INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

UMI[®]
800-521-0600

**MINIMAL DEGREE OF FAITHFUL PERMUTATION
REPRESENTATIONS OF FINITE GROUPS**

by

STEPHANE R. LEMIEUX

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of

Master of Science

School of Mathematics and Statistics

Carleton University
Ottawa, Ontario
May 7, 1999

© copyright
1999, Stephane R. Lemieux

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-48492-0

Canada

The undersigned recommended to
the Faculty of Graduate Studies and Research
acceptance of the thesis

**Minimal Degree of Faithful Permutation Representations
of Finite Groups**

submitted by Stephane R. Lemieux
in partial fulfilment of the requirements for
the degree of Master of Science

Thesis Supervisor

Director, School of Mathematics and Statistics

Carleton University
1999

ABSTRACT

The minimal degree of a faithful permutation representation of a finite group G is the least positive integer n such that G can be embedded in the symmetric group acting on n elements. It is useful in computational group theory to know the minimum degree of a faithful permutation representation of a finite group G and its factor groups. If the former is strictly less than one of the latter then G is said to be exceptional.

Chapter 1 of this thesis reviews methods for finding permutation representations and how to calculate the minimal degree for a group G . In Chapter 2, concrete examples of finite exceptional groups are given as well as methods for constructing exceptional groups. Chapter 3 enumerates various inherent properties of exceptional groups, with special focus on minimalistic characteristics. Chapter 4 is an esoteric analysis of the conjectures which surround minimal degrees and exceptional groups. Chapter 5 gives the main results of this thesis. The minimal degrees of all p -groups of order less than p^5 are calculated, and an attempt is made (Theorem 5.2) to classify all exceptional p -groups of order less than p^6 for odd prime p ; a conjecture as to their existence was raised by Easdown and Praeger [4]. A further note on the classification of p -groups of order p^5 , has been submitted to the Bulletin of the Australian Mathematical Society.

Acknowledgments:

I would like to thank first and foremost Dr. Brian Mortimer for his time, patience, understanding, and genius; any “progress, progress” that I made was by his guidance and encouragement. I would also like to thank Dr. John Poland and Dr. John Dixon for their time and advice.

TABLE OF CONTENTS

	<u>Page</u>
Introduction	1
Chapter 1 How to Find Permutation Representations and Their Minimal Degrees	3
Chapter 2 Examples of Exceptional Groups	9
Chapter 3 Properties of Exceptional Groups	13
Chapter 4 Conjectures	18
Chapter 5 Results	24
Bibliography	44

LIST OF TABLES

	<u>Page</u>
Table 1 Minimal Degrees of p-Groups of Order $< p^5$	25

NOTATION AND DEFINITIONS

S_k	Denotes symmetric group on k elements.
$\text{Cor}_G(H)$	Is the core of a subgroup H in a group G . It is defined to be the intersection of all conjugates of H in G , i.e. $\text{Cor}_G(H) = \bigcap_{g \in G} (g^{-1}Hg)$. It is also the unique largest subgroup of H which is normal in G .
$H * K$	denotes the central product of H and K .
G_B^B	Denotes the action of the set stabilizer G_B restricted to B , where B is a block of imprimitivity
Q_2^n	Denotes the Quaternion group of order 2^n
D_2^n	Denotes the dihedral group of order $(2^n)r$

INTRODUCTION

The minimal degree of a faithful permutation representation of a finite group G , (or simply the degree of G), is the least positive integer n such that G can be embedded in the symmetric group acting on n elements, and is denoted $\mu(G)$.

When designing computer algorithms to calculate various properties of a solvable group G , (such as determining conjugacy class representatives) it is often useful to exploit series such as

$1 = G_0 < G_1 < G_2 < \dots < G_n = G$ of normal subgroups with elementary abelian factors G_i/G_{i-1} . Such algorithms work by solving the appropriate problem successively in the quotients G/G_{n-1} , G/G_{n-2} , ..., $G/G_0 = G$, where at each stage, the solution in G/G_i is lifted through the elementary abelian layer G_i/G_{i-1} to find a solution in G/G_i .

To determine a minimal permutation representation for a subgroup G_i of G is a relatively easy, bounded search since $\mu(G_i) \leq \mu(G)$, $\forall G_i \leq G$. However, if $N \triangleleft G$, it is possible to have $\mu(G) < \mu(G/N)$, which makes the task for factor groups much more difficult. In fact Easdown [3] points out that not only can $\mu(G/N) - \mu(G)$ be made arbitrarily large, but that the same is true for $\mu(G/N)/\mu(G)$. Because of this, most software packages use the right regular representation by default, for factor groups, which is very inefficient because usually $\mu(G/N) \ll |G/N|$ and $|G/N|$ is always the degree of the regular representation.

If G is a finite group with a normal subgroup N such that $\mu(G) < \mu(G/N)$, then G is called exceptional, and N and G/N are said to be a distinguished subgroup and quotient group

respectively. In terms of these definitions, it would be useful to know which groups are exceptional, and what properties typify and cause a group to be exceptional and/or distinguished. It would also be useful to know if certain characteristic subgroups like $\Phi(G)$, the Frattini subgroup, and $\text{Fit}(G)$ the Fitting subgroup, can ever be distinguished. Of further interest is the question of bounds for the minimal degree of a direct product of arbitrary extensions in terms of the minimal degrees of its factors, and when this bound is reached.

CHAPTER 1

A general (not necessarily faithful) representation of a group G can be constructed by considering the action of the group's elements on the cosets of one or more subgroups of G . If $R = \{H, Hx_1, Hx_2, \dots, Hx_k\}$ is a partition of G , with $H \leq G$, then the action of $g \in G$ permutes the cosets of H as defined by $(Hx_i)g \rightarrow Hx_i g$. This gives a homomorphism of $G \rightarrow S_k$ where k is the index of H in G . However, if $1 \neq g \in Z(G) \cap H$, then $Hx_i g = Hgx_i = Hx_i$, $\forall i \in \{1, \dots, k\}$ and so the action of g is trivial and the representation is not faithful.

To insure that the action is faithful, we could take $H = 1$ for which the cosets are just the elements of G and $k = |G|$. This gives the right regular or Cayley representation and is always faithful because $Hx_i g = x_i g = x_i \forall x_i$ if and only if $g = 1$. However, as stated the regular representation seldom yields the minimal degree of G . In fact from D.L. Johnson [9], we have

Theorem 1.1

The regular representation of a group G is minimal if and only if G is:

- (a) a cyclic group of prime power order,*
- or (b) a generalized quaternion 2-group,*
- or (c) the (Klein) four group.*

Another method of ensuring that the representation is faithful is to take the action of G on

several subgroups $H_1, H_2, \dots, H_L$ of G . This action is faithful if and only if $\bigcap_{i=1}^L \text{cor}_G(H_i) = 1$. (We remind the reader that $\text{cor}_G(H_i)$ is the intersection of all of the conjugates of H_i in G .) The degree of this representation is $\sum_{i=1}^L |G : H_i|$. Therefore the minimal degree of faithful representation is the minimum $\sum_{i=1}^L |G : H_i|$, with $\bigcap_{i=1}^L \text{cor}_G(H_i) = 1$ and we say $\{H_1, H_2, \dots, H_L\}$ is a minimal representation of G .

It is noteworthy (though perhaps of little practical value) that D.L. Johnson [9] provides the naive bounds $n \leq \mu(G) \leq |G|$, where n is the natural number defined by $n! \leq |G| < (n+1)!$. This bound is obvious because the regular representation has degree $|G|$ and G cannot possibly be embedded in S_{n-1} since $(n-1)! = |S_{n-1}| < |G|$.

However the research of Johnson with regards to the minimal degrees of a direct product of groups has led to a very useful theorem which we will exploit in Chapters 4 and 5. He proved that for any direct product $H \times K$, the inequality $\mu(H \times K) \leq \mu(H) + \mu(K)$ holds because if $\{H_1, H_2, \dots, H_L\}$ and $\{K_1, K_2, \dots, K_m\}$ are minimal faithful representations of H and K respectively, then $\{H_1 \times K, H_2 \times K, \dots, H_L \times K, H \times K_1, H \times K_2, \dots, H \times K_m\}$ is a faithful representation of $H \times K$. Possibly even more important were his results as to when the reverse inequality holds. He proved that $\mu(H \times K) = \mu(H) + \mu(K)$ whenever $(|H|, |K|) = 1$ and the following theorem:

Theorem 1.2

If $A = A_1 \times A_2 \times \dots \times A_n$ is abelian with each A_i cyclic, of non-trivial prime power order a_i , then $\mu(A) = a_1 + a_2 + \dots + a_n$.

