On Minimal Degrees of Faithful Permutation Representations of Finite Groups

by

Simo Sisize Mthethwa

Submitted in fulfilment of the academic

requirements for the degree of

Master of Science

in the

School of Mathematics, Statistics and Computer Science

University of KwaZulu-Natal

Durban

October 2014

Dedicated to the memory of:

my late mom Bakhethile and my late daughter Zee.

Abstract

The minimal faithful degree of a finite group G, denoted by $\mu(G)$, is the smallest non-negative integer n, such that G is isomorphic to a subgroup of S_n, the symmetric group on n symbols. We study the minimal faithful degrees of certain classes of finite groups and the additivity property of μ in relation to a direct product of finite groups. Concrete examples will be provided on how to calculate $\mu(G)$, for various classes of finite groups. It is not difficult to show that if H is a subgroup of G, then $\mu(H) \leq \mu(G)$. However, if N is a normal subgroup of G, it is possible to have $\mu(G/N) > \mu(G)$. If the latter holds, we call G an exceptional group, N and G/N are called distinguished subgroup and distinguished quotient, respectively. We investigate the extent to which certain classes of groups satisfy the exceptionality property. In the particular case of p-groups (i.e., groups of order p^n, where p is prime and n is a positive integer), for p^5, we provide examples of exceptional and non-exceptional p-groups. Conditions under which a quotient group of a finite group is distinguished will also be explored.

Preface and declaration

The study described in this dissertation was carried out in the School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Durban. This dissertation was completed under the supervision of Professor Bernardo Gabriel Rodrigues from February 2013 to October 2014. The research contained in this dissertation represents original work by the author and has not been submitted in any form to another University nor has it been published previously. Where use was made of the work of others it has been duly acknowledged in the text.

Name:_____ Signature:_____Date:_____

As the candidate's supervisor I have approved this dissertation for submission.

Name:_____ Signature:_____Date:_____

Acknowledgements

I wish to express my sincere gratitude to the following people and organisations who made this dissertation possible:

- Firstly, I would like to thank God for his guidance and help in giving me the strength and courage to complete this study.
- My supervisor Prof. Bernardo Gabriel Rodrigues for his immense support, guidance and encouragement to do this work to the best of my ability. He has been a great mentor and an inspiration to me and his useful advice and constructive criticisms are gratefully appreciated.
- Prof. James Raftery for his unending support. He has been my role model and idol since my undergraduate studies, and still is.
- Prof. Peter Dankelmann for taking his precious time to translate a number of proofs and results in [17] from German to English in a very short space of time.
- My fellow colleague, Mr. Tendai Shumba Mudziiri for helpful discussions on groups, especially p-groups.

- The National Research Foundation for financial assistance through the award of a DST Innovation Masters Scholarship for the year of 2013.
- The school of Mathematics, Statistics and Computer Science for providing me with an academic-friendly environment to do my work.

Glossary of symbols, notation and conventions

G, H, K, N, Q	finite or infinite groups
1_G	the identity element of G
$H \leq G$	H is a subgroup of G
$H < G$	H is a proper subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
$N \triangleleft G$	N is a proper normal subgroup of G
G/N	the factor or quotient group of G by N
$[G : H]$	index of H in G
$G \cong H$	G is isomorphic to H
$\mathsf{ker}\rho$	the kernel of the homomorphism ρ
$\mathsf{Im}\rho$	the image of the homomorphism ρ
$\langle x, y \rangle$	the subgroup generated by x and y
$\mathsf{Aut}(G)$	the automorphism group of G
x^y	conjugation of x by y
$o(g)$	order of g in G
$o(G), \lvert G \rvert$	order of G

$N_G(H)$	the normalizer of the subgroup H in G
$Z(G)$	the centre of G
$Syl_p(G)$	the set of all Sylow p-subgroups of G
$\Phi(G)$	the Frattini subgroup of G
G'	the commutator subgroup of G
gH	the left coset of H in G
X, Y	sets
$X \subseteq Y$	X is a subset of Y
$X \subset Y$	X is a subset of Y and $X \neq Y$
$\emptyset$	empty set
$\|X\|$	the cardinality of the set X
$(\|X\|, \|Y\|)$	the greatest common divisor of $\|X\|$ and $\|Y\|$
D_{2n}	dihedral group of order $2n$
Q_{2^n}	generalised quaternion of order 2^n
V_4	the Klein 4-group
C_n	cyclic group of order n
S_n	the symmetric group on n symbols
S_G	the symmetric group on G
A_n	the alternating group on n symbols
$x \equiv y(modz)$	x is congruent to y modulo z

Contents

Chapter 1

Introduction

In this dissertation, we investigate minimal degrees of faithful permutation representations of finite groups, for various classes of finite groups. That is, we seek for a smallest integer n such that G is embedded into a symmetric group S_n, and we denote n by $\mu(G)$. The study of this topic is one of the classical areas of finite group theory. This subject is largely motivated by Cayley's Theorem which states that every group G is isomorphic to a subgroup of the symmetric group. As a result of Cayley's Theorem, a natural question arose: when G is finite, can a smallest symmetric group in which G is embedded be found? This is an extremely hard question to address when the structure of a finite group G is not known. Hence, we consider different classes of finite groups and deal with each case according to the structure of the group.

In Chapter 2, an introduction to morphisms of groups and permutation representations of groups is given. Well-known content on group actions is provided and the correspondence between group actions and permutation representations is furnished. As a result of the latter, an equivalent defini-

tion of $\mu(G)$ is provided through a correspondence between a group action on a finite set and group action on a set of left cosets for a collection of subgroups of G.

Chapter 3 is devoted to the study of the behaviour of the degree of a minimal faithful representation with respect to a direct product of finite groups. The work in [20] and [36] respectively, constitute the earliest instances in which the question on the conditions under which the degrees of faithful permutation representations are minimal. Within the work done by the authors in [20] and [36], is the investigation of the conditions under which the minimal degree of a faithful permutation representation of a direct product is equal to the sum of the minimal degrees of faithful permutation representations of the direct factors. We provide a self-contained and detailed account of the results of the investigation by the authors in [20] and [36] which will be relevant for the work in this dissertation.

In Chapter 4, different classes of finite groups for which Cayley's Theorem and its proof give rise to a minimal degree, are provided. These classes consist of the cyclic groups of prime-power order, the generalised quaternion 2-groups and Klein 4-groups. The proof that these classes are the only ones with this property was sketched by the author in [20]. A more detailed account of this work and original proofs are provided in this dissertation. In addition, different methods to calculate minimal degrees of faithful permutation representations for various classes of finite groups are used. Some minimal degrees are found directly, while other minimal degrees are found through group action and from the structure of a subgroup lattice of a finite group.

Certainly, $\mu(H) \leq \mu(G)$, for every subgroup H of G. Intuitively, if H and G are finite groups such that $|H| \leq |G|$, we would expect $\mu(H)$ to be less

than or equal to $\mu(G)$. However, this is not the case in general. For, if $N \lhd G$, it is possible to have $\mu(G/N) > \mu(G)$ regardless of the fact that $|G/N| = |G|/|N| \leq |G|$. If $N \lhd G$ and $\mu(G/N) > \mu(G)$, we call G an exceptional group. In Chapter 5, we explore the research carried thus far with regards to the exceptional groups. The work done in [7], [9], [21], [22], [24] and [25] with respect to exceptional groups is reported with more attention to the case where the finite group G is of prime power order. Self-contained and independent proofs of the results found by the authors of the above mentioned articles are provided.

Chapter 2

Preliminaries and background

The main aim of this chapter is to provide standard results from the theory of groups which will be used throughout the dissertation. Most of the results could be found in standard text books such as [5], [6], [10], [11], [12], [14], [23], [29], [30] and [31]. We provide only the proofs of those results that may be of use in the sequel, as most can be found in the relevant literature.

2.1 Morphisms of groups

Definition 2.1.1. *Let G and H be groups. A map $\rho : G \to H$ is said to be a* ***homomorphism*** *if $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$. If in addition ρ is bijective, it is said to be an* ***isomorphism****. If there is an isomorphism from G to H we say that G and H are* ***isomorphic*** *and we write $G \cong H$. An* ***automorphism*** *of G is an isomorphism from G to G.*

A homomorphism may be injective but not onto and viceversa.

Definition 2.1.2. *Let G and H be groups. If there is an injective homomorphism $\rho : G \to H$, we say that G is* ***embedded*** *in H. If there is an onto homomorphism $\rho : G \to H$, we say that H is a* ***homomorphic image*** *of G.*

2.2 Permutation representations

Cayley's Theorem asserts that every group can be embedded in a permutation group. It particularly states that every finite group of order n is isomorphic to a subgroup of S_n, the symmetric group on n symbols, which is really a permutation group. Below, we present Cayley's Theorem which guarantees the existence of a homomorphism from any given group to a permutation group.

Theorem 2.2.1. *Let G be a group. Then G is isomorphic to a subgroup of S_G. In particular, if the order of G is n, then G is isomorphic to a subgroup of S_n.*

Proof. For each $g \in G$, define a bijection ρ_g as follows,

$$\rho_g : G \to G$$
$$\rho_g(x) = gx,$$

for all $x \in G$. Let $g \in G$, then ρ_g is a well defined injection, since for any $x, y \in G$, $x = y \Leftrightarrow gx = gy \Leftrightarrow \rho_g(x) = \rho_g(y)$. It is onto, because if $x \in G$, then $\rho_g(g^{-1}x) = g(g^{-1}) = (gg^{-1}) = 1_G x = x$, for each $g \in G$, where 1_G is the identity element of G. Thus for each $x \in G$, we obtain $\rho_g \in S_G$. Now, define a function ρ as follows,

$$\rho : G \to S_G$$
$$\rho(g) = \rho_g,$$

for all $x \in G$. For any $g, h \in G$, suppose $\rho(g) = \rho(h)$, i.e., suppose $\rho_g = \rho_h$. The latter implies that $\rho_g(x) = \rho_h(x)$, for every $x \in G$. Therefore $gx = hx$. In particular, $g = g1_G = h1_G = h$. This proves that ρ_g is injective. Note that for every $g, h \in G$, and for each $x \in G$, we have

$$(\rho_g \circ \rho_h)(x) = \rho_g(\rho_h(x)) = \rho_g(hx) = g(hx) = (gh)x = \rho_{gh}(x),$$

which implies $\rho(gh) = \rho(g)\rho(h)$. Thus ρ is a homomorphism and so $G \cong \mathsf{Im}\rho \leq S_G$. For finite groups, the result follows by choosing $|G| = n$. This completes the proof. □

Motivated by Theorem 2.2.1 we define the concept of permutation representation of a group.

Definition 2.2.1. *Let G be a finite group and X be a non-empty finite set. A* ***permutation representation*** *of G on X is defined to be a homomorphism*

$$\rho : G \to S_X.$$

If $g \in G$, write ρ_g for $\rho(g) \in S_X$ (so that $\rho_g : X \to X$ is bijection). We sometimes write gx for $\rho_g(x)$. In the case where ρ is injective, we call ρ a ***faithful permutation representation****. The size of the set X is called the* ***degree*** *of the permutation representation ρ.*

Remark 2.2.1. For finite groups, Cayley's Theorem gives the existence of a permutation representation, but it does not guarantee the minimality of the degree of the permutation representation. That is, for a finite group G, the statement of Cayley's Theorem and its proof may or may not produce the smallest symmetric group in which G can be embedded. To illustrate this, take G to be A_5, the alternating group on 5 symbols. Cayley's Theorem

asserts that G is a subgroup of $S_{|G|} = S_{5!/2} = S_{60}$. But we know that $G \leq S_5$ and 5 is much less than 60. So, to find a permutation representation of smallest degree, Cayley's Theorem is not always efficient.

From Cayley's Theorem and Remark 2.2.1, it seems to be a plausible task to search for a permutation representation of smallest degree for various classes of finite groups.

Definition 2.2.2. *The homomorphism τ in Theorem 2.2.1 is called the* ***left regular representation*** *of G.*

Definition 2.2.3. *Let X be a non-empty set and G be a group. An* ***action*** *of G on X is a map $\sigma : G \times X \to X$ such that:*

(i) $\sigma(1_G, x) = x$, *for all* $x \in X$, *and*

(ii) $\sigma(h, \sigma(g, x)) = \sigma(hg, x)$, *for all* $x \in X$ *and for all* $g, h \in G$. *If σ is a one-to-one map then σ is said to be a* ***faithful action****.*

Remark 2.2.2. For calculation purposes and if there is no confusion, we sometimes suppress the action and write gx for $\sigma(g, x)$. In this way, the first condition Definition 2.2.3 could be written as $1_G x = x$, for all $x \in X$. The second condition being written as $h(gx) = (hg)x$, for all $x \in X$ and for all $g, h \in G$. The first condition of Definition 2.2.3 demands the identity element of G to fix all the elements of X, thus behaving the same as the identity element of any permutation group. The second condition states that: applying two elements of G in a sequence is the same as applying their product to the elements of X, which is the case with elements of any permutation group: applying two bijections in a sequence is the same as applying their composition. This is the reason why we always consider group

action as a way of letting the elements of a group permute the elements of a set in which the group is acting.

Definition 2.2.4. *Let σ be an action of G on X. We define the* ***orbit containing*** *x by $Orb_x(G) := \{gx \mid g \in G\}$.*

It is not difficult to show that two orbits are either equal or disjoint.
The correspondence between group action and permutation representation is described in the following theorem.

Theorem 2.2.2. *If $\rho : G \to S_X$ is a permutation representation of G on X, then there exists an action σ of G on X corresponding to ρ. Conversely, if G acts on a non-empty set X, then there exists a permutation representation $\rho : G \to S_X$ corresponding to this action.*

Proof. Let $\rho : G \to S_X$ be a permutation representation of G on X and identify the image of any $g \in G$ by ρ_g in S_X. So, $\rho_g \in S_X$ and ρ_g is a permutation on the set X. For each $g \in G$, define an action σ of G on X as follows,

$$\sigma : G \times X \to X$$
$$\sigma(g, x) = \rho_g(x),$$

for all $x \in X$. Clearly, $\sigma(1_G, x) = \rho_{1_G}(x) = 1_{S_X}(x) = x$. Also, if $g, h \in G$ and $x \in X$, then

$$\sigma(h, \sigma(g, x)) = \sigma(h, \rho_g(x)) = \rho_h(\rho_g(x)) = \rho_{hg}(x) = \sigma(hg, x),$$

i.e., σ is an action of G on X.
Conversely suppose that we have an action σ of G on X. We show that each $g \in G$ induces a permutation representation of G on X. Define ρ as follows,

$$\rho : G \to S_X$$
$$\rho(g) = \rho_g,$$

for all $g \in G$, where ρ_g is given as follows: for each $g \in G$ and for all $x \in X$,

$$\rho_g : X \to X$$
$$\rho_g(x) = \sigma(g, x) := gx.$$

Clearly, $\rho_{1_G}(x) = \sigma(1_G, x) = x$ (because σ is an action). Thus ρ_{1_G} is nothing but 1_{S_X}, the identity map. Again, using the definition of ρ_g and the fact that σ is an action we get

$$\rho_g(\rho_{g^{-1}}(x)) = \rho_g(g^{-1}x) = gg^{-1}x = 1_G x = x.$$

This implies that $\rho_g \rho_{g^{-1}} = 1_{S_X}$. Therefore $\rho_{g^{-1}} = (\rho_g)^{-1}$. This calculation proves that ρ_g is one-to-one because ρ_g has an inverse for each $g \in G$. The onto part of ρ_g is trivial because $x = \sigma(x, 1_G) = \rho_{1_G}(x)$, for all $x \in X$. Thus ρ_g is a permutation on the set X. We now show that $\rho : G \to S_X$ is a homomorphism. Take $g, h \in G$, then for each $x \in X$, we have

$$\rho_g(\rho_h(x)) = \rho_g(hx) = g(hx) = (gh)x = \sigma(gh, x) = \rho_{gh}(x).$$

Thus $\rho_g \rho_h = \rho_{gh}$, for all $g, h \in G$. This implies that $\rho(gh) = \rho(g)\rho(h)$, for all $g, h \in G$ and hence ρ is a homomorphism. □

Theorem 2.2.2 establishes the relationship between group action and permutation representation. In short: if we have a permutation representation we can construct a group action and vice-versa. We now explore the equivalence of permutation representations of a group on different sets.

Definition 2.2.5. *Suppose $\rho : G \to S_X$ and $\sigma : G \to S_Y$ are two permutation representations of G on the sets X and Y, respectively. Identify the image of $g \in G$ under ρ by ρ_g in S_X, also identify by σ_g, the image of g*

under σ in S_Y. Then ρ and σ are said to be ***equivalent*** *if there exists a bijection $\tau : X \to Y$ such that*

$$\tau(\rho_g(x)) = \sigma_g(\tau(x)),$$

for all $x \in X$ and for $g \in G$.

Figure 1 illustrates the idea given in Definition 2.2.5 diagrammatically.

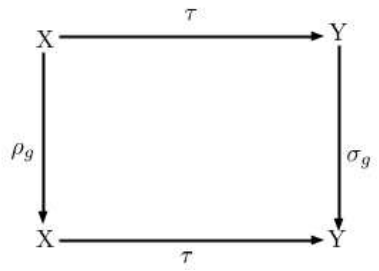

Figure 1

That is, ρ and σ are equivalent if the diagram above commutes, i.e., $\tau\rho_g = \sigma_g\tau$. In Definition 2.2.5 we have two permutation representations of the same group. We now extend to n permutation representations, where $n \in \mathbb{N}$ in the following remark.

Remark 2.2.3. Let $1 \leq i \leq n$, and suppose that for each i, $\rho^i : G \to S_{X_i}$ ($\rho^i(g) = \rho^i_g$) is a permutation representation such that $X_i \bigcap X_j = \emptyset$ for each $i \neq j$. For each $g \in G$, define

$$\bigoplus_{i=1}^{n} \rho^i : G \to S_{\biguplus_{i=1}^{n} X_i}$$

by

$$(\bigoplus_{i=1}^{n} \rho^i)(g) = [\bigoplus_{i=1}^{n} \rho^i]_g$$

where $[\bigoplus_{i=1}^{n} \rho^i]_g : \biguplus_{i=1}^{n} X_i \to \biguplus_{i=1}^{n} X_i$ is defined by $[\bigoplus_{i=1}^{n} \rho^i]_g(x) = \rho_g^i(x)$ whenever $x \in X_i$. Observe that $\bigoplus_{i=1}^{n} \rho^i$ is a permutation representation by definition, since each ρ^i is a permutation representation. Also, $\bigoplus_{i=1}^{n} \rho^i$ is faithful if and only if each ρ_i is faithful for each i. Thus $\bigoplus_{i=1}^{n} \rho_i$ is faithful if and only if $\bigcap_{i=1}^{n} \mathsf{ker}\rho^i = \{1_G\}$.

As pointed out in Remark 2.2.3, a direct sum of permutation representations is a permutation representation. The converse is true if we impose some condition on the permutation representations in the direct sum. To achieve this condition we need to define a new concept.

Definition 2.2.6. *Let $\rho : G \to S_X$ be a permutation representation of a group G on X. We say ρ is **transitive** if for all $x, y \in X$, there exits $g \in G$ such that $\rho_g(x) = y$. That is, if for every $x, y \in X$, there exists $g \in G$ such that $gx = y$. We say G **acts transitively** on X.*

Theorem 2.2.3. *Let σ be an action of G on X. Define a relation R on X by xRy if and only if for all $x, y \in X$, there exists $g \in G$ such that $gx = y$. Then R is an equivalence relation on X.*

Proof. For all $x \in X$, we have $1_G x = x$, since σ is an action. So, xRx for all $x \in X$. This proves that the relation is reflexive.
Let $x, y, z \in X$ and suppose xRy. We therefore have $gx = y$ for some $g \in G$. Observe that $g^{-1}y = g^{-1}gx = 1_G x = x$, so yRx. This proves the symmetry of the relation.
If xRy and yRz, then $gx = y$ and $hy = z$ for some $g, h \in G$. We now have $(hg)x = h(gx) = hy = z$, so xRz. This proves the transitivity of the relation R. □

Remark 2.2.4. If G acts on X, then $x \in Orb_x(G)$ and G acts transitively

on $Orb_x(G)$ for all $x \in X$. Also, X is partitioned into disjoint equivalence classes with respect to the equivalence relation R in Theorem 2.2.3. The equivalence classes under the relation R are orbits of the action σ. From Theorem 2.2.3 and Definition 2.2.4, we observe that the action is transitive if and only if there is exactly one orbit. It is worth noting that the action corresponding to the transitive permutation representation in the sense of Theorem 2.2.2 is also transitive and viceversa.

Theorem 2.2.4. *The centre of any finite group G is a union of all the conjugacy classes of G that consists of one element with respect to the action $\alpha : G \times G \to G$ defined by $\alpha(g, x) = x^g = gxg^{-1}$.*

Proof. First note that the conjugacy class of an element $x \in G$ is the set $[x] := \{x^g \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$. So, conjugacy classes partition G into disjoint union of orbits under the action of α. Observe that $x \in [x]$ for all $x \in G$ as $x = (1_G)x(1_G)^{-1}$. Also note that $[1_G] = \{1_G\}$. Since for each $x \in G$, we have $x \in Z(G)$ if and only if $gx = xg$ for all $g \in G$, it follows that $x \in Z(G)$ if and only if $x = gxg^{-1}$ for all $g \in G$. So, $x \in Z(G)$ if and only if $[x] = \{x\}$, and the result follows.

□

Recall that the permutation representation is said to be finite if the set permuted is finite. The following theorem is of fundamental importance in the study of permutation representations.

Theorem 2.2.5. *Every finite permutation representation is a direct sum of transitive permutation representations.*

Proof. Let $\rho : G \to S_X$ be a permutation representation where X is finite. Then by Theorem 2.2.2, we have a corresponding action σ of G on X. Since

the action partitions the set X into disjoint union of orbits, we have $X = \biguplus_i^n Orb_{x_i}(G)$. Now G acts transitively on each $Orb_{x_i}(G)$. Thus for each i we have a transitive action σ_i of G on $Orb_{x_i}(G)$. From each σ_i, we get a transitive permutation representation ρ_i, by Theorem 2.2.2. Take $\bigoplus_{i=1}^n \rho_i$ to be the desired direct sum. □

Theorem 2.2.5 tells us that, to understand general permutation representations, it is enough to study transitive permutation representations as they are building blocks of the general permutation representations.

2.3 Permutation representations by acting on the cosets

We can construct a permutation representation of any finite group G by letting G act on the cosets of any subgroup H. We are going to let G act on left cosets and we point out that the same can be done to the right cosets (this can be achieved by defining $\rho_g : X \to X$ by $\rho_g(Hx) = Hxg^{-1}$ in Theorem 2.3.1 below). The construction is simple and presented in the following theorem.

Theorem 2.3.1. *Let H be a subgroup of a group G and let $X = G/H$, where $G/H := \{xH \mid x \in G\}$. Then there is a transitive permutation representation $\rho : G \to S_X$, such that $\ker\rho = \bigcap_{g\in G} gHg^{-1}$.*

Proof. For $g \in G$, define $\rho_g : X \to X$, by $\rho_g(xH) = gxH$, for all $x \in G$. It is clear that ρ_g is well defined, one-to-one and onto, i.e, $\rho_g \in S_{G/H}$. Define $\rho : G \to S_X$ by $\rho(g) := \rho_g$, for all $g \in G$. Then ρ is a homomorphism because for each $x \in G$, we have

$$\rho_g(\rho_h(xH)) = \rho_g(hxH) = g(hxH) = (gh)xH = \rho_{gh}(Hx),$$

for every $g, h \in G$. This implies that $\rho(g)\rho(h) = \rho(gh)$ for all $g, h \in G$. Hence ρ is a homomorphism and consequently a permutation representation of G. We also have

$$\begin{aligned} ker\rho &= \{x \in G \mid \rho(x) = 1_{S_X}\} \\ &= \{x \in G \mid \rho_x = 1_{S_{G/H}}\} \\ &= \{x \in G \mid xgH = gH, \text{ for all } g \in G\} \\ &= \{x \in G \mid g^{-1}xgH = H, \text{ for all } g \in G\} \\ &= \{x \in G \mid g^{-1}xg \in H, \text{ for all } g \in G\} \\ &= \{x \in G \mid x \in gHg^{-1}, \text{ for all } g \in G\} \\ &= \bigcap_{g \in G} gHg^{-1}. \end{aligned}$$

It remains to show that ρ is a transitive permutation representation. Now take $xH, yH \in X$. We show that there exists an element $g \in G$, such that $\rho_g(xH) = yH$. Recall that two cosets are either equal or disjoint. If $xH = yH$, then we can take g to be 1_G and we are done. If $xH \neq yH$ then $xH \bigcap yH = \emptyset$. We need $g \in G$ such that $gxH = yH$. If we choose $g = yx^{-1}$, then $gxH = (yx^{-1})xH = yx^{-1}xH = yH$ as desired. □

Definition 2.3.1. *The kernel of ρ in Theorem 2.3.1 is called the* ***core*** *of H in G, and it is abbreviated as $core_G(H)$. If $core_G(H) = \{1_G\}$, then H is said to be* ***core-free****.*

The following lemma will be used of it in the remark that follows and throughout this dissertation.

Lemma 2.3.2. *Let H and K be subgroups of a group G. Then*

$$core_G(H \bigcap K) = core_G(H) \bigcap core_G(K).$$

Proof. Let $x \in core_G(H \bigcap K)$. Then $x \in \bigcap_{g\in G} g(H \bigcap K)g^{-1}$. So, for all $g \in G$, $x = gyg^{-1}$ for some $y \in H \bigcap K$. The fact that $y \in H$ and $y \in K$ implies that $x \in \bigcap_{g\in G} gHg^{-1}$ and $x \in \bigcap_{g\in G} gKg^{-1}$. That is, $x \in core_G(H)$ and $core_G(K)$. Hence $x \in core_G(H) \bigcap core_G(K)$ and so

$$core_G(H \bigcap K) \subseteq core_G(H) \bigcap core_G(K).$$

Now, let $x \in core_G(H) \bigcap core_G(K)$. That is, $x \in core_G(H)$ and $x \in core_G(K)$. Therefore $x \in \bigcap_{g\in G} gHg^{-1}$ and $x \in \bigcap_{g\in G} gKg^{-1}$. So, for all $g \in G$, we have $x = ghg^{-1}$ and $x = gkg^{-1}$, for some $h \in H$ and $k \in K$. We equate and get $ghg^{-1} = gkg^{-1}$,this implies that $h = k$. Whence h is an element of both H and K. Consequently, for all $g \in G$, we have $x = ghg^{-1}$, for some $h \in H \bigcap K$. We now have $x \in \bigcap_{g\in G} g(H \bigcap K)g^{-1}$, i.e., $x \in core_G(H \bigcap K)$ and so

$$core_G(H) \bigcap core_G(K) \subseteq core_G(H \bigcap K)$$

and hence the result. □

Remark 2.3.1. Let $\mathcal{H} = \{H_i\}_{i=1}^n$ be a collection of subgroups of a group G. As in Theorem 2.3.1, for each $g \in G$, define

$$\rho_g^i : G/H_i \to G/H_i, \text{ by}$$

$$\rho_g^i(x_iH_i) = gx_iH_i,$$

for each $i \in \{1, \ldots, n\}$. Then $\mathcal{H} = \{H_i\}_{i=1}^n$ induces a transitive permutation representation

$$\rho : G \to S_{G/H_1} \times \cdots \times S_{G/H_n},$$

defined by

$$\rho(g) = (\rho_g^1, \ldots, \rho_g^n)$$

for all $g \in G$. The permutation representation ρ is faithful if and only if $\mathsf{ker}\rho_g^i = \{1_G\}$, for each $i \in \{1, \ldots, n\}$. This implies that ρ is faithful if and only if $core(\mathcal{H}) := \bigcap_{i=1}^n core_G(H_i) = core_G(\bigcap_{i=1}^n H_i) = \{1_G\}$. The fact that ρ is transitive is a direct consequence of the fact that each $\rho_i : G \to S_{G/H_i}$ defined by $\rho_i(g) = \rho_g^i$ is transitive by Theorem 2.3.1.

Not only the subgroups induce a transitive permutation representation, a weak converse is also valid, i.e., any transitive permutation representation is equivalent to some permutation representation induced by some special type of subgroups. We define these types of subgroups below.

Definition 2.3.2. *Let σ be an action of a group G on some set X. Fix $x_0 \in X$. The **stabiliser of the point** x_0 is the set*

$$G_{x_0} := \{g \in G \mid gx_0 = x_0\}.$$

Theorem 2.3.3. *Let G be a finite group and X a set. Let $\sigma : G \to S_X$ be a transitive permutation representation of G on X. Then σ is equivalent to a permutation representation by left multiplication on the left cosets of some subgroup of G, as in Theorem 2.3.1.*

Proof. Let $x_0 \in X$ be fixed. Let $H := G_{x_0}$. That is, H is the stabiliser of the point x_0. Identify $\sigma(g)$ by σ_g for all $g \in G$. Since σ is transitive on X, then for all $x \in X$, there exists $g \in G$ such that $\sigma_g(x_0) = x$. Now define τ as follows,

$$\tau : X \to G/H$$

$$\tau(x) = gH,$$

for all $x \in X$, where $g \in G$ such that $\sigma_g(x_0) = x$. We need to show that τ is a bijection that obeys the condition in Definition 2.2.5. We start by proving that τ is a one-to-one function. For this, let $x, y \in X$. By transitivity of σ, there exists $g_1, g_2 \in G$ such that $\sigma_{g_1}(x_0) = x$ and $\sigma_{g_2}(x_0) = y$. Suppose $\tau(x) = \tau(y)$. That is, suppose $g_1H = g_2H$. This implies that $g_2^{-1}g_1H = H$. Therefore $g_2^{-1}g_1 \in H$. Thus, there exists $h \in H$ such that $g_2^{-1}g_1 = h$, so that $g_1 = g_2h$. Note that $\sigma_h(x_0) = x_0$, since $h \in H$. Thus, we have

$$x = \sigma_{g_1}(x_0) = \sigma_{g_2h}(x_0) = \sigma_{g_2}(\sigma_h(x_0)) = \sigma_{g_2}(x_0) = y,$$

and so τ is one-to-one. The function τ is onto because if $Y \in G/H$ then $Y = gH$ for some $g \in G$. If we chose $x = \sigma_g(x_0)$, we then have $\tau(x) = gH$. Now, we have $\sigma : G \to S_X$ and by Theorem 2.3.1 we have $\rho : G \to S_{G/H}$, which is a transitive permutation representation on the left coset by left multiplication. We need to show that σ and ρ are equivalent, τ being the required bijection. This means that we need to show that $\tau(\sigma_g(x)) = \rho_g(\tau(x))$, for all $x \in X$, and for all $g \in G$. That is, we want to show that the following diagram commutes:

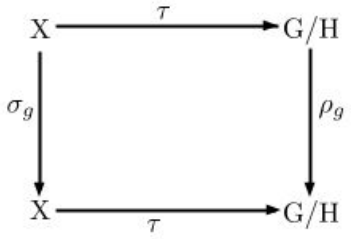

Figure 2

For this, let $x \in X$. We now have $x, x_0 \in X$. Let $g \in G$, then $\tau(\sigma_g(x)) = \tau(\sigma_g(\sigma_{g_1}(x_0))) = \tau(\sigma_{gg_1}(x_0)) = gg_1H = g(g_1H) = \rho_g(g_1H) = \rho_g(\tau(x))$. Whence $\tau(\sigma_g(x)) = \rho_g(\tau(x))$, as desired. □

2.4 The degree of a minimal faithful permutation representation

In Remark 2.3.1 we observed that a collection $\mathcal{H} = \{H_i\}_{i=1}^n$ of subgroups of a group G induces a permutation representation. If $\rho : G \to S_X$ is a finite permutation representation, then $\rho = \bigoplus_{i=1}^n \rho_i$, where each ρ_i is transitive, by Theorem 2.2.5. However Theorem 2.3.3 asserts that ρ_i is equivalent to some permutation representation $\rho^{(i)} : G \to S_{G/H_i}$ on the left cosets by left multiplication, where each H_i is chosen to be $G_{x_{i_0}}$, the stabiliser of a point $x_{i_0} \in G/H_i$. Thus the collection $\mathcal{H} = \{H_i\}_{i=1}^n$ of subgroups yields the transitive summands ρ_i. This correspondence between permutation representations and the collections of subgroups permits us to refer to such collections of subgroups as permutation representations. We make some conventions based on this discussion in the following definition.

