GENERATION PROBLEMS FOR FINITE GROUPS

Jonathan M. McDougall-Bagnall

A Thesis Submitted for the Degree of PhD
at the
University of St. Andrews

2011

Generation Problems for Finite Groups

Jonathan M. McDougall-Bagnall

Thesis submitted for the degree of Doctor of Philosophy

of the University of St Andrews

July 4th, 2011

Abstract

It can be deduced from the Burnside Basis Theorem that if G is a finite p-group with $d(G) = r$ then given any generating set A for G there exists a subset of A of size r that generates G. We have denoted this property $\mathcal{B}$. A group is said to have the basis property if all subgroups have property $\mathcal{B}$. This thesis is a study into the nature of these two properties. Note all groups are finite unless stated otherwise.

We begin this thesis by providing examples of groups with and without property $\mathcal{B}$ and several results on the structure of groups with property $\mathcal{B}$, showing that under certain conditions property $\mathcal{B}$ is inherited by quotients. This culminates with a result which shows that groups with property $\mathcal{B}$ that can be expressed as direct products are exactly those arising from the Burnside Basis Theorem.

We also seek to create a class of groups which have property $\mathcal{B}$. We provide a method for constructing groups with property $\mathcal{B}$ and trivial Frattini subgroup using finite fields. We then classify all groups G where $G/\Phi(G)$ is isomorphic to this construction. We finally note that groups arising from this construction do not in general have the basis property.

Finally we look at groups with the basis property. We prove that groups with the basis property are soluble and consist only of elements of prime-power order. We then exploit the classification of all such groups by Higman [5] to provide a complete classification of groups with the basis property.

1. Candidate's declarations

I, Jonathan McDougall-Bagnall, hereby certify that this thesis, which is approximately 26,000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

I was admitted as a research student in September 2006 and as a candidate for the degree of Doctor of Philosophy in September 2007; the higher study for which this is a record was carried out in the University of St Andrews between 2006 and 2011.

Date ________ Signature of candidate ________________________________

2. Supervisor's declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Ph.D. in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Date ________ Signature of Supervisor ________________________________

3. Permission for electronic publication

In submitting this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that my thesis will be electronically accessible for personal or research use unless exempt by award of an embargo as requested below, and that the library has the right to migrate my thesis into new electronic forms as required to ensure continued access to the thesis. I have obtained any third-party copyright permissions that may be required in order to allow such access and migration, or have requested the appropriate embargo below.

The following is an agreed request by candidate and supervisor regarding the electronic publication of this thesis:

- Access to printed copy and electronic publication of thesis through the University of St Andrews.

Date ________ Signature of Candidate ________________________________

Date ________ Signature of Supervisor ________________________________

Acknowledgments

Before we get into the major dose of mathematics that is my thesis I would like to thank a few people.

I'll begin with the man who has somehow managed to supervise me over the course of the last 5 years, Dr Martyn Quick. Despite my tendency to chat incessantly about football, cricket, or any other sport that has happened to be on, Martyn has managed to guide me through the particular minefield that is research. His constant help and understanding has allowed me to produce something that I am truly proud of, and his enthusiasm for our work has helped me through the darker moments.

I'd also like to thank EPSRC for funding two years of my Ph.D. Without funding I don't think I'd have even considered doing a Ph.D. so, for allowing me the opportunity to do so, thank you.

On a similar note I'd also like to thank my parents. During my first year they provided the financial support I needed to get going and throughout they have been given great support and encouragement to me. Hopefully all this money spent on my education will pay off!

Throughout my time at St Andrews I have met and worked with many different people many of whom I can now call friends. I would like to first mention my office mates Fiona, Yann and Hannah, all of whom shared my office for the majority of my studies and helped provide a fun and relaxed working environment. I'd also like to mention all those physicists masquerading as mathematicians in the Solar Group (you know who you are). You provided a distraction when work was needed, and I would now like to mention that I am placing the blame for my thesis being finished in year 5

down to you lot. Especially James who always wants to distract me when I'm working hard. But in the long run you are all great friends and one of the biggest things I'm going to miss from my studies is hanging out with you.

I would most like to thank my wife Dee. A long time ago (in this galaxy, not one far, far away) I began this thesis with you as my girlfriend; now we are 3 years married and expecting our first child. Your support throughout has been the best I could have wished for, and I am absolutely certain I would have never finished this without you. To our unborn child I would just like to say, never read this thesis - Harry Potter is a much better choice for a bedtime story.

Contents

Chapter 1

Introduction

Generating sets for groups have been a topic of interest for many years; along with presentations, they are one of the easiest ways of describing a group and can themselves tell us something about the internal structure of the group. In this tradition we investigate two generating properties of groups throughout this thesis. We seek to describe how these properties affect the structure of a group and, if possible, provide a classification of all groups with each property. Note that all groups are finite unless stated otherwise.

A *generating set* A of a group G can be defined as being a subset of elements of G from which each element of G can be expressed as a finite product of the elements of A and their inverses. If A is any subset of a group G then we denote $\langle A \rangle$ as the *subgroup of G generated by A*, and if $G = \langle A \rangle$ then we say that A *generates* G. Contrasting this is the idea of non-generators. An element x of a group G is a *non-generator* if for any set A containing x that generates G then $A \backslash \{x\}$ also generates G. It is worth noting here that the set of non-generators is known as the Frattini subgroup, denoted $\Phi(G)$. This is not the traditional definition of the Frattini subgroup. It is more commonly defined as the intersection of all maximal subgroups in a group G (we address this in Section 2.1.1).

Continuing with some notation for a given group G we define $d(G)$ to be the least number of generators required to generate G. For example given a cyclic group C_n then $d(C_n) = 1$, and if G is any non-trivial dihedral group then $d(G) = 2$. This leads us to a simple definition of what it means for a generating set of a group to be minimal.

Definition 1.0.1. *A generating set A is said to be minimal if no proper subset of A is also a generating set.*

Using this definition we can establish our first property.

Definition 1.0.2. *A group G is said to have property $\mathcal{B}$ if all minimal generating sets have the same size.*

We note that this is equivalent to saying that if A is a generating set of a group G then A contains a subset of size $d(G)$ that also generates the group.

It is not immediately obvious whether or not property $\mathcal{B}$ is inherited by subgroups; in fact we will see that this is not the case. This gives rise to our second property.

Definition 1.0.3. *A group G is said to have the basis property if all subgroups of G have property $\mathcal{B}$.*

From this definition it is easy to see that if a group has the basis property then it also has property $\mathcal{B}$.

1.1 History

In this section we will highlight some of the previous research into the two properties we will investigate.

The first work that provided a classification of some of the groups with property $\mathcal{B}$ was the Burnside Basis Theorem [8, 5.3.2]. To describe this we must first define the commutator subgroup of a group G as $G' = [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$.

Theorem 1.1.1 (Burnside Basis Theorem). *Let G be a finite p-group. Then $\Phi(G) = G'G^p$. Also if $|G : \Phi(G)| = p^r$ then every set of generators of G has a subset of size r that also generates G.*

The first part of the Theorem gives us information about the structure of the Frattini subgroup and so the proof is omitted. The second part shows that G behaves like a vector space.

Proof. Let $G = \langle x_1, \ldots, x_d \rangle$. Then the Frattini quotient $G/\Phi(G)$ is generated by the elements $x_1\Phi(G), \ldots, x_d\Phi(G)$. Since $G/\Phi(G)$ is a vector space of dimension r over the field $\mathbb{F}_p$ it has a basis of size r of the form $\{x_{i_1}\Phi(G), \ldots, x_{i_r}\Phi(G)\}$. Thus G is equal to $\langle x_{i_1}, \ldots, x_{i_r}, \Phi(G) \rangle$ and since the Frattini subgroup is the set of non-generators then $G = \langle x_{i_1}, \ldots, x_{i_r} \rangle$. □

Now if G satisfies the hypothesis of the Burnside Basis Theorem then $d(G) = r$. For clearly $d(G)$ cannot be less than r otherwise we could generate $G/\Phi(G)$ by less than r elements contradicting $G/\Phi(G)$ being a vector space of dimension r. Also $d(G)$ cannot be greater than r since the Burnside Basis

Theorem tells us G can be generated minimally by r elements. Therefore if G is a p-group it has property $\mathcal{B}$.

Raffaele Scapellato and Libero Verardi in their 1991 paper [10] investigate a class of groups called matroid groups. They begin by establishing a definition of independence. In their paper a set X is said to be *independent* if for all x in X, $\langle X \backslash \{x\}, \Phi(G) \rangle \neq \langle X, \Phi(G) \rangle$. They then define G to be a matroid group if it satisfies the following properties:

(i) G has property $\mathcal{B}$,

(ii) If X and Y are two minimal generating sets of G of the same size then for all $x \in X \backslash Y$ there exists $y \in Y \backslash X$ such that $(X \backslash \{x\}) \cup \{y\}$ is also a minimal generating set of G,

(iii) Any independent subset X of G is contained in a minimal generating set of G.

It can be noted here that the second two properties are satisfied by vector spaces.

Scapellato and Verardi view the matroid property as being one analogous to that of the Burnside Basis Theorem, stating that as a consequence of the Burnside Basis Theorem all finite p-groups are matroid groups.

In their paper Scapellato and Verardi begin by showing that a group is a matroid group if and only if its quotient by the Frattini subgroup is also a matroid group, and they provide a theorem describing properties of subgroups of a matroid group.

Theorem 1.1.2. *[10, Theorem 1.2] Let G be a matroid group with $\Phi(G) = 1$ and H a proper subgroup of G. Then:*

(i) all the minimal generating sets of H have the same size, $d(H)$;

(ii) for all independent subsets X of H, $|X| \leq d(H)$;

(iii) $d(H) < d(G)$.

In another paper [9] of the same year Scapellato and Verardi show that if a group with trivial Frattini subgroup satisfies conditions (ii) and (iii) from Theorem 1.1.2 then it is a matroid group.

In the second section Scapellato and Verardi prove several results on matroid groups with trivial Frattini subgroup including a classification of all such groups. They begin by showing that if G is a matroid group with $\Phi(G) = 1$ then all elements of G have prime-power order. Then, using the Classification of Finite Simple Groups to eliminate certain examples, they show that a matroid group with $\Phi(G) = 1$ is soluble. The section finishes with a theorem that classifies all such groups.

Theorem 1.1.3. *[10, Theorem 2.5] A finite group G, with $\Phi(G) = 1$, is a matroid group if and only if one of the following conditions is satisfied:*

(i) G is an elementary abelian p-group;

(ii) $|G| = p^n q$ and the Fitting subgroup is elementary abelian of order p^n, where p and q are primes with $p \equiv 1 \pmod{q}$, and an element of order q induces a power automorphism on the Fitting subgroup.

For finite groups the *Fitting subgroup* of G is the largest normal nilpotent subgroup of G. A *power automorphism* is an automorphism that sends an element to some power of that element. By definition a power automorphism preserves subgroups and so greatly restricts the structure of a group.

The final section of the Scapellato and Verardi paper goes on to provide results on how to construct examples of matroid groups and also states a theorem that describes the structure of a matroid group G such that $G/\Phi(G)$ is as described in Theorem 1.1.3.

Theorem 1.1.4. *Theorem [10, 3.1] Let G be a matroid group, such that $|G/\Phi(G)| = p^n q$, and $p \equiv 1 \pmod{q}$. Then:*

(i) G has a unique Sylow p-subgroup;

(ii) all the Sylow q-subgroups of G are cyclic;

(iii) if P is the Sylow p-subgroup of G and Q a Sylow q-subgroup of G, then $\Phi(G) = \Phi(P) \times \Phi(Q)$;

(iv) P possesses an automorphism of order q, which induces a power automorphism on $P/(P \cap \Phi(G))$.

This paper was the major inspiration on our work on property $\mathcal{B}$. We began our work by trying to replicate the results Scapellato and Verardi provided in their paper for groups with property $\mathcal{B}$.

They returned to their work in 1994 [11] focusing on groups that only satisfied their property on independence from the first paper. It should also be noted that whilst Scapellato and Verardi did not explicitly deal with groups with the basis property as a consequence of Theorem 1.1.2 all matroid groups have the basis property.

Work into the basis property has been mostly limited to the world of semigroups. In 1978 Jones published a paper [7] which firstly looked at semigroups with the basis property, looking at groups with the basis property towards the end of the paper. Jones begins his paper by stating that if

S is an inverse semigroup and $U \leqslant V \leqslant S$ then a U-basis for V is a subset X of V which is minimal such that $\langle U \cup X \rangle = S$. From this, one can see that a minimal generating set for V (called a basis in the paper) is simply a $\emptyset$-basis. This leads to the definition of two properties.

Definition 1.1.5. *An inverse semigroup S has the strong basis property if for any inverse subsemigroup V of S and inverse subsemigroup U of V any two U-bases for V have the same size.*

Definition 1.1.6. *An inverse semigroup S has the basis property if for any inverse subsemigroup V of S any two bases for V have the same size.*

In the first four sections of Jones' paper he provides results on the structure of various types of inverse semigroups (including commutative inverse semigroups, Brandt semigroups and groups) with the strong basis property, building on work from a previous paper [6]. He also details two cases where the basis property and the strong basis property are in fact equivalent. This all comes together in Theorem 4.8 of [7] which describes necessary and sufficient conditions for an inverse semigroup to satisfy the strong basis property.

It is in section 5 of Jones' paper where we see the results on the basis property of groups. Here he details results that show that a group with the basis property is soluble and all elements of such a group have prime-power order. He additionally shows that homomorphic images of groups with the basis property also have the basis property. We will provide our own proofs to these results in Chapter 5 (namely Lemma 5.2.2, Lemma 5.2.1 and Corollary 5.2.3). Jones also notes that Graham Higman [5, Theorem 1] classified the soluble groups with all elements of prime-power order in his 1956 paper. A classification of groups with the basis property based on this was announced by N. K. Dickson and Jones in [7], but as far as we can tell this has yet to be published. However a classification of groups with the basis property was announced by A. Al'Khalaf [1] exploiting Higman's result, but his classification requires a technical condition on the p-group. We will also provide a classification in Chapter 5 and whilst ours is also based on Higman's result, our classification is established from a construction of groups with property $\mathcal{B}$.

Following on from the Jones paper is a 2002 paper [2] which shows that the finite quasiprimary groups — that is, those groups in which the order of each element is p^n or q^m for two distinct primes p and q — also satisfy the basis property.

1.2 Thesis Outline

We begin this thesis by establishing some common results from both group and module theory. The results on group theory relate mostly, although not exclusively, to the Frattini subgroup and its properties. We then look at group rings and group algebras which lead us into module theory. Here we establish the basic definitions of module theory and provide several well known results by Maschke, Clifford and Krull–Schmidt. The theorems provided in this chapter are used throughout to establish our results.

Chapter 3 provides several results that hold for groups with property $\mathcal{B}$. We begin by showing that property $\mathcal{B}$ transfers to the quotient by the Frattini subgroup.

Lemma 3.1.1. *A group G has property $\mathcal{B}$ if and only if $G/\Phi(G)$ has property $\mathcal{B}$.*

We then provide examples of groups with and without property $\mathcal{B}$ and show that not only p-groups have property $\mathcal{B}$.

Proposition 3.1.6. *If G is the dihedral group D_p of order $2p$, where p is a prime number, then G has property $\mathcal{B}$.*

Using Lemma 3.1.1 we then establish that dihedral groups of order $2p^n$, denoted D_{2p^n}, also have property $\mathcal{B}$.

We move on to look at subgroups and quotients of groups with property $\mathcal{B}$. When looking at subgroups we provide an example showing that not all subgroups of groups with property $\mathcal{B}$ also have property $\mathcal{B}$, and then state a trio of results which show the conditions for which property $\mathcal{B}$ is inherited by quotients.

Lemma 3.2.2. *If G is a group with property $\mathcal{B}$ and G splits over a minimal normal subgroup M then G/M has property $\mathcal{B}$.*

Proposition 3.2.3. *If G is a group with property $\mathcal{B}$ and M is an abelian minimal normal subgroup of G then G/M has property $\mathcal{B}$.*

Corollary 3.2.4. *If G is a soluble group with property $\mathcal{B}$ then any quotient G/N also has property $\mathcal{B}$.*

Finally, we conclude the chapter by looking at the direct product of groups with property $\mathcal{B}$ and how their structure is affected.

Theorem 3.3.1. *The group $G \times H$ has property $\mathcal{B}$ if and only if $G \times H$ is a p-group.*

In Chapter 4 we provide a construction for groups with property $\mathcal{B}$ and trivial Frattini subgroup. Partly inspired by Scapellato and Verardi (specifically Theorem 1.1.4) and our result on dihedral groups of order $2p^n$, we demonstrate a way of constructing a class of groups with property $\mathcal{B}$ and trivial Frattini subgroup from a finite field. We then classify all groups G with $G/\Phi(G)$ as given by our construction. Note that it follows from Lemma 3.1.1 that all such groups have property $\mathcal{B}$.

Theorem 4.1.4. *Let V be the additive group of the field $\mathbb{F}_{p^n}$ of p^n elements and H the subgroup of the multiplicative group $\mathbb{F}_{p^n}^\star$ of order q^m, where q is a prime such that $q^m \mid p^n - 1$. Define G to be the semidirect product $V \rtimes_\phi H$ where H acts on V by multiplication in $\mathbb{F}_{p^n}$. Then:*

(i) G has property $\mathcal{B}$,

(ii) $d(G) = k + 1$ where V is a direct sum of k irreducible $\mathbb{F}_pH$-modules,

(iii) $\Phi(G)$ is trivial.

Theorem 4.2.1. *Let V be the additive group of the field $\mathbb{F}_{p^n}$ of p^n elements and H the subgroup of the multiplicative group $\mathbb{F}_{p^n}^\star$ of order q^m, where q is a prime such that $q^m \mid p^n - 1$. Let G be any group such that $G/\Phi(G)$ is isomorphic to the semidirect product $V \rtimes_\phi H$ where H acts on V via the multiplication in $\mathbb{F}_{p^n}$. Then:*

(i) G has a unique Sylow p-subgroup P,

(ii) G is the semidirect product of P by Q for any Sylow q-subgroup Q and all Sylow q-subgroups of G are cyclic,

(iii) $\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$ *where* $\langle x^{q^m} \rangle$ *is the subgroup of index* q^m *in* $Q = \langle x \rangle$. *In fact* x^{q^m} *lies in the centre of* G.

Chapter 5 sees us focus our attention on groups with the basis property. As mentioned earlier we establish our own proofs for several results detailed by Jones in [7]. The main result of this chapter is the classification of groups with the basis property.

Theorem 5.3.2. *Let* G *be a finite group. Then* G *has the basis property if and only if either:*

(i) G *is a* p*-group, or*

(ii) $G = P \rtimes Q$ *where* P *is a* p*-group,* Q *a non-trivial cyclic* q*-group and every non-identity element of* Q *acts fixed-point freely on* P.

We conclude with Chapter 6 which provides an in depth summary of the work of the thesis. We also ask some open questions relating to property $\mathcal{B}$ and the basis property, and provide some guidance and motivation for studying these questions.

Chapter 2

Preliminary Results

In this chapter we provide background material for all the mathematics presented in this thesis. Whilst this thesis works within the field of group theory we use group rings and module theory to help prove many of our results. The first section states some standard group theory, mainly focusing on the Frattini subgroup and its properties. The second section highlights the standard definitions of a group ring which leads us into building up some of the fundamental ideas of module theory. Finally we conclude with proofs of Maschke's theorem, Clifford's theorem and the Krull–Schmidt theorem which form the cornerstone of the work we do in module theory.

It should be noted that throughout this thesis all groups are finite; thus when referring to a group we are specifically referring to a finite group.

2.1 Some Basic Group Theory

2.1.1 The Frattini Subgroup

The *Frattini subgroup*, denoted $\Phi(G)$, is most commonly defined as the intersection of all maximal subgroups. As we noted in the previous chapter, the Frattini subgroup also has the property that it is the set of all non-generators of the group, where an element x of a group G is a *non-generator* if for any set A containing x that generates G then $A \backslash \{x\}$ also generates G. We now prove this result.

Lemma 2.1.1 (Frattini). *If G is a group then $\Phi(G)$ is the set of non-generators of G.*

Proof. Assume that there exists $x \in \Phi(G)$ such that $G = \langle x, X\rangle$ but $G \neq \langle X\rangle$, i.e. x is not a non-generator. Now $x \notin \langle X\rangle$ so let M be a subgroup maximal such that $\langle X\rangle \leqslant M$ and $x \notin M$. Now if there exists a subgroup H such that $M < H \leqslant G$ then $x \in H$ and $H = G$ by the maximality of M. Thus M is maximal in G, but since $x \in \Phi(G)$ and the Frattini subgroup is contained in all maximal subgroups, x lies in M. Thus $G = \langle x, X\rangle \leqslant M$ is a contradiction and x is in fact a non-generator. Since x was arbitrary all elements of $\Phi(G)$ are non-generators.

Now suppose that x is a non-generator which does not lie in the Frattini subgroup. Then there exists a maximal subgroup M of G such that $x \notin M$ and so $M \neq \langle x, M\rangle$. However as M is maximal $G = \langle x, M\rangle$ and as x is a non-generator $G = M$ which is a contradiction. Thus $x \in M$ and so does in fact lie in the Frattini subgroup. □

One can quickly establish that the Frattini subgroup is characteristic.

As any automorphism maps a maximal subgroup to a maximal subgroup the intersection of all maximal subgroups will remain fixed under any automorphism — hence the Frattini subgroup is characteristic. We now provide a few more of the basic properties of the Frattini subgroup.

Lemma 2.1.2. *If G is a group, N a normal subgroup of G, and H a subgroup of G then:*

(i) if $N \leqslant \Phi(H)$ then $N \leqslant \Phi(G)$,

(ii) $\Phi(N) \leqslant \Phi(G)$,

(iii) $\Phi(G/N) \geqslant \Phi(G)N/N$ with equality if N is contained in $\Phi(G)$.

Proof. (i) If $N \nleqslant \Phi(G)$ then there exists a maximal subgroup M such that M does not contain N and so $G = MN$. Clearly $H = H \cap G = H \cap MN$ which is, by Dedekind's Modular Law, $(H \cap M)N$. Since N is contained in $\Phi(H)$ it is a set of non-generators of H and so $H = H \cap M$ and thus $H \leqslant M$. But N is a subgroup of H and so $N \leqslant M$ a contradiction.