D. Wright [11] extends the theory by creating a class $\mathfrak{R}$ of groups H with the property that $\exists H_1 \leq H$, H_1 nilpotent and $\mu(H_1) = \mu(H)$. He proves that $\forall H, K \in \mathfrak{R}$, $\mu(H \times K) = \mu(H) + \mu(K)$ and that $\mathfrak{R}$ contains all nilpotent, symmetric, alternating and dihedral groups, and that $\mathfrak{R}$ is closed under direct product. [11] also gives the following example of the existence of groups H and K such that $\mu(H \times K) \neq \mu(H) + \mu(K)$:

The symbols permuted are x_{ij} ($1 \leq i \leq 5$, $1 \leq j \leq 3$). Let

$$a = (x_{12}x_{13})(x_{22}x_{23}) \dots (x_{52}x_{53}),$$

$$b = (x_{11}x_{12}x_{13})(x_{21}x_{22}x_{23}) \dots (x_{51}x_{52}x_{53}),$$

$$\gamma_i = (x_{1i}x_{2i} \dots x_{5i}) \quad (i = 1, 2, 3),$$

$$c_1 = (\gamma_1)^{-1}(\gamma_2)^2(\gamma_3)^{-1} \quad c_2 = (\gamma_1)^{-1}(\gamma_2)^{-1}(\gamma_3)^2 \quad d = \gamma_1\gamma_2\gamma_3,$$

$$H = \langle a, b, c_1, c_2 \rangle \quad \text{and } K = \langle d \rangle.$$

Then

$$a^2 = b^3 = c_1^5 = c_2^5 = [c_1, c_2] = 1,$$

$$b^a = b^{-1}, \quad c_1^a = c_1^b = c_2, \quad c_2^a = c_1, \quad c_2^b = c_1^{-1}c_2^{-1},$$

$$\text{and } \mu(H) = \mu(H \times K) = 15.$$

As a final note on this topic Easdown and Praeger [4] show that if H and K are the direct product of simple groups then $\mu(H \times K) = \mu(H) + \mu(K)$.

Of central importance to this thesis, Johnson provides the necessary theory to give an algorithm, using properties of “primitive” subgroups, for finding the minimal degree for all p -groups of order less than p^5 , which we exploit in Chapter 5 and attempt to extend to cover

p -groups of order p^5 . A subgroup H of G is said to be primitive if $H \neq \bigcap_{H < K \leq G} K$. This should not be confused with the standard definition of the class of primitive groups. From Johnson [8] we realize that the power of using primitive subgroups of abelian groups stems from the fact that H is primitive in G if and only if G/H is cyclic of prime power order. Even with nilpotent groups, H is primitive if and only if it has prime power index in G . The importance of primitive subgroups in minimal representations, especially of p -groups for odd p , is clear from the following lemma from [9].

Theorem 1.3

Let $\mathcal{R} = \{G_1, G_2, \dots, G_n\}$ be a minimal representation of G ; then there exists a minimal representation $\mathcal{S}$ of G such that every element of $\mathcal{S}$ is primitive and $G_i \in \mathcal{S}$ whenever $|G:G_i|$ is odd.

From which we get the corollary:

Corollary 1.4

All subgroups of odd index appearing in any minimal representation of a group G are primitive; further, every minimal representation of a group G of odd order consists entirely of primitive subgroups.

Another useful tool Johnson developed for finding minimal faithful representations is a

series of theorems relating the minimal number of generators of the centre of G to the number of transitive constituents of a minimal faithful representation of G . If $S = \{G_1, G_2, \dots, G_n\}$ is a minimal, faithful representation of G , then the number of transitive constituents of S is n . Furthermore, let $d(G)$ denote the minimum number of generators of G . Then Johnson gives the following theorems:

Theorem 1.5

Let G be a p -group with a minimal representation $S = \{G_1, G_2, \dots, G_n\}$, and let $d = d(Z(G))$, then if p is odd, $n = d$, while if $p = 2$, $d/2 \leq n \leq d$, the bound $n = d$ being achieved.

Corollary 1.6

If G is a nilpotent group whose centre is the direct product of d non-trivial cyclic groups of prime-power order, exactly d_2 of which have 2-power order, then the number n of transitive constituents in any minimal representation of G satisfies the inequality:

$$d \leq n \leq d - d_2/2.$$

Theorem 1.7

Let $\tilde{G}_p$ denote the class of p -groups having minimal representation $S = \{G_1, G_2, \dots, G_n\}$, such that $\{Z(G) \cap G_1, Z(G) \cap G_2, \dots, Z(G) \cap G_n\}$ is a minimal representation of $Z(G)$. Then for every non-abelian $G \in \tilde{G}_p$ with p odd, and such that G is a non-trivial direct product, we have:

$$p\mu(Z(G)) \leq \mu(G) \leq |G : Z(G)|\mu(Z(G))/p.$$

Corollary 1.8

If the hypothesis of Theorem 1.7 holds and also $|G : Z(G)| \neq p^2$; then $\mu(G) = p\mu(Z(G))$.

Note that $\tilde{G}_p$ contains all abelian p -groups and all p -groups, for odd p , whose centres are either cyclic or elementary abelian, and hence that Theorem 1.7 and its corollary apply to all groups of order p^n with p odd and $n \leq 4$.

CHAPTER 2

There would be little point discussing the nature of exceptional groups if none existed or even if it was impossible to tell if any existed, so we proceed immediately to concrete examples of finite exceptional groups. The group $G_1 = \langle x, y \mid x^8 = y^4 = 1, x^y = x^{-1} \rangle$ and $G_2 = \langle x, y, n \mid x^8 = n^2 = 1, y^2 = x^4, x^y = x^{-1}n, [n, x] = [n, y] = 1 \rangle$ are exceptional groups of order 32 with distinguished subgroups $N_1 = \langle x^4 y^2 \rangle$ and $N_2 = \langle n \rangle$ respectively. Minimal faithful representations are $\varphi: G_1 \rightarrow S_{12}$ defined by $\varphi(x) = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ and $\varphi(y) = (1\ 8)(2\ 7)(3\ 6)(4\ 5)(9\ 10\ 11\ 12)$ and $\psi: G_2 \rightarrow S_{12}$ defined by $\psi(x) = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)(9\ 10)$, $\psi(y) = (1\ 2\ 5\ 6)(3\ 4\ 7\ 8)(9\ 11)(10\ 12)$ and $\psi(n) = (1\ 5)(2\ 6)(3\ 7)(4\ 8)(9\ 10)(11\ 12)$, so that $\mu(G_1) = \mu(G_2) = 12$. Furthermore, $G_1/N_1 \cong G_2/N_2 \cong Q_{16} = \langle x, y \mid x^8 = 1, y^2 = x^4, x^y = x^{-1} \rangle$ which is the generalized quaternion group of order 16, and so by Theorem 1.1, has minimal degree 16. Although Johnson's [9] proof does not explicitly state the property of the quaternion group which makes its regular representation minimal, it is that $\langle x^4 \rangle$ is contained in every non-trivial subgroup of Q_{16} . Because of this property, in order to find $\{H_1, H_2, \dots, H_L\}$, $H_i \leq Q_{16}$, such that $\bigcap_{i=1}^L \text{cor}_Q(H_i) = 1$ we must have $\langle 1 \rangle$ among the H_i and so $\mu(Q_{16}) = |Q_{16} : \langle 1 \rangle|$. Easdown and Praeger [4] give a lengthy case by case proof that G_1 and G_2 are in fact the smallest exceptional groups and the only two of order 32.

It also bears mentioning that $N_1 \leq Z(G_1) = \langle x^4, y^2 \rangle$ and $N_2 \leq Z(G_2) = \langle n, x^4 \rangle$, so that G_1/N_1 and G_2/N_2 are both central products. The integral part that central products often play in creating

exceptional groups will be discussed in later chapters. For now however, we merely state a theorem by Easdown and Praeger [4] which will allow us to create more examples of exceptional groups via central products:

Theorem 2.1

Let p be a prime and let G_1, G_2 be non-cyclic p -groups with cyclic centres $Z_1 = \langle a_1 \rangle$ and $Z_2 = \langle a_2 \rangle$ respectively of the same order.

(a) If p is odd then $G_1 \times G_2$ is an exceptional group with distinguished subgroup

$$N = \langle \langle a_1, a_2 \rangle \rangle.$$

(b) If $p = 2$, $\mu(G_1) > \mu(G_2)$ and G_2 is not the generalized quaternion group, then

$$G_1 \times G_2 \text{ is exceptional with distinguished subgroup } N = \langle \langle a_1, a_2 \rangle \rangle.$$

From this theorem, it follows immediately that the following groups are exceptional:

(i) $G = D_2^n \times D_2^m$ for $n > m \geq 3$, with distinguished quotient $G/N \cong D_2^n * D_2^m$ (the central product)

(ii) $G = Q_2^n \times D_2^m$ for $n \geq m \geq 3$, with distinguished quotient $G/N \cong Q_2^n * D_2^m$

Easdown and Praeger [4] note that the smallest of these examples has order 64. By iterative use of the theorem we also get that the following families are exceptional:

(iii) $G = (D_{16} * (*D_8)^n) \times D_8$, with $G/N \cong (D_{16} * (*D_8)^{n+1})$, and

(iv) $G = (Q_8 * (*D_8)^n) \times D_8$, $G/N = (Q_8 * (*D_8)^{n+1})$.

Note that $(*D_8)^n$ is $D_8 * D_8 * \dots * D_8$, the central product of n copies of D_8 .

Easdown and Praeger [4] then attempt to show that $D_2^n \times D_2^m$, $Q_2^n \times D_2^m$, and $Q_2^n \times Q_2^m$, $\forall n, m \geq 3$ are exceptional, again with the central products as the distinguished quotients, by explicitly calculating their minimum degrees of faithful representation. However, partially because of a typo, they fail to prove that $D_2^n \times D_2^m$ and $Q_2^n \times Q_2^m$ are exceptional for $n = m$. In fact their argument proves that $D_2^n \times D_2^m$ and $Q_2^n \times Q_2^m$ are not exceptional. The error is minor but we point it out because it will be of use in later in Chapter 5.