Definition 2.4.1. *If $\mathcal{H} = \{H_i\}_{i=1}^n$ is a collection of subgroups of a group G yielding the transitive summands of the permutation representation of G, we then refer to $\mathcal{H}$ as a **permutation representation** of G, or just a **representation** of G. We call each $H_i \in \mathcal{H}$ a **transitive constituent** of a permutation representation $\mathcal{H}$. We say $\mathcal{H}$ is **faithful** if and only if*

$$core_G(\mathcal{H}) := \bigcap_{i=1}^n core_G(H_i) = core(\bigcap_{i=1}^n H_i) = \{1_G\}.$$

*We say that $\mathcal{H}$ is **regular** (or **Cayley**) if $\mathcal{H} = \{1_G\}$, and $\mathcal{H}$ is called **transitive** if $n = 1$.*

Recall from Definition 2.2.1, that $\rho : G \to S_X$ is a permutation representation and the cardinality of X is the degree of ρ. Therefore the degree of a permutation representation of a group G on the left coset of a subgroup H

is precisely the index of a subgroup H in G. Suppose $\mathcal{H}$ is as in Definition 2.4.1, then the degree of $\mathcal{H}$ is

$$deg(\mathcal{H}) = \sum_{i=1}^{n} [G : H_i],$$

i.e., the sum of all the degrees of transitive permutation representations $\rho^{(i)} : G \to S_{G/H_i}$ on the left cosets by left multiplication.

Definition 2.4.2. *Given a finite group G and a finite set X. If X is of smallest size such that G embeds in S_X, then the cardinality of X is called the* ***minimal faithful degree*** *of G, and it is denoted by $\mu(G)$.*

Let G be a finite group and X be a finite set. We will frequently refer to $\mu(G)$ as just the **minimal degree** of G. If G is embedded in S_X, then the embedding is equivalent to a permutation representation $\mathcal{H} = \{H_i\}_{i=1}^{n}$. Thus we have an equivalent definition of $\mu(G)$.

Definition 2.4.3. *Let G be a finite group and $\mathcal{H} = \{H_i\}_{i=1}^{n}$ be any collection of subgroups of G.*

$$\mu(G) = min\{deg(\mathcal{H}) \mid \textstyle\bigcap_{i=1}^{n} core_G(H_i) = \{1_G\}\}.$$

In this case, $\mathcal{H}$ is called a ***minimal faithful representation*** *of G.*

It is obvious but worth noting that if H is a subgroup of G, then

$$\mu(H) \leqslant \mu(G).$$

It is also easy to think that $\mu(G)$ is always a positive number. This is not true in general. For example, if $G = \{1_G\}$, then we immediately have a faithful permutation representation of G on $\emptyset$: define $\rho : G \to S_\emptyset = \{\iota d\}$ by $\rho(1_G) = \iota d$, where ιd is an identity map. So that $\mu(G) = |\emptyset| = 0$.

Chapter 3

Minimal degrees of finite direct products of finite groups

Let G and H be finite groups. This chapter is devoted to the study of the behaviour of $\mu(G \times H)$ in relation to $\mu(G)$ and $\mu(H)$. It was proven in [20, Proposition 2] that if we have a direct product of two finite groups G and H, then its minimal degree never exceeds the sum of the minimal degrees of G and H, i.e., $\mu(G \times H) \leq \mu(G) + \mu(H)$. A necessary condition for which the reverse inequality is true is also provided in [20, Proposition 2]. We intend to provide a detailed proof of this result and investigate other conditions for which the reverse inequality is true.

3.1 An upper bound for $\mu(G \times H)$

We prove that for any finite groups G and H, $\mu(G) + \mu(H)$ is an upper bound for $\mu(G \times H)$. To achieve this we need to prove the following lemma.

Lemma 3.1.1. *Let G and H be finite groups. If $\mathcal{R} = \{G_i\}_{i=1}^n$ and $\mathcal{H} = \{H_j\}_{j=1}^m$ are faithful representations of G and H respectively, then*

$$\mathcal{D} = \{G_1 \times H, \ldots, G_n \times H, G \times H_1, \ldots, G \times H_m\}$$

is a faithful representation of the direct product $G \times H$.

Proof. Observe that

$$\begin{aligned}
\bigcap_{i=1}^{n} core_{G\times H}(G_i \times H) &= \bigcap_{i=1}^{n} [\bigcap_{\substack{g\in G,\\ h\in H}} (g,h)(G_i \times H)(g^{-1}, h^{-1})] \\
&= \bigcap_{i=1}^{n} [\bigcap_{\substack{g\in G,\\ h\in H}} ((gG_ig^{-1}) \times (hHh^{-1}))] \\
&= \bigcap_{i=1}^{n} [\bigcap_{g\in G} (gG_ig^{-1}) \times \bigcap_{h\in H} (hHh^{-1})] \\
&= \bigcap_{i=1}^{n} [core_G(G_i) \times core_H(H)] \\
&= \bigcap_{i=1}^{n} core_G(G_i) \times \bigcap_{i=1}^{n} core_H(H) \\
&= \{1_G\} \times H.
\end{aligned}$$

Similar calculations shows that $\bigcap_{j=1}^m core_{G\times H}(G\times H_j) = G\times\{1_H\}$. We now have,

$$\begin{aligned}
core(\mathcal{D}) &= [\bigcap_{i=1}^{n} core_{G\times H}(G_i \times H)] \bigcap [\bigcap_{j=1}^{m} core_{G\times H}(G \times H_j)] \\
&= [\{1_G\} \times H] \bigcap [G \times \{1_H\}] \\
&= (1_G, 1_H).
\end{aligned}$$

This show that $\mathcal{D}$ is a faithful representation of $G \times H$. $\square$

It is a result of [20, Proposition 2] that for any finite groups G and H, $\mu(G \times H) \leq \mu(G) + \mu(H)$ and the reverse inequality holds whenever $(|G|, |H|) = 1$. In the following theorem we rely on Lemma 3.1.1 to prove that $\mu(G \times H) \leq \mu(G) + \mu(H)$.

Theorem 3.1.2. *Given any two finite groups G and H, we have*

$$\mu(G \times H) \leq \mu(G) + \mu(H).$$

Proof. Let $\mathcal{R} = \{G_i\}_{i=1}^n$ and $\mathcal{H} = \{H_j\}_{j=1}^m$ be minimal faithful representations of G and H, respectively. Then

$$\mathcal{D} = \{G_1 \times H, \ldots, G_n \times H, G \times H_1, \ldots, G \times H_m\}$$

is a faithful representation by Lemma 3.1.1. We know that $\mu(G \times H)$ is the minimal degree of $G \times H$, is so $\mu(G \times H)$ at most $deg(\mathcal{D})$. Hence

$$\begin{aligned}
\mu(G \times H) \leq deg(\mathcal{D}) &= \sum_{i=1}^{n} [G \times H : G_i \times H] + \sum_{j=1}^{m} [G \times H : G \times H_j] \\
&= \sum_{i=1}^{n} \frac{|G \times H|}{|G_i \times H|} + \sum_{j=1}^{m} \frac{|G \times H|}{|G \times H_j|} \\
&= \sum_{i=1}^{n} \frac{|G||H|}{|G_i||H|} + \sum_{j=1}^{m} \frac{|G||H|}{|G||H_j|} \\
&= \sum_{i=1}^{n} \frac{|G|}{|G_i|} + \sum_{j=1}^{m} \frac{|H|}{|H_j|} \\
&= \sum_{i=1}^{n} [G : G_i] + \sum_{j=1}^{m} [H : H_j] \\
&= deg(\mathcal{R}) + deg(\mathcal{H}) \\
&= \mu(G) + \mu(H).
\end{aligned}$$

This proves the inequality. $\square$

3.2 The additivity property of μ

Theorem 3.1.2 shows that for any given groups G and H, $\mu(G \times H) \leq \mu(G) + \mu(H)$. We now investigate the conditions under which $\mu(G \times H) \geq \mu(G)+\mu(H)$. All of the theory developed in this section builds to address the following question: when is $\mu(G \times H) = \mu(G) + \mu(H)$? In order to respond to this question, we provide some necessary background material.

3.2.1 Primitivity of subgroups in a representation

We define the concept of primitive subgroups and explore the fact that the group may be represented faithfully where the representation consists only of primitive elements. Generally, in a lattice $(\mathcal{L}, \vee, \wedge)$, we say that an element $x \in \mathcal{L}$ is *meet-irreducible* if for any $y, z \in \mathcal{L}$, $x = y \wedge z$ implies that $x = y$ or $x = z$. That is, if $X \subseteq \mathcal{L}$ and $y = \bigwedge_{x \in X} X$, then $y \in X$. We give meet-irreducibility of subgroups in the following definition.

Definition 3.2.1. *Let H be a proper subgroup of a finite group G. We say that*

$$\hat{H} = \bigcap_{\substack{K \leq G, \\ H < K}} K$$

*is a G-**closure** of H. We say H is a **primitive subgroup** of G if $H \neq \hat{H}$.*

Remark 3.2.1. Let G be a finite group. Let $\{K_i\}_{i=1}^n$ be a collection of all subgroups of G which strictly contain a subgroup H of G. If H is primitive, then by definition $H \neq \hat{H} = \bigcap_{i=1}^n K_i$. This implies that if $H = K_r \cap K_s$,

then $H = K_r$ or $H = K_s$, for any $1 \leq r, s \leq n$. Otherwise, we will have

$$\begin{aligned} H \neq \hat{H} &= \bigcap_{i=1}^{n} K_i \\ &= K_1 \cap K_2 \cap \ldots \cap K_r \cap \ldots \cap K_s \cap \ldots \cap K_n \\ &= K_1 \cap K_2 \cap \ldots \cap (K_r \cap K_s) \cap \ldots \cap K_n \\ &= K_1 \cap K_2 \cap \ldots \cap H \cap \ldots \cap K_n \\ &= (\bigcap_{\substack{i=1 \\ i \neq r,s}}^{n} K_i) \cap H \\ &= H. \end{aligned}$$

The last equality of the calculation comes from the fact that $H < K_i$ for $1 \leq i \leq n$ and so $H < \bigcap_{\substack{i=1 \\ i \neq r,s}}^{n} K_i$. This leads to a contradiction. So, primitive subgroups of a finite group G are just meet-irreducible elements of the subgroups lattice of G. Let $\mathcal{L}$ be a finite lattice and $x \in \mathcal{L}$. If x is meet-irreducible then x is a meet of some meet-irreducible elements of the lattice $\mathcal{L}$ because $x = x \wedge x$. Suppose x is not meet-irreducible and $x = x_1 \wedge x_2$ for some $x_1, x_2 \in \mathcal{L}$. If x_i is not meet-irreducible then decompose it as $x_i = x_{i1} \wedge x_{i2}$. If x_{ij} is not meet-irreducible then decompose it as $x_{ij} = x_{ij1} \wedge x_{ij2}$. Since $\mathcal{L}$ is finite, this process will terminate after a finite number of iterations. So x is decomposed as a meet of meet-irreducible elements of $\mathcal{L}$. Hence very element of a finite lattice is a meet of some meet-irreducible elements of the lattice. This implies every subgroup in the subgroup lattice of a finite group G can be expressed as an intersection of primitive subgroups.

Definition 3.2.2. *A **maximal subgroup** of a group G is a subgroup $M < G$ such that there is no subgroup H with $M < H < G$. Let $\mathcal{M}$ be the collection of all maximal subgroups of G. The intersection of all elements of $\mathcal{M}$ is called the **Frattini subgroup** of G. We denote the Fratini subgroup*

of G *by* $\Phi(G)$.

Example 3.2.1. Let M be a maximal subgroup of a finite group G. So M is not strictly contained in any subgroup of the subgroups of G. Therefore $\hat{M} = \emptyset$ and so $M \neq \hat{M}$. Therefore M is primitive. Thus all the maximal subgroups are primitive. However, the converse is not true. A counterexample to this is the trivial subgroup of any cyclic p-group

$$H = \langle x \mid x^{p^n} = 1_G \rangle.$$

Since the subgroup lattice of H is a *chain*, i.e., every subgroup of H is contained in all of the subgroups of H with larger order, therefore the H-closure of $\{1_H\}$ is the non-trivial subgroup of minimum order.

The following lemma first appeared as [20, Lemma 1] and it provides the existence of a minimal faithful representation that consists entirely of primitive elements. It also provides a condition under which an element of the representation is primitive. Due to the relevance of the mechanism employed to prove this result, by following a similar argument as in the proof of [20, Lemma 1], we provide a very detailed proof of it.

Lemma 3.2.2. *Let* $\mathcal{R} = \{G_i\}_{i=1}^n$ *be a minimal faithful representation of the finite group* G. *There exists a minimal faithful representation* $\mathcal{D}$ *of* G *consisting only of primitive elements and* $G_i \in \mathcal{D}$ *whenever* $[G : G_i]$ *is odd.*

Proof. Let $i \in \{1, \ldots, n\}$ and suppose G_i is not primitive. Then there exist two distinct proper subgroups H and K of G both strictly containing G_i such that $G_i = H \bigcap K$. Remove G_i from $\mathcal{R}$ and put H and K into $\mathcal{R}$ to get a new representation $[(\mathcal{R} \setminus G_i) \cup \setminus \{H, K\}]$. Observe that this is still a faithful representation of G since

$$\{1_G\} = core_G(G_i) = core_G(H \bigcap K) = core_G(H) \bigcap core_G(K).$$

Now, observe that

$$deg[(\mathcal{R} \setminus G_i) \cup \{H, K\}] = \mu(G) - [G : G_i] + [G : H] + [G : K].$$

We also have

$$\mu(G) - [G : G_i] + [G : H] + [G : K] \geq \mu(G),$$

because $\mathcal{R}$ is a minimal representation of G. Hence

$$[G : G_i] \quad \leq \quad [G : H] + [G : K] = \frac{[G : G_i]}{[H : G_i]} + \frac{[G : G_i]}{[K : G_i]} \tag{3.1}$$

The denominators $[H : G_i]$ and $[K : G_i]$ are natural numbers greater than 1, because $G_i < H$ and $G_i < K$ by primitivity of G_i. However, $[H : G_i]$ and $[K : G_i]$ cannot exceed 2 otherwise the inequality (3.1) becomes false. It follows that $[H : G_i] = [K : G_i] = 2$. Since $[G : H] = \frac{[G:G_i]}{[H:G_i]}$ is a natural number, then $[G : G_i]$ is even. Consequently, $[G : G_i]$ is even whenever G_i is not primitive (i.e., $[G : G_i]$ is even whenever G_i is not an element of $\mathcal{D}$). From this, we deduce that $G_i \in \mathcal{D}$ whenever $[G : G_i]$ is odd. We now have

$$[G : H] + [G : K] = \tfrac{[G:G_i]}{2} + \tfrac{[G:G_i]}{2} = [G : G_i].$$

Calculating the degree of this representation, we get

$$\begin{aligned} deg[(\mathcal{R} \setminus G_i) \cup \{H, K\}] &= \mu(G) - [G : G_i] + ([G : H] + [G : K]) \\ &= \mu(G) - [G : G_i] + [G : G_i] \\ &= \mu(G). \end{aligned}$$

This proves that $(\mathcal{R} \setminus G_i) \cup \{H, K\}$ is also a minimal representation of G. Note that G is a finite group, so it has a finite number of subgroups, all of which are of finite order. The subgroups of G shall have a finite number

of subgroups too. Therefore, if H or K is not primitive in the construction of $(\mathcal{R} \setminus G_i) \cup \{H, K\}$, we may repeat the same process and after a finite number of iterations we will have a minimal representation $\mathcal{D}$ of the desired type from the representation $\mathcal{R}$. □

The following corollary is immediate. Its content is the same as the content of [20, Corollary 1]. However, the proof of [20, Corollary 1] was omitted, so we provide our own proof below.

Corollary 3.2.3. *All the subgroups of odd index appearing in any minimal faithful representation of a finite group G are primitive. Furthermore, every minimal representation of a group G of odd order consists entirely of primitive subgroups.*

Proof. The first part is a direct consequence of the above lemma. Let G be a group of odd order and $\mathcal{R} = \{G_i\}_{i=1}^n$ be its minimal faithful representation. We claim that $[G : G_i]$ is odd for $1 \leq i \leq n$. For, if $[G : G_i]$ is even, say $[G : G_i] = 2n$ for some integer n, then $|G|/|G_i| = 2n$. This implies that $|G| = 2n|G_i| = 2(n|G_i|)$. Hence $|G|$ is even. This contradicts the the fact that $|G|$ is odd. The result follows from the above lemma. □

From now on, we will use the following terminology.

Definition 3.2.3. *Let H and G be non-trivial finite groups. If*

$$\mu(H \times G) = \mu(H) + \mu(G),$$

*we say that μ is **additive** for H and G. If there is no confusion on the groups to which we are referring to, we simply say that μ is **additive**.*

3.3 The additivity of μ for groups of coprime order

The Chinese Remainder Theorem is a well-known result from elementary Number Theory. We intend to use it in the proof of Lemma 3.3.2. We state the Chinese Remainder Theorem without proof. Its proof can be accessed from any elementary Number Theory textbook (see, for example, [23] for reference).

Theorem 3.3.1. *(Chinese Reminder Theorem) Suppose $n_1, \ldots, n_k$ are positive integers that are pairwise coprime. Then, for any given sequence of integers $a_1, \ldots, a_k$, there exists an integer x solving the system of simultaneous congruences $x \equiv a_i \pmod{n_i}$ for all $1 \leq i \leq k$. Furthermore, all solutions x of these congruences are congruent modulo the product $N = n_1 \cdots n_k$. The solution x is given by $x \equiv (\sum_{i=1}^{k} a_i M_i y_i \,) \pmod{N}$, where $M_i = N/n_i$ and $y_i \equiv (M_i)^{-1} \pmod{n_i}$ for all $1 \leq i \leq k$.*

We provide the following lemma which usually appears as an exercise in the literature, we prove it for completeness.

Lemma 3.3.2. *Let G and H be finite groups whose orders are coprime. If X is a subgroup of the direct product $G \times H$, then there exist subgroups G^* and H^* of G and H respectively, such that $X = G^* \times H^*$.*

Proof. Let $X \leq G \times H$. Choose $G^* = \pi_1(X)$ and $H^* = \pi_2(X)$, where π_i is the projection of the i^{th} coordinate of X. That is, if $(g, h) \in X$ then $\pi_1((g, h)) = g$ and $\pi_2((g, h)) = h$. Thus,

$$G^* = \pi_1(X) = \{g \mid (g, h) \in X\}$$

and

$$H^* = \pi_2(X) = \{h \mid (g, h) \in X\}.$$

If $(x, y) \in X$ then $x \in G^*$ and $y \in H^*$, by definition of G^* and H^*. Hence, $(x, y) \in G^* \times H^*$. So $X \subseteq G^* \times H^*$. Now let $(x, y) \in G^* \times H^*$. Then $x \in G^*$ and $y \in H^*$, which means there exists $g \in G$ and $h \in H$ such that $(x, h), (g, y) \in X$. We know that $(|G|, |H|) = 1$ (i.e., the orders of G and H are coprime), so by the Chinese Remainder Theorem, there exists integers n_1 and n_2 such that $n_1 \equiv 0 \pmod{|H|}$ and $n_1 \equiv 1 \pmod{|G|}$. Applying Chinese Remainder Theorem again we get $n_2 \equiv 0 \pmod{|G|}$ and $n_2 \equiv 1 \pmod{|H|}$. Thus, $|H|$ divides n_1 and $|H|$ divides $n_2 - 1$, also $|G|$ divides n_2 and $|G|$ divides $n_1 - 1$. We now have

$$(x, h)^{n_1} = (x^{n_1}, h^{n_1}) = (x^{n_1 - 1}x, h^{n_1}) = (x, 1_H) \in X.$$

Similarly, $(g, y)^{n_2} = (1_G, y) \in X$. So we can multiply $(x, h)^{n_1}$ by $(g, y)^{n_2}$, and the resulting element will be an element of X since $X \leq G \times H$. Multiplying, we get

$$(x, h)^{n_1}(g, y)^{n_2} = (x, 1_H)(1_G, y) = (x, y) \in X.$$

Hence $G^* \times H^* \subseteq X$. This shows that $X = G^* \times H^*$. □

We provided the first condition for the additivity of μ. The following appears as a converse statement of [20, Proposition 2]. A self-contained and detailed proof of this is provided below.

Theorem 3.3.3. *For any two finite groups G and H, we have*

$$\mu(G \times H) = \mu(G) + \mu(H),$$

whenever G and H have coprime orders.

Proof. Let G and H be finite groups. By Theorem 3.1.2 we have $\mu(G \times H) \leq \mu(G) + \mu(H)$. Let $\mathcal{X} = \{X_i\}_{i=1}^n$ be a minimal faithful representation of $G \times H$

with each X_i primitive in $G \times H$. This type of representation exists by Lemma 3.2.2. If $(|G|, |H|) = 1$, then for each $i \in \{1, \ldots, n\}$ there exist subgroups G_i^* of G and H_i^* of H such that $X_i = G_i^* \times H_i^*$, by Lemma 3.3.2. Since $G_i^* \subseteq G$ and $H_i^* \subseteq H$, then

$$G_i^* \times H_i^* = (G \times H_i^*) \bigcap (G_i^* \times H).$$

We now have

$$X_i = G_i^* \times H_i^* = (G \times H_i^*) \bigcap (G_i^* \times H).$$

So, by the primitivity of X_i, we must have $X_i = G \times H_i$ or $X_i = (G_i \times H)$. Plausibly, we may assume that

$$\mathcal{X} = \{G \times H_1, \ldots, G \times H_{n_1}, G_1 \times H, \ldots, G_{n_2} \times H\},$$

for some positive integers n_1 and n_2. Let $\mathcal{H} = \{H_i\}_{i=1}^{n_1}$ and $\mathcal{R} = \{G_j\}_{j=1}^{n_2}$. Note that only $\{1_H\}$ can be a normal subgroup of H contained in each of the elements of $\mathcal{H}$. For if $N \lhd H$, and $N \leq H_i$ for every $i \in \{1, \ldots, n\}$, then $\{1_G\} \times N$ is in every element $\mathcal{X}$. Since $\{1_G\}$ and N are invariant under conjugation by elements of G and H respectively, we have

$$\{1_G\} \times N \subseteq core_{G \times H}(\mathcal{X}).$$

However, $\mathcal{X}$ is a minimal faithful representation, and so

$$core_{G \times H}(\mathcal{X}) = \{(1_G, 1_H)\}.$$

From this we obtain that

$$\{1_G\} \times N \subseteq core_{G \times H}(\mathcal{X}) = \{(1_G, 1_H)\}.$$

Thus $\{1_G\} \times N = \{(1_G, 1_H)\}$. This forces N to be a trivial subgroup of H. A similar argument shows that $\{1_G\}$ is the only normal subgroup of G contained in each of the elements of $\mathcal{R}$. So, $core_H(\mathcal{H}) = \{1_H\}$ and

$core_G(\mathcal{R}) = \{1_G\}$. This implies that $\mathcal{H}$ and $\mathcal{R}$ are faithful representations of H and G respectively. Hence we have $\mu(H) \leq deg(\mathcal{H})$ and $\mu(G) \leq deg(\mathcal{R})$. Adding these inequalities, we get

$$\begin{aligned}
\mu(H) + \mu(G) &\leq deg(\mathcal{H}) + deg(\mathcal{R}) \\
&= \sum_{i=1}^{n_1} [H : H_i] + \sum_{j=1}^{n_2} [G : G_j] \\
&= \sum_{i=1}^{n_1} \frac{|H|}{|H_i|} + \sum_{j=1}^{n_2} \frac{|G|}{|G_j|} \\
&= \sum_{i=1}^{n_1} \frac{|G|}{|G|}\frac{|H|}{|H_i|} + \sum_{j=1}^{n_2} \frac{|G|}{|G_j|}\frac{|H|}{|H|} \\
&= \sum_{i=1}^{n_1} \frac{|G \times H|}{|H \times H_i|} + \sum_{j=1}^{n_2} \frac{|G \times H|}{|G_j \times H|} \\
&= \sum_{i=1}^{n_1} [G \times H : G \times H_i] + \sum_{j=1}^{n_2} [G \times H : G_j \times H] \\
&= deg(\mathcal{X}) \\
&= \mu(G \times H).
\end{aligned}$$

This shows that $\mu(G \times H) = \mu(G) + \mu(H)$. □

3.4 Minimal permutation representations of a direct product of nilpotent groups

This section is devoted to showing that μ is additive for a direct product of any two finite nilpotent groups. We therefore develop a theory of finite nilpotent groups with a view of providing some characterisation for finite nilpotent groups required to prove the additivity of μ. This theory does not only allow us to provide an original proof of [36, Corollary 1], it will also be widely used in the subsequent sections and chapters.

Definition 3.4.1. *Let G be a group. A* ***normal series*** *for G is a chain*

$$\{1_G\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G,$$

of subgroups of G such that $G_i \trianglelefteq G$ for $0 \leq i \leq n$. If in addition, we have $G_{i-1}/G_i \subseteq Z(G/G_i)$ for $1 \leq i \leq n$, this normal series is called a ***central series****. A group G is said to be* ***nilpotent*** *if it has a central series. The least n such that $G_n = \{1_G\}$ is called the* ***nilpotency class*** *of the central series and each G_{i-1}/G_i is called a* ***factor*** *of the central series.*

The following example will be used later to deduce that

$$\mu(G \times H) = \mu(G) + \mu(H),$$

for any finite abelian groups G and H.

Example 3.4.1. Let G be an abelian group. Then, the chain $\{1_G\} \leq G$ is a central series for G because $\{1_G\} \trianglelefteq G$ and $G/\{1_G\} = G \subseteq Z(G/\{1_G\}) = Z(G) = G$. So G is nilpotent.

Definition 3.4.2. *Let G be a group and $x, y \in G$. The* ***commutator*** *of x and y is the element $[x, y] = xyx^{-1}y^{-1}$. The subgroup $G' = \langle [x, y] \mid x, y \in G \rangle$, generated by all commutators of elements of G is called the* ***derived subgroup*** *or the* ***commutator subgroup*** *of G. The* ***derived series*** *for G is defined recursively as follows,*

$$G^{(0)} = G \text{ and } G^{(i+1)} = (G^{(i)})', \text{ for } i \geq 0,$$

that is, $G^{(i+1)} := \langle [x, y] | x, y \in G^{(i)} \rangle$. We also write $G^{(2)} = G''$, $G^{(3)} = G'''$ etc. If H and K are subgroups of G then the ***commutator subgroup*** *of G* ***generated by*** *H* ***and*** *K, denoted by $[H, K]$, is defined by*

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle,$$

i.e., the subgroup generated by all commutators $[h, k]$ *where* $h \in H$ *and* $k \in K$. *So,* $G' = [G, G]$. *The derived series for* G *is now recursively defined as*

$$G^{(0)} = G \text{ and } G^{(i+1)} = [G^{(i)}, G^{(i)}], \text{ for all } i \geq 0.$$

If a group G is abelian, then $[x, y] = xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = 1_G$ for all $x, y \in G$. Thus $G' = \{1_G\}$. So, the subgroup G' can be realised as a measure of how far a group G is from being abelian. Another type of series that will help us characterise nilpotent groups is defined below.

Definition 3.4.3. *The* ***lower central series*** *for a group* G *is the chain of subgroups of the group* G *defined by*

$$\gamma_1(G) = G \text{ and } \gamma_{i+1}(G) = [\gamma_i(G), G], \text{ for } i \geq 1.$$

Few properties of derived and lower central series are given in the following lemma.

Lemma 3.4.2. *Let* G *be a group. The following properties hold:*

(i) *If* $H_1 \leq K_1 \leq G$ *and* $H_2 \leq K_2 \leq G$, *then* $[H_1, H_2] \subseteq [K_1, K_2]$. *Moreover,* $[H_1, H_2] \leq [K_1, K_2]$.

(ii) $G^{(n)} \subseteq \gamma_{n+1}(G)$, *for any* $n \geq 0$.

(iii) *If* H *is a subgroup of* G, *then* $\gamma_i(H) \subseteq \gamma_i(G)$ *for all* $i \geq 0$.

(iv) *If* $\rho : G \to H$ *is an onto homomorphism, then* $\rho(\gamma_i(G)) = \gamma_i(H)$ *for all* $i \geq 0$.

(v) $\gamma_{i+1}(G) \subseteq \gamma_i(G)$ *for all* $i \geq 0$.

