3

Model Subgroups of Finite Soluble Groups

Ben Carr

A thesis submitted to the University of Warwick for the degree of Doctor of Philosophy

Mathematics Institute
University of Warwick

December 1998

Contents

Acknowledgements

Firstly, I would like to thank my supervisor, Dr. Trevor Hawkes, for his strong support, excellent advice (not only of a mathematical nature) and unfailing enthusiasm over the last four years, without which I am sure that I would have fallen by the way-side.

Additional thanks go to Professor Martin Isaacs and Professor Michael Slattery, who both found time to speak to me about my research when I visited the United States in 1996.

I am grateful to the Engineering and Physical Sciences Research Council and to the University of Warwick for their financial support as I am to all the administrative staff at the Mathematics Institute for being so efficient and approachable.

I would also like to offer my heartfelt thanks to Stéphanie and my parents for their continual encouragement and unstinting support throughout my research. Finally, I would like to thank Lucie just for being.

Declaration

All the material in this thesis is, to the best of my knowledge, original work of the author and has not been published before, except for the attributed sources cited in the text.

Abstract

In this thesis we begin the study of finite groups possessing a model subgroup, where a model subgroup H of a finite group G is defined to be a subgroup satisfying

$$1_H \uparrow^G = \sum_{\chi \in Irr(G)} \chi.$$

We show that a finite nilpotent group possesses a model subgroup if and only if it is abelian and that a Frobenius group with Frobenius complement C and Frobenius kernel N possesses a model subgroup if and only if

(a) N is elementary abelian of order r^n.

(b) C is cyclic of order $(r^n - 1)/(r^d - 1)$, for some d dividing n.

(c) The finite field $F = \mathbb{F}_{r^n}$ has an additive abelian subgroup H_F of order r^d satisfying $Norm_{F/K}(H_F) = K$, where $K = \mathbb{F}_{r^d}$.

We then go on to conjecture that a finite soluble group G possessing a model subgroup is either metabelian or has a normal subgroup N such that G/N is a Frobenius group with cyclic Frobenius complement of order $2^n + 1$ and elementary abelian Frobenius kernel of order 2^{2n}. We consider a series of cases that need to be excluded in order to prove the conjecture and present some examples that shed light on the problems still to be overcome.

Introduction

The starting point for the material contained in this thesis was the following definition cited by Gollan [9]. A *model* of length k for the complex representations of G, or shorter a *model* for G, is a set $\tau_1, \ldots, \tau_k$ of monomial characters of G such that

$$\sum_{\chi \in Irr(G)} \chi = \sum_{i=1}^{k} \tau_i.$$

Gollan's interest in models stemmed from the fact that given any complex irreducible character χ of G and a model for G, one can construct a complex irreducible representation of G affording the character χ. Gollan's paper focussed on whether or not some of the sporadic simple groups had models. His results, that the smallest Janko group J_1 has a model, but the sporadic simple groups

$$J_3\,,\ Ru\,,\ O'N\,,\ M_{11}\,,\ M_{22}\,,\ McL\,,\ J_2$$

do not, are deceptively discouraging, because searches for models for other specific finite groups have been successful. In particular, Kljacko [10] has found a model for the full general linear group over a finite field and Inglis, Richardson and Saxl [11] have found a model for the symmetric group of degree n.

To be precise Inglis, Richardson and Saxl found an involution model for the symmetric group of degree n. In other words a set $\tau_1, \ldots, \tau_k$ of monomial characters of G and a set of conjugacy class representatives $e_1, \ldots, e_k$ of the set $\{g \in G : g^2 = 1\}$, such that each τ_i is induced from some linear character of the centralizer of e_i and

$$\sum_{\chi \in Irr(G)} \chi = \sum_{i=1}^{k} \tau_i.$$

Notice that if a finite group G has an involution model then

$$\sum_{\chi \in Irr(G)} \chi(1) = 1 + t,$$

where t is the number of involutions in G, and consequently by a result of Frobenius and Schur [1, Corollary 4.6, page 51] every irreducible character of G is afforded by a real representation. From here Baddeley [12] took up the mantle and considered whether certain Weyl groups possessed involution models. He found involution models for Weyl groups of type B_n and type D_n for odd n. However, $W(D_4)$ was discovered not to possess an involution model and this put paid to hopes that the existence of an involution model might be both a necessary and sufficient condition for all representations to be afforded by a real representation.

Although involution models have been studied in some depth there is one type of model that has received more attention than probably any other. Suppose that the set $\tau_1, \ldots, \tau_k$ of monomial characters is a model of length $k = |Irr(G)|$ for G, then we say that G possesses a model of maximal length or more commonly that G is an M-group. Much work has been done to try to classify M-groups. Perhaps the best known result to date being that of Taketa [1, Corollary 5.13, page 67] which states that every M-group is soluble. The converse is false however, although it is true that every supersolvable group [1, Corollary 6.22, page 87] is an M-group, the smallest counter-example being $SL(2,3)$.

The goal of this thesis is to begin the study of the opposite question to that of whether a finite group possesses a model of maximal length. Namely when does a finite group possess a model of minimal length. In other words when does a finite group possess a model of length 1.

In chapter 1 we state and prove a series of well-known results, which play a crucial role in the major theorems of this dissertation. In particular, we determine the faithful irreducible representations of an abelian group over a finite field, we introduce Zsigmondy's theorem, and we examine the structure and describe the irreducible characters of special p- groups and Frobenius groups.

In chapter 2 we show, using Frobenius reciprocity, that a finite group G possesses a model of length 1 if and only if it has a model subgroup, where a model subgroup is defined to be a subgroup H of G such that

$$1_H \uparrow^G = \sum_{\chi \in Irr(G)} \chi.$$

We then go on to prove that a finite nilpotent group has a model subgroup if and only if it is abelian.

In chapter 3 we show that a Frobenius group G with Frobenius complement C and Frobenius kernel N has a model subgroup if and only if the following conditions are satisfied.

(a) N is elementary abelian of order r^n.

(b) C is cyclic of order $(r^n - 1)/(r^d - 1)$, for some d dividing n.

(c) The finite field $F = \mathbb{F}_{r^n}$ has an additive abelian subgroup H_F of order r^d satisfying $Norm_{F/K}(H_F) = K$, where $K = \mathbb{F}_{r^d}$.

One of the key observations in the proof is that if G is a non-abelian special 2-group of rank $2n$ and the order of the centre of G is greater than 2^n, then the number of maximal subgroups of the centre of G whose quotients are extra-special is even. This fact is itself a generalization, in the case where $p = 2$, of a result of Beisiegel [6, Satz 1], which states that if P is a special p-group of rank $2n$ and P/N is extra-special for every maximal subgroup N of the centre of P, then the rank of the centre of P is less than or equal to n.

In chapter 4 we define a $\mathcal{X}$-group to be either an abelian group or a group G with subgroups $G_1, \dots G_m, A$ satisfying the following statements :

(a) $G = G_1 \dots G_m A$;

(b) $[G_i, G_j] = 1$ for $i \neq j$;

(c) $[G_i, A] = 1$ for $1 \leq i \leq m$;

(d) G_i is not nilpotent for $1 \leq i \leq m$;

(e) G_i' is a minimal normal subgroup of G_i for $1 \leq i \leq m$;

(f) A is abelian.

We prove that a non-abelian $\mathcal{X}$-group possesses a model subgroup if and only if $G/Z(G)$ is a direct product of Frobenius groups satisfying the statements outlined on the previous page. We show that every epimorphic image of a $\mathcal{X}$-group is itself a $\mathcal{X}$-group and we define a minimal non-$\mathcal{X}$-group to be a finite soluble group not contained in the class but whose other epimorphic images are. We then move onto the main focus of the chapter which is to give the following classification of minimal non-$\mathcal{X}$-groups :

Case A G is a p-group, G' is cyclic of order p and is the unique minimal normal subgroup of G.

Case B $G = UA$, where U and A are subgroups satisfying the following conditions.

(i) U is a central product of subgroups $G_1, \dots, G_m$ with amalgamated centres;

(ii) $G_i = G_i'C_i$, where $(|G_i'|, |C_i|) = 1$, for $1 \leq i \leq m$;

(iii) G_i' is an extraspecial p-group for all i;

(iv) $Z(U) = Z(G_i) = Z(G_i')$ for all i;

(v) $G_i/Z(U)$ is a Frobenius group at $C_iZ(U)/Z(U) \cong C_i$ with minimal Frobenius kernel $G_i'/Z(U)$ for all i;

(vi) A is a p-group and $Z(U) \subseteq A \subseteq C_G(U)$;

(vii) Either A is cyclic or $A' = Z(U)$ is the unique minimal normal subgroup of A.

Case C $G = G'C$ and the following conditions hold :

(i) $(|G'|, |C|) = 1$;

(ii) $\Phi(G')$ is the unique minimal normal subgroup of G of order r^m;

(iii) $G/\Phi(G')$ is a Frobenius group at $C\Phi(G')/\Phi(G')$ with minimal Frobenius kernel $G'/\Phi(G')$ of order r^n;

(iv) $M = C_C(\Phi(G'))$;

(v) G' is either homocyclic or special.

Case D $G = (G'A)C$ and the following conditions hold :

(i) $(|G'A|, |C|) = 1$;

(ii) $K = [G', A]$ is the unique minimal normal subgroup of G;

(iii) $A/K = Z(G/K)$;

(iv) G/A is a Frobenius group at CA/A with minimal Frobenius kernel $G'A/A$;

(v) $G'A$ is an r-group;

(vi) A is elementary abelian;

(vii) G' is elementary abelian, homocyclic or special;

(viii) $K = \Phi(G'A) = (G'A)'$ and $K \subseteq Z(G'A)$.

Case E $G = G_1G_2$ and the following conditions hold:

(i) $G_i = G_i'C_i$;

(ii) $(|G_i'|, |C_i|) = 1$;

(iii) $K = [G_1', G_2']$ is the unique minimal normal subgroup of G;

(iv) $G/K \cong G_1/K \times G_2/K$;

(v) G_i/K is a Frobenius group at C_iK/K with minimal Frobenius kernel G_i'/K of order r^{n_i};

(vi) G_i' is elementary abelian;

(vii) $G_1'G_2'$ is special.

Case F $G = G''X$ and the following conditions hold:

(i) $G'' \cap X = 1$;

(ii) G'' is the unique minimal normal subgroup of G;

(iii) X is a non-abelian $\mathcal{X}$-group;

(iv) $X \subseteq Aut(G'')$.

Case G There exists a group L and a monomorphism μ from G into L satisfying the following conditions:

(i) $L = L_0 \times \cdots \times L_m$;

(ii) L_i is a Frobenius group with minimal Frobenius kernel L_i';

(iii) $\mu(G') = L_0' \times \cdots \times L_m'$;

(iv) $L = \mu(G)L_i$ for $0 \leq i \leq m$.

In Chapter 5 we consider under what circumstances a non-metabelian minimal non- $\mathcal{X}$-group satisfying the co-prime condition

$$(|G : G'|, |G' : G''|) = 1$$

can possess a model subgroup, and arrive at the following conclusions.

If G is a minimal non-$\mathcal{X}$-group satisfying the conditions outlined in **Case B**, then G does not possess a model subgroup.

If G is a minimal non-$\mathcal{X}$-group of derived length 3 satisfying the conditions outlined in **Case C** and G possesses a model subgroup, then $n = 6$, $r = 2$, $m < n$ and M acts reducibly on $G'/\Phi(G')$. We give an example of a finite group possessing a model subgroup which satisfies these conditions.

If G is a minimal non-$\mathcal{X}$-group satisfying the conditions outlined in **Case E** and G possesses a model subgroup, then the G_i/K are Frobenius groups with elementary abelian Frobenius kernels of order 2^{n_1} and cyclic Frobenius complements of order $2^{\frac{n_1}{2}}+1$. We give an example of a finite group possessing a model subgroup which satisfies these conditions whose derived subgroup is of a form outlined by Beisiegel [6, Lemma 4].

If G is a minimal non-$\mathcal{X}$-group satisfying $(|G:G'|, |G':G''|)$ and the conditions outlined in **Case F**, then G either does not admit a model subgroup or there exists a normal subgroup N of G such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius complement of order $2^n + 1$.

In Chapter 6 we prove that if a metabelian group G possesses a model subgroup and

$$(|G:G'|, |G':G''|) = 1,$$

then there exists a monomorphism μ_G from G to a $\mathcal{X}$-group.

Putting this together with the results from our case studies, we prove that if G is a finite soluble group and we assume that G possesses a model subgroup,

$$(|G:G'|, |G':G''|) = 1$$

and the monomorphism $\mu_{G/G''}$ is in fact an isomorphism, then G satisfies one of the following statements :

(a) G is metabelian.

(b) G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius complement of order $2^n + 1$.

(c) G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^6 and cyclic Frobenius kernel of order $(2^6 - 1)/(2^2 - 1)$.

We go on to show that if G is a minimal non-$\mathcal{X}$-group of derived length 3 satisfying the conditions in **Case D** and G possesses a model subgroup, then G/A is a Frobenius group with elementary abelian Frobenius kernel $G'A/A$ of order 2^n and cyclic Frobenius complement of order $2^n + 1$. And consequently we can prove that if G is a finite nilpotent-by-abelian group and G/G'' is a $\mathcal{X}$-group, then G possesses a model subgroup only if one of the statements above is satisfied.

We formulate the following conjecture.

Conjecture 1 If a finite soluble group G possesses a model subgroup, then G satisfies one of the following two statements :

(a) G is metabelian.

(b) G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius complement of order $2^n + 1$.

We end by giving an example of a minimal non-$\mathcal{X}$-group satisfying the conditions in **Case G** and a metabelian minimal non-$\mathcal{X}$-group satisfying the conditions in **Case D** which both possess model subgroups, giving an indication of what the structure of the additional minimal counter-examples that would need to be considered might look like.

Chapter 1

Background

In this chapter we state and prove a series of results, for reference purposes, that play a crucial role in this thesis. However, more general standard results about finite groups that can be found in Huppert [2] and about character theory that can be found in Isaacs [1] will be stated without proof when required.

1.1 Irreducible representations of abelian groups over finite fields

The result in this section can be found in Doerk and Hawkes [5, (9.8) Theorem, page 161-162].

