2, \ldots, g_n; h][(1),(1),\ldots,(1);(1)] \\
&= [g_1(1), g_2(1), \ldots, g_n(1); h(1)] \\
&= [g_1, g_2, \ldots, g_n; h] = \theta
\end{aligned}
$$

and

$$
\begin{aligned}
&[(1),(1),\ldots,(1);(1)][g_1, g_2, \ldots, g_n; h] \\
&= [(1)g_1, (1)g_2, \ldots, (1)g_n; (1)h] \\
&= [g_1, g_2, \ldots, g_n; h] = \theta
\end{aligned}
$$

Each $\theta \in G \wr H$ has an inverse in $G \wr H$. If $\theta = [g_1, g_2, \ldots, g_n; h]$, then $\theta^{-1} = [(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})^{h^{-1}}; h^{-1}]$

since

$$
\begin{aligned}
&[g_1, g_2, \ldots, g_n; h][(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})^{h^{-1}}; h^{-1}] \\
&= [(g_1, g_2, \ldots, g_n)(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})^{h^{-1}h}; hh^{-1}] \\
&= [(g_1, g_2, \ldots, g_n)(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) \; ; \; (1)] \\
&= [g_1g_1^{-1}, g_2g_2^{-1}, \ldots, g_ng_n^{-1}; \; (1)]
\end{aligned}
$$

$= [(1),(1),\ldots,(1);\ (1)] = I$

Similarly $[(g_1^{-1},g_2^{-1},\ldots,g_n^{-1})^{h^{-1}};h^{-1}][g_1,g_2,\ldots,g_n;h]$

$= [(g_1^{-1},g_2^{-1},\ldots,g_n^{-1})^{h^{-1}}(g_1,g_2,\ldots,g_n)^{h^{-1}};\ h^{-1}h]$

$= [\{(g_1^{-1},g_2^{-1},\ldots,g_n^{-1})(g_1,g_2,\ldots,g_n)\}^{h^{-1}};\ (1)]$

$= [(g_1^{-1}g_1,g_2^{-1}g_2,\ldots,g_n^{-1}g_n)^{h^{-1}};\ (1)]$

$= [((1),(1),\ldots,(1))^{h^{-1}};\ (1)]$

$= [(1),(1),\ldots,(1);\ (1)] = I.$

Thus, $G \wr H$ is a group. This is Theorem 1 of Chapter II.

Theorem 2. The order of the wreath product of G by H is $|G|^n\ |H|$, where $n = |B|$.

Since there are $|G|^n$ possible choices of n-tuples of G* and $|H|$ possible choices of $h \in H$, $|G \wr H| = |G|^n|H|$.

$G \wr H$ is a group of permutations on A x B. It follows then that $G \wr H$ is a subgroup of the symmetric group on A x B, S_{mn}. It is shown in section (d), Chapter IV that for $m > 1$, $n > 1$, $S_m \wr S_n$ is a proper subgroup of S_{mn}.

The following example of a wreath product helps to understand the nature of the concept. Let A = {1,2,3,4}; B = {1,2,3}; G = {(1),(12)} a permutation group of order two on the set A; and H = {(1), (123), (132)} a group of order three on B. Since $|A| = 4$, $|B| = 3$, $|A \times B| = 12$. $|G| = 2$ and $|H| = 3$ means $|G \wr H| = 2^3 \cdot 3 = 24$. $G \wr H$ consists of 24 elements of S_{12}, which altogether contains 12! permutations.

The ordered pairs of A x B are expressed as letters.

a = (1,1)	g = (3,1)
b = (1,2)	h = (3,2)
c = (1,3)	i = (3,3)
d = (2,1)	j = (4,1)
e = (2,2)	k = (4,2)
f = (2,3)	l = (4,3)

The elements (permutations) of $G \wr H$ are

θ_1 = [(1),(1),(1);(1)]	θ_{13} = [(1),(12),(12);(123)]
θ_2 = [(1),(1),(12);(1)]	θ_{14} = [(12),(1),(12);(123)]
θ_3 = [(1),(12),(1);(1)]	θ_{15} = [(12),(12),(1);(123)]
θ_4 = [(12),(1),(1);(1)]	θ_{16} = [(12),(12),(12);(123)]
θ_5 = [(1),(12),(12);(1)]	θ_{17} = [(1),(1),(1);(132)]
θ_6 = [(12),(1),(12);(1)]	θ_{18} = [(1),(1),(12);(132)]
θ_7 = [(12),(12),(1);(1)]	θ_{19} = [(1),(12),(1);(132)]
θ_8 = [(12),(12),(12);(1)]	θ_{20} = [(12),(1),(1);(132)]
θ_9 = [(1),(1),(1);(123)]	θ_{21} = [(1),(12),(12);(132)]
θ_{10} = [(1),(1),(12);(123)]	θ_{22} = [(12),(1),(12);(132)]
θ_{11} = [(1),(12),(1);(123)]	θ_{23} = [(12),(12),(1);(132)]
θ_{12} = [(12),(1),(1);(123)]	θ_{24} = [(12),(12),(12);(132)]

In Table 1 which follows, the g_i and h components of each θ are arranged in column. Beneath these components in the same column, are the ordered pairs to which each θ maps a,b,c,...,l. Following this table is an explanation concerning how it is constructed.

Table 1

	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7	θ_8
g_1	(1)	(1)	(1)	(12)	(1)	(12)	(12)	(12)
g_2	(1)	(1)	(12)	(1)	(12)	(1)	(12)	(12)
g_3	(1)	(12)	(1)	(1)	(12)	(12)	(1)	(12)
h	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)
a	(1,1)	(1,1)	(1,1)	(2,1)	(1,1)	(2,1)	(2,1)	(2,1)
b	(1,2)	(1,2)	(2,2)	(1,2)	(2,2)	(1,2)	(2,2)	(2,2)
c	(1,3)	(2,3)	(1,3)	(1,3)	(2,3)	(2,3)	(1,3)	(2,3)
d	(2,1)	(2,1)	(2,1)	(1,1)	(2,1)	(1,1)	(1,1)	(1,1)
e	(2,2)	(2,2)	(1,2)	(2,2)	(1,2)	(2,2)	(1,2)	(1,2)
f	(2,3)	(1,3)	(2,3)	(2,3)	(1,3)	(1,3)	(2,3)	(1,3)
g	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)
h	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)
i	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)
j	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)
k	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)
l	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)

Table 1, continued

	θ_9	θ_{10}	θ_{11}	θ_{12}	θ_{13}	θ_{14}	θ_{15}	θ_{16}
g_1	(1)	(1)	(1)	(12)	(1)	(12)	(12)	(12)
g_2	(1)	(1)	(12)	(1)	(12)	(1)	(12)	(12)
g_3	(1)	(12)	(1)	(1)	(12)	(12)	(1)	(12)
h	(123)	(123)	(123)	(123)	(123)	(123)	(123)	(123)
a	(1,2)	(1,2)	(1,2)	(2,2)	(1,2)	(2,2)	(2,2)	(2,2)
b	(1,3)	(1,3)	(2,3)	(1,3)	(2,3)	(1,3)	(2,3)	(2,3)
c	(1,1)	(2,1)	(1,1)	(1,1)	(2,1)	(2,1)	(1,1)	(2,1)
d	(2,2)	(2,2)	(2,2)	(1,2)	(2,2)	(1,2)	(1,2)	(1,2)
e	(2,3)	(2,3)	(1,3)	(2,3)	(1,3)	(2,3)	(1,3)	(1,3)
f	(2,1)	(1,1)	(2,1)	(2,1)	(1,1)	(1,1)	(2,1)	(1,1)
g	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)
h	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)
i	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)
j	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)
k	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
l	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)

Table 1, continued

	θ_{17}	θ_{18}	θ_{19}	θ_{20}	θ_{21}	θ_{22}	θ_{23}	θ_{24}
g_1	(1)	(1)	(1)	(12)	(1)	(12)	(12)	(12)
g_2	(1)	(1)	(12)	(1)	(12)	(1)	(12)	(12)
g_3	(1)	(12)	(1)	(1)	(12)	(12)	(1)	(12)
h	(132)	(132)	(132)	(132)	(132)	(132)	(132)	(132)
a	(1,3)	(1,3)	(1,3)	(2,3)	(1,3)	(2,3)	(2,3)	(2,3)
b	(1,1)	(1,1)	(2,1)	(1,1)	(2,1)	(1,1)	(2,1)	(2,1)
c	(1,2)	(2,2)	(1,2)	(1,2)	(2,2)	(2,2)	(1,2)	(2,2)
d	(2,3)	(2,3)	(2,3)	(1,3)	(2,3)	(1,3)	(1,3)	(1,3)
e	(2,1)	(2,1)	(1,1)	(2,1)	(1,1)	(2,1)	(1,1)	(1,1)
f	(2,2)	(1,2)	(2,2)	(2,2)	(1,2)	(1,2)	(2,2)	(1,2)
g	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)	(3,3)
h	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)	(3,1)
i	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)	(3,2)
j	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)
k	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)	(4,1)
l	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)	(4,2)

Understanding Table 1 may be facilitated by looking at several examples.

Example 1: $a^{\theta_4} = (1,1)^{[(12),(1),(1);(1)]}$

$= (1^{\phi(1)[(12),(1),(1)]}, 1^{(1)}) = (1^{(12)}, 1^{(1)}) = (2,1)$

The first component of a, 1, is mapped to 2 because the g_1-component of θ_4 is (12).

Example 2: $b^{\theta_5} = (1,2)^{[(1),(12),(12);(1)]}$

$= (1^{\phi(2)[(1),(12),(12)]}, 2^{(1)}) = (1^{(12)}, 2^{(1)}) = (2,2).$

The first component of b, 1, is mapped to 2 because the g_2-component of θ_5 is (12).

Example 3: $f^{\theta_{13}} = (2,3)^{[(1),(12),(12);(123)]}$

$= (2^{\phi(3)[(1),(12),(12)]}, 3^{(123)}) = (2^{(12)}, 3^{(123)})$

$= (1,1).$

The first component of f, 2, is mapped to 1 by the g_3- component of θ_{13}.

Example 4: $d^{\theta_{14}} = (2,1)^{[(12),(1),(12);(123)]}$

$= (2^{\phi(1)[(12),(1),(12)]}, 1^{(123)}) = (2^{(12)}, 1^{(123)})$

$= (1,2).$

The first component of d, 2, is acted upon by the g_1-component of θ_{14}.

The twenty-four elements of G≀H may be expressed as permutations of the set containing a,b,c,...,.l.