(vi) $[H_1, H_2] = [H_2, H_1]$ *for all* $H_1, H_2 \leq G$.

Proof. (i) The first part follows by the definition of the commutator of two subgroups. The fact that $[H_1, H_2] \leq [K_1, K_2]$ comes from that $[H_1, H_2]$ is a subgroup of G and hence a subgroup of any subgroup of G containing it.

(ii) We proceed by induction on n. For $n = 0$, $G^{(0)} = G$ and $\gamma_1(G) = G$, so $G^{(0)} \subseteq \gamma_1(G)$. Now suppose that $G^{(i)} \subseteq \gamma_{i+1}(G)$, then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [\gamma_{i+1}(G), G^{(i)}] \subseteq [\gamma_{i+1}(G), G] = \gamma_{i+2}(G).$$

This shows that $G^{(n)} \subseteq \gamma_{n+1}(G)$, for any $n \geq 0$.

(iii) We proceed by induction on i. The result is true for $i = 0$ since $\gamma_1(H) = H \subseteq G = \gamma_1(G)$. Now suppose $\gamma_k(H) \subseteq \gamma_k(G)$ for $k > 0$. Since $H \subseteq G$ and $\gamma_k(H) \subseteq \gamma_k(G)$, by definition we have $\gamma_{k+1}(H) = [\gamma_k(H), H] \subseteq [\gamma_k(G), G] = \gamma_{k+1}(G)$, and hence the result.

(iv) We proceed by induction on i. For $i = 0$, we have $\rho(\gamma_1(G)) = \rho(G) = H = \gamma_1(H)$. Suppose $\rho(\gamma_k(G)) = \gamma_k(H)$ for $k > 0$. Let $[x, g] \in [\gamma_k(G), G] = \gamma_{k+1}(G)$. Since ρ is a surjective homomorphism, we have

$$\begin{aligned} \rho([x, g]) &= \rho(xgx^{-1}g^{-1}) \\ &= \rho(x)\rho(g)\rho(x^{-1})\rho(g^{-1}) \\ &= \rho(x)\rho(g)(\rho(x))^{-1}(\rho(g))^{-1} \\ &= [\rho(x), \rho(g)], \end{aligned}$$

and $[\rho(x), \rho(g)] \in [\rho(\gamma_k(G)), \rho(G)] = [\gamma_k(H), H] = \gamma_{k+1}(H)$. So $\rho(\gamma_{k+1}(G)) \subseteq \gamma_{k+1}(H)$. Reversing the calculations above we get the reverse containment. From this we deduce that $\gamma_i(G)$ is a characteristic subgroup of G (i.e., $\gamma_i(G)$ is invariant under all automorphisms of G). Hence, $\gamma_i(G) \trianglelefteq G$.

(v) Let $[x, g] \in \gamma_{i+1}(G)$, so $x \in \gamma_i(G)$ and $g \in G$. Since $[x, g]^{-1} = (xgx^{-1}g^{-1})^{-1} = gxg^{-1}x^{-1} = x^g x^{-1}$ and $x^g \in \gamma_i(G)$ (since $\gamma_i(G) \trianglelefteq G$ by (iv)), then $[x, g]^{-1} \in \gamma_i(G)$. Since $\gamma_i(G) \leq G$, we get $[x, g] \in \gamma_i(G)$.

(vi) If $[a, b] = aba^{-1}b^{-1} \in [H_1, H_2]$, then $[a, b]^{-1} \in [H_1, H_2]$. However, $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} \in [H_2, H_1]$. So, $[a, b] \in [H_2, H_1]$ because $[H_2, H_1]$ is a subgroup of G. This implies $[H_1, H_2] \subseteq [H_2, H_1]$. Similarly, $[H_2, H_1] \subseteq [H_1, H_2]$.

□

Given any group, we can attempt to construct a central series as follows: we let $Z_0(G) = \{1_G\}$ and $Z_1(G) = Z(G)$. Note that $Z(G/Z_1(G)) \trianglelefteq G/Z_1(G)$, so by the Correspondence Theorem, there corresponds a unique subgroup $Z_2(G) \leq G$ such that $Z_1(G) \subseteq Z_2(G)$. Define the next term of the series to be $Z_2(G)$, the unique subgroup of G such that $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$. Inductively, for any $i \geq 0$, we define $Z_{i+1}(G)$ to be the unique subgroup such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. We now give a definition based on this discussion.

Definition 3.4.4. *Let G be a group. The **upper central series** for G is the chain of subgroups defined inductively by*

$$Z_0(G) = \{1_G\}$$

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)), \text{ for all } i \geq 0.$$

We point out that an upper central series need not be a central series, since we can have $Z_i(G) \lhd G$ for all $i \geq 0$. For example, if we take $G = S_3$, then $Z(G)$ is trivial and so $Z_i(G) \lhd G$ for all $i \geq 0$. But if $Z_n(G) = G$ for some n, then

$$\{1_G\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_n(G) = G$$

is indeed a central series. The proof of the following lemma will explore that the upper central series is a central series if and only if the group G is nilpotent. It will also explicit the relationship between central, lower central and upper central series with respect to the nilpotency of a group.

Lemma 3.4.3. *Let G be a group. The following conditions are equivalent.*

(i) G is nilpotent.

(ii) $\gamma_{n+1}(G) = \{1_G\}$ for some integer n.

(iii) $Z_n(G) = G$ for some integer n.

Proof. Suppose G is nilpotent and let $\{1_G\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G$ be a central series for G. For all $i \geq 0$, we first claim that:

$$\gamma_{i+1}(G) \subseteq G_i \tag{3.2}$$

To see this, we proceed by induction on i. For $i = 0$, we have $\gamma_1(G) = G = G_0$, so the result is true. Suppose $\gamma_k(G) \subseteq G_{k-1}$ for some $k > 0$. We show that the result is valid for $k + 1$. Let $[x, g] \in \gamma_{k+1}(G) = [\gamma_k(G), G]$ be arbitrary elements. So, $x \in \gamma_k(G)$ and $g \in G$. Since $\gamma_k(G) \subseteq G_{k-1}$, it follows that $x \in G_{k-1}$. Hence $xG_k \in G_{k-1}/G_k$. However,

$$\{1_G\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G$$

is a central series for G, so $G_{k-1}/G_k \subseteq Z(G/G_k)$. Hence $xG_k \in Z(G/G_k)$,

this implies that $(xG_k)(gG_k) = (gG_k)(xG_k)$. We now have

$$\begin{aligned}
[x,g]G_k &= (xgx^{-1}g^{-1})G_k \\
&= (xG_k)(gG_k)(x^{-1}G_k)(g^{-1}G_k) \\
&= (xG_k)(gG_k)(xG_k)^{-1}(gG_k)^{-1} \\
&= (gG_k)(xG_k)(xG_k)^{-1}(gG_k)^{-1} \\
&= 1_{G_{k-1}/G_k} \\
&= G_k.
\end{aligned}$$

So, $[x,g] \in G_k$. This implies that $\gamma_{k+1}(G) \subseteq G_k$. So the containment in (3.2) is true. For all $i \geq 0$, we also claim that:

$$G_{n-i} \subseteq Z_i(G) \tag{3.3}$$

We proceed by induction on i again. For $i = 0$, $Z_0(G) = \{1_G\} = G_n$, so the results is valid. Now suppose that $G_{n-k} \subseteq Z_k(G)$ for some $k > 0$. We show that the result is true for $k+1$. Choose $x \in G_{n-(k+1)} = G_{n-k-1}$ and $g \in G$ arbitrarily. Note that $G_{n-k-1}/G_{n-k} \subseteq Z(G/G_{n-k})$ because

$$\{1_G\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G$$

is a central series for G. Therefore $x(G_{n-k})g(G_{n-k}) = (gG_{n-k})(xG_{n-k})$. It follows that $[x,g]G_{n-k} = G_{n-k}$, hence $[x,g] \in G_{n-k}$. Therefore $[x,g] \in Z_k(G)$. This implies that $[x,g]Z_k(G) = Z_k(G)$. So, $(xgx^{-1}g^{-1})Z_k(G) = Z_k(G)$, i.e., $(xZ_k(G))(gZ_k(G))(xZ_k(G))^{-1}(gZ_k(G))^{-1} = Z_k(G)$, so that

$$(xZ_k(G))(gZ_k(G)) = (gZ_k(G))(xZ_k(G)).$$

Thus $xZ_k(G) \in Z(G/Z_k(G))$. Now,

$$\{1_G\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_n(G) = G,$$

implies that $Z(G/Z_{k+1}(G)) = Z_{k+1}/Z_k(G)$, and hence $xZ_k(G) \in Z_{k+1}/Z_k(G)$. This shows that $x \in Z_{k+1}$, from which we deduce $G_{n-(k+1)} \subseteq Z_{k+1}$. Hence, the containment in (3.3) is true.

Now, from (3.2), $\gamma_{n+1}(G) \subseteq G_n = \{1_G\}$, and $G = G_0 = Z_n(G)$ by the containment in (3.3). This implies that $\gamma_{n+1}(G) = \{1_G\}$ and $G = Z_n(G)$, respectively. Therefore (i) implies both (ii) and (iii).

Suppose $\gamma_{n+1}(G) = \{1_G\}$ for some n, then

$$\{1_G\} = \gamma_{n+1}(G) \subseteq \cdots \subseteq \gamma_1(G) = G$$

is a central series for G. For if $x \in \gamma_i(G)$ and $g \in G$ then $[x, g] \in \gamma_{i+1}(G)$. Therefore $[x, g]\gamma_{i+1}(G) = \gamma_{i+1}(G)$. From this, we get $(x\gamma_{i+1}(G))(g\gamma_{i+1}(G)) = (g\gamma_{i+1}(G))(x\gamma_{i+1}(G))$. This implies $x\gamma_{i+1}(G) \in Z(G/\gamma_{i+1}(G))$. Thus $\gamma_i(G)/\gamma_{i+1}(G) \subseteq Z(G/\gamma_{i+1}(G))$. Also $\gamma_{i+1}(G) \trianglelefteq G$ for all $i \geq 0$, by Lemma 3.4.2 (iv). Therefore G is nilpotent. So (ii) implies (i). However (i) implies (iii), so (ii) implies (iii) as well.

Suppose $Z_n(G) = G$ for some integer n. Then G is nilpotent possessing

$$\{1_G\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots \subseteq Z_n(G) = G$$

as a central series for G. This is trivial since

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \text{ (and so } Z_{i+1}(G)/Z_i(G) \subseteq Z(G/Z_i(G))).$$

So, (iii) implies (i). Again, (i) implies (ii), so (iii) implies (ii). Hence all of the above conditions are equivalent. □

Lemma 3.4.4. *Homomorphic images and subgroups of nilpotent groups are nilpotent.*

Proof. Let G be nilpotent. Then $\gamma_{n+1}(G) = \{1_G\}$ for some n. Let $H \leq G$, then by Lemma 3.4.2 (iii), we have $\gamma_{n+1}(H) \subseteq \gamma_{n+1}(G) = \{1_G\}$. So,

$\gamma_{n+1}(H) = \{1_G\}$, and H is nilpotent. If H is a homomorphic image of G, then there exists an onto homomorphism $\rho : G \to H$. Now by Lemma 3.4.2 (iv), we have

$$\{1_H\} = \rho(\{1_G\}) = \rho(\gamma_{n+1}(G)) = \gamma_{n+1}(H).$$

So H is nilpotent. □

We now present the so-called normaliser condition for nilpotent groups. This is going to be used later to show that a Sylow p-subgroup of a nilpotent group is normal.

Lemma 3.4.5. *Let G be a nilpotent group. If $H < G$ then $H < N_G(H)$.*

Proof. Since G is nilpotent, by Lemma 3.4.2 (v) and Lemma 3.4.3 it follows that the lower central series of G is of the form

$$\{1_G\} = \gamma_{n+1}(G) \subseteq \cdots \subseteq \gamma_2(G) \subseteq \gamma_1(G) = G.$$

Observe that $\{1_G\} = \gamma_{n+1}(G) \subseteq H$. So we can choose the smallest i such that $\gamma_i(G) \subseteq H$. Therefore $\gamma_{i-1}(G) \nsubseteq H$. But $[\gamma_{i-1}(G), H] \subseteq [\gamma_{i-1}(G), G]$, since H is contained in G. Moreover, $[\gamma_{i-1}(G), G] = \gamma_i(G)$ and $\gamma_i(G) \subseteq H$, so $[\gamma_{i-1}(G), G] \subseteq H$. If $x \in \gamma_{i-1}(G)$ and $h \in H$, then $[x, h] = xhx^{-1}h^{-1} = h^x h^{-1} \in H$. Hence $H^x = H$ for all $x \in \gamma_{i-1}(G)$, thus $\gamma_{i-1}(G) \subseteq N_G(H)$. Since $\gamma_{i-1}(G) \nsubseteq H$, we can choose $x_0 \in N_G(H)$ such that $x_0 \in \gamma_{i-1}(G)$ but $x_0 \notin H$. This is illustrated diagrammatically in Figure 3 below.

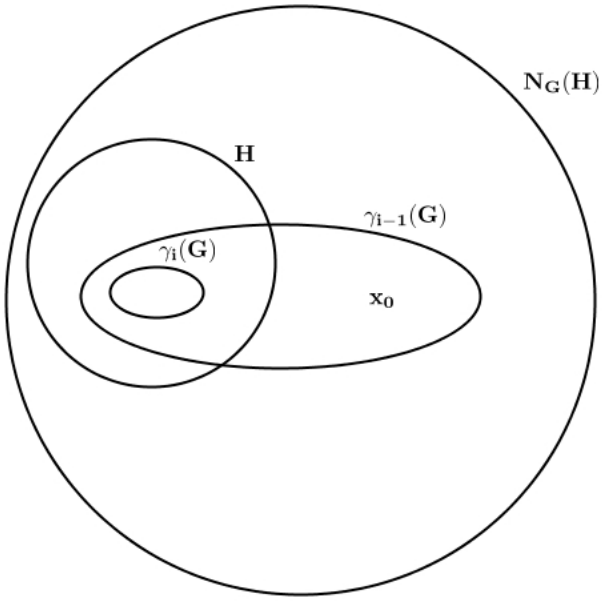

Figure 3

We deduce that $H < N_G(H)$. □

For the sake of completeness, we prove the following simple lemma which usually appear as an exercise in most of the standard textbooks. We will employ the corollary of this lemma to prove that a finite nilpotent group is a direct product of its Sylow p-subgroups.

Lemma 3.4.6. *Let G and H be groups. Let $G \times H$ be a direct product of G and H. Then*

$$Z(G \times H) = Z(G) \times Z(H).$$

Proof. Let $(g, h) \in Z(G \times H)$. Then for every $(x, y) \in G \times H$, we have $(g, h)(x, y) = (x, y)(g, h)$. Therefore $(gx, hy) = (xg, yh)$. By equality of pairs we get $gx = xg$ and $hy = yh$, for all $x \in G$ and $y \in H$. Thus $g \in Z(G)$

and $h \in Z(H)$, i.e., $(g,h) \in Z(G) \times Z(H)$. Conversely, suppose $(g,h) \in Z(G) \times Z(H)$. Then $g \in Z(G)$ and $h \in Z(H)$. Therefore, for all $x \in G$ and $y \in H$ we have $gx = xg$ and $hy = yh$. This implies that $(gx, hy) = (xg, yh)$, i.e., $(g,h)(x,y) = (x,y)(g,h)$. So that $(g,h) \in Z(G \times H)$. □

A corollary of Lemma 3.4.6 follows by a simple induction on the number of factors in the direct product.

Corollary 3.4.7. *Let $G = G_1 \times \cdots \times G_n$ be a direct product. Then*

$$Z(G) = Z(G_1) \times \cdots \times Z(G_n).$$

Proof. For $n = 2$, the result is true by Lemma 3.4.6. Suppose $G = G_1 \times \cdots \times G_k$ and $Z(G) = Z(G_1) \times \cdots \times Z(G_k)$. Consider $G = G_1 \times \cdots \times G_k \times G_{k+1}$. Then, by Lemma 3.4.6 and by the induction hypothesis, we have $Z(G) = Z(G_1 \times \cdots \times G_k) \times Z(G_{k+1}) = Z(G_1) \times \cdots \times Z(G_k) \times Z(G_{k+1})$. □

Theorem 3.4.8. *If G and H are nilpotent, then the direct product $G \times H$ is nilpotent.*

Proof. First note that $Z_k(G \times H) = Z_k(G) \times Z_k(H)$. We proceed by induction on k. For $k = 1$, the result is true by Lemma 3.4.6. Suppose $Z_k(G \times H) = Z_k(G) \times Z_k(H)$ for some $k > 1$. Then

$$\frac{G \times H}{Z_k(G \times H)} = \frac{G \times H}{Z_k(G) \times Z_k(H)} = \frac{G}{Z_k(G)} \times \frac{H}{Z_k(H)}.$$

So the center of $Z(\frac{G \times H}{Z_k(G \times H)}) = Z(\frac{G}{Z_k(G)} \times \frac{H}{Z_k(H)})$. However, by Lemma 3.4.6

$$Z(\frac{G}{Z_k(G)} \times \frac{H}{Z_k(H)}) = Z(\frac{G}{Z_k(G)}) \times Z(\frac{H}{Z_k(H)}) = \frac{Z_{k+1}(G)}{Z_k(G)} \times \frac{Z_{k+1}(H)}{Z_k(G)}.$$

Hence $Z_{k+1}(G \times H) = Z_{k+1}(G) \times Z_{k+1}(H)$. Since G and H are nilpotent, we can choose a natural number n such that $Z_n(G \times H) = Z_n(G) \times Z_n(H) = G \times H$, by Theorem 3.4.3. So $G \times H$ is nilpotent. □

3.4.1 Some characterisations of finite nilpotent groups

We are now ready to present some characterisation theorems of finite nilpotent groups. The first characterisation for finite nilpotent groups which is of our interest is presented in the following theorem.

Theorem 3.4.9. *Let G be a finite group. Then the following conditions are equivalent.*

(i) G is a non-trivial nilpotent group.

(ii) Every non-trivial homomorphic image of G has a non-trivial center.

(iii) G appears as a member of its central series.

Proof. Suppose G is a non-trivial nilpotent group. Let

$$\{1_G\} = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_0 = G$$

be a central series for G, then the first non-trivial term G_k, say, is contained in the center of G, since $G_k/G_{k+1} \subseteq Z(G/G_{k+1}) = Z(G)$ (because G_{k+1} is trivial). So $Z(G)$ is non-trivial. By Lemma 3.4.4, all the homomorphic images of G are nilpotent. Therefore the result follows for any homomorphic image of G. Thus (i) implies (ii).

Now suppose that every non-trivial homomorphic image of G has a non-trivial center. If $Z_i(G)$ is the ith term of the upper central series of G, then $Z_{i+1}/Z_i(G) = Z(G/Z_i(G))$ is non-trivial since $G/Z_i(G)$ is a homomorphic image of G. Therefore $Z_i(G) \subset Z_{i+1}(G)$ unless $Z_i(G) = G$. So, the terms of the upper central series are strictly increasing. The latter together with the fact that G is a finite group imply that not every term of the upper central series will be proper in G. That is, eventually $Z_m(G) = G$ for some m. This proves that (ii) implies (iii).

Finally, suppose that G appears as a member of its upper central series. By Lemma 3.4.3, it follows that (iii) implies (i). □

We now want to characterise finite nilpotent groups as built from its Sylow p-subgroups. To accomplish this, we need few more results. The following result asserts that a normaliser of any Sylow p-subgroups normalises itself.

Lemma 3.4.10. *Let G be a finite group and let $P \in Syl_p(G)$ for some prime p. Then $N_G(N_G(P)) = N_G(P)$.*

Proof. Note that $H \leq N_G(H)$ for any $H \leq G$. Taking $H = N_G(P)$, we get $N_G(P) \leq N_G(N_G(P))$. So $N_G(P) \subseteq N_G(N_G(P))$. We only need to show that $N_G(N_G(P)) \subseteq N_G(P)$. To do this, first note that $P \trianglelefteq N_G(P)$ since $P^x = P$ for all $x \in N_G(P)$. Since $P \in Syl_p(G)$, then P is a p-subgroup of maximal order in G, hence in $N_G(P)$. So $P \in Sly_p(N_G(P))$. Moreover, P is the unique Sylow p-subgroup of $N_G(P)$, since $P \trianglelefteq N_G(P)$. Now let $x \in N_G(N_G(P)) = \{g \in G \mid (N_G(P))^g = N_G(P)\}$. We need to show that $g \in N_G(P)$. As $P \trianglelefteq N_G(P)$, it follows that $P^x \leq (N_G(P))^x = N_G(P)$. So P^x is also Sylow p-subgroups of $N_G(P)$. As $|P| = |P^x|$, by the uniqueness of P in $N_G(P)$, we have that $P^x = P$. This implies that $x \in N_G(P)$, and so $N_G(N_G(P)) \subseteq N_G(P)$. □

Since our interest is to describe the structure of a finite nilpotent group using finite p-groups, we start by first proving that finite p-groups are themselves nilpotent.

Lemma 3.4.11. *Every finite p-group is nilpotent.*

Proof. Let G be a p-group. Thus $|G| = p^m$ for some prime p and a positive integer m. Let us proceed by induction on the order of the group, which

implies that we proceed by induction on m. If $m = 1$, then $|G| = p$. So G is cyclic. Let $G = \langle x \rangle$. So, for every non-negative integer n, we have

$$\begin{aligned}
\gamma_{n+1}(G) &= [\gamma_n(G), G] \\
&= \langle [x^i, x^j] \mid x^i \in \gamma_n(G), x^j \in G \rangle \\
&= \langle x^i x^j x^{-i} x^{-j} \mid x^i \in \gamma_n(G), x^j \in G \rangle \\
&= \langle x^{i+j-i-j} \mid x^i \in \gamma_n(G), x^j \in G \rangle \\
&= \{1_G\}.
\end{aligned}$$

Thus G is nilpotent. Suppose $|G| = p^k$, and assume that all the p-groups of order smaller than $|G|$ are nilpotent. We know that $Z(G) \trianglelefteq G$ and since $Z(G) \neq \{1_G\}$, then the quotient group $G/Z(G)$ is a p-group of order smaller than $|G|$. Hence, by the induction hypothesis $G/Z(G)$ is a nilpotent group. By Lemma 3.4.3, we have $\gamma_{n+1}(G/Z(G)) = \{1_{G/Z(G)}\}$ for some n. Let $\rho : G \to G/Z(G)$ be the natural homomorphism. By Lemma 3.4.2 (iv), we have $\rho(\gamma_{n+1}(G)) = \gamma_{n+1}(G/Z(G)) = \{1_{G/Z(G)}\}$, therefore $\gamma_{n+1}(G) \subseteq \mathsf{ker}\rho = Z(G)$. Now $\gamma_{n+2}(G) = [\gamma_{n+1}(G), G] \subseteq [Z(G), G]$. However $[Z(G), G] = \{1_G\}$ because $[x, g] = xgx^{-1}g^{-1} = gxx^{-1}g^{-1} = 1_G$ for all $x \in Z(G)$ and $g \in G$. Therefore, $\gamma_{n+2}(G) = \{1_G\}$. So by induction G is a nilpotent group. □

We are now ready to provide a characterisation for nilpotent groups as being constructed from their Sylow p-subgroups. The following theorem and its proof will be extensively used to prove the additivity property of μ for finite nilpotent groups in the subsection that follows. So its proof is provided regardless of its frequent availability in the literature.

Theorem 3.4.12. *Let G be a finite group. The following conditions are equivalent:*

(i) G is nilpotent.

(ii) Every Sylow p-subgroup of G is normal.

(iii) G is a direct product of Sylow p_i-subgroups, for different primes p_i.

Proof. We show that (*i*) implies (*ii*) and (*ii*) implies (*iii*) and finally that (*iii*) implies (*i*). Suppose G is nilpotent and let $P \in Syl_p(G)$. By Lemma 3.4.10 we have $N_G(N_G(P)) = N_G(P)$. So $N_G(P)$ is not a proper subgroup of $N_G(N_G(P))$. By the contraposition of Lemma 3.4.5 we get that $N_G(P)$ is not a proper subgroup of G. Since $N_G(P) \leq G$, we conclude that $N_G(P) = G$. This proves that $P \trianglelefteq G$.

Now suppose every Sylow p-subgroup of G is normal. We need to show that G is a direct product of Sylow p_i-groups, for different primes p_i. Let $|G| = \Pi_{i=1}^{n} p_i^{\alpha_i}$ be prime-power decomposition of $|G|$. If $P_i \in Syl_{p_i}(G)$ for each i, then by assumption, $P_i \trianglelefteq G$. We claim that $P_1P_2\cdots P_n \cong P_1 \times P_2 \times \cdots \times P_n$. We proceed by induction on the number of factors. For $n = 1$ the result is trivial because $P_1 \cong P_1$. Now assume $P_1P_2\cdots P_k \cong P_1 \times P_2 \times \cdots \times P_k$, for $1 < k < n$, we show that the result holds for $k+1$. Note that $P_1P_2\cdots P_k \trianglelefteq G$. For if $x_1x_2\cdots x_k \in P_1P_2\cdots P_k$, where $x_i \in P_i$ for each i, then for all $g \in G$, we have

$$gx_1x_2\cdots x_kg^{-1} = gx_1g^{-1}gx_2g^{-1}\cdots gx_kg^{-1} \in P_1P_2\cdots P_k$$

since each $gx_ig^{-1} \in P_i$, as $P_i \trianglelefteq G$. Also since $P_{k+1} \trianglelefteq G$ and $(|P_i|, |P_{k+1}|) = 1$ for $1 \leq i \leq k$. It follows that

$$(|P_1P_2\cdots P_k|, |P_{k+1}|) = (|P_1| \cdot |P_2| \cdots |P_k|, |P_{k+1}|) = 1.$$

Hence $(P_1P_2\cdots P_k) \bigcap P_{k+1} = \{1_G\}$ and so $P_1P_2\cdots P_kP_{k+1}$ is a direct prod-

uct of $P_1P_2\cdots P_k$ and P_{k+1}. Therefore, we have

$$P_1P_2\cdots P_kP_{k+1} = (P_1P_2\cdots P_k)\times P_{k+1} \cong P_1\times P_2\times\cdots\times P_k\times P_{k+1}$$

So the result is true for $k+1$. We deduce that $P_1P_2\cdots P_n \cong P_1\times P_2\times\cdots\times P_n$ and so $|P_1P_2\cdots P_n| = |P_1\times P_2\times\cdots\times P_n| = |P_1|\times|P_2|\times\cdots\times|P_n| = |G|$. From this we conclude that $P_1P_2\cdots P_n \cong P_1\times P_2\times\cdots\times P_n = G$. Lastly, suppose G is a direct product of Sylow p_i-subgroups. We need to show that G is nilpotent. We will proceed by induction on the order of the group G. The result is true if $n = 1$, because if $|G| = p_1^{\alpha_1}$ then G is a p_1-group, so it is nilpotent by Lemma 3.4.11. Now suppose G is a direct product of Sylow p_i-subgroups, for different primes p_i, say $G = P_1\times P_2\times\cdots\times P_n$. and assume the result is true for groups of order smaller then $|G| = \Pi_{i=1}^n p_i^{\alpha_i}$. Consider $Z(G) = Z(P_1)\times Z(P_2)\times\cdots\times Z(P_n)$ (by Corollary 3.4.7), and note that $Z(G)$ is non-trivial since each $Z(P_i)$ is non-trivial. So $G/Z(G) = P_1/Z(P_1)\times P_2/Z(P_2)\times\cdots\times P_n/Z(P_n)$ is a direct product of p_i-groups of order smaller than $|G|$. By induction hypothesis, $G/Z(G)$ is a nilpotent group. So, by Lemma 3.4.3, we have $\gamma_{n+1}(G/Z(G)) = \{1_{G/Z(G)}\} = Z(G)$. Consider the natural map $\rho : G\to G/Z(G)$. Arguing as in the proof of Lemma 3.4.11, we get that G is nilpotent. □

3.4.2 The additivity of μ for finite nilpotent groups

In [36, Theorem 2], it is shown that μ is additive for finite p-groups. We do not reprove this result, but use it as a lemma to prove that μ is additive for finite nilpotent groups. This is more general since all finite p-groups are nilpotent.

Lemma 3.4.13. *Let $G = H\times K$, where H and K are non-trivial finite p-groups, then $\mu(G) = \mu(H) + \mu(K)$.*

Proof. See [36, Theorem 2]. □

The following result appears as [36, Corollary 2] and the details of its proof are omitted. We provide a detailed proof in the following theorem.

Theorem 3.4.14. *Let G and H be non-trivial finite nilpotent groups. Then,*

$$\mu(G \times H) = \mu(G) + \mu(H).$$

Proof. By Theorem 3.4.8, $G \times H$ is nilpotent. Let $|G \times H| = \Pi_{i=1}^{n} p_i^{\alpha_i}$ be a prime-power decomposition of $|G \times H|$. Since G is nilpotent, it follows by Theorem 3.4.12 that, for each $i \in \{1, \ldots, n\}$, there exist $P_i \in Syl_{p_i}(G)$ such that $P_i \trianglelefteq G$. Moreover $G = P_1 \times P_2 \times \cdots \times P_n$. Similarly for H, there exist normal $Q_i \in Syl_{p_i}(H)$ such that $H = Q_1 \times Q_2 \times \cdots \times Q_n$. We now have

$$\begin{aligned} G \times H &= P_1 \times P_2 \times \cdots \times P_n \times Q_1 \times Q_2 \times \cdots \times Q_n \\ &\cong (P_1 \times Q_1) \times (P_2 \times Q_2) \times \cdots \times (P_n \times Q_n). \end{aligned}$$

Hence $\mu(G \times H) = \mu[(P_1 \times Q_1) \times (P_2 \times Q_2) \times \cdots \times (P_n \times Q_n)]$. Since $p_i \neq p_j$ for $i \neq j$, then $(|P_i \times Q_i|, |P_j \times Q_j|) = 1$. Also, P_i and Q_i are p_i-groups. Therefore the conditions of Theorem 3.3.3 applied to $(P_1 \times Q_1) \times (P_2 \times Q_2) \times \cdots \times (P_n \times Q_n)$ and Lemma 3.4.13 applied to each $P_i \times Q_i$, we have

$$\begin{aligned} \mu(G \times H) &= \mu[(P_1 \times Q_1) \times (P_2 \times Q_2) \times \cdots \times (P_n \times Q_n)] \\ &= \mu(P_1 \times Q_1) + \mu(P_2 \times Q_2) + \cdots + \mu(P_n \times Q_n) \\ &= \mu(P_1) + \mu(Q_1) + \mu(P_2) + \mu(Q_2) + \cdots + \mu(P_n) + \mu(Q_n) \\ &= [\mu(P_1) + \mu(P_2) + \cdots + \mu(P_n)] + [\mu(Q_1) + \mu(Q_2) + \cdots + \\ &\quad \mu(Q_n)]. \end{aligned}$$

Now apply Lemma 3.4.13 to both $[\mu(P_1) + \mu(P_2) + \cdots + \mu(P_n)]$ and $[\mu(Q_1) + \mu(Q_2) + \cdots + \mu(Q_n)]$ to get

$$\mu(P_1) + \mu(P_2) + \cdots + \mu(P_n) = \mu(P_1 \times P_2 \times \cdots \times P_n) = \mu(G)$$

and

$$\mu(Q_1) + \mu(Q_2) + \cdots + \mu(Q_n) = \mu(Q_1 \times Q_2 \times \cdots \times Q_n) = \mu(H).$$

Therefore

$$\begin{aligned} \mu(G \times H) &= \mu(P_1 \times P_2 \times \cdots \times P_n) + \mu(Q_1 \times Q_2 \times \cdots \times Q_n) \\ &= \mu(G) + \mu(H) \end{aligned}$$

□

Using Theorem 3.4.14, we deduce the following corollary which deals with the additivity property of μ for finite abelian groups.