Theorem 1.1.1 *Let A be an abelian group of order n, let q be a prime power satisfying $(q, n) = 1$, and let m be the smallest natural number such that*

$$n \mid q^m - 1 \ \textit{in other words} \ m \equiv o(q) \, mod n.$$

Suppose that V is an irreducible $F_q[A]$-module faithful for A. Then

$$A = < a >$$

is cyclic and there exists a primitive nth root of unity ϵ of F_{q^m} such that V is isomorphic to F_{q^m} viewed as an $F_q[A]$-module via the A-action

$$xa^i = x\epsilon^i \quad \textit{(field multiplication)}$$

for all $x \in F_{q^m}$ and $0 \leq i \leq n-1$. Furthermore $F_{q^m} = F_q(\epsilon)$ and the dimension of V over F_q equals m.

Proof. Let $E = Hom_{F_q[A]}(V,V) \subseteq Hom_{F_q}(V,V)$ and let

$$\rho : F_q[A] \rightarrow Hom_{F_q}(V,V)$$

denote the representation of $F_q[A]$ afforded by V, thus $vb = v\rho(b)$ for all $v \in V$ and $b \in F_q[A]$. Since A is abelian, $F_q[A]$ is commutative, and therefore $\rho(F_q[A]) \subseteq E$. By Schur's lemma E is a division algebra, and therefore

$$\rho(F_q[A]) - \{0\}$$

is a group, because $\rho(F_q[A]) - \{0\}$ is a finite multiplicatively closed subset of the group $E^\times$. We have proved that $K = \rho(F_q[A])$ is an extension field of F_q. So $\rho(A)$ is a subgroup of $K^\times$, the multiplicative group of K, and is cyclic as a consequence. Because V is a faithful A-module, A is isomorphic to $\rho(A)$. So $A = < a >$ and

$$K = \rho(F_q[A]) = F_q(\epsilon),$$

where $\epsilon = \rho(a)$ is a primitive nth root of unity. Moreover, when K is viewed as an F_q-space, it becomes an A-module over F_q if we define

$$xa^i = x\epsilon^i \quad \text{(field multiplication)}$$

for all $x \in K$ and $0 \leq i \leq n-1$. Now let $r = |K : F_q|$. Since $K^\times$, which is cyclic of order $q^r - 1$, contains the element ϵ of order n, we have

$$q^r \equiv 1 \bmod n,$$

and therefore m divides r; in particular F_{q^m} is a subfield of F_{q^r}. But by hypothesis n divides $q^m - 1$, and so the multiplicative group of F_{q^m} contains the unique subgroup $< \epsilon >$ of order n in $F_{q^r}^\times$. Since $F_{q^r} = K = F_q(\epsilon)$, we therefore have $K \subseteq F_{q^m}$; hence

$$K = F_{q^m}.$$

So regarding V as a $Hom_{F_q}(V, V)$-module in the natural way, we may also regard V as a F_{q^m}-module (vector space over F_{q^m}) by restriction. If U is a non-zero F_{q^m}-subspace of V, then

$$U = UF_{q^m} = U\rho(F_q[A]) = U(F_q[A]);$$

hence U is an $F_q[A]$-submodule of V, and it follows from the irreducibility of V that the dimension of V over F_{q^m} equals 1. Thus if w is a fixed non-zero vector in V, the map

$$\theta : x \to wx$$

is a F_{q^m}-module isomorphism from the regular module F_{q^m} onto V since $\theta(F_{q^m})$ is a non-zero F_{q^m}- subspace of V. Regarding F_{q^m} as an $F_q[A]$-module via the A- action described above for $x \in F_{q^m}$ we obtain

$$(xa)\theta = (x\epsilon)\theta = w(x\epsilon) = (wx)\epsilon = (wx)\rho(a) = (x)\theta\rho(a) = (x)\theta a,$$

and therefore θ is the desired $F_q[A]$- isomorphism from F_{q^m} onto V. The proof is complete. □

1.2 Zsigmondy's Theorem

All of the results in this section can be found in Huppert and Blackburn [7, pages 503-509].

Lemma 1.2.1 *Let ϕ_n be the nth cyclotomic polynomial over the field of rational numbers. Let q be a prime , let a be an integer prime to $q > 2$ and let f be the order of a modulo q. For each non-zero integer x, let $w_q(x) = max\{l \,|q^l \, divides x\}$. Then the following hold.*

(a) $w_q(\phi_f(a)) > 0$.

(b) $w_q(\phi_{fq^i}(a)) = 1$ *for all* $i \geq 1$.

(c) $w_q(\phi_m(a)) = 0$ *for all other* $m \geq 1$.

Proof. (a) As f is the order of a modulo q, $w_q(a^i - 1) = 0$ if f does not divide i. Thus $w_q(\phi_i(a)) = 0$ if f does not divide i. From

$$\phi_f(a) \prod_{i|f, i \neq f} \phi_i(a) = a^f - 1,$$

it follows that $w_q(\phi_f(a)) = w_q(a^f - 1) > 0$. (b) Put $n = fq^i$, $r = fq^{i-1}$. Then

$$\begin{aligned} \frac{a^n - 1}{a^r - 1} &= \frac{((a^r - 1) + 1)^q - 1}{a^r - 1} \\ &= (a^r - 1)^{q-1} + q(a^r - 1)^{q-2} + \cdots \binom{q}{2} (a^r - 1) + q. \end{aligned}$$

Since $a^r - 1 \equiv 0 \bmod q$ and $\binom{q}{2} \equiv 0 \bmod q$, we have $(a^n - 1)/(a^r - 1) \equiv q \mathrm{mod} q^2$; thus

$$w_q\left(\frac{a^n - 1}{a^r - 1}\right) = 1, \quad \text{and} \quad \sum_{d|n, d\nmid r} w_q(\phi_d(a)) = 1,$$

because $(a^n - 1)/(a^r - 1) = \prod_{d|n, d\nmid r} \phi_d(a)$. Hence there exists a $d|n$ such that d does not divide r and $w_q(\phi_d(a)) = 1$. Thus $w_q(a^d - 1) > 0$ and $f|d$. The only integer d satisfying these conditions is $d = n$; thus $w_q(\phi_n(a)) = 1$.
(c) If $w_q(\phi_m(a)) \neq 0$, $w_q(a^m - 1) \neq 0$ and $f|m$. So we have to show that $w_q(\phi_m(a)) = 0$ if $m = fq^i l$ with $i \geq 0$, $l > 1$ and q not a divisor of l. If $r = fq^i$, $\phi_m(a)$ is a divisor of $(a^m - 1)/(a^r - 1)$. Since $a^r \equiv 1 \, mod \, q$, we have

$$\begin{aligned} \frac{a^m - 1}{a^r - 1} &= \frac{((a^r - 1) + 1)^l - 1}{a^r - 1} \\ &= (a^r - 1)^{l-1} + l(a^r - 1)^{l-2} + \cdots + l. \end{aligned}$$

Thus $w_q(\phi_m(a)) = 0$. The proof is complete. □

Lemma 1.2.2 *Let ϕ_n be the nth cyclotomic polynomial over the field of rational numbers. Let a be an odd integer. For each non-zero integer x, let $w_2(x) = max\{l \, | 2^l dividesx\}$. Then the following hold.*

(a) $w_2(\phi_{2^i}(a)) = 1$ *for* $i \geq 2$.

(b) $w_2(\phi_n(a)) = 0$ *for* $n \neq 2^i$ $(i = 0, 1, \ldots)$.

Proof. Write $n = 2^i l$ with $i \geq 0$, l odd and $l \geq 1$. If $l > 1$, then

$$\frac{a^n - 1}{a^{2^i} - 1} = (a^{2^i} - 1)^{l-1} + l(a^{2^i} - 1)^{l-2} + \cdots + l \not\equiv 0 \bmod 2$$

and $w_2(\phi_n(a)) = 0$. If $l = 1$, then

$$\phi_{2^i}(a) = \frac{a^n - 1}{a^{2^i} - 1} = a^{2^{i-1}} + 1,$$

so for $i \geq 2$, $\phi_{2^i}(a) \equiv 2 \bmod 4$ and $w_2(\phi_{2^i}(a)) = 1$. □

Lemma 1.2.3 *Let $\Phi_n(x,y) = y^{\phi(n)}\phi_n(x/y)$, where ϕ is the Euler function and ϕ_n is the nth cyclotomic polynomial. Let*

$$L(n) = inf|\Phi_n(a,b)|,$$

where a,b run through all complex numbers for which $|a| \geq |b|+1$ and $|b| \geq 1$. Then the following hold.

(a) *If p divides n, $L(np) \geq L(n)$ and $L(np) \geq (1+p)^{\phi(n)}$.*

(b) *If p does not divide n, $L(np) \geq L(n)^{p-1}$.*

(c) *For $p \geq 5$, $L(p) > 2p$.*

(d) *For $p \geq 5$, $L(2p) > 2p$.*

Proof. (a) Since p divides n, $\Phi_n(a,b) = \Phi_n(a^p, b^p)$. Since $|a| \geq |b|+1$ and $|b| \geq 1$, $|a|^p \geq |b|^p + 1$ and $|b|^p \geq 1$, so $L(np) \geq L(n)$. Also

$$\Phi_n(a,b) = \prod_{\epsilon}(a - \epsilon b) \geq (|a| - |b|)^{\phi(n)},$$

where ϵ runs through the $\phi(n)$ primitive nth roots of unity. But for $|a| \geq |b| + 1$ and $|b| \geq 1$,

$$\begin{aligned} |a|^p - |b|^p &= ((|a| - |b| + |b|)^p - |b|^p \\ &\geq (|a| - |b|)^p + p(|a| - |b|)^{p-1}|b| \\ &\geq 1 + p. \end{aligned}$$

Hence $|\Phi_n(a,b)| \geq (1+p)^{\phi(n)}$ and $L(np) \geq (1+p)^{\phi(n)}$.

(b) Since p does not divide n,

$$\Phi_{np}(a,b) = \prod_{\epsilon^p = 1 \neq \epsilon} \Phi_n(a, b\epsilon).$$

So $L(np) \geq L(n)^{p-1}$.

(c) We have

$$|\Phi_p(a,b)| = \left|\frac{a^p - b^p}{a - b}\right| \geq \frac{|a^p| - |b^p|}{|a+b|} = \frac{x^p - y^p}{x+y},$$

where $x = |a|$, $y = |b|$. Thus $x \geq y + 1$ and

$$\begin{aligned}(x^p - y^p)(1+2y) &= x(1+y)(x^{p-1} - (1+y)^{p-1}) + y(x^p - (1+y)^p)\\ &\quad +y^p(x-(1+y)) + (x+y)((1+y)^p - y^p)\\ &\geq (x+y)((1+y)^p - y^p).\end{aligned}$$

Hence

$$|\Phi_p(a,b)| \geq \frac{x^p - y^p}{x+y} \geq \frac{(1+y)^p - y^p}{1+2y}.$$

But $y = |b| \geq 1$, so

$$(1+y)^p - 2^p = \sum_{i=0}^{p} \binom{p}{i} (y^i - 1) \geq y^p - 1$$

and

$$(1+y)^p - 2^p y = \sum_{i=0}^{p} \binom{p}{i} (y^i - y) \geq y^p - y.$$

Therefore

$$\begin{aligned}3(1+y)^p - 2^p(1+2y) &= ((1+y)^p - 2^p) + 2((1+y)^p - 2^p y)3y^p\\ &\geq (2^p - 1)(1+2y)\\ &\geq y^p - 1 + 2(y^p - y) = 3y^p - (1+2y).\end{aligned}$$

Hence $3(1+y)^p - 3y^p \geq (2^p - 1)(1+2y)$ and

$$|\Phi_p(a,b)| \geq \frac{(1+y)^p - y^p}{1+2y} \geq \frac{2^p - 1}{3}.$$

Hence $L(p) \geq \frac{2^p-1}{3}$ and for $p \geq 5$, $L(p) > 2p$.

(d) Follows from (b) and the identity $\phi_{2p}(a,b) = \phi_p(a,-b)$. □

Lemma 1.2.4 *Let $\Phi_n(x,y) = y^{\phi(n)}\phi_n(x/y)$, where ϕ is the Euler function and ϕ_n is the nth cyclotomic polynomial. Let*

$$L(n) = inf|\Phi_n(a,b)|,$$

where a,b run through all complex numbers for which $|a| \geq |b|+1$ and $|b| \geq 1$. Then $L(n) > \prod_{p|n} p$, where p runs through all prime divisors of n, except when $n = 1, 2, 3$ or 6.

Proof. We shall prove the result by induction on n. If n is divisible by the square of a prime p, then $L(n) \geq L(n/p)$ by Lemma 1.2.3(a). The assertion then follows by induction unless n/p is $1, 2, 3$ or 6. Since p divides n/p, the only possibilites are $n = 4, 9, 12$ or 18. But by the second assertion of (a), $L(4) \geq 3$, $L(9) \geq 16$, $L(12) \geq 9$ and $L(18) \geq 16$. So we may assume that n is square-free. Let p be the greatest prime divisor of n and write $n = pm$. By hypothesis, $p \geq 5$. If $m = 1$, the assertion follows from Lemma 1.2.3(c); if $m = 2$, it follows from Lemma 1.2.3(d). If $m = 3$,$n = 3p$ and $L(n) \geq 4p^2 > 6p$ by Lemma 1.2.3(b) and (c).Similarly if $m = 6$, $L(n) \geq L(2p^2) > 4p^2 > 6p$ by Lemma 1.2.3(b) and (d). For other values of m, $L(m) > \prod_{q|m} q$ by the inductive hypothesis. Thus $L(m) > 3$, because m cannot be a power of 2 since m is square-free. Hence $L(m)^{p-1} \geq pL(m)$ and it follows that $L(n) \geq L(m)^{p-1} \geq pL(m) > \prod_{q|n} q$ by Lemma 1.2.3(b). The proof is complete. □

Theorem 1.2.5 *Let a, n be integers greater than 1. Then except in the cases $n = 2$, $a = 2^b - 1$ and $n = 6$, $a = 2$, there is a prime q with the following properties.*

(a) *q divides $a^n - 1$.*

(b) *q does not divide $a^i - 1$ whenever $0 < i < n$.*

(c) *q does not divide n.*

In particular, n is the order of a modulo q.