One class of exceptional 2-groups which is not a class of direct products is of the form $H_{m,n} = \langle x, y \mid x^a = y^b = 1, a = 2^n, b = 2^m, x^y = x^{-1} \rangle$ for $2 \leq m < n$, with $N = \langle x^c y^2 \mid c = 2^{n-1} \rangle \triangleleft H_{m,n}$ and $H_{m,n}/N \cong Q_2^{n+1}$. Hence $\mu(H_{m,n}/N) = 2^{n+1} > 2^n + 2^m \leq \mu(H_{m,n})$, the latter inequality true because $H_{m,n} \cong \langle (1, 2, \dots, 2^n), (1, 2^n)(2, 2^{n-1} - 1) \dots (2^{n-1}, 2^{n-1} + 1)(2^{n+1} + 1, 2^{n+1} + 2, \dots, 2^n + 2^m) \rangle$. Note that the smallest group in this class $H_{2,3}$ is the exceptional group G_1 of order 32.

Up until now all examples have been of exceptional 2-groups so we turn to p -groups where p is an odd prime. If we set $G = \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, xz = zx, yz = zy \rangle$, then $G \times G$ is an exceptional group of order p^6 . If $H = Z_p \text{ wr } Z_p$, then $H \times H$ is an exceptional group of order $p^{2(p+1)}$, with distinguished quotient $H * H$. For $n \geq 1$,

$$G = \langle x_1, \dots, x_p^n, y_1, \dots, y_p^n, z \mid x_i^a = y_i^a = z_i^a = 1 \text{ for } a = p^n \text{ and all } i, \\$$

$$[x_i, x_j] = [x_i, z] = [y_i, y_j] = 1 \text{ for all } i, j, x_i y_j = y_j x_{i+1} \text{ for all } i < a, \\$$

$$\text{and all } j, y_j x_a = y_j x_1 \text{ for all } j, y_i z = z y_{i+1} \text{ for } i < a \rangle$$

is an exceptional group of order $p^{n(a+1)}$ where $a = p^n$, with distinguished subgroup

$$N = \langle x_1 \dots x_p^n y_1^{-1} \dots y_a^{-1} \rangle.$$

The only exceptional group given by Easdown and Praeger [4] which is not a p -group is

the direct product $D_{2^n} \times D_{2^m}$, with $2 < n < m$, n and m are odd, and $2^n > 4$, $2^m > 4$, and having the central product as quotient. They also mention that although all of the examples given were solvable groups, Liebeck found unsolvable examples, although no reference is given.

We end this chapter with a means of constructing exceptional groups by direct product, given by Easdown and Praeger[4]:

Theorem 2.2

If G and H are groups and G is an exceptional group then $G \times H$ is also an exceptional group if either

(a) $(|G|, |H|) = 1$, or

(b) G and H are both nilpotent.

The proof is straight forward because in both (a) and (b) we have $\mu(G \times H) = \mu(G) + \mu(H)$.

CHAPTER 3

With the examples from the previous section in mind we can investigate the properties of exceptional groups. We begin with the trivial assertion that all exceptional groups are non-abelian, since any quotient G/N of an abelian group G is isomorphic to a subgroup G . As mentioned earlier, the two exceptional groups of order 32 are the smallest exceptional groups and so cannot have proper subgroups or non-trivial quotients which are themselves exceptional. An exceptional group G is called S -minimal, Q -minimal, or SQ -minimal if no proper subgroup, quotient, or section respectively is exceptional. Through out this chapter, unless otherwise stated, G will denote an exceptional group with distinguished subgroup N and distinguished quotient G/N . Immediately from these definitions we have the following theorem by Easdown and Praeger[4]:

Theorem 3.1

- (a) *If G is S -minimal then N is contained in the Frattini Subgroup $\Phi(G)$, that is N is contained in every maximal subgroup of G .*
- (b) *If M is a normal subgroup of G contained in N then either M is a distinguished subgroup of G or G/M is exceptional with distinguished subgroup N/M . In particular if G is Q -minimal then every nontrivial normal subgroup of G contained in N is distinguished.*

Thus if G is SQ-minimal then we may take N to be a minimal normal subgroup of G contained in the nilpotent group $\Phi(G)$, so we can assume N is elementary abelian. This will be very useful in Chapter 5 when proving that certain families of groups are not exceptional by assuming we have a least counterexample.

By considering the action of a distinguished subgroup in a minimal representation, we get from [4]:

Theorem 3.2

Suppose that G is minimally represented on $X = \bigcup_{i=1}^r X_i$ with orbits $X_1, \dots, X_r$. Then a distinguished subgroup N is intransitive on each X_i if G is S -minimal, and is non-trivial on each X_i if G is Q -minimal. In particular if G is SQ-minimal then G acts imprimitively on each X_i so $|X_i|$ is a number greater than one which is not prime.

With the desire to better facilitate computer processing of finite quotient groups, and in particular their permutation representation, Derek Holt [7] produced the following theorems:

Theorem 3.3

Let G be a finite permutation group with $\mu(G) = d$. Let A be a class of finite abelian groups closed under subgroup, quotient, and direct product, and let N be a normal A -subgroup of G . Then there exists a normal A -subgroup M of G with $N \leq M$ such that $\mu(G/M) \leq d$. In particular if N is a maximal normal A -subgroup of G then $\mu(G/N) \leq d$.

However, eight years earlier, presumably unknown to Holt, Easdown and Praeger [4] proved the slightly stronger theorem:

Theorem 3.4

Suppose that H is a finite group with a nontrivial abelian normal subgroup K . Then H has an abelian normal subgroup L containing K for which $\mu(H/L) < \mu(H)$ and the prime divisors of $|L|$ and $|K|$ are the same. If K is elementary abelian then L may be chosen to be elementary abelian.

It would be interesting to know under what circumstances $\mu(L/K) \leq \mu(H)$ was true. This would make computing with the sequence of elementary factors G_i/G_{i-1} (mentioned in the Introduction) much easier because if $\mu(G) < \mu(G_i/G_{i-1})$ then if G_{i-1} is elementary abelian we have that there exists $G_{i-1} < K < G$, such that G_i/K , K/G_{i-1} , and $G_{i-1}/1$ are all elementary abelian and the minimal degrees of all of these quotients would all be less than that of G as Holt required.

Although the two theorems are similar the proofs have striking differences. Holt embeds G in S_X and partitions the set X that G acts on into the orbits w_i induced by N . He takes Y to be a subset of X with one representative from each of the orbits of N and finds $L \leq S_X$ isomorphic to the direct product of the induced action groups N^{w_i} and proves that there is an M in G such that $G/M \cong D$, the setwise stabilizer of Y in GL . The point is that the extension G of M by G/M may be nonsplit so he embeds G in the larger group to force the extension to split.

Easdown and Praeger on the other hand make use of the fact that if G is transitive and imprimitive, G^* the group induced on the blocks of imprimitivity, and G_B^B the action of the set stabilizer G_B restricted to some block B , then G can be embedded in $G_B^B \text{ wr } G^*$. Easdown and Praeger partition X into the orbits of X_i of G and partition each X_i into Y_i the set of orbits of X_i induced by N , (here we use Holt's notation for consistency.) They then embed G into $\prod G^{w_i}_{w_i} \text{ wr } G^{(i)}$, where $G^{(i)}$ the group is the group G^{X_i} induces on Y_i . L is chosen in the same way as Holt does and $\prod G^{w_i}_{w_i} \text{ wr } G^{(i)}$ is normal in L . The rest of the proof is essentially the same as Holt's.

Holt's [7] second theorem, immediately below, is even stronger in the general sense that the abelian criterion is dropped.

Theorem 3.5

Let G be a finite group with $\mu(G) \leq d$. Let $\mathcal{L}$ be a class of finite groups closed under subgroup, quotient, and group extension. Let $N = O_{\mathcal{L}}(G)$ be the largest normal $\mathcal{L}$ -subgroup of G . Then $\mu(G/N) \leq d$.

A disappointing limitation of this theorem is that it requires $\mathcal{L}$ to be closed under arbitrary extensions instead of just direct products so that nilpotent groups do not form such a class and we don't have the result that $\mu(G/\text{Fit}(G)) \leq \mu(G)$. This topic is covered in more detail in the next chapter.

CHAPTER 4

Although much progress has been made in the study of minimal degrees of faithful permutation representations and exceptional groups, there still remain many unanswered questions and open conjectures. The main conjectures in this area of study are of course “Which finite groups are exceptional?” and “What causes a group to be exceptional?”

Are All Central Products Exceptional?

In response to the first question, Holt [7] mentioned in passing that “We are likely to have a negative result [that is $\mu(G) \geq \mu(G/N)$] whenever the quotient $[G/N]$ is some sort of central product.” We can only assume that he meant whenever $G \cong H \times K$ and $G/N \cong H * K$ where $H * K$ is a non-trivial central product; i.e. $H * K \cong (H \times K)/X$ with $X \neq 1$ a subgroup of $Z(H \times K)$. We begin Chapter 5 by providing a counter example to this idea. However, as we saw in most of the examples in Chapter 2, quotients which are isomorphic to central products often play a crucial role in forming exceptional groups. Gorenstein [5] (pg 29) gives the alternate definition of central product:

Definition 4.1

Let H, K, M be groups with $M \subseteq Z(H)$ and suppose there is an isomorphism θ of M into $Z(K)$. Then if we identify M with its image $M\theta$, there exists a group G of the form $G = HK$ with $M = H \cap K \subseteq Z(G)$ such that H centralizes K . G is said to be a central product of H and K .