Corollary 3.4.15. *Let G and H be finite abelian groups. Then $\mu(G \times H) = \mu(G) + \mu(H)$.*

Proof. Since G and H are abelian, then G and H are nilpotent, by Example 3.4.1. The result follows by Theorem 3.4.14. □

Remark 3.4.1. In the above corollary we have $\mu(G \times H) = \mu(G) + \mu(H)$ for finite abelian groups G and H. A finite abelian group G can be decomposed into the direct product $G = G_1 \times G_2 \times \cdots \times G_n$ of cyclic groups such that each G_i has order $p_i^{\alpha_i}$, where each p_i is a prime divisor of $|G|$: this is known as the Fundamental Theorem of Finite Abelian Groups. By Corollary 3.4.2 we have $\mu(G) = \mu(G_1 \times G_2 \times \cdots \times G_n) = \mu(G_1) + \mu(G_2) + \cdots + \mu(G_n)$. Moreover, we have $\mu(G) = |G_1| + |G_2| + \cdots + |G_n| = \Sigma_{i=1}^{n} p_i^{\alpha_i}$. The latter is shown in [20, Theorem 2] by induction on n, the number of direct factors. This result will be deduced from the proof of Theorem 4.1.6 where we show that if the order of the finite abelian group G is $p_i^{\alpha_i}$, then $\mu(G) = p_i^{\alpha_i}$.

3.5 The class $\mathcal{G}$ of D.Wright

In Theorem 3.4.14, we have shown what appears as [36, Corollary 2], that is, μ is additive for finite nilpotent groups. Using this fact, in [36], the author defined the class, $\mathcal{G}$, of groups such that μ is additive for the direct product of the elements in the class.

Definition 3.5.1. *The defining property of $\mathcal{G}$ is that: a group G is in the class $\mathcal{G}$ whenever G has a nilpotent subgroup G_1 for which $\mu(G_1) = \mu(G)$.*

In the subsection that follows, we shall explore the details as to why the class in the above definition is defined the way it is.

3.5.1 The additivity of μ for the class $\mathcal{G}$

In [36], it is stated without proof that if G and H are non-trivial finite groups and $G, H \in \mathcal{G}$, then $\mu(G \times H) = \mu(G) + \mu(H)$. The latter together with the fact that $\mathcal{G}$ is closed under direct products is the content of the following theorem. The proof of this theorem will clarify the reason for the definition of the class $\mathcal{G}$.

Theorem 3.5.1. *Let G and H be non-trivial groups such that $G, H \in \mathcal{G}$. Then $\mu(G \times H) = \mu(G) + \mu(H)$ and $G \times H \in \mathcal{G}$.*

Proof. If $G, H \in \mathcal{G}$ then there exist nilpotent subgroups K and Q of G and H, respectively, such that $\mu(K) = \mu(G)$ and $\mu(Q) = \mu(H)$. Nilpotent groups are closed under direct products by Theorem 3.4.8, so $K \times Q$ is a nilpotent subgroup of $G \times H$. It follows by Theorem 3.4.14 that $\mu(K \times Q) = \mu(K) + \mu(Q)$. Using Theorem 3.1.2 we get $\mu(G \times H) \leq \mu(G) + \mu(H)$. Also, since $K \times Q \leq G \times H$, then $\mu(K \times Q) \leq \mu(G \times H)$. Putting these results

together, we have

$$\mu(G \times H) \leq \mu(G) + \mu(H) = \mu(K) + \mu(Q) = \mu(K \times Q) \leq \mu(G \times H).$$

We now have $\mu(G \times H) = \mu(G) + \mu(H) = \mu(K \times Q)$, and so $G \times H \in \mathcal{G}$, and the proof is complete. □

Remark 3.5.1. It is a result of D. Wright [36] that the symmetric, alternating and dihedral groups are elements of the class $\mathcal{G}$. The author in [33] improved the extent of $\mathcal{G}$ by showing that all groups of minimal degree at most 6 are contained in $\mathcal{G}$ and listed the groups of minimal degree at most 9 that are not contained in $\mathcal{G}$. Despite all this work, the full extent of $\mathcal{G}$ is not known.

3.6 The additivity property of μ for simple groups

Another class of groups for which μ is additive is the class of simple groups. This is shown in [7, Theorem 3.1] and we present it below.

Theorem 3.6.1. *Let S_i be a simple group with minimal degree $\mu(S_i)$ for $i = 1, \ldots, n$. If*

$$G = S_1 \times \cdots \times S_n,$$

then $\mu(G) = \Sigma_{i=1}^{n} \mu(S_i)$.

Proof. See [7, Theorem 3.1]. □

3.7 Theorem on the additivity of μ

Here, we summarise the results that are currently known regarding the additivity of μ for different classes of finite groups. We are actually trying to

address the question: under what condition(s) is $\mu(G \times H) = \mu(G) + \mu(H)$ for finite groups G and H? The following theorem combines all the results we discussed in this chapter to address this question.

Theorem 3.7.1. *Let G and H be finite groups. Then*

$$\mu(G \times H) = \mu(G) + \mu(H)$$

whenever

(i) $(|G|, |H|) = 1$.

(ii) *G and H are finite nilpotent groups. Furthermore, the result is valid if*

(a) *G and H are finite p-groups,*

(b) *G and H are finite abelian groups.*

(iii) *G and H are finite simple groups.*

(iv) *G and H are elements of the class $\mathcal{G}$.*

We point out that Theorem 3.7.1 in its present form captures the current results known about the additivity of μ for given finite groups G and H with the properties described. Further research on the problem may see the content of the theorem extended to other classes of finite groups. Current research on the topic poses the question on the extent of the elements of the class $\mathcal{G}$. In [36], the question was posed as to whether $\mu(G \times H) = \mu(G) + \mu(G)$ for all finite groups. A counter-example was provided by the referee and it is provided in the addendum of [36]. So, for finite groups G and H, it is not always true that $\mu(G \times H) = \mu(G) + \mu(H)$. This give rise to an open problem: which classes of groups could be added in the list of Theorem 3.7.1?

Chapter 4

Examples on finding the minimal degrees

In this chapter we present the known methods used in finding the minimal degree for some specific classes of finite groups. But, we first need to determine the classes of groups for which Cayley's representation is the permutation representation of minimal degree.

4.1 Minimality of Cayley's representations

The Klein 4-group is nothing but any group isomorphic to $C_2 \times C_2$ and the generalised quaternion group of order 2^n is a group presented as

$$Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, x^y = x^{-1} \rangle, \text{ for } n \geq 3.$$

We mentioned in Chapter 2 that the degree of Cayley's representation is not always minimal. In [20, Theorem 1], it is shown that the degree of Cayley's representation is minimal if and only if the group under consideration is a cyclic group of prime-power order, a generalised quaternion group or the

Klein 4-group. We provide an original and detailed proof of this theorem as it is an integral part when finding the minimal degrees of the group with similar structure to the listed above. To prove [20, Theorem 1], we need to provide a number of preliminary results.

Definition 4.1.1. *Let G be an abelian group. The **rank** of G, denoted by $\mathsf{rank}(G)$, is the cardinality of a maximal linearly independent subset of G over the set of integers. A **free abelian group** is a group G with a subset which generates the group G with the only relation $xy = yx$.*

It follows from Definition 4.1.1 that the rank of an abelian group G is the size of the largest free abelian group contained in G. For finitely generated abelian groups, the rank is the number of elements that minimally generate the group. The fact that non-cyclic p-groups always possess a copy of $C_p \times C_p$, for an odd prime p will be widely used when providing a proof of [20, Theorem 1]. However, to prove the latter we will need to prove some auxiliary lemmas. The first lemma is as follow.

Lemma 4.1.1. *Let p be a prime number and let $G = \langle x_1\rangle \times \cdots \times \langle x_n\rangle := \prod_{i=1}^{n}\langle x_i\rangle$ be an abelian p-group of rank n, where $o(x_i) = p^{\alpha_i}$ for each i, i.e, $\langle x_i\rangle \cong C_{p^{\alpha_i}}$. Define a map $\rho : G \to G$ by $\rho(x) = x^p$. Then, ρ is a homomorphism and the following holds:*

(i) $\mathsf{ker}\rho = \langle x_1^{p^{\alpha_1-1}}\rangle \times \langle x_2^{p^{\alpha_2-1}}\rangle \times \cdots \times \langle x_n^{p^{\alpha_n-1}}\rangle := \prod_{i=1}^{n}\langle x_i^{p^{\alpha_i-1}}\rangle$.

(ii) $\mathsf{Im}\rho = \prod_{i=1}^{n}\langle x_i^p\rangle$.

(iii) $\mathsf{ker}\rho$ *and* $G/\mathsf{Im}\rho$ *are isomorphic to the elementary abelian group of order p^n. Moreover,* $\mathsf{rank}(\mathsf{ker}\rho) = \mathsf{rank}(G/\mathsf{Im}\rho) = \mathsf{rank}(G) = n$.

Proof. (i) Since G is abelian then for all $g, h \in G$ we have $\rho(gh) = (gh)^p = g^p h^p = \rho(g)\rho(h)$. So ρ is a homomorphism. If $\prod_{i=1}^{n} a_i \in \mathsf{ker}\rho$, then

$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} x_i^{b_i}$ for some integers b_i, and $\rho(\prod_{i=1}^{n} a_i) = 1_G$. Therefore $(x_i^{b_i})^p = x_i^{pb_i} = 1_G$ for each i. This implies that $o(x_i) = p^{\alpha_i}$ divides pb_i. So $pb_i = zp^{\alpha_i}$ for some integer z, and $b_i = zp^{\alpha_i - 1}$. Now $a_i \in \langle x_i^{p^{\alpha_i - 1}} \rangle$ for all i, and so $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} x_i^{b_i} = \prod_{i=1}^{n} x_i^{zp^{\alpha_i - 1}} \in \prod_{i=1}^{n} \langle x_i^{p^{\alpha_i - 1}} \rangle$. Thus $\mathsf{ker}\rho \subseteq \prod_{i=1}^{n} \langle x_i^{p^{\alpha_i - 1}} \rangle$.

If $\prod_{i=1}^{n} a_i \in \prod_{i=1}^{n} \langle x_i^{p^{\alpha_i - 1}} \rangle$, then $a_i = (x_i^{p^{\alpha_i - 1}})^z = x_i^{zp^{\alpha_i - 1}}$ for some integer z, for each i. From this, we deduce that $a_i^p = (x_i^{zp^{\alpha_i - 1}})^p = x_i^{zpp^{\alpha_i - 1}} = x_i^{zp^{\alpha_i}} = (x_i^{p^{\alpha_i}})^z = (1_G)^z = 1_G$. Therefore $\prod_{i=1}^{n} a_i \in \mathsf{ker}\rho$, from which we obtain

$\prod_{i=1}^{n} \langle x_i^{p^{\alpha_i - 1}} \rangle \subseteq \mathsf{ker}\rho$.

(ii) If $\prod_{i=1}^{n} a_i \in \mathsf{Im}\rho$, then there exists $\prod_{i=1}^{n} b_i \in G = \prod_{i=1}^{n} \langle x_i \rangle$ such that $\rho(\prod_{i=1}^{n} b_i) = \prod_{i=1}^{n} a_i$. But $\prod_{i=1}^{n} b_i = \prod_{i=1}^{n} x_i^{z_i}$ for some integers z_i. Observe that $\rho(\prod_{i=1}^{n} b_i) = \rho(\prod_{i=1}^{n} x_i^{z_i}) = (\prod_{i=1}^{n} x_i^{z_i})^p = \prod_{i=1}^{n} x_i^{pz_i}$, hence $\prod_{i=1}^{n} x_i^{pz_i} = \prod_{i=1}^{n} a_i$. It follows that $a_i = x_i^{pz_i}$, for each i. Therefore $a_i \in \langle x_i^p \rangle$, and so $\prod_{i=1}^{n} a_i \in \prod_{i=1}^{n} \langle x_i^p \rangle$. This shows that $\mathsf{Im}\rho \subseteq \prod_{i=1}^{n} \langle x_i^p \rangle$.

If $\prod_{i=1}^{n} a_i \in \prod_{i=1}^{n} \langle x_i^p \rangle$, then for each i, there exists z_i such that $a_i = x_i^{pz_i}$. It is now transparent that $\rho(\prod_{i=1}^{n} x_i^{z_i}) = \prod_{i=1}^{n} a_i$, and so $\prod_{i=1}^{n} a_i \in \mathsf{Im}\rho$. Hence $\prod_{i=1}^{n} \langle x_i^p \rangle \subseteq \mathsf{Im}\rho$.

(iii) We first note that for a cyclic p-group, $P = \langle x \rangle$, of order p^m, we have $\mathsf{ker}\rho \cong P/\mathsf{Im}\rho \cong C_p$, where $\rho : P \to P$ is defined by $\rho(x^i) = (x^i)^p$ for all $x^i \in P$. To see this, observe that $\mathsf{ker}\rho = \langle x^{p^{m-1}} \rangle$ and $\mathsf{Im}\rho = \langle x^p \rangle$, by part (i) and part (ii) of this lemma, respectively. Also observe that, if $x^i \in G$ with $o(x^i) = l$ and $l = rs$ for some positive integers r and s, then $o((x^i)^r) = s$. This holds since we have $((x^i)^r)^s = (x^i)^{rs} = x^l = 1_G$, and so $o((x^i)^r)$ divides s. Now suppose that $o((x^i)^r) = z$ for some positive integer $z < s$. Then $(x^i)^{rz} = ((x^i)^z)^r = 1_G$, and

$rz < rs = l$, a contradiction. So, such z does not exist. Therefore $o((x^i)^r) = s$. Using this property, we get that, since $o(x) = p^m$ and $p^m = p^{m-1}p$ then $o(x^{p^{m-1}}) = p$. It follows that, $|\mathsf{ker}\rho| = p$. Similarly, since $o(x^p) = p^{m-1}$, we have, $|\mathsf{Im}\rho| = p^{m-1}$. It follows that $|P/\mathsf{Im}\rho| = |P|/|\mathsf{Im}\rho| = p^m/p^{m-1} = p$. Since both $\mathsf{ker}\rho$ and $P/\mathsf{Im}\rho$ are cyclic of order p, then $\mathsf{ker}\rho \cong P/\mathsf{Im}\rho \cong C_p$. If we define $\rho_i : \langle x_i\rangle \to \langle x_i\rangle$ by $\rho_i(x_i^j) = (x_i^j)^p$ for all $x_i^j \in \langle x_i\rangle$ then part (i) of this lemma becomes $\mathsf{ker}\rho = \mathsf{ker}\prod_{i=1}^n \rho_i = \prod_{i=1}^n \mathsf{ker}\rho_i \cong \prod_{i=1}^n C_p$. Part (ii) becomes $\mathsf{im}\rho = \mathsf{Im}\ \prod_{i=1}^n \rho_i = \prod_{i=1}^n \mathsf{Im}\rho_i$ and so $G/\mathsf{Im}\rho = (\prod_{i=1}^n \langle x_i\rangle)/(\prod_{i=1}^n \mathsf{Im}\rho_i) \cong \prod_{i=1}^n (\langle x_i\rangle/\mathsf{Im}\rho_i) \cong \prod_{i=1}^n C_p$. Hence $\mathsf{ker}\ \rho \cong G/\mathsf{im}\rho \cong \prod_{i=1}^n C_p$. That is, $\mathsf{ker}\rho$ and $G/\mathsf{Im}\rho$ are isomorphic to the elementary abelian group of order p^n. So, $\mathsf{ker}\rho$ and $G/\mathsf{Im}\rho$ are both generated by n elements. In particular, $\mathsf{rank}(\mathsf{ker}\rho) = \mathsf{rank}(G/\mathsf{Im}\rho) = \mathsf{rank}(G) = n$.

□

Lemma 4.1.2. *Let p be an odd prime and G a group of order p^3. Then the map $\rho : G \to G$ defined by $\rho(g) = x^p$ is a homomorphism such that $\mathsf{Im}\rho \leq Z(G)$. Furthermore, if G is non-cyclic, then $|\mathsf{ker}\rho| \in \{p^2, p^3\}$.*

Proof. If G is abelian, then it follows that $\rho(gh) = (gh)^p = g^p h^p = \rho(g)\rho(h)$. In addition, we have $\mathsf{Im}\rho \leq Z(G) = G$. If G is non-cyclic abelian, by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to either $C_p \times C_p \times C_p = \langle x_1\rangle \times \langle x_2\rangle \times \langle x_3\rangle$ or $C_{p^2} \times C_p = \langle y_1\rangle \times \langle y_2\rangle$. It follows by Lemma 4.1.1 (iii) that $\mathsf{ker}\rho$ is an elementary abelian group of order p^3 or p^2, respectively. That is, $|\mathsf{ker}\rho| \in \{p^2, p^3\}$, and we are done.
Now suppose G is non-abelian. Therefore $Z(G) \neq G$. Since every p-group has a non-trivial center, $|Z(G)| \neq 1$. So $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p^2$, then $G/Z(G)$ is cyclic of order p. That is $G/Z(G) \cong C_p$. However, the latter

implies that G is abelian. This is a contradiction, so $|Z(G)| \neq p^2$. Therefore $|Z(G)| = p$. This implies that $|G/Z(G)| = p^2$, so that $G/Z(G)$ is abelian. Hence, for any $x, y \in G$, we have $(xZ(G))(yZ(G)) = (yZ(G))(xZ(G))$. This implies that $(xy)Z(G) = (yx)Z(G)$, and so $((xy)Z(G))((yx)Z(G))^{-1} = 1_{G/Z(G)}$. The latter implies that $(xyx^{-1}y^{-1})Z(G) = Z(G)$, hence $xyx^{-1}y^{-1} = [x, y] \in Z(G)$. Therefore the $G' \leq Z(G)$. Since G is non-abelian, $G' \neq \{1_G\}$. Hence $|G'| \geq p = |Z(G)|$. It follows that $G' = Z(G) \cong C_p$. It is now clear that $[x, y]^p = 1_G$. Since p divides $p(p-1)/2$, then $[x, y]^{p(p-1)/2} = 1_G$. Using the fact that $G' = Z(G) \cong C_p$, is not difficult to verify that $x^p y^p = [x, y]^{p(p-1)/2}(xy)^p$. Since $[x, y]^{p(p-1)/2} = 1_G$, it follows that $x^p y^p = (xy)^p$. That is, $\rho(xy) = (xy)^p = \rho(x)\rho(y) = \rho(x)\rho(y)$. Thus ρ is a homomorphism. Finally, observe that $[x^p, y] = x^p y x^{-p} y^{-1} = x^p y(\underbrace{x^{-1}x^{-1} \cdots x^{-1}x^{-1}}_{p\text{-times}})y^{-1} = x^p y(\underbrace{x^{-1}(y^{-1}y)x^{-1} \cdots x^{-1}(y^{-1}y)x^{-1}}_{p\text{-times}})y^{-1} = x^p(\underbrace{(yx^{-1}y^{-1}) \cdots (yx^{-1}y^{-1})}_{p\text{-times}}) = x^p(yx^{-1}y^{-1})^p = (xyx^{-1}y^{-1})^p = [x, y]^p = 1_G$, for all $x, y \in G$. We now have $[x^p, y] = 1_G$, so that $x^p y = yx^p$. Therefore $\rho(x)y = y\rho(x)$, for all $x, y \in G$. It follows that $\mathsf{Im}\rho \leq Z(G)$. By the First Isomorphism Theorem, $G/\mathsf{ker}\rho \cong \mathsf{Im}\rho \leq Z(G)$. Since $|Z(G)| = p$, then $|G/\mathsf{ker}\rho| = |G|/|\mathsf{ker}\rho| \in \{1, p\}$. Now, since $|G| = p^3$, we deduce that $|\mathsf{ker}\rho| \in \{p^2, p^3\}$. The proof is now complete. □

There are exactly $p + 1$ unique p-subgroups of order p of an elementary abelian p-group of order p^2. We prove this fact in the following lemma.

Lemma 4.1.3. *Let p be a prime number. Then there are $p + 1$ subgroups of order p in any group $G \cong C_p \times C_p$.*

Proof. Suppose $G = \langle x \rangle \times \langle y \rangle \cong C_p \times C_p$. We claim that $\langle x \rangle, \langle xy \rangle, \langle xy^2 \rangle, \langle xy^3 \rangle, \ldots, \langle xy^{p-1} \rangle$ and $\langle y \rangle$ are the only distinct subgroups of order p in G. Identify

$\langle x\rangle$ by $\langle x\rangle \times \{1_G\}$ and $\langle y\rangle$ by $\{1_G\} \times \langle y\rangle$ in G. Therefore $|\langle x\rangle| = |\langle y\rangle| = |\langle x\rangle \times \{1_G\}| = |\{1_G\} \times \langle y\rangle| = p$. Then $\langle x\rangle$ and $\langle y\rangle$ are distinct subgroups of order p in G. Consider the group $\langle xy^k\rangle$, for $0 \leq k \leq p-1$. We need to find the order of xy^k, for each k. To do this, suppose $(xy^k)^n = 1_G$, for some positive integer n. Since G is abelian, this implies that $x^n y^{kn} = 1_G$. So, $y^{kn} = x^{-n} \in \langle x\rangle \cap \langle y\rangle = \{1_G\}$. It follows that $y^{kn} = x^{-n} = 1_G$. Since $o(x) = o(y) = p$, we have that p divides both kn and $-n$, and so p divides n. On the other hand, $(xy^k)^p = x^p y^{kp} = x^p (y^p)^k = 1_G (1_G)^k = 1_G$, that is, $o(xy^k)$ divides p. Consequently, $o(xy^k) = p$. To prove that the subgroups $\langle x\rangle, \langle xy\rangle, \langle xy^2\rangle, \langle xy^3\rangle, \ldots, \langle xy^{p-1}\rangle$ and $\langle y\rangle$ are all distinct from one another, it is enough to show that the generator of each subgroup is not an element of another subgroup. That is, we show that $xy^k \notin \langle xy^l\rangle$, whenever $\langle xy^k\rangle \neq \langle xy^l\rangle$, for $0 \leq k, l \leq p-1$. Suppose to the contrary, that is, suppose that $xy^k \in \langle xy^l\rangle$ for some integers k and l where $0 \leq k, l \leq p-1$ such that $\langle xy^k\rangle \neq \langle xy^l\rangle$. Then there exists an integer z, such that $xy^k = (xy^l)^z$. Since G is abelian, we have $xy^k = x^z y^{lz}$, and so $x^{1-z} = y^{lz-k} \in \langle x\rangle \cap \langle y\rangle = \{1_G\}$. Therefore $x^{1-z} = y^{lz-k} = 1_G$, and so p divides both $1-z$ and $lz-k$. Now observe that $lz - k = l(z-1) + l - k$, so that p divides $l(z-1) + (l-k)$. This holds if an only if p divides both $l(z-1)$ and $(l-k)$. However, $0 \leq k, l \leq p-1$, so p divides $l-k$ implies that $l = k$, since $0 \leq l - k \leq p-1 < p$. This contradicts the condition that $\langle xy^k\rangle \neq \langle xy^l\rangle$. So, we have shown that the subgroups $\langle x\rangle, \langle xy\rangle, \langle xy^2\rangle, \langle xy^3\rangle, \ldots, \langle xy^{p-1}\rangle$ and $\langle y\rangle$ are all distinct from one another. Moreover, since each subgroup has order p, then each subgroup is isomorphic to C_p. Clearly if we let $\mathcal{O} = \{\langle x\rangle, \langle xy\rangle, \langle xy^2\rangle, \langle xy^3\rangle, \ldots, \langle xy^{p-1}\rangle, \langle y\rangle\}$, then $|\mathcal{O}| = p+1$.

We now show that there is no other p-subgroup of order p in G except the above mentioned subgroups. Suppose H is a subgroup of order p in G.

Then $H = \langle g \rangle \cong C_p$, for some $g \in G$. Now, the intersection of any two subgroups in $\mathcal{O}$ is $\{1_G\}$. Also, 1_G is in the union of all subgroups in $\mathcal{O}$ and each of the $p+1$ elements in $\mathcal{O}$ contains $p-1$ non-trivial elements. So, the number of elements of G that fall into the union of all the subgroups in $\mathcal{O}$ is $1 + (p+1)(p-1) = p^2 = |G|$. So that the union of all the subgroups in $\mathcal{O}$ is G, i.e., $G = \bigcup \mathcal{O} = \bigcup_{k=0}^{p} \langle xy^k \rangle \cup \langle y \rangle$. It follows that $g \in P$, for some $P \in \mathcal{O}$. Therefore $H = \langle g \rangle \leq P$. However, $|H| = |P| = p$, implies $H = P$. So, the subgroups of G in $\mathcal{O}$ are the only subgroups of order p. □

We are now ready to prove that a finite non-cyclic p-group contains a normal subgroup isomorphic to $C_p \times C_p$, for p odd.

Theorem 4.1.4. *Let G be a finite non-cyclic p-group of order p^α, for p odd. Then G contains a normal subgroup H that is isomorphic to the elementary abelian group $C_p \times C_p$.*

Proof. We proceed by induction on the $|G| = p^\alpha$, that is, we proceed by induction on α. Note that $\alpha \neq 1$ since G is non-cyclic. So we start the induction at $\alpha = 2$. Therefore $|G|$ is a group of order p^2, and so G is abelian. It follows that $G \cong C_p \times C_p$. Take $H = G$, then H is a normal subgroup of G isomorphic to $C_p \times C_p$. Hence, the result holds for $\alpha = 2$. Suppose the result holds for any p-group of order p^k, where $k > 2$. We show that the result holds for groups of order p^{k+1}. Since G is a p-group, then $Z(G) \neq \{1_G\}$. Therefore p divides $|Z(G)|$, and so there exists $z \in Z(G)$ of order p, by Cauchy's Theorem. The central subgroup $P = \langle z \rangle$ is normal in G. So, the group G/P is a p-group of order p^k. We consider two cases, namely, the case where G/P is cyclic and the case where G/P is non-cyclic.

Suppose G/P is cyclic, then by the Third Isomorphism Theorem, we have $(G/P)/(Z(G)/P) \cong G/Z(G)$. Now, G/P is cyclic, so $G/Z(G)$ is cyclic since

$G/Z(G)$ is isomorphic to a quotient group of G/P. It follows that G is abelian. Since G is non-cyclic, then G is generated by at least two elements. In particular, G is a finite abelian group with $\mathsf{rank}(G) \geq 2$. Let $\rho : G \to G$ be defined by $\rho(x) = x^p$, for all $x \in G$. Then, by Lemma 4.1.1 (iii), $\mathsf{ker}\rho$ is the elementary abelian p-group whose rank is the same as that of G. Thus $\mathsf{ker}\rho \cong \underbrace{C_p \times C_p \times \cdots C_p}_{r\text{-times}}$, for some integer $r \geq 2$. It is now clear that $\mathsf{ker}\rho$ contains a normal subgroup H isomorphic to $C_p \times C_p$, where the normality of $H \leq G$ follows by the fact that G is abelian.

Now suppose G/P is non-cyclic. By the induction hypothesis, there is a normal subgroup $Q \leq G/P$ such that $Q \cong C_p \times C_p$. By the Correspondence Theorem, there exists a normal subgroup M of G such that $Q = M/P$. Note that $p^2 = |Q| = |M/P| = |M|/|P| = |M|/p$, so M is a subgroup of order p^3 and M is non-cyclic since M/P is non-cyclic. Let $\rho : M \to M$ be defined by $\rho(x) = x^p$, for all $x \in M$. Since M is a p-group of order p^3, by Lemma 4.1.2, $\mathsf{Im}\rho \leq Z(M)$ and $|\mathsf{ker}\rho| \in \{p^2, p^3\}$. Moreover, if $x \in \mathsf{ker}\rho$ such that $x \neq 1_G$, then $o(x) = p$. That is, $\mathsf{ker}\rho$ consists precisely of the elements of M of order p. Now, if $\beta \in \mathsf{Aut}(M)$, then $o(\beta(x)) = p$, since β preserves the order of elements. In particular, $\beta(x) \in \mathsf{ker}\rho$. Thus $\beta(\mathsf{ker}\rho) \subseteq \mathsf{ker}\rho$. Since M is finite, we have $\beta(\mathsf{ker}\rho) = \mathsf{ker}\rho$. Therefore $\mathsf{ker}\rho$ is characteristic subgroup of M. So $\mathsf{ker}\rho$ is normal in G since M is normal in G.

Now, if $|\mathsf{ker}\rho| = p^2$, then $\mathsf{ker}\rho$ is isomorphic to either C_{p^2} or $C_p \times C_p$. However, $\mathsf{ker}\rho$ has no element of order p^2. Therefore $\mathsf{ker}\rho \cong C_p \times C_p$. So, taking $H = \mathsf{ker}\rho$, we have that H is normal in G and $H \cong C_p \times C_p$.