(ii) This follows from part (i). Since $\Phi(N)$ is characteristic in N it is normal in G and clearly $\Phi(N) \leqslant \Phi(N)$. Thus by replacing N and H in part (i) by $\Phi(N)$ and N, here $\Phi(N) \leqslant \Phi(G)$.

(iii) Maximal subgroups of G/N have the form M/N where M is a maximal subgroup of G containing N by the Correspondence Theorem. Thus if J is the intersection of all maximal subgroups of G that contain N then $\Phi(G/N) = J/N$. Now J contains $\Phi(G)$, as $\Phi(G)$ is the intersection of all maximal subgroups of G, and J contains N so $J \geqslant \Phi(G)N$. Thus we can deduce that $\Phi(G/N) \geqslant \Phi(G)N/N$.

Now if $N \leqslant \Phi(G)$ then N is contained in all maximal subgroups M of G. So $J = \Phi(G)$ and the result follows. □

2.1.2 Other Group Theory Results

Here we list a number of results that hold for groups. We begin by describing a result known as the Frattini argument. It describes the relationship between normal subgroups and their Sylow subgroups in the original group.

Lemma 2.1.3. *If H is a normal subgroup of a finite group G and P a Sylow p-subgroup of H then $G = N_G(P)H$.*

Proof. Let $g \in G$ then $P^g \leqslant H$ and P^g is a Sylow p-subgroup of H. Thus $P^g = P^h$ for some $h \in H$ by Sylow's Theorem. Therefore gh^{-1} is contained in the normaliser $N_G(P)$ and so g is contained in $N_G(P)H$. Hence $G \leqslant N_G(P)H$ and thus $G = N_G(P)H$. □

Throughout this thesis we work a great deal with elements of prime-power order and how elements of co-prime order interact. To that end we provide a result that shows how automorphisms of q-power order affect p-groups ([3, 5.3.5]).

Theorem 2.1.4. *Let p and q be distinct primes. If A is a q-group of automorphisms of the p-group P, then $P = CH$, where $C = C_P(A)$ and $H = [P, A]$. In particular, if $H \leqslant \Phi(P)$ then $A = 1$.*

To prove this we use the following results from Gorenstein's book [3]. We omit the proofs as they are not used elsewhere in this thesis ([3, 5.2.3], [3, 5.3.2] and [3, 2.6.4]). It can be noted here that Lemma 2.1.7 is a particularly well known result.

Lemma 2.1.5. *Let p and q be distinct primes and let A be a q-group of automorphisms of the abelian p-group P. Then we have*

$$P = C_P\left(A\right) \times \left[P, A\right].$$

Lemma 2.1.6. *Let p and q be distinct primes and let A be a q-group of automorphisms of the p-group P that stabilises some normal series of P. Then $A = 1$.*

Here a group of automorphisms A of a group G *stabilises* a normal series, $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$, if every automorphism of A fixes every normal subgroup G_i and the induced action on the factors G_i/G_{i+1} is trivial.

Lemma 2.1.7. *If K is a non-trivial normal subgroup of the p-group G, then $K \cap Z(G) \neq 1$.*

Proof of Theorem 2.1.4. The proof of this theorem can be split into two cases. First assume that H lies in $Z(P)$, the centre of P. Now let ϕ be an element of A and define α_ϕ to be the mapping from P to its subgroup H that takes an element x and sends it to $x^{-1}\left(x\phi\right)$. Now if $x, y \in P$ then

$$\left(xy\right)\alpha_\phi = \left(xy\right)^{-1}\left(xy\right)\phi = y^{-1}x^{-1}\left(x\phi\right)\left(y\phi\right),$$

as ϕ is an automorphism and

$$y^{-1}x^{-1}\left(x\phi\right)\left(y\phi\right) = x^{-1}\left(x\phi\right)y^{-1}\left(y\phi\right).$$

as $x^{-1}\left(x\phi\right)$ is an element of $H \leqslant Z(P)$. So $\left(xy\right)\alpha_\phi = \left(x\right)\alpha_\phi\left(y\right)\alpha_\phi$ and thus α_ϕ is a homomorphism. As α_ϕ maps P into itself it is in fact an endomorphism for each $\phi \in A$. The kernel of α_ϕ will be the set of all elements $x \in P$ such that $x\phi = x$ which is simply the centraliser of ϕ in

P. One can also see by definition the image of α_ϕ is a subgroup of H. Since $H \leqslant Z(P)$ the image of P under α_ϕ is contained in an abelian group, thus the derived subgroup $P' = [P, P]$ is contained in the kernel of α_ϕ. Now $\ker \alpha_\phi = \left\{x \in P \mid x^{-1}(x\phi) = 1\right\} = \{x \in P \mid x\phi = x\} = C_P(\phi)$ and so $P' \leqslant C_P(\phi)$ for all elements $\phi \in A$. Thus P' lies in $C = C_P(A)$.

Now let $\bar{P} = P/P'$, $\bar{C} = C_{\bar{P}}(A)$ and $\bar{H} = \left[\bar{P}, A\right]$. By definition $\bar{P}$ is abelian and so by Lemma 2.1.5 $\bar{P} = \bar{C} \times \bar{H}$. Now $\bar{H}$ is the image of H in $\bar{P}$ and so $P = C_1H$ where C_1 is the pre-image of $\bar{C}$ in P. However A acts trivially on P' and $\bar{C}$, and so A stabilises this series $C_1 \trianglerighteq P' \trianglerighteq 1$. Hence by Lemma 2.1.6 we have thet A acts trivially on C_1. Thus $C_1 \leqslant C$ and $P = CH$.

Now we assume that $H \nleqslant Z(P)$ and certainly $H \neq 1$. For $x, y \in P$ and $\phi \in A$ then

$$\begin{aligned}
[xy, \phi]\,[y, \phi]^{-1} &= (xy)^{-1}(xy)\phi\left(y^{-1}(y\phi)\right)^{-1}, \\
&= y^{-1}x^{-1}(x\phi)(y\phi)(y\phi)^{-1}y, \\
&= y^{-1}x^{-1}(x\phi)y, \\
&= [x, \phi]^y .
\end{aligned}$$

So $[x, \phi]^y$ is equal to $[xy, \phi]\,[y, \phi]^{-1}$ which is in $[P, A] = H$. Hence H is normal in P. Thus by Lemma 2.1.7 $K = H \cap Z(P)$ is non-trivial. Certainly $Z(P)$ is A-invariant since it is characteristic and so we can also see that for

$\phi, \psi \in A$ and $x \in P$

$$\begin{aligned}
[x, \phi]^{-1} [x, \phi\psi] &= \left(x^{-1}(x\phi)\right)^{-1} \left(x^{-1}(x\phi)\psi\right), \\
&= \left((x\phi)^{-1}x\right) \left(x^{-1}(x\phi)\psi\right), \\
&= (x\phi)^{-1}(x\phi)\psi, \\
&= [x, \phi]^{\psi}.
\end{aligned}$$

Thus $[x, \phi]^{\psi} = [x, \phi]^{-1} [x, \phi\psi] \in [P, A] = H$ so H is A-invariant. Therefore K is also A-invariant. Now define D to be the subgroup of P generated by all $x \in P$ such that $[x, A] \leqslant K$. Clearly C is contained in D. Again we pass to a quotient so let $\bar{P} = P/K$ and let $\bar{C} = C_{\bar{P}}(A)$ and $\bar{H} = \left[\bar{P}, A\right]$, similarly to before. If $x \in P$ and $[x, A]$ is in K then A centralises the image of x in $\bar{P}$. It follows therefore from the definition of D that the image of D in $\bar{P}$ is contained in $\bar{C}$. Conversely if $\bar{x}$ is an element of $\bar{C}$ then $[\bar{x}, A]$ is the identity in $\bar{P}$ and so $[x, A]$ lies in K where x is any pre-image of $\bar{x}$ in P. Thus $x \in D$ and so the image of D in $\bar{P}$ is $\bar{C}$. We also note that as before $\bar{H}$ is the image of H in $\bar{P}$.

Since K is non-trivial the order of $\bar{P}$ is strictly less than the order of P. We now proceed by induction and assume the result holds for groups of order less than P (our base case $|P| = 2$ obviously holds). By induction on the order of P we have $\bar{P} = \bar{C}\bar{H}$, and from above this implies that $P = DH$. If $[x, A]$ lies in K for every choice of $x \in P$, then $H = [P, A] \leqslant K \leqslant Z(P)$ which contradicts the assumption. So $D < P$ and D is invariant under A as both K and $\bar{C}$ are. Now recall that $C \leqslant D$ and hence by induction $D = C\,[D, A]$. Now $P = DH = C\,[D, A]\,H = CH$ since as $D < P$ then $[D, A] \leqslant K \leqslant H$.

Finally if H is a subgroup of the Frattini subgroup of P then $P = C\Phi(P)$. However, as observed previously, $\Phi(P)$ is the set of non-generators which implies that $P = C = C_P(A)$. Thus A is trivial. □

As a corollary of this theorem we have a result by Philip Hall found in Robinson [8, 5.3.3].

Corollary 2.1.8 (Hall)**.** *Let G be a group of order p^m and let $|G : \Phi(G)| = p^r$. Then the order of $C_{\mathrm{Aut}(G)}(G/\Phi(G))$ divides $p^{(m-r)r}$ and the order of $\mathrm{Aut}(G)$ divides $np^{(m-r)r}$ where $n = |GL(r,p)|$.*

Proof. Take a prime q with $q \neq p$ that divides the order of the centraliser. Let A be the Sylow q-subgroup of the centraliser and so by definition $[G, A] \leqslant \Phi(G)$. Theorem 2.1.4 says that A is trivial and thus the results follows. □

2.2 Module Theory, Group Rings and Group Algebras

2.2.1 Modules, Representations and Group Rings

The idea of a module over a ring is that of a generalised vector space, where instead of taking the scalars to be from a field we take them from a ring. Modules also generalise abelian groups as abelian groups can be viewed as modules over $\mathbb{Z}$. Hence, like a vector space, a module is an additive abelian group with multiplication between scalars from the ring and elements in the module distributive. We define this formally below:

Definition 2.2.1. *If R is a ring then a right R-module is an abelian group M together with an operation $M \times R \to M$ (usually denoted as xr for $r \in R$*

and $x \in M$) such that given $r, s \in R$ and $x, y \in M$ the following hold:

- $(x + y)r = xr + yr$,
- $x(r + s) = xr + xs$,
- $x(rs) = (xr)s$,
- $x1_R = x$ *if R has an identity element.*

Similarly one can define a left R-module, and if R is a commutative ring then left R-modules become right R-modules by defining $xr := rx$. In this case we refer to the object as an R-module. An additive subgroup N of M is an R-submodule of M such that if x is any element of N and $r \in R$ then xr also lies in N. We can also see that if F is a field then an F-module is in fact a vector space over the field F.

Vector spaces and modules are important in representation theory. If G is a group, F a field and V a vector space over F then a homomorphism ρ which maps from G to the general linear group $GL(V)$ is a *linear representation* of G over F, often also called an F-representation. Throughout this thesis we use vector spaces of finite dimension, n, where n is also known as the *degree* of the representation. It is also worth defining that if $\ker \rho$ is trivial then the representation is said to be *faithful*.

Group rings and group algebras are the basic structures that allow us to look at module representations of groups. If G is a group and R any ring with an identity then the group ring, typically written RG, is defined to be the set of all sums $\sum_{g \in G} r_g g$ where r_g is an element of R. The group ring then has the following rules of addition and multiplication:

$$\left(\sum_{g\in G} r_g g\right) + \left(\sum_{g\in G} s_g g\right) = \sum_{g\in G} \left(r_g + s_g\right) g,$$

and

$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} s_g g\right) = \sum_{g\in G}\left(\sum_{hk=g} r_h s_k\right) g.$$

One can see that under these operations RG is a ring with an identity element $1_R 1_G$, often written simply as 1. One can also see that RG contains a copy of R (by making $r_g = 0$ for all non-identity elements in G) as a subring and a copy of G within its set of invertible elements (where $r_g = 1_R$ and $r_h = 0$ for all $g, h \in G$ with $g \neq h$).

If F is a field then the group ring FG is not only a ring but also has the natural vector space structure:

$$f\left(\sum_{g\in G} f_g g\right) = \sum_{g\in G} f f_g g,$$

where f is an element of the field. This comes from the definition of group ring multiplication with $r_1 = f$ and all other $r_g = 0$. This FG is known as the *group algebra* of G over F. In fact the group algebra FG is a module over itself where submodules correspond to right ideals. The dimension of the group algebra FG as a vector space is simply the size of the group G, as the elements of G form a basis. Often the field taken for the group algebra is the real or complex numbers in the research field known as ordinary representation theory. However throughout this thesis our field will be finite, since our module representations correspond to conjugation of elementary abelian subgroups.

Now suppose that $\rho : G \to GL(M)$ is an F-representation of G with degree n. Then M can be viewed as a right FG-module via:

$$x\left(\sum_{g\in G} f_g g\right) = \sum_{g\in G} f_g\left(xg^{\rho}\right),$$

where x is an element of M, and g^{ρ} is the action of ρ on the element g. One can see this satisfies the module axioms. In fact one can show that the class of F-representations of G with degree n and the class of n-dimensional right FG-modules are in one-to-one correspondence — thus we call two representations *equivalent* if they arise from two isomorphic modules. Since all groups are finite the group algebra FG is finite dimensional and all finitely generated FG-modules are finite dimensional.

2.2.2 Completely Reducible Modules

Let M be an FG-module where F is a finite field. If M contains a proper non-zero submodule then M is said to be *reducible*. However if M contains no such submodule then it is an *irreducible*, or *simple*, module. One can obtain irreducible FG-modules from the group algebra as shown below.

Lemma 2.2.2. *An irreducible FG-module is isomorphic (as a module) with some quotient FG/I where I is a maximal right ideal of FG.*

Proof. Let M be an irreducible FG-module and choose a non-zero element $x \in M$. If r is an element of the group algebra then $\phi : r \mapsto xr$ is a homomorphism of modules. Now ϕ has non-zero image since x is a non-zero element, and since M is irreducible the image of ϕ must in fact be M. So by the first isomorphism theorem M is isomorphic to the quotient FG/I where $I = \ker\phi$. Since M is irreducible I must be a maximal right ideal by the Correspondence Theorem. □

If M and N are FG-modules the *external direct sum* is

$$M \oplus N = \{\, (m, n) \mid m \in M, n \in N \,\},$$

with operations

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)\,,$$

and

$$(m, n)\, r = (mr, nr)\,,$$

with $r \in FG$. If V is any FG-module possessing two submodules M and N such that $V = M + N$ and $M \cap N = 0$, then $V \cong M \oplus N$ (defined as above). We call this situation the *internal direct sum* and note that due to this isomorphism we view internal and external direct products the same. A module that can be written in a non-trivial way as a direct sum is known as *decomposible*, otherwise it is known as *indecomposible*. Note that $M \cong M \oplus 0$ always holds so this is not included as a valid decomposition. If M is a direct sum of irreducible submodules then M is said to be *completely reducible*. The condition we frequently use for complete reducibility is Maschke's theorem [8, 8.1.2].

Theorem 2.2.3 (Maschke)**.** *If G is a finite group and F a finite field of characteristic co-prime to the order of G, then every FG-module is completely reducible.*

To prove Maschke's Theorem we use the following lemma.

Lemma 2.2.4. *Let F be a finite field and M an FG-module. Then the following are equivalent:*

(i) M is a sum of irreducible submodules,

(ii) M is a direct sum of irreducible submodules,

(iii) for all submodules N there is a complement P such that $M = N \oplus P$.

Proof. $(ii) \Rightarrow (i)$ This is trivial as a direct sum of irreducible submodules is clearly a sum of irreducible submodules.

$(i) \Rightarrow (ii)$ Suppose that $M = \sum_{i \in I} N_i$ as a sum of irreducible submodules. Now choose $J \subseteq I$ to be maximal such that $L = \sum_{j \in J} N_j$ is the direct sum $\bigoplus_{j \in J} N_j$. Assume that L is not equal to M. Thus there exists an N_i such that $N_i \nsubseteq L$. Now $N_i \cap L$ is not equal to N_i by definition and so $N_i \cap L = 0$ as N_i is an irreducible submodule. However this implies that $N_i + L = N_i \oplus L$, which contradicts the maximality of J. Thus M must be L and so M is a direct sum of irreducibles.

$(iii) \Rightarrow (ii)$ Assume that (iii) holds. Now take N to be a direct sum of irreducible submodules of M of largest dimension. We now claim that $N = M$. If $N \neq M$ then $M = N \oplus P$, for some complement P, by our assumption. Let V be an irreducible submodule of P so $N + V = N \oplus V$ as V is a submodule of the complement of N. But $N \oplus V$ is a direct sum of irreducible submodules of larger dimension, contradicting our choice of N. Thus $M = N$ and is a direct sum of irreducible submodules.

$(ii) \Rightarrow (iii)$ Let $M = \bigoplus_{i \in I} N_i$ be a direct sum of irreducible of submodules and let N be a submodule of M. Now choose $J \subseteq I$ to be maximal such that $N \cap \bigoplus_{i \in J} N_i = 0$. Thus we can then form the direct sum $L = \bigoplus_{i \in J} N_i \oplus N$. If $N_j \nleq L$ then $N_j \cap L = 0$ as N_j is irreducible. Thus $N_j + L = N_j \oplus L = N_j \oplus \left(\bigoplus_{i \in J} N_i\right) \oplus N$ which is $\bigoplus_{i \in J \cup \{j\}} N_i \oplus N$. This implies $\bigoplus_{i\in J\cup\{j\}} N_i \cap N$ is zero contradicting the maximality of J. Hence $L = M$ and for any submodule N of M there exists $P = \bigoplus_{i\in J} N_i$, such that $N \cap P = 0$ and P is a complement such that $M = N \oplus P$. □

Proof of Maschke's Theorem. Let M be an FG-module of finite dimension. To show that M is completely reducible we need only that show any submodule N is a direct summand of M by Lemma 2.2.4.

Viewing M as a vector space we can write $M = N \oplus L$, where L is a subspace of M. Define π to be the projection from M to N which is a linear map. To construct an FG-homomorphism we use an averaging process. Define π_1 to be the mapping from M to M such that for $m \in M$ and $g \in G$

$$m\pi_1 = \frac{1}{|G|}\sum_{g\in G}(mg)\,\pi g^{-1}.$$

This exists since G is a finite group of order not divisible by the characteristic of F, and as π is a linear mapping so is π_1. In fact π_1 is an FG-homomorphism as it is compatible with the multiplication of G since for any given $m \in M$

$$\begin{aligned}(mx)\,\pi_1 x^{-1} &= \frac{1}{|G|}\sum_{g\in G}(mxg)\,\pi g^{-1}\cdot x^{-1},\\ &= \frac{1}{|G|}\sum_{y\in G}(my)\,\pi y^{-1}, \text{ (after substituting } y = xg)\\ &= m\pi_1,\end{aligned}$$

and thus $(mx)\pi_1 = m\pi_1 x$. Since the image of π is N and N is a submodule of M the image of π_1 is a submodule of N. However given any elements $n \in N$ and $g \in G$ then $(ng)\,\pi = ng$ and so

$$n\pi_1 = \frac{1}{|G|}\sum_{g\in G}(ng)\,\pi g^{-1} = \frac{1}{|G|}\sum_{g\in G}ngg^{-1} = \frac{1}{|G|}\sum_{g\in G}n = n,$$

which is why we need the averaging process. Thus N is a submodule of the image of π_1 and so $\operatorname{im}\pi_1 = N$. Now since any element of N under π_1 maps to itself π_1 is a projection map from M into N. If $x \in N \cap \ker\pi_1$ then $x\pi_1 = 0$ which implies $x = 0$ and hence $N \cap \ker\pi_1 = 0$. If m is any element of M then $m = m\pi_1 + (m - m\pi_1)$ with $m\pi_1 \in \operatorname{im}\pi_1 = N$. Now $(m - m\pi_1)\,\pi_1 = m\pi_1 - m\pi_1 = 0$ as π_1 is an idempotent. Thus $m - m\pi_1$ is contained in the kernel of π_1 and so $M = \operatorname{im}\pi_1 + \ker\pi_1$. Therefore $M = N \oplus \ker\pi_1$. □

Maschke's Theorem requires the characteristic of the field to be co-prime to the order of the group G. This actually includes the case where the characteristic is zero, however we will not use such fields in this thesis.

The next result on module theory we use is the Krull–Schmidt Theorem. The Krull–Schmidt Theorem holds for a variety of algebraic structures but we apply it to modules. Note we only give a special case of the theorem.

Theorem 2.2.5 (Krull–Schmidt)**.** *Let F be a finite field and M an FG-module. If $M_1 \oplus \cdots \oplus M_n$ and $N_1 \oplus \cdots \oplus N_m$ are two decompositions of M into irreducible submodules, then $n = m$.*

For the proof of this theorem we use the Jordan–Hölder Theorem. The Jordan–Hölder Theorem tells us that if $M = M_1 \supset M_2 \supset \cdots \supset M_n = 0$ and $M = N_1 \supset N_2 \supset \cdots \supset N_m = 0$ are two composition series not only are they of equal length but there exists a bijection that shows the factors are isomorphic. We only show that given two chains of submodules, they are of equal length.

Theorem 2.2.6 (Jordan–Hölder)**.** *Let F be a finite field and M be an FG-*

module and let $M = M_1 \supset M_2 \supset \cdots \supset M_n = 0$ and $M = N_1 \supset N_2 \supset \cdots \supset N_m = 0$ be two composition series. Then both series are of the same length.

Proof. Let $M = M_1 \supset M_2 \supset \cdots \supset M_n = 0$ and $M = N_1 \supset N_2 \supset \cdots \supset N_m = 0$ be two composition series. We proceed by induction on n. If $n = 1$ then M is an irreducible module and so the result follows. So assume that $n > 1$ and the theorem holds for values less than n. If $M_2 = N_2$ then by induction the theorem holds and we conclude $m = n$. So assume that $M_2 \neq N_2$ and so $M_2 + N_2 = M$. Thus the quotients $M/M_2 \cong N_2/\left(M_2 \cap N_2\right)$ and $M/N_2 \cong N_2/\left(M_2 \cap N_2\right)$ are simple. Now if we take a composition series for $M_2 \cap N_2$ we see by induction this must have composition length $n - 2$. However this means that N_2 has a descending chain of length $n - 1$, but by induction the theorem holds for N_2 and so all chains have length $n - 1$. Therefore $n = m$. □

Proof of Krull–Schmidt Theorem. Let $M_1 \oplus \cdots \oplus M_n$ and $N_1 \oplus \cdots \oplus N_m$ be two decompositions of M as a direct sum of irreducible submodules. Certainly $0 \subset M_1 \subset M_1 \oplus M_2 \subset \cdots \subset M$ and $0 \subset N_1 \subset N_1 \oplus N_2 \subset \cdots \subset M$ are two composition series, whose factors are $M_1, \ldots, M_n$ and $N_1, \ldots N_m$ precisely. The result then follows from the Jordan–Hölder Theorem. □

The final condition for complete reducibility that we use in this thesis is Clifford's Theorem [8, 8.1.3]. We do not use this as often as Maschke's Theorem however, unlike Maschke's Theorem, it makes no restrictions on the field or the group.