Proof. Suppose that for each prime divisor q of $a^n - 1$, there exists i such that $0 < i < n$ and q divides $a^i - 1$. since $a^i - 1 = \prod_{d|i} \phi_d(a)$, it follows in particular that for each prime divisor q of $\phi_n(a)$, there exists $d < n$ such that q divides $\phi_d(a)$. Let f be the order of a modulo q. Since $w_q(\phi_n(a)) > 0$ and $w_q(\phi_d(a)) > 0$, it follows from Lemma 1.2.1 that if $q > 2$, $n = fq^k$ and $d = fq^j$, where $0 \leq j < k$. Thus q divides n. Furthermore, $w_q(\phi_n(a)) = 1$ by Lemma 1.2.1. If $w_2(\phi_n(a)) > 0$, we see from Lemma 1.2.2 that $n = 2^i$ and, if $n > 2$, $w_2(\phi_n(a)) = 1$. It follows that if $n > 2$,

$$|\phi_n(a)| = \prod_q q^{w_q(\phi_n(a))} \leq \prod_{q|n} q.$$

By Lemma 1.2.4, however

$$|\phi_n(a)| = |\Phi_n(a, 1)| > \prod_{q|n} q,$$

except when $n = 1, 2, 3$ or 6. Further, $\phi_3(a) = a^2 + a + 1 > 3$ for all $a > 1$, and $\phi_6(a) = a^2 - a + 1 > 6$ for all $a \geq 3$. Thus only the cases $n = 2$ and $a = 2$, $n = 6$ remain. If the assertion is false for $n = 2$, each prime divisor of $a^2 - 1$ divides $a - 1$. It follows at once that 2 is the only prime divisor of $a + 1$, since $(a + 1, a - 1) \leq 2$; thus $a = 2^b - 1$. Apart from the stated exceptions, then, there is always a prime q such that q divides $a^n - 1$ and q does not divide $a^i - 1$ for $0 < i < n$. Thus n is the order of a modulo q. Hence n divides $q - 1$ and q does not divide n. □

1.3 Symplectic spaces

In this section we shall establish some well-known facts about symplectic spaces, which can be found in Huppert [2, pages 215-219].

Let V be a finite dimensional vector space over a field K. Then an *alternating bilinear* form f on V is a map

$$f : V \times V \to K$$

with the following properties :

$$\begin{aligned} f(k_1u + k_2v\,, w) &= k_1f(u\,, w) + k_2f(v\,, w) \\ f(u\,, k_1v + k_2w) &= k_1f(u\,, v) + k_2f(u\,, w) \\ f(u\,, u) &= 0 \end{aligned}$$

for all $u, v, w \in V$ and $k_i \in K$. Clearly $f(v\,, w) = -f(w\,, v)$ for all $v, w \in V$, because

$$\begin{aligned} 0 = f(v + w\,, v + w) &= f(v\,, v) + f(v\,, w) + f(w\,, v) + f(w\,, w) \\ &= f(v\,, w) + f(w\,, v). \end{aligned}$$

A *symplectic space* is a composite object consisting of a finite dimensional vector space V and an alternating form f on V. Suppose that V and W are two symplectic spaces with alternating bilinear forms f and g. Then we call a bijective linear map γ from V to W with

$$f(v_1, v_2) = g(\gamma(v_1)\,, \gamma(v_2))$$

for all $v_i \in V$ an *isometry*. We say that V and W are isometric, if an isometry from V to W exists. The group of isometries from V into itself is called the symplectic group on V and is denoted by $Sp(V)$.

Let K be a field of characteristic 2. Let $f : V \times V \to K$ be a bilinear form, and let $q : V \to K$ be a map satisfying

$$q(au + bv) = a^2q(u) + b^2q(v) + abf(u, v)$$

for all $a, b \in K$ and $u, v \in V$. Such a map is called a *quadratic form* on V. On setting $a = b = 1$ and $u = v$ we obtain $f(u, u) = 0$ for all $u \in V$, and so f is a symplectic form on V. If this form f is non-degenerate, we say that the quadratic form q is *non-degenerate.* The group of non-singular maps $\alpha : V \to V$ which satisfy

$$q(\alpha(v)) = q(v)$$

for all $v \in V$ is called the orthogonal group on V and is denoted by $O(V)$. Clearly $O(V) \subseteq Sp(V)$.

Let U be a subspace of V. Then the *orthogonal complement* of U in V is the subspace

$$U^{\perp} = \{v \in V : f(u, v) = 0 \ \ for \ all \ \ u \in U\}.$$

In particular, the *radical* of V is the subspace

$$R(V) = V^{\perp} = \{v \in V : f(u, v) = 0 \ \ for \ all \ \ u \in V\}.$$

We say that V is non-degenerate, if $R(V) = 0$.

Lemma 1.3.1 *Let U be a subspace of the symplectic space V. Then*

$$Dim\ U^{\perp} \geq Dim\ V - Dim\ U.$$

Furthermore, if U is non-degenerate, then $V = U \perp U^{\perp}$.

Proof. Let $\{u_1, \ldots, u_k\}$ be a basis of U. Then $U^\perp$ is the solution space of the k linear equations $f(u_i, x) = 0$ and

$$Dim\ U^\perp \geq Dim\ V - k = Dim\ V - Dim\ U.$$

If U is non-degenerate, then $U \cap U^\perp = R(U) = 0$ and

$$Dim\ \left(U + U^\perp\right) = Dim\ U + Dim\ U^\perp \geq Dim\ V.$$

Thus $V = U \perp U^\perp$. □

If v_1 and v_2 are elements of V with $f(v_1, v_2) = 1$, then we call the set $\{v_1, v_2\}$ a *hyperbolic pair* and the two dimensional symplectic space generated by a hyperbolic pair is called a *hyperbolic plane.* Clearly a hyperbolic plane is non-degenerate.

Theorem 1.3.2 *Let V be a symplectic space of dimension n over with $Dim\ R(V) = r$. Then*

$$V = H_1 \perp \cdots \perp H_m \perp R(V),$$

where the H_i are hyperbolic planes, and V is uniquely determined up to isomorphism by the numbers n and r. In particular, $n - r = 2m$ is even.

Proof. If $V = R(V)$, then there is nothing to prove. If $h_1 \in V - R(V)$, then there is an element h_2 of V with $(h_1, h_2) = 1$ and $H_1 = < h_1, h_2 >$ is a hyperbolic plane. So

$$V = H_1 \perp H_1^\perp \quad and \quad R(V) = R(H_1) \perp R(H_1^\perp) = R(H_1^\perp),$$

by Lemma 1.3.1. The result follows by induction on n. □

Lemma 1.3.3 *Let V be a non-degenerate sympletic space and $\{x_1, \ldots, x_r\}$ be a linearly independent set of V with $(x_i, x_j) = 0$ for $i \neq j$. Then there exists a linearly independent set $\{y_1, \ldots, y_r\}$ of V such that $H_i = < x_i, y_i >$ is a hyperbolic plane and*

$$V = H_1 \perp \cdots \perp H_r \perp V',$$

for some subspace V' of V.

Proof. Let $*$ be the linear map from V to its dual V^* such that

$$* : v \rightarrow v^*,$$

where $v^*(w) = f(v, w)$ for all $w \in V$. Then $v^* = 0$ if and only if $v \in R(V)$. So $*$ is a bijective linear map from V to V^*, because $R(V) = 0$ and $Dim\ V = Dim\ V^*$. Hence, there exists an element y_1 of V with

$$\begin{aligned} x_1^*(y_1) &= f(x_1, y_1) &&= 1 \quad \textit{and} \\ x_i^*(y_1) &= f(x_i, y_1) &&= 0 \quad \textit{for } i \in \{2, \ldots, r\}. \end{aligned}$$

So $H_1 = < x_1, y_1 >$ is a hyperbolic plane and by Lemma 1.3.1 $V = H_1 \perp H_1^{\perp}$. Furthermore, $x_i \in H_1^{\perp}$ for $i \in \{2, \ldots, r\}$ and $H_1^{\perp}$ is non- degenerate, because

$$0 = R(V) = R(H_1) \perp R(H_1^{\perp}).$$

The result follows by induction on r. □

Lemma 1.3.4 *Let V be a non-degenerate symplectic space. Let U_1 and U_2 be subspaces of V and let γ be an isometry from U_1 to U_2. Then there is an isometry Γ from V to itself with $\Gamma = \gamma$ on U_1.*

Proof. By Theorem 1.3.2, there exist hyperbolic planes $H_1, \ldots, H_m$ such that

$$U_1 = H_1 \perp \cdots \perp H_m \perp R(U_1).$$

Furthermore, $R(U_2) = \gamma(R(U_1))$ and if we let $H_i' = \gamma(H_i)$, then

$$U_2 = H_1' \perp \cdots \perp H_m' \perp R(U_2).$$

So $H = H_1 \perp \cdots \perp H_m$ and $H' = H_1' \perp \cdots \perp H_m'$ are non-degenerate. Let $L = H^\perp$ and $L' = H'^\perp$. Then, by Lemma 1.3.1,

$$V = H \perp L = H' \perp L'$$

and $R(L) = R(L') = 0$, because

$$0 = R(V) = R(H) \perp R(L) = R(H') \perp R(L').$$

Clearly $R(U_1) \subsetneq H^\perp = L$ and $R(U_2) \subsetneq H'^\perp = L'$. So if we choose a basis $\{x_1, \ldots, x_r\}$ for $R(U_1)$, then $f(x_i, x_j) = 0$ for all $i, j \in \{1, \ldots, r\}$ and, by Lemma 1.3.3,

$$L = S_1 \perp \cdots \perp S_r \perp M,$$

where $S_i = < x_i, y_i >$ and $f(x_i, y_i) = 1$. Similarly

$$L' = S_1' \perp \cdots \perp S_r' \perp M',$$

where $S_i' = < \gamma(x_i), y_i' >$ and $(\gamma(x_i), y_i') = 1$. Thus

$$\begin{aligned} V = H \perp L &= H_1 \perp \cdots \perp H_m \perp S_1 \perp \cdots \perp S_r \perp M \\ &= H_1' \perp \cdots \perp H_m' \perp S_1' \perp \cdots \perp S_r' \perp M'. \end{aligned}$$

Now $R(M) \subseteq R(L) = 0$ and $R(M') \subseteq R(L') = 0$. So M and M' are non-degenerate symplectic spaces of equal dimension. Hence M is isomorphic to M', by Theorem 1.3.2, and there is an isometry δ from M to M'. Therefore the linear map Γ defined by

$$\begin{aligned} \Gamma(h) &= \gamma(h) \quad \textit{for all } h \in H_1 \perp \cdots \perp H_m, \\ \Gamma(x_i) &= \gamma(x_i) \quad (1 \leq i \leq r), \\ \Gamma(y_i) &= \gamma(y_i') \quad (1 \leq i \leq r), \\ \Gamma(m) &= \delta(m) \quad \textit{for all } m \in M. \end{aligned}$$

is an isometry of V to itself with $\Gamma = \gamma$ on U_1. □

Suppose that U is a subspace of a symplectic space V. Then U is called *isotropic*, if $(u, u') = 0$ for all $u, u' \in U$.

Theorem 1.3.5 *Let V be a non-degenerate sympletic space of dimension $2n$. If U is an isotropic subspace of V, then Dim $U \leq n$ and U is contained in an isotropic subspace of dimension n of V.*

Proof. Let $\{u_1, \ldots, u_r\}$ be a basis for U. By Lemma 1.3.3,

$$V = H_1 \perp \cdots \perp H_r \perp V'$$

with hyperbolic planes $H_i = < u_i, v_i >$. So $2r \leq Dim\ V = 2n$. By Theorem 1.3.2,

$$V = V_1 \perp \cdots \perp V_n$$

with hyperbolic planes $V_i = < x_i, y_i >$. The linear map γ with $\gamma(u_i) = x_i$ for $(1 \leq i \leq r)$ is an isometry from U onto $< x_1, \ldots, x_r >$. Let Γ be the isometry of V, whose existence is guaranteed by Lemma 1.3.4, which restricts to γ. Then

$$\Gamma(U) = \gamma(U) = < x_1, \ldots, x_r > \subsetneq < x_1, \ldots, x_n >$$

and U lies in the isotropic subspace $\Gamma^{-1}(< x_1, \ldots, x_n >)$. □

1.4 Special p-groups

In this section we shall prove some well-known facts about extra-special p-groups, and some additional facts that will prove useful later.

Let G be a non-abelian p-group. If $Z(G) = G' = \Phi(G)$ is elementary abelian, then G is called *special.* If G is a special p-group and the centre of G has order p, then G is called *extra-special.*

Theorem 1.4.1 *Let G be an extra-special p-group. Then the following statements hold.*

(a) *If $G' = < c >$, then $G/Z(G)$ can be viewed as a non-degenerate symplectic space over $GF(p)$ with alternating bilinear form f defined by*

$$f(\bar{g}_1, \bar{g}_2) = a,$$

where $\bar{g}_1 = g_1 Z(G)$, $\bar{g}_2 = g_2 Z(G)$ and $[g_1, g_2] = c^a$;

(b) *$G/Z(G)$ has order p^{2m};*

(c) *G is a central product of non-abelian groups of order p^3 with amalgamted centres;*

(d) *Every maximal abelian normal subgroup of G has order p^{m+1}.*

Proof. Huppert [2, Satz 13.7 pages 353-355]. (a) Clearly f is well-defined and since G has class 2,

$$[g_1g_2\,,g_3] = [g_1\,,g_3][g_2\,,g_3] \text{ and } [g_1\,,g_2g_3] = [g_1\,,g_2][g_1\,,g_3]$$

for all $g_i \in G$. Thus $G/Z(G)$ can be viewed as a symplectic space over $GF(p)$, because $[g\,,g] = 1$ for all $g \in G$. Furthermore, the symplectic space $G/Z(G)$ is non-degenerate, because $[g\,,h] = 1$ for all $h \in G$ if and only if $g \in Z(G)$.

(b) By Theorem 1.3.2,

$$Dim\ G/Z(G) = 2m$$

and $G/Z(G)$ has order p^{2m}.

(c) By Theorem 1.3.2, $G/Z(G)$ has a basis $\{\bar{x}_1, \ldots, \bar{x}_m, \bar{y}_1, \ldots, \bar{y}_m\}$ such that

$$f(\bar{x}_i, \bar{y}_i) = 1 \text{ and } f(\bar{x}_i, \bar{x}_i) = f(\bar{y}_i, \bar{y}_i) = 0$$

for all i and

$$f(\bar{x}_i, \bar{x}_j) = f(\bar{y}_i, \bar{y}_j) = f(\bar{x}_i, \bar{y}_j) = 0$$

for $i \neq j$.

Let $\bar{x}_i = x_iZ(G)$ and $\bar{y}_j = y_jZ(G)$. Then G is a central product of the non-abelian groups $G_i =< x_i, y_i, Z(G) >$ of order p^3 with amalgamated centres.