Now, suppose $|\mathsf{ker}\rho| = p^3$ and let $K = \mathsf{ker}\rho$. Again, $\mathsf{ker}\rho$ has no element of order p^2 or p^3, so $K = \mathsf{ker}\rho \cong C_p \times C_p \times C_p$. It follows that $K/P \cong C_p \times C_p$. Let $\mathcal{O} := \{Q/P \leq K/P \mid o(Q/P) = p\}$. By Lemma 4.1.3, $|\mathcal{O}| = p + 1$.

Now, note that G/P acts on the elements of $\mathcal{O}$ by conjugation. Given $Q/P \in \mathcal{O}$, we denote by $(G/P)_{Q/P}$, the stabiliser of Q/P and denote by $Orb_{G/P}(Q/P)$, the orbit of Q/P. By the Orbit-Stabilizer Theorem, we have $|G/P| = |(G/P)_{Q/P}| \times |Orb_{G/P}(Q/P)|$, which implies that $\frac{|G/P|}{|(G/P)_{Q/P}|} = |Orb_{G/P}(Q/P)|$, that is, $[G/P : (G/P)_{Q/P}] = |Orb_{G/P}(Q/P)|$. Now G/P is a p-group, so $|Orb_{G/P}(Q/P)|$ is a power of p. Since $|\mathcal{O}| = p + 1$, then there is one orbit of order p and another of order 1. Let $N/P \leq K/P$ be in the orbit of order 1. Then N/P is normal in G/P since the action under consideration is conjugation. By the Correspondence Theorem, N is a normal subgroup of G. Since $N/P \in \mathcal{O}$, then $|N/P| = p$, and so $|N| = p^2$ since $|P| = p$. It follows that N is an elementary abelian subgroup of K. Finally, set $H = N \cong C_p \times C_p$ and the result follows. □

The semidihedral group of order 2^n is a group presented by $SD_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, x^y = x^{2^{m-2}-1} \rangle$. Theorem 4.1.5 below is a more general result in contrast with the above theorem. The difference being the fact that $p = 2$ is taken into consideration and that the order of the normal abelian group is not specified to be p^2 as in Theorem 4.1.4. However, we will use both Theorem 4.1.4 and Theorem 4.1.5 for the remainder of this dissertation.

Theorem 4.1.5. *(i) If P is a p-group with no non-cyclic abelian normal subgroups, then either P is cyclic or $p = 2$ and P is isomorphic to D_{2n}, $n \geq 4$, Q_{2^n}, $n \geq 3$, or SD_{2^n}, $n \geq 4$.*
(ii) If P is a p-group with at most one subgroup of order p, then either P is cyclic or $p = 2$ and P is isomorphic to Q_{2^n}, $n \geq 3$.

Proof. See [13, Theorem 4.10] or [18, Theorem 6.11 and Theorem 6.12]. □

Definition 4.1.2. *Let G be a group with the property that there exists a*

positive integer n such that, for every $g \in G$, $g^n = 1_G$. The ***exponent*** *of G, denoted $\mathsf{exp}(G)$, is the smallest positive integer n such that, for every $g \in G$, $g^n = 1_G$.*

Thus, for every finite group G, $\mathsf{exp}(G)$ divides $|G|$. Also, for every group G that has an exponent, we have $o(g)$ divides $\mathsf{exp}(G)$, for every $g \in G$.

Theorem 4.1.6. *The degree of Cayley's representation of a group G is minimal if and only if G is*

(i) a cyclic group of prime-power order, or

(ii) a generalised quaternion 2-group, or

(iii) the Klein 4-group.

Proof. (i) Suppose G is a cyclic group of prime-power order, say $|G| = p^n$. Then $G \cong C_{p^n}$. It follows that the subgroup lattice of G is a chain. That is, every subgroup of G is contained in all of the subgroups of G of larger order. Hence, every non-trivial subgroup of G contains the first non-trivial subgroup and this non-trivial subgroup contains the trivial subgroup. So, Cayley's representation is the only faithful representation of minimal degree. Therefore, $\mu(G) = |G| = \mu(C_{p^n}) = p^n$.

(ii) Suppose $G = Q_{2^n}$, the generalised quaternion. Then G is presented as $Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, x^y = x^{-1} \rangle$, for $n \geq 3$. Note that $Z(Q_{2^n}) = \langle x^{2^{n-2}} \rangle = \{1_{Q_{2^n}}, x^{2^{n-2}}\}$ $(= \{1_{Q_{2^n}}, y^2\} = \langle y^2 \rangle)$, so $|Z(Q_{2^n})| = 2$. It follows by Theorem 4.1.5 (ii) that $Z(Q_{2^n})$ is the unique subgroup of order 2 in Q_{2^n}. However, all the subgroups of Q_{2^n} have order 2^m, for some $m \leq n$. Therefore the order of $Z(Q_{2^n})$ divides

the order of all other subgroups Q_{2^n}. Since $Z(Q_{2^n})$ is the unique subgroup of order 2, and by Lagrange's Theorem, we have that all the non-trivial subgroups of Q_{2^n} contains the normal subgroup $Z(Q_{2^n})$. So, Cayley's representation is the only representation with a trivial core. Hence, Cayley's representation is the only faithful representation of minimal degree. This implies that $\mu(Q_{2^n}) = |Q_{2^n}| = 2^n$.

(iii) Suppose that G is the Klein 4-group. Then $G \cong C_2 \times C_2$. It follows by Corollary 3.4.2 that $\mu(G) = \mu(C_2 \times C_2) = \mu(C_2) + \mu(C_2) = 2 + 2 = 4 = |G|$. So, the Cayley's representation is of minimal degree.

Conversely suppose that Cayley's representation is of minimal degree for G. We prove that G is a cyclic group of prime-power order, a generalised quaternion 2-group, or the Klein 4-group. We start by proving that G is a p-group. Suppose to the contrary that G is not a p-group. So the prime power decomposition of $|G|$ contains at least two distinct primes p and q. Write $|G| = p^n q^m z$, where n, m and z are positive integers such that z is divisible by neither p nor q. By Sylow's Theorem, there exist subgroups H_p and H_q of G with orders p^n and q^m, respectively. Moreover,

$$core_G(H_p) = \bigcap_{g \in G} (H_p)^g \leq H_p,$$

similarly $core_G(H_q) \leq H_q$. We now have,

$$core_G(H_p) \bigcap core_G(H_q) \leq H_p \bigcap H_q = \{1_G\}.$$

Hence

$$core_G(H_p) \bigcap core_G(H_g) = \{1_G\}.$$

This shows that $\mathcal{H} = \{H_p, H_q\}$ is a faithful representation of G. Furthermore,

$$\begin{aligned} deg(\mathcal{H}) &= \sum_{H \in \mathcal{H}} [G : H] \\ &= [G : H_p] + [G : H_q] \\ &= q^m z + p^n z \\ &= (q^m + p^n) z \\ &< p^n q^m z \\ &= |G|. \end{aligned}$$

Since $deg(\mathcal{H}) < |G|$ then the Cayley's representation is not minimal: a contradiction, and so G is a p-group. Let $|G| = p^n$, for some positive prime p and positive integer n. We show that $p = 2$.

Suppose p is odd, then by Theorem 4.1.4, G contains a copy of $C_p \times C_p$. Therefore G has a subgroup $H = P \times Q \cong C_p \times C_p$, where P and Q are subgroups of G of order p, such that $P \cap Q = \{1_G\}$. Now,

$$core_G(P \cap Q) \leq P \cap Q = \{1_G\},$$

which implies that

$$core_G(P) \bigcap core_G(Q) = core_G(P \cap Q) = \{1_G\}.$$

This shows that $\mathcal{R} = \{P, Q\}$ is a faithful representation of G. Since $|G| = p^n$

and $|P| = |Q| = p$ and p is odd, it follows that

$$\begin{aligned} deg(\mathcal{R}) &= \sum_{H \in \mathcal{R}} [G : H] \\ &= [G : P] + [G : Q] \\ &= p^{n-1} + p^{n-1} \\ &= 2p^{n-1} \\ &< pp^{n-1} \\ &= p^n \\ &= |G|. \end{aligned}$$

This again contradicts the minimality of Cayley's representation. So, G is a 2-group, say $|G| = 2^r$, for some integer positive r. We now show that G cannot contain an element of order 4 and more than one element of order 2. Suppose $x, y \in G$ are such that $o(x) = 4$ and $o(y) = 2$ and y is not a power of x. It follows that $\langle x \rangle \cap \langle y \rangle = \{1_G\}$ and so

$$core_G(\langle x \rangle \cap \langle y \rangle) \leq \langle x \rangle \cap \langle y \rangle = \{1_G\}.$$

Therefore

$$core_G(\langle x \rangle) \bigcap core_G(\langle y \rangle) = core_G(\langle x \rangle \cap \langle y \rangle) = \{1_G\}.$$

Hence, $\mathcal{O} = \{\langle x \rangle, \langle y \rangle\}$ is a faithful representation of G with

$$deg(\mathcal{O}) = [G : \langle x \rangle] + [G : \langle y \rangle] = \tfrac{|G|}{4} + \tfrac{|G|}{2} = \tfrac{3}{4}|G| < |G|.$$

This again, contradicts the minimality of Cayley's representation. So, we now have that G is a 2-group which does not have an element of order 4 or G is a 2-group with at most one element of order 2. That is, G is a 2-group with $\mathsf{exp}(G) = 2$ (since $\mathsf{exp}(G)$ divides $|G| = 2^r$ and 4 does not divide 2^r) or G is a 2-group with at most one element of order 2. We consider these two

cases separately.

Suppose G is a 2-group with $\mathsf{exp}(G) = 2$, and write $|G| = 2^r = 2 \times 2^{r-1}$. Then we can express G as a direct product, i.e., $G = K_1 \times K_2$, for some subgroups K_1 and K_2, such that $|K_1| = 2$ and $|K_2| = 2^{r-1}$. We deduce that

$$core_G(K_1) \bigcap core_G(K_2) = core_G(K_1 \cap K_2) = \{1_G\}.$$

So the representation $\mathcal{K} = \{K_1, K_2\}$ is faithful. Since Cayley's representation is minimal, we must have $\mu(G) = |G| = 2^r$. Now, by the minimality of $\mu(G)$, we obtain $\mu(G) \leq deg(\mathcal{K}) = [G : K_1] + [G : K_2]$, so that, $2^r \leq 2^{r-1} + 2$. However, the latter inequality holds only for $r = 1$ and $r = 2$. We consider both cases:

(i) If $r = 1$, then $|G| = 2$, and so G is cyclic.

(ii) If $r = 2$, then $|G| = 2^2 = 4$ and $G \cong C_{2^2}$ or $G \cong C_2 \times C_2$. That is, G is a cyclic group of prime-power order or G is the Klein 4-group.

Finally, suppose that G has at most one subgroup of order 2. Then by Theorem 4.1.5 (ii), we obtain that G is a cyclic group of prime-power order or a generalised quaternion. □

Remark 4.1.1. As a result of the above theorem, we deduce that $\mu(C_{p^n}) = p^n$, so that if $G = \langle g \rangle$ such that $|G| = |\langle g \rangle| = p^n$, for some prime p, and positive integer n, then $\mu(G) = p^n$. We also deduce that $\mu(Q_{2^n}) = 2^n$ and $\mu(C_2 \times C_2) = 4$,

4.2 Concrete examples on finding $\mu(G)$

We now produce a few concrete examples on how to find the minimal degree of a given finite group. We start by examining in detail the dihedral group

D_{2n}, for the case where $n = 4$.

Example 4.2.1. $D_8 = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle$ is a dihedral group of order 8. From $x^4 = y^2 = 1$, we have $x^{-1} = x^3$ and $y = y^{-1}$. From $x^y = x^{-1}$, we get $yxy^{-1} = x^{-1}$. So that $yx = x^{-1}y$. From this, we have $yx^m = x^{-m}y = x^{4-m}y$, for all $m \in \mathbb{Z}$. Using these equations we get

$$D_8 = \{1_{D_8}, x, x^2, x^3, y, xy, x^2y, x^3y\}.$$

Let us find conjugacy classes of D_8 (under inner automorphism $\alpha : D_8 \times D_8 \to D_8$ defined by $\alpha(a, b) = a^b$ for all $a, b \in D_8$). We have $x^y = x^{-1} = x^3$, and so $(x^i)^y = (x^y)^i = x^{-i}$ for all $i \in \mathbb{Z}$, because α is a homomorphism. Thus $[x]$ contains x and $x^y = x^3$. Also, since $(x^3)^y = x^{-3} = x$, we conclude that $[x] = \{x, x^3\}$. Now $(x^2)^y = (x^y)^2 = x^{-2} = x^2$, so $[x^2] = \{x^2\}$. Note that $y^x = xyx^{-1} = xxy = x^2y$. Conjugating x^2y by x again, we obtain $(x^2y)^x = (x^2)^x(y^x) = x^2x^2y = x^4y = y$. We now conjugate x^2y by y to obtain $(x^2y)^y = (x^2)^y(y)^y$ because α is a homomorphism. Therefore $(x^2y)^y = (x^2)^y(y)^y = (yx^2y^{-1})y = (x^{-2}yy^{-1})y = x^2y$. We now have $[y] = \{y, x^2y\}$. Finally, observe that $(xy)^x = x^xy^x = xx^2y = x^3y$, and since we have exhausted all the non-identity elements of D_8, we deduce that $[xy] = \{xy, x^3y\}$. So the conjugacy classes of D_8 are:

(i) $[1_{D_8}] = \{1_{D_8}\}$

(ii) $[x] = \{x, x^3\}$

(iii) $[x^2] = \{x^2\}$

(iv) $[y] = \{y, x^2y\}$

(v) $[xy] = \{xy, x^3y\}$.

Using Theorem 2.2.4, we have

$$Z(D_8) = (1_{D_8}) \cup (x^2) = \{1_{D_8}\} \cup \{x^2\} = \langle x^2 \rangle$$

We now find all normal subgroups of D_8, by just finding the unions of conjugacy classes which contain the identity element and closed under products. These unions will be closed under inverses too, because in a finite group, G we always have that, for all $g \in G$, $g^{-1} = g^m$ for some positive integer m. Specifically, $x^{-1} = x^3$ and $y^{-1} = y$ for D_8. Using Lagrange's Theorem, we obtain the following non-trivial normal subgroups of D_8:

(i) $(1_{D_8}) \cup (x) \cup (x^2) = \{1_{D_8}, x, x^2, x^3\} = \langle x \rangle$

(ii) $(1_{D_8}) \cup (x^2) \cup (y) = \{1_{D_8}, x^2, y, x^2y\} = \langle x^2, y \rangle$

(iii) $(1_{D_8}) \cup (x^2) \cup (xy) = \{1_{D_8}, x^2, xy, x^3y\} = \langle x^2, xy \rangle$

(iv) $Z(D_8) = (1_{D_8}) \cup (x^2) = \{1_{D_8}\} \cup \{x^2\} = \langle x^2 \rangle$.

The other two trivial normal subgroups of D_8 are $\{1_{D_8}\}$ and D_8. The subgroups which are not normal in D_8 are $\langle y \rangle$, $\langle xy \rangle$, $\langle x^2y \rangle$ and $\langle x^3y \rangle$. All these subgroups have two elements. The normal subgroup lattice and the lattice of all subgroups are shown on Figure 4 and Figure 5, respectively.

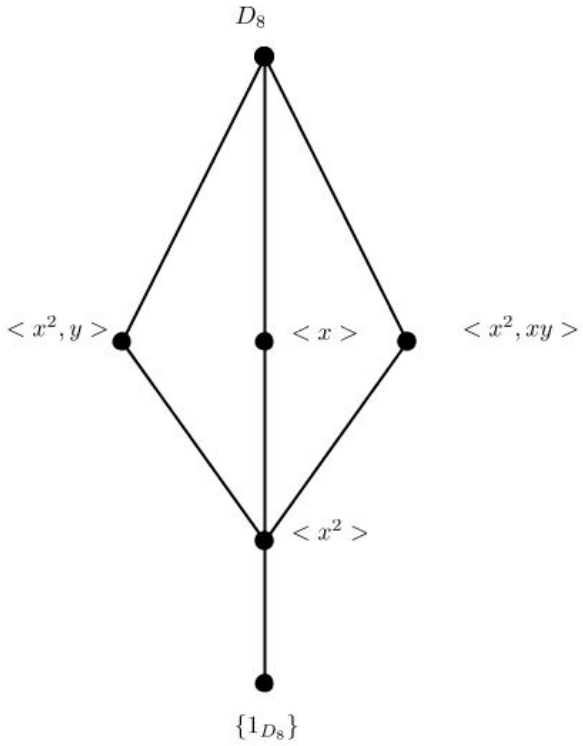

Figure 4

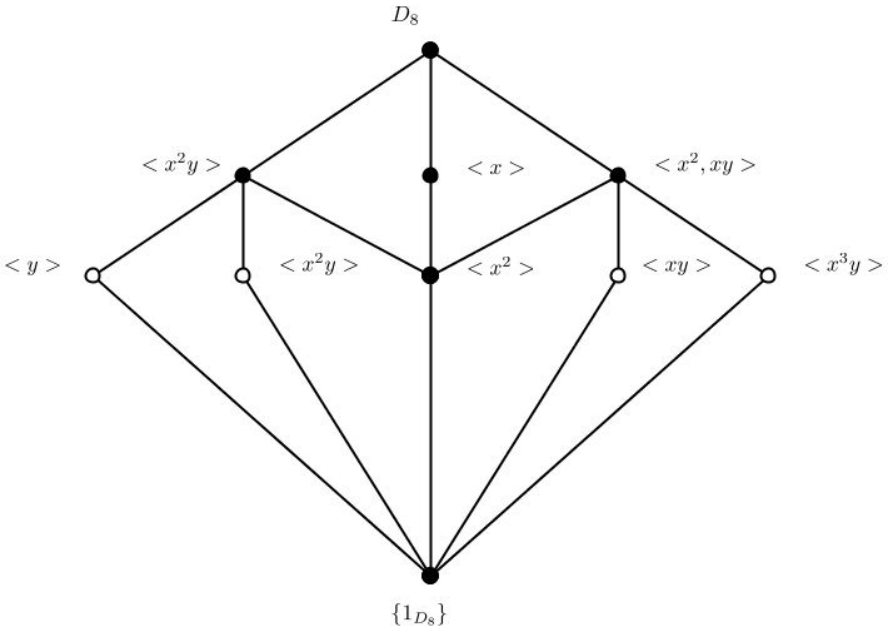

Figure 5

Let $\mathcal{D}$ be any minimal faithful representation of D_8. Then by inspecting the lattices in Figure 4 and Figure 5 we see that if $\mathcal{D}$ contained a normal subgroup and do not contain $\{1_{D_8}\}$, then it must contain one of these: $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$ or $\langle x^3y\rangle$. Notice that if $H \in \{\langle y\rangle, \langle xy\rangle, \langle x^2y\rangle$ or $\langle x^3y\rangle\}$, then $core_{D_8}(H) = \{1_{D_8}\}$, since for each case, H has only $\{1_{D_8}\}$ as its (normal) subgroup. However, $[D_8 : H] = 4$ and H is not normal. So, by minimality of $\mathcal{D}$, $\mathcal{D}$ must contain only one of the subgroups which are not normal. Thus $\mathcal{D}$ consist of only one subgroup, i.e., $\mathcal{D}$ is a transitive permutation representation, hence $\mu(D_8) = [D_8 : H] = 4$.

In the following example we find the minimal degree of the group

$$Q = \langle a, b \mid a^3 = b^4 = 1, a^b = a^{-1}\rangle$$

by constructing a subgroup of the symmetric group S_7 that is isomorphic to

Q. Furthermore, we also clarify that $Q \notin \mathcal{G}$. So, not all the finite groups are in the class $\mathcal{G}$.

Example 4.2.2. Consider the group $Q = \langle a, b \mid a^3 = b^4 = 1,\ a^b = a^{-1} \rangle$. We prove that $\mu(Q) = 7$. We will show this directly, i.e., we show that $n = 7$ is the smallest integer such that Q is embeds in S_n. To accomplish this, we construct $G \leq S_7$ such that $Q \cong G$. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 \end{pmatrix} = (123)(4)(5)(6)(7) = (123) \in S_7$$

and

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = (13)(2)(4567) = (13)(4567) \in S_7.$$

Notice that $\alpha^{-1} = (123)^{-1} = (321) = (132)$ and

$$\begin{aligned} \alpha^\beta = \beta\alpha\beta^{-1} &= [(13)(4567)][(123)][(13)(4567)]^{-1} \\ &= (13)(4567)(123)(7654)(31) \\ &= (132)(4)(5)(6)(7) \\ &= (132) \\ &= \alpha^{-1}. \end{aligned}$$

Also, $\alpha^2 = (123)(123) = (132)$ and

$$\begin{aligned} \alpha^3 &= (123)(123)(123) \\ &= (1)(2)(3) \\ &= (1)(2)(3)(4)(5)(6)(7) \\ &= 1_{S_7}. \end{aligned}$$

Therefore $o(\alpha) = 3$. Lastly, observe that $\beta^2 = (13)(4567)(13)(4567) = (1)(2)(3)(46)(57) = (46)(57)$, while $\beta^3 = (13)(4765)$, and $\beta^4 = 1_{S_7}$. Hence $o(\beta) = 4$. Let G be a group generated by α and β. So G has the presentation

$$G = \langle \alpha, \beta \mid \alpha^3 = \beta^4 = 1_{S_7},\ \alpha^\beta = \alpha^{-1} \rangle.$$

It follows that Q and G have the same structure: essentially, $Q \cong G$ under the map $a \mapsto \alpha$ and $b \mapsto \beta$, i.e., we map the generators of Q to the generators G. It follows that $\mu(Q) = \mu(G) \leq \mu(S_7) = 7$. That is, $\mu(Q) \leq 7$. Now, we argue that there does not exist a set X, of cardinality less that 7, such that G embeds in S_X. We prove this by contradiction. Suppose there is an injection $\rho : Q \to S_X$ where $|X| \leq 6$. Hence $Q \cong \rho[Q] \leq S_X$. So $\rho[Q]$ acts on X, since $\rho[Q]$ consists of the permutations of the elements of X. Now, using the method in Example 4.2.1, we can find all the non-trivial subgroups of Q and observe that each non-trivial subgroup contains either $\langle a \rangle \cong C_3$ or $\langle b^2 \rangle \cong C_2$, both of which are normal in Q. If $\rho[Q]$ acts transitively on X, then the stabiliser of each point $x_0 \in X$, $\rho[Q]_{x_0} = \{\delta \in \rho[Q] \mid \delta(x_0) = x_0\}$ must be trivial to ensure the faithfulness of the action. However, if $\rho[Q]$ acts transitively on X, we have $|X| = [\rho[Q] : \rho[Q]_{x_0}] = |\rho[Q]|/|\rho[Q]_{x_0}| = Q/|\rho[Q]_{x_0}|$ by Theorem 2.3.3 and Theorem 2.3.1. So $|X| = |Q|/|\rho[Q]_{x_0}| = 12/1 = 12$. This contradicts the fact that $|X| \leq 6$. It follows that $\rho[Q]$ is not transitive on X. Now $|\langle b \rangle| = 4$, therefore $\rho[Q]$ has an orbit of size 4 and another of size 2. So Q posses two subgroups H and K of G such that $[Q : H] = 4$ and $[Q : K] = 2$ such that $core_Q(H) \cap core_Q(K) = \{1_Q\}$. Since $|Q| = 12$, $[Q : H] = 4$ and $[Q : K] = 2$, we have $|H| = 3$ and $|K| = 6$. So, 3 divides both $|H|$ and $|K|$. Therefore $\langle a \rangle \subseteq H \cap K$, since $\langle a \rangle \in Syl_3(Q) = \{\langle a \rangle\}$. Using the fact that $\langle a \rangle$ is normal in Q, we get $core_Q(H \cap K) \neq \{1_Q\}$. This is a contradiction since $\{1_Q\} \neq core_Q(H \cap K) =$

$core_Q(H) \cap core_Q(K) = \{1_Q\}$. We therefore conclude that $\mu(G) = \mu(Q) = 7$. We can use the method provided in Example 4.2.1 to find all the subgroups of Q to see that the nilpotent subgroups of Q are as follow: $\langle b^2 \rangle \cong C_2$, $\langle a \rangle \cong C_3$, $\langle a, b^2 \rangle \cong \langle a \rangle \times \langle b^2 \rangle \cong C_3 \times C_2$ and $\langle b \rangle \cong C_4$. Therefore, $\mu(\langle b^2 \rangle) = \mu(C_2) = 2$, $\mu(\langle a \rangle) = \mu(C_3) = 3$, $\mu(\langle a, b^2 \rangle) = \mu(\langle a \rangle \times \langle b^2 \rangle) = \mu(C_3 \times C_2) = 3 + 2 = 5$. None of the minimal degrees of the nilpotent subgroups is equal to $\mu(Q) = 7$, so $Q \notin \mathcal{G}$.

4.3 Finding the minimal degree of the dihedral group D_{2n}

In Example 4.2.1 we proved that $\mu(D_8) = 4$ using the subgroup lattice of D_8. Using an argument similar to that used in [36, Claim *2*], we to generalise the result that $\mu(D_8) = 2^2$ =the sum of the prime-power decomposition of $n = 4$.

Example 4.3.1. Consider the $D_{2n} = \langle x, y \mid x^n = y^2 = 1, x^y = x^{-1} \rangle$, the dihedral group of order $2n$, for $n \geq 2$. Let $n = \Pi_{i=1}^{r} p_i^{\alpha_i}$ be the prime-power decomposition of n. We show that

$$\mu(D_{2n}) = \textstyle\sum_{i=1}^{r} p_i^{\alpha_i}.$$

Since $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ is the prime-power decomposition of n, then $p_i \neq p_j$ for $i \neq j$. Therefore $(p_i, p_j) = 1$, and since p_k's are distinct prime numbers, we have $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for all $i \neq j$. It follows that

$$C_n \cong C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \cdots \times C_{p_r^{\alpha_r}}.$$

Since $\langle x \rangle \cong C_n$, and $\langle x \rangle \leq D_{2n}$, we have $\mu(\langle x \rangle) = \mu(C_n)$ and $\mu(\langle x \rangle) \leq$

$\mu(D_{2n})$, respectively. However, by Theorem 3.3.3 we get

$$\begin{aligned}\mu(\langle x\rangle) &= \mu(C_n)\\ &= \mu(C_{p_1^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_2}})\\ &= \mu(C_{p_1^{\alpha_1}}) + \mu(C_{p_2^{\alpha_2}}) + \cdots + \mu(C_{p_r^{\alpha_r}}),\end{aligned}$$

since $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for $i \neq j$. Since each $C_{p_i^{\alpha_i}}$ is a cyclic abelian p_i-group, by Remark 3.4.1 we have $\mu(C_{p_i^{\alpha_i}}) = |C_{p_i^{\alpha_i}}| = p_i^{\alpha_i}$ for each i. Consequently,

$$\mu(\langle x\rangle) = p_1^{\alpha_1} + p_2^{\alpha_2} + \cdots + p_r^{\alpha_r} = \textstyle\sum_{i=i}^{r} p_i^{\alpha_i}.$$

We now have $\mu(\langle x\rangle) = \sum_{i=i}^{r} p_i^{\alpha_i} \leq \mu(D_{2n})$. It remains only to show that $\mu(D_{2n}) \leq \sum_{i=i}^{r} p_i^{\alpha_i}$. To accomplish this, let

$$a_i = (x_{i,1} \;\; x_{i,2} \cdots x_{i,p_i^{\alpha_i}}) \in S_{\sum_{i=1}^{r} p_i^{\alpha_i}}$$

and

$$b_i = \begin{cases} (x_{i,1} \;\; x_{i,p_i^{\alpha_i}})(x_{i,2} \;\; x_{i,p_i^{\alpha_i-1}}) \cdots (x_{i,k} \;\; x_{i,k+2}), & k = \frac{p_i^{\alpha_i-1}}{2} \; and \; p \; odd \\ (x_{i,1} \;\; x_{i,p_i^{\alpha_i}})(x_{i,2} \;\; x_{i,p_i^{\alpha_i-1}}) \cdots (x_{i,k} \;\; x_{i,k+1}), & k = \frac{p_i^{\alpha_i}}{2} \; and \; p = 2. \end{cases}$$

Now notice that, for p odd, we have
$a_i^{b_i} = b_i a_i b_i^{-1} = (x_{i,1} \;\; x_{i,p_i^{\alpha_i}})(x_{i,2} \;\; x_{i,p_i^{\alpha_i-1}}) \cdots (x_{i,k} \;\; x_{i,k+2})(x_{i,1} \;\; x_{i,2} \cdots$
$x_{i,p_i^{\alpha_i}})(x_{i,k+2} \;\; x_{i,k}) \cdots (x_{i,p_i^{\alpha_i-1}} \;\; x_{i,2})(x_{i,p_i^{\alpha_i}} \;\; x_{i,1}) = (x_{i,1} \;\; x_{i,p_i^{\alpha_i}} \;\; x_{i,p_i^{\alpha_i-1}} \cdots$
$x_{i,2}) = (x_{i,p_i^{\alpha_i}} \;\; x_{i,p_i^{\alpha_i-1}} \cdots x_{i,2} \;\; x_{i,1}) = a_i^{-1}$. Similarly, for $p = 2$ we have $a_i^{b_i} = a_i^{-1}$. Thus each b_i is a product of transpositions that invert any cycle in $S_{\sum_{i=1}^{r} p_i^{\alpha_i}}$, under conjugation. Now, if we define $\alpha = \prod_{i=1}^{r} a_i$ and $\beta = \prod_{i=1}^{r} b_i$, then $\alpha^{\beta} = \alpha^{-1}$. Again, for p odd, we have the following
$b_i^2 = (x_{i,1} \;\; x_{i,p_i^{\alpha_i}})(x_{i,2} \;\; x_{i,p_i^{\alpha_i-1}}) \cdots (x_{i,k} \;\; x_{i,k+2})(x_{i,1} \;\; x_{i,p_i^{\alpha_i}})(x_{i,2} \;\; x_{i,p_i^{\alpha_i-1}})$
$\cdots (x_{i,k} \;\; x_{i,k+2}) = (x_{i,1})(x_{i,2}) \cdots (x_{i,k}) \cdots (x_{i,p_i^{\alpha_i}}) = 1_{S_{\sum_{i=1}^{r} p_i^{\alpha_i}}}$. Similar calculations yield $b_i^2 = 1_{S_{\sum_{i=1}^{r} p_i^{\alpha_i}}}$ for $p = 2$, and so $o(b_i) = 2$ for each i. It follows

that $o(\beta) = o(\prod_{i=1}^{r} b_i) = lcm(\{o(b_i)\}_{i=1}^{r}) = 2$, where lcm means lowest common multiple. Before we find the order of α, observe that $lcm(\{p^{\alpha_i}\}_{i=1}^{r}) = \Pi_{i=1}^{r} p_i^{\alpha_i}$ since $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for $i \neq j$. We find the order of α as follows, $o(\alpha) = o(\prod_{i=1}^{r} a_i) = lcm(\{o(a_i)\}) = lcm(\{p^{\alpha_i}\}_{i=1}^{r}) = \Pi_{i=1}^{r} p_i^{i} = n$. Consider a subgroup of $S_{\sum_{i=1}^{r} p_i^{\alpha_i}}$ given by

$$G = \langle \alpha, \beta \mid \alpha^n = \beta^2 = 1_{S_{\sum_{i=1}^{r} p_i^{\alpha_i}}}, \alpha^\beta = \alpha^{-1} \rangle.$$

We now have $D_{2n} \cong G$ under the map defined by $x \mapsto \alpha$ and $y \mapsto \beta$. Consequently, $\mu(D_{2n}) = \mu(G) \leq \mu(S_{\sum_{i=1}^{r} p_i^{\alpha_i}}) = \sum_{i=1}^{r} p_i^{\alpha_i} = \mu(C_n)$. Finally, we have $\mu(D_{2n}) = \sum_{i=1}^{r} p_i^{\alpha_i} = \mu(C_n)$.