Theorem 2.2.7 (Clifford)**.** *Let G be any group, F any finite field, M an irreducible FG-module, and H a normal subgroup of G. Then:*

(i) if S is an irreducible FH-submodule of M, then M is the sum of Sg for all $g \in G$ and each Sg is an irreducible FH-module. Thus M is completely reducible as an FH-module,

(ii) if $S_1, \ldots, S_k$ are representatives of the isomorphism types of irreducible FH-submodules of M and M_i is the sum of all FH-submodules of M isomorphic to S_i, then $M = M_1 \oplus \cdots \oplus M_k$ and M_i is a direct sum of FH-modules isomorphic with S_i,

(iii) G permutes the M_i transitively by means of the right action on M.

Proof. (i) Let S be an irreducible FH-module of M and consider $L = \sum_{g \in G} Sg$. Given $x \in G$

$$Lx = \left(\sum_{g \in G} Sg \right) x = \sum_{g \in G} Sgx = \sum_{y \in G} Sy = L,$$

and so L is an FG-submodule of M. However as M is irreducible $L = M$ and so $M = \sum_{g \in G} Sg$. Now take, for all $h \in H$, $Sgh = Sghg^{-1}g$ which is contained in Sg as $ghg^{-1} \in H$. Thus Sg is an FH-submodule of M. If $T \leqslant Sg$ as an FH-submodule then $Tg^{-1} \leqslant S$ which implies that Tg^{-1} is also an FH-submodule of S. Note here this is using the same observation that as S is an FH-submodule so is Sg and applying it to T and Tg^{-1}. Therefore as S is irreducible then $Tg^{-1} = 0$ or S and therefore $T = 0$ or Sg and thus Sg is an irreducible FH-submodule. Hence M is a sum of irreducible FH-submodules and Lemma 2.2.4 tells us that M is completely reducible.

(ii) Pick $S_1, \ldots, S_k$ to be representatives for each of the isomorphism types of irreducible FH-submodules of M, i.e. if $S \leqslant M$ is an irreducible

FH-submodule then S is isomorphic to S_i and $S_i \ncong S_j$, for $i \neq j$, as FH-modules. It should be noted that we can do this as any irreducible FH-module occurs as a quotient of FH (by Lemma 2.2.2), and hence (as H is finite dimensional) as a composition factor. The complete Jordan–Hölder Theorem tells us that there is only a finite collection of irreducible FH-modules.

Now let M_i be the sum of all FH-submodules S of M such that $S \cong S_i$. By part (i) M is the sum of all irreducible FH-submodules of M and so $M = M_1 + \cdots + M_k$. Lemma 2.2.4 gives us that M_i is a direct sum of some FH-submodules isomorphic to S_i.

Claim: $M_1 + \cdots + M_j = M_1 \oplus \cdots \oplus M_j$ for all j.

Proceeding by induction our base case of $j = 1$ holds trivially, so assume the claim holds for $j-1$. Now suppose $M_j \cap (M_1 \oplus \cdots \oplus M_{j-1})$ is non-zero. So $M_j \cap (M_1 \oplus \cdots \oplus M_{j-1})$ is an FH-submodule and choose $N \leqslant M_j \cap (M_1 \oplus \cdots \oplus M_{j-1})$ to be an irreducible FH-submodule. Now $N \leqslant M_j$, which is the direct sum of submodules isomorphic to S_j, and all composition factors of M_j are isomorphic to S_j as FH-modules. The Jordan–Hölder Theorem tells us that N must be isomorphic to S_j. As N is contained in $M_1 \oplus \cdots \oplus M_{j-1}$, which is the direct sum of copies of $S_1, \ldots, S_{j-1}$, N is isomorphic as FH-modules to some S_i for $i \in \{1, \ldots, j-1\}$. This is a contradiction and so the intersection $M_j \cap (M_1 \oplus \cdots \oplus M_{j-1})$ must in fact be zero. Thus by induction $M_1 + \cdots + M_j = M_1 \oplus \cdots \oplus M_j$ for all j.

As a result of this claim $M = M_1 \oplus \cdots \oplus M_k$.

(iii) Suppose S is an irreducible FH-submodule of M. Since Sg is irreducible as an FH-module from part (i), so Sg is isomorphic to S_j for some j. If $S \cong T \leqslant M_i$ as FH-modules then let ϕ be the isomorphism from S to T. Now define θ to be the mapping from Sg to Tg by $(sg)\theta = (s\phi)g$ for $s \in S$. Clearly θ is a bijection so it remains to show that it is a homomorphism of FH-modules. So for $g \in G$, $h \in H$ and $s \in S$

$$\begin{aligned}
(sg \cdot h)\,\theta &= \left(sghg^{-1}g\right)\theta, \\
&= \left(sghg^{-1}\right)\phi \cdot g \text{ (by definition)} \\
&= (s\phi)\left(ghg^{-1}g\right) = (s\phi)\,(gh) \text{ (as } \phi \text{ is an homomorphism)} \\
&= (sg)\,\theta \cdot h.
\end{aligned}$$

Hence $Sg \cong S_j$ for all irreducible $S \leqslant M_i$ and thus $Sg \leqslant M_j$ for all irreducible $S \leqslant M_i$. Therefore $M_ig \leqslant M_j$. However $S_ig \cong S_j$ and so $S_i \cong S_jg^{-1}$. Thus, by the same argument, $M_jg^{-1} \leqslant M_i$ and hence $M_j \leqslant M_ig$. This implies that $M_ig = M_j$ and so G permutes the M_i.

Now if $\{M_{i_1}, \ldots, M_{i_l}\}$ is an orbit then $N = M_{i_1} + \cdots + M_{i_l}$ is an FG-submodule. Thus $N = M$, as M is irreducible, and G in fact permutes the M_i transitively. □

Chapter 3

Theoretical Observations

In this chapter we establish several results for groups with property $\mathcal{B}$. We seek to explain how having property $\mathcal{B}$ affects the structure of a group. It is not clear from the definition that property $\mathcal{B}$ is inherited by quotients or subgroups, and in this chapter we establish the cases in which property $\mathcal{B}$ can be inherited. We begin by showing some basic properties of groups with the property $\mathcal{B}$ and provide examples of groups with and without property $\mathcal{B}$. Later we show that in general subgroups do not inherit property $\mathcal{B}$ from their parent groups and provide an example to highlight this. We do however show that in certain cases property $\mathcal{B}$ transfers to quotients of groups with property $\mathcal{B}$.

In the final section we seek to investigate how property $\mathcal{B}$ affects the structure of a group. In particular we show that if a group G has property $\mathcal{B}$, and can be expressed as a direct product, then G is a p-group.

3.1 Property $\mathcal{B}$: The Basics

As established in the Introduction a group G with property $\mathcal{B}$ is defined to be a group where every minimal generating set has size $d(G)$, where $d(G)$ is the smallest number of elements required to generate G. Equivalently a group with property $\mathcal{B}$ is a group where each generating set of G contains a minimal generating set of size $d(G)$ as a subset. We begin by highlighting a result that will be key to our investigations into the structure of groups with property $\mathcal{B}$.

Lemma 3.1.1. *A group G has property $\mathcal{B}$ if and only if $G/\Phi(G)$ has property $\mathcal{B}$.*

Proof. Let $\pi : G \to G/\Phi(G)$ be the natural map and let $X = \{a_1, a_2, \ldots, a_k\}$ be a set of elements in G. Note this set generates G if and only if $G/\Phi(G)$ is generated by $Y = \{\Phi(G)\, a_1, \ldots, \Phi(G)\, a_k\}$. Indeed this is obvious in one direction, from π, since if X generates G then the set of all $\Phi(G)\, a_i$, for all $i \in \{1, \ldots, k\}$, will generate $G/\Phi(G)$. Now if $G/\Phi(G)$ is generated by Y then G would be generated by $\{a_1, \ldots, a_k\} \cup \Phi(G)$. Since the Frattini subgroup is the set of non-generators we have that $G = \langle a_1, \ldots, a_k\rangle = \langle X\rangle$.

Now if G has property $\mathcal{B}$ given a generating set Y for $G/\Phi(G)$ we can pass this to a generating set X for G as above. We can reduce this to a minimal generating set X' for G of size $d(G)$ since G has property $\mathcal{B}$. Using π again we can now pass this minimal generating set to Y', its image in $G/\Phi(G)$. Note that $Y' \leqslant Y$. From above the set Y' would be of size $d(G)$ and is a minimal generating set of $G/\Phi(G)$. Otherwise $G/\Phi(G)$ could be generated by a subset of Y' and so G would be generated by the pre-image of this subset under π, which would be of size less than $d(G)$, a contradiction. Hence $d\left(G/\Phi\left(G\right)\right) = d(G)$. Now if there exists a minimal generating set Z of $G/\Phi\left(G\right)$ of size not equal to $d(G)$ then its pre-image under π, Z' say, would generate G. Then Z' would be a minimal generating set for G as Z is a minimal generating set for $G/\Phi\left(G\right)$. This contradicts G having property $\mathcal{B}$ and so Z must be of size $d(G)$.

A similar argument proves the converse. □

From the Introduction we know that all p-groups have property $\mathcal{B}$ (Burnside Basis Theorem 1.1.1). Despite this groups with property $\mathcal{B}$ are not common. For example, cyclic groups of non-prime-power order do not have property $\mathcal{B}$. To prove this we first show a well known result of cyclic groups.

Lemma 3.1.2. *If m and n are co-prime then $C_{mn} \cong C_m \times C_n$.*

Proof. If $G = C_{mn} = \langle x \rangle$ then the order of x is mn. Now let A be the group generated by x^m and B the group generated by x^n. Then clearly $|G : A|= m$ and $|G : B|= n$ and hence $G/A = \langle Ax \rangle \cong C_m$ and $G/B = \langle Bx \rangle \cong C_n$. Since $n = |A|$ and $m = |B|$ are co-prime then the intersection $A \cap B$ is trivial. Now $G/\left(A \cap B\right)$ is isomorphic to a subgroup of $G/A \times G/B$ (by the mapping $g \mapsto (Ag, Bg)$) but since $G/\left(A \cap B\right)$ and $G/A \times G/B$ are both of order mn they are in fact isomorphic. Thus

$$C_{mn} \cong \frac{G}{A \cap B} \cong \frac{G}{A} \times \frac{G}{B} \cong C_m \times C_n.$$

□

Proposition 3.1.3. *If G is a cyclic group of non-prime-power order n, then G does not have property $\mathcal{B}$.*

Proof. Let $G = \langle x \rangle$ be as hypothesised. Since G is cyclic $d(G) = 1$. Now as G has order n, which can be written as a product of prime-powers $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$. From the well established result $C_{mn} \cong C_m \times C_n$ (Lemma 3.1.2) we can establish that $G \cong C_{p_1^{i_1}} \times C_{p_2^{i_2}} \times \cdots \times C_{p_k^{i_k}}$ with each direct factor generated by x_i say. Hence $\{x_1, x_2, \ldots, x_k\}$ is a minimal generating set for G of size $k > 1$ since omitting any of the x_i would mean that the factor $\langle x_i \rangle$ would not be generated. Thus the result holds. □

The smallest non-p-group with property $\mathcal{B}$ is the symmetric group on three points.

Example 3.1.4. *The symmetric group on three points S_3 has property $\mathcal{B}$ with $d(G) = 2$.*

As a permutation group the elements of the symmetric group on three points S_3 are $\{(1), (12), (13), (23), (123), (132)\}$. Now as S_3 is not cyclic $d(S_3) \neq 1$ and since $\{(12), (23)\}$ generates S_3 minimally $d(S_3) = 2$. It remains to show that any generating set of S_3 contains a subset of size two that generates S_3.

If a set X generates S_3 it can't consist only of even permutations, otherwise it would generate A_3 not S_3. So it must contain at least one odd permutation. Choose τ to be that odd permutation and σ to be a permutation not found in $\langle \tau \rangle$ then the two element subset $\{\sigma, \tau\}$ of X contains either two odd permutations or an even permutation and an odd permutation. If σ is even and τ is odd then $\langle \sigma, \tau \rangle = S_3$ as $\langle \sigma \rangle = A_3 \cong C_3$. If σ and τ are both odd then $\langle \sigma, \tau \rangle \geqslant \langle \sigma\tau^{-1}, \tau \rangle = S_3$ as $\sigma\tau^{-1}$ is even and so $\langle \sigma\tau^{-1}, \tau \rangle$ is as in the first case. Hence S_3 has property $\mathcal{B}$. However this is the only symmetric group with property $\mathcal{B}$.

Proposition 3.1.5. *The symmetric group S_n does not have property $\mathcal{B}$ for $n > 3$.*

Proof. The symmetric group can be generated by the set of transpositions $\{(12), (23), (34), \ldots, ((n-1)n)\}$. We can see this is minimal since obviously none of the individual transpositions can be generated by a combination of any of the other transpositions. In fact if we omit one of these transpositions, $\{(i\ (i+1))\}$ say, then the set of remaining transpositions $\{(12), \ldots, ((i-1)i), ((i+1)(i+2)), \ldots, ((n-1)n)\}$ generates $S_i \times S_{n-i}$ with S_i being the symmetric group on the points $\{1, \ldots, i\}$ and S_{n-i} the symmetric group on the points $\{i+1, \ldots, n\}$. The set of transpositions is of size greater than $d(S_n) = 2$ and so the symmetric group does not have property $\mathcal{B}$. □

It is well known that S_3 is isomorphic to the dihedral group of order six. Unlike the symmetric group case however, there is a class of dihedral groups that have property $\mathcal{B}$.

Proposition 3.1.6. *If G is the dihedral group D_p of order $2p$, where p is a prime number, then G has property $\mathcal{B}$.*

Proof. We know that $d(G) = 2$ and $G = \langle a, b \mid a^p = b^2 = 1, bab^{-1} = a^{-1} \rangle$. Take a generating set A for G. Since $A \nsubseteq \langle a \rangle$ then A consists of elements of the form a^i for some $i \in \{1, \ldots p-1\}$ and $a^j b$ for some $j \in \{1, \ldots p\}$ or just of elements of the form $a^j b$. Since p is prime a^i is of order p and elements of the form $a^j b$ are of order two. In the first case all we need to do is take a subset consisting of one of the powers of a and an element of the form $a^j b$

to generate D_p. If the generating set just consists of elements of the form $a^j b$ then all we need to do is take two elements of this form and we generate D_p since $a^{j_1} b a^{j_2} b = a^k$ as $bab^{-1} = bab = a^{-1}$. Hence G has property $\mathcal{B}$. □

Corollary 3.1.7. *The dihedral group D_{p^n} of order $2p^n$, where p is a prime number, has property $\mathcal{B}$.*

Proof. Now $D_{p^n} = \langle a, b \mid a^{p^n} = b^2 = 1, bab^{-1} = a^{-1} \rangle$ and the Frattini subgroup of D_{p^n} is the intersection all the maximal subgroups of D_{p^n}. Certainly $\langle a \rangle$ has index two in D_{p^n} and so is maximal. Now $\langle a^p \rangle$ is the unique subgroup of $\langle a \rangle$ of order p^{n-1}, so is characteristic in $\langle a \rangle$. Hence $\langle a^p \rangle \trianglelefteq D_{p^n}$, so $\langle a^p, b \rangle = \langle a^p \rangle \langle b \rangle$ is a subgroup of D_{p^n}. This has index p in D_{p^n} and so is maximal. The same argument shows that subgroups of the form $\langle a^p, a^i b \rangle$ are also maximal.

Conversely if M is a maximal subgroup of D_{p^n} and $M \neq \langle a \rangle$ then $M \cap \langle a \rangle < \langle a \rangle$. So $M \cap \langle a \rangle$ is contained in $\langle a^p \rangle$. Thus

$$M = (M \cap \langle a \rangle) \langle a^i b \rangle \leqslant \langle a^p \rangle \langle a^i b \rangle = \langle a^p, a^i b \rangle.$$

The intersection of these maximal subgroups is clearly cyclic and since $\langle a^p \rangle$ is contained in $\langle a \rangle$ the Frattini subgroup of D_{p^n} is $\langle a^p \rangle$. Thus

$$D_{p^n} / \Phi(D_{p^n}) = D_{p^n} / \langle a^p \rangle = D_p,$$

and as D_p has property $\mathcal{B}$, by Lemma 3.1.1 D_{p^n} also has property $\mathcal{B}$. □

3.2 Property $\mathcal{B}$, Subgroups and Quotients

We begin this section by looking at how property $\mathcal{B}$ relates to subgroups of groups with property $\mathcal{B}$. If the subgroups of a group with property $\mathcal{B}$ also have property $\mathcal{B}$ then it is said to have the basis property which we discuss in Chapter 5. However not all groups with property $\mathcal{B}$ have the basis property. The following example highlights this.

Example 3.2.1. *The group with presentation $G = \langle x, y \mid x^4 = 1, y^3 = 1, x^{-1}yx = y^{-1}\rangle = C_3 \rtimes C_4$ has property $\mathcal{B}$. However G has the subgroup $\langle x^2 y\rangle$, isomorphic to the cyclic group of order 6 which does not have property $\mathcal{B}$.*

We shall first observe that G has property $\mathcal{B}$. The cyclic subgroups of G generated by x, xy and xy^2 are of order 4. Clearly x has order 4. Note that

$$(xy)^2 = xyxy = x^2x^{-1}yxy = x^2y^{-1}y = x^2 \neq 1,$$

and

$$(xy)^4 = \left(x^2\right)^2 = x^4 = 1,$$

so xy is of order 4. Also note that

$$\left(xy^2\right)^2 = xyyxyy = xyxx^{-1}yxyy = xyxy^{-1}yy = xyxy = (xy)^2 = x^2 \neq 1,$$

and

$$\left(xy^2\right)^4 = \left(x^2\right)^2 = x^4 = 1,$$

so xy^2 is of order 4. These subgroups of order 4 are maximal as they have index 3, as is the cyclic subgroup of order 6 generated by x^2y. These are in fact the only maximal subgroups and so the Frattini subgroup of G is the intersection of them which is $\langle x^2\rangle$. By Lemma 3.1.1, G has property $\mathcal{B}$ if and only if $G/\Phi(G)$ has property $\mathcal{B}$. In this case

$$G/\Phi(G) = G/\langle x^2\rangle = \langle x, y \mid x^2 = 1, y^3 = 1, x^{-1}yx = y^{-1}\rangle = C_3 \rtimes C_2$$

which is isomorphic to the symmetric group on three points. As we saw earlier in Example 3.1.4, S_3 has property $\mathcal{B}$ and thus so does G. Hence G is a group with property $\mathcal{B}$ with a subgroup that does not have property $\mathcal{B}$.

Lemma 3.1.1 shows that the Frattini quotient of a group G has property $\mathcal{B}$ if and only if G has property $\mathcal{B}$. However it is not as simple a proof to show that all quotients of a group of property $\mathcal{B}$ also have property $\mathcal{B}$. If we impose restrictions on the structure of G and a minimal normal subgroup of G, we can force property $\mathcal{B}$ to transfer to quotients.

Lemma 3.2.2. *If G is a group with property $\mathcal{B}$ and G splits over a normal subgroup M, then G/M has property $\mathcal{B}$.*

Proof. Let Q be a complement of M so $Q \cong G/M$. Pick elements $x_1, \ldots, x_d$ with d minimal such that $\langle x_1, \ldots, x_d \rangle^Q = M$. Now G is generated by $A = \{x_1, \ldots, x_d, y_1, \ldots, y_k\}$, where $\{y_1, \ldots, y_k\}$ is a minimal generating set for Q. We now show that A is a minimal generating set for G. If we removed one of the y_j we would no longer generate Q, as the y_j form a minimal generating set for Q. The choice of the x_i and the minimality of d ensures we cannot remove any of the x_i otherwise we would not generate M, and thus A is a minimal generating set for G. Since G has property $\mathcal{B}$ all minimal generating sets for G are of size $d + k$. Since d is fixed this forces k to be uniquely determined and thus Q has property $\mathcal{B}$. □

Proposition 3.2.3. *If G is a group with property $\mathcal{B}$ and M is an abelian minimal normal subgroup of G, then G/M has property $\mathcal{B}$.*

Proof. If G splits over M then G/M has property $\mathcal{B}$ by Lemma 3.2.2. Assume G does not split over M and let Q be G/M. Let $x_1, x_2, \ldots, x_d$ be elements of G such that $A = \{Mx_1, Mx_2, \ldots, Mx_d\}$ is a minimal generating set for Q and let $X = \langle x_1, x_2, \ldots, x_d \rangle$. Then $G = MX$ and $M \cap X \neq 1$ since our extension does not split. Now pick a non-identity element $y \in M \cap X$ and form the normal closure $\langle y \rangle^X$. Since M is abelian $\langle y \rangle^X = \langle y \rangle^{MX} = \langle y \rangle^G = M$; thus M is contained in X and hence $G = MX = X$. It follows that $\{x_1, x_2, \ldots, x_d\}$ is a generating set for G and it is necessarily minimal from our original assumption. Now G has property $\mathcal{B}$ and so $d(G) = d$. Since we took A to be arbitrary all minimal generating sets of Q are of the same size. Hence Q has property $\mathcal{B}$ with $d(Q) = d(G)$. □

From this we can establish the following corollary.