(d) If M is a maximal abelian normal subgroup of G, then $Z(G) \subsetneq M$ and $M/Z(G)$ is a subspace of $G/Z(G)$ with

$$f(\bar{m}_1\,, \bar{m}_2) = 0$$

for all $\bar{m}_1, \bar{m}_2 \in M/Z(G)$. So $M/Z(G)$ is a maximal isotropic subspace of $G/Z(G)$ and, by Theorem 1.3.5, M has order p^{m+1}. □

Theorem 1.4.2 *Let G be an extra-special 2-group of order 2^{2m+1}. Then one of the following two cases arises :*

(i) *G is a central product of m dihedral groups of order 8 with amalgamated centres.*

(ii) *G is a central product of $m-1$ dihedral groups of order 8 and a quarternion group of order 8 with amalgamated centres.*

In case (i) G has maximal abelian normal subgroups of type $(4, \underbrace{2, \ldots, 2}_{m-1})$ and type $(\underbrace{2, \ldots, 2}_{m+1})$; in case (ii) every maximal abelian normal subgroup of G is of type $(4, \underbrace{2, \ldots, 2}_{m-1})$.

Proof. Huppert [2, Satz 13.8, pages 355-356]. By Theorem 1.4.1, G is a central product of non-abelian groups of order 8. So in order to prove that one of the two cases arises we need only show that a central product of two quarternion groups with amalgamated centres can be regarded as a central product of two dihedral groups with amalgamated centres.

Let G be the central product of Q_1 and Q_2 with amalgamated centres, where

$$Q_1 =< q_1, q_2 \mid q_1^4 = q_2^4 = 1, q_1^{q_2} = q_1^{-1}, q_1^2 = q_2^2 >$$

and

$$Q_2 =< q_3, q_4 \mid q_3^4 = q_4^4 = 1, q_3^{q_4} = q_3^{-1}, q_3^2 = q_4^2 > .$$

Then G can be regarded as a central product of $D_1 =< d_1, d_2 >$ and $D_2 =< d_3, d_4 >$ with amalgamated centres, where

$$d_1 = q_1q_4\ ,\ d_2 = q_2q_4\ ,\ d_3 = q_1q_2q_3\ ,\ d_4 = q_1q_2q_3q_4.$$

Note that d_1, d_2 and d_3, d_4 of D_1 and D_2 respectively are not the conventional generators of the dihedral group. In particular, $d_i^2 = 1$ for $i \in \{1, 2, 3, 4\}$.

To complete the proof we begin by showing that every extra special 2-group G of order 2^{2m+1} has an abelian normal subgroup of type $(4, \underbrace{2, \ldots, 2}_{m-1})$. Since G is non-abelian, there is an element a of G of order 4. Furthermore, $< a > \lhd G$, since $G' =< a^2 >$. Let U be a maximal abelian normal subgroup of G containing a. Then $|U| = 2^{m+1}$ by Theorem 1.4.1 and U is an abelian normal subgroup of G of type $(4, \underbrace{2, \ldots, 2}_{m-1})$, because $o(a) = 4$ and the exponent of $G/Z(G)$ is 2.

Let G be a central product of dihedral groups $D_1, \ldots, D_m$ of order 8 with amalgamated centres, where $D_i =< a_i, b_i >$ with $a_i^2 = 1$ for $i \in \{1, \ldots, m\}$. Then clearly $< Z(G), a_1, \ldots, a_m >$ is a maximal abelian normal subgroup of G of type $(\underbrace{2, \ldots, 2}_{m+1})$.

Let G be a central product of dihedral groups $D_1, \ldots, D_{m-1}$ of order 8 and a quarternion group Q of order 8 with amalgamated centres. Let U be a maximal abelian normal subgroup G. Then every element a of U can be written $a = a_1a_2$ with $a_1 \in D_1 \ldots D_{m-1}$ and $a_2 \in Q$; where a_1 and a_2 are uniquely determined upto factors of $Z(G)$. We define $U_i (i = 1, 2)$ as the subgroup generated by all the a_i. Then U_1 and U_2 are abelian normal subgroups of $D_1 \dots D_{m-1}$ and Q respectively. Since $U \subseteq U_1 U_2$ and

$$U_1 \cap U_2 = Z(G)$$

it follows with help from Theorem 1.4.1 that

$$2^{m+1} = |U| \subseteq \frac{|U_1||U_2|}{2} \subseteq \frac{2^m 2^2}{2} = 2^{m+1}.$$

So $U = U_1 U_2$ and U_2 is a maximal abelian normal subgroup of Q. So U_2 is cyclic of order 4 and the exponent of U is 4. □

Theorem 1.4.3 *Let G be an extra-special 2-group of order 2^{2m+1} and let $Z(G) = < c >$. Let q be the function from $G/Z(G)$, regarded as a vector space over $GF(2)$, into $GF(2)$ defined by*

$$q(\bar{g}) = a,$$

where $\bar{g} = gZ(G) \in G/Z(G)$ and $g^2 = c^a$. Then q is a quadratic form on $G/Z(G)$ satisfying the following statements.

(a) *If G is a central product of dihedral groups $D_1, \dots, D_m$ of order 8, then $G/Z(G)$ has a basis $\{\bar{a}_1, \dots, \bar{a}_m, \bar{b}_1, \dots, \bar{b}_m\}$ satisfying the following conditions :*

$$q(\bar{a}_i) = q(\bar{b}_i) = 0 \textit{ and } f(\bar{a}_i, \bar{b}_j) = \delta_{ij} \textit{ for all } i, j$$

(b) *If G is a central product of dihedral groups $D_1, \dots, D_{m-1}$ of order 8 and a quarternion group of order 8 then $G/Z(G)$ has a basis*

$$\{\bar{a}_1, \dots, \bar{a}_{m-1}, \bar{b}_1, \dots, \bar{b}_{m-1}, \bar{x}, \bar{y}\}$$

satisfying the following conditions :

$$q(\bar{a}_i) = q(\bar{b}_i) = f(\bar{a}_i, \bar{x}) = f(\bar{a}_i, \bar{y}) = f(\bar{b}_i, \bar{x}) = f(\bar{b}_i, \bar{y}) = 0,$$

$$f(\bar{a}_i, \bar{b}_j) = \delta_{ij} \textit{ for all } i, j \textit{ and}$$

$$q(\bar{x}) = q(\bar{y}) = f(\bar{x}, \bar{y}) = 1.$$

Proof. Huppert [2, Satz 13.8(c) and Bemerkungen 13.9, pages 355- 357] The function q is clearly well-defined on $G/Z(G)$. Since $(gh) = g^2h^2[h, g]$ for all $g, h \in G$, it follows that

$$q(\bar{x}, \bar{y}) = q(\bar{x}) + q(\bar{y}) + f(\bar{y}, \bar{x}),$$

where f is the alternating bilinear form of Theorem 1.4.1. So q is a quadratic form and the result follows from Theorem 1.4.2 and the systems of generators and relations given above for a quarternion and dihedral group. □

Theorem 1.4.4 *Let G be an extra-special 2-group of order 2^{2m+1}. Let $A = Aut(G)$ and let $I = Inn(G)$. Then*

(a) *A/I is isomorphic to a subgroup of $O(q)$, the orthogonal group for the quadratic form q associated with G.*

(b) *If G is a central product of dihedral groups $D_1, \ldots, D_m$ of order 8 with amalgamated centres, then*

$$|A/I| \, | 2^{(2m(2m-2)/4)+1}(2^m - 1)\Pi_{i=1}^{m-1}(2^{2i} - 1) \, ;$$

(c) *If G is a central product of dihedral groups $D_1, \ldots, D_{m-1}$ of order* 8 *and Q is a quarternion group of order* 8 *with amalgamated centres, then*

$$|A/I| \, |2^{(2m(2m-2)/4)+1}(2^m+1)\Pi_{i=1}^{m-1}(2^{2i}-1) \; ;$$

(d) *If G is a central product of dihedral groups D_1, D_2, D_3 of order* 8 *with amalgamated centres, then A/I is isomorphic to a subgroup of S_8.*

Proof. (a) Doerk and Hawkes [5, (20.8) Theorem, page 81] Let $\alpha \in Aut(G)$ and let $\bar{\alpha}$ be the automorphism induced by α on $G/Z(G)$. Then $\bar{\alpha} \in O(q)$ and the map $\alpha \to \bar{\alpha}$ defines a homomorphism from $Aut(G)$ to $O(q)$, since α centralizes $Z(G)$. So in order to show that A/I is isomorphic to a subgroup of $O(q)$, we need to prove that

$$C_{Aut(G)}(G/Z(G)) = Inn(G).$$

Let Z denote the centre of G, and let $\{x_1Z, \ldots, x_{2m}Z\}$ be a basis for $G/Z(G)$. If $\alpha \in C_{Aut(G)}(G/Z(G))$, then $\alpha(x_iZ) = x_iZ$ and so $\alpha(x_i) = x_iz_i$ for some $z_i \in Z$: furthermore, α is uniquely determined by the sequence $(z_1, \ldots, z_{2m})$ because $G =< x_1, \ldots, x_{2m} >$. Therefore the number of distinct α's in $C_{Aut(G)}(G/Z(G))$ is bounded above by 2^{2m}, the number of such sequences. However, $C_{Aut(G)}(G/Z(G))$ obviously contains every inner automorphism of G and the result follows.

(b) , (c) and (d) now follow from Theorem 1.4.3 and Kleidman and Liebeck [4, Proposition 2.5.5 and Proposition 2.9.1, Pages 29 and 43]. □

Theorem 1.4.5 *Let G be an extra-special p-group of order p^{2m+1}. Then G has the following irreducible characters :*

(a) *p^{2m} linear characters*

(b) *$p-1$ faithful irreducible characters of degree p^m, which can be described in the following way. Let U be a maximal abelian normal subgroup of G and $\lambda \neq 1_{Z(G)}$ be a linear character of the $Z(G)$. If μ is an extension of λ in U, then μ^G is an irreducible character of G. Every linear character $\lambda \neq 1_{Z(G)}$ gives rise to exactly one irreducible character χ in this way and $\chi_{Z(G)} = \chi(1)\lambda$.*

Proof. Huppert [2, Satz 16.4, pages 562-563] Since $|G/G'| = p^{2m}$, the group G has exactly p^{2m} linear characters. Let λ be a linear character of $Z(G)$ with $\lambda \neq 1$ and let U be a maximal abelian normal subgroup of G. Then U has order p^{m+1}, by Theorem 1.4.1, and λ extends to U. Suppose that $\mu \in Irr(U)$ is an extension of λ. Then

$$\mu^G(g) = \frac{1}{|U|}\sum_{x\in G}\mu^\circ(x^{-1}gx),$$

where $\mu^\circ(u) = \mu(u)$ for $u \in U$ and $\mu^\circ(s) = 0$ for $s \in G - U$. If $g \notin U$, then $x^{-1}gx \notin U$ for all $x \in G$ and $\mu^G(g) = 0$. If $g \in U$, then

$$\mu^G(g) = \frac{1}{|U|}\sum_{x\in G}\mu(g[g,x]) = \frac{\mu(g)}{|U|}\sum_{x\in G}\lambda([g,x]),$$

because $[g,x] \in G' = Z(G)$. Since G has class 2, the map $x \to [g,x]$ is a homomorphism from G to G'. For $g \in Z(G)$ we have

$$\mu^G(g) = \frac{\lambda(g)}{|U|}|G| = p^m\lambda(g) = \mu^G(1)\lambda(g).$$

For $g \notin Z(G)$ with help from the orthogonality relations and remembering that $\lambda \neq 1_{Z(G)}$ we have

$$\mu^G(g) = p^{2m}\frac{\mu(g)}{|U|}\sum_{y\in Z(G)}\lambda(y) = p^m\mu(g) < \lambda, 1_{Z(G)} > = 0.$$

So μ^G does not depend on the choice of the maximal abelian normal subgroup U or on the choice of the extension μ of λ. The irreducibility of μ^G follows from

$$\begin{aligned} < \mu^G, \mu^G > &= \frac{1}{|G|} \sum_{g \in Z(G)} \mu^G(g)\mu^G(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g \in Z(G)} p^{2m} \lambda(g)\lambda(g^{-1}) = \frac{p^{2m+1}}{|G|} = 1. \end{aligned}$$

Finally, the sum of the squares of the degrees of the irreducible characters listed above is equal to the order of G and as a result we have found all the irreducible characters of G. □

Lemma 1.4.6 *Let G be an extra-special p-group of order p^{2m+1} and let H be an abelian subgroup of G. Suppose that $H \cap Z(G) = 1$ and $1_H \uparrow G$ is multiplicity-free. Then $HZ(G)$ is a maximal abelian normal subgroup of G and H has order p^m.*

Proof. Clearly, $HZ(G) = H \times Z(G)$ is a normal abelian subgroup of G and

$$1_H \uparrow HZ(G) = 1_{HZ(G)} + \lambda_1 + \cdots + \lambda_{r-1},$$

where each λ_i restricts to a distinct non-linear character of $Z(G)$. If $HZ(G)$ is not a maximal abelian normal subgroup of G. Then there exists a maximal abelian subgroup U of G containing $HZ(G)$. Furthermore, if $n = |U : HZ(G)|$, then

$$\begin{aligned} 1_H \uparrow U &= (1_H \uparrow HZ(G)) \uparrow U \\ &= 1_U + \mu_1 + \cdots + \mu_{n-1} \\ &\quad +\lambda_{11} + \cdots + \lambda_{1n} + \cdots + \lambda_{(r-1)1} + \cdots + \lambda_{(r-1)n} \end{aligned}$$

where λ_{ij} restricts to λ_i for all $j \in \{1, \dots, n\}$ and $i \in \{1, \dots, r-1\}$, and by Theorem 1.4.5 every non-linear irreducible character of G will appear as a constituent of $1_H \uparrow G$ with multiplicity n. The proof is complete. □

Lemma 1.4.7 *Let G be a non-abelian p-group. Suppose that $\Phi(G)$ has order p and $Z(G)$ has order p^{k+1}. Then $G = QZ(G)$, where Q is extra-special and $Q \cap Z(G) = \Phi(G)$. Furthermore, the restriction of every irreducible character of G to Q is irreducible. If θ is an irreducible character of Q, then there are exactly p^k irreducible characters of G, whose restriction to Q equals θ.*

Proof. We can view $G/\Phi(G)$ as a vector space over $GF(p)$. Since $\Phi(G) \subseteq Z(G)$, the group $Z(G)/\Phi(G)$ can be viewed as a subspace of $G/\Phi(G)$. If $Q/\Phi(G)$ is a complementary subspace of $Z(G)/\Phi(G)$ in $G/\Phi(G)$, then

$$G = QZ(G) \quad \text{and} \quad Q \cap Z(G) = \Phi(G).$$

Furthermore, $Z(Q) = \Phi(G)$, because $Z(Q) \subseteq Z(G)$. Thus Q is non- abelian, because G is non-abelian, and Q' must equal $\Phi(G)$. Finally, it is not difficult to see that $\Phi(Q)$ must also equal $\Phi(G)$, establishing our claim that Q is extra-special. Let $D = Q \times Z(G)$ and let

$$\overline{Q} = \{(q\,,1) \mid q \in Q\} \quad \text{and} \quad \overline{Z(G)} = \{(1\,,z) \mid z \in Z(G)\}.$$

Suppose that γ is a map from D to G defined by $\gamma((q,z)) = qz$. Then

$$\begin{aligned} \gamma((q_1,z_1)(q_2,z_2)) &= \gamma((q_1q_2,z_1z_2)) = q_1q_2z_1z_2 = q_1z_1q_2z_2 \\ &= \gamma((q_1,z_1))\gamma((q_2,z_2)), \end{aligned}$$

for all $q_i \in Q$ and $z_i \in Z(G)$. So γ is an epimorphism from D to G with kernel $K = \{(k\,,k^{-1}) \mid k \in Q \cap Z(G)\}$. Furthermore, the map

$$\Gamma : D/K = (\overline{Q}K/K)(\overline{Z(G)}K/K) \to G = QZ(G)$$

defined by $\Gamma((q,z)K) = \gamma((q,z)) = qz$ is an isomorphism with

$$\Gamma(\overline{Q}K/K) = Q.$$

So every irreducible character of G restricts to an irreducible character of Q if and only if every irreducible character of D/K restricts to an irreducible character of $\overline{Q}K/K$.