Remark 4.3.1. Notice that $C_n \cong \langle x \rangle \leq D_{2n}$. Since $\langle x \rangle$ is cyclic, it is therefore abelian, hence $\langle x \rangle$ is nilpotent by Corollary 3.4.1. So D_{2n} has a nilpotent subgroup $\langle x \rangle$ such that $\mu(\langle x \rangle) = \mu(D_{2n})$. Hence $D_{2n} \in \mathcal{G}$. This establishes the fact we discussed in Remark 3.5.1.

Chapter 5

On exceptional groups

In what follows, G denotes a non-trivial finite group. As noted earlier in Chapter 2, if $H \leq G$ then $\mu(H) \leq \mu(G)$. However if $N \lhd G$, it is possible to have $\mu(G/N) > \mu(G)$. We will examine certain classes of finite groups satisfying the property that $\mu(G/N) > \mu(G)$ for some $N \lhd G$. We need to know what causes $\mu(G/N)$ to be greater than $\mu(G)$. We analyse the latter especially in the case where the group G is a finite p-group. The reason for for our choice will be made clear shortly.

5.1 Theory of minimal exceptional groups

In [7, Example 0.1] and in [7, Example 0.2], it was shown that for groups $G = \langle x, y \mid x^8 = y^4 = 1, x^y = x^{-1} \rangle$ and $H = \langle x, y, n \mid x^8 = n^2 = 1, y^2 = x^4, x^y = x^{-1}n, n^x = n^y = n \rangle$, of order 32, there exist normal subgroups $N_1 = \langle x^4 y^2 \rangle$ and $N_2 = \langle n \rangle$ of G and H, respectively, such that $\mu(G/N_1) > \mu(G)$ and $\mu(H/N_2) > \mu(H)$. These examples serve to motivate the following.

Definition 5.1.1. *Let G be a finite group, and $N \lhd G$. If $\mu(G/N) > \mu(G)$,*

then G is called ***exceptional****. Furthermore, N and G/N are called* ***distinguished subgroup*** *and* ***distinguished quotient*** *of G, respectively.*

We want to investigate the properties of exceptional groups and their distinguished subgroups and quotients. Before we do this, we a make few remarks.

Remark 5.1.1. The groups in [7, Example 0.1] and [7, Example 0.2] do not only guarantee the existence of exceptional groups, they are also the smallest exceptional groups. So, any exceptional group of order 32 is isomorphic to either $G = \langle x, y \mid x^8 = y^4 = 1, x^y = x^{-1} \rangle$ or $H = \langle x, y, n \mid x^8 = n^2 = 1, y^2 = x^4, x^y = x^{-1}n, n^x = n^y = n \rangle$. This is shown in [7, Theorem 1.5].

We need to explore some properties of minimal exceptional groups. To do this, we need to define some concept.

Definition 5.1.2. *Let G be group. A* ***section*** *of G is a quotient group H/N, where $H \leq G$ and $N \lhd G$.*

We define the minimality of an exceptional group as follows.

Definition 5.1.3. *Let G be an exceptional group. G is called S-**minimal**, Q-**minimal** or SQ-**minimal** if G has no proper subgroup, quotient or section that is exceptional.*

Note that the exceptional groups $G = \langle x, y \mid x^8 = y^4 = 1, x^y = x^{-1} \rangle$ and $H = \langle x, y, n \mid x^8 = n^2 = 1, y^2 = x^4, x^y = x^{-1}n, n^x = n^y = n \rangle$, satisfy the conditions of Definition 5.1.3. Also, the distinguished subgroups and distinguished quotients associated with the exceptionality of G and H are p-groups, respectively. Since the distinguished quotients are p-groups, then they are nilpotent groups by Lemma 3.4.11. In the next subsection we investigate S-minimal groups with nilpotent distinguished quotients.

5.1.1 S-minimal exceptional groups with nilpotent distinguished quotients

The main goal of this section is to show that the only S-minimal groups with nilpotent distinguished quotients are p-groups. We need a number of results to accomplish this. One of these results is found as Lemma 1.1 in [7] and it is presented below.

Lemma 5.1.1. *Let G be an exceptional group and N be a distinguished subgroup of G. The following holds.*

(i) If G is S-minimal, then $N \leq \Phi(G)$

(ii) If $K \lhd G$ and $K \leq N$, then either K is itself a distinguished subgroup of G or G/K is exceptional with a distinguished subgroup N/K. In particular, if G is Q-minimal, then every non-trivial normal subgroup of G contained in N is distinguished.

Proof. (i) Let G be S-minimal. We prove that N is contained in every maximal subgroup of G. Take M to be any maximal subgroup of G and suppose to the contrary that M does not contain N. Since $N \lhd G$, then $NM \leq G$. Since M is maximal, it is not contained in N. Therefore $|NM| = |G|$, and so $G = NM$. Therefore $G/N = NM/N \cong M/(N \cap M)$. However, G is S-minimal, so the subgroup M of G is not exceptional. Therefore $\mu(M/(N \cap M)) \leq \mu(M)$. Thus $\mu(G/N) = \mu(M/(N \cap M)) \leq \mu(M) \leq \mu(G)$, i.e., $\mu(G/N) \leq \mu(G)$. This contradicts the fact that G is exceptional with N distinguished. We conclude that $N \leq M$ for all maximal subgroups M of G. This implies that $N \leq \Phi(G)$.

(ii) Let $K \lhd G$ and $K \leq N$. Then $(G/K)/(N/K) \cong G/N$. If K is not distinguished, then $\mu(G/K) \leq \mu(G) < \mu(G/N) = \mu((G/K)/(N/K))$, i.e., G/K is exceptional with a distinguished subgroup N/K. If N/K is not distinguished then $\mu(G) < \mu(G/N) = \mu((G/K)/(N/K)) \leq \mu(G/K)$. Therefore $\mu(G) < \mu(G/K)$, and so K is a distinguished subgroup of G. If G is Q-minimal, then the subgroup N/K of G/K is never distinguished, so we always have $\mu(G) < \mu(G/K)$, so that every non-trivial normal subgroup of G contained in N is distinguished.

□

We will also need the Sylow structure of a distinguished normal subgroup and the Sylow structure of a distinguished quotient of an S-minimal group G. These structures will be a special case of the general structures provided in the following lemma.

Lemma 5.1.2. *Let N be a normal subgroup and P a p-Sylow subgroup of G. Then*

(i) *$N \cap P$ is a p-Sylow subgroup of N.*

(ii) *PN/N is a p-Sylow subgroup of G/N.*

(iii) *$N_G(P)N/N = N_{G/N}(PN/N)$.*

Proof. See [17, Hilfssatz 7.7] □

We point out that the statement of Lemma 5.1.2 (i) is not true for subgroups that are not normal.

Theorem 5.1.3. *(The Frattini argument) Let N be a normal subgroup of G and P be a Sylow p-subgroup of N. Then $G = N_G(P)N$.*

Proof. See [18, Lemma 1.13] □

Definition 5.1.4. *A subset X of G is said to be a set of* ***non-generators*** *for G if for every subset S of G such that $G = \langle X, S\rangle$, we have $G = \langle S\rangle$.*

We point out that the set of all non-generators for a group G forms a subgroup of G. We now show that the Frattini subgroup of a finite group G is a set of non-generators of G.

Theorem 5.1.4. *Let G be a finite group. The Frattini subgroup of G is a set of non-generators for G.*

Proof. Suppose $G = \langle \Phi(G), S\rangle$ for some $S \subseteq G$. If $G = \langle S\rangle$, then we are done. If $G \neq \langle S\rangle$, then there exists a maximal subgroup M of G such that $\langle S\rangle \leq M < G$. Since $\Phi(G) \leq M$, then $\Phi(G) \cup S \subseteq M$. Therefore $\langle \Phi(G) \cup S\rangle = \langle \Phi(G), S\rangle \leq M < G$. That is, $G \leq M < G$, a contradiction. Hence $G = \langle S\rangle$, and so $\Phi(G)$ is a set of non-generators for G. □

Corollary 5.1.5. *If $G = H\Phi(G)$ for some subgroup $H \leq G$, then $G = H$.*

Proof. If $G = H\Phi(G)$, then $G = \langle H, \Phi(G)\rangle$. Now by Theorem 5.1.4 we obtain $G = \langle H\rangle = H$. □

If G/N is a nilpotent group, it does not follow that G is nilpotent. However, if $N \leq \Phi(G)$ and G/N is a nilpotent group, then G is nilpotent. This will be a direct consequence of the following result and will be used shortly to prove that the only S-minimal groups with nilpotent distinguished quotients are p-groups.

Theorem 5.1.6. *Let N and M be normal subgroups of G with $N \trianglelefteq M$ and $N \leq \Phi(G)$. If M/N is nilpotent, then M is nilpotent.*

Proof. Let P be a Sylow p-subgroup of M. Then PN/N is a Sylow p-subgroup of M/N, by Lemma 5.1.2 (ii). Note that $PN/N \leq M/N$. Since M/N is nilpotent, then by Lemma 3.4.4 we have PN/N is nilpotent. Also, $PN/N \trianglelefteq M/N$ by Theorem 3.4.12 (ii). So PN/N is the unique Sylow p-subgroup of M/N. Now let $\varphi \in \mathsf{Aut}(M/N)$. Since PN/N is the unique subgroup of M/N of order $|PN/N|$, it follows that $\varphi|_{PN/N}$, the restriction of the automorphism φ of M/N to PN/N, is an injection of PN/N onto a subgroup of order $|PN/N|$ in M/N. Therefore $\varphi(PN/N) = PN/N$. Thus PN/N is a characteristic subgroup of M/N. Since $M/N \trianglelefteq G/N$, it follows that PN/N is a characteristic subgroup of G/N. This implies that $PN/N \trianglelefteq G/N$ and so $PN \trianglelefteq G$. Since P is a Sylow p-subgroup of the normal subgroup PN of G, then by Lemma 5.1.3, we have

$$G = N_G(P)(PN) = (N_G(P)P)N = N_G(P)N.$$

Since $N \leq \Phi(G)$, we have $N_G(P)N \subseteq N_G(P)\Phi(G)$. By Corollary 5.1.5, we have $N_G(P)\Phi(G) = N_G(P)$. It follows that $G = N_G(P)$, and so $P \trianglelefteq G$. However $P \leq M \leq G$, and so $P \trianglelefteq M$. Since this holds for all Sylow p-subgroups of M, it follows by Theorem 3.4.12 that M is nilpotent. □

We now present the main theorem of this section.

Theorem 5.1.7. *Any S-minimal exceptional group with nilpotent distinguished quotient is a p-group for some prime p.*

Proof. Let G be an S-minimal exceptional group, with a distinguished subgroup N. By Lemma 5.1.1 (i), we have $N \leq \Phi(G)$. Now if G/N is nilpotent, taking $G = M$ in Theorem 5.1.6, we have G is nilpotent. Take a prime divisor, p, of $|G|$. If G is not a p-group, then by Theorem 3.4.12 we can decompose G into a direct product of its Sylow p_i-subgroups, for different

primes p_i. Without loss of generality, suppose G is a direct product of two Sylow p_i-subgroups, say $G = P_1 \times P_2$, where $P_1 \in Syl_{p_1}(G)$ and $P_2 \in Syl_{p_2}(G)$. Since $p_1 \neq p_2$, then $(|P_1|, |P_2|) = 1$. By Lemma 5.1.2 (i), $N \cap P_1$ and $N \cap P_2$ are Sylow p_1-subgroup and Sylow p_2-subgroup of N, respectively. Since G is a nilpotent group, by Lemma 3.4.4, we have N is nilpotent. Therefore $N = (N \cap P_1) \times (N \cap P_2)$, by Theorem 3.4.12. It is now clear that

$$G/N = (P_1 \times P_2)/((N \cap P_1) \times (N \cap P_2)) = P_1/(N \cap P_1) \times P_2/(N \cap P_2).$$

We now have $\mu(G/N) = \mu(P_1/(N \cap P_1) \times P_2/(N \cap P_2))$. It follows by Theorem 3.1.2 that

$$\mu(P_1/(N \cap P_1) \times P_2/(N \cap P_2)) \leq \mu(P_1/(N \cap P_1)) + \mu(P_2/(N \cap P_2)).$$

Since G is S-minimal, then P_1 and P_2 are not exceptional. This implies that $\mu(P_1/(N \cap P_1) \leq \mu(P_1)$ and $\mu(P_2/(N \cap P_2) \leq \mu(P_2)$, respectively. Adding these inequalities we get

$$\mu(P_1/(N \cap P_1)) + \mu(P_2/(N \cap P_2)) \leq \mu(P_1) + \mu(P_2).$$

Since $G = P_1 \times P_2$ and $(|P_1|, |P_2|) = 1$, we have $\mu(G) = \mu(P_1 \times P_2) = \mu(P_1) + \mu(P_2)$, by Theorem 3.3.3. Combining all these equations and inequalities, we get

$$\begin{aligned}
\mu(G/N) &= \mu(P_1/(N \cap P_1) \times P_2/(N \cap P_2)) \\
&\leq \mu(P_1/(N \cap P_1)) + \mu(P_2/(N \cap P_2)) \\
&\leq \mu(P_1) + \mu(P_2) \\
&= \mu(P_1 \times P_2) \\
&= \mu(G)
\end{aligned}$$

So $\mu(G/N) \leq \mu(G)$. This contradicts the fact that G is exceptional with distinguished subgroup N. Hence G is a p-group. $\square$

5.2 Quotient groups which are not distinguished

In passing, it is mentioned in [7] that a finite abelian group cannot be exceptional. We prove this fact using the following lemma and deduce that no quotient group of an abelian group is distinguished. Although the following lemma is well-known, an original proof is provided for completeness.

Lemma 5.2.1. *Let G be a finite abelian group. If $N \leq G$, then there exists $H \leq G$ such that $G/N \cong H$.*

Proof. By the Fundamental Theorem of Finite Abelian Groups, we can write

$$G = G_1 \times G_2 \times \cdots \times G_n,$$

where each G_i is a non-trivial cyclic p_i-subgroup of G such that $|G_1| \leq |G_2| \leq \cdots \leq |G_n|$. Therefore it is enough to show this lemma where G is a non-trivial abelian p-group. Once again, by the Fundamental Theorem of Finite Abelian Groups we have

$$G = C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_r}}. \tag{5.1}$$

where $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_r$. Since G/N is a homomorphic image of G, G/N is a non-trivial finite abelian p-group generated by r elements, the images of the generators of G under the natural homomorphism. So G/N has at most r direct factors. Moreover,

$$\begin{aligned} G/N &= (C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_r}})/N \\ &\cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_s}}, \end{aligned}$$

where $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_s$ and $s \leq r$.
Since $o(g)$ divides p^{α_r} for all $g \in G$, then $o(gN)$ divides p^{α_r} for all $gN \in G/N$. So $p^{\beta_s} \leq p^{\alpha_r}$, this implies that p^{β_s} divides p^{α_r}. By Sylow's Theorem, it

follows that $C_{p^{\alpha_r}}$ has a subgroup, $H_{p^{\beta_s}}$, of order p^{β_s}.

Let us now count the number of elements of order greater than $p^{\alpha_{r-1}}$ in G. An element of order greater than $p^{\alpha_{r-1}}$ in G/N will be an image of one of these. If $g \in G$, then $g = (g_1, g_2, \ldots, g_{r-1}, g_r)$, where $g_i \in C_{p^{\alpha_i}}$. So $g^{p^{\alpha_{r-1}}} = (g_1, g_2, \ldots, g_{r-1}, g_r)^{p^{\alpha_{r-1}}} = (g_1^{p^{\alpha_{r-1}}}, g_2^{p^{\alpha_{r-1}}}, \ldots, g_{r-1}^{p^{\alpha_{r-1}}}, g_r^{p^{\alpha_{r-1}}})$ $= (1_{C_{p^{\alpha_1}}}, 1_{C_{p^{\alpha_2}}} \ldots, 1_{C_{p^{\alpha_{r-1}}}}, g_r^{p^{\alpha_{r-1}}})$. So at most one of the p^{β_i} is greater than $p^{\alpha_{r-1}}$. If such p^{β_i} exists, it will be p^{β_s}, since β_s is maximal amongst all β_i. Consequently, $p^{\beta_{s-1}} \leq p^{\beta_{r-1}}$, and so $p^{\beta_{s-1}}$ divides $p^{\beta_{r-1}}$. By Sylow's Theorem, $C_{p^{\alpha_{r-1}}}$ has a subgroup, $H_{p^{\beta_{s-1}}}$, of order $p^{\beta_{s-1}}$.

Continuing in this way, we get that each $C_{p^{\alpha_i}}$ in the direct product (5.1) has a subgroup, $H_{p^{\beta_i}}$, of order p^{β_i}. Since cyclic groups of the same order are isomorphic, we have $H_{p^{\beta_j}} \cong C_{p^{\alpha_j}}$ for $1 \leq j \leq s$, hence $H = H_{p^{\beta_1}} \times H_{p^{\beta_2}} \times \cdots \times H_{p^{\beta_s}} \cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_s}} \cong G/N$. □

We now prove that finite abelian groups are never exceptional.

Theorem 5.2.2. *If G is a finite abelian group, then G is not exceptional. Moreover, quotient groups of finite abelian groups are never distinguished.*

Proof. Let $N \lhd G$, then by Lemma 5.2.1, there exists $H \leq G$ such that $G/N \cong H$. Therefore $\mu(G/N) = \mu(H) \leq \mu(G)$. The second statement of the theorem is now transparent. □

A distinguished quotient of an exceptional group is never cyclic. This is shown in [7] and we provide a detailed proof below.

Theorem 5.2.3. *Let $N \lhd G$. If $\mu(G/N) > \mu(G)$, then G/N is not cyclic.*

Proof. Assume $\mu(G/N) > \mu(G)$ and suppose to the contrary that G/N is cyclic, say $G/N = \langle gN \rangle$, for some $g \in G$. Then $|\langle gN \rangle| \leq |\langle g \rangle|$. So $\mu(G/N) =$

$\mu(\langle gN\rangle) \leq \mu(\langle g\rangle) \leq \mu(G)$. This contradicts the assumption that $\mu(G/N) > \mu(G)$, and the result follows. □

The following result is found in [24].

Proposition 5.2.4. *Let $N \lhd G$. If G/N is a distinguished quotient, then G/N is not isomorphic to $C_{p^{n-1}} \times C_p$. That is, if $\mu(G/N) > \mu(G)$, then $G/N \ncong C_{p^{n-1}} \times C_p$.*

Proof. See [24, Theorem 5.2 and Corollary 5.3]. □

Remark 5.2.1. (i) Despite what was proved in Theorem 5.2.2, Theorem 5.2.3 and in Proposition 5.2.4, much still remains to be understood. For example, it remains unknown whether or not distinguished quotients can be abelian.

(ii) The fact that distinguished quotients cannot be elementary abelian was proved in [21]. On the other hand, it is shown in [22, Theorem 1] that if G/N has no non-trivial abelian normal subgroup, then $\mu(G/N) \leq \mu(G)$. This shows that a distinguished quotient must have at least one non-trivial abelian normal subgroup.

(iii) If G is a nonabelian finite p-group with an abelian maximal subgroup, then $\mu(G/G') \leq \mu(G)$. The latter was shown in [9].

(iv) The smallest example G, if it exists, of an exceptional group with abelian distinguished quotient G/N must be a p-group. For, by the proof of Lemma 5.1.1 (i), $N \leq \Phi(G)$ and by the proof of Theorem 5.1.7, G is a p-group.

For a prime number p, a distinguished quotient can never have order p, by Theorem 5.2.3. The fact that a distinguished quotient can never have order p^2 is presented in Corollary 5.2.5 below.

Corollary 5.2.5. *Let $N \lhd G$. If $\mu(G/N) > \mu(G)$, then $|G/N| \neq p^2$.*

Proof. Let $\mu(G/N) > \mu(G)$. Suppose $|G/N| = p^2$, the $G/N \cong C_{p^2}$ or $C_p \times C_p$. However, G/N cannot be isomorphic to $C_p \times C_p$, by Remark 5.2.1 (ii). By Theorem 5.2.3, we deduce that G/N cannot be cyclic, excluding the possibility of $G/N \cong C_{p^2}$. □

5.3 Construction of exceptional direct products of finite groups

In this section we provide some conditions under which the direct product of two groups is exceptional. The following construction of an exceptional group is due to [7].

Theorem 5.3.1. *Let G and H be finite groups such that G is exceptional with a distinguished subgroup N. If $(|G|, |H|) = 1$ or G and H are both nilpotent, then $G \times H$ is exceptional.*

Proof. The result is trivial if H is a trivial group. So, suppose H is a non-trivial finite group. First note that $(G \times H)/(N \times \{1_H\}) \cong (G/N) \times (H/\{1_H\}) = (G/N) \times H$ under the map $\pi((g,h)(N \times \{1_H\})) = (gN, h)$, for all $g \in G$ and $h \in H$. We now have $\mu((G\times H)/(N\times\{1_H\})) = \mu((G/N)\times H)$. Also, since N is a distinguished subgroup of G, then $\mu(G/N) > \mu(G)$.
Now suppose $(|G|, |H|) = 1$. Then $(|G/N|, |H|) = (|G|/|N|, |H|) = 1$, so that $\mu((G/N) \times H) = \mu(G/N) + \mu(H)$ by Theorem 3.3.3. Since $\mu(G/N) >$

$\mu(G)$, then $\mu(G/N) + \mu(H) > \mu(G) + \mu(H)$. Since $(|G|, |H|) = 1$, we have $\mu(G)+\mu(H) = \mu(G\times H)$. Combining the equations and the inequality above we obtain

$$\begin{aligned} \mu((G \times H)/(N \times \{1_H\})) &= \mu((G/N) \times H) \\ &= \mu(G/N) + \mu(H) \\ &> \mu(G) + \mu(H) \\ &= \mu(G \times H) \end{aligned}$$

That is, $\mu((G \times H)/(N \times \{1_H\})) > \mu(G \times H)$. So $G \times H$ is exceptional. Now suppose G and H are both nilpotent. Then by Lemma 3.4.4 we have that G/N is nilpotent. Therefore $\mu((G/N) \times H) = \mu(G/N) + \mu(H)$, by Theorem 3.4.14. Also $\mu(G/N) > \mu(G)$, so that $\mu(G/N) + \mu(H) > \mu(G) + \mu(H)$. As in the first case, we have $\mu((G \times H)/(N \times \{1_H\})) > \mu(G \times H)$. Hence $G \times H$ is exceptional, with a distinguished subgroup $N \times \{1_H\}$. □

To provide another class of exceptional direct product we need some results. A detailed proof of the following is available in [20, Theorem 3], and so we do not reprove it here.

Theorem 5.3.2. *Let G be a p-group whose center $Z(G)$ is minimally generated by d elements, and let $\mathcal{R} = \{G_i\}_{i=1}^{n}$ be a minimal representation of G, then for odd p, $n = d$, while if $p = 2$, $d/2 \leq n \leq d$, the bound $n = d$ being achieved.*

Proof. See [20, Theorem 3]. □

Another construction of a class of an exceptional direct product of two finite groups, where the direct factors are non-cyclic p-groups with cyclic centers

is provided in [7, Theorem 2.1]. An expanded proof of [7, Theorem 2.1] is provided below.

Theorem 5.3.3. *Let p be a prime number and G and H be non-cyclic p-groups with cyclic centers $Z(G) = \langle x \rangle$ and $Z(H) = \langle y \rangle$, respectively, where $|Z(G)| = |Z(H)|$. Then the following holds.*

(i) If p is odd, then $G \times H$ is an exceptional group with distinguished subgroup $N = \langle (x, y) \rangle$

(ii) If $p = 2$, $\mu(G) > \mu(H)$ and H is not a generalised quaternion group, then $G \times H$ is an exceptional group with distinguished subgroup $N = \langle (x, y) \rangle$.

Proof. We claim that $(G \times H)/N$ has the cyclic center $(Z(G) \times Z(H))/N = \langle (x, 1_H)N \rangle = \langle (1_G, y)N \rangle$. This holds since $(a, b)N \in Z((G \times H)/N)$ if and only if $((a, b)N)((g, h)N) = ((g, h)N)((a, b)N)$, for all $(g, h) \in G \times H$. This is valid if and only if $(ag, bh)N = (ga, hb)N$. But $(ag, bh)N = (ga, hb)N$ if and only if $((ag, bh)N)((ga, hb)N)^{-1} = 1_{(G\times H)/N}$. However,

$$\begin{aligned} ((ag, bh)N)((ga, hb)N)^{-1} &= (ag, bh)N((ga, hb)^{-1}N) \\ &= ((ag, bh)N)((a^{-1}g^{-1}, b^{-1}h^{-1})N) \\ &= (aga^{-1}g^{-1}, bhb^{-1}h^{-1})N \\ &= ([a, g], [b, h])N \end{aligned}$$

and $1_{(G\times H)/N} = N = \langle (x, y) \rangle$. So, $(a, b)N \in Z((G \times H)/N)$ if and only if $([a, g], [b, h])N = N$, i.e., $([a, g], [b, h]) \in N$ for all $(g, h) \in G \times H$. This holds if only if $([a, g], [b, h]) = (x, y)^i = (x^i, y^i)$. Hence $[a, g] = x^i$ and $[b, h] = y^i$, for some integer i. Taking $g = 1_G$ and $h = 1_H$, these conditions become $[a, g] = 1_G$ and $[b, h] = 1_G$, respectively, for all $(g, h) \in G \times H$. Now, $ag = ga$

and $ah = hb$ for all $(g, h) \in G \times H$, implies that $a \in Z(G)$ and $b \in Z(H)$, respectively. Therefore $Z((G \times H)/N) = \langle (x, 1_H)N \rangle = \langle (1_G, y)N \rangle$. Observe that $Z(G), Z(H)$ and $Z((G \times H)/N)$ are all generated by one element. So by Theorem 5.3.2, any minimal representations $\mathcal{R}, \mathcal{D}$ and $\mathcal{O}$ of G, H and $(G \times H)/N$, consist of one core-free subgroup K_1, K_2 and K_3, respectively. Since G, H and $(G \times H)/N$ are p-groups, we have $\mu(G) = [G : K_1] = p^{n_1}$, $\mu(H) = [H : K_2] = p^{n_2}$, and $\mu((G \times H)/N) = [(G \times H)/N : K_3] = p^{n_3}$, for some positive integers n_1, n_2 and n_3. Without lost of generality, assume $\mu(G) \geq \mu(H)$.

Since H is non-cyclic, if p is odd, then by the contraposition of Theorem 4.1.5 (ii), H has at least two subgroups of order p. Since $Z(H)$ is cyclic of order p, choose $K = \langle k \rangle \leq H$ such that $Z(H) \cap K = \{1_H\}$. Now, note that $G \times K \cong (G \times K)N/N \leq (G \times H)/N$. It follows that $\mu((G \times H)/N) \geq \mu(G \times K)$. However, $\mu(G \times K) = \mu(G) + \mu(K)$, by Theorem 3.4.13. Also, $\mu(G) + \mu(K) > \mu(G)$, and so $\mu((G \times H)/N) > \mu(G)$. Thus we have $\mu((G \times H)/N) \geq p\mu(G)$. Since p is odd, the latter implies that $\mu((G \times H)/N) > 2\mu(G)$. By Theorem 3.4.13 and by the assumption that $\mu(G) \geq \mu(H)$, we have $2\mu(G) = \mu(G) + \mu(G) \geq \mu(G) + \mu(H) = \mu(G \times H)$. So, $\mu((G \times H)/N) > \mu(G \times H)$. This proves (i).

Finally, if $p = 2$, and H is not Q_{2^n}, then by the contrapositive statement of Theorem 4.1.5 (ii), it follows that H has a cyclic abelian group $K = \langle h \rangle$, for some $h \in H$. Using a similar argument to that in the case where p is odd, we have $\mu((G \times H)/N) \geq p\mu(G)$. Since $p = 2$, we have $\mu((G \times H)/N) \geq 2\mu(G) = \mu(G) + \mu(G)$. Now, if $\mu(G) > \mu(H)$ then $\mu(G) + \mu(G) > \mu(H) + \mu(G)$. It follows from Theorem 3.4.13 that $\mu(H) + \mu(G) = \mu(G \times H)$. Hence $\mu((G \times H)/N) > \mu(G \times H)$, and we have the result. $\square$

Definition 5.3.1. *Let G and H two be groups. Let $M \leq Z(G)$ and $N \leq Z(H)$ such that $M \cong N$ under an isomorphism $\rho : M \to N$. Let $X = \{(x, (\rho(x))^{-1}) \mid x \in M\}$. Then, the quotient group $(G \times H)/X$, denoted $G *_\rho H$, is called the* ***central product*** *of G and H with respect to ρ. Where there is no confusion, we simply write $G * H$ for a central product of G and H.*

Corollary 5.3.4. *The following classes of 2-groups are exceptional;*

(i) $D_{2^n} \times D_{2^m}$, *with distinguished quotient* $(D_{2^n} \times D_{2^m})/N \cong D_{2^n} * D_{2^m}$, *for* $n > m \geq 3$.