θ_1	$= I$	θ_{13}	$= (abf)(cde)(ghi)(jkl)$
θ_2	$= (cf)$	θ_{14}	$= (aef)(bcd)(ghi)(jkl)$
θ_3	$= (be)$	θ_{15}	$= (aec)(bfd)(ghi)(jkl)$
θ_4	$= (ad)$	θ_{16}	$= (aecdbf)(ghi)(jkl)$
θ_5	$= (be)(cf)$	θ_{17}	$= (acb)(dfe)(gih)(jlk)$
θ_6	$= (ad)(cf)$	θ_{18}	$= (acedfb)(gih)(jlk)$
θ_7	$= (ad)(be)$	θ_{19}	$= (acbdfe)(gih)(jlk)$
θ_8	$= (ad)(be)(cf)$	θ_{20}	$= (afedcb)(gih)(jlk)$
θ_9	$= (abc)(def)(ghi)(jkl)$	θ_{21}	$= (ace)(bdg)(gih)(jlk)$
θ_{10}	$= (abcdef)(ghi)(jkl)$	θ_{22}	$= (afb)(ced)(gih)(jlk)$
θ_{11}	$= (abfdec)(ghi)(jkl)$	θ_{23}	$= (afe)(bdc)(gih)(jlk)$
θ_{12}	$= (aefdbc)(ghi)(jkl)$	θ_{24}	$= (afbdce)(gih)(jlk)$

The elements $\theta_1,\theta_2,\ldots,\theta_8$ are every distinct product of the cycles (ad),(be),and (cf). These eight elements form a group since each one is its own inverse and θ_1 is the identity. The h-component of each of these is (1), so $\{\theta_1,\theta_2,\ldots,\theta_8\}$ is similar to the G* defined on page 7. Refer to $\{\theta_1,\theta_2,\ldots,\theta_8\}$ as G*.

$\{\theta_9,\theta_{10},\ldots,\theta_{16}\}$ is not closed under the operation (composition of mappings). Since the h-component of each of these elements is (123), it is seen that $\theta_9 G^* = G^*\theta_9 = \{\theta_9,\theta_{10},\ldots,\theta_{16}\}$.

Similarly, $\{\theta_{17},\theta_{18},\ldots,\theta_{24}\}$ is not closed under the operation. Since each h-component is $(132) = (123)^{-1}$, this set consists of inverses of $\theta_9 G^*$. Also $\theta_{17}G^* = G^*\theta_{17} = \{\theta_{17},\theta_{18},\ldots,\theta_{24}\}$.

Table 2 which follows is the multiplication (or composition of mappings) table for $G \wr H$ as defined in this example. It was computed from the cyclic forms of $\theta_i \in G \wr H$. For brevity, only the subscripts of the θ_i are listed. Using this table as reference, one can demonstrate how products of elements of $G \wr H$ may be computed without reference to ordered pairs of A x B.

Table 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	1	5	6	3	4	8	7	10	9	13	14	11	12	16	15	18	17	21	22	19	20	24	23
3	5	1	7	2	8	4	6	11	13	9	15	10	16	13	14	19	21	17	23	18	24	20	22
4	6	7	1	8	2	3	5	12	14	15	9	16	10	11	13	20	22	23	17	24	18	19	21
5	3	2	8	1	7	6	4	13	11	10	16	9	15	14	12	21	19	18	24	17	23	22	20
6	4	8	2	7	1	5	3	14	12	16	10	15	9	13	11	22	20	24	18	23	17	21	19
7	8	4	3	6	5	1	2	15	16	12	11	14	13	9	10	23	24	20	19	22	21	17	18
8	7	6	5	4	3	2	1	16	15	14	13	12	11	10	9	24	23	22	21	20	19	18	17
9	11	12	10	15	13	14	16	17	19	20	18	23	21	22	24	1	3	4	2	7	5	6	8
10	13	14	9	16	11	12	15	18	21	22	17	24	19	20	23	2	5	6	1	8	3	4	7
11	9	15	13	12	10	16	14	19	17	23	21	20	18	24	22	3	1	7	5	4	2	8	6
12	15	9	14	11	16	10	13	20	23	17	22	19	24	18	21	4	7	1	6	3	8	2	5
13	10	16	11	14	9	15	12	21	18	24	19	22	17	23	20	5	2	8	3	6	1	7	4
14	16	10	12	13	15	9	11	22	24	18	20	21	23	17	19	6	8	2	4	5	7	1	3
15	12	11	16	9	14	13	10	23	20	19	24	17	22	21	18	7	4	3	8	1	6	5	2
16	14	13	15	10	12	11	9	24	22	21	23	18	20	19	17	8	6	5	7	2	4	3	1
17	20	18	19	22	23	21	24	1	4	2	3	6	7	5	8	9	12	10	11	14	15	13	16
18	22	17	21	20	24	19	23	2	6	1	5	4	8	3	7	10	14	9	13	12	16	11	15
19	23	21	17	24	20	18	22	3	7	5	1	8	4	2	6	11	15	13	9	16	12	10	14
20	17	22	23	18	19	24	21	4	1	6	7	2	3	8	5	12	9	14	15	10	11	16	13
21	24	19	18	23	22	17	20	5	8	3	2	7	6	1	4	13	16	11	10	15	14	9	12
22	18	20	24	17	21	23	19	6	2	4	8	1	5	7	3	14	10	12	16	9	13	15	11
23	19	24	20	21	17	22	18	7	3	8	4	5	1	6	2	15	11	16	12	13	9	14	10
24	21	23	22	19	18	20	17	8	5	7	6	3	2	4	1	16	13	15	14	11	10	12	9

In the demonstration of closure of G≀H on page 8, it is seen that in $\theta_i\theta_j$, the h-component of θ_i permutes the g-components of θ_j. For the example given here,

$$(g_1,g_2,g_3)^h = (g_{1^h},g_{2^h},g_{3^h}).$$

In particular, $(g_1,g_2,g_3)^{(123)}$

$$= (g_{1(123)},g_{2(123)},g_{3(123)})$$

$$= (g_2,g_3,g_1)$$

Similarly, $(g_1,g_2,g_3)^{(132)} = (g_3,g_1,g_2)$

The following two examples demonstrate the computation of $\theta_i\theta_j$ without reference to ordered pairs of A x B.

Example 1: $\theta_9\theta_{15} = [(1),(1),(1);(123)][(12),(12),(1);(123)]$

$$= [((1),(1),(1))((12),(12),(1))^{(123)};(123)(123)]$$

$$= [((1),(1),(1))((12),(1),(12));(132)]$$

$$= [(12),(1),(12);(132)] = \theta_{22}.$$

Inspection of the multiplication table reveals the same result, $\theta_9\theta_{15} = \theta_{22}$.

Example 2: $\theta_{14}\theta_{21} = [(12),(1),(12);(123)][(1),(12),(12);(132)]$

$$= [((12),(1),(12))((1),(12),(12))^{(123)};(123)(132)]$$

$$= [((12),(1),(12))((12),(12),(1));(1)]$$

$$= [(1),(12),(12);(1)] = \theta_5$$

The multiplication table shows $\theta_{14}\theta_{21} = \theta_5$.

Chapter III: The Importance of Wreath Products

The concept of the wreath product facilitates construction of Sylow p-subgroups of the symmetric group S_n. It is shown in section 3 of Chapter 4 that for some prime p, if P_r is a Sylow p-subgroup of S_{p^r}, P_{r+1}, a Sylow p-subgroup of $S_{p^{r+1}}$, has the same structure as $P_r \wr \langle c \rangle$, where c is a cycle of order p in $S_{p^{r+1}}$. A Sylow p-subgroup of S_n consists of the direct product of groups of this form.

Chapter IV: Theorems Connected with the Wreath Product

Section 1: The structure of a wreath product is given in this chapter by presenting four theorems. Theorem 1 demonstrates that the permutations $\theta \in G \wr H$ for which $h = (1)$ form a group isomorphic to G^* as defined on page 7, and Theorem 2 shows this group to be a normal subgroup. Theorem 3 demonstrates $(G \wr H)/\{\theta : \theta \in G \wr H,\ h = (1)\}$ isomorphic to H. Theorem 4 establishes that $\{\theta : \theta \in G \wr H$ and $g_i = (1)$ for all $i\}$ is isomorphic to H.

Theorem 1: $\{\theta : \theta \in G \wr H,\ h = (1)\} \approx G^*$

Let f be a mapping from $\{\theta : \theta \in G \wr H,\ h = (1)\}$ to G^* such that for $\theta = [g_1, g_2, \ldots, g_n; (1)]$. $\theta^f = (g_1, g_2, \ldots, g_n)$.

If $\theta_1 = [p_1, p_1, \ldots, p_n; (1)]$ and $\theta_2 = [r_1, r_2, \ldots, r_n; (1)]$,

$$
\begin{aligned}
(\theta_1\theta_2)^f &= [p_1 r_{1(1)}, p_2 r_{2(1)}, \ldots, p_n r_{n(1)}; (1)]^f \\
&= [p_1 r_1, p_2 r_2, \ldots, p_n r_n; (1)]^f \\
&= (p_1 r_1, p_2 r_2, \ldots, p_n r_n) \\
&= (p_1, p_2, \ldots, p_n)(r_1, r_2, \ldots, r_n) \\
&= \theta_1^f \theta_2^f
\end{aligned}
$$

Since f is a one-to-one correspondence which preserves operations it is an isomorphism. Thus $\{\theta : \theta \in G \wr H,\ h = (1)\}$ is a subgroup of $G \wr H$ and is isomorphic to G^*, the direct product of n copies of G. Henceforth, $\{\theta : \theta \in G \wr H,\ h = (1)\}$ is referred to as G^*.

Theorem 2: G^* is a normal subgroup of $G \wr H$.

Let f be a mapping from $G \wr H$ to H such that for $\theta = [g_1, g_2, \ldots, g_n; h]$ an element of $G \wr H$, $\theta^f = h$. Then for $\theta_1 = [g_1, g_2, \ldots, g_n; h]$ and $\theta_2 = [p_1, p_2, \ldots, p_n; k]$.

$$\begin{aligned}(\theta_1 \theta_2)^f &= [g_1 p_1 h, g_2 p_2 h, \ldots, g_n p_n h; hk]^f \\ &= hk \\ &= \theta_1{}^f \theta_2{}^f\end{aligned}$$

So f is a homomorphism onto H. The elements of G^* are mapped to the identity element of H by f, so G^* is the kernel of f. By the first Theorem on Homomorphisms, G^* is a normal subgroup of $G \wr H$.

Theorem 3: $(G \wr H)/G^* \simeq H$.

Application of the Third Theorem on Homomorphism establishes this.

Theorem 4: $K = \{\theta \mid \theta \in G \wr H \text{ and } \theta = [(1),(1),\ldots,(1);h]\}$ is isomorphic to H.

Clearly $|K| = |H|$. If $\theta = [(1),(1),\ldots,(1);h]$ and $\theta^f = h$, then $(\theta_i \theta_j)^f = h_i h_j = \theta_i{}^f \theta_j{}^f$. Since f is one-to-one and onto and since f preserves the operations, $K \simeq H$.

Consider the example given in Chapter One.

$A = \{1,2,3,4\}$, $B = \{1,2,3\}$

$a = \langle (12) \rangle$, $H = \langle (123) \rangle$

It is seen that $G^* \simeq G \times G \times G$

Also G^* is a normal subgroup of $G \wr H$, since for $p \in G \wr H$, $\theta \in G^*$, the h-component of $p^{-1}\theta p$ is $h_p^{-1}h_p = (1)$.

In this case, $(G \wr H)/G^* \cong \{G^*, \theta_9 G^*, \theta_{17} G^*\}$. The isomorphism involved is

$(G^*)^f = (1)$

$(\theta_9 G^*)^f = (123)$

$(\theta_{17} G^*)^f = (132)$

$K = \{\theta_1, \theta_9, \theta_{17}\}$ $\quad$ $(\theta_1)^f = (1)$

$(\theta_9)^f = (123)$

$(\theta_{17})^f = (132)$

Section 2: Associativity of the Wreath Product

If the process of forming the wreath product is considered to be a binary operation, it is associative. If K is a permutation group on a set C, then $(G \wr H) \wr K \simeq G \wr (H \wr K)$. If $(A \times B) \times C$ and $A \times (B \times C)$ are equated with $A \times B \times C$, the two wreath products are identical.