If $\hat{\chi} \in Irr(D/K)$, then there exists a $\chi \in Irr(D)$ such that $ker\chi \supseteq K$ and $\hat{\chi}(dK) = \chi(d)$ for all $d \in D$. If $\chi \in Irr(D)$, then $\chi((q,z)) = \theta(q)\phi(z)$, where $\theta \in Irr(Q)$ and $\phi \in Irr(Z(G))$, for all $q \in Q$ and $z \in Z(G)$. So

$$\hat{\chi}((q,1)K) = \chi((q,1)) = \theta(q)\phi(1) = \theta(q)$$

for all $q \in Q$. Thus the restriction of $\hat{\chi}$ to $\overline{Q}K/K$ is irreducible, because

$$< \hat{\chi}_{\overline{Q}K/K}, \hat{\chi}_{\overline{Q}K/K} > = < \theta, \theta > = 1.$$

If θ is an irreducible character of Q, then θ^G has degree

$$\theta(1)|G : Q| = \theta(1)p^k.$$

But from above we know that every irreducible constituent of θ^G is an extension of θ to G. So every irreducible constituent of θ^G occurs with multiplicity one and has degree $\theta(1)$. Thus G has exactly p^k irreducible characters, whose restriction to Q equals θ. □

Lemma 1.4.8 *Let G be a non-abelian special p-group and let $\mathcal{M}$ be the set of maximal subgroups of $Z(G)$. Then*

$$Irr(G) - Irr(G/Z(G)) = \bigcup_{M \in \mathcal{M}} \left(Irr(G/M) - Irr(G/Z(G))\right).$$

Furthermore if $M \in \mathcal{M}$, then G/M is a non- abelian p-group and $\Phi(G/M)$ has order p. Thus

$$Irr(G) - Irr(G/Z(G)) = \bigcup_{M \in \mathcal{M}} \{\chi \in Irr(G/M) | \chi(1) \neq 1\}$$

Proof. Suppose that $\chi \in Irr(G)$. Then $\chi_{Z(G)} = \chi(1)\lambda$ for some $\lambda \in Irr(Z(G))$ and $ker\lambda \supseteq M_1$ for some $M_1 \in \mathcal{M}$, since $Z(G)$ is elementary abelian. So $ker\chi \supseteq M_1$. Suppose that $ker\chi \supseteq M_2$, where $M_1 \neq M_2 \in \mathcal{M}$. Then $ker\chi \supseteq M_1M_2 = Z(G)$ and

$$Irr(G) - Irr(G/Z(G)) = \bigcup_{M \in \mathcal{M}} (Irr(G/M) - Irr(G/Z(G))).$$

Since $M \not\supseteq G'$, the factor group G/M is a non-abelian p-group. Furthermore, $\Phi(G/M) = \Phi(G)/M = Z(G)/M$ has order p, because M is a maximal subgroup of the elementary abelian p-group $Z(G)$. So by Lemma 1.4.7 $G = (Q/M)Z(G/M)$, where Q/M is extra-special and $Q/M \cap Z(G/M) = \Phi(G/M)$ and the restriction of every irreducible character of G to Q is irreducible. Thus the kernel of an irreducible character of G/M does not contain $Z(G)$ if and only if it's restriction to Q/M is faithful. The result follows by Theorem 1.4.5. □

1.5 Frobenius groups

Let G be a finite group and let C be a subgroup of G, with $1 < C < G$. Assume that $C \cap C^g = 1$ whenever $g \in G - C$. Then C is a *Frobenius complement* in G. A group which contains a Frobenius complement is called a *Frobenius group*.

Lemma 1.5.1 *Let G be a Frobenius group with Frobenius complement C. Then $|C|$ divides $|G : C| - 1$.*

Proof. Huppert [2, Satz 8.3 page 497] Since $\bigcap_{g \in G} C^g = 1$, we can view G as a permutation group acting on the set of right cosets of C in G. In particular, we can view C as a permutation group acting on the set of right cosets of C in G. Suppose that $Ch \neq C$ is a right coset of C in G. Then $C \cap C^h = 1$ is the stabilizer of Ch in C and Ch is contained in an orbit of length $|C|$. The result follows. □

Lemma 1.5.2 *Let C be a Frobenius complement in G. Let*

$$N = \left(G - \bigcup_{g \in G} C^g \right) \cup \{1\}$$

Then $|N| = |G : C|$. If $M \lhd G$ with $M \cap C = 1$, then $M \subseteq N$.

Proof. Isaacs [1, (7.3) Lemma, page 100]. Since $C = N_G(C)$, there are $|G : C|$ distinct subgroups of the form C^g. These contain exactly $|G : C| \left(|C| - 1\right)$ non- identity elements. The remaining elements of G constitute the set N. We have

$$|N| = |G| - |G : C| \left(|C| - 1\right) = |G| - |G| + |G : C| = |G : C|.$$

If $M \lhd G$ with $M \cap C = 1$, then $M \cap C^g = 1$ for all $g \in G$ and thus $M \subseteq N$. The proof is complete. □

Lemma 1.5.3 *Let C be a Frobenius complement in G. Let θ be a class function of C which satisfies $\theta(1) = 0$. Then $(\theta^G)_C = \theta$.*

Proof. Isaacs [1, (7.4) Lemma, page 100]. Let $1 \neq c \in C$. Then

$$\theta^G(c) = \frac{1}{|C|} \sum_{x \in G} \theta^\circ(xcx^{-1}),$$

where θ° is defined by $\theta^\circ(c) = \theta(c)$ if $c \in C$ and $\theta^\circ(y) = 0$ if $y \notin C$. If $\theta^\circ(xcx^{-1}) \neq 0$, then $1 \neq xcx^{-1} \in C \cap C^{x^{-1}}$ and $x \in C$. Then $\theta^\circ(xcx^{-1}) = \theta(c)$. We have

$$\theta^G(c) = \frac{1}{|C|} \sum_{x \in C} \theta(c) = \theta(c).$$

Since $\theta^G(1) = |G : H|\theta(1) = 0$, the proof is complete. □

Theorem 1.5.4 *Let G be a Frobenius group and let C be a Frobenius complement in G. Then $N = \left(G - \bigcup_{g \in G} C^g\right) \cup \{1\}$ is a normal subgroup of G with $NC = G$ and $C \cap N$=1.*

Proof. Isaacs [1, (7.2) Theorem, page 100-101]. Let $1_C \neq \varphi \in \mathit{Irr}(C)$ and write $\theta = \varphi - \varphi(1)1_C$ so that $\theta(1) = 0$. Now

$$\langle \theta^G, \theta^G \rangle = \langle \theta, (\theta^G)_C \rangle = \langle \theta, \theta \rangle$$

by Frobenius reciprocity and Lemma 1.5.3. Thus $\langle \theta^G, \theta^G \rangle = 1 + \varphi(1)^2$. Now $\langle \theta^G, 1_G \rangle = \langle \theta, 1_C \rangle = -\varphi(1)$. We may therefore write $\theta^G = \varphi^* - \varphi(1)1_G$, where φ^* is a class function of G, $\langle \varphi^*, 1_G \rangle = 0$, and $1 + \varphi(1)^2 = \langle \varphi^*, \varphi^* \rangle + \varphi(1)^2$, so that $\langle \varphi^*, \varphi^* \rangle = 1$. Since θ is a difference of characters, so is θ^G and hence φ^* is a difference of characters also. Since $\langle \varphi^*, \varphi^* \rangle = 1$, it follows that $\pm\varphi^* \in \mathit{Irr}(G)$. Furthermore, $c \in C$, then

$$\varphi^*(c) = \theta^G(c) + \varphi(1) = \theta(c) + \varphi(1) = \varphi(c).$$

In particular, $\varphi^*(1) > 0$ and thus $\varphi^* \in Irr(G)$. For every non-principal $\varphi \in Irr(C)$, we have now chosen an extension, $\varphi^* \in Irr(G)$. Let $M = \bigcap_{\varphi \in Irr(C)} ker\varphi^*$. If $m \in M \cap C$, then $\varphi(m) = \varphi^*(m) = \varphi^*(1) = \varphi(1)$ for all $\varphi \in Irr(C)$ and thus $m = 1$. By Lemma 1.5.2, $M \subseteq N$. Conversely, if $g \in G$ lies in no conjugate of C, then

$$\varphi^*(g) - \varphi(1) = \theta^G(g) = 0$$

and $g \in ker\varphi^*$. It follows that $M = N$ and hence the normal subgroup M satisfies $|M| = |G : C|$. We have $|MC| = |M||C| = |G : C||C| = |G|$ and the result follows. □

The normal subgroup whose existence is guaranteed by Theorem 1.5.4 is called the *Frobenius kernel* of G. If $T = \{g_1, \ldots, g_j\}$ is a right transversal for C in G, then the decomposition

$$G = N \cup C^{g_1} \cup \cdots \cup C^{g_j}$$

into subgroups of G, any two of which have trivial intersection, is called the *Frobenius partition* of G.

1.6 Characters of Frobenius groups

We shall now go on to describe the irreducible characters of a Frobenius group.

Lemma 1.6.1 *Let G be a Frobenius group with Frobenius complement C and Frobenius Kernel N. Then $C_G(n) \subseteq N$ for all $1 \neq n \in N$.*

Proof. Suppose $g \in G - N$ is such that $n^g = n$ for some $1 \neq n \in N$. Then from the Frobenius partition of G, we see that there exixts an $h \in G$ with $g^h = c$ for some $c \in C$. Thus $m^c = m$, where $m = n^h$. Since $m \in G - C$,

$$m^{-1}cm = c \in C \cap C^m = 1$$

and g must equal the identity. In particular, $g \notin G - N$. □

Theorem 1.6.2 *Let A be a group which acts on $Irr(G)$ and on the set of conjugacy classes of G. Assume that $\chi(g) = \chi^a(g^a)$ for all $\chi \in Irr(G)$, $a \in A$ and $g \in G$; where g^a is an element of $Cl(g)^a$. Then for each $a \in A$, the number of fixed irreducible characters of G is equal to the number of fixed classes.*

Proof. Isaacs [1, (6.32) Theorem, pages 93-94], Let χ_i and K_j be the irreducible characters and conjugacy classes of G for $1 \leq i, j \leq k$. Choose $g_j \in K_j$ and write $g_i^a = g_j$ if $K_i^a = K_j$. Let $X = (\chi_i(g_j))$, the character table of G, viewed as a matrix. For $a \in A$, let $P(a) = (p_{ij})$, where $p_{ij} = 0$ unless $\chi_i^a = \chi_j$, in which case $p_{ij} = 1$. Similarly, define $Q(a) = (q_{ij})$, where $q_{ij} = 1$ if $K_i^a = K_j$ and is zero otherwise. The (u, v) entry of the matrix $P(a)X$ is

$$\sum_i p_{ui}\chi_i(g_v) = \chi_u^a(g_v)$$

since only when $\chi_i = \chi_u^a$ is $p_{ui} \neq 0$. Similarly, the (u, v) entry of the matrix $XQ(a)$ is

$$\sum_j \chi_u(g_j)q_{jv} = \chi_u(g^{a^{-1}})$$

since only when $g_j = g_u^{a^{-1}}$ is $q_{jv} \neq 0$. The hypothesis of the theorem now implies that $P(a)X = XQ(a)$. Thus $Q(a) = X^{-1}P(a)X$ since the orthogonality relations guarantee that X is non-singular. We conclude that

$Trace(P(a)) = Trace(Q(a))$. Since $Trace(P(a))$ is the number of $\chi \in Irr(G)$ which a fixes and $Trace(Q(a))$ is the number of a- fixed conjugacy classes, the proof is complete. □

Theorem 1.6.3 *Let $N \triangleleft G$ and assume that $C_G(n) \subseteq N$ for all $1 \neq n \in N$. Then for $\varphi \in Irr(N)$, with $\varphi \neq 1_N$, we have $I_G(\varphi) = N$ and $\varphi\uparrow^G \in Irr(G)$.*

Proof. Isaacs [1, (6.34)(a) Theorem pages 94], Let $\varphi \in Irr(N)$, $\varphi \neq 1_N$. To show that $\varphi^G \in Irr(N)$, it suffices to show that $I_G(\varphi) = N$. Therefore by Theorem 1.6.2 we need to show that no element $g \in G - N$ can normalize any non-trivial conjugacy class of N. Suppose then, $g \in G - N$ normalizes $\mathcal{K}$, a class of N. Let $k \in \mathcal{K}$. Then $k^g \in \mathcal{K}$ and thus $k^g = k^n$ for some $n \in N$. Therefore $gn^{-1} \in C(k)$. Since $gn^{-1} \notin N$ and $k \in N$, the hypothesis yields $k = 1$ and thus $\mathcal{K} = \{1\}$. The result follows. □

Theorem 1.6.4 *Let G be a Frobenius group with Frobenius complement C and Frobenius Kernel N. Then G has the following irreducible characters.*

(a) *The lifts of the irreducible characters of $G/N \cong C$.*

(b) $\frac{|Irr(N)|-1}{|C|}$ *irreducible characters, of the following form : $\varphi\uparrow^G$, where φ is a non-trivial character of N. Two non-trivial irreducible charcters of N, induce the same irreducible character of G if and only if they are conjugate in G.*

Proof. Isaacs [1, (6.34)(b) Theorem pages 94], Let $\chi \in Irr(G)$ with $N \not\subseteq ker\chi$. Then χ_N has an irreducible constituent $\varphi \neq 1_N$. So χ is a constituent of $\varphi\uparrow^G$, by Frobenius reciprocity. But Lemma 1.6.1 and Theorem 1.6.3 state that $\varphi\uparrow^G$ is irreducible. Thus $\varphi\uparrow^G = \chi$. Now φ has $|C|$ conjugates in G, since

$I_G(\varphi) = N$ by Theorem 1.6.3. So there are exactly $|C|$ irreducible characters of N, whose induced character equals χ. The result follows. □

1.7 Fixed-point free automorphisms

Suppose that α is an automorphism of N. Then we say that α is *fixed-point free*, if the only element of N left fixed by α is the identity. A subgroup C of $Aut(N)$ is called *fixed-point free*, if every non-identity element of C is a fixed-point free automorphism of N. The following results can be found in Huppert [2, Satz 8.5, page 497-506].