(ii) $Q_{2^n} \times D_{2^m}$, *with distinguished quotient* $(Q_{2^n} \times D_{2^m})/N \cong Q_{2^n} * D_{2^m}$, *for* $n \geq m \geq 3$. *The smallest 2-group in this class is* $Q_{2^3} \times D_{2^3} = Q_8 \times D_8$ *of order 64.*

(iii) $(D_{16} * (*D_8)^n) \times D_8$ *is exceptional with distinguished quotient isomorphic to* $D_{16} * (*D_8)^{n+1}$, *where* $(*D_8)^n = \underbrace{D_8 * D_8 * \cdots * D_8}_{n\text{-times}}$.

(iv) $Q_8 * (*D_8)^n) \times D_8$ *is exceptional with distinguished quotient isomorphic to* $Q_8 * (*D_8)^{n+1}$.

Proof. It is not difficult to show that the two non-cyclic 2-groups, $D_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, x^y = x^{-1} \rangle$ and $Q_{2^n} = \langle a^{2^{n-1}} = b^4 = 1, a^{2^{n-2}} = b^2, a^b = a^{-1} \rangle$, have cyclic centers, $Z(D_{2^n}) = \langle x^{2^{n-2}} \rangle = \{1, x^{2^{n-2}}\}$ and $Z(Q_{2^n}) = \langle a^{2^{n-2}} \rangle = \{1, a^{2^{n-2}}\}$, respectively. So that $Z(D_{2^n}) \cong Z(Q_{2^n})$, under the map $x^{2^{n-2}} \mapsto a^{2^{n-2}}$. Thus $|Z(D_{2^n})| = |Z(Q_{2^n})|$. Therefore, (i) follow as a direct consequence of Theorem 5.3.3 (ii) with distinguished subgroups $N = \langle (x^{2^{n-2}}, x^{2^{m-2}}) \rangle$. Similarly, (ii) follow as a direct consequence of Theorem 5.3.3 (ii) with distinguished $N = \langle (a^{2^{n-2}}, a^{2^{m-2}}) \rangle$. The second part

of (ii) follows by taking $n = m = 3$. Parts (iii) and (iv) respectively follow by repeated use of Theorem 5.3.3 with suitable choices of n and m. $\square$

Remark 5.3.1. In [7, Proposition 2], it is stated that for $n, m > 2$, the groups $D_{2^n} \times D_{2^m}$, $Q_{2^n} \times D_{2^m}$, and $Q_{2^n} \times Q_{2^m}$, are exceptional with distinguished quotients $(D_{2^n} \times D_{2^m})/N \cong D_{2^n} * D_{2^m}$, $(Q_{2^n} \times D_{2^m})/N \cong Q_{2^n} * D_{2^m}$, and $(Q_{2^n} \times Q_{2^m})/N \cong Q_{2^n} * Q_{2^m}$, respectively. The authors attempted to prove this without the use of Theorem 5.3.3, but did not succeed in the case where $n = m$. In fact, their argument shows that $D_{2^n} \times D_{2^m}$, and $Q_{2^n} \times Q_{2^m}$ are not exceptional.

Example 5.3.5. We point out that the distinguished quotients of the two examples of the smallest exceptional groups of order 32, $G = \langle x, y \mid x^8 = y^4 = 1, x^y = x^{-1} \rangle$ and $H = \langle x, y, n \mid x^8 = n^2 = 1, y^2 = x^4, x^y = x^{-1}n, n^x = n^y = n \rangle$, are central products. This is so because the distinguished subgroups $N_1 = \langle x^4y^2 \rangle = \{1, x^4y^2\} \leq Z(G) = \langle x^4, y^4 \rangle$ and $N_2 = \langle n \rangle = \{1, n\} \leq Z(H) = \langle n, x^4 \rangle$, respectively. Thus, $|N_1| = |N_2| = 2$, and so $N_1 \cong N_2$. Hence G/N_1 and H/N_2 are central product by definition.

Observe that all the classes of exceptional groups provided in this section were a direct product of two finite groups. In the next section, classes of exceptional groups that do not decompose into a direct product are provided.

5.4 Exceptional p-groups

If G is a finite nilpotent group, then G is a direct product of its Sylow p-subgroups, for different primes p, by Theorem 3.4.12. Therefore, to determine whether G is exceptional or not, we need to determine whether G has a Sylow p-subgroup that is exceptional. More generally, if the order of a

finite group G is divisible by some power of a prime, say p^α, then by Sylow's Theorem, there exists a subgroup H of G such that $|H| = p^\alpha$. So, instead of searching for distinguished subgroups of general finite G whose structure is not known, we can focus on the search for distinguished subgroups of its p-subgroups. This shall reduce the abstractness of the problem, since the isomorphism classes of some p-groups and their properties are available, see, for example [1], [2], [3] and [4]. This is among the reasons that make exceptional p-group worth examining.

5.4.1 Minimal degrees of p-groups of order less than p^5

Definition 5.4.1. *A finite p-group G is termed* ***extraspecial*** *if $Z(G) = G' = \Phi(G)$.*

Remark 5.4.1. (i) In [7], a class of exceptional p-groups of order p^6 is exhibited. The groups in this class are given by the direct product $G \times G$ of order p^6, where G is an extraspecial group of order p^3. At that time, the authors in [7] were unaware of the existence of exceptional p-group of order less than p^6, for p odd.

(ii) Much later, in [24], a proof was given which shows indirectly that the exceptional p-groups of order less than p^n do not exist, for $n \leq 4$ and p odd.

(iii) In [25], the author provided an example of a p-group of order p^5.

We will provide a direct proof of the fact that is mentioned Remark 5.4.1 (*ii*). We will also provide a detailed proof of the fact that we stated in Remark 5.4.1 (*iii*). In order to do this, we need a few more results. Recall

that H is called a primitive subgroup of G if its G-closure is not itself, i.e., $H \neq \hat{H} = \bigcap_{\substack{K \leq G, \\ H < K}} K$.
We also remarked that, in a finite group, primitive subgroups are just meet-irreducible elements of the subgroup lattice. We use the latter in proving the following lemma.

Lemma 5.4.1. *Let G be a finite group of odd order, and N be a normal subgroup of G. Then G/N is cyclic of prime-power order if and only if N is primitive.*

Proof. Observe that showing the statement of this lemma is equivalent to showing that G is cyclic of prime-power order if and only if $\{1_G\}$ is primitive. Suppose that G is cyclic of prime-power order, then the subgroup lattice of G is a chain. It follows that the G-closure of $\{1_G\}$ is a non-trivial subgroup of minimum order. Therefore the G-closure of $\{1_G\}$ is not $\{1_G\}$, and so $\{1_G\}$ is primitive.
Conversley, suppose that $\{1_G\}$ is primitive in G and that $G = G/\{1_G\}$ is not cyclic of prime-power order. Then $|G|$ is divisible by at least two odd (as $|G|$ is odd) primes p and q. By Sylow's Theorem, there exist two non-trivial subgroups of G, namely a p-subgroup P and a q-subgroup Q. Since $(|P|, |Q|) = 1$, we have $P \cap Q = \{1_G\}$. But, this contradicts the the meet-irreducibility and the primitivity of $\{1_G\}$. Consequently, G is divisible by exactly one prime. This proves that G is a p-group for some odd prime p. Since G is of prime-power order, and we supposed G is not cyclic, by Theorem 4.1.4, we have G contains a subgroup H that isomorphic to $C_p \times C_p$. Set $H = \langle x \rangle \times \langle y \rangle$, for some distinct elements $x, y \in G$, each of order p, such that $\langle x \rangle \cap \langle y \rangle = \{1_G\}$. Again, this contradicts the meet-irreducibility and the primitivity of $\{1_G\}$. So G is cyclic of prime-power order. □

In the following we define the notion of induced representation and supply as an example, a class of p-groups which satisfies this definition.

Definition 5.4.2. *Denote by $\tilde{G}_p$ the class of p-groups with the property that $G \in \tilde{G}_p$ if and only if G has a minimal representation $\mathcal{R} = \{G_i\}_{i=i}^{n}$ such that $\mathcal{R}_{Z(G)} = \{G_i \cap Z(G)\}_{i=i}^{n}$ is a minimal representation of $Z(G)$. The representation $\mathcal{R}_{Z(G)}$ is called the* ***induced representation*** *of $Z(G)$.*

Remark 5.4.2. Note that $G \in \tilde{G}_p$ if and only if, from a representation of G, we can find a representation of the center by just intersecting the transitive constituents of the representation of G with $Z(G)$. Notice, as remarked in [35] that extending a representation of $Z(G)$ to a representation of G is in general not always possible. However, if G is an abelian p-group, any representation of G is the induced representation of $Z(G)$ (since $Z(G) = G$). If $\mathcal{R}_{Z(G)}$ is an induced representation of $Z(G)$, then each $G_i \cap Z(G) \in \mathcal{R}_{Z(G)}$ is a direct factor of $Z(G)$, i.e., $Z(G) = H \times (G_i \cap Z(G))$ for some abelian subgroup H of G (see [20, Example 4]).

Another result which is stated without proof in [20, Remark 1] shall be proved in the following lemma. This lemma will be used to find an upper bound and a lower bound of $\mu(G)$, where $G \in \tilde{G}_p$.

Lemma 5.4.2. *Let p be an odd prime. If G is a p-group whose centre is either cyclic or elementary abelian, then $G \in \tilde{G}_p$.*

Proof. Suppose G is a p-group, where p is an odd prime. Let $\mathcal{R}$ be a representation of G. If the center of G is cyclic, then $d(Z(G)) = 1$, and by Theorem 5.3.2, we have that $|\mathcal{R}| = 1$. So, $\mathcal{R}$ consists of one core-free subgroup H. Therefore $\mathcal{R}$ is a transitive representation of G. Since $core_G(H) = \{1_G\}$ and $H \cap Z(G) \trianglelefteq H$, it follows that $H \cap Z(G) = \{1_G\}$, and

so $core_G(H \cap Z(G)) = \{1_G\}$. This implies that $\{H \cap Z(G)\}$ is a faithful representation of $Z(G)$. Now, $Z(G)$, a cyclic p-group, forces $\mu(Z(G)) = |Z(G)|$ by Theorem 4.1.6. Thus we obtain

$$deg(\{H \cap Z(G)\}) = [Z(G) : H \cap Z(G)] = [Z(G) : \{1_G\}] = |Z(G)| = \mu(Z(G)),$$

and so $\{H \cap Z(G)\}$ is a faithful representation of $Z(G)$ of minimal degree. Hence, $G \in \tilde{G}_p$.

Now suppose that $Z(G)$ is an elementary abelian group, and let $\mathcal{R} = \{G_1, \ldots, G_n\}$ be a minimal faithful representation of G with all G_i primitive. This representation exists by Lemma 3.2.2, and so by Theorem 5.3.2 we have $d(Z(G)) = n$. Therefore $Z(G) \cong \underbrace{C_p \times \cdots \times C_p}_{n\text{-times}}$. Since G is of odd order and each G_i is primitive, by Lemma 5.4.1, we must have G/G_i is cyclic for each i. We claim that the representation $\{G_1 \cap Z(G), \ldots, G_n \cap Z(G)\}$ is the induced representation of $Z(G)$. But, since $\mathcal{R} = \{G_1, \ldots, G_n\}$ is faithful, we have $G_i \cap Z(G) = \{1_G\}$, for each i; otherwise $G_i \cap Z(G) \trianglelefteq G_i$ and so $core_G(G_i) \neq \{1_G\}$, a contradiction. Hence, $\bigcap_{i=1}^{n}(G_i \cap Z(G)) = \{1_G\}$. Now,

$$\begin{aligned} core_G(\{G_1 \cap Z(G), \ldots, G_n \cap Z(G)\}) &= \bigcap_{i=1}^{n} core_G(G_i \cap Z(G)) \\ &= core_G(\bigcap_{i=1}^{n}(G_i \cap Z(G))) \\ &= core_G(\{1_G\}) \\ &= \{1_G\}. \end{aligned}$$

From this, we deduce that $\{G_1 \cap Z(G), \ldots, G_n \cap Z(G)\}$ is a faithful representation for $Z(G)$. Moreover, by the Second Isomorphism Theorem for groups, for each i, we have

$$Z(G)/(G_i \cap Z(G)) \cong Z(G)G_i/G_i.$$

Since $Z(G)G_i/G_i \leq G/G_i$ and G/G_i is cyclic, we have $Z(G)G_i/G_i$ is cyclic. Hence, $Z(G)/(G_i \cap Z(G))$ is cyclic for all $1 \leq i \leq n$, and so $Z(G)/(G_i \cap Z(G)) \cong C_p$. The degree of this representation with respect to the center is

$$\begin{aligned} deg(\bigcup_{i=1}^{n}\{(G_i \cap Z(G))\}) &= deg(\{G_1 \cap Z(G), \ldots, G_n \cap Z(G)\}) \\ &= [Z(G) : G_1 \cap Z(G)] + \cdots + [Z(G) : G_n \cap Z(G)] \\ &= \underbrace{|C_p| + \cdots + |C_p|}_{n\text{-times}} \\ &= \mu(C_p) + \cdots + \mu(C_p) = \mu(C_p \times \cdots \times C_p) \\ &= \mu(Z(G)). \end{aligned}$$

Therefore $\{G_1 \cap Z(G), \ldots, G_n \cap Z(G)\}$ is indeed $R_{Z(G)}$; thus showing that $G \in \tilde{G_p}$. □

It is trivial that $\tilde{G_p}$ contains all the abelian p-groups. In fact [20, Remark 1] states that $\tilde{G_p}$ contains all groups of order p^n, with p odd and $n \leq 4$. Using Lemma 5.4.2 we give a much simpler proof of this result, in Theorem 5.4.3 below.

Theorem 5.4.3. *For an odd prime p, $\tilde{G_p}$ contains all p-groups of order p, p^2, p^3 and p^4.*

Proof. Let G be a group of order p, p^2, p^3 and p^4 respectively. If G is abelian, then the result follows. It is thus plausible to prove this in the case where G is not abelian. The proof follows by considering a number of cases. If $|G| = p^3$, then $|Z(G)| \in \{p, p^2, p^3\}$. But if $|Z(G)| = p^3$, then G is abelian and we are done. However, if $|Z(G)| = p$, or p^2 then $Z(G)$ is cyclic or elementary abelian, and the result follows by Lemma 5.4.2. If $|G| = p^4$, then $|Z(G)| \in \{p, p^2, p^3, p^4\}$. But if $|Z(G)| = p^4$, then $Z(G) = G$ and so G

is abelian and the result follows. If $|Z(G)| = p^3$, then $G/Z(G)$ is cyclic, and so G is abelian and the result follows. If $Z(G) = p^2$, then $Z(G) \cong C_{p^2}$ or $Z(G) \cong C_p \times C_p$. Therefore $G \in \tilde{G}_p$ by Lemma 5.4.2. If $|Z(G)| = p$, then $Z(G)$ is cyclic and the result follows by Lemma 5.4.2. □

The following theorem appears in [20, Proposition 3] and the proof was omitted. Later, we extensively use this theorem and its corollary to find the minimal degrees of some p-groups. As a result, we provide explicit and original proofs.

Theorem 5.4.4. *Let G be a non-abelian group in the class $\tilde{G}_p$, where p is an odd prime. Further, suppose G is not a non-trivial direct product. Then, $p\mu(Z(G)) \leq \mu(G) \leq \frac{1}{p}[G : Z(G)]\mu(Z(G))$.*

Proof. By Lemma 3.2.2, G has a minimal representation $\mathcal{R} = \{G_i\}_{i=i}^n$ such that each G_i is primitive in G. Since $G \in \tilde{G}_p$, then $\mathcal{R}_{Z(G)} = \{G_i \cap Z(G)\}_{i=1}^n$ is a minimal representation of $Z(G)$. Now, if $G_i = G_i \cap Z(G)$ for some i, then $G_i \leq Z(G)$, and so G_i is an abelian normal subgroup of G, since $Z(G)$ is an abelian normal subgroup of G. As p is odd, then $|G|$ is odd. But G_i is primitive, then G/G_i is cyclic by Lemma 5.4.1, and so $G/G_i = \langle gG_i \rangle$ for some $g \in G$. Let $x, y \in G$ be arbitrary. Since $G = \biguplus_{k=1}^r (g^k G_i)$ (the disjoint union of cosets of G_i in G), then $x \in g^{j_1} G_i$ and $y \in g^{j_2} G_i$ for some integers j_1, j_2. So we can write $x = g^{j_1} z_1$ and $y = g^{j_2} z_2$, for some $z_1, z_2 \in G_i$. Now, using the fact that the elements of G_i commute with all the element of G, we get $xy = (g^{j_1} z_1)(g^{j_2} z_2) = g^{j_1} g^{j_2} z_1 z_2 = g^{j_1 + j_2} z_1 z_2 = g^{j_2 + j_1} z_2 z_1 = g^{j_2} g^{j_1} z_2 z_1 = g^{j_2} z_2 g^{j_1} z_1 = (g^{j_2} z_2)(g^{j_1} z_1) = yx$. Therefore G is abelian and we derive a contradiction with the assumption. Hence $G_i \neq G_i \cap Z(G)$, that is, $G_i \cap Z(G) < G_i$. It follows that $|G_i \cap Z(G)| < |G_i|$ for all i, and so $p|G_i \cap Z(G)| \leq |G_i|$. Dividing by $|G|$ both sides of the last inequality, we get

$\frac{p|G_i \cap Z(G)|}{|G|} \leq \frac{|G_i|}{|G|}$. Inverting the last inequality we get $\frac{|G|}{p|G_i \cap Z(G)|} \geq \frac{|G|}{|G_i|}$, that is, $\frac{1}{p}[G : G_i \cap Z(G)] \geq [G : G_i]$. From the last inequality we get

$$\begin{aligned}
[G : G_i] &\leq \frac{1}{p}[G : G_i \cap Z(G)] \\
&= \frac{1}{p}\frac{|G|}{|G_i \cap Z(G)|} \\
&= \frac{1}{p}\frac{|G|}{|Z(G)|}\frac{|Z(G)|}{|G_i \cap Z(G)|} \\
&= \frac{1}{p}[G : Z(G)][Z(G) : G_i \cap Z(G)].
\end{aligned}$$

We therefore calculate the upper bound as follows,

$$\begin{aligned}
\mu(G) &= [G : G_1] + \cdots + [G : G_n] \\
&\leq \frac{1}{p}[G : Z(G)][Z(G) : G_1 \cap Z(G)] + \cdots + \frac{1}{p}[G : Z(G)][Z(G) : G_n \cap \\
&\quad Z(G)] \\
&= \frac{1}{p}[G : Z(G)]([Z(G) : G_1 \cap Z(G)] + \cdots + [Z(G) : G_n \cap Z(G)]) \\
&= \frac{1}{p}[G : Z(G)](\mu(Z(G))) \\
&= \frac{1}{p}[G : Z(G)]\mu(Z(G)).
\end{aligned}$$

That is, $\mu(G) \leq \frac{1}{p}[G : Z(G)]\mu(Z(G))$. This proves one inequality. To prove that $p\mu(Z(G)) \leq \mu(G)$, suppose that G is not a non-trivial direct product. We claim that $G \neq Z(G)G_i$, for each i. Suppose that $G = Z(G)G_i$ for some i. By the discussion in Remark 5.4.2, it follows that $G_i \cap Z(G)$ is a direct factor of $Z(G)$. So, $Z(G) = H \times (G_i \cap Z(G))$ for some abelian subgroup H of G. Therefore $Z(G) = H(G_i \cap Z(G))$ and $H \cap (G_i \cap Z(G)) = \{1_G\}$, by definition of the direct product. However, since $G_i \cap Z(G) \leq G_i$, we have $HG_i = H(G_i \cap Z(G))G_i = [H(G_i \cap Z(G))]G_i = [Z(G)]G_i = Z(G)G_i = G$. Also, since $H \leq Z(G)$ then $H = H \cap Z(G)$. Thus, $H \cap G_i = (H \cap Z(G)) \cap G_i =$

$H \cap (G_i \cap Z(G)) = \{1_G\}$. Now observe that $H \neq G$, because G is non-abelian, also $G_i \neq G$ since $G_i \in \mathcal{R}$, and $\mathcal{R}$ is a minimal representation of G. So $H < G$ and $G_i < G$, and hence $G = H \times G_i$. So G is a direct product of two non-trivial subgroups. This contradicts the fact that G is not a non-trivial direct product. Consequently, $G \neq Z(G)G_i$ for all i, that is, $|Z(G)G_i| < |G|$. It follows that $p|Z(G)G_i| \leq |G|$. Dividing the last inequality by $|G_i|$, we have $p\frac{|Z(G)G_i|}{|G_i|} \leq \frac{|G|}{|G_i|}$, and so, $p\frac{[\frac{|Z(G)||G_i|}{|G_i \cap Z(G)|}]}{|G_i|} \leq \frac{|G|}{|G_i|}$. This implies that $p[\frac{|Z(G)|}{|G_i \cap Z(G)|}] \leq \frac{|G|}{|G_i|}$. Therefore $p[Z(G) : G_i \cap Z(G)] \leq [G : G_i]$. We calculate the lower bound as follows,

$$\begin{aligned} p\mu(G) &= p([Z(G) : G_1 \cap Z(G)] + \cdots + [Z(G) : G_n \cap Z(G)]) \\ &= p[Z(G) : G_1 \cap Z(G)] + \cdots + p[Z(G) : G_n \cap Z(G)] \\ &\leq [G : G_1] + \cdots + [G : G_n] \\ &= \mu(G). \end{aligned}$$

That is, $p\mu(G) \leq \mu(G)$, which proves the lower bound. Hence $p\mu(Z(G)) \leq \mu(G) \leq \frac{1}{p}[G : Z(G)]\mu(Z(G))$. □

An immediate corollary of the above theorem follows.

Corollary 5.4.5. *Suppose G satisfies the hypotheses of Theorem 5.4.4, further suppose that $[G : Z(G)] = p^2$, then $\mu(G) = p\mu(Z(G))$.*

Proof. By Theorem 5.4.4, $p\mu(Z(G)) \leq \mu(G) \leq \frac{1}{p}[G : Z(G)]\mu(Z(G))$. Substitute $[G : Z(G)] = p^2$ into the last inequality to get $p\mu(Z(G)) \leq \mu(G) \leq \frac{1}{p}(p^2)\mu(Z(G))$. This implies that $p\mu(Z(G)) \leq \mu(G) \leq p\mu(Z(G))$, and so $\mu(G) = p\mu(Z(G))$. □

In [24] the table with the orders, minimal degrees, centers and presentations of all p-groups of order less than or equal to p^4 is provided. The proofs

on how to find the degrees are also provided in [24]. We now provide this table. For the sake of readability and legibility, we present the tables in landscape format. For the isomorphism classes of p-groups of order than equal to p^4, see [4, *Table of groups of order* p^n, p *an odd prime*]. For the rest of the entries in the table, see the table [24, *Minimal degree of faithful representation of* p*-groups of order* $< p^5$].

Theorem 5.4.6. *Let G be a p-group of order less than or equal to p^4, then G is isomorphic to one of the G_i in the following table. The center and the minimal degrees of each group are given.*

Table 5.3.1: Minimal degrees for p-groups of order less than p^5

Group	Order	Group Presentation	Center	Minimal Degree
G_1	p	C_p	G_1	p
G_2	p^2	C_{p^2}	G_2	p^2
G_3	p^2	$C_p \times C_p$	G_3	$2p$
G_4	p^3	C_{p^3}	G_4	p^3
G_5	p^3	$C_{p^2} \times C_p$	G_5	$p^2 + p$
G_6	p^3	$C_p \times C_p \times C_p$	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	$\langle x, y \mid x^4 = y^4 = 1, xy = yx^{-1}, x^2 = y^2 \rangle \cong Q_8$	$\langle x^2 \rangle$	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	C_{p^4}	G_{10}	p^4

Table 5.3.1: Minimal degrees for p-groups of order less than p^5 (continued)				
G_{11}	p^4	$C_{p^3} \times C_p$	G_{11}	$p^3 + p$
G_{12}	p^4	$C_{p^2} \times C_{p^2}$	G_{12}	$2p^2$
G_{13}	p^4	$C_{p^2} \times C_p \times C_p$	G_{13}	$p^2 + 2p$
G_{14}	p^4	$C_p \times C_p \times C_p \times C_p$	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
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	$\langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yx^{p+1}, yz = zy, xz = zx \rangle$	$\langle x^p, z \rangle$	$p^2 + p$
G_{19}	p^4	$\langle x, y, z \mid x^{p^2} = y^p = z^p = 1, xy = yxz, zy = yz, xz = zx \rangle$	$\langle x^p, z \rangle$	$2p^2$
G_{20}	2^4	$\langle x, y, z \mid x^4 = y^4 = z^2 = 1, xy = yx^3, x^2 = y^2, xz = zx, yz = zy \rangle \cong Q_8 \times C_2$	$\langle x^2 \rangle$	10
G_{21}	2^4	$\langle x, y \mid x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$	$\langle x^4 \rangle$	8
G_{22}	2^4	$\langle x, y \mid x^8 = y^2 = 1, x^y = x^3 \rangle$	$\langle x^4 \rangle$	8
G_{23}	2^4	$\langle x, y \mid x^8 = y^4 = 1, xy = yx^{-1}, x^4 = y^2 \rangle \cong Q_{16}$	$\langle x^4 \rangle$	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

Table 5.3.1: Minimal Degrees for p-groups of Order less than p^5 (continued)					
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	$\langle x, y, w, z \mid x^p = y^p = w^p = z^p = 1, xy = yxz, xz = zx, xw = wx, yz = zy, yw = wy, zw = wz \rangle$	$\langle w, z \rangle$	$p^2 + p$	†
G_{28}	3^4	$\langle x, y, z \mid x^9 = y^3 = x^3 = 1, xy = yxz, xz = zx, yz = zx^6y \rangle$	$\langle x^3 \rangle$	27	
G_{29}	p^4, $p > 3$	$\langle x, y, w, z \mid x^p = y^p = w^p = z^p = 1, xy = yxz, zy = yzw, xz = zx, zw = wz, xw = wx, yw = wy \rangle$	$\langle w \rangle$	p^2	

An integer z is called a **quadratic residue modulo** n if there exists an integer x such that $x^2 \equiv z \pmod{n}$. Otherwise, z is called a **quadratic non-residue modulo** n. In the presentation of G_{26}, α is any quadratic non-residue modulo p.

We now prove directly that, for an odd prime p, all the groups of order p^n, where $n < 5$ are non-exceptional.

Theorem 5.4.7. *Exceptional p-groups of order $< p^5$, for an odd prime p, do not exist.*

Proof. Let G be a p-group of order $< p^5$. If $|G| \leq p^3$, then G/N is either cyclic or elementary abelian of order p^2, for any $N \lhd G$. So, it follows by Theorem 5.2.3 or Corollary 5.2.5, respectively, that G/N is never a distinguished quotient. Therefore, G is never exceptional. We now deal with the case where $|G| = p^4$. Suppose $|G| = p^4$, and note that if $N \lhd G$ such that $|N| > p$, then G/N either is cyclic or elementary abelian. Therefore, as in the case where $|G| \leq p^3$, we have that G is not exceptional. Suppose now that $|N| = p$. That is, $N = \langle n \rangle$, for some $n \in G$, such that $o(n) = p$. It follows that $|G/N| = p^3$. Therefore, by the Table 3.5.1, we have that G/N is isomorphic to one of the following:

(i) $G_4 = C_{p^3}$.

(ii) $G_5 = C_{p^2} \times C_p$.

(iii) $G_6 = C_p \times C_p \times C_p$.

(iv) $G_7 = \langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$.

(v) $G_9 = \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, zx = xz, zy = yz \rangle$.

Observe that the group in (i) is cyclic and the group in (iii) is elementary abelian. By Theorem 5.2.3 and Remark 5.2.1, we have that G/N is never distinguished, and so G is not exceptional. Suppose G/N is isomorphic to $C_{p^2} \times C_p$. It follows that $\mu(G/N) = \mu(C_{p^2} \times C_p) = \mu(C_{p^2}) + \mu(C_p) =$

$p^2 + p$. If G contains an element g of order p^3, then $\mu(G/N) = p^2 + p < p^2 \times p = p^3 = \mu(\langle g \rangle) \leq \mu(G)$, that is, $\mu(G/N) < \mu(G)$, and so G is not exceptional. Suppose G does not contain any element of p^3. Note that $N = \langle n \rangle$ is cyclic, and so abelian, hence $N = \langle n \rangle \leq Z(G)$. That is, $n \in Z(G)$. Since $G/N \cong C_{p^2} \times C_p$, it follows that there exists $h \in G$, such that $o(hN) = p^2$. Since $hn = nh$ and $o(n) = p$, we have $\langle h, n \rangle = \langle h \rangle \times \langle n \rangle \cong C_{p^2} \times C_p$. So $\mu(G/N) = \mu(C_{p^2} \times C_p) = \mu(\langle h \rangle \times \langle n \rangle) = \mu(\langle h, n \rangle) \leq \mu(G)$. Therefore G is not exceptional. Suppose $G/N \cong G_7 = \langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$ or $G/N \cong G_9 = \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, zx = xz, zy = yz \rangle$. So G is non-abelian. Suppose $G = H \times K$, where H and K are non-trivial. If $|H| = |K| = p^2$, then H and K are abelian. So G is abelian, a contradiction. So, without loss of generality, we assume $|H| = p^3$ and $|K| = p$. Since G is non-abelian, H is also non-abelian. It follows that $H \cong G_7$ or $H \cong G_9$. Hence, $\mu(G/N) = p^2 = \mu(G_7) = \mu(G_9) = \mu(H) \leq \mu(G)$, and G is not exceptional. Finally, suppose that G does not decompose into a non-trivial direct product. Since G is not abelian, then $Z(G) \neq G$, i.e., $Z(G) < G$ and so $\mu(Z(G)) < \mu(G)$. It follows by Theorem 5.4.4 that $\mu(G) \geq p(Z(G))$. However, $p\mu(Z(G)) \geq p^2 = \mu(G/N)$. So, $\mu(G/N) \leq \mu(G)$, and so G is not exceptional. □

5.4.2 Exceptional groups of order p^5

We now provide exceptional p-groups of order p^5, where p is an odd prime. The following is found in [25, Theorem 1] and its proof is explained below.