Theorem 1: The operation of forming wreath products is associative.

If G, H, and K are permutation groups on sets A, B, and C respectively with $|A| = m$, $|B| = n$, $|C| = p$, then $(G \wr H) \wr K \simeq G \wr (H \wr K)$.

first $|(G \wr H) \wr K| = |G \wr (H \wr K)|$

$|(G \wr H)\ K| = |G \wr H|^p |K| = (|G|^n |H|)^p |K| = |G|^{np} |H|^p |K|$.

$|G \wr (H \wr K)| = |G|^{np} |H \wr K|$ since $|B \times C| = np$;

and $|G|^{np} |H \wr K| = |G|^{np} |H|^p |K|$ since $|H \wr K| = |H|^p |K|$

Thus $|(G \wr H) \wr K| = |G \wr (H \wr K)|$

Since the orders of the two wreath products are the same, a one-to-one onto mapping from one to the other that is an isomorphism completes the proof.

If $\phi \in (G \wr H) \wr K$, then ϕ is of the form $[(g_1, g_2, \ldots, g_n; h_1), (g_{n+1}, \ldots, g_{2n}; h_2), \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p); k]$

Let f be a mapping from $(G \wr H) \wr K$ into $G \wr (H \wr K)$ such that for $\phi \in (G \wr H) \wr K$,

$$\phi^f = [(g_1, g_2, \ldots, g_n; h_1), (g_{n+1}, \ldots, g_{2n}; h_2), \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p); k]^f = [g_1, g_2, \ldots, g_{pn}; (h_1, h_2, \ldots, h_p; k)] \in G \wr (H \wr K)$$

Clearly f is a one-to-one onto mapping. Also it is the desired isomorphism. If $\phi = [(g_1, g_2, \ldots, g_n; h_1), (g_{n+1}, \ldots, g_{2n}; h_2) \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p); k]$ and $\phi' = [(g'_1, g'_2, \ldots, g'_n; h'_1), (g'_{n+1}, \ldots, g'_{2n}; h'_2), \ldots, (g'_{(p-1)n+1}, \ldots, g'_{pn}; h'_p); k']$, consider $(\phi\phi')^f$. k acts upon the subscripts of the h'_i's.

So $(\phi\phi')^f = [(g_1, g_2, \ldots, g_n; h_1)(g'_{(1^k-1)n+1}, \ldots, g'_{(1^k-1)n+n}; h'_{1^k}), \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p)(g'_{(p^k-1)n+1}, \ldots, g_{(p^k-1)n+n}; h'_{p^k}); kk']^f$.

Each h_i may be considered to be acting only on the numbers 1, 2, ..., n,

So $(\phi\phi')^f = [(g_1 g'_{(1^k-1)n+1^h}, \ldots, g_n g'_{(1^k-1)n+n^{h_1}}; h_1 h'_{1^k}), \ldots, (g_{(p-1)n+1} g'_{(p^k-1)n+1^{h_p}}, \ldots, g_{pn} g'_{(p^k-1)n+n^{hp}}; h_p h'_{p^k}); kk']^f$

$(\phi\phi')^f = [g_1 g'_{(1^k-1)n+1^{h_1}}, g_2 g'_{(1^k-1)n+2^{h_1}}, \ldots, g_n g'_{(1^k-1)n+n^{h_1}}, \ldots,$

$g_{(p-1)n+1} g'_{(p^k-1)n+1^{hp}}, \ldots, g_{pn} g'_{(p^k-1)n+n^{hp}}; (h_1 h'_{1^k}, h_2 h'_{2^k}, \ldots,$

Since the orders of the two wreath products are the same, a one-to-one onto mapping from one to the other that is an isomorphism completes the proof.

If $\phi \in (G \wr H) \wr K$, then ϕ is of the form $[(g_1, g_2, \ldots, g_n; h_1), (g_{n+1}, \ldots, g_{2n}; h_2), \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p); k]$

Let f be a mapping from $(G \wr H) \wr K$ into $G \wr (H \wr K)$ such that for $\phi \in (G \wr H) \wr K$,

$$\phi^f = [(g_1, g_2, \ldots, g_n; h_1), (g_{n+1}, \ldots, g_{2n}; h_2), \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p); k]^f = [g_1, g_2, \ldots, g_{pn}; (h_1, h_2, \ldots, h_p; k)] \in G \wr (H \wr K)$$

Clearly f is a one-to-one onto mapping. Also it is the desired isomorphism. If $\phi = [(g_1, g_2, \ldots, g_n; h_1), (g_{n+1}, \ldots, g_{2n}; h_2) \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p); k]$ and $\phi' = [(g'_1, g'_2, \ldots, g'_n; h'_1), (g'_{n+1}, \ldots, g'_{2n}; h'_2), \ldots, (g'_{(p-1)n+1}, \ldots, g'_{pn}; h'_p); k']$, consider $(\phi\phi')^f$. k acts upon the subscripts of the h'_i's.

So $(\phi\phi')^f = [(g_1, g_2, \ldots, g_n; h_1)(g'_{(1^k-1)n+1}, \ldots, g'_{(1^k-1)n+n}; h'_{1^k}), \ldots, (g_{(p-1)n+1}, \ldots, g_{pn}; h_p)(g'_{(p^k-1)n+1}, \ldots, g_{(p^k-1)n+n}; h'_{p^k}); kk']^f$.

Each h_i may be considered to be acting only on the numbers 1, 2, ..., n,

So $(\phi\phi')^f = [(g_1 g'_{(1k-1)n+1}{}^{h}, \ldots, g_n g'_{(1^k-1)n+n}{}^{h_1}; h_1 h'_{1^k}), \ldots, (g_{(p-1)n+1} g'_{(p^k-1)n+1}{}^{h_p}, \ldots, g_{pn} g'_{(p^k-1)n+n}{}^{hp}; h_p h'_{p^k}); kk']^f$

$(\phi\phi')^f = [g_1 g'_{(1^k-1)n+1}{}^{h_1}, g_2 g'_{(1^k-1)n+2}{}^{h_1}, \ldots, g_n g'_{(1^k-1)n+n}{}^{h_1}, \ldots,$

$g_{(p-1)n+1} g'_{(p^k-1)n+1}{}^{hp}, \ldots, g_{pn} g'_{(p^k-1)n+n}{}^{hp}; (h_1 h'_{1^k}, h_2 h'_{2^k}, \ldots,$

$h_p h'_p{}^k; kk')] = [g_1 g'_{(1^k-1)n+1^{h_1}}, \ldots, g_{pn} g'_{(p^k-1)n+n^{h_p}}; (h_1, h_2, \ldots,$

$h_p; k)(h'_1, h'_2, \ldots, h'_p; k')]$.

If we allow $(i^k - 1)n + j^{h_i} = (j^{h_i}, i^k)$, then $(\phi\phi')^f =$
$[g_1 g'_{(1^{h_1}, 1^k)}, g_2 g'_{(2^{h_1}, 1^k)}, \ldots, g_n g'_{(n^{h_1}, 1^k)}, \ldots, g_{(p-1)n+1} g'_{(1^{h_p}, p^k)},$
$\ldots, g_{pn} g'_{(n^{h_p}, p^k)}; (h_1, h_2, \ldots, h_p; k)(h'_1, h'_2, \ldots, h'_p; k')] = [(g_1, g_2, \ldots,$
$g_{pn})(g'_{(1,1)}, g'_{(2,1)}, \ldots, g'_{(n,p)})^{(h_1, h_2, \ldots, h_p; k)}; (h_1, h_2, \ldots h_p; k)$
$(h'_1, h'_2, \ldots, h'_p; k')] = [g_1, g_2, \ldots, g_{pn}; (h_1, h_2, \ldots, h_p; k)]$
$[g'_{(1,1)}, g'_{(2,1)}, \ldots, g'_{(n,p)}; (h'_1, h'_2, \ldots, h'_p; k')] = [g_1, g_2, \ldots, g_{pn};$
$(h_1, h_2, \ldots, h_p; k)][g'_1, g'_2, \ldots, g'_{np}; (h'_1, h'_2, \ldots, h'_p; k')] = \phi^f (\phi')^f$.

Thus f preserves the operation and is an isomorphism.

Theorem 2: If $(A \times B) \times C = A \times (B \times C) = A \times B \times C$, then $(G \wr H) \wr K$ is identical with $G \wr (H \wr K)$.

To demonstrate this, it suffices to show that for $\phi \in (G \wr H) \wr K$ as defined in Theorem 1, and isomorphism f as defined in Theorem 1, $\phi = \phi^f$

$$((a,b),c)^\phi = ((a,b)^{(g_{(c-1)n+1}, \ldots, g_n; h_c)}; c^k)$$
$$= ((a^{g_{(c-1)n+b}}, b^{h_c}), c^k)$$
$$= (a^{g_{(c-1)n+b}}, (b^{h_c}, c^k))$$
$$= (a^{g_{(c-1)n+b}}, (b,c)^{(h_1, h_2, \ldots, h_p; k)})$$

Let $(c-1)n + b = (b,c)$.

Then $((a,b),c)^{\phi} = (a^{g(b,c)},(b,c)^{(h_1,h_2,\ldots,h_p;k)})$
$= (a,(b,c))^{\phi^f}$

Section 3: Construction of Sylow p-subgroups of S_n

Here is perhaps the most outstanding aspect of wreath products, the construction of Sylow p-subgroups of S_n. The computation of the order of Sylow p-subgroups and the construction thereof with wreath products is demonstrated in this section with an example.

(1.) Computation of the order of a Sylow p-subgroup of S_n.

The order of S_n is $n!$. If $|S| = n! = p^m s$ for some prime p such that $(p,s) = 1$, the Sylow p-subgroups have order p^m by a corollary of the First Sylow Theorem. When n is expressed in base p, $n = a_0p^k + a_1p^{k-1} + \ldots + a_{k-1}p + a_k$ where $0 < a_i < p - 1$, and $M = [\frac{n}{p}] + [\frac{n}{p^2}] + \ldots + [\frac{n}{p^k}]$.

To show this, consider $[\frac{n}{p}]$. $[\frac{n}{p}]$ is the number of factors of $n! = n(n-1)(n-2)\ldots3\cdot2\cdot1$ which contain at least the first power of p; that is, p, 2p, 3p,...,kp, where $k = [\frac{n}{p}]$.

$[\frac{n}{p^2}]$ is the number of factors of $n!$ which contain p^2 as a factor. Hence p appears as a factor of $n!$ at least this many more times. Similar remarks hold for $[\frac{n}{p^3}],\ldots,[\frac{n}{p^k}]$.

$[\frac{n}{p^i}] = 0$ for $i > k + 1$, since $p^{k+1} > n$.