Thus if we again consider the representation $\{H_1 \times K, H_2 \times K, \dots, H_L \times K, H \times K_1, H \times K_2, \dots, H \times K_m\}$ of $H \times K$ where $\{H_1, H_2, \dots, H_L\}$ and $\{K_1, K_2, \dots, K_m\}$ are minimal faithful representations of H and K respectively, then we note that it does not provide a faithful representation of G because $(\bigcap \text{cor}_G(H_i \times K)) \cap (\bigcap \text{cor}_G(H \times K_i)) \supseteq H \cap K \neq 1$.

It is no coincidence that most of the examples of exceptional groups given were 2-groups. 2-groups are particularly susceptible to being exceptional because they often admit the relation $x^y = x^{-1}$, as in the minimal exceptional group $G_1 = \langle x, y \mid x^8 = y^4 = 1, x^y = x^{-1} \rangle$. The relation allows for the highest non-trivial power of x and the highest non-trivial power of y to be in the centre. Setting these elements (in the case of G_1 , x^4 and y^2) equal to one another to obtain the quotient forces the centre of the quotient to be cyclic of order 2 and not only to be contained in every subgroup whose pull back contained one of the two, but also forces the other subgroups of order 2 generated by the product of a power of x and a power of y to be equal to one another. Easdown said it more elegantly "This is not surprising [that exceptional groups exist] ... If the lattice of subgroups of the homomorphic image is more restricted than the lattice of subgroups of the

original group then conceivably the minimal faithful degree of the homomorphic image could be higher.”

Do Exceptional p -groups Order $< p^6$, p odd prime, Exist?

Although there exist exceptional 2-groups of order as small as 32, it is unlikely that there are any exceptional p -groups, of order less than p^6 , for p an odd prime. Easdown and Praeger mentioned in their paper that they did not know if any existed. In the next chapter we work towards a proof that there are none. The problem is broken down into essentially 45 cases and all but 3 have been eliminated. Research continues on the remaining 3. Chapter 2 included an example by Easdown and Praeger of an exceptional group of order p^6 , for p odd.

Are $\text{Fit}(G)$ and $\Phi(G)$ Ever Distinguished Subgroups?

In the last chapter, we mentioned that Holt’s theorem (Theorem 3.5) did not give us that the degree of $G/\text{Fit}(G)$ was always less than the degree of G and he wished to know if it was true. He noted however that if it were true of the Frattini subgroup $\Phi(G)$ then since $\text{Fit}(G/\Phi(G)) = \text{Fit}(G)/\Phi(G)$, which is abelian, Theorem 3.5 would imply the result for $\text{Fit}(G)$.

Shortly (relatively) after Holt posed the question John Cossey [2] answered it in the affirmative as the sole purpose of his paper Quotients of Permutation Groups. He gave a simple proof that if d is the minimal degree of G and n is the number of distinct primes dividing $|F(G)|$ then the minimal degree of $G/F(G)$ is at most nd , before proving the stronger bound d . The proof borrowed the method Holt used but also used induction on $|F(G)'|$, the base case implying that

$F(G)$ is a maximal abelian normal subgroup of G and thus giving the result by Holt's theorem.

When Does $\mu(H \times K) = \mu(H) + \mu(K)$?

Johnson [9] and Wright [11] both studied the question as to which groups H and K satisfy the equality $\mu(H \times K) = \mu(H) + \mu(K)$. As mentioned earlier, Johnson showed $\mu(H \times K) \leq \mu(H) + \mu(K)$ was always true and that $\mu(H \times K) = \mu(H) + \mu(K)$ whenever the orders of H and K were relatively prime. He also showed in Theorem 1.1 that the minimal degree of a direct product of finitely many cyclic subgroups of prime power order is equal to the sum of the degrees of the cyclic subgroups which is also equal to the sum of the orders of the cyclic subgroups. Wright showed that the equality holds if H and K are nilpotent or even if they have nilpotent subgroups H_1 and K_1 respectively with $\mu(H) = \mu(H_1)$ and $\mu(K) = \mu(K_1)$. He went on to show that among these groups are all the symmetric and alternating groups and all dihedral groups. Further he showed that the class of such groups is closed under direct product. However, the full extent of the class of all groups that have a nilpotent subgroup of the same degree is not yet known. Wright even wondered if it were ever true that $\mu(H \times K) \neq \mu(H) + \mu(K)$ but a counter example was given in chapter 2. As mentioned there too Easdown and Praeger showed that the direct product of simple groups has minimal degree equal to the sum of the degrees of the simple subgroups. This was the only example given of a group, not in the class mentioned above, for which the degree of the direct product is equal to the sum of the degrees of the subgroups in the direct product so further exploration is also required here.

Are Abelian Quotients Ever Distinguished?

Probably the conjecture which holds the most interest in the study of exceptional groups is whether a distinguished quotient can ever be abelian, that is, does there exist a finite group G with normal subgroup N such that $\mu(G) < \mu(G/N)$, with G/N abelian? Easdown and Praeger gave the result that the answer is negative when G/N is cyclic. Later Easdown on his own showed that the least counter-example must be a p -group, if it exists. Praeger, working with Kovacs [10] showed that a distinguished quotient can not be elementary abelian. We use all of these results extensively in the next chapter to work towards a classification of all exceptional p -groups of order less than p^6 , for p an odd prime, or rather that none exist. As well we prove and use the minor result that $Z_p^n \times Z_p$ is never a distinguished quotient. Despite this progress a complete answer to the question of the existence of a distinguished abelian quotient is not yet known.

What is the Extent of the Class $\check{G}_p$?

In Chapter 2, we mentioned that Johnson named the class $\check{G}_p$ of all p -groups G having minimal representation $\{G_1, G_2, \dots, G_n\}$ such that $\{Z(G) \cap G_1, Z(G) \cap G_2, \dots, Z(G) \cap G_n\}$ is a minimal representation of $Z(G)$. He also posed the question “What is the extent of $\check{G}_p$?” He asserted that it contained not only all abelian p -groups but also all p -groups for odd p whose centres are either cyclic or elementary abelian, and hence all groups of order p^n with p odd and $n \leq 4$. This allowed us to use the conclusion in Proposition 5 to classify the minimal degrees of

all such p groups, which appear in table form in the next chapter (proof of the minimality is given immediately following the table.) If we could show $\check{G}_p$ includes all p -groups G , for p odd, with centre isomorphic to $Z_p^2 \times Z_p$, then we could expand the scope of Theorem 1.7 to allow us to find the minimal degrees of all p -groups of order p^5 . In Chapter 5, we show that if $|G| = p^5$ and $Z(G) \cong Z_p^2 \times Z_p$, then the lower bound of Theorem 1.7 is still true for G . This helps us in the classification of exceptional groups of order p^5 .

CHAPTER 5

In this chapter we present the author's results on the topics of degrees of minimal representations and exceptional groups. Most results are in direct response to the conjectures made by others which were introduced in Chapter 4.

Not Every Central Product is Exceptional

We begin this Chapter with the obvious result that since $Q_2^n * Q_2^n$ is not a distinguished quotient of $Q_2^n \times Q_2^n$, it serves as a counter example to Holt's conjecture that every central product yields a distinguished quotient of the direct product.

Minimal Degrees of p-groups of order $< p^5$

We now use the method D. L. Johnson [9] gave to determine the minimal degree of a faithful representation of all p-groups of order p^n , where p is prime and $n \leq 4$. The resulting degrees are summarized in the table below and their proof immediately follows the table. The centres of the groups are included in the tables because Theorem 1.5 gives us that the number of subgroups in a minimal representation of a p-group is d if p is odd and between $d/2$ and d if p is even, where d is the minimal number of generators of the centre of G.

Burnside classified the isomorphism classes for all such p-groups, and their presentations are taken from his book, Theory of Groups of Finite Order[1].

**MINIMAL DEGREE OF FAITHFUL REPRESENTATION OF P-GROUPS
OF ORDER $< p^5$**

Group	ORDER	PRESENTATION	Centre	DEGREE
G_1	p	Z_p	G_1	p
G_2	p^2	Z_p^2	G_2	p^2
G_3	p^2	$Z_p \times Z_p$	G_3	$2p$
G_4	p^3	Z_p^3	G_4	p^3
G_5	p^3	$Z_p^2 \times Z_p$	G_5	$p^2 + p$
G_6	p^3	$Z_p \times Z_p \times Z_p$	G_6	$3p$
G_7	p^3	$\langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$	$\langle x^p \rangle$	p^2
G_8	2^3	$Q_8 \cong \langle x, y \mid x^4 = y^4 = 1, xy = yx^{-1}, x^2 = y^2 \rangle$	$\langle x^2 \rangle$	8
G_9	p^3 odd	$\langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, zx = xz, zy = yz \rangle$	$\langle z \rangle$	p^2
G_{10}	p^4	Z_p^4	G_{10}	p^4
G_{11}	p^4	$Z_p^3 \times Z_p$	G_{11}	$p^3 + p$
G_{12}	p^4	$Z_p^2 \times Z_p^2$	G_{12}	$2p^2$
G_{13}	p^4	$Z_p^2 \times Z_p \times Z_p$	G_{13}	$p^2 + 2p$
G_{14}	p^4	$Z_p \times Z_p \times Z_p \times Z_p$	G_{14}	$4p$
G_{15}	p^4	$\langle x, y \mid x^{p^3} = y^p = 1, xy = yx^{p+1} \rangle$	$\langle x^{p^2} \rangle$	p^3