Corollary 3.2.4. *If G is a soluble group with property $\mathcal{B}$ then any quotient G/N also has property $\mathcal{B}$.*

Proof. Assume G is soluble and has property $\mathcal{B}$. We proceed by induction on the order of G. Clearly if G is the trivial group then any quotient G/N has property $\mathcal{B}$, so assume the result holds for soluble groups of order less than the order of G. Now let M be a minimal normal subgroup of G such that M is a subgroup of N. Note that since G is soluble M is elementary abelian. By the Third Isomorphism Theorem we have that,

$$G/N \cong \frac{G/M}{N/M},$$

and by Proposition 3.2.3 we have that G/M has property $\mathcal{B}$. By induction the quotient of G/M by N/M has property $\mathcal{B}$ and thus G/N has property $\mathcal{B}$. □

It is not straightforward to show that property $\mathcal{B}$ is inherited by quotients of insoluble groups. The proof of this would probably require heavy use of the Classification of Finite Simple Groups. A first step would be to verify that no almost simple group has property $\mathcal{B}$. We observe in the following that no non-abelian simple group has property $\mathcal{B}$.

Example 3.2.5. *If G is a non-abelian simple group then G does not have property $\mathcal{B}$.*

Proof. It is well known that if G is a non-abelian simple group then $d(G) = 2$. In fact much more is true, for example Guralnick–Kantor [4] showed that given any non-trivial element of a non-abelian simple group G, one can find another element of G such that the two generate G. Now let T be the set of all elements of order 2. Now $\langle T \rangle = G$ since $\langle T \rangle$ is normal in G. Choose a minimal subset T_0 of T such that $\langle T_0 \rangle = G$. We now show that the size of T_0 is greater than two. If $x, y \in T_0$ have order 2 and $a = xy$ then $x^{-1}ax = yx = (xy)^{-1} \in \langle a \rangle$ and $y^{-1}ay = y^{-1}ay^2 = yx = (xy)^{-1} \in \langle a \rangle$. Thus $\langle a \rangle$ is normal in $\langle x, y \rangle$ and so $\langle x, y \rangle = \langle a, x \rangle$. This is a dihedral group, as from above, $x^{-1}ax = a^{-1}$ gives us the required form, hence T_0 must be of size three or greater. Thus we have two minimal generating sets of different size and so G does not have property $\mathcal{B}$. □

From Proposition 3.1.5 we also know that symmetric groups on n points for $n \geq 4$ do not have property $\mathcal{B}$. In view of this it would be surprising that insoluble groups have property $\mathcal{B}$.

3.3 Products of Groups with Property $\mathcal{B}$

In this section we demonstrate how property $\mathcal{B}$ relates to direct products of groups. In particular we provide evidence to support our belief that groups with property $\mathcal{B}$ are rare. Our theorem in this section shows that those groups with property $\mathcal{B}$ that arise from direct products are precisely those that are provided by the Burnside Basis Theorem.

Theorem 3.3.1. *The group $G \times H$ has property $\mathcal{B}$ if and only if $G \times H$ is a p-group.*

Proof. If $G \times H$ is a p-group then it has property $\mathcal{B}$ by the Burnside Basis Theorem. It remains to show that if $G \times H$ has property $\mathcal{B}$ then it is a p-group. Assume $G \times H$ has property $\mathcal{B}$ and let $A = \{a_1, a_2, \dots a_d\}$ and $B = \{b_1, b_2, \dots, b_e\}$ be any two minimal generating sets for G and H respectively. Now the set $C = \{(a_1, 1), \dots, (a_d, 1), (1, b_1), \dots, (1, b_e)\}$ minimally generates $G \times H$ since removing any element would stop us generating one of the direct factors. This implies $d(G \times H) = d + e$. It follows that G must have property $\mathcal{B}$, with $d(G) = d$, since if G has two generating sets of size d and d' respectively then $d(G \times H) = d + e = d' + e$ and hence d' must equal d. Similarly one can see H must have property $\mathcal{B}$ also and $d(H) = e$.

Now let X be any generating set for G. Using the well known isomorphism $C_{mn} \cong C_m \times C_n$ (m,n co-prime, Lemma 3.1.2) we construct from X a generating set $X^\star$ for G consisting of elements of prime-power order. This is done by replacing any element x of order $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ with the k elements x^{r_j} where $r_j = n/p_j^{i_k}$ (for $j = 1, \dots, k$). Then, as G has property $\mathcal{B}$, we can find $X' \subseteq X^\star$ such that X' is a minimal generating set for G of size d. In the same way if Y is a generating set for H we can produce a minimal generating set Y' for H of size e consisting only of elements of prime-power order. Take $A = X'$ and $B = Y'$ in the previous paragraph to produce a minimal generating set C for $G \times H$ of size $d + e$. If $a \in X'$ and

$b \in Y'$ were to have co-prime order then we could replace $(a, 1)$ and $(1, b)$ by (a, b) and hence we would be able to produce a generating set for $G \times H$ of size smaller than $d + e$. Therefore there is a prime p such that every element in X' and every element in Y' has p-power order. Moreover if we chose a different generating set for G, say X_1, but the same generating set Y for H the same argument would show that Y' and thus X_1' would contain no elements of co-prime order. However we have already shown that Y' is generated by elements of p-power order and so the same must be true of X_1'. Thus p does not depend on the choice of X. A similar argument shows p does not depend on the choice of Y.

We now show that G is a p-group. Suppose there exists a prime $q \neq p$ that divides the order of G. Let x be any element of q-power order and let $Z \subseteq X$ be such that $X = \{x\} \cup Z$ generates G. Applying the method of the previous paragraph we construct the set $X^\star = \{x\} \cup Z^\star$. Note that since x is of q-power order it must be contained in $X^\star$. Now $X^\star$ contains a subset X' that generates G minimally and consists of elements of p-power order. Therefore $x \notin X'$ which implies that $X' = Z'$ and it follows that $Z^\star$ and hence Z generate G. Thus x is a non-generator of G and so is contained in the Frattini subgroup. Therefore any Sylow q-subgroup of G $(q \neq p)$ is contained in the Frattini subgroup. So $G/\Phi(G)$ is a p-group and $P\Phi(G)/\Phi(G)$ is the Sylow p-subgroup of $G/\Phi(P)$ if P is a Sylow p-subgroup of G. So $G = \langle P, \Phi(G)\rangle$ but $\Phi(G)$ is the set of non-generators and thus $G = P$. Similarly H is a p-group and hence $G \times H$ is a p-group. □

Chapter 4

A Standard Construction of Groups with Property $\mathcal{B}$

In this chapter we seek to construct a class of groups with property $\mathcal{B}$. We have already seen that dihedral groups of order $2p^n$, for prime-powers p^n, have property $\mathcal{B}$ and in fact closely resemble the groups studied by Scapellato and Verardi 1.1.4. All of these dihedral groups with property $\mathcal{B}$ have the structure

$$C_{p^n} \rtimes C_2,$$

where the cyclic group of order two acts by inversion. It is no surprise that the class of groups we construct are of a generalised form of the dihedral groups $P \rtimes Q$ where P is a p-group and Q a cyclic q-group. We begin by showing that certain groups of the form

$$\underbrace{(C_p \times \cdots \times C_p)}_{n \text{ times}} \rtimes C_{q^m},$$

where q^m is a prime-power which divides $p^n - 1$, have property $\mathcal{B}$ and trivial Frattini subgroup. In the definition of these groups we show how the action of the complement on the normal subgroup is defined in terms of field multiplication. We then classify all groups G for which $G/\Phi(G)$ has this form. Lemma 3.1.1 tells us that all such G must have property $\mathcal{B}$.

In Section 4.1 we construct our class of groups and show that they have both property $\mathcal{B}$ and trivial Frattini subgroup. In the following Section we then seek to generalise results from [10] to obtain detailed information on the structure of groups in which the Frattini quotient is isomorphic to our constructed examples. Finally we look at some examples of groups constructed with the forms described in the previous two sections, focusing on previous examples looked at in Chapter 3.

4.1 Setting up the Construction

We first take two prime numbers p and q such that q^m divides $p^n - 1$ for $n, m \in \mathbb{N}$ (note here that $\mathbb{N}$ does not include 0). Taking the field $\mathbb{F}_{p^n}$, we define V to be the additive group of $\mathbb{F}_{p^n}$ and let H be the unique cyclic group of order q^m embedded in the multiplicative group of $\mathbb{F}_{p^n}$. We take a mapping ϕ from H into the automorphism group of V such that the image of $h \in H$ under ϕ is the mapping $\alpha_h : v \mapsto vh$. Given $v, w \in V$ we can see that $(v + w)\,\alpha_h = (v + w)\,h$, which by the distributive law of V is $vh + wh = v\alpha_h + w\alpha_h$, and so α_h is a homomorphism. Since α_h is clearly a mapping from V to V, and is invertible since $vhh^{-1} = v$, we can see it is an automorphism. The maps $(h_1h_2)\phi$ and $(h_1\phi)(h_2\phi)$ are equal since they both send v to vh_1h_2 by the associativity of multiplication in $\mathbb{F}_{p^n}$, and so ϕ

is a homomorphism. Hence we can form the semidirect product G of V by H, denoted as usual by $G = V \rtimes_\phi H$, where H acts on V by multiplication in $\mathbb{F}_{p^n}$. We denote elements of the semidirect product as pairs.

By definition V is an elementary abelian p-group and so can be viewed as a vector space over the field $\mathbb{F}_p$. This means we can view ϕ as a linear representation from H into the group of invertible $n \times n$ matrices under multiplication modulo p

$$\phi : H \longrightarrow \mathrm{Aut}(V) = GL\left(V\right) = GL\left(n, p\right).$$

Let R denote the group algebra $\mathbb{F}_pH$. So ϕ induces upon V the structure of an R-module. Since the characteristic p of our field is co-prime to the order of the group H, we can apply Maschke's Theorem 2.2.3. This gives us that viewed as an R-module V is a direct sum of k irreducible R-submodules $V_1 \oplus \cdots \oplus V_k$. Now since each V_i is irreducible it is generated as an R-module by a single element v_i, and thus V is generated as an R-module by k elements.

Let $H = \langle x \rangle$, then elements of the group algebra R have the form $\sum_{j=0}^{q^m-1} \lambda_j x^j$, where the λ_j are elements of the field $\mathbb{F}_p$. So elements of V_i have the form

$$v_i \left(\sum_{j=0}^{q^m-1} \lambda_j x^j \right) = \sum_{j=0}^{q^m-1} \lambda_j v_i \left(x^j \phi \right) = \sum_{j=0}^{q^m-1} \lambda_j v_i x^j,$$

this being an evaluation of sums and products in $\mathbb{F}_{p^n}$. The module action of H on V corresponds to conjugation in the semidirect product and hence V_i is contained in the subgroup of G generated by v_i and x. Thus G is generated by the set $\{(v_1, 1), (v_2, 1), \ldots, (v_k, 1), (0, x)\}$. We now show this generating set is minimal. The subgroup

$$\langle (v_1, 1), \ldots, (v_{i-1}, 1), (v_{i+1}, 1), \ldots, (v_k, 1), (0, x) \rangle,$$

is contained in the subgroup $(V_1 \oplus \ldots V_{i-1} \oplus V_{i+1} \cdots \oplus V_k) \rtimes H$, while if we remove $(0, x)$ we generate only a subgroup of V. Thus we have proved:

Lemma 4.1.1. *Let G be a group of the form $V \rtimes_\phi H$ where H acts on V by multiplication in the field $\mathbb{F}_{p^n}$, then G is minimally generated by a set containing $k+1$ elements.*

The elements in this minimal generating set are of either order p or of q power order. If there existed elements of order pq^i in these groups then it could be possible to form a smaller minimal generating set. Since we are establishing a group with property $\mathcal{B}$ the following lemma is a helpful result.

Lemma 4.1.2. *If G is a group of the form $V \rtimes_\phi H$, where H acts on V by multiplication in the field $\mathbb{F}_{p^n}$, then G contains no elements of order pq^i for any $i \geq 1$.*

Proof. By construction the conjugation of $(v, 1)$ by $(0, h)$ is simply $(vh, 1)$. Thus our semidirect product multiplication is $(v, h)(w, k) = \left(v + wh^{-1}, hk\right)$, as is standard. As $(v, 1)$ lies in V it clearly is an element of order p. Similarly $(1, h)$ is an element of H and so has q power order. Hence if G contained any elements of order pq^i then they would be of the form (v, h) where h is not the identity.

Claim: $(v, h)^n = \left(v + vh^{-1} + vh^{-2} + \cdots + vh^{-(n-1)}, h^n\right)$.

Taking a base case of $(v, h)^2$ it is clear to see from our defined multiplication this is $\left(v + vh^{-1}, h^2\right)$. Proceeding inductively we assume that

$$(v,h)^i = \left(v + vh^{-1} + vh^{-2} + \cdots + vh^{-(i-1)}, h^i\right),$$

and so

$$\begin{aligned}(v,h)^{i+1} &= \left(v + vh^{-1} + vh^{-2} + \cdots + vh^{-(i-1)}, h^i\right)(v,h), \\ &= \left(\left(v + vh^{-1} + vh^{-2} + \cdots + vh^{-(i-1)}\right) + vh^{-i}, h^i h\right), \\ &= \left(v + vh^{-1} + vh^{-2} + \cdots + vh^{-(i-1)} + vh^{-i}, h^{i+1}\right).\end{aligned}$$

Hence the induction holds.

Claim: $(v,h)^{q^m}$ is trivial.

By our first claim $(v,h)^{q^m}$ is $\left(v + vh^{-1} + vh^{-2} + \cdots + vh^{-(q^m-1)}, h^{q^m}\right)$. The first entry is v multiplied by the geometric sum $\sum_{i=0}^{q^m-1} h^{-i} = \sum_{i=0}^{q^m-1} (1/h)^i$. Evaluating this geometric sum using standard techniques gives

$$\sum_{i=0}^{q^m-1} (1/h)^i = \frac{(1/h)^{q^m} - 1}{1/h - 1}.$$

Since h is a non-trivial element of a group of order q^m, this sum is zero. Hence $(v,h)^{q^m}$ is equal to $(0,1)$ which is the identity element in G, thus an element of the form (v,h) has q power order. □

We know that V is a direct sum of irreducible submodules by Maschke's Theorem. In fact we can see that any submodule vR of V is irreducible.

Lemma 4.1.3. *Let $v, w \in V$ with v, w both non-zero, then $vR \cong wR$. In particular all vR are irreducible for all $v \in V$.*

Proof. If v is a non-zero element of V, define $\theta_v : R \to vR$ by $r \mapsto vr$. Since V is the additive group of our field $\mathbb{F}_{p^n}$, the kernel of θ_v consists of those elements $r = \sum_{h \in H} \lambda_h h$ in R such that the sum $\sum_{h \in H} \lambda_h h$ equals 0 when evaluated in $\mathbb{F}_{p^n}$. In particular θ_v is independent of the choice of v. Hence if v and w are two non-zero elements of V, then $\ker \theta_v = \ker \theta_w$, so by the First Isomorphism Theorem $vR \cong R/\ker \theta_v = R/\ker \theta_w \cong wR$.

Given that all submodules vR of V are isomorphic to each other to show they are all irreducible we need only show that there exists one vR that is irreducible. As V is a direct sum of irreducible submodules, it has at least one irreducible submodule U. Lemma 2.2.2 says U is cyclic, say $U = wR$. The first part of this lemma says $vR \cong wR$, so vR is also irreducible. □

Theorem 4.1.4. *Let V be the additive group of the field $\mathbb{F}_{p^n}$ of p^n elements and H the subgroup of the multiplicative group $\mathbb{F}^{\star}_{p^n}$ of order q^m. Define G to be the semidirect product $V \rtimes_{\phi} H$ where H acts on V by multiplication in $\mathbb{F}_{p^n}$. Then:*

(i) G has property $\mathcal{B}$,

(ii) $d(G) = k + 1$ where V is a direct sum of k irreducible $\mathbb{F}_p H$-modules,

(iii) $\Phi(G)$ is trivial.

Proof. We retain the notation already established in this section. By Lemma 4.1.1 we know that G is minimally generated by $k + 1$ elements. Let A be an arbitrary generating set for G, we show that A possesses a subset of size $k + 1$ that generates G. Parts *(i)* and *(ii)* follow from this observation.

Claim: There exists some a_1 in A such that $H = \langle a_1 \pi \rangle$ where $\pi : G \to H$ is the projection map such that $\ker \pi = V$.

Define $\pi : G \to H$ to be the projection map such that the kernel of π is V.

Then $A\pi$ generates H since A is a generating set for G. The group H is cyclic of prime-power order and so there exists an element a_1 in A such that $H = \langle a_1\pi\rangle$.

Claim: We can construct $w_i \in V$ from the elements of A such that $A' = \{a_1, w_1, \ldots, w_l\}$ generates G.

By Lemma 4.1.2 there are no elements of order pq^i in G and so a_1 is of order q^m since $|H| = q^m$. Hence all other elements of A are of the form $a = wa_1^j$ where $w \in V$, $j \geq 0$ with $j = j(a)$ depending on the choice of a. Thus $aa_1^{-j} = w$ is an element of V and so is of order p. Now let $w_1, \ldots, w_l$ be the collection of all such $aa_1^{-j(a)}$ and we define A' to be the set $\{a_1, w_1, \ldots, w_l\}$. This is a generating set for G by construction.

Claim: $V = W = \sum_{i=1}^{l} w_iR$.

Let $W = \sum_{i=1}^{l} w_iR$ be the submodule of V generated by the w_i. The intersection $V \cap \langle a_1\rangle$ is trivial since the order of a_1 is q^m and V is a p-group. Since A is a generating set for G it follows that $G = W\langle a_1\rangle$. Now

$$\begin{aligned} W &= W\left(V \cap \langle a_1\rangle\right), \\ &= V \cap W\langle a_1\rangle \text{ (by Dedekind's Modular Law)} \\ &= V \cap G, \\ &= V. \end{aligned}$$

Claim: V is a direct sum of exactly k summands w_iR.

By the proof of Lemma 2.2.4, W is the direct sum of some of the distinct w_iR. Since V is the direct sum of k isomorphic irreducible submodules by the Krull–Schmidt Theorem (Theorem 2.2.5), W must be of the same form. Thus V is the direct sum of k isomorphic irreducible submodules $w_{i_1}R, w_{i_2}R, \dots, w_{i_k}R$. Hence there exists a subset $\{w_{i_1}, w_{i_2}, \dots, w_{i_k}, a_1\}$ of A' of size $k+1$ that generates G. By taking the k elements of A of the form $a = w_i a_1^j$ for each $w_i \in A'$ we create a subset of A of size $k+1$ that generates G. Thus G has property $\mathcal{B}$ with $d(G) = k+1$.

It now remains to prove that $\Phi(G)$ is trivial.

Claim: $(V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_k) \rtimes H$ are maximal subgroups of G and $\Phi(G) \leqslant H$.

We can see that the $K_i = (V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_k) \rtimes H$ is a subgroup of G since $V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_k$ is a submodule of V and so inherits the field multiplication action of H. This subgroup is in fact maximal as any non-trivial element of G not contained in K_i generates V_i as a module under the action of H. The intersection of all such K_i is clearly H and so $\Phi(G) \leqslant H$.

Claim: No non-trivial subgroup of H is normal in G.

Let $(0,h)$ be any element of H and $(v,1)$ be any element of V with $v \neq 0$. If $(0,h)$ was in a non-trivial subgroup of H that was normal in G then the conjugate of $(0,h)$ by $(v,1)$ would also lie in H. The conjugate $(0,h)^{(v,1)} = (-v,1)(0,h)(v,1) = (-v,h)(v,1)$ since we work additively in V. By the multiplication we defined for semidirect products this is $(-v,h)(v,1) = \left(-v + vh^{-1}, h\right)$. Thus if $(0,h)^{(v,1)}$ lies in H then $-v + vh^{-1}$ must be 0. So $v = vh^{-1}$ and under the field multiplication this implies $h = 1$ as $v \neq 0$. Hence no non-trivial element of H conjugates back into H.

Now $\Phi(G) \leqslant H$ and $\Phi(G) \lhd G$ so by our previous claim $\Phi(G) = 1$. □

Actually the group that we have constructed is a Frobenius group.

Lemma 4.1.5. *Let V be the additive group of the field $\mathbb{F}_{p^n}$ of p^n elements and H the subgroup of the multiplicative group $\mathbb{F}_{p^n}^\star$ of order q^m. Define G to be the semidirect product $V \rtimes_\phi H$ where H acts on V by multiplication in $\mathbb{F}_{p^n}$. Then G is a Frobenius group.*

Proof. A group G is a *Frobenius group* if it contains a non-trivial proper subgroup K such that $K \cap K^g$ is trivial for all $g \in G \backslash K$. We seek to show that H is such a subgroup. Let $v \neq 0$ and $k, h \neq 1$ such that (v, k) is any element in $G \backslash H$ and $(0, h)$ is any non-trivial element of H. Then $(0, h)^{(v,k)} = \left(-vk, k^{-1}\right)(0, h)(v, k)$ as we work additively in V and multiplicatively in H. By the multiplication we defined for semidrect products this is

$$\begin{aligned} \left(-vk, k^{-1}\right)(0, h)(v, k) &= \left(-vk, k^{-1}h\right)(v, k) \\ &= \left(-vk + v\left(k^{-1}h\right)^{-1}, k^{-1}hk\right) \\ &= \left(-vk + vh^{-1}k, h\right). \end{aligned}$$

Thus if $(0, h)^{(v,k)}$ lies in H then $-vk + vh^{-1}k$ must be zero and so $vk = vh^{-1}k$. Now since $v \neq 0$ then $k = h^{-1}k$ and thus $h^{-1} = h = 1$. Thus no non-trivial element of H conjugates back to H and thus $H \cap H^{(v,k)} = 1$ for $(v, k) \notin H$. Therefore G is a Frobenius group. □

In Lemma 4.1.3 we established the structure of the irreducible submodules of V. We can show that these submodules actually construct groups of the form described in Theorem 4.1.4.

Lemma 4.1.6. *(i) There is a unique finite field of characteristic p generated by a subgroup of order q^m of its multiplicative group, namely the* *field $\mathbb{F}_{p^r}$ where r is minimal such that $\mathbb{F}_{p^r}$ has a multiplicative subgroup of order q^m.*

(ii) Any irreducible submodule of V is isomorphic to the additive group of $\mathbb{F}_{p^r}$ (r as in (i)) viewed as an R-module via the field multiplication in $\mathbb{F}_{p^r}$.

Proof. (i) Given the minimality of r, if H is a multiplicative subgroup of $\mathbb{F}_{p^r}$ of order q^m then the field generated by H must be $\mathbb{F}_{p^r}$. Let K and L be two finite fields of characteristic p generated by multiplicative subgroups of order q^m. Now there exists a finite field F that contains both K and L. However the subgroup of order q^m embedded in the multiplicative group of F is unique, and thus K and L are generated by the same subgroup and are equal.