Since $[\frac{n}{p^i}] = [\frac{a_0p^k+a_1p^{k-1}+\ldots+a_{k-1}p+a_k}{p^i}]$

$$= \frac{a_0p^k + a_1p^{k-1} +\ldots+ a_{k-i}p^i}{p^i}$$

$$= a_0p^{k-1} + a_1p^{k-2} +\ldots+ a_{k-1} \quad \text{for } 1 < i < k,$$

$$M = [\frac{n}{p}] + [\frac{n}{p2}] +\ldots+ [\frac{n}{p^k}]$$

$$= (a_0p^{k-1} + a_1p^{k-2} +\ldots+ a_{k-2}p + a_{k-1})$$

$$+ (a_0p^{k-2} + a_1p^{k-3} +\ldots+ a_{k-2}) +\ldots+ (a_0+ a_1) + a_0.$$

Factoring out the coefficient a_i's yields $M = a_0(p^{k-1} + p^{k-2} + \ldots+ p + 1) + a_1(p^{k-2} +\ldots+ p + 1) +\ldots+ a_{k-2}(p + 1) + a_{k-1}$.

(2.) Construction of Sylow p-subgroups

The information developed above show that a Sylow p-subgroup of S_{p^r} has order p^{N_r}, where $N_r = [\frac{p^r}{p}] + [\frac{p^r}{p^2}] +\ldots+ [\frac{p^r}{p^r}] = p^{r-1} + p^{r-2} +\ldots+ p + 1$. Constructing Sylow p-subgroups for S_p, $S_{p^2},\ldots,$ S_{p^k} easily generalizes to constructing a Sylow p-subgroup for S_n. Writing $n = a_0p^k + a_1p^{k-1} +\ldots+ a_{k-1}p + a_k$, partition the n letters into a_0 sets of p^k letters, a_1 sets of p^{k-1} letters,..., a_{k-1} sets of p letters and a_k sets of single letters. When the appropriate Sylow p-subgroups in each set are constructed, then the direct product of these is a group P of order p^m and is a Sylow p-subgroup of S_n.

The wreath product may be used in this construction of Sylow p-subgroups of S_n. For some prime p, a Sylow p-subgroup of S_p, the symmetric group on 1, 2, ..., p, is of order p, since $p^{N_1} = p^{p^{1-1}} = p^{p^0} = p^1 = p$. Therefore this Sylow p-subgroup is cyclic and may be generated by the cycle (123...p). In any event, this Sylow p-subgroup is isomorphic to <(123...p)>. S_{p^2} on 1, 2, ..., p^2 has a subgroup which is the direct product of the cyclic groups generated by $a_1 = (12...p)$, $a_2 = (p+1,\dots, 2p),\dots, a_p = ((p-1)p+1,\dots, p^2)$. This direct product has order p^p. This direct product is not a Sylow p-subgroup of S_{p^2}, since a Sylow p-subgroup of S_{p^2} has order p^{p+1}. Consider the element $b = [1,p+1,2p+1,\dots,(p-1)p+1][2,p+2,\dots,(p-1)p+2]\dots[p,2p,\dots,p\ ]$ of order p.

$b^{-1}a_ib = a_{i+1}$, where the subscripts are taken modulo p.

Consider $a_i = [(i-1)p+1,(i-1)p+2,\dots,ip]$, $b^{-1} = [(p-1)p+1,(p-2)p+1,\dots,p+1,p][(p-1)p+2,\dots,p+2,2]\dots[p^2,p^2-p,\dots,2p,p]$,

so
$$\begin{aligned} b^{-1}a_ib = \{&[p^2- p + 1, p^2 - 2p + 1,\dots, p + 1, 1]\\ &[p^2 - p + 2, p^2 - 2p + 2,\dots, p + 1, 2]\\ &\dots[p^2, p^2 - p,\dots, 2p, p]\}\\ &\{[(i - 1)p + 1, (i - 1)p + 2,\dots, ip]\}\\ &\{[1,p + 1,2p + 1,\dots,p^2 - p + 1]\\ &[2,p + 2,\dots,p^2 - p + 2]\\ &\dots[p,2p,\dots,p^2]\} \end{aligned}$$

b^{-1} takes $ip + 1$ to $(i - 1)p + 1$, then a_i maps $(i - 1)p + 1$ to $(i - 1)p + 2$. But b takes $(i - 1)p + 2$ to $ip + 2$. So $b^{-1}a_ib$

maps $ip + 1$ to $ip + 2$. A similar argument holds for $ip + 2$ being mapped to $ip + 3$, and so on. If b^{-1} maps an element to one which is fixed by a, b immediately reverses this action. Hence $b^{-1}a_ib = [ip + 1, ip + 2, \ldots, (i + 1)p] = a_{i+1}$.

Also $(b^{-1}a_ib)^2 = a^2{}_{i+1}$ or $b^{-1}a_ibb^{-1}a_ib = a^2{}_{i+1}$ or $b^{-1}a^2{}_ib = a^2{}_{i+1}$.

This generalizes to $b^{-1}a^n{}_ib = a^n{}_{i+1}$ by induction.

From the results above, it is seen that from $b^{-1}a_ib = a_{i+1}$ one may derive $a_i = ba_{i+1}b^{-1}$.

$ba_ib^{-1} = b^2a_{i+1}b^{-2} = a_{i-1}$

Again by induction, $b^ma_ib^{-m} = a_{i-m}$. Combining these results, it is discovered that

$b^ma^n{}_ib^{-m} = a^n{}_{i-m}$ for all natural numbers m and n. This information is necessary to show that $b^ma^n{}_i$ is of an order which is a power of p for all natural numbers m and n. Consider $(b^ma^n{}_i)^p = b^ma^n{}_ib^ma^n \ldots b^ma^n{}_i$

$$= (b^ma^n{}_ib^{-m})b^mb^ma^n{}_i \ldots b^ma^n{}_i$$

$$= a^n{}_{i-m}(b^{2m}a^n{}_ib^{-2m})b^{2m}b^ma^n{}_i \ldots b^ma^n{}_i$$

$$= a^n{}_{i-m}a^n{}_{i-2m}(b^{3m}a^n{}_ib^{-3m})b^{3m}b^ma^n{}_i \ldots b^ma^n{}_i$$

$$= a^n{}_{i-m}a^n{}_{i-2m}a^n{}_{i-3m} \cdots a^n{}_{i-(p-1)m}b^{(p-1)m}b^ma^n{}_i$$

$$= a^n{}_{i-m}a^n{}_{i-2m} \cdots a^n{}_{i-(p-1)m}a^n{}_i$$

If $(p,n) = 1$, this element is of order p, so long as (p,m) also equals 1. If p divides m, this element is the identity, being $(a^n{}_i)^p = a^{np}{}_i = (1)$.

If $(p,n) = 1$ and $(p,m) = 1$, $(b^m a^n{}_i)^p$ is of order p, hence $b^m a^n{}_i$ is of order p^2. So $b^m a^n{}_i$ is an element of a p-group. Since $a^n{}_i b^m = b^m a^n_{i+m}$, $a^n{}_i b^m$ is also an element of a p-group.

The p-group generated by b and a_i's cannot have order greater than p^{p+1}, since p^{p+1} is the order of a Sylow p-subgroup of S_{p^2}. It cannot have order less than p^{p+1} since $|\langle a_1\rangle x \langle a_2\rangle x \ldots x \langle a_p\rangle| = p^p$. No a_i generates a_j for $j \neq i$, nor will any a_i generate b. Similar b will not generate any a_i. So this group is a Sylow p-subgroup of S_{p^2}. This subgroup may be generated by a, and b.

This Sylow p-subgroup is the wreath product of $\langle a_1\rangle$ and the group generated by the first cycle of b. The set associated with $\langle a_1\rangle$ is $A = \{1,2,\ldots,p\}$ and the set associated with the first cycle of b is $B = \{1,p+1,2p+1,\ldots,(p-1)p+1\}$. The elements of $A \times B$ are $(j,ip+1)$ for $j = 1,2,\ldots,p$; $i = 0,1\ldots,p-1$. Call the first cycle of b by the letter c, then $|\langle a_1\rangle \wr \langle c\rangle| = |\langle a_1\rangle|^{|B|}|\langle c\rangle| = p^p p = p^{p+1}$.

If $(j,ip+1)$ is identified with $ip+j$, $\langle a_1\rangle \wr \langle c\rangle$ is a subgroup of S_{p^2}. Since $|\langle a_1\rangle \wr \langle c\rangle| = p^{p+1}$, it is a Sylow p-subgroup of S_{p^2}. Sylow p-subgroups are conjugate, hence they are isomorphic. So $\langle a_1,b\rangle$ may be equated with $\langle a_1\rangle \wr \langle c\rangle$.

Let P_r be a Sylow p-subgroup of S_{p^r} on $1,2,\ldots,p^r$. The letters $1,\ldots,p^r,p^{r+1},\ldots,2p^r,\ldots,p^{r+1}$ are those permuted by elements of

$S_{p^{r+1}}$. Let $c = [1,p^{r+1},2p^r+1,\ldots,(p-1)p^r + 1][2,p^r+2,2p^r+2,\ldots,(p-1)p^r+2]\ldots[j,p^r+j,2p^r+j,\ldots,(p-1)p^r+j]\ldots[p^r,2p^r,\ldots,p^{r+1}]$.

Then let $P_r^{(i)} = c^{-i}P_rc^i$. Since $P_r^{(i)}$ is a conjugate of P_r in $S_{p^{r+1}}$, it is a group of order p^{N_r}. Moreover, it is a permutation group of the letters $ip^r + 1,\ldots,(i+1)p^r$. To see this, consider p, an element of P_r. p is a permutation on $1,\ldots,p^r$. c^{-1} maps $p^r + j$ to j for $1 \leq j \leq p^r$. p takes j to k for $1 \leq k \leq p^r$ and c maps k to $p^r + k$. So $c^{-1}pc$ permutes the elements $p^r + m$ for $1 \leq m \leq p^r$. Similarly, c^{-2} maps $2p^r + j$ to j, and c^2 takes k to $2p^r + k$, so $c^{-2}pc^2$ permutes the elements $2p^r + m$. In general, $c^{-i}pc^i$ permutes elements $ip^r + m$ for $m = 1,\ldots,p^r; i = 0,\ldots,p - 1$.

Since each $P_r^{(i)}$ displaces a distinct set of letters, the group they generate is their direct product.

$$\left| P_r X P_r^{(1)} X \ldots X P_r^{(p-1)} \right| = (p^{N_r})^p = p^{pN_r}.$$

Since no $p \in P_r$ generates c and c generates no element of P_r, the group generated by c and P_r is of order p^{pN_r+1}. But $pN_r + 1$

$$\begin{aligned}
&= p(p^{r-1} + p^{r-2}+\ldots+ p + 1) + 1 \\
&= (p^r + p^{r-1} +\ldots+ p^2 + p) + 1 \\
&= p^{(r+1)-1} + p^{(r+1)-2} +\ldots+ p^2 + p + 1 \\
&= N_{r+1}
\end{aligned}$$

So c and P_r generate P_{r+1}, a Sylow p-subgroup of $S_{p^{r+1}}$.