Lemma 1.7.1 *The following statements are equivalent :*

(a) *G is a Frobenius group with Frobenius complement C and Frobenius Kernel N.*

(b) *$G = NC$ with $C < G$ and $N \triangleleft G$. The mapping μ from C into $Aut(N)$ defined by $n^{c^\mu} = c^{-1}nc$ for $c \in C$ and $n \in N$ is an isomorphism from C onto a fixed-point-free group of automorphisms of N.*

Proof. $(a) \Rightarrow (b)$: Let $c \in C$ and $n \in N$ with $n^c = n$. Then

$$n^{-1}cn = c \in C \cap C^n.$$

If $n \neq 1$, then $n \in G - C$ and $C \cap C^n = 1$, so $c = 1$. If $c \neq 1$, then $n \in C$ and thus $n = 1$. The proof is complete.

$(b) \Rightarrow (a)$: Let $g \in N \cap C$. Then $g = g^g$ and $g = 1$, since we are assuming that C acts fixed-point freely on N. So $N \cap C = 1$ and $G = NC$ is a semi-direct product of N and C. Let $c_1 \in C \cap C^g$ with $g \in G - C$. Then $g = cn$

with $c \in C$ and $1 \neq n \in N$. So $C^g = C^n$ and

$$c_1 = c_2^n \in C \cap C^n$$

with $c_2 \in C$. Since $N \lhd G$, we have

$$c_1 c_2^{-1} = \left[n, c_2^{-1}\right] \in N \cap C = 1,$$

and $c_1 = c_2$. So $n^c = n$ and $c = 1$, since $n \neq 1$. Thus $C \cap C^g = 1$ and G is a Frobenius group with Frobenius complement C. □

Lemma 1.7.2 *Let α be a fixed-point free automorphism of N. The map $\mu : N \to N$ with $\mu(n) = n^{-1}n^{\alpha}$ is a bijection.*

Proof. Suppose that $n_1, n_2 \in R$ such that

$$n_1^{-1}n_1^{\alpha} = \mu(n_1) = \mu(n_2) = n_2^{-1}n_2^{\alpha}.$$

Then $n_1 n_2^{-1} = (n_1 n_2^{-1})^{\alpha}$ and $n_1 = n_2$, because α acts fixed-point freely on N. The result follows. □

Lemma 1.7.3 *Let C be a fixed-point free group of automorphisms of N. Suppose that C has even order. Then C has a unique element c of order 2 and $n^c = n^{-1}$ for all $n \in N$. Moreover, N must be abelian.*

Proof. Let $c \in C$ with $O(c) = 2$ and $\mu(c)$ be the bijective map from N onto itself defined Lemma 1.7.2. Then for all $n \in N$ there exists an $m \in N$ such that $n = m^{-1}m^c$ and

$$n^c = (m^{-1}m^c)^c = (m^{-1})^c m^{c^2} = (m^c)^{-1}m = (m^{-1}m^c)^{-1} = n^{-1}.$$

If c_1 and c_2 are involutions of C. Then $c_2^{-1}c_1 \in C_C(N) = 1$. Thus $c_1 = c_2$. Finally, N is abelian, because it admits an automorphism that maps every element to its inverse. □

Lemma 1.7.4 *Let α be a fixed-point free automorphism of N and let R be a normal subgroup of N with $R^\alpha = R$. Then α induces a fixed-point free automorphism on R and N/R.*

Proof. Clearly α acts fixed-point freely on R. So by Lemma 1.7.2

$$R = \{r^{-1}r^\alpha | r \in R\}.$$

Now let $n \in N$ and $nR = n^\alpha R$. Then $n^{-1}n^\alpha \in R$, so $n^{-1}n^\alpha = r^{-1}r^\alpha$ for some $r \in R$. It follows that $nr^{-1} = (nr^{-1})^\alpha$ and n must equal r. Therefore α induces a fixed-point free automorphism $\bar{\alpha}$ on N/R with $(nR)^{\bar{\alpha}} = n^\alpha R$. □

Lemma 1.7.5 *Let V be a vector space of any dimension over a field K and let C be a finite group of linear maps of V into itself. Let C be fixed point free, in other words $vc \neq v$ for all $1 \neq c \in C$ and $0 \neq v \in V$. Suppose that $|C| = pq$, where p and q are not necessarily distinct primes. Then C is cyclic.*

Proof. If $p = q$ and C is not cyclic, then C has exactly $p + 1$ subgroups C_i of order p. Then $C = \bigcup_{i=1}^{p+1} C_i$ and $C_i \cap Cj = 1$ for $i \neq j$. If $p > q$ and C not cyclic. Then C has exactly one p-Sylow subgroup C_1 and p distinct q-Sylow subgroups $C_2, \ldots, C_{p+1}$. Once again $C = \bigcap_{i=1}^{p+1} C_i$ and $C_i \cap C_j = 1$ for $i \neq j$. We shall now consider the two cases simultaneously. Let $0 \neq v \in V$ and $1 \neq c' \in C$. Then

$$\left(\sum_{c \in C} vc\right) c' = \sum_{c \in C} vc,$$

so, since C is fixed point free, $\sum_{c\in C} vc = 0$. We can show similarly that $\sum_{c\in C_i} vc = 0$. Hence

$$0 = \sum_{c\in C} vc = -pv + \sum_{i=1}^{p+1} \sum_{c\in C_i} vc = -pv$$

and the characteristic of K is p. Let $d \in C$ of order p. Since the characteristic of K equals p we have

$$0 = v\,(d^p - 1) = v\,(d-1)^p\,.$$

Therefore there is an i with $0 \leq i < p$ and $v\,(d-1)^i \neq 0$, but $v\,(d-1)^{i+1} = 0$. Thus $w = v\,(d-1)^i$ and $wd = w \neq 0$ contradicting our assumption that C acts fixed-point freely on V. □

Theorem 1.7.6 ***[Thompson]*** *If N has a fixed-point free automorphism of prime order, then N is nilpotent.*

Proof. Huppert [2, Satz 8.13, page 502]. □

Lemma 1.7.7 *Let P be a non-cyclic p-group for some prime $p > 2$. Then P contains an elementary abelian subgroup of order p^2.*

Proof. We shall prove the result by induction on the order of P. If P is a non-cyclic p-group of order p^2 then P itself is elementary abelian. Assume P is a non-cyclic p-group of order greater than p^2 and every non-cyclic p-group of order less than P has an elementary abelian subgroup of order p^2. Let Q be a normal subgroup of P of order p. Suppose that P/Q is cyclic. Then P is abelian and every minimal generating set of P has two elements. Thus $\Omega_1(P)$ is elementary abelian of order p^2. So we may assume that P/Q

is non-cyclic and as a result contains an elementary abelian subgroup T/Q of order p^2. So $T' \subseteq Q$ and this fact combined with our assumption that $p > 2$ ensures that

$$(xy)^p = x^p y^p [x, y]^{\binom{p}{2}} = x^p y^p.$$

So the map $t \rightarrow t^p$ is a homomorphism from T to Q, whose kernel has exponent p and order greater than or equal to p^2. Thus every subgroup of the kernel of order p^2 is elementary abelian. The result follows. □

Theorem 1.7.8 *Let C be a fixed-point free group of automorphisms of N. Suppose that C has odd order. Then every p-Sylow subgroup of C is cyclic.*

Proof. We can assume that $C \neq 1$. So C contains an element of prime order, which induces a fixed point free automorphism of prime order on N. So N is nilpotent by Theorem 1.7.6. Let Q be a p-Sylow subgroup of the nilpotent group N. Then by Lemma 1.7.4 every element of C induces a fixed-point free automorphism on $Q/\Phi(Q)$. So C is isomorphic to a group of fixed- point free automorphisms of the elementary abelian group $Q/\Phi(Q)$. Since we can view $Q/\Phi(Q)$ as a vector space over $GF(p)$, Lemma 1.7.5 states that every subgroup of order pq of C is cyclic. So every p-Sylow subgroup of C must be cyclic by Lemma 1.7.7. The proof is complete. □

Chapter 2

Model subgroups

Let G be a finite group and let $Irr(G)$ be the set of irreducible characters of G. Suppose there exists a set $\mathcal{M}$ of monomial characters of G satisfying

$$\sum_{\chi \in Irr(G)} \chi = \sum_{\tau \in \mathcal{M}} \tau.$$

Then we say that $\mathcal{M}$ is a model of length n for G, where n is the cardinality of $\mathcal{M}$.

2.1 Definition

Suppose that G has a model of length 1. Then a linear character λ of a subgroup H of G exists such that

$$\lambda \uparrow^G = \sum_{\chi \in Irr(G)} \chi.$$

By Frobenius reciprocity, we have $\langle \lambda, 1_H \rangle = \langle \lambda \uparrow^G, 1_G \rangle = 1$. So λ must be the trivial character of H. With this observation in mind, we shall call H a *model subgroup* of G if

$$1_H\uparrow^G = \sum_{\chi \in Irr(G)} \chi.$$

Theorem 2.1.1 *Let G be a finite group. Then H is a model subgroup of G if and only if*

$$\sum_{h \in H} \chi(h) = |H|,$$

for all $\chi \in Irr(G)$.

Proof. Let $\chi \in Irr(G)$. Then

$$\begin{aligned} \sum_{h \in H} \chi(h) &= |H| \left(\frac{1}{|H|} \sum_{h \in H} \chi(h) \right) \\ &= |H| \left(\frac{1}{|H|} \sum_{h \in H} \chi(h) \overline{1_H(h)} \right) = |H| \langle \chi_H, 1_H \rangle. \end{aligned}$$

The result follows by Frobenius reciprocity. □

Corollary 2.1.2 *Let G be a finite group. Then G is abelian if and only if the trivial subgroup of G is the unique model subgroup of G.*

Proof. By Theorem 2.1.1 the trivial subgroup of a finite group G is a model subgroup if and only if every irreducible character of G is linear, which is the case if and only if G is abelian. Since two model subgroups of a finite group G have the same index in G, it follows that the trivial subgroup must be the unique model subgroup if it is a model subgroup. □

2.2 Examples

So every finite abelian group has a model subgroup. However, it is not true that a finite group G, which has a model subgroup, is necessarily abelian. We shall illustrate this statement with the following examples.

Let G be the alternating group of degree 4. Then G is generated by the permutations (12)(34) and (123). The order of G is 12 and the elements

$$(1)\ ,\ (12)(34)\ ,\ (123)\ ,\ (132)$$

form a set of conjugacy class representatives of G. So G has four irreducible characters. Since $G' = <(12)(34), (13)(24)>$ and $G/G' \cong C_3$, we obtain

g_i	(1)	(12)(34)	(123)	(132)
$\|C_G(g_i)\|$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4				

where $\omega = e^{\frac{2\pi i}{3}}$. Since the sum of the squares of the irreducible characters equals the order of G, the degree of χ_4 must be 3. Finally, using the orthogonality relations to completely determine χ_4, we obtain

g_i	(1)	(12)(34)	(123)	(132)
$\lvert C_G(g_i)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

where $\omega = e^{\frac{2\pi i}{3}}$. Now $\chi((1)) + \chi((12)(34)) = 2$ for all $\chi \in Irr(G)$. So, by Theorem 2.1.1, the subgroup of order two generated by the permutation (12)(34) is a model subgroup of G.

Let $F = \mathbb{F}_{2^n}$ and let ϵ be a primitive generator of F. Suppose that

$$G = [F^+] < \epsilon >,$$

the external semi-direct product of the elementary abelian group F^+ and the cyclic group $< \epsilon >$ of order $2^n - 1$ via σ, where σ is the homomorphism from $< \epsilon >$ to $Aut(F^+)$ defined by

$$x^{\sigma(\epsilon^i)} = x\epsilon^i \quad \text{(field multiplication)}$$

for all $x \in F^+$ and $0 \leq i \leq 2^n - 1$. Then G is a Frobenius group with Frobenius complement $< \epsilon >$ and Frobenius kernel F^+ by Lemma 1.7.1. So G has $2^n - 1$ linear characters $\lambda_1, \ldots, \lambda_{2^n - 1}$ and a unique non-linear character χ of order $2^n - 1$ by Theorem 1.6.4. Furthermore, if ρ is the regular character of F^+, then

$$\chi_{F^+} = \rho - 1_{F^+}.$$

Now suppose that M is a maximal subgroup of F^+. Then

$$\sum_{m \in M} \lambda_i(m) = |M|,$$

because $M \subseteq \ker \lambda_i$ for all i, and

$$\begin{aligned}\sum_{m \in M} \chi(m) &= \sum_{m \in M} \rho(m) - 1_{F^+}(m) \\ &= (|F^+| - 1) + \sum_{1 \neq m \in M} -1 \\ &= (2^n - 1) - (2^{n-1} - 1) = 2^{n-1} = |M|.\end{aligned}$$

Thus M is a model subgroup of G by Theorem 2.1.1. When $n = 2$, the finite group G has order 12 and is isomorphic to A_4.