(ii) As in Lemma 4.1.3 let v be a non-zero element of V and let θ_v be the homomorphism from R to vR. Since R is commutative the kernel of θ_v is a maximal ideal of R. Thus the structure of $R/\ker\theta_v$ is that of a field. If h is contained in the intersection of H and $1+\ker\theta_v$ then $v(h-1)=0$ in the field $\mathbb{F}_{p^n}$. Thus $H\cap(1+\ker\theta_v)=1$ and therefore $(H-1)\cap\ker\theta_v=0$. So, for h_1,$h_2\in H$, if $h_1\theta_v=h_2\theta_v$, then $h_1=h_2$. Thus H embeds in the multiplicative group of $R/\ker\theta_v$. As H generates R it then follows that the image of H in $R/\ker\theta_v$ generates $R/\ker\theta_v$ and so by part (i) $R/\ker\theta_v$ is isomorphic to $\mathbb{F}_{p^r}$. If an element of the additive group of $R/\ker\theta_v$ is given by $\ker\theta_v+s$ then an element $h\in H$ acts by multiplication such that $(\ker\theta_v+s)h=\ker\theta_v+sh=(\ker\theta_v+s)(\ker\theta_v+h)$. Therefore vR is isomorphic to $R/\ker\theta_v$, where $R/\ker\theta_v$ is viewed as an R-module via the field multiplication in $R/\ker\theta_v$. □

4.2 Quotients by the Frattini Subgroup

We know from Lemma 3.1.1 that if any group has property $\mathcal{B}$ then the quotient of the group by its Frattini subgroup also has property $\mathcal{B}$. In this section we provide a description of the structure of a group G in which the quotient $G/\Phi(G)$ is isomorphic to the group constructed in Section 4.1. We also outline the structure of the Frattini subgroup of such a group G.

Theorem 4.2.1. *Let V be the additive group of the field $\mathbb{F}_{p^n}$ of p^n elements and H the subgroup of the multiplicative group $\mathbb{F}^{\star}_{p^n}$ of order q^m. Let G be any group such that $G/\Phi(G)$ is isomorphic to the semidirect product $V \rtimes_{\phi} H$ where H acts on V via the multiplication in $\mathbb{F}_{p^n}$. Then:*

(i) G has a unique Sylow p-subgroup P,

(ii) G is the semidirect product of P by Q for any Sylow q-subgroup Q and all Sylow q-subgroups of G are cyclic,

(iii) $\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$ where $\langle x^{q^m} \rangle$ is the subgroup of index q^m in $Q = \langle x \rangle$. In fact x^{q^m} lies in the centre of G.

Proof. *(i)* Let P be a Sylow p-subgroup of G. Then the quotient of $P\Phi(G)$ by $\Phi(G)$ is a Sylow p-subgroup of $G/\Phi(G)$ and $P\Phi(G)/\Phi(G)$ is normal in $G/\Phi(G)$, by our hypothesis. This implies that $P\Phi(G)$ is normal in G by the Correspondence Theorem and since $P\Phi(G) \trianglelefteq G$ the Sylow p-subgroup of $P\Phi(G)$ is $P\Phi(G) \cap P = P$. The Frattini Argument (Lemma 2.1.3) states that if N is a normal subgroup of G with Sylow p-subgroup P then $G = N_G(P)N$. Applying this to $P\Phi(G)$ gives us that G is equal to $N_G(P)P\Phi(G)$. Clearly P is contained in its own normaliser and so G is in fact equal to

$N_G(P)\Phi(G)$. Since $\Phi(G)$ is the set of non-generators of G we have that $G = N_G(P)$ and thus P is normal in G. Hence P is the unique Sylow p-subgroup.

(ii) Let Q be a Sylow q-subgroup.

Claim: G is the semidirect product $P \rtimes Q$.

Our hypothesis on $G/\Phi(G)$ ensures that $G = PQ\Phi(G)$ and since P is normal, PQ is a subgroup of G. Now $\Phi(G)$ is the set of non-generators and so $G = PQ$. Since P and Q are Sylow subgroups for different primes their intersection is trivial and so $G = P \rtimes Q$.

Consider the quotient group $\bar{G} = G/(P \cap \Phi(G))$, where we use bar notation for images of subgroups in G.

Claim: $\Phi(\bar{G}) \leqslant \bar{Q}$.

The quotient $\bar{G}$ has maximal subgroups in bijection with those of G, as the maximal subgroups of G always contain $P \cap \Phi(G)$, and so we apply the Correspondence Theorem. Thus we observe that $\Phi(\bar{G}) = \overline{\Phi(G)}$. Applying the Third Isomorphism Theorem we see that $G/\Phi(G)$ is isomorphic to $\bar{G}/\Phi(\bar{G})$. Therefore $\bar{G}$ satisfies the hypothesis of the theorem. Hence the Sylow p-subgroup of $\Phi(\bar{G})$ is

$$\frac{P}{P \cap \Phi(G)} \cap \frac{\Phi(G)}{P \cap \Phi(G)} = \frac{P}{P \cap \Phi(G)} \cap \Phi(\bar{G}),$$

which is trivial. This ensures that $\Phi(\bar{G})$ is a q-group and so $\Phi(\bar{G}) \leqslant \bar{Q}$.

Claim: $\Phi(\bar{G})$ is contained in every maximal subgroup of $\bar{Q}$ and so $\Phi(\bar{G}) \leqslant \Phi(\bar{Q})$.

Let W be a maximal subgroup of Q. Then PW is maximal in G and thus $\Phi(G) \leqslant PW$ with W a Sylow q-subgroup of PW. Passing into the quotient group we can see that $\Phi\left(\bar{G}\right) \leqslant \overline{PW}$ and $\bar{W}$ is a Sylow q-subgroup of $\overline{PW}$ as W is a Sylow q-subgroup of PW. Since $\Phi\left(\bar{G}\right)$ is a q-group then $\Phi\left(\bar{G}\right) \leqslant \bar{W}$. Now $\bar{W}$ is an arbitrary maximal subgroup of $\bar{Q}$ (since W is an arbitrary maximal subgroup of Q) and so $\Phi\left(\bar{G}\right) \leqslant \Phi\left(\bar{Q}\right)$.

Claim: $\bar{Q}/\Phi\left(\bar{Q}\right)$ is cyclic.

We have

$$\bar{Q} = \frac{Q\left(P \cap \Phi(G)\right)}{P \cap \Phi(G)} \text{ and } \Phi\left(\bar{G}\right) = \frac{\Phi(G)}{P \cap \Phi(G)},$$

and so

$$\frac{\bar{Q}}{\Phi\left(\bar{G}\right)} \cong \frac{Q\left(P \cap \Phi(G)\right)}{\Phi(G)} = \frac{Q\Phi(G)}{\Phi(G)}.$$

By our hypothesis $\bar{Q}/\Phi\left(\bar{G}\right)$ is cyclic and by the Third Isomorphism Theorem

$$\frac{\bar{Q}}{\Phi\left(\bar{Q}\right)} = \frac{\bar{Q}/\Phi\left(\bar{G}\right)}{\Phi\left(\bar{Q}\right)/\Phi\left(\bar{G}\right)},$$

so $\bar{Q}/\Phi\left(\bar{Q}\right)$ is cyclic as it is the quotient of a cyclic group.

Claim: $\bar{Q}$ and Q are cyclic.

Now $\bar{Q} = \langle x, \Phi\left(\bar{Q}\right)\rangle$ for some x, then as the Frattini subgroup is the set of non-generators, $\bar{Q} = \langle x \rangle$ and so is cyclic. We know that

$$\bar{Q} = \frac{Q\left(P \cap \Phi(G)\right)}{P \cap \Phi(G)},$$

and since Q and $P \cap \Phi(G)$ intersect trivially $\bar{Q} \cong Q$ and so Q is cyclic.

(iii) We begin by proving the following claim.

Claim: $G/\Phi(P) \cong P/\Phi(P) \rtimes \left(Q\Phi(P)\right)/\Phi(P)$.

Note that the Frattini subgroup of P is characteristic in P. Since P is normal in G, $\Phi(P) \trianglelefteq G$ and we have

$$G/\Phi(P) = \frac{P \rtimes Q}{\Phi(P)} \cong \frac{P}{\Phi(P)} \rtimes \frac{Q\Phi(P)}{\Phi(P)}.$$

Claim: $P/\Phi(P)$ can be viewed as an $\mathbb{F}_pQ$-module and is a direct sum of irreducible submodules.

By the Second Isomorphism Theorem

$$\frac{Q\Phi(P)}{\Phi(P)} \cong \frac{Q}{Q \cap \Phi(P)} \cong Q,$$

and so

$$G/\Phi(P) \cong \frac{P}{\Phi(P)} \rtimes Q,$$

where Q inherits its action on $P/\Phi(P)$ from its action on P. By Maschke's Theorem, $P/\Phi(P)$ is a sum of irreducible $\mathbb{F}_pQ$-modules, say $V_1 \oplus \cdots \oplus V_s$.

Claim: $\Phi(P) = \Phi(G) \cap P$.

Similarly to the proof of Theorem 4.1.4 part *(iii)* define $M_i^\star$ to be the maximal subgroup

$$M_i^\star = (V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_s) \rtimes Q,$$

of $P/\Phi(P)$. Now $M_i^\star$ corresponds to a subgroup M_i of G and the Correspondence Theorem forces M_i to be maximal, so we can write $M_i^\star = M_i/\Phi(P)$. By construction the intersection of all $M_i^\star$ with $P/\Phi(P)$ is trivial and hence $\bigcap_{i=1}^{s}(M_i \cap P) = \Phi(P)$. Since $\Phi(G)$ is contained within all the M_i then $\Phi(G) \cap P \leqslant \Phi(P)$. By the original hypothesis $P\Phi(G)/\Phi(G) \cong P/(\Phi(G) \cap P)$ is an elementary abelian p-group. Using Burnside's Basis Theorem (1.1.1) we have that $\Phi(P) = P^pP' \leqslant \Phi(G) \cap P$. Hence $\Phi(P) = \Phi(G) \cap P$, and since $\Phi(G) \cap P$ is normal in G, $\Phi(P) \trianglelefteq \Phi(G)$ follows immediately.

Claim: $\left[P, \Phi(P)\langle x^{q^m}\rangle\right] \leqslant \Phi(P)$.

Since G is the semidirect product of P and Q, we define $\theta : Q \to \mathrm{Aut}(P)$ to be the homomorphism determined by the action of Q on P. There now exist two natural mappings $\pi_1 : G \to G/\Phi(P)$ and $\pi_2 : G/\Phi(P) \to G/\Phi(G)$ since $\Phi(P)$ is contained within $\Phi(G)$. We showed previously that

$$G/\Phi(P) \cong P/\Phi(P) \rtimes Q,$$

and we note here that

$$G/\Phi(G) \cong P/\Phi(P) \rtimes Q/\langle x^{q^m}\rangle.$$

So the kernel of the mapping π_2 is $\langle x^{q^m}\rangle\Phi(P)/\Phi(P)$. By the First Isomorphism Theorem $\ker \pi_2$ is normal in $G/\Phi(P)$ and so by the Correspondence Theorem $\langle x^{q^m}\rangle\Phi(P)$ is a normal subgroup of G. Hence

$$\left[P, \langle x^{q^m}\rangle\Phi(P)\right] \leqslant P \cap \langle x^{q^m}\rangle\Phi(P) \leqslant \left(P \cap \langle x^{q^m}\rangle\right)\Phi(P) = \Phi(P).$$

Claim: $\langle x^{q^m}\rangle$ commutes with P.

From the previous claim we can note that $\langle x^{q^m}\rangle$ commutes with P modulo $\Phi(P)$. Hence $\langle x^{q^m}\rangle\theta \leqslant C_{\mathrm{Aut}(P)}(P/\Phi(P))$. By a theorem of Philip Hall (see 2.1.8) this centraliser is a p-group so $\langle x^{q^m}\rangle$ is contained in the kernel of θ. Thus $\langle x^{q^m}\rangle$ commutes not just with $\Phi(P)$ but with P and $\Phi(G) = \Phi(P) \times \langle x^{q^m}\rangle$. So $\langle x^{q^m}\rangle$ commutes with P and obviously commutes with $Q = \langle x\rangle$ and therefore x^{q^m} lies in the centre of PQ which is the centre of G. □

4.3 Examples of Groups of the Constructed Form

We now look at a few examples of groups that have the form as previously described. We begin by looking at a re-working of Example 3.1.4.

Example 4.3.1. *The symmetric group on 3 points, $S_3 \cong C_3 \rtimes C_2$ has property $\mathcal{B}$ and is a group of the form described in Theorem 4.1.4.*

Proof. From Example 3.1.4 we know that S_3 has property $\mathcal{B}$ and so it remains to show it is of the desired form. Take $V = \{0, 1, 2\}$ to be the additive group of the field $\mathbb{F}_3$ and $H = \{1, 2\}$ the multiplicative group of $\mathbb{F}_3$. Clearly $V \cong C_3$ and $H \cong C_2$. Using the homomorphism $\phi : H \to \mathrm{Aut}(V)$, as we constructed, if $v \in V$ then $1\phi = \alpha_1 : v \mapsto v$ and $2\phi = \alpha_2 : v \mapsto 2v$ under the field multiplication from $\mathbb{F}_3$. Forming the semidirect product $G = V \rtimes_\phi H$, under the action of ϕ, and our semigroup multiplication, we observe that G is not abelian and so we can deduce it must be be isomorphic to S_3. □

We now look at how a class of groups all fit the forms constructed in the previous sections. In Chapter 3 Proposition 3.1.6 told us that dihedral groups of order $2p$, where p is an odd prime, have property $\mathcal{B}$. We now investigate how these dihedral groups relate to the forms described in Theorems 4.1.4 and 4.2.1.

Proposition 4.3.2. *Dihedral groups of order $2p$ for some odd prime p are of the form described in Theorem 4.1.4 being isomorphic to $C_p \rtimes C_2$.*

Proof. It is well known that the dihedral group D_p is isomorphic to $C_p \rtimes C_2$ where the cyclic group of order two acts by inversion. Also note that C_p is isomorphic to the additive group of $\mathbb{F}_p$. The field multiplication action of a unique subgroup of order two embedded in the multiplicative group of $\mathbb{F}_p$ is the same as the inversion action of the C_2. This is because when p is odd the element of order two in the multiplicative group of the field $\mathbb{F}_p^\star$ is -1. Now $(-1)^2 = 1$ and since p is not two -1 is not equal to 1 modulo p. Note that, in the notation of our constuction, $v\left((-1)\,\theta\right) = -v$ is the inverse of v in $\mathbb{F}_p$ viewed as an additive group. Thus D_p has the form as described in Theorem 4.1.4. □

Following on from Proposition 3.1.6 we explained that a dihedral group of order $2p^n$ has Frattini quotient isomorphic to D_p and thus by Lemma 3.1.1 D_{p^n} has property $\mathcal{B}$. Therefore we can see that D_{p^n} satisfies the hypothesis of Theorem 4.2.1.

Proposition 4.3.3. *Dihedral groups of order $2p^n$, for some odd prime p, are of the form described in Theorem 4.2.1.*

Proof. From the proof of Corollary 3.1.7 we saw that the quotient of D_{p^n} by its Frattini subgroup is isomorphic to D_p which from above is $C_p \rtimes C_2$ and is constructed via multiplication in the field $\mathbb{F}_p$. Thus D_{p^n} satisfies the hypothesis of Theorem 4.2.1. □

Chapter 5

Classifying Groups with the Basis Property

A group G is said to have the basis property if all subgroups of G have property $\mathcal{B}$. In this chapter we provide some examples of groups with the basis property and then establish some results that hold for all groups with the basis property. We finish by providing a classification of all groups with the basis property and showing how this links in with the matroid groups classified by Scapellato and Verardi [10].

5.1 An Introduction to Groups with the Basis Property

We know that a p-group has property $\mathcal{B}$ from our previous work. Since a subgroup of a p-group is itself a p-group we can conclude that all p-groups have the basis property. In fact we can generalise this slightly to say that any group with property $\mathcal{B}$ and only p-groups as subgroups has the basis property. As a consequence, the smallest non-p-group with the basis property is the symmetric group on 3 points. As we have shown previously this has property $\mathcal{B}$ and subgroups isomorphic to C_3, C_2 and the trivial subgroup. We now provide an example of a class of groups that have the basis property.

Example 5.1.1. *If p is a prime then the dihedral group of order $2p^n$, D_{p^n}, has the basis property.*

Proof. If D_{p^n} is a p-group then it has the basis property as observed above. So assume that D_{p^n} is not a p-group, i.e. that $p \neq 2$. Thus D_{p^n} has the form $P \rtimes \langle b \rangle$ where P is a p-group and $\langle b \rangle$ is a subgroup of order 2. Let H be a subgroup of D_{p^n}. First note that $H \cap P$ is normal in H and isomorphic to a cyclic group of order of a power of p. Now let π be the mapping from D_{p^n} to $\langle b \rangle$. The kernel of this mapping is P and so $H\pi$ is either trivial or $\langle b \rangle$. If $H\pi = 1$ then $H = H \cap P$ and so is a cyclic p-group. So let $H\pi = \langle b \rangle$. Now H has a Sylow 2-subgroup so let h be a non-trivial element of H in this Sylow 2-subgroup. Since D_{p^n} is not a p-group then its Sylow 2-subgroup is $\langle b \rangle$ and so $h\pi = b$. Thus $H = (H \cap P) \langle h \rangle = (H \cap P) \rtimes \langle h \rangle$ and h acts by inversion. Therefore H is isomorphic to a dihedral group of order $2p^m$ ($m \leq n$) or H is isomorphic to C_2 if $H \cap P$ is trivial. Thus any subgroup of a dihedral group of order $2p^n$ is either a smaller dihedral group of the same form or cyclic of prime-power order. Hence D_{p^n} has the basis property. □

Of course not all groups with property $\mathcal{B}$ have the basis property.

Example 5.1.2. *Let $G = (C_2 \times C_2) \rtimes_\phi C_9$ where ϕ is the composition of* *the natural map from C_9 into C_3 and the mapping of C_3 into the unique subgroup of order three into* $\mathrm{Aut}(C_2 \times C_2) = S_3$*. Then G has property $\mathcal{B}$ but not the basis property.*

Proof. Note that ϕ is the composite of the natural map from C_9 into C_3 and the homomorphism that occurs in our construction via field multiplication, specifically the homomorphism $C_3 \mapsto \mathrm{Aut}(C_2 \times C_2)$ coming from our construction via the multiplication in the field $\mathbb{F}_4$. Then $\ker \phi$ is isomorphic to the cyclic group of order 3 and so $\ker \phi$ is the unique subgroup of order 3 in G. Now let M be a maximal subgroup of G that does not contain $\ker \phi$. As M is maximal in G then G is in fact equal to $M \ker \phi$, with the intersection of M and the kernel trivial, as $\ker \phi$ is a minimal normal subgroup. Thus G is equal to $\ker \phi \rtimes M$, but this contradicts $\ker \phi$ being the unique subgroup of order 3. This follows as M has a subgroup of order 3 by Sylow's Theorem. Thus $\ker \phi$ is contained in every maximal subgroup of G and so is contained in the Frattini subgroup of G. However, the quotient of G by $\ker \phi$ is constructed by field multiplication in $\mathbb{F}_4$ and has trivial Frattini subgroup by Theorem 4.2.1 part (iii); thus $G/\Phi(G)$ has property $\mathcal{B}$, and so by Lemma 3.1.1 so does G. However G does not have the basis property, as it contains the subgroup $C_2 \times C_2 \times \ker \phi$ isomorphic to $C_2 \times C_2 \times C_3$. □

5.2 Properties of Groups with the Basis Property

The examples of groups with the basis property so far have all been constructed from elements of prime-power order. This is true for all groups with the basis property, a result which is shown in Jones [7].

Lemma 5.2.1. *If G is a group with the basis property then G consists of elements of prime-power order.*

Proof. Let G be a group with the basis property and suppose that x is an element of G not of prime-power order. Since G has the basis property then all subgroups of G must have property $\mathcal{B}$. However the subgroup $\langle x \rangle$ of G does not have property $\mathcal{B}$, as it is isomorphic to a cyclic group of non-prime-power order. Hence no element of G can be of non-prime-power order. □

In our previous chapter we showed that non-abelian simple groups do not have property $\mathcal{B}$. Clearly this implies that a group with the basis property contains no non-abelian simple subgroups. This result coupled with the previous lemma gives us the following result.

Lemma 5.2.2. *If G is a group with the basis property then G is soluble.*

Proof. Let G be a minimal counter example by order. Since G contains no non-abelian simple subgroups, G is not simple. Let M be a minimal normal subgroup of G. If H is a proper subgroup of G, then it has the basis property and so is soluble by the assumption on G. Hence H/M has property $\mathcal{B}$ by Corollary 3.2.4. Hence G/M and M have the basis property and so by the assumption on G are soluble. This implies G is simple, a contradiction. □

This result is also available in Jones [7]. The major difference between the proof in Jones and ours is that when proving G cannot be simple he does not use the Classification of Finite Simple Groups. Instead Jones uses a result by Thompson [12] that shows all finite minimal simple groups are two generated. Using this result he then shows a group with the basis property can not be simple. From Lemma 5.2.2 one can quickly establish the following result.

Corollary 5.2.3. *If G is a group with the basis property then any homomorphic image of G has the basis property.*

From Corollary 3.2.4 it follows that any homomorphic image of G has property $\mathcal{B}$. The Correspondence Theorem then tells us that the quotient has the basis property.

5.3 Classifying Groups with the Basis Property

From the previous section we have established that finite groups with the basis property are soluble and only contain elements of prime-power order. Groups of this type have been classified in Graham Higman's 1956 paper [5, Theorem 1].

Theorem 5.3.1 (Higman, 1956)**.** *Let G be a soluble group in which every element is of prime-power order. Let p be a prime such that G has a non-trivial normal p-subgroup, and let P be the greatest such normal p-subgroup. Then G/P is either:*

(i) a cyclic q-group, for q a prime other than p,

(ii) a generalised quaternion group and p is odd,

(iii) a group of order $p^a q^b$ with cyclic Sylow subgroups and q is a prime that divides $p^a - 1$.

Thus G has order divisible by at most two primes, and G/P is metabelian.