Now consider P_r acting on letters $1,\ldots,p^r$, and d a cycle of order p, $d = (u_0u_1\ldots u_{p-1})$. The wreath product $P_r \wr \langle d\rangle$ permutes symbols (i,u_j) for $i = 1,\ldots,p^r$; $j = 0,\ldots,p-1$.

$$|P_r \wr \langle d\rangle| = |P_r|^p |\langle d\rangle| = |P_r|^p \cdot p$$

$$= [p^{(p^{r-1}+p^{r-2}+\ldots+p+1)}]^p \cdot p$$

$$= p^{p(p^{r-1}+p^{r-2}+\ldots+p+1)} \cdot p^1$$

$$= p^{p^r+p^{r-1}+\ldots+p^2+p+1}$$

$$= p^{N_{r+1}}$$

So $P_r \wr \langle d\rangle$ is a Sylow p-subgroup of $S_{p^{r+1}}$. If (i,u_j) is identified with $i + jp^r$, then, within isomorphism, P_{r+1} as defined above and $P_r \wr \langle d\rangle$ are the same.

To illustrate the preceding discussion, a Sylow 3-subgroup of S_{13} is constructed. $13 = 1\cdot 3^2 + 1\cdot 3 + 1$. So the thirteen letters are partitioned into one set of nine letters, one set of three letters, and one set of one letter. A Sylow 3-subgroup of S_{13} is $\mathcal{S} = P_2 \times P_1 \times I$ where P_r (for r = 1,2) is a Sylow 3-subgroup of S_{3^r}.

Let $P = \langle(123)\rangle$,

and $P_2 = \langle(123),(147)(258)(369)\rangle$.

$P_2 \simeq P_1 \wr \langle 147\rangle$.

Investigate the construction of P_2.

Allow $a = (123)$ and $b = (147)(258)(369)$.

So $b^{-1}a_1b = [(174)(285)(396)](123)[(147)(258)(369)]$

$= (456)$. Let $a_2 = (456)$.

$b^{-1}a_2b = [(174)(285)(396)](456)[(147)(258)(369)] = (789)$

Let $(789) = a_3$

$b^{-1}a_3b = [(174)(285)(396)](789)[(147)(258)(369)] = (123) = a_1$

Each of the a_i displaces a distinct set of letters, so the group they generate is their product. Now $|\langle a_1\rangle \times \langle a_2\rangle \times \langle a_3\rangle| = 3^3$. Since b is of order 3, the group generated by P_1 and b must have order at least 3^{3+1}. Since $b \in S_{32}$ and $P_1 \subsetneq S_{32}$, the order of the group generated by P_1 and b cannot be of order greater than 3^{3+1}. Hence P_1 and b generate P_2, a Sylow 3-subgroup of S_{32}.

Consider $P_1 \wr \langle(147)\rangle$. Since P_1 permutes 3 elements and $\langle(147)\rangle$ permutes 3 elements, $p_1 \wr \langle(147)\rangle$ permutes 9 elements. So $P_1 \wr \langle(147)\rangle \subsetneq S_{32}$.

Here it is necessary to allow $1 = u_0$, $4 = u_1$, $7 = u_2$ so that (147) may be called $c = (u_0 u_1 u_2)$. Then $P \wr \langle c\rangle$ permutes symbols (i,u_j) for $i = 1,2,3$; $j = 0,1,2$.

$|P_1 \wr \langle c\rangle| = 3^3 \cdot 3 = 3^{3+1}$, the order of a Sylow 3-subgroup of S_{32}. If (i,u_j) is identified with $i + 3j$, $P_1 \wr \langle c\rangle$ is the same as P_2 within isomorphism, since Sylow subgroups are conjugate by the Second Sylow Theorem.

If P_2 is allowed to permute the letters $1,2,\ldots,9$; P_1 to permute 10,11,12; and the identity group to map 13 to itself then

$$\mathcal{S} = \langle(123),(147)(258)(369)\rangle \times \langle(10,11,12)\rangle \times I$$
$$= (P_1 \wr \langle(147)\rangle) \times P_1 \times I.$$
$$|\mathcal{S}| = |P_2|\cdot|P_1|\cdot|I| = 3^{3+1}\cdot 3 = 3^5 = 243.$$

Note that $5 = 1(3^{2-1}+1)+1$. If $a_0 = 1$, $a_1 = 1$, $a_2 = 1$, and $p = 3$, then $13 = a_0p^2 + a_1p + a_2$.

$13! = p^m s$, $M = a\ (p^{2-1}+1) + a_1$

It should be noted that any Sylow 3-subgroup of S_{13} is isomorphic to any Sylow 3-subgroup of either S_{12} or S_{14}.

$P_2 \times P_1 \approx P_2 \times P_1 \times I \approx P_2 \times P_1 \times I \times I.$

In general, for $n = a_0 p^r + a_1 p^{r-1} + \ldots + a_{r-1}p + a_r$, where $0 \leq a_i \leq p-1$, a Sylow p-subgroup $\mathcal{S}$ in S_n is

$$\mathcal{S} = \underbrace{(P_r \times P_r \times \ldots \times P_r)}_{a_0 \text{ times}} \times \underbrace{(P_{r-1} \times P_{r-1} \times \ldots \times P_{r-1})}_{a_1 \text{ times}} \times \ldots$$

$$\times \underbrace{(P_1 \times P_1 \times \ldots \times P_1)}_{a_{r-1} \text{ times}} \times \underbrace{(I \times I \times \ldots \times I)}_{a_r \text{ times}}$$

If $\mathcal{S}_0$ is designated the Sylow p-subgroup of S_n when $a_r = 0$, $\mathcal{S}_1$ the Sylow p-subgroup of S_n when $a_r = 1$, and so on up to $\mathcal{S}_{p-1}$ for $a_r = p-1$, it is seen that

$$\mathcal{S}_0 \approx \mathcal{S}_1 \approx \mathcal{S}_2 \approx \ldots \approx \mathcal{S}_{p-1}.$$

The complete construction of a Sylow 3-subgroup of S_9 is helpful in computing the number of Sylow 3-subgroups of S_{13} that actually exist. It happens that there are over three million distinct Sylow 3-subgroups of S_{13}. To establish this, proceed as follows:

Since $\mathcal{S} = P_2 \times P_1 \times I$, the number of Sylow 3-subgroups of S_9 and of S_3 must be taken into account. The Third Sylow Theorem dictates that the number in each case must be of the form $1 + 3k$. For S_9, 1 + 3k must divide 9! The same may be said for S_3, 1 + 3j must divide 3! Matters are simplified for S_3. The cyclic subgroup of order 3 is the only Sylow 3-subgroup of S_3.

The elements of a Sylow 3-subgroup of S_9 are found to be cycles of order 3, products of disjoint cycles of order 3, and cycles of order 9. Cycles such as (123) and (145) cannot belong to the same Sylow 3-subgroup, since (123)(145) = (12345), a cycle of order 5. Nor can (123) and (124) belong to the same Sylow 3-subgroup, since (123)(124) = (14)(23), an element of order 2. No two single 3-cycles of a Sylow 3-subgroup can permute the same letters of 1,2,...,9 .

It is known that a Sylow 3-subgroup of S_9 is generated by a 3-cycle and a permutation of three disjoint 3-cycles. Choice of either of these is restricted by choice of the other. There are $\binom{9}{3} = \frac{9\cdot 8\cdot 7}{3\cdot 2}$ = 84 distinct 3-cycles and their inverses. Since the other generator, a properly selected triple, transmutes a 3-cycle into two conjugate disjoint 3-cycles, divide 84 by 3 to obtain 28. For instance, consider the 28 3-cycles involving 1, none of which is an inverse of any of the others;

(123), (124), (125), (126), (127), (128), (129),

(134), (135), (136), (137), (138), (139),

(145), (146), (147), (148), (149),

(156), (157), (158), (159),

(167), (168), (169),

(178), (179),

(189).

Once a 3-cycle has been chosen as generator, selection of the other generator, a triple of disjoint 3-cycles, is restricted. Each of the 3-cycles of the triple must permute exactly one of the elements of the given 3-cycle, since otherwise permutations having orders other than powers of 3 are obtained. Consider (123) and (147)(235)(689); (123)(147)(235)(689) = (1347)(25)(689) which is of order 12.

With this restriction, there are $\binom{6}{2}$ ways of selecting the letters of the first factor of the triple, and 2 distinct ways of ordering these letters. For the second factor there are $\binom{4}{2}$ ways of selecting the letters and 2 distinct ways of ordering them. There remains $\binom{2}{2}$ or one way to select the letters for the third factor, and two ways of ordering them. Altogether there are

$$\binom{6}{2}\binom{4}{2}2^3 = \frac{6\cdot 5}{2} \cdot \frac{4\cdot 3}{2} \cdot 2^3 = 6\cdot 5\cdot 4\cdot 3\cdot 2$$

$= 6!$ possible triples of disjoint 3-cycles.

Note that (6!)(28) does not yield a number of the form $1 + 3k$. A Sylow 3-subgroup of S_9 must contain several triples of the proper form. The example which is constructed below shows that any Sylow 3-subgroup of S_9 contains 18 such triples.

Let the letters a,b,c...,i be the nine elements permuted by members of S_9. Select α_1 = (abc), β = (adi)(bch)(cfg); then

$$\beta^{-1}\alpha_1\beta = (\text{def}) = \alpha_2$$

$$\beta^{-1}\alpha_2\beta = (\text{ihg}) = \alpha_3$$

$$\beta^{-1}\alpha_3\beta = (\text{abc}) = \alpha_1$$

A Sylow 3-subgroup of S_9 contains 81 elements. The subgroup $<\alpha_1, \alpha_2, \alpha_3>$ accounts for twenty-seven of these elements, which are all products $\alpha_1{}^m\alpha_2{}^n\alpha_3{}^r$ where m = 0,1,2; n = 0,1,2; and r = 0,1,2.

Other than β and β^{-1}, there remain 52 elements yet to be inspected. Thirty-six of them are 9-cycles. The other sixteen are the desired triples of 3-cycles.

Consider $\alpha_1\beta$, $\alpha_2\beta$, $\alpha_3\beta$, $\alpha_1{}^{-1}\beta$, $\alpha_2{}^{-1}\beta$ and $\alpha_3{}^{-1}\beta$. Each of these generates six 9-cycles distinct from those generated by the other five. Table 3 lists these products on pages 37-38.

It is not necessary to consider $\beta\alpha_1$, $\beta\alpha_2$, and so forth. $\beta^{-1}\alpha_1\beta = \alpha_2$ means $\alpha_1\beta=\beta\alpha_2$. Similarly, $\alpha_2\beta = \beta\alpha_3$ and $\alpha_3\beta = \beta\alpha_1$.