2.3 Epimorphic images

Lemma 2.3.1 *Let G be a finite group and let N be a normal subgroup of G. Let $\chi \in Irr(G/N)$ and let $\hat{\chi}$ be the corresponding irreducible character of G/N. Suppose that H is a subgroup of G. Then*

$$\langle 1_{HN/N}, \hat{\chi}_{HN/N} \rangle = \langle 1_H, \chi_H \rangle.$$

Proof.

$$\begin{aligned}\langle 1_{HN/N}, \hat{\chi}_{HN/N} \rangle &= \frac{1}{|HN/N|} \sum_{Nh \in \frac{HN}{N}} \hat{\chi}(Nh) = \frac{|H \cap N|}{|H|} \sum_{Nh \in \frac{HN}{N}} \hat{\chi}(Nh) \\ &= \frac{1}{|H|} \sum_{h \in H} \hat{\chi}(Nh) \\ &= \frac{1}{|H|} \sum_{h \in H} \chi(h) = \langle 1_H, \chi_H \rangle.\end{aligned}$$

The proof is complete. □

Theorem 2.3.2 *Let G be a finite group and let N be a normal subgroup of G. Suppose that H is a model subgroup of G. Then HN/N is a model subgroup of G/N.*

Proof. Suppose that $\chi \in Irr(G/N)$ and $\hat{\chi}$ is the corresponding irreducible character of G/N. Then

$$\langle 1_{HN/N}, \hat{\chi}_{HN/N} \rangle = \langle 1_H, \chi_H \rangle,$$

by Lemma 2.3.1, and

$$\langle 1_H, \chi_H \rangle = 1,$$

because H is a model subgroup of G. The result follows from Theorem 2.1.1.

□

Corollary 2.3.3 *Let G be a finite group and let H be a model subgroup of G. Then H is a subgroup of G'.*

Proof. By Theorem 2.3.2, we know that HG'/G' is a model subgroup of G/G'. But G/G' is abelian. So HG'/G' is the trivial subgroup of G/G', by Corolla ry 2.1.2. Thus H must be a subgroup of G'. □

2.4 Direct Products

Theorem 2.4.1 *Suppose that H_1 and H_2 are model subgroups of G_1 and G_2 respectively. Then*

$$H = H_1 \times H_2$$

is a model subgroup of $G = G_1 \times G_2$.

Proof. Let $\chi \in Irr(G)$. Then $\chi = \theta\phi$ for some $\theta \in Irr(G_1)$ and $\phi \in Irr(G_2)$. Thus

$$\begin{aligned}\sum_{h\in H}\chi(h) &= \sum_{h_1\in H_1}\sum_{h_2\in H_2}\theta(h_1)\phi(h_2)\\ &= \left(\sum_{h_1\in H_1}\theta(h_1)\right)\left(\sum_{h_2\in H_2}\phi(h_2)\right).\end{aligned}$$

But H_1 and H_2 are model subgroups of G_1 and G_2 respectively. So

$$\begin{aligned}\sum_{h_1\in H_1}\theta(h_1) &= |H_1| \text{ and}\\ \sum_{h_2\in H_2}\phi(h_2) &= |H_2|,\end{aligned}$$

by Theorem 2.1.1. Hence

$$\sum_{h\in H}\chi(h) = |H_1| \times |H_2| = |H|,$$

and H is a model subgroup of G by Theorem 2.1.1. □

Theorem 2.4.2 *Suppose that $G = G_1 \times \cdots \times G_m$. Then H is a model subgroup of G if and only if the following statements hold.*

(a) $H = (H \cap G_1) \times \cdots \times (H \cap G_m)$.

(b) *$H \cap G_i$ is a model subgroup of G_i for $i \in \{1, \ldots, m\}$.*

Proof. We may assume without loss of generality that $m = 2$.

Suppose that H is a model subgroup of G. Then

$$\frac{HG_1}{G_1} \cong \frac{H}{H\cap G_1}$$

is a model subgroup of $G/G_1 \cong G_2$ by Theorem 2.3.2. So G_2 has a model subgroup of order

$$\frac{|H|}{|H \cap G_1|}.$$

We can show similarly that G_1 has a model subgroup of order

$$\frac{|H|}{|H \cap G_2|}.$$

Thus by Theorem 2.4.1 G has a model subgroup of order

$$\frac{|H|}{|H \cap G_1|} \times \frac{|H|}{|H \cap G_2|} = \frac{|H|^2}{|H \cap G_1| \times |H \cap G_2|}.$$

But the order of a model subgroup is determined by the sum of the character degrees of G and is thus uniquely determined. So

$$|H| = \frac{|H|^2}{|H \cap G_1| \times |H \cap G_2|},$$

which implies that

$$H = (H \cap G_1) \times (H \cap G_2).$$

Let ρ be the isomorphism from G_1 to G/G_2 satisfying $\rho(g_1) = g_1G_2$ for all $g_1 \in G_1$. Then

$$\rho_1(H \cap G_1) = HG_2/G_2$$

and $H \cap G_1$ is a model subgroup of G_1, since HG_2/G_2 is a model subgroup of G/G_1. We can show similarly that $H \cap G_2$ is a model subgroup of G_2.

Now suppose that $H = (H \cap G_1) \times (H \cap G_2)$ and $H \cap G_i$ is a model subgroup of G_i for $i \in \{1, 2\}$. Then H is a model subgroup of G by Theorem 2.4.1. The proof is complete. □

2.5 Central Products

Lemma 2.5.1 *Let G be a finite group and let N be a normal subgroup of G. Suppose that $G' \cap N = 1$. Then every irreducible character of G is of the form $\chi\lambda$, where $\chi \in Irr(G/N)$ and $\lambda \in Irr(G/G')$.*

Proof. Since $G' \cap N = 1$, the normal subgroup $N \subseteq Z(G)$ and

$$NG' = N \times G'.$$

Suppose that $\phi \in Irr(N)$. Then $\varphi = \phi 1_{G'}$, is a linear character of NG' such that $G' \subseteq ker\varphi$ and $\varphi_N = \phi$. Hence

$$\varphi \in Irr(NG'/G')$$

and there exists a $\lambda \in Irr(G/G')$ such that $\lambda_{NG'} = \varphi$. Thus $\lambda_N = \phi$. So we can choose

$$\lambda_1, \ldots, \lambda_{|N|} \in Irr(G/G')$$

such that $(\lambda_i)_N \neq (\lambda_j)_N$ for $i \neq j$. Now let $\chi, \theta \in Irr(G/N)$. Suppose that $\chi\lambda_i = \theta\lambda_j$. Then

$$\chi(1)(\lambda_i)_N = (\chi\lambda_i)_N = (\theta\lambda_j)_N = \theta(1)(\lambda_j)_N.$$

Thus $\lambda_i = \lambda_j$ and $\chi = \theta$. We have found $|Irr(G/N)| \times |N|$ distinct irreducible characters of G and the sum of the squares of the degrees of these characters is equal to $|G|$. So every irreducible character of G has the form $\chi\lambda$, where $\chi \in Irr(G/N)$ and $\lambda \in Irr(G/G')$. □

Theorem 2.5.2 *Let G be a finite group and let N be a normal subgroup of G. Suppose that $G' \cap N = 1$. Then G has a model subgroup if and only if G/N has a model subgroup.*

Proof. Suppose that G has a model subgroup, then G/N has a model subgroup by Theorem 2.3.2.

Suppose that G/N has a model subgroup H/N. Let $\mu \in Irr(G)$. Then by Lemma 2.5.1 $\mu = \chi\lambda$, for some $\chi \in Irr(G/N)$ and $\lambda \in Irr(G/G')$. So

$$\sum_{h \in H \cap G'} \mu(h) = \sum_{h \in H \cap G'} \chi\lambda(h) = \sum_{h \in H \cap G'} \chi(h)\lambda(h) = \sum_{h \in H \cap G'} \chi(h).$$

Then $N \subseteq H \subseteq G$ and $H \subseteq NG'$ since $H/N \subseteq (G/N)'$, by Corolla ry 2.3.3. Thus $H = NG' \cap H = N(G' \cap H)$.

$$\sum_{h \in H \cap G'} \chi(h) = \sum_{Nh \in H/N} \tilde{\chi}(Nh) = |H/N| = |H \cap G'|,$$

by Theorem 2.1.1 and $H \cap G'$ is a model subgroup of G. □

Theorem 2.5.3 *Let G be a central product of $G_1, \dots, G_m$. Suppose that $G_i' \cap Z(G_i) = 1$ for all i. Then G has a model subgroup if and only if G_i has a model subgroup for $1 \leq i \leq m$.*

Proof. Suppose that G has a model subgroup. Let

$$\hat{G}_i = G_1 \dots G_{i-1}G_{i+1} \dots G_m.$$

Then the quotient group

$$\frac{G_i}{G_i \cap \hat{G}_i} \cong \frac{G}{\hat{G}_i}$$

has a model subgroup by Theorem 2.3.2. But

$$G_i \cap \hat{G}_i \subseteq Z(G_i)$$

and thus intersects trivially with G_i'. Hence G_i has a model subgroup by Theorem 2.5.2.

Suppose that G_i has a model subgroup for $1 \leq i \leq m$. Let

$$D = G_1 \times \cdots \times G_m.$$

Then the map ϵ from D to G defined by

$$\epsilon : (g_1, \ldots, g_m) \rightarrow g_1 \ldots g_m$$

is an epimorphism. Furthermore, D has a model subgroup by Theorem 2.4.2. Hence G has a model subgroup by Theorem 2.3.2. □

2.6 Nilpotent groups

We have already seen that non-abelian finite groups with model subgroups exist. However non-abelian finite nilpotent groups with model subgroups do not.

Lemma 2.6.1 *Let G be a finite group and let H be a model subgroup of G. Then $H \cap Z(G) = 1$.*

Proof. Let $\chi \in Irr(G)$. Since H is a model subgroup of G, we have $\langle \chi_H, 1_H \rangle = 1$. So $\langle \chi_{H \cap Z(G)}, 1_{H \cap Z(G)} \rangle \neq 0$ and $\chi_{H \cap Z(G)} = \chi(1) 1_{H \cap Z(G)}$. Thus $H \cap Z(G)$ is a subgroup of the kernel of χ and

$$H \cap Z(G) \subseteq \bigcap_{\chi \in Irr(G)} ker \chi = 1.$$

The proof is complete. □

Theorem 2.6.2 *Let G be a finite nilpotent group. Then G has a model subgroup if and only if G is abelian.*

Proof. Suppose that G is minimal such that G is non-abelian and G has a model subgroup, H say. Then $HZ(G)/Z(G)$ is a model subgroup of $G/Z(G)$, by Theorem 2.3.2. So $G/Z(G)$ must be abelian, by the minimality of G. Thus G' is a subgroup of Z(G). Since H is a subgroup of G' and $H \cap Z(G) = 1$, by Corolla ry 2.3.3 and Lemma 2.6.1 we see that H must be the trivial subgroup of G. But this contradicts Corolla ry 2.1.2 and the result follows. □

Chapter 3

Frobenius groups

In the previous chapter we gave some examples of Frobenius groups possessing model subgroups. We shall now derive necessary and sufficient conditions for a Frobenius group to admit a model subgroup.

3.1 Complements and model subgroups

In this section we shall prove that if a Frobenius group admits a model subgroup, then its Frobenius complement is cyclic of odd order.

Theorem 3.1.1 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that G has a model subgroup. Then C has odd order.*

Proof. Let $\chi \in Irr(G)$ satisfying $N \not\subseteq ker\chi$. Then by Theorem 1.6.4 $\chi = \theta^G$ for some $\theta \in Irr(N)$ and

$$\chi_N = \theta_1 + \cdots + \theta_{|C|},$$

where $\theta = \theta_1, \ldots, \theta_{|C|}$ are the conjugates of θ in G. Let c be the unique element of C of order 2 satisfying

$$n^c = n^{-1}$$

for all $n \in N$, whose existence is guaranteed by Lemma 1.7.3. If K is a subgroup of N, then

$$\begin{aligned} < 1_K , \theta_K > &= \frac{1}{|K|}\sum_{k\in K}\theta(k) \\ &= \frac{1}{|K|}\sum_{k\in K}\theta(k^{-1}) \\ &= \frac{1}{|K|}\sum_{k\in K}\theta^c(k) \quad = < 1_K , \theta^c_K > . \end{aligned}$$

So $< 1_K , \chi_K >= 2m$ for some $m \geq 0$. Now suppose that H is a model subgroup of G and $K = H \cap N$. Then

$$\sum_{k\in K}\chi(k) = \sum_{h\in H}\chi(h) = |H|,$$

by Theorem 2.1.1 and because χ vanishes outside N. Furthermore, HN/N is a model subgroup of G/N by Theorem 2.3.2 and $HN/N \cap Z(G/N) = 1$ by Lemma 2.6.1. However

$$|HN/N| = \frac{|H|}{|H \cap N|} = \frac{|H|}{|K|} = \frac{1}{|K|}\sum_{k\in K}\chi(k) = < 1_K , \chi_K >= 2m$$

and the subgroup HN/N of $G/N \cong C$ must contain the unique element of G/N of order 2. This element is clearly contained in the centre of G/N contradicting $HN/N \cap Z(G/N) = 1$. The proof is complete. □

Lemma 3.1.2 *Let G be a finite group. Suppose that every p-Sylow subgroup of G is cyclic. Then G is soluble.*

Proof. Huppert [2, Satz 2.8, page 420] Let P be a p-Sylow subgroup of G, where p is the smallest prime dividing the order of G. Then

$$N_G(P) \supseteq C_G(P) \supseteq P,$$

because P is cyclic, and $N_G(P)/C_G(P) \subseteq Aut(P)$. Now suppose that

$$1 \neq nC_G(P) \in N_G(P)/C_G(P)$$

induces the automorphism α on P and the non-trivial automorphism $\bar{\alpha}$ on

$$P/\Phi(P) \cong C_p.$$

Then p does not divide the order of $\bar{\alpha}$. So $1 \neq o(\bar{\alpha})|p-1$ and

$$(o(\alpha), p-1) \neq 1.$$

But if q is a prime dividing the order of α then $q > p$. Therefore $N_G(P)$ must equal $C_G(P)$ and consequently P has a normal p-complement R in G. The result follows by induction. □

Lemma 3.1.3 *Let G be a finite group. Suppose that G'/G'' and G''/G''' are cyclic. Then $G'' = G'''$.*

Proof. Huppert [2, Satz 2.10, page 420] Assume that $G''' = 1$. Then G'' is cyclic and the group $G/C_G(G'')$, which is isomorphic to a subgroup of $Aut(G'')$, is abelian. So $G' \subseteq C_G(G'')$ and $G'' \subseteq Z(G')$. But G'/G'' is cyclic and thus G' must be abelian. Hence $G'' = 1$ and the result follows. □

Theorem 3.1.4 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that G has a model subgroup. Then C is cyclic of odd order.*

Proof. If G has a model subgroup then so must C by Theorem 2.3.2. Furthermore, we may assume that all the p-Sylow subgroups of C are cyclic, by Theorem 3.1.1 and Theorem 1.7.8. So C'/C'' and C''/C''' are cyclic, and $C'' = C'''$ by Lemma 3.1.3. Since C is soluble by Lemma 3.1.2, we have established that $C'' = 1$. Hence C' is a normal cyclic subgroup of C and since every subgroup of a cyclic group is characteristic, every subgroup of C' is a normal subgroup of C. If H is a model subgroup of C, then H must be contained in C' by Corolla ry 2.3.3. Thus H is a normal subgroup of C and

$$1_H \uparrow^C = \sum_{\chi \in Irr(C/H)} \chi(1)\chi.$$

So we must have $H = C' = 1$ and the result follows. □

3.2 A necessary arithmetic condition

We shall now prove that a Frobenius group with an abelian Frobenius kernel of prime power order has a model subgroup only if it satisfies a specific arithmetic condition.