Group	ORDER	PRESENTATION	Centre	DEGREE
G_{16}	p^4	$\langle x, y, z \mid x^{p^2} = y^p = z^p = 1, yz = zyx^p, xy = yx, xz = zx \rangle$	$\langle x \rangle$	p^3
G_{17}	p^4	$\langle x, y \mid x^{p^2} = y^{p^2} = 1, xy = yx^{p+1} \rangle$	$\langle x^p, y^p \rangle$	$2p^2$
G_{18}	p^4	$\langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, xz = zx, yz = zy \rangle$	$\langle x^p, z \rangle$	$p^2 + p$
G_{19}	p^4	$\langle x, y, z, \mid x^{p^2} = y^p = z^p = 1, xy = yxz, yz = zy, zx = xz \rangle$	$\langle x^p, z \rangle$	$2p^2$
G_{20}	2^4	$Q_8 \times Z_2 \cong \langle x, y, z \mid x^4 = y^4 = z^2 = 1, xy = yx^3, x^2 = y^2, xz = zx, yz = zy \rangle$	$\langle x^2 \rangle$	10
G_{21}	2^4	$D_{16} \cong \langle x, y \mid x^8 = y^2 = 1, xy = yx^{-1} \rangle$	$\langle x^4 \rangle$	8
G_{22}	2^4	$\langle x, y \mid x^8 = y^2 = 1, xy = yx^3 \rangle$	$\langle x^4 \rangle$	8
G_{23}	2^4	$Q_{16} \cong \langle x, y \mid x^8 = y^4 = 1, xy = yx^{-1}, x^4 = y^2 \rangle$	$\langle x^4 \rangle$	16
G_{24}	p^4 odd	$\langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$	$\langle x^p \rangle$	p^2
G_{25}	p^4 odd	$\langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^p, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$	$\langle x^p \rangle$	p^3
G_{26}	p^4 odd	$\langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^{\alpha p}, xy = yx^{p+1}, xz = zxy, yz = zy \rangle^*$	$\langle x^p \rangle$	p^3
G_{27}	p^4 odd	$\langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, xz = zx, xw = wx, yw = wy, zw = wz \rangle$	$\langle w, z \rangle$	$p^2 + p$
G_{28}	3^4	$\langle x, y, z \mid x^9 = y^3 = z^3 = 1, xy = yxz, xz = zx, yz = zx^6y \rangle$	$\langle x^3 \rangle$	27
G_{29}	$p^4, p > 3$	$\langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, zy = yzw, xz = zx, zw = wx, xw = wy, yw = wy \rangle$	$\langle w \rangle$	p^2

* Here, α is any non-residue mod p .

Proof of Minimal Degrees:

Note that the minimal degrees of the abelian groups follow directly from Johnson's Theorem 2, and so are self evident.

The non-abelian isomorphism classes are as follows:

$G_7 = \langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$, has centre $Z(G) = \langle x^p \rangle$ which has order p . Thus $|G : Z(G)| = p^2$, and so by Corollary 1.8, $\mu(G) = p\mu(Z(G)) = p^2$.

$G_8 = \langle x, y \mid x^4 = y^4 = 1, xy = yx^{-1}, x^2 = y^2 \rangle \cong Q_8$. By Theorem 1.1 we have $\mu(G) = 8$.

$G_9 = \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, zx = xz, zy = yz \rangle$, has $Z(G) = \langle z \rangle \cong Z_p$ and so $|G : Z(G)| = p^2$. Again by Corollary 1.8, $\mu(G) = p\mu(Z(G)) = p^2$.

$G_{15} = \langle x, y \mid x^{p^3} = y^p = 1, xy = yx^{p+1} \rangle$, has centre $Z(G) = \langle x^{p^2} \rangle \cong Z_p$ which is cyclic.

Hence by Theorem 1.5, a minimal representation of G is transitive and so the minimal degree of

G is a power of p . By Theorem 1.7, we have the inequality: $p\mu(Z(G)) \leq \mu(G) \leq |G :$

$Z(G)|\mu(Z(G))/p$ which implies that $p^2 \leq \mu(G) \leq p^3$. However, $G \geq \langle x \rangle$ and $|\langle x \rangle| = p^3$, so

$\mu(G) \geq p^3$. $\therefore \mu(G) = p^3$.

$G_{16} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, yz = zyx^p, xy = yx, xz = zx \rangle$, has centre $Z(G) = \langle x \rangle \cong Z_p^2$ so $|G : Z(G)| = p^2$ and, by Corollary 1.8, $\mu(G) = p\mu(Z(G)) = p^3$.

$G_{17} = \langle x, y \mid x^{p^2} = y^{p^2} = 1, xy = yx^{p+1} \rangle$. It is obvious that $\langle x^p \rangle \leq Z(G)$ but also note that $xy^p = yx^{p+1}y^{p-1} = yxy^{p-1}x^p = y^2x^{p+1}y^{p-2}x^p = y^2xy^{p-2}x^{2p} = \dots = y^pxx^{p^2} = y^px$ and so $\langle y^p \rangle \leq Z(G)$ as well. Thus we have $Z(G) = \langle x^p, y^p \rangle \cong Z_p \times Z_p$, and $|G : Z(G)| = p^2$. $\therefore \mu(G) = p\mu(Z_p \times Z_p) = 2p^2$. Note that since $Z(G)$ is not cyclic, we must have an intransitive minimal representation so $\mu(G)$ should not be a power of p .

$G_{18} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, xz = zx, yz = zy \rangle$, note that $G = \langle x, y \rangle \rtimes \langle z \rangle$ so by Theorem 2 of Wright[11], we have $\mu(G) = \mu(\langle x, y \rangle) + \mu(\langle z \rangle)$. But $\langle x, y \rangle \cong \langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$ which has minimal degree p^2 and $\langle z \rangle \cong Z_p$ which has minimal degree p . $\therefore \mu(G) = p^2 + p$.

$G_{19} = \langle x, y, z, \mid x^{p^2} = y^p = z^p = 1, xy = yxz, yz = zy, zx = xz \rangle$, has centre $Z(G) = \langle x^p, z \rangle \cong Z_p \times Z_p$. Thus $|G : Z(G)| = p^2$ and by Corollary 3, $\mu(G) = p\mu(Z(G)) = p(2p) = 2p^2$.

$G_{20} = \langle x, y, z \mid x^4 = y^4 = z^2 = 1, xy = yx^3, x^2 = y^2, xz = zx, yz = zy \rangle \cong Q_8 \times Z_2$, Theorem 2 of Wright gives $\mu(G) = \mu(Q_8) + \mu(Z_2) = 8 + 2 = 10$.

$G_{21} = \langle x, y \mid x^8 = y^2 = 1, xy = yx^{-1} \rangle \cong D_{16}$. In fact, $\mu(D_{16})$ is well known to be 8, but for the sake of completeness we derive it as follows: $Z(G) = \langle x^4 \rangle \cong Z_2$ so by Theorem 1.7, $2\mu(\langle x^4 \rangle) \leq \mu(G) \leq |G : \langle x^4 \rangle| \mu(\langle x^4 \rangle)/2 \Rightarrow 4 \leq \mu(G) \leq 8$. But G has a subgroup $\langle x \rangle$ of order 8 so $\mu(G) \geq 8$. $\therefore \mu(G) = 8$.

$G_{22} = \langle x, y \mid x^8 = y^2 = 1, xy = yx^3 \rangle$, has centre $Z(G) = \langle x^4 \rangle \cong Z_2$ and by a process identical to the case before, we have $\mu(G) = 8$.

$G_{23} = \langle x, y \mid x^8 = y^4 = 1, xy = yx^{-1}, x^4 = y^2 \rangle \cong Q_{16}$. Hence Johnson's Theorem 1.1, gives $\mu(Q_{16}) = 16$.

$G_{24} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$, has centre $Z(G) = \langle x^p \rangle \cong Z_p$ so again we have $p\mu(Z(G)) \leq \mu(G) \leq |G : Z(G)| \mu(Z(G))/p \Rightarrow p^2 \leq \mu(G) \leq p^3$. Since $Z(G)$ is cyclic we know a minimal representation of G must be transitive, and so $\mu(G) = p^2$ or $\mu(G) = p^3$. Note that $|G : \langle x \rangle| = p^2 = |G : \langle y, z \rangle|$ and $\text{cor}_G(\langle x \rangle) = \langle x^p \rangle$ and $\text{cor}_G(\langle y, z \rangle) \leq \langle z \rangle$. (The latter being true because $x\langle y, z \rangle x^{-1} = \langle xyx^{-1}, xzx^{-1} \rangle = \langle yx^p, zxyx^{-1} \rangle = \langle yx^p, zy x^p \rangle = \langle yx^p, z \rangle$ and $\text{cor}_G(\langle y, z \rangle) \leq (x\langle y, z \rangle x^{-1} \cap \langle y, z \rangle)$.) $\therefore \langle x^p \rangle \cap \langle z \rangle = 1 \Rightarrow \{\langle x \rangle, \langle y, z \rangle\}$ is a faithful representation of G of degree $2p^2$. $\therefore \mu(G) \leq 2p^2$ and so $\mu(G) = p^2$.