Using this theorem we can form a classification for all groups with the basis property.

Theorem 5.3.2. *Let G be a finite group. Then G has the basis property if and only if either:*

(i) G is a p-group, or

(ii) $G = P \rtimes Q$ where P is a p-group, Q a non-trivial cyclic q-group, and every non-identity element of Q acts fixed-point freely on P.

Here an element y of Q is said to act *fixed-point freely* if its centraliser $C_P(y)$ is trivial. To show every non-identity element of Q acts fixed-point freely it is sufficient to show a generator z of the unique subgroup of order q acts fixed-point freely. For if $g \in Q$ and g is non-trivial then $\langle z \rangle \leqslant \langle g \rangle$, so $z = g^m$ for some m. If g fixes a point then so does z.

Certainly one direction of this proof is relatively straight forward. We have already shown that if G is a p-group then it has the basis property. Let us then consider a group $G = P \rtimes Q$, where P is a p-group, Q is a non-trivial cyclic q-group, and every non-trivial subgroup of Q acts fixed-point freely on P. The following lemma helps us establish that groups of this form are in fact those from Chapter 4.

Lemma 5.3.3. *Let G be the semidirect product of an elementary abelian p-group P by a cyclic q-subgroup Q. Then the following are equivalent:*

(i) every non-identity element of Q acts fixed-point freely on P,

(ii) $G = P \rtimes Q$ is constructed via the field multiplication in some finite field $\mathbb{F}_{p^n}$.

Proof. (ii) ⇒ (i): Recall from Chapter 4 that if G is constructed via the field multiplication in $\mathbb{F}_{p^n}$ then $G = V \rtimes H$ where V is the additive group of $\mathbb{F}_{p^n}$ and H is the unique subgroup of order q^m embedded in the multiplicative group of $\mathbb{F}_{p^n}$. In the proof of Lemma 4.1.6 we noted that $h \in H$ fixes v when $v(h-1) = 0$ and thus either $h = 1$ or $v = 0$. Hence if $G = P \rtimes Q$ is constructed via the field multiplication in $\mathbb{F}_{p^n}$, then every non-identity element of Q acts fixed-point freely on P.

(i) ⇒ (ii): We begin by assuming that (i) holds and thus every non-trivial subgroup of Q acts fixed-point freely on P. If we view P as an $\mathbb{F}_pQ$-module, by Maschke's Theorem, we can write P as a direct sum of irreducible submodules

$$P = V_1 \oplus V_2 \oplus \cdots \oplus V_k.$$

Now each V_i is a quotient of the group algebra $\mathbb{F}_pQ$ and so $V_i \cong \mathbb{F}_pQ/I_i$ where I_i is a maximal ideal of $\mathbb{F}_pQ$. As I_i is maximal, the quotient $\mathbb{F}_pQ/I_i$ has the structure of a finite field. Since every non-trivial subgroup of Q acts fixed-point freely on P it certainly acts fixed-point freely on V_i. Hence the intersection $Q \cap (1 + I_i)$ is trivial. Thus Q embeds in the multiplicative group of the field $\mathbb{F}_pQ/I_i$ such that the image of Q in this quotient generates it as a field. Therefore each $\mathbb{F}_pQ/I_i$ is isomorphic to the field $\mathbb{F}_{p^r}$ where r is minimal such that $\mathbb{F}_{p^r}$ has a multiplicative subgroup of order q^m as in Lemma 4.1.6 part (i).

As the V_i are all isomorphic to the finite field $\mathbb{F}_{p^r}$ then P can viewed as a direct copy of k copies of $\mathbb{F}_{p^r}$. Here Q acts on each summand by multiplication from its embedding in the multiplicative group of $\mathbb{F}_{p^r}$. From Lemma 4.1.6 part (ii) we see this is true for V, the additive group of the field $\mathbb{F}_{p^{rk}}$, which is the base of our group when it is constructed via field multiplication. Hence P and V are isomorphic as $\mathbb{F}_p Q$-modules we deduce that $P \rtimes Q$ is isomorphic to $V \rtimes Q$ as constructed by the field multiplication in $\mathbb{F}_{p^{rk}}$. □

Returning to our proof of Theorem 5.3.2 remember that $G = P \rtimes Q$, where P is a p-group, Q is a non-trivial cyclic q-group, and every non-identity element of Q acts fixed-point freely on P. Note that if x is an element of Q the set of fixed-points is $\{y \in P \mid y^x = y\} = \{y \in P \mid xy = yx\} = C_P(x)$. Now if H is a subgroup of G then its Sylow p-subgroup $H \cap P$ is normal by the Second Isomorphism Theorem. If $\bar{Q}$ is a Sylow q-subgroup of H then by Sylow's Theorem, $\bar{Q} \leqslant Q^g$ for some element $g \in G$ and if $\bar{x} \in \bar{Q}$ is a non-identity element then $\bar{x} = g^{-1}xg$ for some non-identity element $x \in Q$. Thus the centraliser of $\bar{x}$ in $H \cap P$ is $C_{H \cap P}\left(x^g\right)$, which is contained in $C_P\left(x^g\right)$. This is $C_P\left(x\right)^g$ as P is normal in H and so is trivial as non-identity elements of Q act fixed-point freely on P. Hence all subgroups of G satisfy the hypothesis, so to show that G has the basis property, it is sufficient to show that the hypothesis on G ensures that G has property $\mathcal{B}$.

Claim: Every non-identity element of Q acts fixed-point freely on $P/\Phi\left(P\right)$. We temporarily work in the quotient group $G/\Phi\left(P\right)$. Let x be a non-identity element of Q and R the subgroup $\langle x \rangle$ of Q. Suppose that x has fixed-points in $P/\Phi\left(P\right)$ and let $U = \mathrm{Fix}_{P/\Phi(P)}\left(x\right)$ the set of all such fixed-points. Then

$$\begin{aligned}
U &= \mathrm{Fix}_{P/\Phi(P)}\left(x\right), \\
&= \{\, y \in P/\Phi\left(P\right) \mid x^{y} = x \,\}, \\
&= \{\, y \in P/\Phi\left(P\right) \mid y^{-1}xy = x \,\}, \\
&= \{\, y \in P/\Phi\left(P\right) \mid xy = yx \,\}, \\
&= C_{P/\Phi(P)}\left(x\right).
\end{aligned}$$

By Maschke's Theorem $P/\Phi\left(P\right) = U \oplus W$ when viewed as an $\mathbb{F}_pR$-module. By definition $[U, R] = 0$, as we are working in modules, so if U, the set of fixed points $\mathrm{Fix}_{P/\Phi(P)}\left(x\right)$, is not trivial then $[P\Phi\left(P\right), R] \leqslant W < P/\Phi\left(P\right)$. Thus $[P, R]$ is a proper subgroup of P. Now Theorem 2.1.4 tells us that $P = C_P(R) \cdot [P, R]$ and so $C_P\left(R\right) \neq 1$. Thus $C_P\left(x\right)$ cannot be trivial which contradicts the existence of fixed-points. Thus the claim must hold.

Recall that we are working in the quotient $G/\Phi\left(P\right)$ which is isomorphic $P/\Phi\left(P\right) \rtimes Q$ since $\Phi\left(P\right) \cap Q = 1$. Therefore $P/\Phi\left(P\right)$ is an elementary abelian subgroup and thus by Lemma 5.3.3 the quotient $G/\Phi\left(P\right)$ is constructed via field multiplication and so has property $\mathcal{B}$.

Returning from the quotient to our original group G, we have shown that $G/\Phi\left(P\right)$ is constructed via field multiplication and so $\Phi\left(G/\Phi\left(P\right)\right) = 1$ from Theorem 4.1.4. Hence $\Phi\left(G\right) \leq \Phi\left(P\right)$. However, since P is normal in G, it follows from Lemma 2.1.2 that this is in fact equality. Therefore $G/\Phi\left(G\right)$ has property $\mathcal{B}$ and G has property $\mathcal{B}$ by Lemma 3.1.1.

5.4 Proof of Theorem 5.3.2: The Converse

Let G be a group with the basis property. To prove the converse of Theorem 5.3.2 we use the following proposition.

Proposition 5.4.1. *Let G be a finite group with the basis property. Then $G/\Phi(G)$ is a semidirect product constructed via the multiplication in some field.*

To prove this we begin by assuming that G is a minimal counter example. Since G has the basis property it is soluble by Lemma 5.2.2, and every quotient also has the basis property. Now if $\Phi(G)$ is non-trivial then $G/\Phi(G)$ satisfies the conclusion by the minimality of G and thus so does G. So $\Phi(G)$ is trivial. Any non-identity element must be of prime-power by Lemma 5.2.1 and thus we can apply Theorem 5.3.1. So let p be a prime such that G has a non-trivial normal p-subgroup, and let P be the maximal normal p-subgroup of G. Then G/P is either:

(i) a cyclic q-group, for q a prime other than p,

(ii) a generalised quaternion group and p is odd,

(iii) a group of order $p^a q^b$ with cyclic Sylow subgroups and q is a prime that divides $p^a - 1$.

We begin with Case (ii).

5.4.1 Case (ii): G/P is a generalised quaternion group with p an odd prime

The following lemma helps us show how a group of the form shown in Case (ii) of Higman's Theorem cannot have the basis property.

Lemma 5.4.2. *Let Q be a generalised quaternion group and V be an irreducible $\mathbb{F}_pQ$-module for an odd prime p on which Q acts faithfully. Then the group $V \rtimes Q$ has minimal generating sets of cardinality 2 and 3. In particular, $V \rtimes Q$ does not have property $\mathcal{B}$.*

Proof. Let Q be a generalised quaternion group with presentation

$$\langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, b^{-1}ab = a^{-1} \rangle,$$

and let H be the semidirect product $V \rtimes Q$. If v is a non-zero element of V then $\{a, b, v\}$ is a minimal generating set for H, as omitting either a or b would fail to generate Q and omitting v would only generate Q. As Q acts faithfully on V the action of a on V does not commute with the action of b on V. Thus b is not represented by $-I \in Z(GL(V))$ (where I is the identity matrix) and so there exists $v \in V$ such that $v \neq 0$ and, denoting the action of Q on V by exponentiation, $v^b \neq -v$. Let L be the subgroup of H generated by vb and a. We seek to show this is in fact H. Certainly $VL = H$. Now $(vb)^2 = (v + v^{b^{-1}})b^2$. From the definition of L it contains $a^{2^{n-2}} = b^2 = (vb)^2(v + v^{b^{-1}})^{-1}$ so it follows that L contains $v + v^{b^{-1}} \neq 0$. Hence L contains $\langle v + v^{b^{-1}} \rangle^L = \langle v + v^{b^{-1}} \rangle^{VL} = V$. It follows that $L = H$ and so H has a minimal generating set of size 2. □

Suppose that Case (ii) holds. Let Q be the Sylow 2-subgroup, so $Q \cap P$ is trivial, $G = P \rtimes Q$ and $Q \cong G/P$. We know that quotients of groups with the basis property also have the basis property so we quotient by the Frattini subgroup of P. Thus we can assume P is elementary abelian and so can view it as an $\mathbb{F}_pQ$-module. By Maschke's Theorem P is the direct sum of irreducible submodules. Letting V be one of these irreducible summands of P, we can construct the subgroup $V \rtimes Q$ by the same action of Q on P. This has the basis property as it is a subgroup of $G/\Phi(P)$. Now if there is an element of Q in the kernel of the action of Q on V this element would commute with all elements of V, giving us an element of non-prime-power order in $V \rtimes Q$ — contradicting the fact that $V \rtimes Q$ has the basis property. Thus the action of Q on V is faithful. However Lemma 5.4.2 states such a group, $V \rtimes Q$, does not have the property $\mathcal{B}$. Thus G does not have the basis property and hence Case (ii) does not hold.

5.4.2 Case (iii): $G/P = C_{q^m} \rtimes C_{p^n}$ where $q^m = kp^n + 1$, with no elements of composite order

Again we begin by letting $Q = G/P = C_{q^m} \rtimes C_{p^n}$, with $C_{q^m} = \langle y \rangle$ and $C_{p^n} = \langle x \rangle$. If $m = 0$ then $G = P$ and our group is as in Case (i). Equally if $n = 0$ then G is also as in Case (i), so assume that $m, n \neq 0$. Note that no non-identity elements of $\langle x \rangle$ commute with any non-identity elements of $\langle y \rangle$. Let M be a minimal normal subgroup of G. The following theorem gives us detail on the structure of M.

Theorem 5.4.3. *If M is a non-trivial irreducible $\mathbb{F}_pQ$-module then, when viewed as an $\mathbb{F}_p\langle x \rangle$-module, M is a direct sum of copies of the group algebra $\mathbb{F}_p\langle x \rangle$.*

Proof. We begin the proof by letting $R = \mathbb{F}_p\langle x \rangle$ let π be the projection map from the free $\mathbb{F}_p$-algebra $\mathbb{F}_p[X]$ to R that is defined by $X \mapsto x$.

Claim: R has a chain of submodules $R = R_0 > R_1 > \cdots > R_{p^n} = 0$ where each quotient is trivial as an $\mathbb{F}_p\langle x\rangle$-module.

Note that π is surjective as $X \mapsto x$. Now $X^{p^n} - 1$ lies in $\ker\pi$ and so the ideal $\big(X^{p^n} - 1\big)$ will be contained in $\ker\pi$. The dimension of the quotient of $\mathbb{F}_p[X]$ by an ideal $(f(X))$ is the degree of $f(X)$ and so

$$p^n = \dim \frac{\mathbb{F}_p[X]}{(X^{p^n} - 1)} \geqslant \dim \frac{\mathbb{F}_p[X]}{\ker\pi} = \dim R,$$

by the First Isomorphism Theorem. Note the ideal $\big(X^{p^n} - 1\big) = (X-1)^{p^n}$ as we are in characteristic p. Now $\ker\pi = \Big((X-1)^{p^n}\Big)$, as the dimension of R is p^n, and hence $R \cong \mathbb{F}_p[X]/\Big((X-1)^{p^n}\Big)$ as rings. So as the ring structure of R induces its module structure it follows $\mathbb{F}_p[X]/\Big((X-1)^{p^n}\Big)$ can also be viewed as an $\mathbb{F}_p\langle x\rangle$-module.

Submodules of R are ideals of R and these correspond to ideals of $\mathbb{F}_p[X]$ containing $\Big((X-1)^{p^n}\Big)$. Since $\mathbb{F}_p[X]$ is a principal ideal domain its ideals are of the form $(f(X))$. Such an ideal contains $\Big((X-1)^{p^n}\Big)$ if and only if $f(X)$ divides $(X-1)^{p^n}$, and so $f(X) = (X-1)^i$ where $0 \le i \le p^n$. These ideals form a chain and so we deduce that R has a chain of submodules

$$R = R_0 > R_1 > \cdots > R_{p^n} = 0,$$

where R_i corresponds to $\Big((X-1)^i\Big) \subseteq \mathbb{F}_p[X]$.

Let $\beta(X)$ be an element of the ideal $\Big((X-1)^i\Big)$ of $\mathbb{F}_p[X]$. Then the element $\beta(X)(X-1)$ is contained in the ideal $\Big((X-1)^{i+1}\Big)$ of $\mathbb{F}_p[X]$. So

$$\Big(\Big((X-1)^{i+1}\Big) + \beta(X)\Big)(X-1) = 0,$$

in $\mathbb{F}_p[X]/\left((X-1)^{i+1}\right)$ and hence

$$\left(\left((X-1)^{i+1}\right)+\beta\left(X\right)\right)X=\left((X-1)^{i+1}\right)+\beta\left(X\right).$$

As x acts upon $\mathbb{F}_p[X]/\left((X-1)^{i+1}\right)$ via right multiplication by X, we can conclude that $\left((X-1)^{i}\right)/\left((X-1)^{i+1}\right)$, and hence R_i/R_{i+1}, is a trivial $\mathbb{F}_p\langle x\rangle$-module.

Now observe that the dimension of R_i/R_{i+1} is 1 and so there is a homomorphism $\theta : R_i \to \mathbb{F}_p$ with kernel R_{i+1}. We can also note that an element $\beta \in R_i$ has the form

$$\beta=\sum_{j=i}^{p^n-1} b_j\left(x-1\right)^j,$$

since an element of $\left((X-1)^{i}\right)$ has the form

$$\left(X-1\right)^i g(X)=\sum_{j=i}^{p^n-1} b_j\left(X-1\right)^j+\left(X-1\right)^{p^n}h(X),$$

for some $b_j \in \mathbb{F}_p$ and $h(X)\in\mathbb{F}_p[X]$. Thus θ maps β to b_i.

Claim: $\mathbb{F}_pQ$ has a chain of $\mathbb{F}_pQ$-submodules $S=S_0>S_1>\cdots>S_{p^n}=0$ where $S_i=\bigoplus_{j=0}^{q^m-1}R_iy^j$.

Let $S=\mathbb{F}_pQ$ and define S_i to be $\sum_{j=0}^{q^m-1}R_iy^j$. Now Ry^j is the subspace of S spanned by the set $\left\{y^j, xy^j, x^2y^j, \ldots, x^{p^n-1}\right\}$. Thus S is the direct product $\bigoplus_{j=0}^{q^m-1}Ry^j$ as we are partitioning the basis for S. As $R_iy^j \leqslant Ry^j$ we conclude that S_i is in fact a direct sum $\bigoplus_{j=0}^{q^m-1}R_iy^j$.

Now S_i is closed under addition since for all $r,s\in R_i$ then $ry^j+sy^j=(r+s)y^j\in R_iy^j$. We can also note that S_i is closed under multiplication by y as $R_iy^jy=R_iy^{j+1}$ and so y simply cyclically permutes the summands. Multiplication by x in S_i is as follows

$$R_iy^jx=R_ixx^{-1}y^jx=R_ix^{-1}y^jx,$$

as $R_i x = R_i$ since R_i is an $\mathbb{F}_p\langle x\rangle$-module. As $\langle y\rangle$ is normal in Q then $x^{-1}y^j x = y^k$ for some k. Thus $R_i y^j x = R_i y^k$ and so S_i is closed under multiplication by x. Hence S_i is an $\mathbb{F}_pQ$-submodule.

Recall that $R_i > R_{i+1}$ and so we conclude that $S_i > S_{i+1}$. Hence S has a chain of $\mathbb{F}_pQ$-submodules

$$S = S_0 > S_1 > \cdots > S_{p^n} = 0,$$

with $\dim S_i = q^m \dim R_i = q^m\,(p^n - i)$.

Claim: The quotients S_i/S_{i+1} are all isomorphic to each other.

Take $\Omega = \{\omega_i \mid i \in \{0, 1, \ldots, q^m - 1\}\}$ and let V be a vector space over $\mathbb{F}_p$ with basis Ω. Define $\omega_i y = \omega_{i+1}$ (under addition modulo q^m) and $\omega_i x = \omega_k$ wherever $\left(y^i\right)^x = y^k$. Recall $Q = \langle y\rangle \rtimes \langle x\rangle$ where no non-identity elements of $\langle x\rangle$ commute with any non-identity elements of $\langle y\rangle$. Thus Q has a presentation of the form

$$\langle x, y \mid y^{q^m} = x^{p^n} = 1, x^{-1}yx = y^t\rangle,$$

for some t. Clearly $\omega_i y^{q^m} = \omega_i$. Recall that the action of x on ω_i was defined as $\omega_i x = \omega_k$ wherever $\left(y^i\right)^x = y^k$. Conjugation by x induces a permutation on the elements of $\langle y\rangle$ and so $\left(y^i\right)^{x^{p^n}} = y^i$, thus $\omega_i x^{p^n} = \omega_i$. This gives us a homomorphism $\psi : F \to GL(V)$ where $F = \langle x, y\rangle$ is the free group on two letters. In order to show we have an action we seek to induce a homomorphism $\sigma : Q \to GL(V)$, so we show that the kernel of the natural map $F \to Q$ to be contained in $\ker\psi$. Since $\omega_i y^{q^m} = \omega_i$ and $\omega_i x^{p^n} = \omega_i$ for all i then x^{p^n},$y^{q^m} \in \ker\psi$. However, from the presentation of Q,

$$\ker\sigma = \langle y^{q^m}, x^{p^n}, x^{-1}yxy^{-t}\rangle^F.$$

So to show we have an action we need to show that $\omega_i x^{-1} y x = \omega_i y^t$. This follows from the definition of the action of x and y on the ω_i.

Define $\phi : S_i \to V$ by

$$\sum_{j=0}^{q^m-1} r_j y^j \mapsto \sum_{j=0}^{q^m-1} (r_j\theta)\, \omega_j,$$

where $r_0, \ldots, r_{q^m-1} \in R_i$.

Taking any $s \in S_i$, say $s = \sum_{j=0}^{q^m-1} r_j y^j$, then

$$\begin{aligned} (sy)\,\phi &= \left(\left(\sum_{j=0}^{q^m-1} r_j y^j\right) y\right) \phi, \\ &= \left(\sum_{j=0}^{q^m-1} r_j y^{j+1}\right) \phi, \\ &= \sum_{j=0}^{q^m-1} (r_j\theta)\, \omega_{j+1}, \end{aligned}$$

and

$$\begin{aligned} (s\phi)\, y &= \left(\left(\sum_{j=0}^{q^m-1} r_j y^j\right) \phi\right) y, \\ &= \sum_{j=0}^{q^m-1} (r_j\theta)\, \omega_j y, \\ &= \sum_{j=0}^{q^m-1} (r_j\theta)\, \omega_{j+1}, \end{aligned}$$

under the action of y on Ω. Thus $(sy)\phi = (s\phi)y$ for all $s \in S_i$.

We also calculate

$$\begin{aligned}
(sx)\,\phi &= \left(\left(\sum_{j=0}^{q^m-1} r_j y^j\right) x\right)\phi, \\
&= \left(\sum_{j=0}^{q^m-1} (r_j x)(y^j)^x\right)\phi, \\
&= \sum_{j=0}^{q^m-1} \left((r_j x)\theta\right)\omega_{(y^j)^x}, \\
&= \left(\sum_{j=0}^{q^m-1} (r_j\theta)\omega_{y^j}\right)\cdot x, \\
&= \left(\sum_{j=0}^{q^m-1} r_j y^j\right)\phi\cdot x, \\
&= (s\phi)\,x,
\end{aligned}$$

under the action of x on Ω. Hence $(sx)\phi = (s\phi)x$ and ϕ is an $\mathbb{F}_pQ$ homomorphism. An element $s \in S_i$ lies in the kernel of ϕ if and only if $\sum_{j=0}^{q^m-1} (r_j\theta)\,\omega_j = 0$. Since the ω_i form a basis this is only true if all $r_j\theta$ are zero. This holds if all r_j lie in the kernel of θ which is R_{i+1}. This implies that

$$\ker\phi = \bigoplus_{j=0}^{q^m-1} R_{i+1}y^j = S_{i+1}.$$

Applying the First Isomorphism Theorem we see $S_i/S_{i+1} \cong V$.