So far, sixty-five of the 81 elements have been given. Sixteen remain to be found. These are triples of 3-cycles in which the three letters of α_1 are apportioned one to each factor. There can be no more than 18 such elements, β and β^{-1} included, in a Sylow 3-subgroup of S , since there are 63 elements which are not of this form. There are exactly 18 elements of this form. The following nine elements are distinct triples of the appropriate form, none of which are inverses of one another:

β	$\alpha_1\alpha_2\alpha_3\beta^{-1}$
$\alpha_1\alpha_2\alpha_3\beta$	$\alpha_1\alpha_3\beta^{-1}\alpha_2$
$\alpha_1\alpha_2\beta\alpha_3$	$\alpha_1\beta^{-1}\alpha_2\alpha_3$
$\alpha_1\beta\alpha_2\alpha_3$	$\alpha_2\beta^{-1}\alpha_1\alpha_3$
$\alpha_1\alpha_3\beta\alpha_2$	

Table 3

$(\alpha_1\beta) = (abc)(adi)(beh)(cfg) = (aehbfgcdi)$

$(\alpha_1\beta)^2 = (ahfciebgd)$

$(\alpha_1\beta)^3 = (abc)(def)(ihg) = \alpha_1\alpha_2\alpha_3$

$(\alpha_1\beta)^4 = (afibdhceg)$

$(\alpha_1\beta)^5 = (agechdbif)$

$(\alpha_1\beta)^6 = (acb)(dfe)(igh) = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$

$(\alpha_1\beta)^7 = (adgbeicfh)$

$(\alpha_1\beta)^8 = (aidcgfbhe)$

$(\alpha_1\beta)^9 = (a)$, the identity

$(\alpha_2\beta) = (def)(adi)(beh)(cfg) = (adhbegcfi)$

$(\alpha_2\beta)^2 = (ahecidbgf)$

$(\alpha_2\beta)^3 = (abc)(def)(ihg) = \alpha_1\alpha_2\alpha_3$

$(\alpha_2\beta)^4 = (aeibfhcdg)$

$(\alpha_2\beta)^5 = (agdchfbie)$

$(\alpha_2\beta)^6 = (acb)(dfe)(igh) = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$

$(\alpha_2\beta)^7 = (afgbdiceh)$

$(\alpha_2\beta)^8 = (aifcgebhd)$

$(\alpha_2\beta)^9 = (a)$

$(\alpha_3\beta) = (ihg)(adi)(beh)(cfg) = (adibehcfg)$

$(\alpha_3\beta)^2 = (aiecgdbhf)$

$(\alpha_3\beta)^3 = (abc)(def)(ihg) = \alpha_1\alpha_2\alpha_3$

$(\alpha_3\beta)^4 = (aegbficdh)$

$(\alpha_3\beta)^5 = (ahdcifbge)$

$(\alpha_3\beta)^6 = (acb)(dfe)(igh) = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$

$(\alpha_3\beta)^7 = (afhbdgcei)$

$(\alpha_3\beta)^8 = (agfchebid)$

$(\alpha_3\beta)^9 = (a)$

$(\alpha_1^{-1}\beta) = (acb)(adi)(beh)(cfg) = (afgcehbdi)$

$(\alpha_1^{-1}\beta)^2 = (agebifchd)$

$(\alpha_1^{-1}\beta)^3 = (acb)(dfe)(igh) = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$

$(\alpha_1^{-1}\beta)^4 = (aeicdgbfh)$

$(\alpha_1^{-1}\beta)^5 = (ahfbgdcie)$

$(\alpha_1^{-1}\beta)^6 = (abc)(def)(ihg) = \alpha_1\alpha_2\alpha_3$

$(\alpha_1^{-1}\beta)^7 = (adhcfibeg)$

$(\alpha_1^{-1}\beta)^8 = (aidbhecgf)$

$(\alpha_1^{-1}\beta)^9 = (a)$

$(\alpha_2^{-1}\beta) = (dfe)(adi)(beh)(cfg) = (adgcfhbei)$

$(\alpha_2^{-1}\beta)^2 = (agfbidche)$

$(\alpha_2^{-1}\beta)^3 = (acb)(dfe)(igh) = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$

$(\alpha_2^{-1}\beta)^4 = (aficegbdh)$

$(\alpha_2^{-1}\beta)^5 = (ahdbgecif)$

$(\alpha_2^{-1}\beta)^6 = (abc)(def)(ihg) = \alpha_1\alpha_2\alpha_3$

$(\alpha_2^{-1}\beta)^7 = (aehcdibfg)$

$(\alpha_2^{-1}\beta)^8 = (aiebhfcgd)$

$(\alpha_2^{-1}\beta)^9 = (a)$

$(\alpha_3^{-1}\beta) = (igh)(adi)(beh)(cfg) = (adicfgbeh)$

$(\alpha_3^{-1}\beta)^2 = (aifbhdcge)$

$(\alpha_3^{-1}\beta)^3 = (acb)(dfe)(igh) = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$

$(\alpha_3^{-1}\beta)^4 = (afhceibdg)$

$(\alpha_3^{-1}\beta)^5 = (agdbiechf)$

$(\alpha_3^{-1}\beta)^6 = (abc)(def)(ihg) = \alpha_1\alpha_2\alpha_3$

$(\alpha_3^{-1}\beta)^7 = (aegcdhbfi)$

$(\alpha_3^{-1}\beta)^8 = (ahebgfcid)$

$(\alpha_3^{-1}\beta)^9 = (a)$

These nine elements and their inverses are the eighteen desired triples. Any one of these may be considered to be the second generator, the triple of disjoint 3-cycles of this particular Sylow 3-subgroup. For instance, if $\alpha_1\alpha_2\alpha_3\beta = \gamma$, then $\beta = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}\gamma$. Recall that there are 6! = 720 ways of selecting an appropriate triple. Since each Sylow 3-subgroup of S_9 contains 18 of these, there are 720/18 = 40 ways of selecting a distinct Sylow 3-subgroup once the single 3-cycle generator is chosen. Recall that there are 28 such 3-cycles to choose as generators. Altogether there are $28 \cdot 40 = 1120$ Sylow 3-subgroups of S_9.

The criteria of the Third Sylow Theorem are satisfied. 1120 = 1 + 1119 = 1 +3(373). $1120 = 2^5 \cdot 5 \cdot 7$ divides $9! = 2^7 \cdot 3^4 \cdot 5 \cdot 7$.

With this information one can calculate the number of Sylow 3-subgroups of S_{13}. There are $\binom{13}{9}\binom{4}{3}$ ways of selecting the letters permuted by S_{13} to construct a Sylow 3-subgroup,

$$\mathcal{S} = P_2 \times P_1 \times I.$$

$$\binom{13}{9}\binom{4}{3} = \frac{13 \cdot 12 \cdot 11 \cdot 10}{4 \cdot 3 \cdot 2} \cdot 4 = 2860 = 1 + 2859 = 1 + (953)3.$$

Note that both 1120 and 2860 are of the form 1 + 3k. Hence their product is of the same form.

$$(1120)(2860) = 3{,}203{,}200 = 1 + 3{,}203{,}199 = 1 + 3(1{,}067{,}733).$$

$3{,}203{,}200 = 2^7 5^2 \cdot 7 \cdot 11 \cdot 13$ divides $13! = 2^{10} 3^5 5^2 \cdot 7 \cdot 11 \cdot 13$. So the criteria of the Third Sylow Theorem are satisfied. The number of Sylow 3-subgroups of S_{13} is 3,203,200.

It is not too difficult to compute the number of Sylow 3-subgroups of S_{12} and S_{14}. There are $\binom{12}{9}$ ways of selecting letters to construct a Sylow 3-subgroup of S_{12}.

$$\binom{12}{9} = \frac{12\cdot 11\cdot 10}{3\cdot 2} = 220.$$

(1120)(220) = 246,000, the number of Sylow 3-subgroups of S_{12}.

For S_{14}, there are $\binom{14}{9}\binom{5}{3} = \dfrac{14\cdot 13\cdot 12\cdot 11\cdot 10}{5\cdot 4\cdot 3\cdot 2} \cdot \dfrac{5\cdot 4}{2} = 20{,}020$ ways to select the letters.

(1120)(22020) = 22,422,400, the number of Sylow 3-subgroups of S_{14}.

When considering the number of Sylow 3-subgroups of S_{15}, some difficulty is encountered.

$$\binom{15}{9}\binom{6}{3} = 100100 = 2 + 100098 = 2 + 3(33{,}366).$$

Multiplying 100100 by 1120 yields another number of the form $2 + 3k$, an undesirable result in light of the Third Sylow Theorem. The problem is solved when the fact that $P_2 \times (P_1 \times P_1)$ and $(P_2 \times P_1) \times P_1$ are isomorphic but not identical is taken into account. Doubling 100,100 yields 200,200.

(200,200)(1120) = 224,224,000 = 1 + 224,223,999 = 1 + 3(74,741,333).

224,224,000 = $2^8 5^3 7^2 \cdot 11 \cdot 13$ divides 15! = $2^{11} 3^6 5^3 7^2 \cdot 11 \cdot 13$. So the number of Sylow 3-subgroups of S_{15} is 224,224,000.

Section 4: Theorem--For $m > 1$, $n > 1$, $S_m \wr S_n$ is a proper subgroup of S_{mn}.

If $M = \{1,2,\ldots,m\}$ and $N = \{1,2,\ldots,n\}$ $|M \times N| = mn$, so it is easily seen that $S_m \wr S_n \subsetneq S_{mn}$. If either $m = 1$ or $n = 1$, then $S_m \wr S_n = S_{mn}$.

$m = 1$ implies $|S_m \wr S_n| = (m!)^n n! = n! = (mn)! = |S_{mn}|$.

$n = 1$ implies $|S_m \wr S_n| = (m!)^n n! = m! = (mn)! = |S_{mn}|$.

It is understood that m and n are natural numbers. Induction is used to show that when both m and n are greater than 1, $S_m \wr S_n$ is a proper subgroup of S_{mn}. Consider $m = n = 2$. $|S_m \wr S_n| = (2!)^2 2! < (2\cdot2)! = |S_{mn}|$ since $(2!)^2\cdot 2! = 2^2\cdot 2 = 8$ and $(2\cdot 2)! = 4! = 24$.

Assume for some $k \in N$, the natural numbers, that $(k!)^2\cdot 2! < (2k)!$.

$[(k+1)!]^2\cdot 2! = (k+1)^2(k!)^2\cdot 2!$ while $[2(k+1)]! = [(2k+2)(2k+1)][(2k)!]$.

$(k+1)^2 < (2k+2)(2k+1)$ for all $k \in N$, so $[(k+1)!]^2\cdot 2! < [2(k+1)]!$.

Therefore for all $m > 1$, $m \in N$, $(m!)^2\cdot 2! < (2m)!$.

Assume for some $j \in N$ that $(m!)^j\cdot j! < (mj)!$

$(m!)^{(j+1)}(j+1)! = (m!)(j+1)(m!)^j j!$ and $[(j+1)m]! = [(j+1)m][(j+1)m-1]\ldots[(j+1)m-(m-1)][(jm)!]$.

It happens that

$(m!)(j+1) < [(j+1)m][(j+1)m-1]\ldots[(j+1)m-(m-1)]$

or $(m!)(j+1) < [(j+1)m][(j+1)m-1]\ldots[jm+1]$

So $(m!)^{j+1}(j+1)! < [(j+1)m]!$

Therefore for all $m > 1$, $n > 1$,

$(m!)^n n! < (mn)!$

$|S_m \wr S_n| < |S_{mn}|$

$S_m \wr S_n$ is a proper subgroup of S_{mn}.

Chapter V: Wreath Products of Small Orders

Section 1: Possible Orders of Wreath Products

Theorem: Since $|G \wr H| = |G|^{|B|}|H|$ where B is the set of elements permuted by H, $|H|$ must divide $|B|!$

H is a permutation group on B, so H is a subgroup of $S_{|B|}$. By LaGrange's Theorem, $|H|$ must divide $|S_{|B|}|$. $|S_{|B|}| = |B|!$

Since this chapter concerns wreath products of small orders, the concept of "small" must be defined. Here it is considered to be less than or equal to 100.