Minimal Permutation Representations

$G_{25} = \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^p, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$, has centre

$Z(G) = \langle x^p \rangle \cong Z_p$ so a minimal representation must be transitive and $p^2 \leq \mu(G) \leq p^3$ so $\mu(G) = p^2$ or $\mu(G) = p^3$. But $G \geq \langle y, z \rangle \cong Z_p^2 \times Z_p$ so $\mu(G) \geq p^2 + p$ and thus $\mu(G) = p^3$.

$G_{26} = \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^{ap}, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$. The proof is

identical to the last case that $\mu(G) = p^3$, because z still has order p^2 .

$G_{27} = \langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, xz = zx, xw = wx, yz = zy, yw = wy,$

$zw = wz \rangle$, note that $G = \langle x, y, z \rangle \times \langle w \rangle \cong G_9 \times Z_p$ and so $\mu(G) = p^2 + p$.

$G_{28} = \langle x, y, z \mid x^9 = y^3 = z^3 = 1, xy = yxz, xz = zx, yz = zx^6y \rangle$. The argument is identical

to that for G_{26} , with the substitution $p = 3$. $\therefore \mu(G) = 27$.

$G_{29} = \langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, zy = yzw, xz = zx, zw = wz, xw = wx, yw = wy \rangle$. Similar arguments will give $\mu(G) = p^2$ or $\mu(G) = p^3$. Note that $|G : \langle x, z \rangle| = p^2$. $\therefore$ In order to show $\mu(G) = p^2$, we need only show that $\text{cor}_G(\langle x, z \rangle) = 1$. Now, $y^{-1} \langle x, z \rangle y = \langle y^{-1}xy, y^{-1}zy \rangle = \langle xz, zw \rangle$ and $\langle xz, zw \rangle \cap \langle x, z \rangle = \langle xz \rangle$ so $\text{cor}_G(\langle x, z \rangle) \leq \langle xz \rangle$.

Furthermore,

$$y^2 \langle x, z \rangle y^2 = y^{-1} \langle xz, zw \rangle y = \langle y^{-1}xzy, y^{-1}zwy \rangle = \langle xz^2w, zw^2 \rangle.$$

$$\therefore \text{cor}_G(\langle x, z \rangle) \leq \langle xz \rangle \cap \langle xz^2w, zw^2 \rangle. \text{ Since } \langle x, z, w \rangle \text{ is abelian, } \forall g \in \langle xz^2w, zw^2 \rangle,$$

$$\exists i, j \in \{1, 2, \dots, p\} \text{ such that } g = (xz^2w)^i (zw^2)^j = x^i z^{2i+j} w^{i+2j}. \therefore g \in \langle xz \rangle \Rightarrow 2i + j \equiv i \pmod{p},$$

$$\text{and } i + 2j \equiv 0 \pmod{p} \Rightarrow p \mid i + j \text{ and } p \mid i + 2j \Rightarrow p \mid j \Rightarrow p \mid i \Rightarrow g = 1. \therefore \text{cor}_G(\langle x, z \rangle) = 1 \text{ and}$$

$$\mu(G) = p^2.$$

This completes the proof of the minimal degrees of p -groups of order $< p^5$.

For the remainder of paper, let x, y, z and w denote a representative of each of the pull-back of x, y, z and w respectively (i. e. if $\phi: G \rightarrow G/N$ is the natural homomorphism, then $\phi(x) = x, \phi(y) = y$, etc.)

As mentioned earlier, all that is needed to extend the above algorithm for finding minimal degrees, to the cases where $|G| = p^5$, is to deal with the case where $Z(G) \cong Z_p^2 \times Z_p$. Although we can not add p-groups of this sort to the class $\tilde{G}p$, we can show that the lower bound for $\mu(G)$ given by Theorem 1.7 holds for p-groups, with p odd, for which $|G| = p^5$ and $Z(G) \cong Z_p^2 \times Z_p$. This should be sufficient since, as demonstrated above, it is usually only the lower bound which is necessary to determine the minimal degree.

Theorem 5.1

If p is an odd prime, $|G| = p^5$, and $Z = Z(G) \cong Z_p^2 \times Z_p$ then $\mu(G) \geq p\mu(Z(G)) = p^3 + p^2$.

Proof:

Z is minimally generated by 2 elements so every minimal faithful representation of G consists of two primitive subgroups, say $\{G_1, G_2\}$. For each G_i , $Z \cap G_i \neq 1$ since G_i must have a normal subgroup which must intersect the centre; otherwise $\text{cor}_G(G_i) = 1$ and $\{G_i\}$ is a faithful representation of degree less than $\{G_1, G_2\}$. Note also that $(Z \cap G_1) \cap (Z \cap G_2) = 1$. Thus $\{Z \cap G_1, Z \cap G_2\}$ is a faithful representation of Z.

Now, $Z \cap G_i \neq 1$ gives $p^3 > |Z : Z \cap G_i| > 1$ so $|Z : Z \cap G_i| = p$ or p^2 . $\mu(Z) = p^2 + p$ so we can not have $|Z : Z \cap G_i| = p$ for $i = 1$ and $i = 2$. If $|Z : Z \cap G_1| = p$ and $|Z : Z \cap G_2| = p^2$, or visa versa, then $\{Z \cap G_1, Z \cap G_2\}$ is a minimal faithful representation of Z and so G satisfies the hypothesis of Theorem 1.7 and we have $\mu(G) \geq p\mu(Z(G)) = p^3 + p^2$. $\therefore$ We can assume $|Z : Z \cap G_1| = p^2 = |Z : Z \cap G_2|$. Then $|Z \cap G_1| = p = |Z \cap G_2|$ and

$$|ZG_i| = |Z||G_i|/|Z \cap G_i| = p^3 |G_i|/p \leq p^5 = |G|. \therefore |G_i| \leq p^3 \Rightarrow |G : G_i| \geq p^2.$$

Suppose $|G : G_1| = |G : G_2| = p^2$. Then $|ZG_i| = p^5 = |G| \Rightarrow ZG_1 = ZG_2 = G$. Now $G_i \triangleleft ZG_i \Rightarrow G_i \triangleleft G \Rightarrow G_1 G_2 \leq G$. $|G_1 G_2| = |G_1||G_2|/|G_1 \cap G_2| = p^6/|G_1 \cap G_2| \leq p^5 \Rightarrow |G_1 \cap G_2| = p$. But $G_1 \triangleleft G, G_2 \triangleleft G \Rightarrow G_1 \cap G_2 \triangleleft G$ which contradicts the assumption that $\{G_1, G_2\}$ is a faithful representation of G . $\therefore \mu(G) \geq p^3 + p^2$.

Next we prove a theorem which will be a helpful tool in the classification of exceptional p -groups of order $< p^6$, for p an odd prime.

Theorem 5.2

If a finite p -group G , has a normal subgroup N such that G/N has order p^b and a cyclic subgroup of order p^{b-1} and (for $p = 2$) G/N is not isomorphic to the Generalized Quaternion group, then G/N is not a distinguished quotient (i. e. $\mu(G) \geq \mu(G/N)$.)

Proof:

By way of contradiction, we assume in each case that G is a counter-example. Note that since N is a normal subgroup of a p -group, $N \cap Z(G) \neq 1$, so let $\langle \mathbf{n} \rangle \leq N \cap Z(G)$ with $\mathbf{n} \neq 1$.

By Marshall Hall [6], (theorem 12.5.1, pg 187), the seven isomorphism classes of groups of order p^a which have a cyclic subgroup of order p^{a-1} are:

Case 1) for $n \geq 1$, $G/N = \langle x \mid a = p^n, x^a = 1 \rangle \cong Z_p^n$

Trivial. (Proven by Easdown and Praeger [4].)

Case 2) for $n \geq 2$, $G/N = \langle x, y \mid a = p^{n-1}, x^a = y^p = 1, xy = yx \rangle \cong Z_p^{n-1} \times Z_p$

$\mu(G/N) = p^{n-1} + p$, by Theorem 1.2. We know $x^a \in \langle n \rangle$ and if $x^a \neq 1$ then $|x| \geq p^n$ and

$\mu(G) \geq \mu(\langle X \rangle) = p^n > p^{n-1} + p = \mu(G/N)$, so we can assume $X^a = 1$. But in this case,

$xn = nx$ and thus G/N is isomorphic to a subgroup of $\langle x, n \rangle \leq G$, so again G/N is not distinguished.

Case 3) for $n \geq 3$, p odd, $G/N = \langle x, y \mid a = p^{n-1}, x^a = y^p = 1, xy = yx^{p^{n-1}} \rangle$

$Z(G/N) = \langle x^{a/p} \rangle$ which is cyclic so a minimal representation of G/N must be transitive and Proposition 3 applies so $p\mu(Z(G/N)) \leq \mu(G/N) \leq |G/N : Z(G/N)|\mu(Z(G/N))/p$
 $\Rightarrow p^2 \leq \mu(G/N) \leq p^{n-1}$. But G/N has a element of order p^{n-1} so $\mu(G/N) = p^{n-1}$. As with the last case, $|x| \geq p^{n-1}$, so $\mu(G) \geq p^{n-1}$ and G/N is not distinguished.

Case 4) (Generalized Quaternion) $n \geq 3$, $p = 2$, $G/N = \langle x, y \mid a = 2^{n-2}, x^{2a} = 1, y^2 = x^a \rangle$

This is the exception which we know is a distinguished quotient of the two smallest exceptional groups of order 32.