Hence $\mathbb{F}_pQ$ can be written as a chain of $\mathbb{F}_pQ$-submodules

$$\mathbb{F}_pQ = S = S_0 > S_1 > S_2 > \cdots > S_{p^n} = 0,$$

with each quotient $S_i/S_{i+1} \cong V$, where V is a vector space over $\mathbb{F}_p$ with basis Ω and the above action of Q on V.

We now investigate the irreducible factors of V.

Proposition 5.4.4. *When viewed as an $\mathbb{F}_pQ$-module, V is a direct sum of irreducible submodules one of which is the trivial module and the rest are direct sums of copies of $\mathbb{F}_p\langle x\rangle$ as $\mathbb{F}_p\langle x\rangle$-modules.*

Proof. First let us view V as an $\mathbb{F}_p\langle y\rangle$-module. The action of y on the ω_i implies that $V \cong \mathbb{F}_p\langle y\rangle$ when viewed as an $\mathbb{F}_p\langle y\rangle$-module. Thus similarly to R earlier

$$V \cong \frac{\mathbb{F}_p[Y]}{(Y^{q^m}-1)},$$

where y acts on the right hand side via multiplication by Y. By Maschke's Theorem V is a direct sum of irreducible $\mathbb{F}_p\langle y\rangle$-modules. Now $Y^{q^m}-1 = f_1(Y)f_2(Y)\dots f_k(Y)$ as a product of irreducible polynomials. These are distinct as the derivative of $Y^{q^m}-1 = q^mY^{q^m-1}$ is co-prime to $Y^{q^m}-1$. So let $g_i(Y)$ be the polynomial

$$g_i(Y) = f_1(Y)\dots f_{i-1}(Y)f_{i+1}(Y)\dots f_k(Y),$$

and $(g_i(Y))$ the ideal it generates. We define $V_i = (g_i(Y))\,/\,\big(Y^{q^m}-1\big)$. We observe here that V_i is a $\mathbb{F}_p\langle y\rangle$-submodule of V.

Claim 1: The V_i are irreducible $\mathbb{F}_p\langle y\rangle$-modules.

Suppose $I = (h(Y))$ is an ideal of $\mathbb{F}_p[Y]$ such that $\big(Y^{q^m}-1\big) \subseteq I \subseteq (g_i(Y))$. So $h(Y)$ divides $Y^{q^m}-1 = g_i(Y)f_i(Y)$ and $g_i(Y)$ divides $h(Y)$. Therefore $h(Y)$ must be equal to $g_i(Y)$ or $Y^{q^m}-1$ up to multiplication by a scalar. Thus I is equal to $(g_i(Y))$ or $I = \big(Y^{q^m}-1\big)$ and hence V_i is an irreducible $\mathbb{F}_p\langle y\rangle$-module.

Claim 2: V is the direct sum $V_1 \oplus \dots \oplus V_k$.

If we take two irreducible summands V_i and V_j with $i \neq j$, then $V_i \neq V_j$

since $f_i(Y) \mid g_j(Y) = f_1(Y) \dots f_i(Y) \dots f_{j-1}(Y) f_{j+1}(Y) \dots f_k(Y)$ but $f_i(Y)$ does not divide $g_i(Y) = f_1(Y) \dots f_{i-1}(Y) f_{i+1}(Y) \dots f_k(Y)$. We now prove that

$$V_1 + \dots + V_i = V_1 \oplus \dots \oplus V_i = \frac{(s_i(Y))}{(Y^{q^m} - 1)},$$

where $s_i(Y)$ is defined to be the polynomial $f_{i+1}(Y) \dots f_k(Y)$. We proceed by induction. Clearly the base case holds by definition as $s_1(Y) = g_1(Y)$. Now assume this holds for i and let

$$W = V_1 \oplus \dots \oplus V_i = \frac{(s_i(Y))}{(Y^{q^m} - 1)}.$$

Since the V_i are irreducible $W \cap V_{i+1}$ is equal to 0 or V_{i+1}. If $W \cap V_{i+1} \neq 0$ then $V_{i+1} \subseteq W$ which implies that $(g_{i+1}(Y)) \subseteq (s_i(Y))$ and so $s_i(Y)$ divides $g_{i+1}(Y)$. However $g_{i+1}(Y)$ does not have $f_{i+1}(Y)$ as a factor, unlike $s_i(Y)$, and so we have a contradiction. Hence $W \cap V_{i+1} = 0$ and

$$V_1 + \dots + V_i + V_{i+1} = W + V_i = W \oplus V_{i+1} = V_1 \oplus \dots \oplus V_{i+1} = \frac{(s_{i+1}(Y))}{(Y^{q^m} - 1)},$$

where $(s_i(Y)) + (g_i(Y)) = (s_{i+1}(Y))$ and $s_{i+1}(Y)$ is defined as

$$s_{i+1}(Y) = \gcd(s_i(Y), g_i(Y)) = f_{i+2}(Y) \dots f_k(Y).$$

This implies that

$$V_1 \oplus \dots \oplus V_k = \frac{(1)}{(Y^{q^m} - 1)} = \frac{\mathbb{F}_p[Y]}{(Y^{q^m} - 1)} = V.$$

Claim 3: $V_i \cong V_j$ if and only if $i \neq j$.

The $\gcd(g_1(Y), \dots, g_{i-1}(Y), g_{i+1}(Y), \dots, g_k(Y))$ is $f_i(Y)$ and thus

$$\begin{aligned} V_i &\cong \frac{V}{V_1 \oplus \dots V_{i-1} \oplus V_{i+1} \oplus \dots \oplus V_k}, \\ &\cong \frac{\mathbb{F}_p[Y]}{(Y^{q^m} - 1)} \Big/ \frac{(f_i(Y))}{(Y^{q^m} - 1)}, \end{aligned}$$

which by the Third Isomorphism Theorem is $\mathbb{F}_p[Y]/\left(f_i(Y)\right)$.

Now $V_i \cong \mathbb{F}_p[Y]/I$ where $I = (f_i(Y))$. Assume that the degree of $f_i(Y)$ is d and that $f_i(Y) = Y^d + c_{d-1}Y^{d-1} + \cdots + c_1Y + c_0$. The elements of V_i can be uniquely expressed as $I + b(Y)$ where the degree of $b(Y)$ is less than the degree of $f_i(Y)$. This holds as for any polynomial $f(Y)$, elements of $\mathbb{F}_p[Y]/\left(f(Y)\right)$ have the form $(f(Y)) + b(Y)$, where the degree of $b(Y)$ is less than the degree of $f(Y)$, as $\mathbb{F}_p[Y]$ is a Euclidean domain. Thus V_i has a basis $B = \left\{I + 1, I + Y, \ldots, I + Y^{d-1}\right\} = \{v_1, v_2, \ldots, v_d\}$ and thus we can consider multiplication by Y as a linear map from V to V where $\left(I + Y^j\right)Y = I + Y^{j+1}$ by the group action. Thus $\left(I + Y^{d-1}\right)Y = I + Y^d = -\sum_{l=0}^{d-1} c_l \left(I + Y^l\right)$ as $f_i(Y)$ is in I. Now the matrix of this linear map with respect to the basis B is the companion matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & c_{d-1} \end{pmatrix},$$

and so the characteristic polynomial of A is the determinant of $Y - A$ which is

$$\begin{vmatrix} Y & -1 & 0 & \cdots & 0 \\ 0 & Y & -1 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ c_0 & c_1 & c_2 & \cdots & Y + c_{d-1} \end{vmatrix}.$$

This is equal to $f_i(Y)$ which we prove by induction on d. For the 1×1 case this holds as the characteristic polynomial is $Y + c_0$ which is $f_i(Y)$ for degree

1. So assume it holds for $d-1$. By expanding down the first column A has characteristic polynomial equal to

$$Y\begin{vmatrix} Y & -1 & 0 & \cdots & 0 \\ 0 & Y & -1 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ c_1 & c_2 & c_3 & \cdots & Y+c_{d-1} \end{vmatrix} + (-1)^{d-1}c_0 \begin{vmatrix} -1 & 0 & \cdots & 0 \\ Y & -1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & Y & -1 \end{vmatrix}.$$

By induction the first part of this equation is equal to

$$Y\left(Y^{d-1}+c_{d-1}Y^{d-2}+\cdots+c_1\right) = Y^d + c_{d-1}Y^{d-1} + \cdots + c_1Y,$$

and the second part involves a upper triangular matrix and so is equal to c_0. Thus the characteristic polynomial is equal to $Y^d + c_{d-1}Y^{d-1} + \cdots + c_1Y + c_0 = f_i(Y)$ as claimed.

If $V_i = \mathbb{F}_p/\left(f_i(Y)\right)$ and $V_j = \mathbb{F}_p/\left(f_j(Y)\right)$ were isomorphic as $\mathbb{F}_p\langle y\rangle$-modules then there would exist an isomorphism $\phi : V_i \to V_j$. Now V_i has basis B from above and so $B\phi$ is a basis for V_j. If v_l is an element of the basis B then $v_l y = \left(I + Y^{l-1}\right)Y = \sum_{k=1}^{d} a_{lk}v_l$ under the action of y where the a_{lk} are elements of the matrix representation A. Thus

$$(v_l\phi)\,y = (v_ly)\,\phi = \left(\sum_{k=1}^{d} a_{lk}v_l\right)\phi = \sum_{k=0}^{d} c_{lk}\,(v_l\phi)\,.$$

Therefore multiplication by y with respect to the bases B on V_i and $B\phi$ on V_j have the same matrix. So the characteristic polynomial of multiplication by y with respect to the bases B on V_i and $B\phi$ on V_j is $f_i(Y)$, and the characteristic polynomial of multiplication by y with respect to the standard basis on V_j is $f_j(Y)$. However characteristic polynomials are independent of basis and so $f_i(Y)$ must equal $f_j(Y)$. But here the $f_i(Y)$ are distinct and thus V_i is not isomorphic to V_j for $i \neq j$.

Claim 4: V is a direct sum of a trivial module and copies of $\mathbb{F}_p\langle x\rangle$ when viewed as an $\mathbb{F}_p\langle x\rangle$-module.

We will now decompose V as an $\mathbb{F}_p\langle x\rangle$-module. Recall that x acts by permuting the ω_i by $\omega_i x = \omega_k$ wherever $\left(y^i\right)^x = y^k$. Thus there exists one orbit of length one, corresponding to conjugating the identity. Recall our observation that no non-identity element of $\langle x\rangle$ commutes with any non-identity element of $\langle y\rangle$. Thus no non-identity element of $\langle x\rangle$ fixes any non-identity element of $\langle y\rangle$. Therefore all stabilisers of non-identity powers y^i are trivial and so the Orbit-Stabiliser Theorem tells that all other orbits are of length p^n. So take an index set $\left\{j_0, j_1, \ldots, j_{(q^m-1)/p^n}\right\}$ such that

$$\left\{y^{j_0}, y^{j_1}, \ldots, y^{j_{(q^m-1)/p^n}}\right\},$$

are representations for these orbits, with $j_0 = 0$ and $y^{j_0} = 1$ corresponding to the orbit of length one. It is worth noting here that $\omega_i \mapsto y^i$ is an $\langle x\rangle$-isomorphism from Ω to $\langle y\rangle$, where this is an isomorphism of sets acted upon by the group $\langle x\rangle$. We can see this is an $\langle x\rangle$-isomorphism from the definition of the action x on Ω as $\omega_i x = \omega_k$ wherever $\left(y^i\right)^x = y^k$.

Let $W_i = \text{Span}\left\{\omega_{j_i}, \omega_{j_i}\cdot x, \omega_{j_i}\cdot x^2, \ldots, \omega_{j_i}\cdot x^{p^n-1}\right\}$. As $\langle x\rangle$ acts regularly on the set $\left\{\omega_{j_i}, \omega_{j_i}\cdot x, \omega_{j_i}\cdot x^2, \ldots, \omega_{j_i}\cdot x^{p^n-1}\right\}$ we can see that each W_i is isomorphic to $\mathbb{F}_p\langle x\rangle$ as an $\mathbb{F}_p\langle x\rangle$-module. Hence $V = W_0 \oplus W_1 \oplus \cdots \oplus W_{(q^m-1)/p^n}$ as an $\mathbb{F}_p\langle x\rangle$-module. Note that this is a direct sum as we have a partition of the basis of Ω.

Let L be an irreducible $\mathbb{F}_pQ$-submodule of V and let N be an irreducible $\mathbb{F}_p\langle y\rangle$-submodule of L and thus V. Now V is a direct sum of k pairwise non-isomorphic irreducible $\mathbb{F}_p\langle y\rangle$-submodules from Claims 1,2 and 3. So we can define $\pi_i : V \to V_i$ to be the natural projection map. Since N is not zero $N\pi_i = V_i$, for some i, and since N is irreducible $\ker \pi_i = 0$. Thus $N \cong V_i$ as an $\mathbb{F}_p\langle y\rangle$-module. Since $V_i \ncong V_j$ for all $i \neq j$, if $N\pi_j \neq 0$ the same argument as before tells us that $\ker \pi_j = 0$ and $N \cong V_j$ implying that $i = j$ by assumption on the V_i. Thus $N\pi_j = 0$ for $j \neq i$ and $N \leqslant V_i$. Since V_i is irreducible as an $\mathbb{F}_p\langle y\rangle$-module N must equal V_i.

By Clifford's Theorem part (i) there exists a set $\{i_1, \dots i_d\}$ such that $L = V_{i_1} \oplus \cdots \oplus V_{i_d}$ with each V_{i_j} a different irreducible $\mathbb{F}_p\langle y\rangle$-submodule of L. Since the V_i are pairwise non-isomorphic the homogeneous components of L are the V_{i_j}. Thus part (iii) of Clifford's Theorem tells us that Q permutes these V_{i_j} transitively and thus $\{V_{i_1}, \dots, V_{i_d}\}$ is an $\langle x\rangle$-orbit. Therefore we conclude that an irreducible $\mathbb{F}_pQ$-submodule L of V is a direct sum of some $\langle x\rangle$-orbit on $\{V_1 \dots, V_k\}$. So let $\{M_1, \dots, M_r\}$ be the set of all such irreducible $\mathbb{F}_pQ$-submodules L. Since $V = V_1 \oplus \cdots \oplus V_k$ we see that

$$V = M_1 \oplus \cdots \oplus M_r. \tag{5.1}$$

Remember that the decomposition of V into irreducible $\mathbb{F}_p\langle x\rangle$-modules is

$$V = W_0 \oplus W_1 \oplus \cdots \oplus W_{(q^m-1)/p^n}. \tag{5.2}$$

The Krull–Schmidt Theorem tells us that any two decompositions of V into a direct sum of irreducible submodules are the same length. Thus we see that equation (5.2) is a refinement of equation (5.1) and so each M_i is a direct sum of copies of the W_j.

Since only W_0 is trivial we conclude only one of the W_i is a trivial $\mathbb{F}_p\langle x\rangle$-module and all the others are copies of $\mathbb{F}_p\langle x\rangle$. Thus V is a direct sum of irreducible $\mathbb{F}_pQ$-submodules which are a trivial module and submodules which are direct sums of copies of $\mathbb{F}_p\langle x\rangle$ when viewed as an $\mathbb{F}_p\langle x\rangle$-module.

□

We now conclude the proof of Theorem 5.4.3. If M is an irreducible $\mathbb{F}_pQ$-module it is isomorphic to a composition factor of S and hence isomorphic to a composition factor of S_i/S_{i+1}, as S has a chain of submodules $S = \mathbb{F}_pQ = S_0 > S_1 > S_2 > \cdots > S_{p^n} = 0$. As S_i/S_{i+1} is isomorphic to V this M is isomorphic to a composition factor of V, i.e. one of the M_i. Thus the conclusion is proved. □

Recall that M is a minimal normal subgroup of G with $Q = G/P = C_{q^m} \rtimes C_{p^n} = \langle y \rangle \rtimes \langle x \rangle$ and P the largest normal p-subgroup of G. Now as $\Phi(G) = 1$ we note that $\Phi(P) = 1$, by Lemma 2.1.2 (i), and thus P is elementary abelian.

Claim: $M = P$.

Assume $M \neq P$ then $M < P$. By assumption on the minimality of G, G/M is not a counter example to Theorem 5.3.2 nor a p-group, as $m \neq 0$. Therefore G/M satisfies the conclusion of Theorem 5.3.2 and so $G/\Phi(G)$ is constructed via field multiplication. Hence G/M is of the form of Theorem 4.2.1. So G/M is either the semidirect product of a Sylow q-subgroup by a Sylow p-subgroup or the semidirect product of a Sylow p-subgroup by a Sylow q-subgroup. If it is the first case then G/M has a non-trivial normal q-subgroup QM/M and a non-trivial normal p-subgroup P/M. These commute as $G/M = QM/M \times P/M$, $QM/M \cap P/M = 1$ and both QM/M and P/M are normal in G/M. Thus G/M does not have the basis property. If the second case holds G/P has normal Sylow subgroups for both primes p and q. This implies G/P is the direct product of these two Sylow subgroups and so G/P contains elements of composite order and hence does not have the basis property. This contradicts the assumption that G has the basis property.

Hence $M = P$ and so P is a minimal normal subgroup of G. As $\Phi(G)$ is trivial there exists a maximal subgroup such that P is not contained in this maximal subgroup. This maximal subgroup is a complement for P as it is maximal. Hence G is the semidirect product $P \rtimes Q$ with $Q = G/P = C_{q^m} \rtimes C_{p^n} = \langle y \rangle \rtimes \langle x \rangle$. We can see that G will be generated minimally by three elements $\{z, y, x\}$ where z is a non-trivial element of P. If P is trivial as an $\mathbb{F}_pQ$-module then z and y commute and so zy is an element of order pq^m. Hence G would be minimally generated by two elements $\{zy, x\}$ and so G would have neither property $\mathcal{B}$ nor the basis property.

Assume that P is a non-trivial $\mathbb{F}_pQ$-module. By Theorem 5.4.3 $P = W_1 \oplus \cdots \oplus W_t$ as a direct sum of copies of $\mathbb{F}_p\langle x \rangle$ when viewed as an $\mathbb{F}_p\langle x \rangle$-module. Take z to be a generator of W_1 as an $\mathbb{F}_p\langle x \rangle$-module. Now

$$A := \langle z, x \rangle = W_1 \rtimes \langle x \rangle = C_p \wr C_{p^n},$$

as $\mathbb{F}_p\langle x \rangle = \mathbb{F}_p \oplus \mathbb{F}_p x \oplus \mathbb{F}_p x^2 \oplus \cdots \oplus \mathbb{F}_p x^{p^n-1}$.

Claim: In A there exists an element a of order p^{n+1}.

We begin by showing that $(zx)^k = zz^{x^{-1}}z^{x^{-2}} \cdots z^{x^{-(k-1)}}x^k$. Proceed by induction on k. Clearly this holds for $k = 1$ and in fact holds for $k = 2$ as $(zx)^2 = zxzx = zxzx^{-1}xx = zz^{x^{-1}}x^2$, so assume that this holds for $k - 1$.

Thus

$$\begin{aligned}
(zx)^k &= (zx)^{k-1}(zx), \\
&= zz^{x^{-1}}z^{x^{-2}}\cdots z^{x^{-(k-2)}}x^{k-1}(zx), \\
&= zz^{x^{-1}}z^{x^{-2}}\cdots z^{x^{-(k-2)}}x^{k-1}zx^{-(k-1)}x^{k-1}x, \\
&= zz^{x^{-1}}z^{x^{-2}}\cdots z^{x^{-(k-2)}}z^{x^{-(k-1)}}x^k.
\end{aligned}$$

Hence $(zx)^{p^n} = zz^{x^{-1}}z^{x^{-2}}\cdots z^{x^{-(p^n-1)}}x^{p^n} = zz^{x^{-1}}z^{x^{-2}}\cdots z^{x^{-(p^n-1)}}$. Now as W_1 is a direct summand we work additively so, $W_1 = \mathbb{F}_p z + \mathbb{F}_p z^x + \mathbb{F}_p z^{x^2} + \cdots + \mathbb{F}_p z^{x^{p^n-1}}$ and is spanned by all such elements $\left\{z, z^x, \ldots, z^{x^{p^n-1}}\right\}$. Thus $(zx)^{p^n}$ is the sum of the basis vectors of W_1 and so is non-trivial. Now W_1 is normal in A with quotient $A/W_1 \cong C_{p^n}$. So for any element g of A then $g^{p^n} \in W_1$ which is elementary abelian p-group and so $g^{p^{n+1}}$ is trivial. Thus $(zx)^{p^{n+1}}$ is trivial and hence $a = (zx)$ is our required element.

Now we have observed that a^{p^n} is a non-trivial element of P. As P is a minimal normal subgroup, $\langle a^{p^n}\rangle^G = P$. Therefore

$$\langle a^{p^n}\rangle^{P\langle x,y\rangle} = \langle a^{p^n}\rangle^{P\langle a,y\rangle} = \langle a^{p^n}\rangle^{\langle a,y\rangle} = P.$$

Thus $\langle a, y\rangle \geqslant P$ and so $\langle a, y\rangle \geqslant P\langle a, y\rangle = G$. Therefore $z, x \in \langle a, y\rangle$ and so G is minimally generated by a and y. Thus G, a group of the form described in case (ii) of Higman's Theorem, does not have the basis property.

5.4.3 Case (i): G/P is a cyclic q-group with q a prime not equal to p

Let G be as in case (i) of Higman's Theorem and so a semidirect product of a p-subgroup P by a cyclic q-subgroup Q. Since $\Phi(G) = 1$ we have that $\Phi(P) = 1$ and thus P is elementary abelian. If any element of Q centralises a non-identity element of P then we would have an element not of prime-power order, contradicting the fact that G has the basis property. Thus every non-identity element of Q acts fixed-point freely on P. Applying Lemma 5.3.3 we see that G is constructed via the field multiplication in some field $\mathbb{F}_q$. Thus we have shown Proposition 5.4.1 holds.