S_n has a cycle c of order n, so $<c> \wr <(1)>$ has order n when $(1) \in S_1$. This case is trivial. $G \wr H$ is nontrivial if both $|G| > 1$ and $|H| > 1$.

If $|G| = 2$ and $|B| = 2$, then $|H| = 2$. $|G \wr H| = 2^2 \cdot 2 = 8$. This is the smallest possible order for a non-trivial wreath product.

For $|G| = 2$ and $|B| = 3$, $|H|$ may be 2,3 or 6.

$2^3 \cdot 6 = 48$

$2^3 \cdot 3 = 24$

$2^3 \cdot 2 = 16$

If $|G| = 2$ and $|B| = 4$, $|H|$ can have value 2,3,4,6,8,12 or 24.

$2^4 \cdot 2 = 32$	$2^4 \cdot 6 = 96$
$2^4 \cdot 3 = 48$	$2^4 \cdot 8 = 128 > 100$
$2^4 \cdot 4 = 64$	

When $|G| = 2$ and $|B| = 5$, the possibilities for $|H|$ are 2,3,4,5,6, 8,10,12,15,20,24,30,60, and 120.

$$2^5 \cdot 2 = 64$$

$$2^5 \cdot 3 = 96$$

$$2^5 \cdot 4 = 128 > 100$$

$|G| = 2$ and $|B| = 6$ means the smallest value for $|H|$ is 2. $2^6 \cdot 2 = 128 > 100$.

If $|G| = 3$, $|B| = 2$ means $|H| = 2$ and $|G \wr H| = 3^2 \cdot 2 = 18$.

When $|G| = 3$ and $|B| = 3$, the possibilities for $|G \wr H|$ are $3^3 \cdot 2$, $3^3 \cdot 3$, and $3^3 \cdot 6$.

$$3^3 \cdot 2 = 54 \qquad\qquad 3^3 \cdot 6 = 162 > 100$$

$$3^3 \cdot 3 = 81$$

$|G| = 3$ and $|B| = 4$ means the lowest value of $|G \wr H|$ is $3^4 \cdot 2 = 162 > 100$.

$|G| = 4$ and $|B| = 2$ yields $|G \wr H| = 4^2 \cdot 2 = 32$.

$|G| = 4$ and $|B| = 3$ means $|G \wr H| > 4^3 \cdot 2 = 128 > 100$.

$|G| = 5$ and $|B| = 2$ yields $|G \wr H| = 5^2 \cdot 2 = 50$.

$|G| = 6$, $|B| = 2$ implies $|G \wr H| = 6^2 \cdot 2 = 72$.

$|G| = 7$, $|B| = 2$ means $|G \wr H| = 7^2 \cdot 2 = 98$.

The possible orders less than or equal to 100 are 8,16,18,24,32, 48,50,54,64,72,81,96, and 98.

Section 2: Isomorphisms between Wreath Products

In this section, three theorems and a corollary are presented to establish the conditions in which two wreath products are isomorphic. It follows from these theorems that wreath products of some particular orders are always isomorphic. A counter example is given to show that two wreath products of order 32 are not necessarily isomorphic.

Before Theorem 1 can be presented, it must be understood that the exponential notation for mappings behaves the same way as the functional notation; that is, $(g_1,g_2,\ldots,g_n)^{hk}$ is equivalent to $(hk)[(g_1,g_2,\ldots,g_n)] = h(k[(g_1,g_2,\ldots,g_n)])$. An example is presented to demonstrate this.

Let $G = S_2$ and $H = S_3$, then $G \wr H = S_2 \wr S_3$. Consider $[(1),(12),(12);(123)]$ and $[(12),(1),(12);(13)]$. The product of these is

$$\begin{aligned}
&[(1),(12),(12);(123)][(12),(1),(12);(13)] \\
&= [((1),(12),(12))((12),(1),(12))^{(123)};(123)(13)] \\
&= [(1)(1),(12)(12),(12)(12);(12)] \\
&= [(1),(1),(1);(12)]
\end{aligned}$$

If $h = (123)$ and $k = (13)$, $hk = (123)(13) = (12)$.

Notice how (12) acts on (g_1,g_2,g_3).

$(12)[(g_1,g_2,g_3)] = (g_2,g_1,g_3)$.

$(123)(13)[(g_1,g_2,g_3)] = (123)[(g_3,g_2,g_1)] = (g_2,g_1,g_3)$.

However, if ordinary mapping notation is used $[(g_1,g_2,g_3)](hk) = \{[(g_1,g_2,g_3)]h\}k = \{[(g_1,g_2,g_3)](123)\}(13) = [(g_2,g_3,g_1)](13) = (g_1,g_3,g_2)$, which is not the same element of $G \times G \times G$ unless $g_1 = g_2 = g_3$. In general $(g_2, g_1, g_3) \neq (g_1, g_3, g_2)$.

Theorem 1: If $G \simeq G'$, where G and G' are permutation groups over some sets A and A', $|A|$ not necessarily equal to $|A'|$, and $H' = a^{-1}Ha$ where $|B| = |B'|$ and $a \in S_{|B|}$, then $G \wr H \simeq G' \wr H'$.

Clearly, $G \simeq G'$ means $|G| = |G'|$, and $H' = a^{-1}Ha$ yields $|H| = |H'|$. So $|G \wr H| = |G|^{|B|}|H| = |G'|^{|B'|}|H'| = |G' \wr H'|$. A one-to-one onto mapping between the two wreath products can be designed.

Let ϕ_1 be an isomorphism between G and G'. ϕ_2 is an isomorphism between $G \times G \times \ldots \times G$ and $G' \times G' \times \ldots \times G'$ if $(g_1, g_2, \ldots, g_n)^{\phi_2} = (g_1{}^{\phi_1}, g_2{}^{\phi_1}, \ldots, g_n{}^{\phi_1})$ for $n = |B| = |B'|$.

Designate the elements of $G \times G \times \ldots \times G$ as v_i. So elements of $G' \times G' \times \ldots \times G'$ are $v_i{}^{\phi_2}$.

Then allow ϕ_3 to be a mapping from $G \wr H$ to $G' \wr H'$ defined by $[v_i; h_i]^{\phi_3} = [(a^{-1}\phi_2)(v_1); a^{-1}ha]$.

ϕ_3 is an isomorphism. That it is one-to-one and onto follows from the facts that a^{-1} and ϕ_2 are one-to-one and onto. That it preserves operations is demonstrated as follows:

$$\begin{aligned}
&[v_1; h_1]^{\phi_3}[v_2; h_2]^{\phi_3} \\
&= [(a^{-1}\phi_2)(v_1); a^{-1}h_1a][(a^{-1}\phi_2)(v_2); a^{-1}h_2a] \\
&= \{[(a^{-1}\phi_2)(v_1)][(a^{-1}\phi_2)(v_2)]^{a^{-1}h_1a}; a^{-1}h_1aa^{-1}h_2a\} \\
&= \{[(a^{-1}\phi_2)(v_1)][(a^{-1}h_1a)(a^{-1}\phi_2)(v_2)]; a^{-1}h_1h_2a\} \\
&= \{[(a^{-1}\phi_2)(v_1)][(a^{-1}h_1\phi_2)(v_2)]; a^{-1}h_1h_2a\}.
\end{aligned}$$

Now $h_i\phi_2 = \phi_2 h_i$ for all $h_i \in H$ or $\phi_2 = h_i^{-1}\phi_2 h_i$. ϕ_2 merely renames the components of $(g_1, g_2, \ldots, g_n)$. In $(g_1, g_2, \ldots, g_n)^{h_i^{-1}\phi_2 h_i}$, h_i changes the order of the components, ϕ_2 renames them, and h_i^{-1} restores the original order.

So
$$\begin{aligned}[v_1;h_1]^{\phi_3}[v_2;h_2]^{\phi_3} &= \{[(a^{-1}\phi_2)(v_1)][(a^{-1}\phi_2 h_1)(v_2)];a^{-1}h_1h_2a\} \\ &= \{[(a^{-1}\phi_2)(v_1)][(a^{-1}\phi_2)(v_2^{h_1})];a^{-1}h_1h_2a\} \\ &= [(a^{-1}\phi_2)(v_1v_2^{h_1});a^{-1}h_1h_2a] \\ &= [v_1v_2^{h_1};h_1h_2]^{\phi_3} \\ &= \{[v_1;h_1][v_2;h_2]\}^{\phi_3}\end{aligned}$$

So $G \wr H \simeq G' \wr H'$

Corollary to Theorem 1: If $G \simeq G'$ and $H = H'$ for $|B| = |B'|$, then $G \wr H \simeq G' \wr H'$.

This follows immediately, since $H' = (1)^{-1}H(1)$.

Theorem 2: If $|G| = |G'| = p$ for some prime p and $H' = a^{-1}Ha$ for $|B| = |B'|$ and $a \in S_{|B|}$, then $G \wr H \simeq G' \wr H'$.

If $|G| = |G'| = p$ for some prime, G and G' must both be cyclic groups. Cyclic groups of the same order are isomorphic.

Theorem 3: $G \simeq G'$ and $|H| = |H'| = |B| = |B'| = 2$ or $|H| = |H'| = |B| = |B'| = 3$ yields $G \wr H \simeq G' \wr H'$.

This follows from the corollary to Theorem 1, since $H = H'$ in both cases. There is only one group of order 2 which permutes a set of two elements. Similarly, there is only one group of order 3 which permutes a set of three elements.

Theorems 2 and 3 permit the conclusion that two wreath products of order 8, 18, 24, 50, 81, or 98 are isomorphic, since each of these numbers is of the form $p^2 \cdot 2$ or $p^3 \cdot 3$ where p is a prime. This is the only way they can be written in the form $m^k n$ where n divides k!.

There remain seven other possible orders less than 100 for which isomorphisms might possibly be constructed. Looking at the circumstances in which these values occur, one finds that there are at least eleven distinct wreath products:

$16 = 2^3 \cdot 2$

$32 = 2^4 \cdot 2 = 4^2 \cdot 2$

$48 = 2^3 \cdot 6 = 2^4 \cdot 3$

$54 = 3^2 \cdot 2$

$64 = 2^4 \cdot 4 = 2^5 \cdot 2$

$72 = 6^2 \cdot 2$

$96 = 2^4 \cdot 6 = 2^5 \cdot 3$

Theorems 1 and 2 permit the conclusion that in cases where $|G \wr H| = |G' \wr H'| = 16$ or $|G \wr H| = |G' \wr H'| = 54$, then $G \wr H \simeq G' \wr H'$. In these cases $|G| = |G'| = p$ for $p = 2,3$, so $G \simeq G'$. There are three permutation groups of order 2 on a set of 3 elements, but they are conjugates of one another.

$<(12)> = (123)<(23)>(132) = (132)<(13)>(123)$.

In the event that $|G| = |G'| = 2$ and $|H| = |H'| = 6$ for $|B| = |B'| = 3$, then $G' \wr H' \simeq G \wr H$. This follows since $G \simeq G'$ and $H = H' = S_3$. $|G \wr H| = |G' \wr H'| = 48$.