Case 5) (Dihedral) $n \geq 3$, $p = 2$, $G/N = \langle x, y \mid a = 2^{n-1}, x^a = y^2 = 1, xy = yx^{-1} \rangle$

$\mu(G/N) = 2^{n-1}$, and $|x| \geq 2^{n-1}$ so $\mu(G) \geq 2^{n-1}$ and G/N is not distinguished.

Minimal Permutation Representations

Case 6) $n \geq 4, p = 2, G/N = \langle x, y \mid a = 2^{n-2}, x^{2a} = y^2 = 1, xy = yx^{a+1} \rangle$

$Z(G/N) = \langle x^2 \rangle \cong Z_2^{n-2}$. By example 1 Johnson[9], $\langle y \rangle \cap Z(G/N) = 1 \Rightarrow \mu(G/N)$

$\leq |G/N : \langle y \rangle| = 2^{n-1}$. However, $|x| = 2^{n-1}$ so $\mu(G/N) \geq 2^{n-1} \Rightarrow \mu(G/N) = 2^{n-1}$, and again

$|x| \geq 2^{n-1}$ so $\mu(G) \geq 2^{n-1}$ and G/N is not distinguished.

Case 7) $n \geq 4, p = 2, G/N = \langle x, y \mid a = 2^{n-2}, x^{2a} = y^2 = 1, xy = yx^{a-1} \rangle$

$Z(G/N) = \langle x^2 \rangle \cong Z_2$ so example 1 of Johnson[9] applies and the proof is identical to

Case 6.

On Distinguished Abelian Quotients

As an immediate corollary to Theorem 5.2, we can extend the class of abelian quotients that are never exceptional by:

Corollary 5.3

$Z_p^{n-1} \times Z_p$ is never isomorphic to a distinguished quotient of an exceptional group. That is if $G/N \cong Z_p^{n-1} \times Z_p$ then $\mu(G) \geq \mu(G/N)$.

TOWARDS A CLASSIFICATION OF ALL EXCEPTIONAL P-GROUPS OF ORDER $< p^6$, FOR ODD PRIME p .

We now state and prove the main theorems of this thesis. Research continues on the exceptions listed in the theorem, as it is not known whether an exceptional p -group of order p^5 do exist with a distinguished quotient isomorphic to one of the exceptions.

Theorem 5.4

If G is an exceptional p -group of order $< p^6$, for odd prime p , then G is an extension of a distinguished quotient G/N of order p^4 by a central subgroup N of order p , and G/N is isomorphic to one or the following:

$$1) \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, yz = zy x^p, xy = yx, xz = zx \rangle$$

$$2) \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^p, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$$

$$3) \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^{ap}, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$$

$$4) \langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, xz = zx, xw = wx, yz = zy, \\ yw = wy, zw = wz \rangle$$

Proof:

We proceed by way of contradiction taking cases with the order of G ascending (i.e. groups of order p first, then groups of order p^2 , etc.) That way, we may assume in each case that we have a minimal counter example. Thus G can be taken to be SQ-minimal and N to be elementary abelian, with $\mu(G/N) > \mu(G)$. There are 25 isomorphism classes of p -groups of order

$\leq p^4$, for p -odd but we can reduce the number of cases for p^4 by considering all extensions of quotients of order p^3 by a central subgroup of order p . Similarly for groups of order p^5 , we take all extensions of groups of order p^4 by a central element of order p and extensions of groups of order p^3 by groups of order p^2 which intersect the centre non-trivially. This method is necessary for groups of order p^5 as their isomorphism classes are not readily available. We sometimes consider the isomorphism classes out of order so that we may group similar proofs.

For $|G|=p$, G is simple and so cannot be exceptional. For $|G|=p^2$, G is abelian and so every quotient is isomorphic to a subgroup of G and so G cannot be exceptional.

For $|G|=p^3$, $|G/N|=p^2$ or p , so G/N is cyclic or elementary abelian neither of which can be a distinguished quotient (proven by Easdown and Praeger[4] and Kovacs and Praeger[10] respectively.) $\therefore G$ cannot be exceptional.

For $|G|=p^4$, $|G/N| > p^2$ or G/N is cyclic or elementary abelian, as in the last case.

Thus we can assume $|G/N|=p^3$ and thus G/N is isomorphic to one of the following:

- 1) Z_p^3 ,
- 2) $Z_p^2 \times Z_p$,
- 3) $Z_p \times Z_p \times Z_p$,
- 4) $\langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$, or
- 5) $\langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, zx = xz, zy = yz \rangle$.

However, we can immediately dismiss the cyclic and elementary abelian cases. Also by Lemma A, we know 4) and 2) cannot be distinguished so we are left with 5). For the remaining case, $\mu(G/N) = p^2$. Again N is a normal subgroup and so intersects the centre of G non-trivially; so let

$1 \neq \langle n \rangle \in Z(G) \cap N$. We know $x^p, y^p, z^p \in \langle n \rangle$. If any of x^p, y^p or z^p are not equal to 1 then G has an element of order p^2 and so $\mu(G) \geq \mu(G/N)$, contradicting the assumption that G is exceptional. Since G/N is not a non-trivial direct product, either G is not a non-trivial direct product or $G = \langle x, y, z \rangle \times \langle n \rangle$. In the latter case, G has a subgroup isomorphic to G/N and so is not exceptional. In the former case, G satisfies proposition 3, and we get, $p\mu(Z(G)) \leq \mu(G) \Rightarrow p^2 \leq \mu(G)$ as $\mu(Z(G)) \geq p$, and again G is not exceptional.

For $|G| = p^5$, we have either $|G/N| = p^3$ with $N \cong Z_p \times Z_p$ or $|G/N| = p^4$ with $N \cong Z_p$.

Again we let $1 \neq \langle n \rangle \in Z(G) \cap N$. Suppose $|G/N| = p^3$. Then G/N is of one of five isomorphism types listed immediately above, but with the same argument as for $|G| = p^5$, the only possibility is the fifth type and the argument for this type is the same as above except that $G < \langle x, y, z \rangle \times \langle n \rangle$ instead of the equality.

If $|G/N| = p^4$, then G/N appears as one of the isomorphism types in the main chart at the beginning of this chapter and so we deal with each in turn, omitting the cyclic and elementary abelian cases.

For $G/N \cong Z_p^3 \times Z_p$ or $\langle x, y \mid x^{p^3} = y^p = 1, xy = yx^{p+1} \rangle$, Theorem 5.2 applies so neither quotient is distinguished.

If $G/N \cong G_{12} = \langle x, y \mid x^{p^2} = y^{p^2} = 1, xy = yx \rangle \cong Z_p^2 \times Z_p^2$, both x^{p^2} or y^{p^2} must equal 1 or G would have a cyclic subgroup of order p^3 and $\mu(G) \geq p^3 > p^2 = \mu(G/N)$. Furthermore G must be non-abelian and $\langle n \rangle \leq Z(G)$ so without loss of generality we can take $xy = yxn$; therefore, neither x or y is in $Z(G)$. However, $x^p y = yx^p n^p = yx^p$ and $xy^p = yxny^{p-1} = \dots = y^p x n^p = y^p x$ so $x^p, y^p \in Z(G)$. $\therefore Z(G) = \langle x^p, y^p, n \rangle \cong Z_p \times Z_p \times Z_p$ and Theorem 1.7 applies so that $\mu(G) \geq p\mu(Z(G)) = 3p^3 > 2p^2 = \mu(G/N)$ and G is not exceptional.

For $G/N \cong G_{13} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx, xz = zx, yz = zy \rangle \cong Z_p^2 \times Z_p \times Z_p$, $\mu(G/N) = p^2 + p$. The equation $xy = yx$, would imply $\langle x, y, n \rangle \cong G/N$ so again we can take $xy = yxn$. However, this means $\langle x, y, n \rangle \cong \langle x, y, z, \mid x^{p^2} = y^p = z^p = 1, xy = yxz, yz = zy, zx = xz \rangle$ which has minimal degree $2p^2 > \mu(G/N)$.

For $G/N \cong G_{17} = \langle x, y \mid x^{p^2} = y^{p^2} = 1, xy = yx^{p+1} \rangle$, $\mu(G/N) = 2p^2$. Here we can assume both x^{p^2} and y^{p^2} are 1. Since $xy = yx^{p+1}n^i$ for some i , we get $x^p y = yx^{p(p+1)}n^{ip} = yx^p$ so $x^p \in Z(G)$ and $xy^p = yx^{p+1}n^i y^{p-1} = \dots = y^p x^a n^p$ where $a = (p+1)^p \equiv 1 \pmod{p^2}$ so $xy^p = y^p x$ and $y^p \in Z(G)$. $\therefore Z(G) = \langle x^p, y^p, n \rangle \cong Z_p \times Z_p \times Z_p$ and $\mu(G) \geq p\mu(Z(G)) = 3p^3 > 2p^2 = \mu(G/N)$.

For $G/N \cong G_{18} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, xz = zx, yz = zy \rangle$, $\mu(G/N) = p^2$.

The element x has order at least p^2 so this case is trivial.

For $G/N \cong G_{19} = \langle x, y, z, \mid x^{p^2} = y^p = z^p = 1, xy = yxz, yz = zy, zx = xz \rangle$, $\mu(G/N) = 2p^2$.