5.4.4 Concluding Theorem 5.3.2

From Proposition 5.4.1 we can see that if G is a finite group with the basis property then $G/\Phi(G)$ is constructed via multiplication in some finite field. If a group has the basis property it certainly has property $\mathcal{B}$, thus G is of the form described in Theorem 4.2.1. So $G = P \rtimes Q$ where P is the unique Sylow p-subgroup and Q is any cyclic Sylow q-subgroup of G. It remains to show that every non-identity element y of Q acts fixed-point freely on P. As G has the basis property it contains no elements of co-prime order. Thus no element of Q centralises a non-identity element of P, as it would imply there exist elements of co-prime order. Hence we conclude that no non-identity element of Q acts fixed-point freely on P and so Theorem 5.3.2 holds.

Chapter 6

Conclusions and Future Work

In this chapter we summarise the main results of the thesis. Throughout we provide a series of open questions that, if solved, would give further insight in to the nature of the properties we have presented.

In Chapter 3 we began our work on property $\mathcal{B}$. By presenting a few examples of groups that do and do not have property $\mathcal{B}$ we sought to highlight how rare groups with property $\mathcal{B}$ are. Following on from Burnside's Basis Theorem we quickly noted that all p-groups had property $\mathcal{B}$. The main example of non-p-groups with property $\mathcal{B}$ given was that of the class of dihedral groups, showing that all dihedral groups of order $2p^n$ have property $\mathcal{B}$, for p an odd prime. As a counter example we then showed that for $n > 3$ all symmetric groups, S_n, do not have property $\mathcal{B}$.

The first main result we presented was the following lemma which shows that property $\mathcal{B}$ transfers from the group to its quotient by the Frattini subgroup.

Lemma 3.1.1. *A group G has property $\mathcal{B}$ if and only if $G/\Phi(G)$ has property $\mathcal{B}$.*

This lemma is useful as it aids in providing a classification of groups with property $\mathcal{B}$. For example, it allowed us to focus on constructing groups with property $\mathcal{B}$ and trivial Frattini subgroup, and then look at groups with quotient by the Frattini subgroup isomorphic to our construction. In general subgroup and quotient inheritance is useful as it gives us greater understanding of the structure of a group and often makes a classification much simpler. However given examples such as Example 3.2.1, we know that property $\mathcal{B}$ is not inherited by subgroups. This leads us to our first open question.

Question 6.0.5. *Under what conditions is property $\mathcal{B}$ inherited by subgroups?*

Whilst this is the basis property, were we to find other conditions in which property $\mathcal{B}$ is inherited by subgroups we could then use our classification of groups with the basis property (Theorem 5.3.2) to further investigate the basis property. For example if a group has property $\mathcal{B}$ and trivial Frattini subgroup does that imply the group has the basis property?

Throughout the rest of Chapter 3 we focused on inheritance by quotients. Lemma 3.1.1 also holds for the basis property; in fact we were able to show that all quotients of groups with the basis property have the basis property. However it is uncertain whether this is the case for property $\mathcal{B}$, as we were only able to prove that the quotients of groups with property $\mathcal{B}$ inherited property $\mathcal{B}$ under certain circumstances.

Lemma 3.2.2. *If G is a group with property $\mathcal{B}$ and G splits over a minimal normal subgroup M then G/M has property $\mathcal{B}$.*

Proposition 3.2.3. *If G is a group with property $\mathcal{B}$ and M is an abelian minimal normal subgroup of G then G/M has property $\mathcal{B}$.*

Corollary 3.2.4. *If G is a soluble group with property $\mathcal{B}$ then any quotient G/N also has property $\mathcal{B}$.*

From these three results we can see that quotients inherit property $\mathcal{B}$ under a strict set of conditions leading us naturally in to a second open question.

Question 6.0.6. *Is property $\mathcal{B}$ always inherited by quotients?*

All our examples of groups with property $\mathcal{B}$ have been soluble implying this question may have a positive answer. Despite not having a positive answer to Question 6.0.6 in general the previous three results do help us towards a classification. For example we can note that quotients of any soluble group do inherit property $\mathcal{B}$. This leads us to another open question, which were we to solve it, would make a classification easier.

Question 6.0.7. *Are all groups with property $\mathcal{B}$ soluble?*

It should be noted that a positive answer to this question would answer Question 6.0.6. Given that all non-abelian simple groups do not have property $\mathcal{B}$ (Example 3.2.5) and that the symmetric groups on four or more points also do not have property $\mathcal{B}$ (Proposition 3.1.5) it seems likely that the answer to Question 6.0.7 is yes. To begin to answer this question the first obvious step would be to investigate whether or not all almost simple groups have property $\mathcal{B}$. Note A is an almost simple group if there exists a non-abelian simple subgroup S of A such that $S \leqslant A \leqslant \mathrm{Aut}(S)$.

The large number of counter examples we have come across have led us to the conclusion that groups with property $\mathcal{B}$ are rare. The final result of Chapter 3 further emphasises this.

Theorem 3.3.1. *The group $G \times H$ has property $\mathcal{B}$ if and only if $G \times H$ is a p-group.*

This result places a great restriction on the structure of a group with property $\mathcal{B}$ leading us to consider how a class of groups with property $\mathcal{B}$ may look.

Following on from this, in Chapter 4 we sought to construct a class of groups with property $\mathcal{B}$. The inspiration for this was the work of Scapellato and Verardi [10] whose classification of matroid groups closely matched the only class of groups we had found that all had property $\mathcal{B}$, namely the dihedral groups of order $2p^n$. Identifying the form of these dihedral groups as $C_{p^n} \rtimes C_2$, where the cyclic 2-group acts by inversion, we were able to generalise to construct a class of groups with property $\mathcal{B}$, shown in the following theorem.

Theorem 4.1.4. *Let V be the additive group of the field $\mathbb{F}_{p^n}$ of p^n elements and H the subgroup of the multiplicative group $\mathbb{F}_{p^n}^{\star}$ of order q^m. Define G to be the semidirect product $V \rtimes_{\phi} H$ where H acts on V by multiplication in $\mathbb{F}_{p^n}$. Then:*

(i) G has property $\mathcal{B}$,

(ii) $d(G) = k + 1$ *where* V *is a direct sum of* k *irreducible* $\mathbb{F}_p H$*-modules,*

(iii) $\Phi(G)$ *is trivial.*

Our result that quotients by the Frattini subgroup inherit property $\mathcal{B}$ gave us a next natural step. Given that a group G has property $\mathcal{B}$ if and only if $G/\Phi(G)$ also has property $\mathcal{B}$, then if $G/\Phi(G)$ was isomorphic to a group of the form described in Theorem 4.1.4 we would know that G must have property $\mathcal{B}$. Thus we could construct a much larger class of groups with property $\mathcal{B}$.

Theorem 4.2.1. *Let* V *be the additive group of the field* $\mathbb{F}_{p^n}$ *of* p^n *elements and* H *the subgroup of the multiplicative group* $\mathbb{F}^{\star}_{p^n}$ *of order* q^m*. Let* G *be any group such that* $G/\Phi(G)$ *is isomorphic to the semidirect product* $V \rtimes_{\phi} H$ *where* H *acts on* V *via the multiplication in* $\mathbb{F}_{p^n}$*. Then:*

(i) G *has a unique Sylow* p*-subgroup* P*,*

(ii) G *is the semidirect product of* P *by* Q *for any Sylow* q*-subgroup* Q*. All Sylow* q*-subgroups of* G *are cyclic,*

(iii) $\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$ *where* $\langle x^{q^m} \rangle$ *is the subgroup of index* q^m *in* $Q = \langle x \rangle$*. In fact* x^{q^m} *lies in the centre of* G*.*

All examples of groups with property $\mathcal{B}$ provided in this thesis are of this form, with Theorem 4.2.1 being a generalisation of Theorem 4.1.4. In fact further analysis in GAP using a simple brute force algorithm has shown that for order less than 500 if a group has property $\mathcal{B}$ it is of this form. Due to computational limitations any further examination would require a more targeted approach, focusing on group shape as well as order. This leads us in to our next open question.

Question 6.0.8. *If G is a group with property $\mathcal{B}$ and trivial Frattini subgroup, is it of the form described in Theorem 4.1.4?*

A first step to answering this question may be to proceed by induction on the group order of a soluble group G with trivial Frattini subgroup. Assume that if any group with property $\mathcal{B}$ is of order less than G then it is either a q-group (for some prime q) of the form in Theorem 4.1.4 if its Frattini subgroup is trivial, or of the form of Theorem 4.2.1 otherwise. If M is a minimal normal subgroup of G then as G is soluble M would be elementary abelian. We would continue by considering several cases on the structure of M and G/M which would have property $\mathcal{B}$ by Corollary 3.2.4. Thus, for p and q distinct primes, we would have the following cases.

(i) M is an elementary abelian q-group and G/M is a q-group,

(ii) M is an elementary abelian q-group and G/M is a p-group,

(iii) M is an elementary abelian q-group and G/M is the semidirect product of a p-group by a cyclic q-group (p,q distinct primes),

(iv) M is an elementary abelian q-group and G/M is the semidirect product of a q-group by a cyclic p-group (p,q distinct primes),

(v) M is an elementary abelian r-group and G/M is the semidirect product of a q-group by a cyclic p-group (p,q and r distinct primes).

Note that case (i) implies that G is a q-group and thus has property $\mathcal{B}$. This fits in with any expected classification theorem of groups with property $\mathcal{B}$.

We have made some progress in these cases.

Lemma 6.0.9 (Progress in Case (ii))**.** *Suppose G is a soluble group with property $\mathcal{B}$ and $\Phi(G) = 1$ and assume that such a group of order less than G is either a q-group (for some prime q), of the form in Theorem 4.1.4 if its Frattini subgroup is trivial, or of the form of Theorem 4.2.1 otherwise. If $G = M \rtimes_{\phi} P$ is the semidirect product of an elementary abelian q-group M by a cyclic p-group P then* $\ker\phi$ *is trivial.*

Proof. Let $K = \ker\phi$ and assume that $K \neq 1$. Clearly $K < P$ otherwise G would equal $M \times P$ and G could not have property $\mathcal{B}$ by Theorem 3.3.1. Also note that M is not a maximal subgroup of G as $M < MK < MP = G$. Let H be any maximal subgroup of G. Then H is not contained in the unique Sylow q-subgroup of G and so p divides the order of H and H contains an element h of order p. Thus $\langle h\rangle^g \leqslant P$ for some element $g \in G$. This implies that $\langle h\rangle^g$ is the unique subgroup of order p in P as P is cyclic. Therefore $\langle h\rangle^g$ must be contained in K as K is a non-trivial subgroup of P, and thus $\langle h\rangle \leqslant K^{g^{-1}} = K$. Thus $\langle h\rangle$ is the unique subgroup of order p in K. Note K is normal in G as, by definition, it commutes with M and is normal in P. This implies that every maximal subgroup of G contains the unique subgroup of K of order p and thus the intersection of these maximal subgroups is non-trivial. However this contradicts the assumption that $\Phi(G) = 1$, and so $\ker\phi$ is trivial. □

Theorem 6.0.10 (Progress in Case (iii))**.** *Suppose G is a soluble group with property $\mathcal{B}$ and $\Phi(G) = 1$ and assume that such a group of order less than G is either a q-group (for some prime q), of the form in Theorem 4.1.4 if* *its Frattini subgroup is trivial, or of the form of Theorem 4.2.1 otherwise. If* $G = M \rtimes_{\phi} H$ *is a semidirect product with* M *an elementary abelian* q*-group and* $H \cong P \rtimes Q$ *where* P *is a* p*-group and* Q *a cyclic* q*-group, then* $\ker \phi$ *is trivial.*

Proof. Let $K = \ker \phi$ and assume that $K \neq 1$. Note that $H = PQ$ and since $H = G/M$ and G is soluble Corollary 3.2.4 tells us that H has property $\mathcal{B}$. Now $P/\Phi(P)$ is an elementary abelian p-group and so is a direct sum $V_1 \oplus \cdots \oplus V_k$ as an $\mathbb{F}_p Q$-module.

Claim: $P \cap K$ is trivial.

Suppose $P \cap K$ is non-trivial and suppose $y_1 \in (P \cap K) \backslash \Phi(P)$. As $P/\Phi(P)$ is an elementary abelian p-group it has the structure of a vector space over $\mathbb{F}_p$ and so we can extend y_1 to form a basis

$$\{y_1 \Phi(P), y_2 \Phi(P), \ldots, y_k \Phi(P)\},$$

for $P/\Phi(P)$. Then $P = \langle y_1, y_2, \ldots, y_k, \Phi(P) \rangle$ which is just $\langle y_1, y_2, \ldots, y_k \rangle$, as $\Phi(P)$ is the set of non-generators of P. Note that $\{y_1, y_2, \ldots, y_k\}$ is a minimal generating set for P as $\{y_1 \Phi(P), y_2 \Phi(P), \ldots, y_k \Phi(P)\}$ is a basis for $P/\Phi(P)$. Now y_1 lies in $P \cap K$ and so commutes with M. Thus we can pick any non-identity element z of M and a generator x for Q. Then $\{x, y_1, y_2, \ldots, y_k, z\}$ is a minimal generating set for G as removing x or z would fail to generate Q and M respectively, and removing a y_i would fail to generate P as they form a minimal generating set for P. Thus we have a minimal generating set of size $k + 2$ for G. However as y_1 and M, in particular $z \in M$, commute we can replace y_1 and z in the generating set by $y_1 z$. Thus $\{x, y_2, \ldots, y_k, y_1 z\}$ is a minimal generating set for G of size $k+1$ contradicting the assumption that G has property $\mathcal{B}$. Therefore $P \cap K \leqslant \Phi(P)$.

Since P and K are both normal in H we can deduce that $P \cap K$ is also normal in H. In fact as ϕ is the homomorphism from $H \to \mathrm{Aut}(M)$ then $P \cap K$ is normal in G. Recall that our inductive hypothesis states that as $G/(P \cap K)$ is of order less than G it is either a group of prime-power order or a semidirect product of the form specified in Theorem 4.2.1. Now we can note that as $P \cap K$ is contained in the Frattini subgroup of P, both p and q must divide the order of $G/(P \cap K)$. Hence $G/(P \cap K)$ is not a group of prime-power order so we can assume that $G/(P \cap K)$ is of the form specified in Theorem 4.2.1. Thus $G/(P \cap K)$ has a normal Sylow subgroup of prime-power order. Now if $G/(P \cap K)$ has a normal Sylow q-subgroup so does $G/M(P \cap K)$. Note that $M(P \cap K)$ is normal in G and $M(P \cap K)$, so $M(P \cap K)$ corresponds to a normal subgroup of $G/M = H$. This normal subgroup of G/M is,

$$\begin{aligned} M(P \cap K) \cap H &= (P \cap K)(M \cap H), \text{ (by Dedekind's Modular Law)} \\ &= P \cap K, \end{aligned}$$

and thus

$$\frac{G}{M(P \cap K)} \cong \frac{H}{P \cap K}.$$

But $H/(P \cap K)$ has a normal p-subgroup, namely $P/(P \cap K)$. Thus $H/(P \cap K)$ has a normal Sylow p-subgroup and a normal Sylow q-subgroup which commute and so we have elements of composite order. But $H/(P \cap K)$ has property $\mathcal{B}$ by Corollary 3.2.4 and so we get a contradiction.

If $G/(P \cap K)$ has a normal Sylow p-subgroup then it would be $P/(P \cap$

K). From the Correspondence Theorem we can conclude that P must be normal in G. Now $[M,P] \leqslant M \cap P = 1$ as M is normal in G. Thus M and P commute which gives us commuting generators of co-prime order, contradicting the assumption that G has property $\mathcal{B}$. Hence $P \cap K$ is trivial.

So K is a q-group. Applying Sylow's Theorem $K \leqslant Q^g$ so $K^{g^{-1}} \leqslant Q$. Thus $K \leqslant Q$ since K is normal in G as by definition it commutes with M and is normal in H. As K is non-trivial, by induction $G/K = M \rtimes (H/K)$ has a normal Sylow subgroup with the other cyclic. If this is a normal Sylow q-subgroup then Q/K is normal in H/K and by the Correspondence Theorem Q is normal in H, contradicting the fact that H has property $\mathcal{B}$ as Q would now commute with P. Thus G/K has a normal Sylow p-subgroup and a cyclic Sylow q-subgroup $M \rtimes Q/K$. Since M is elementary abelian then Q/K is trivial and so $Q = K$. Thus Q is normal in H giving the same contradiction as before, and $K = \ker \phi$ is trivial. □

Therefore we have shown that M is a faithful $\mathbb{F}_q H$-module. This actually links in with Section 5.4.2 where we showed that a group G with normal subgroup P and $G/P = C_{q^m} \rtimes C_{p^n}$ where $q^m = kp^n + 1$, with no elements of composite order does not have the basis property. Generalising this result would be the main element of solving Case (iii).

Our final results chapter saw us switch focus to look at the basis property. As we have already mentioned, work by Jones [7] has already provided a solid foundation in describing the structure of groups with the basis property.

Lemma 5.2.1. *If G is a group with the basis property then G consists of elements of prime-power order.*

Lemma 5.2.2. *If G is a group with the basis property then G is soluble.*

Corollary 5.2.3. *If G is a group with the basis property then any homomorphic image of G has the basis property.*

Using this as a first step and linking in with the citations in Jones' paper we saw that Higman's 1956 paper [5] would be a useful basis, as it provided a classification of all finite soluble groups where every element is of prime-power order. As a result we were able to provide a classification of all groups with the basis property.

Theorem 5.3.2. *Let G be a finite group. Then G has the basis property if and only if either:*

(i) G is a p-group, or

(ii) $G = P \rtimes Q$ where P is a p-group, Q a non-trivial cyclic q-group, and every non-identity element of Q acts fixed-point freely on P.

Being able to classify all groups with the basis property brings up the obvious question of what other algebraic structures have the basis property and for that matter property $\mathcal{B}$. If we were to consider looking at infinite groups then obviously we would be restricted to looking at finitely generated groups. We can note immediately the following example.

Example 6.0.11. *The infinite cyclic group, isomorphic to the integers under addition does not have property $\mathcal{B}$.*

Proof. Clearly $d(\mathbb{Z}) = 1$ as $\mathbb{Z}$ has a minimal generating set $\{1\}$. We can also note that for two co-prime integers p and q, $\{p, q\}$ is also a minimal generating set for $\mathbb{Z}$. This follows from the identity $ap + bq = gcd(p, q)$. Thus $\mathbb{Z}$ does not have property $\mathcal{B}$. □

If we were to look at other algebraic structures with the basis property a starting place would be two papers [6] and [7] by Jones. As mentioned in the Introduction, Jones' work on inverse semigroups provides the following classification for inverse semigroups with the strong basis property. Recall that if a semigroup has the strong basis property it also has the basis property but not vice versa.

Theorem 6.0.12. *[7, Theorem 4.8] An inverse semigroup has the strong basis property if and only if:*

(i) it is completely semisimple,

(ii) each non-isolated maximal subgroup is a primary $\tilde{N}$-group,

(iii) each isolated maximal subgroup has the strong basis property.

Note that a maximal subgroup of an inverse semigroup is *isolated* if it constitutes a whole $\mathcal{D}$ class, otherwise it is *non-isolated.* A group G is an *$\tilde{N}$-group* if for any subgroups H and K of G, H is maximal in K implies H is normal in K. Jones also provides a classification for Brandt semigroups with the basis property.

Theorem 6.0.13. *[7, Theorem 6.1] Let S be a Brandt semigroup with maximal (non-zero) subgroup G. Then S has the basis property if and only if G does.*

However Jones only mentions property $\mathcal{B}$ (called the *generating property* in [7]) in reference to groups. In our work constructing examples of groups with property $\mathcal{B}$ gave us the motivation to look at classifying groups with the basis property. Perhaps one starting point would be to construct examples of monoids and semigroups with property $\mathcal{B}$ before going on to look at the basis property for all semigroups, not just inverse semigroups. The following Lemma provides a class of semigroups with property $\mathcal{B}$.

Lemma 6.0.14. *Let $S = \langle x \mid x^a = x^b \rangle$ be a monogenic semigroup with a and b not equal to 1. Then S has property $\mathcal{B}$.*

Proof. Let S be a monogenic semigroup with has presentation $S = \langle x \mid x^a = x^b \rangle$, with a and b integers such that $a > b > 1$. By definition S is generated by a single element, x, so take A to be any generating set of size greater than 1. Now A must contain x in order to generate x as no other power of x is equal to x and thus S has property $\mathcal{B}$. □

However not all finite monogenic semigroups have property $\mathcal{B}$. For example the cyclic groups of composite order are also monogenic semigroups and by Lemma 3.1.2 do not have property $\mathcal{B}$.

Bibliography

[1] Ahmad Al′-Khalaf. Finite groups with the basis property. *Dokl. Akad. Nauk BSSR*, 33(11):972–974, 1051, 1989.

[2] Abdulla Aljouiee. Basis property conditions on some groups. *Int. J. Math. Comput. Sci.*, 3(3):173–183, 2008.

[3] Daniel Gorenstein. *Finite Groups.* Chelsea Publishing Company, second edition, 1980.

[4] Robert M. Guralnick and William M. Kantor. Probabilistic generation of finite simple groups. *J. Algebra*, 234(2):743–792, 2000. Special issue in honor of Helmut Wielandt.

[5] Graham Higman. Finite groups in which every element has prime power order. *J. London Math. Soc.*, 32:335–342, 1957.

[6] Peter R. Jones. A basis theorem for free inverse semigroups. *J. Algebra*, 49(1):172–190, 1977.

[7] Peter R. Jones. Basis properties for inverse semigroups. *J. Algebra*, 50(1):135–152, 1978.

[8] Derek J. S. Robinson. *A Course in the Theory of Groups.* Springer, second edition, 1995.

[9] Raffaele Scapellato and Libero Verardi. Sur les ensembles générateurs minimaux d'un groupe fini. *Ann. Sci. Univ. Clermont-Ferrand II Math.*, 26:51–60, 1990.

[10] Raffaele Scapellato and Libero Verardi. Groupes finis qui jouissent d'une propriété analogue au théorème des bases de Burnside. *Boll. Un. Mat. Ital. A (7)*, 5(2):187–194, 1991.

[11] Raffaele Scapellato and Libero Verardi. Bases of certain finite groups. *Ann. Math. Blaise Pascal*, 1(2):85–93, 1994.

[12] John G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.