Theorem 5.4.8. *Let p be an odd prime and let $G = \langle x, y, z, w \mid x^{p^2} = y^p = z^p = w^p = 1, [y, z] = x^p w^{-1}, [x, z] = w, [x, y] = [x, w] = [y, w] = [z, w] = 1 \rangle$. Then G is an exceptional group of order p^5 with a distinguished subgroup*

$N = \langle w \rangle$ *and a distinguished quotient isomorphic to* G_{16}. *Furthermore,* $\mu(G) = 2p^2$.

Proof. First note that, for all $g, h \in G$, $[g, h] = 1$ if and only if $gh = hg$. From the presentation of G, $[x, w] = [y, w] = [z, w] = 1$, so w commutes with all the generators x, y and z of G. Also, $[w, x^p] = [y, x^p] = [z, x^p] = 1$, and so x^p commutes with all the generators of G. No other elements of G commutes with all the generators of G. It follows that $Z(G) = \langle x^p, w \rangle = \langle x^p \rangle \times \langle w \rangle$. Observe that $Z(G) = \langle x^p, w \rangle \cong C_p \times C_p$, so $G \in \tilde{G}_p$. Also note that $\mu(Z(G)) = 2p$. Now, by Theorem 5.3.2, the number of transitive constituents in any minimal representation $\mathcal{R}$ of G is 2. Also, by Theorem 5.4.4,

$$p\mu(Z(G)) \leq \mu(G) \leq \tfrac{1}{p}[G : Z(G)]\mu(Z(G)),$$

that is,

$$p(2p) \leq \mu(G) \leq \tfrac{1}{p}(p^3)(2p).$$

It follows that $2p^2 \leq \mu(G) \leq 2p^3$. Let $H = \langle y, z \rangle$ and $K = \langle x, y \rangle$. We will prove that $\mathcal{R} = \{H, K\}$ is a representation of G such that $\mu(G) = 2p^2$. We start by showing that $\mathcal{R}$ is a faithful representation. Note that $z \in H$, $zw = wz$ and $[x, z] = w$, so $xzx^{-1}z^{-1} = w$, this implies that $xzx^{-1} = zw = wz \notin H$. The latter implies that H is not a normal subgroup of G. However, $\langle y, x^p w^{-1} \rangle$ is a normal subgroup of G. To see this, note that $x^p w^{-1} \in Z(G)$ and y commutes with both x and w. Also $[y, z] = x^p w^{-1}$, so $yzy^{-1}z^{-1} = x^p w^{-1}$. It follows that, $(yzy^{-1}z^{-1})^{-1} = (x^p w^{-1})^{-1}$, so that $zyz^{-1}y^{-1} = wx^{-p}$. The latter implies that $zyz^{-1} = wx^{-p}y \in \langle y, x^p w^{-1} \rangle$. Therefore, $\langle y, x^p w^{-1} \rangle \trianglelefteq G$. Also, since $[y, z] = x^p w^{-1} \in H$ and $y \in H$, we have $\langle y, x^p w^{-1} \rangle \leq H$, and so $\langle y, x^p w^{-1} \rangle$ is normal in H, hence

$$core_G(H) \leq \langle y, x^p w^{-1} \rangle.$$

Since $y \in K$ and $zyz^{-1} = wx^{-p}y \notin K$, it follows that K is not a normal subgroup of G. However, $\langle xy \rangle$ is a normal subgroup of G. To see this, note that xy commutes with both x and y, since $[x, y] = 1$ and so $xy = yx$. From $[x, z] = w$, we have $(xzx^{-1}z^{-1}) = w^{-1}$ and so $zxz^{-1}x^{-1} = w^{-1}$. From this, we have $w^{-1}xz = zx$. Hence

$$\begin{aligned} z(xy)z^{-1} &= (zx)yz^{-1} = w^{-1}x(zyz^{-1}) = w^{-1}xwx^{-p}y = w^{-1}wxx^{-p}y \\ &= x^{-p+1}y = x^{-p+1}y^{-p+1} = (xy)^{-p+1} = (xy)^{1-p} \in \langle xy \rangle. \end{aligned}$$

Now $\langle xy \rangle \trianglelefteq G$ and $\langle xy \rangle \leq K$, so that $\langle xy \rangle$ is normal in K. Therefore $core_G(K) \leq \langle xy \rangle$. We now have

$$core_G(H) \bigcap core_G(K) \leq \langle y, x^p w^{-1} \rangle \bigcap \langle xy \rangle.$$

However, $\langle xy \rangle$ is cyclic of order p^2, and $\langle y, x^p w^{-1} \rangle$ is elementary abelian and so $\langle y, x^p w^{-1} \rangle \bigcap \langle xy \rangle = \{1\}$. Hence $core_G(H) \bigcap core_G(K) = \{1\}$. This proves that $\mathcal{R}$ is a faithful representation. We need to find the degree of $\mathcal{R}$. Observe that $o([y, z]) = o(x^p w^{-1}) = p$. Let $a = [y, z] = x^p w^{-1}$ and note that $[y, a] = yay^{-1}a^{-1} = yx^p w^{-1}y^{-1}wx^{-p} = yx^p w^{-1}wy^{-1}x^{-p} = yx^p y^{-1}x^{-p} = x^p yy^{-1}x^{-p} = x^p x^{-p} = 1$. Similarly, $[z, a] = 1$. Therefore, H can now be presented by

$\langle y, z, a \mid y^p = z^p = a^p = 1, [y, z] = a, [y, a] = [z, a] = 1 \rangle$

$= \langle y, z, a \mid y^p = z^p = a^p = 1, yzy^{-1}z^{-1} = a, ya = ay, za = az \rangle$

$= \langle y, z, a \mid y^p = z^p = a^p = 1, yz = azy, ya = ay, za = az \rangle$

$= \langle y, z, a \mid y^p = z^p = a^p = 1, yz = zay, ya = ay, za = az \rangle$

$= \langle y, z, a \mid y^p = z^p = a^p = 1, yz = zya, ya = ay, za = az \rangle$

$\cong G_9$.

Therefore $|H| = |G_9| = p^3$, and so $[G : H] = p^2$. Certainly $K = \langle x, y \rangle =$

$\langle x\rangle \times \langle y\rangle \cong C_{p^2} \times C_p$, and so $|K| = p^3$. It follows that $[G : K] = p^2$. Therefore $deg(\mathcal{R}) = [G : H] + [G : K] = p^2 + p^2 = 2p^2$. By minimality of $\mu(G)$, we have $\mu(G) \leq 2p^2$. We now have $2p^2 \leq \mu(G) \leq 2p^3$ and $\mu(G) \leq 2p^2$. This implies that $2p^2 \leq \mu(G) \leq 2p^2$, and so $\mu(G) = 2p^2$. On the other hand, factoring $N = \langle w\rangle$ out of G, we get $G/N = G/\langle w\rangle \cong G_{16} = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, yz = zyx^p, xy = yx, xz = zx\rangle$. Therefore, from Table 5.3.1, we have $\mu(G/N) = p^3$. Hence, $\mu(G/N) = p^3 > 2p^2 = \mu(G)$, proving that G is exceptional. □

We now present another two examples of exceptional groups of order p^5. These are found in [19, Theorem 5]

Theorem 5.4.9. *The following group of order p^5 are exceptional.*

(i) $G = \langle x, y, z, w \mid x^{p^2} = y^p = z^{p^2} = w^p = 1, z^p = x^{\alpha p}w, [x, z] = yw, [x, y] = x^p, [y, z] = [x, w] = [y, w] = [z, w] = 1\rangle$, *and*

(ii) $G = \langle x, y, z, w \mid x^{p^2} = y^p = z^{p^2} = w^p = 1, x^p = z^p w, [x, y] = x^p, [x, z] = y, [y, z] = [x, w] = [y, w] = [z, w] = 1\rangle$.

In the presentation of G in (i), α is any quadratic non-residue modulo p. Further, in both cases, $\mu(G) = 2p^2$ and $N = \langle w\rangle$ is a distinguished subgroup.

Proof. The proof follow by using arguments that are similar to those used in the proof of Theorem 5.4.8.

For (i), $Z(G) = \langle x^p, w\rangle \cong C_p \times C_p$, so $G \in \tilde{G}_p$. Also $\mu(Z(G)) = 2p$. By Theorem 5.3.2, the number of transitive constituents in any minimal representation $\mathcal{R}$ of G is 2. So by Theorem 5.4.4,

$$p\mu(Z(G)) \leq \mu(G) \leq \tfrac{1}{p}[G : Z(G)]\mu(Z(G)),$$

that is,

$$p(2p) \leq \mu(G) \leq \tfrac{1}{p}(p^3)(2p).$$

It follows that $2p^2 \leq \mu(G) \leq 2p^3$. In this case, set

$$H = \langle x, y \mid x^{p^2} = y^p = 1, [x, y] = x^p \rangle \cong G_7$$

and

$$K = \langle y, z \mid y^p = z^{p^2} = 1, [y, z] = 1 \rangle \cong C_p \times C_{p^2},$$

which are respectively a non-abelian subgroup and abelian subgroup, of order p^3. If we let $\mathcal{R} = \{H, K\}$, similar argument to that used in the proof of Theorem 5.4.8 shows that

$$core_G(\mathcal{R}) = core_G(H \cap K) = core_G(H) \bigcap core_G(K) = \{1\}.$$

Now $G/N = G/\langle w \rangle = \langle x, y, z \mid x^{p^2} = y^p = z^{p^2} = 1, z^p = x^{\alpha p}, [x, y] = x^p, [x, z] = y, [y, z] = 1 \rangle \cong G_{26}$. From Table 5.3.1, we have $\mu(G/N) = \mu(G_{26}) = p^3$. Now, by minimality of $\mu(G)$, we have

$$\mu(G) \leq deg(\mathcal{R}) = [G : H] + [G : K] = p^2 + p^2 = 2p^2 < p^3 = \mu(G/N).$$

Therefore G is exceptional.

For (ii), the proof is identical to the one above with $Z(G) = \langle x^p, w \rangle$,

$$H = \langle x, y \mid x^{p^2} = y^p = 1, [x, y] = x^p \rangle \cong G_7$$

and

$$K = \langle y, z \mid y^p = z^{p^2} = 1, [y, z] = 1 \rangle \cong C_p \times C_{p^2}.$$

In this case, $G/N = G/\langle w \rangle \cong \langle x, y, z \mid x^{p^2} = y^p = z^{p^2} = 1, x^p = z^p, [x, y] = x^p, [x, z] = y, [y, z] = 1 \rangle = \langle x, y, z \mid x^{p^2} = y^p = 1, z^p = x^p, xy = yx^{p+1}, xz = zxy, yz = zy \rangle \cong G_{25}$. From this, we obtain

$$\mu(G) = 2p^2 < p^3 = \mu(G_{25}) = \mu(G/N).$$

Hence, G is exceptional. □

5.5 Non-exceptional p-groups of order p^5

In Theorem 5.4.8 and Theorem 5.4.9, we provided three exceptional groups of order p^5 with distinguished quotients isomorphic to G_{16}, G_{25} and G_{26} of Table 5.3.1. Not all p-groups of order p^5 are exceptional. To provide a non-exceptional group of order p^5, we introduce a definition.

Definition 5.5.1. *Let K and Q be two groups. A group G is an **extension** of the group Q by the group K if G has a normal subgroup $N \cong K$ such that $G/N \cong Q$. We say that Q is **extended** by $N \cong K$ to G or $N \cong K$ **extends** Q to G. Moreover, if $N \leq Z(G)$, then G is called a **central extension**.*

In each of the exceptional groups of order p^5 provided in Theorem 5.4.8 and Theorem 5.4.9, G is an extension of its distinguished quotient by the distinguished subgroup $N = \langle w \rangle \leq Z(G)$. That is, G is a central extension of G_{16}, G_{25} or G_{26}, by $N = \langle w \rangle$. In fact, the following is shown in [24, Theorem 5.4].

Theorem 5.5.1. *If G is an exceptional group of order p^5, for p odd, 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 G_{16}, G_{25}, G_{26} or G_{27}.*

Proof. See [24, Theorem 5.4]. □

The statement of Theorem 5.5.1 implies that, up to isomorphism, any exceptional group of order p^5, p odd, is a central extension of G_i by some distinguished central subgroup N, for some $i = 16, 25, 26, 27$. However, G_{27}

cannot be extended by any distinguished central subgroup N, to an exceptional p-group G of order p^5 with $G/N \cong G_{27}$. This appears as [19, Theorem 6], we end this chapter by providing the proof of this result. We need the following definition.

Definition 5.5.2. *A group G is a **semidirect product** of a subgroup N and a subgroup H, if the following conditions are satisfied:*

1. $G = NH$
2. $N \trianglelefteq G$
3. $N \cap H = \{1_G\}$.

We write $N \rtimes H$ to indicate that G is a semidirect product of N and H.

It shall be noted that if G is a semidirect product of N and H, then $|G| = |N||H|$. We are now ready to prove the existence of non-exceptional p-group of order p^5.

Theorem 5.5.2. *The group $G_{27} = \langle x, y, w, z \mid x^p = y^p = w^p = z^p = 1, xy = yxz, xz = zx, xw = wx, yz = zy, yw = wy, zw = wz\rangle$, of order p^4, cannot be extended by a central subgroup N to an exceptional group G of order p^5 with distinguished quotient G/N isomorphic to G_{27}.*

Proof. Suppose the group $G_{27} = \langle x, y, w, z \mid x^p = y^p = w^p = z^p = 1, xy = yxz, xz = zx, xw = wx, yz = zy, yw = wy, zw = wz\rangle$, of order p^4, can be extended by a central subgroup N to an exceptional group G of order p^5 with distinguished quotient G/N isomorphic to G_{27}. We claim that $|Z(G)| = p$. Suppose $|Z(G)| \in \{p^2, p^3, p^4, p^5\}$.
Now, if $|Z(G)| = p^2$, then $Z(G) \cong C_{p^2}$ or $Z(G) \cong C_p \times C_p$. So $\mu(Z(G)) = p^2$ or $2p$ by Table 5.3.1. By Theorem 5.4.4, we have

$$p\mu(Z(G)) \leq \mu(G) \leq \tfrac{1}{p}[G : Z(G)]\mu(Z(G)).$$

Using the fact that $\mu(G_{27}) = p^2 + p$ and the lower bound $\mu(G) \geq p\mu(Z(G))$, we have

$$\mu(G) \geq p(p^2) = p^3 > p^2 + p = \mu(G_{27}) = \mu(G/N)$$

or

$$\mu(G) \geq p(2p) = 2p^2 = p^2 + p^2 > p^2 + p = \mu(G_{27}) = \mu(G/N),$$

respectively. In both cases, we have $\mu(G) > \mu(G/N)$, contradicting the exceptionality of G.

If $|Z(G)| = p^3$, then $[G : Z(G)] = p^2$. So, by Corollary 5.4.5, we have $\mu(G) = p\mu(Z(G))$. Also, since $Z(G)$ is abelian and $|Z(G)| = p^3$, we have $\mu(Z(G)) \in \{p^3, p^2 + p, 3p\}$, by Table 3.5.1. Hence $\mu(G) = p\mu(Z(G)) \in \{p^4, p^3 + p^2, 3p^2\}$. Notice that all the elements in the set $\{p^4, p^3 + p^2, 3p^2\}$ are strictly greater than $\mu(G/N) = p^2 + p$. Again, we have a contradiction since G is exceptional.

If $|Z(G)| = p^4$, we get the same contradiction as in the case where $|Z(G)| = p^3$, since $\mu(Z(G)) \in \{p^4, p^3 + p, 2p^2, p^2 + 2p, 4p\}$ and $\mu(G) \geq p\mu(Z(G)) \in \{p^5, p^4 + p^2, 2p^3, p^3 + 2p^2, 4p^2\}$. All the elements of this set are strictly greater than $\mu(G/N) = p^2 + p$.

If $|Z(G)| = p^5$, then $Z(G) = G$ and so G is abelian. By Theorem 5.2.2, G is not exceptional.

We conclude that $|Z(G)| = p$ and so $Z(G) \cong \langle w \rangle$. Now the center is generated by just one element. Therefore, if n is the number of constituents of a minimal representation of G, then $n = d(Z(G)) = 1$, by Theorem 5.3.2. So the minimal representation of G has only one core-free transitive constituent H. Also, $|H|$ is of prime-power order, since $H \leq G$. It follows that

$\mu(G) = [G : H] = |G|/|H| = p^k$ for some positive integer k. If $k = 1$, then H is a subgroup of order p^4 in a group of order p^5. Therefore $H \trianglelefteq G$, and so $core_G(H) = H$, which contradicts $core_G(H) = \{1_G\}$. If $k = 2$, then H is a subgroup of order p^3 in G. Since p is odd, by Table 3.5.1, H is isomorphic to one following of groups:

(i) C_{p^3}.

(ii) $C_{p^2} \times C_p$.

(iii) $C_p \times C_p \times C_p$.

(iv) $G_7 = \langle x, y \mid x^{p^2} = y^p = 1, xy = yx^{p+1} \rangle$.

(v) $G_9 = \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yxz, zx = xz, zy = yz \rangle$.

We prove that each case leads to a contradiction. Now, $k = 2$ implies that $\mu(G) = [G : H] = |G|/|H| = p^2$. Since $\mu(H) \leq \mu(G) = p^2$ and $\mu(C_{p^3}) = p^3$ then $H \ncong C_{p^3}$. Also, since $\mu(C_{p^2} \times C_p) = p^2 + p$, then $H \ncong C_{p^2} \times C_p$. Suppose $H \cong G_7$ or $H \cong G_9$. Note that the elements of the group $\langle w \rangle$ commute with the elements of H. Also, H is core-free, so H has no non-trivial normal subgroups. It follows that $H \cap Z(G) \cong H \cap \langle w \rangle = \{1_G\}$. That is, $G_7 \cap \langle w \rangle = \{1_G\}$ and $G_9 \cap \langle w \rangle = \{1_G\}$, since we are assuming that $H \cong G_7$ or $H \cong G_9$. Therefore, $G_7\langle w \rangle = G_7 \times \langle w \rangle$ and $G_9\langle w \rangle = G_9 \times \langle w \rangle$. Now note that $G_7\langle w \rangle \cong H\langle w \rangle \leq G$ and $G_9\langle w \rangle \cong H\langle w \rangle \leq G$. Therefore, $\mu(G_7\langle w \rangle) \leq \mu(G) = p^2$ and $\mu(G_9\langle w \rangle) \leq \mu(G) = p^2$. However, by Lemma 3.4.13, we have $\mu(G_7\langle w \rangle) = \mu(G_7 \times \langle w \rangle) = \mu(G_7) + \mu(\langle w \rangle) = p^2 + p > p^2 = \mu(G)$, a contradiction. Similarly, $\mu(G_9\langle w \rangle) > \mu(G)$, a contradiction again. Thus we have $H \ncong G_7$ or $H \ncong G_9$. The only case that remains is $H \cong C_p \times C_p \times C_p$. Suppose $H \cong C_p \times C_p \times C_p$. By Theorem 4.1.5 (i), G has a normal abelian

subgroup P of order p^3. Since $core_G(H) = \{1_G\}$, then H does not contain any non-trivial normal subgroups of G. But P is a non-trivial normal subgroup of G, so $P \cap H = \{1_G\}$. We now have $PH \leq G$ and $PH = P \rtimes H$, so $|PH| = |P \rtimes H| \leq |G| = p^5$. However, $|P \rtimes H| = |P||H| = p^3p^3 = p^6$, a contradiction.

So we must have that $k > 2$, that is, $\mu(G) = [G : H] = |G|/|H| \geq p^3$. Consequently, $\mu(G_{27}) = p^2 + p < p^2 \times p = p^3 \leq \mu(G)$. So, G is not an exceptional group of order p^5 whenever $G/N \cong G_{27}$ with N central in G. □

So, G_{27} should not be a part of the statement of Theorem 5.5.1.

Chapter 6

Remarks and conclusions

The work carried out in this dissertation explores a number of open questions. The extent of the class of finite groups for which μ is additive is not known. As remarked towards the end of Chapter 3, it is not known whether or not the content of Theorem 3.7.1 is exhaustive. That is, it is still unknown whether the class of finite groups for which μ is additive consists only of finite groups of coprime order, finite nilpotent (and hence finite p-groups and finite abelian groups), finite simple groups and elements of the class $\mathcal{G}$. Note that within the class of finite groups for which μ is additive, we have the class $\mathcal{G}$ whose extent is also not known. So, before one attempts to investigate the extent of the class of finite groups for which μ is additive, it will be plausible to first investigate the extent of the class $\mathcal{G}$.

In Theorem 5.2.2, it is shown that the class of finite abelian groups does not have exceptional elements. From this we deduced that if G is abelian and N is a subgroup of G, then the abelian quotient G/N is never distinguished. Also, in Theorem 5.2.3, we proved that a distinguished quotient of an exceptional group is never cyclic. We also remarked that distinguished quotients

cannot be elementary abelian and that this is shown in [21]. From this, we also deduced in Corollary 5.2.5 that distinguished quotients are never isomorphic to abelian groups of order p^2. Despite all this work, the following remains as a conjecture.

Conjecture 6.1. *If G is a finite group and N is a normal subgroup of G such that G/N is abelian, then G/N is not distinguished.*

In an attempt to address this conjecture, it is shown in [22, Theorem 1] that if the quotient G/N has no non-trivial abelian normal subgroup, then G/N is not distinguished. So, for G/N to be distinguished, G/N must posses at least one non-trivial abelian subgroup which is normal and abelian in G/N. Note that the converse statement of [22, Theorem 1] does not hold. That is, it is not true that if G/N is not distinguished then G/N has no non-trivial abelian normal subgroup. A simple counter example to the converse of [22, Theorem 1] is the content of Theorem 5.2.3, since every non-trivial subgroup of a cyclic group is abelian and normal. So, when one is attempting to prove or disprove Conjecture 6.1, G should be chosen to be a non-abelian group and N should be chosen such that the abelian quotient G/N is not cyclic, not elementary abelian and not have order p^2 since the research carried thus far shows that the result is already affirmative in all these cases.

There are open questions on the exceptional groups. For example, the extent of the class of exceptional groups is not known. Moreover, the extent of the class of exceptional p-groups is not known. By Theorem 5.4.7, we know that there are no exceptional p-groups of order less that p^5, for an odd prime p. For an odd prime p, by Theorem 5.5.1 we know that if G is an exceptional group of order p^5, then G is a central extension of a distinguished G/N of order p^4 by some subgroup $N \leq Z(G)$ of order p, where G/N is isomorphic

to G_{16}, G_{25}, G_{26} or G_{27}. However, Theorem 5.5.2 shows that G_{27} cannot be centrally extended to an exceptional group of order p^5. Thus, the exceptional groups of order p^5 provided in Theorem 5.4.8 and Theorem 5.4.9 are central extensions of distinguished quotients which are isomorphic to G_{16}, G_{25} and G_{26}. An open question with regard to this arises: for an odd prime p, can exceptional p-groups of order higher than p^5 be found via central extensions where the distinguished quotient is isomorphic to a p-group of smaller order? Of course, to address this question, the isomorphism classes of p-groups of order higher than p^5 should be considered. We should mention at this point that finite group theorists have been interested in counting groups of prime-power order, as a preliminary step to assist in explicitly listing such groups. Determining the number of p-groups of a given order seems easier than listing them as in the latter situation we require a complete list of explicit presentations of all isomorphism types of groups of that order which is not redundant. However, determining the number of p-groups is a difficult problem on its own. For example, we already have the following facts:

(i) There are $2p + 61 + 2\text{gcd}(p-1,3) + \text{gcd}(p-1,4)$ groups of order p^5.

(ii) There are 267 groups of order 2^6 and 504 groups of order 3^6. For $p \geq 5$, the number of groups of order p^6 is $3p^2 + 39p + 344 + 24\text{gcd}(p-1,3) + 11\text{gcd}(p-1,4) + 2\text{gcd}(p-1,5)$.

(iii) The numbers of groups of order 2^7, 3^7 and 5^7 are respectively 2328, 9310 and 34297. For $p > 5$, the number of groups of order p^7 is

$$3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455 + (4p^2 + 44p + 291) \times \gcd(p-1,3) + (p^2 + 19p + 135) \times \gcd(p-1,4) + (3p + 31) \times \gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) + \gcd(p-1,9).$$

Definition 6.0.3. *A function f defined over the primes is **polynomial on residue classes (PORC)** if it is the sum of terms of the form $a(p) \cdot b(p)$, where $a(p)$ is a product of terms of the form $gcd(p, c(p))$, such that $b(p)$ and $c(p)$ are polynomials in p with rational coefficients.*

G. Higman [16] conjectured the following.

Conjecture 6.2. *(PORC Conjecture) The number of groups order p^n, for a fixed positive integer n and a prime number p is PORC.*

Conjecture 6.2 has been proved correct for $n \leq 7$. For the details of the proofs of the facts mentioned in (i), (ii), (iii) and for further reading with regard to the enumeration of the groups of order p^n (also for the current status with regard to PORC Conjecture) the reader is referred to the readings of articles like [15], [16], [26], [27], [28] and the thesis in [34]. Despite the fact that the number of groups of order p^5, p^6 and p^7 is known, the respective isomorphism classes of these groups are not known. So the complexity on the problem of finding all exceptional p-groups of order $\geq p^5$ through (or possibly not through) central extensions go as far as finding the isomorphism classes of such groups. Regrettably, the isomorphism classes of p-groups of order $\geq p^5$ are not known. Thus, alternative methods of establishing exceptional p-groups of order $> p^4$ need to be established. We would like to stress at this point that the only class of exceptional groups that we are aware of, which is not in the class of p-groups, is the class of the direct product $D_{2^n q} \times D_{2^m r}$, where m, n, q, r are such that $2 \leq n \leq m$, q and r are odd, $2^n q > 4$ and

$2^m r > 4$. The distinguished quotient associated with the exceptionality of $D_{2^n q} \times D_{2^m r}$ is the central product $D_{2^n q} * D_{2^m r}$. For a detailed account of this class of exceptional groups, the reader is submitted to the readings of [7, Proposition 2.8].

Bibliography

[1] Y. Berkovich, *Groups of Prime Power Order*, Vol. 1, de Gruyter Expositions in Mathematics 46, Berlin, 2008.

[2] Y. Berkovich and Z. Janko, *Groups of Prime Power Order*, Vol. 2, de Gruyter Expositions in Mathematics 47, Berlin, 2008.

[3] Y. Berkovich and Z. Janko, *Groups of Prime Power Order*, Vol. 3, de Gruyter Expositions in Mathematics 56, Berlin, 2011.

[4] W. Burnside, *Theory of Groups of Finite Order*, 2nd Edition, Cambridge University Press, London, 1911.

[5] P. J. Cameron, *Permutation Groups*, Vol. 45, London Mathematical Society Student Texts, Cambridge University Press, Cambridge, UK, 1999.

[6] J. D. Dixon and B. Mortimer, *Permutation Groups*, Vol. 163, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[7] D. Easdown and C. E. Praeger, On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.,* **38**, (1988), 207-220.

[8] B. Elias, L. Silberman and R. Takloo-Bighash, *Minimal permutation representations of nilpotent groups*, Experiment. Math., **19**, (2010), 121-128.

[9] C. Franchi, On minimal degrees of permutation representations of abelian quotients of finite groups, *Bull. Aust. Math. Soc.,* **84**, (2011), 408-413

[10] J. F. Humphreys, *A Course in Group Theory*, Oxford University Press, Oxford, 1996.

[11] J. A Galliani, *Contemporary Abstract Algebra*, Houghton Miffin Company, New York, 2006.

[12] J. Gilbert and L. Gilbert, *Elements of Mordern Algebra*, PSW-KENT Publishing Co., Columbia, 1988.

[13] D. Gorenstein, *Finite Groups*, 2nd Edition, Chelsea Publishing Co., New York, 1980.

[14] I. N. Herstein, *Topics in Algebra*, John Wiley and Sons, Inc., New York, 1975.

[15] G. Higman, Enumerating p-groups. I: Inequalities, *Proc. London Math. Soc.,* **10**, (1960), 24-30.

[16] G. Higman, Enumerating p-groups. II: Problems whose solution is PORC, *Proc. London Math. Soc.,* **10**, (1960), 566-582.

[17] B. Huppert, *Eindliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, 1967.

[18] M. Isaacs, *Finite Group Theory*, American Mathematical Society, Rhodes Island, 2008.

[19] R. Jiang, Exceptional p-groups of order p^5, *arXiv preprint arXiv:1104.3226*, (2011).

[20] D. L. Johnson, Minimal permutation representation of finite groups, *Amer. J. Math.,* **93**, no. 4, (1971), 857-866.

[21] L. G. Kovács and C. E. Praeger, Finite permutation groups with large abelian quotients. *Pacific. J. Math.,* **136**, no. 2, (1989), 283-292.

[22] L. G. Kovács and C. E. Praeger, On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.,* **62**, (2000), 311-316.

[23] L. Lauritzen, *Concrete Abstract Algebra*, Cambridge University Press, New York, 2003.

[24] S. R. Lemieux, *Minimal Degree of Faithful Permutation Representations of Finite Groups*, MSc Thesis, Carleton University, Ottawa, 1999.

[25] S. R. Lemieux, Finite exceptional p-groups of small order, *Comm. Algebra,* **35**, (2007), 1890-1894.

[26] M. F. Newman, E. A. O'Brien and M. R. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, *J. Algebra,* **278**, (2004), 383-401.

[27] E. A. O'Brien, The p-group generation algorithm, *J. Symbolic Comput.,* **9**, (1990), 677-698.

[28] E. A. O'Brien and M. R. Vaughan-Lee, The groups with order p^7 for odd prime p, *J. Algebra,* **292**, (2005), 243-358.

[29] J. S. Rose, *A Course on Group Theory*, Dover Publications, Inc., New York, 1978.

[30] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th Edition, Springer-Verlag, New York, Inc., 1995

[31] C. Sah, *Abstract Algebra*, Academic Press Inc. (London) Ltd, New York, 1967.

[32] N. Saunders, Strict inequalities for minimal degrees of direct products, *Bull. Austral. Math. Soc.,* **79**, 2009.

[33] N. Saunders, *Minimal Faithful Permutation Representations of Finite Groups*, PhD Thesis, University Sydney, 2011.

[34] B. E. Witty, *Enumeration of groups of prime-power order*, PhD Thesis, Australian National University, 2006.

[35] D. Wright, The non-minimality of induced central representation, *Pac. J. Math.* **53**, no. 1, (1974), 301-306.

[36] D. Wright, *Degrees of minimal embeddings for some direct product*, *Amer. J. Math.* **97**, no. 4, (1975), 897-903.