Again $x^{p^2} = 1$. If $z^p = 1$ then $xy = yxz$ or $xy = yxzn$ and in either case $x^p y = yx^p$ and $Z_p \times Z_p \cong \langle x^p, n \rangle \leq Z(G)$ so $\mu(G) \geq p\mu(Z(G)) \geq 2p^2$. Therefore, without loss of generality we can assume that $z^p \neq 1$. The commutator $x^{-1}z^{-1}xz \in \langle n \rangle$ so either $\langle x, z \rangle \cong Z_p^2 \times Z_p^2$, or $\langle x, z \rangle = \langle x, z \mid x^{p^2} = z^{p^2} = 1, xz = zx^{p+1} \rangle \cong G_7$ and in either case $\mu(\langle x, z \rangle) = 2p^2 = \mu(G/N)$ so G/N is not distinguished.

For $G/N \cong G_{24} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$, $\mu(G/N) = p^2$. $x^{p^2} = 1$ or else $\mu(G) \geq p^3$. $\therefore \langle x, n \rangle \cong Z_p^2 \times Z_p$ so $\mu(G) \geq p^2 + p > \mu(G/N)$.

For $G/N \cong G_{28} = \langle x, y, z \mid x^9 = y^3 = z^3 = 1, xy = yxz, xz = zx, yz = zx^6y \rangle$, $\mu(G/N) = 27$.

Since this is an actual group, not a family of groups, we were able to use the computer application GAP to determine whether or not G/N could be a distinguished quotient of a group of order 243. There are 67 non-isomorphic groups of order 243, but to be exceptional they must have exponent p^2 or p . This reduce the search to 24 cases. One by one each can be eliminated, because none of the 24 can have G/N as a quotient with $N < Z(G)$.

For $G/N \cong G_{29} = \langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, zy = yzw, xz = zx, zw = wz, xw = wx, yw = wy \rangle$, $\mu(G/N) = p^2$. Since G is a p -group, $|Z(G)| \geq p$ so Theorem 1.7 gives $p^2 \leq p\mu(Z(G)) \leq \mu(G)$. This completes the proof of Theorem 5.4.

We are left with the four possible exceptions to the theorem.

If $G/N \cong G_{16} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, yz = zyx^p, xy = yx, xz = zx \rangle, \mu(G/N) = p^3$.

Theorem 5.1 enables us to dismiss the cases where $Z(G) \cong Z_p^2 \times Z_p$. Theorem 1.7 gives that $Z(G) \neq Z_p^2$. $Z(G) \cong Z_p$ only if $x^{p^2} = 1$, but then G has an element of order p^3 and is not exceptional. $\therefore$ We must have $Z(G) \cong Z_p \times Z_p$.

We also have G/N isomorphic to either $G_{25} = \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^p, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$, or $G_{26} = \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^{\alpha p}, xy = yx^{p+1}, xz = zxy, yz = zy \rangle$ (α is any non-residue mod p).

For $G/N \cong G_{27} = \langle x, y, z, w \mid x^p = y^p = z^p = w^p = 1, xy = yxz, xz = zx, xw = wx, yz = zy, yw = wy, zw = wz \rangle, \mu(G/N) = p^2 + p$. If $Z(G) \neq Z_p$ or $Z_p^2 \times Z_p$ then Theorem 3.5 gives $\mu(G) \geq \mu(G/N)$. If $Z(G) \cong Z_p^2 \times Z_p$, then by Theorem 5.1, $\mu(G) \geq p\mu(Z(G)) = p^3 + p^2 > p^2 + p = \mu(G/N)$. The final possibility is that $Z(G) \cong Z_p$. Note that if $p = 3$, $\mu(G) > p^2$ since $|S_9| = 9!$ is not divisible by $3^5 = |G|$.

Other Exceptional p-groups

By Theorem 2.1, for any fixed odd prime p , direct product of any two groups from $\{ G_7, G_9, G_{15}, G_{16}, G_{24}, G_{25}, G_{28}, G_{29} \}$ is an exceptional group with distinguished quotient isomorphic to the central product. Also the direct product of anyone of these groups with itself is exceptional with distinguished quotient isomorphic to the central product. The following theorem is an extension of Theorem 2.1, with similar proof, which yields the same property for

the smaller set $\{G_{17}, G_{19}\}$.

Theorem 5.6

Suppose p is an odd prime greater than 3, and H, K be non-abelian p -groups with centres $Z_1 = \langle a_1, b_1 \rangle$ and $Z_2 = \langle a_2, b_2 \rangle$ respectively, each centre isomorphic to $Z_p \times Z_p$. Further suppose $\mu(H) = 2p^m$ and $\mu(K) = 2p^n$. Then $H \times K$ is an exceptional group with distinguished quotient isomorphic to the central product $H * K$, and distinguished subgroup $N = \langle (a_1, a_2), (b_1, b_2) \rangle$.

Proof:

First we claim that $G/N = (H \times K)/N$ has centre $(Z_1 \times Z_2)/N = \langle (a_1, 1)N, (b_1, 1)N \rangle = \langle (1, a_2)N, (1, b_2)N \rangle$. Now $(u, v)N \in Z(G/N)$ if and only if, for all $(h, k) \in H \times K$, we have $[(u, v), (h, k)] = ([u, h], [v, k]) \in N$; i.e. for all $(h, k) \in H \times K$ there are integers i, j for which $[u, h] = (a_1)^i(b_1)^j$ and $[v, k] = (a_2)^i(b_2)^j$. Taking $k = 1$ gives $[u, h] = 1$, for all $h \in H$ and taking $h = 1$ gives $[v, k] = 1$ for all $k \in K$, thus proving the claim.

Thus G/N also has centre isomorphic to $Z_p \times Z_p$ and so, by Theorem 1.5, we have $\mu(G/N) = p^c + p^d$ for some integers c and d .

We can assume $\mu(H) \geq \mu(K)$. Since K is not cyclic, Gorenstein [5] Theorem 5.4.10, implies that K has a subgroup $X = \langle x \rangle \neq 1$ such that $X \cap Z_2 = 1$. Then $H \times X \cong (H \times X)N/N \leq G/N$ so that $\mu(G/N) \geq \mu(H \times X) = \mu(H) + \mu(X)$ by Wright [11] Theorem 2. Thus $\mu(G/N) > \mu(H)$ so we have $p^c + p^d > 2p^m$.

If $c = d$, we get $2p^c > 2p^m$ which implies $\mu(G/N) = 2p^c \geq 2pp^m > 4p^m \geq \mu(G)$. Otherwise, we may assume $c > d$. Then $p^c > 2p^m - p^d$. If $d \leq m$, then $p^c > p^m$ which implies $\mu(G/N) > p^c \geq pp^m > 4p^m \geq \mu(G)$ since $p > 3$. If $d > m$ then $c > d$ gives $2p^d > 2p^m$ which again implies $\mu(G/N) = 2p^c \geq 2pp^m > 4p^m \geq \mu(G)$. Therefore $\mu(G/N) > \mu(G)$ and G is exceptional.

As a direct result of Theorem 5.6, the following direct products are exceptional:

$G_{17} \times G_{17}$, $G_{17} \times G_{19}$ and $G_{19} \times G_{19}$, with distinguished quotients the central products $G_{17} * G_{17}$, $G_{17} * G_{19}$ and $G_{19} * G_{19}$, respectively for $p > 3$.

Thus, in this chapter we have extended used Johnson's[9] algorithm to find the minimal degrees of faithful permutation representations of finite p -groups of order $\leq p^4$ as well as extend the algorithm to cover groups of order p^5 , where p is an odd prime. We also extended the work being done to determine if abelian quotients can ever be distinguished, by showing that if the quotient is of the form $Z_p^a \times Z_p$, then the it is not distinguished. Finally our attempt to classify exceptional p -groups of order p^5 , where p is odd, has severely limited the possible isomorphism classes of exceptional groups, by limiting the possible distinguished quotients to 4 isomorphism classes.

BIBLIOGRAPHY

- [1] W. Burnside, Theory of Groups of Finite Order. Dover Publications Inc., 1911.
- [2] John Cossey, "Quotients of Permutation Groups". Math. Research Report No. MRR 051-97.
- [3] David Easdown, "Minimal Faithful Permutation and Transformation Representations of Groups and Semigroups". Contemporary Mathematics, Vol. 131 (1992), part 3, 75-84.
- [4] David Easdown and Cheryl E. Praeger, "On Minimal Faithful Permutation Representations of Finite Groups". Bulletin Australian Mathematical Society, Vol. 38 (1988), 207-220.
- [5] Daniel Gorenstein, Finite Groups. Harper and Row, New York, 1968.
- [6] Marshall Hall Jr., The Theory of Groups. Macmillan Company, New York, 1959.
- [7] D. F. Holt, "Representing Quotients of Permutation Groups". Quarterly Journal Of Mathematics, Vol. 48 (1997), No. 2, 347-350.
- [8] D. L. Johnson, "A Note on Supersoluble Groups". Canadian Journal of Mathematics, Vol. 23 (1971), No. 3, 562-564.
- [9] D. L. Johnson, "Minimal Permutation Representations of Finite Groups". American Journal of Mathematics, Vol 93 (1971), 857-866
- [10] L. G. Kovacs and Cheryl E. Praeger, "Finite Permutation Groups with Large Abelian Quotients". Pacific Journal of Mathematics, Vol. 136 (1989), No. 2, 283-292.
- [11] D. Wright, "Degrees of Minimal Embeddings for some Direct Products". American Journal Of Mathematics, Vol. 97 (1976), 897-903.