If $|G| = |G'| = 2$ and $|H| = |H'| = 3$ for $|B| = |B'| = 4$, then $G \wr H \simeq G' \wr H'$. This conclusion is permitted since $G \simeq G'$ and the four permutation groups of order 3 on a set of four elements are conjugates of one another:

$$\begin{aligned} \langle(123)\rangle &= (14)\langle(234)\rangle(14) \\ &= (34)\langle(124)\rangle(34) \\ &= (24)\langle(134)\rangle(24). \end{aligned}$$

Again, $|G \wr H| = |G' \wr H'| = 48$.

If $|G \wr H| = |G' \wr H'| = 72$ and $G \simeq G'$, then $G \wr H \simeq G' \wr H'$.

In this case $|H| = |H'| = |B| = |B'| = 2$, so $H = H'$, by Theorem 3.

For two wreath products of the same order, it is always possible to devise a one-to-one onto correspondence between them. In the instances above, an isomorphism can always be constructed. But there are cases in which an isomorphism cannot exist between the two wreath products. An example involving wreath products of order 32 demonstrates this.

Let $G = \langle(12)\rangle$ for any set A and let $G' = G$. Let $H = \langle(12)\rangle$ for $|B| = 4$ and $H' = \langle(12)(34)\rangle$ for $|B'| = 4$.

$|G \wr H| = 2^4 \cdot 2 = 32 = |G' \wr H'|$.

Clearly $G \simeq G'$ amd $H \simeq H'$, since H and H' are of order 2. But there does not exist an isomorphism between $G \wr H$ and $G' \wr H'$. Table 4 lists the elements of each which do not involve the identity element of H or H'. There is no need to list those elements since $G^* \simeq G \times G$

x G x G ≃ G' x G' x G' x G' ≃ G'*. In Table 4, allow (12) to be represented by 1, and (1) to be represented by 0. Also let (12)(34) = ϕ.

Every element of either G* or G'* has order 2. Inspection of Table 4 reveals that G≀H has eight elements of order 4, while G'≀H' contains twelve such elements. Since isomorphisms preserve order, there can be no isomorphism between G≀H and G'≀H'.

This example illustrates that mere isomorphism between H and H' is not sufficient to guarantee isomorphism between G≀H and G'≀H'. In this case, $H' \neq a^{-1}Ha$ for any $a \in S_4$. (12) is an odd permutation; that is, it is the product of an odd number of transpositions, a transposition being a cycle of order 2. (12)(34) is an even permutation. A permutation is either even or odd, but not both. Hence $a^{-1}(12)a \neq (12)(34)$ for any $a \in S_4$.

There remain some unanswered questions about wreath products of orders 48, 64, 72, and 96. Concerning 64, it can be asserted that if H = <(12)> and H' = <(12)(34)> for $|B| = |B'| = 5$. $H' \neq a^{-1}Ha$, for any $a \in S_5$ for the same reasons as those given in the preceding paragraph. It is suspected that construction of a table similar to Table 4 would reveal the two wreath products involved do not contain the same number of elements of the same order. This is a topic for further study.

It is also suspected that construction of tables would reveal irreconcileable differences in the following instances:

Table 4: Elements of $G \wr H$

order	a	a^2	a^3	a^4
2	[00001]	[00000]		
4	[10001]	[11000]	[01001]	[00000]
4	[01001]	[11000]	[10001]	[00000]
2	[00101]	[00000]		
2	[00011]	[00000]		
2	[11001]	[00000]		
4	[01101]	[11000]	[10101]	[00000]
2	[00111]	[00000]		
4	[10101]	[11000]	[01101]	[00000]
4	[10011]	[11000]	[01011]	[00000]
4	[01011]	[11000]	[10011]	[00000]
2	[11101]	[00000]		
2	[11011]	[00000]		
4	[10111]	[11000]	[01111]	[00000]
4	[01111]	[11000]	[10111]	[00000]
2	[11111]	[00000]		

Table 4: Elements of $G' \wr H'$

order	a	a^2	a^3	a^4
2	[0000ϕ],	[00000]		
4	[1000ϕ]	[11000]	[0100ϕ]	[00000]
4	[0100ϕ]	[11000]	[1000ϕ]	[00000]
4	[0010ϕ]	[00110]	[0001ϕ]	[00000]
4	[0001ϕ]	[00110]	[0010ϕ]	[00000]
2	[1100ϕ]	[00000]		
4	[0110ϕ]	[11110]	[1001ϕ]	[00000]
2	[0011ϕ]	[00000]		
4	[1010ϕ]	[11110]	[0101ϕ]	[00000]
4	[1001ϕ]	[11110]	[0110ϕ]	[00000]
4	[0101ϕ]	[11110]	[1010ϕ]	[00000]
4	[1110ϕ]	[00110]	[1101ϕ]	[00000]
4	[1101ϕ]	[00110]	[1110ϕ]	[00000]
4	[1011ϕ]	[11000]	[0111ϕ]	[00000]
4	[0111ϕ]	[11000]	[1011ϕ]	[00000]
2	[1111ϕ]	[00000]		

$|G| = 2$, $|H| = 2$, $|B| = 4$, $|G'| = 4$, $|H'| = 2$, $|B'| = 2$;
$|G \wr H| = |G' \wr H'| = 32$.

$|G| = 2$, $|H| = 6$, $|B| = 3$, $|G'| = 2$, $|H'| = 3$, $|B'| = 4$;
$|G \wr H| = |G' \wr H'| = 48$.

$|G| = 2$, $|H| = 4$, $|B| = 4$, $|G'| = 2$, $|H'| = 2$, $|B'| = 5$;
$|G \wr H| = |G' \wr H'| = 64$.

$|G| = |G'| = 6$. $|H| = |H'| = |B| = |B'| = 2$ where $G = S_3$ and G' is a cyclic group of order 6. $|G \wr H| = |G' \wr H'| = 72$.

$|G| = |G'| = 2$, $|H| = 6$, $|B| = 4$; $|H'| = 3$, $|B'| = 5$;
$|G \wr H| = |G' \wr H'| = 96$.

Here it can be noted that for $|G| = |G'| = 2$, $|H| = |H'| = 3$ for $|B| = |B'| = 5$, then $|G \wr H| = |G' \wr H'| = 96$ and $G \wr H \simeq G' \wr H'$. There are ten permutation groups of order 3 on a set of five elements, but they are all conjugate, since they are the Sylow 3-subgroups of S_5.

Chapter VI: Some Further Results of the Study

Section 1: Theorem:

If G and H are p-groups for some prime p, then $G \wr H$ is a p-group.

Since G and H are p-groups, $|G| = p^m$ for some $m \in N$ and $|H| = p^n$ for some $n \in N$. If $|B| = k$, where B is the set of elements permuted by H, then $|G \wr H| = |G|^{|B|}|H| = (p^m)^k p^n = p^{km}p^n = p^{km+n}$.

So $G \wr H$ is a p-group, since the order of each of its elements must divide p^{km+n}.

This result should not be surprising, since the construction of Sylow p-subgroups of S_{p^r} involved the formation of wreath products of p-groups.

Section 2: Theorem:

For any prime p, $(p-2)! = 1 + kp$ for some $k \in N$.

For S_p there are p! orderings of the p elements. However as p-cycles there are only (p-1)! distinct elements of S_p since there are p ways of selecting the first entry of the p-cycle. Each p-cycle is of order p; hence it will generate p-1 distinct p-cycles and the identity. Each collection of these p-1 distinct p-cycles and the identity compose a group. So there are $\frac{(p-1)!}{p-1} = (p-2)!$ cyclic subgroups of order p of S_p. These are the Sylow p-subgroups of S_p. Since the number of Sylow p-subgroups of any group is of the form $1 + kp$ by the Third Sylow Theorem, $(p-2)! = 1 + kp$ for some $k \in N$.

Section 3: Theorem:

The operation of forming wreath products is not commutative. $G \wr H \neq H \wr G$ in general.

Consider the example given in Chapter II; $A = \{1,2,3,4\}$, $B = \{1,2,3\}$, $G = \langle(12)\rangle$ and $H = \langle(123)\rangle$.

$$|G \wr H| = |G|^{|B|}|H| = 2^3 \cdot 3 = 24$$

$$|H \wr G| = |H|^{|A|}|G| = 3^4 \cdot 2 = 162.$$

So $G \wr H$ an $H \wr G$, having different orders are not even isomorphic, let alone equal. Since 24 does not divide 162, $G \wr H \nleq H \wr G$ by LaGranges Theorem. However, $G \wr H \subsetneq S_{12}$ and $H \wr G \subsetneq S_{12}$.

Section 4: The set of finite permutation groups with the operation of wreath product is a semi-group.

A semigroup is a set upon which an associative binary operation is well-defined. In Chapter II it is seen that a wreath product is a permutation group. Associativity of the operation is demonstrated in Section 2 of Chapter IV.

Section 5: Any group G is isomorphic to a wreath product.

By Cayley's Theorem, $G \cong P$ where P is some permutation group of the elements of G. $P = P \wr S_1$.

Chapter VII: Conclusion

The basic intent of this paper was to present the wreath product in a form understandable to the person with only a basic knowledge of permutation groups and abstract algebra. The failing of many texts is that they are too concise. They give no examples, and their definitions depend upon too much esoteric information given beforehand. This thesis has attempted to define the wreath product as simply as possible. It has provided examples and proofs where none existed in the available literature, and fleshed out some proofs which were presented in the texts, Hall in particular. Special attention has been given to construction of Sylow p-subgroups of symmetric groups, this being one of the important applications of wreath products.

A great deal of time and space has been devoted to calculation of the number of Sylow 3-subgroups of S_{13}. The concept of the wreath product was not used here.

Some questions have been left unanswered about isomorphisms between wreath products of certain orders. However, a theorem which assisted greatly has been proven in that particular section.

A particularly exciting result of this study is the theorem presented in Section 2, Chapter VI, that for any prime p, $(p-2)! = 1 + kp$ for some natural number k. This is an application of group theory to problems in number theory.

Topics for further study might include development of a smooth algorithm for constructing a Sylow p-subgroup of S_n, element by element.

In the construction of a Sylow 3-subgroup of S_9 in Section 3, Chapter IV, trial-and-error was used. Also direct use of the concept of the wreath product in this matter might be developed.

Another topic for further study involves the unanswered questions about isomorphisms between wreath products of orders 32, 48, 64, 72, and 96. One might construct counter examples to demonstrate non-isomorphisms, or one might devise and prove theorems demonstrating existence or non-existence of isomorphisms.

The importance of wreath products rests partially on Sylow p-subgroups. The question now is, what good are Sylow p-subgroups. This is something for further study.

Nothing has been said in this paper about twisted wreath products or restricted wreath products. Nor was anything mentioned concerning the wreath product being a special type of semi-direct product. Again these are topics for further study.

If the reader goes away from this thesis with a better understanding of wreath products and a higher appreciation of permutation groups in general, this thesis accomplished part of its purpose. If the paper has engendered in the reader a desire to investigate further the wreath product and its applications, it has done still more.

BIBLIOGRAPHY

Hall, Marshall, Jr. The Theory of Groups. New York: the Macmillan Company, 1959.

Passman, Donald. Permutation Groups. New York: W.A. Benjamin, Inc., 1968.

Rotman, Joseph J. The Theory of Groups. Boston: Allyn and Bacon, Inc., 1973.

Scott, William R. Group Theory. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1968