Theorem 3.2.1 *Let G be a Frobenius group with Frobenius complement C and abelian Frobenius kernel N of order r^n, where r is a prime. Suppose that G has a model subgroup. Then C is cyclic of odd order and*

$$|G : N| = |C| = \frac{r^n - 1}{r^d - 1},$$

where d divides n.

Proof. Since G is a Frobenius group, $|C|$ divides $|N| - 1$ by Lemma 1.5.1. So there exists an x such that $|C|x = r^n - 1$. Suppose that H is a model subgroup of G. Then C is cyclic by Theorem 3.1.4 and

$$|G:H| = \sum_{\chi\in Irr(G)} \chi(1) = |C| + |N| - 1 = |C|\,(1+x)\,,$$

by Theorem 1.6.4 and our assumption that N is abelian. So $x = r^d - 1$ for some $d \leq n$. Finally d must divide n, since x divides $r^n - 1$. □

Theorem 3.2.2 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that G has a model subgroup. Then N has prime power order.*

Proof. Suppose that G is a minimal counter-example. By Theorem 1.7.6, N is nilpotent and can be written as a direct product of its p-Sylow subgroups. So $N = P_1 \times \cdots \times P_j$, for some $j > 1$. Let

$$M = \Phi(P_1) \times \Phi(P_2) \times P_3 \cdots \times P_j.$$

Then G/M has a model subgroup by Theorem 2.3.2 and G/M is a Frobenius group, by Lemma 1.7.4, with Frobenius complement C/M and Frobenius kernel

$$N/M \cong \frac{P_1}{\Phi(P_1)} \times \frac{P_2}{\Phi(P_2)},$$

contradicting the minimality of G. So we may assume that G is a Frobenius group with Frobenius complement C and abelian Frobenius kernel $N = L \times K$, where L and K are elementary abelian of order r^n and p^m respectively, $r \neq p$. Let H be a model subgroup of G. Then $H \subseteq G' \subseteq N$, by Theorem 3.2.1 and Corolla ry 2.3.3. So $H \cap L$ and $H \cap K$ are the r and p Sylow subgroups of H. Thus

$$H = (H \cap L) \times (H \cap K)\,.$$

Now K is a characteristic subgroup of N and thus a normal subgroup of G. So G/K is a Frobenius group with Frobenius complement $C/K \cong C$ and Frobenius kernel $N/K \cong L$. So HK/K is a model subgroup of G/K by Theorem 2.3.2 and

$$|G : N| = \frac{r^n - 1}{r^d - 1} ,$$

where d is some divisor of n, by Theorem 3.2.1. Furthermore,

$$|H \cap L| = |H : H \cap K| = |HK : K| = r^{n-d},$$

by Theorem 3.2.1. We can show similarly that HL/L is a model subgroup of G/L,

$$|G : N| = \frac{p^m - 1}{p^e - 1} ,$$

where e is some divisor of m and

$$|H \cap K| = |H : H \cap L| = |HL : L| = p^{m-e}.$$

We shall derive a contradiction by evaluating the index of H in G in two different ways. From above we have

$$|G : H| = |G : N| \left(r^d p^e\right).$$

But Theorem 3.2.1 states that

$$\begin{aligned} |G : H| &= |G : N| + (r^n p^m - 1) \\ &= |G : N| \left(\left(r^d - 1\right) p^m + p^e\right) \\ &= |G : N| p^e \left(\left(r^d - 1\right) p^{m-e} + 1\right). \end{aligned}$$

Comparing the two values for the index of H in G, we see that m must equal e, which implies that $C = 1$ contradicting our assumption that G was a Frobenius group with Frobenius complement C. □

3.3 Kernels and model subgroups

In this section we shall prove that if a Frobenius group G admits a model subgroup, then its Frobenius kernel is a minimal normal subgroup of G.

Lemma 3.3.1 *Let G be a finite group, let n be an integer greater than zero and θ_n be the class function on G defined by*

$$\theta_n(g) = |\{h \in G \mid h^n = g\}|.$$

Suppose that $\nu_n(\chi)$ is the uniquely determined complex number

$$\theta_n = \sum_{\chi \in Irr(G)} \nu_n(\chi)\chi.$$

Then

$$\nu_n(\chi) = \frac{1}{|G|}\sum_{g \in G} \chi(g^n).$$

for all $\chi \in Irr(G)$.

Proof. Isaacs [1, (4.4) Lemma, page 49-50] By the orthogonality relations we have

$$\nu_n(\chi) = \langle \theta_n, \chi \rangle = \frac{1}{G}\sum_{g \in G} \theta_n(g)\overline{\chi(g)}.$$

Since $\theta_n(g)\overline{\chi(g)} = \sum_{h \in G; h^n = g} \overline{\chi(h^n)}$, we have

$$\nu_n(\chi) = \frac{1}{G}\sum_{h \in G} \overline{\chi(h^n)}.$$

Finally replace by h by h^{-1} to obtain the result. □

Lemma 3.3.2 *Let $N \lhd G$ and let $\chi \in Irr(G)$ with $N \subseteq ker\chi$. Let $\nu_n(\chi)$ be as above and let $\hat{\nu}_n(\chi)$ be the corresponding number in G/N. Then $\nu_n(\chi)$ equals $\hat{\nu}_n(\chi)$.*

Proof. Isaacs [1, (4.7) Lemma, page 51-52] We have

$$\begin{aligned} \hat{\nu}_n(\chi) &= \frac{1}{|G:N|}\sum_{Ng\in G/N}\chi((Ng)^n) = \frac{1}{|G:N|}\frac{1}{|N|}\sum_{g\in G}\chi(Ng^n) \\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g^n) = \nu_n(\chi). \end{aligned}$$

The proof is complete. □

Theorem 3.3.3 *Let $\chi \in Irr(G)$. Then $\nu_2(\chi) = 1\,, 0$ or -1 and $\nu_2(\chi) \neq 0$ if an only if χ is real- valued.*

Proof. Isaacs [1, (4.5) Theorem, pages 50-51] □

Corollary 3.3.4 *Let G have exactly t involutions. Then*

$$1 + t = \sum_{\chi\in Irr(G)} \nu_2(\chi)\chi(1),$$

where $\nu_2(\chi) = 0$ if $\chi \neq \overline{\chi}$ and $\nu_2 = \pm 1$ if $\chi = \overline{\chi}$.

Proof. Isaacs [1, (4.6) Corollary, page 51] Since $\theta_2(1) = 1 + t$, the result follows immediately from Theorem 3.3.3. □

Theorem 3.3.5 *Let G be a non-abelian special 2-group of rank $2n$. Let $\mathcal{M}$ be the set of maximal subgroups of the centre of G and let*

$$\mathcal{M}_E = \{M \in \mathcal{M} \mid G/M \text{ is extraspecial}\}.$$

Suppose that the order of the centre of G is greater than 2^n. Then

$$|\mathcal{M}_E| \equiv 0 \, mod 2.$$

Proof. Suppose that M is a maximal subgroup of the centre of G. Then G/M is a non-abelian 2-group and $\Phi(G/M)$ has order 2 by Lemma 1.4.8. Hence $G/M = (Q/M)Z(G/M)$, where Q/M is extra-special and $Q/M \cap Z(G/M) = \Phi(G/M)$, by Lemma 1.4.8. If $Z(G/M)$ has order 2^{2k_m+1}, then G/M has 2^{2n} linear characters and 2^{2k_m} irreducible characters of degree 2^{n-k_m}. Furthermore, the restriction of every irreducible character of G/M to Q/M is irreducible. So every non-linear character of G/M restricts to μ, the unique non- linear character of Q/M given by Theorem 1.4.5. Suppose that

$$\nu_2(M) = \frac{1}{|G/M|} \sum_{gM \in G/M} \mu((gM)^2).$$

Then for any non-linear irreducible character χ of G/M

$$\begin{aligned}\nu_2(\chi) &= \frac{1}{|G/M|} \sum_{gM \in G/M} \chi((gM)^2) \\ &= \frac{1}{|G/M|} \sum_{gM \in G/M} \mu((gM)^2) = \nu_2(M).\end{aligned}$$

By Lemma 1.4.8 we have

$$Irr(G) - Irr(G/Z(G)) = \dot{\bigcup_{M \in \mathcal{M}}} \{\chi \in Irr(G/M) \mid \chi(1) \neq 1\}.$$

If $\lambda \in Irr(G/Z(G))$, then

$$\begin{aligned}\nu_2(\lambda) &= \frac{1}{|G/Z(G)|} \sum_{gZ(G) \in G/Z(G)} \lambda((gZ(G))^2) \\ &= \frac{1}{|G/Z(G)|} \sum_{gZ(G) \in G/Z(G)} \lambda(1) = 1\end{aligned}$$

Thus if G has exactly t involutions, then

$$1 + t = 2^{2n} + 2^n \sum_{M \in \mathcal{M}} \nu_2(M) 2^{k_m},$$

by Corolla ry 3.3.4 and Lemma 3.3.2. Now suppose that the order of the centre of G is greater than 2^n. Then $2^{n+1}|1+t$, because the set $\{g \in G : g^2 = 1\}$ is a union of cosets of the centre of G. Therefore

$$\sum_{M \in \mathcal{M}_E} \nu_2(M) \equiv 0 \ mod\ 2,$$

where $\mathcal{M}_E = \{M \in \mathcal{M} : |Z(G/M)| = 2\}$. Clearly $M \in \mathcal{M}_E$ if and only if G/M is extraspecial. Since the non-linear irreducible character of an extraspecial 2-group is real valued, $\nu_2(M) = \pm 1$ for $M \in \mathcal{M}_E$ by Theorem 3.3.3. Thus

$$|\mathcal{M}_E| \equiv 0 \operatorname{mod} 2$$

and the proof is complete. □

Theorem 3.3.6 *Let G be a Frobenius group with Frobenius complement C and abelian Frobenius kernel N of order r^n, where r is a prime. Suppose that G has a model subgroup. Then N is a minimal normal subgroup of G. In particular, N is elementary abelian.*

Proof. By Theorem 3.2.1 $|G : N| = \frac{r^n-1}{r^d-1}$, where d divides n. Now suppose that $1 \neq M \lhd G$ and $M \subset N$. Then M has order r^m for some $0 < m < n$ and G/M is a Frobenius group with Frobenius complement C/M and abelian Frobenius kernel N/M. So by Theorem 3.2.1 $|G : N| = \frac{r^{n-m}-1}{r^e-1}$ where e divides $n-m$ and

$$\frac{r^n-1}{r^d-1} = \frac{r^{n-m}-1}{r^e-1}.$$

If this identity holds, then $e < d < n-m < n$. Rearranging the equation we obtain

$$r^d\left(r^{n-m} - r^{n-m-d} - 1\right) = r^e\left(r^n - r^{n-e} - 1\right)$$

and d must equal e contradicting the inequality above. □

Theorem 3.3.7 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N of prime power order. Suppose that G has a model subgroup. Then N is abelian.*

Proof. Suppose that G is a minimal counter-example to the claim and S is a minimal normal subgroup of G contained in N. Then by Lemma 1.7.4 the factor group G/S is a Frobenius group with Frobenius complement C/S and Frobenius kernel N/S. In addition, G/S has a model subgroup by Theorem 2.3.2. Thus N/S must be abelian, because G is a minimal counter-example to the claim. So N/S is a minimal normal subgroup of G/S by Theorem 3.3.6. Hence

$$S = Z(N) = N' = \Phi(N)$$

and N is a non-abelian special r-group. Suppose that $\mathcal{S}$ is the set of maximal subgroups of S. Then

$$Irr(N) - Irr(N/S) = \dot{\bigcup_{T \in \mathcal{S}}} \{\chi \in Irr(N/T) \mid \chi(1) \neq 1\},$$

by Lemma 1.4.8. Furthermore, if $T \in \mathcal{S}$, then N/T is a non-abelian r-group and $\Phi(N/T)$ has order r. Now let

$$\{T_1, \ldots, T_j\}$$

be a complete set of orbit representatives of $\mathcal{S}$ viewed as a C-set and let

$$\mathcal{S}_1, \ldots, \mathcal{S}_j$$

be the C-orbit containing T_i. Then by Lemma 1.4.7 there exists a $k_i \geq 0$ such that for all $U \in \mathcal{S}_i$, the factor group N/U has r^n linear characters and

$$(r-1)r^{k_i} \text{ irreducible characters of degree } r^{\frac{1}{2}(n-k_i)},$$

where r^n is the order of N/S. Let $C_i = \{c \in C \,|\, T_i^c = T_i\}$. Then $c \in C_{T_i}$ if and only if c acts fixed- point freely on S/T_i by Lemma 1.7.4. Thus

$$|\mathcal{S}_i| = \frac{|C|}{\ell_i},$$

for some ℓ_i dividng $r-1$ by Lemma 1.7.1 and Lemma 1.5.1. Let $Irr(N/\mathcal{S}_i)$ be the set of non- linear irreducible characters of N, which contain an element of $\mathcal{S}_i$ in their kernel. Then

$$Irr(N) - Irr(N/S) = Irr(N/\mathcal{S}_1)\,\dot{\cup}\cdots\dot{\cup}\,Irr(N/\mathcal{S}_j)$$

by Lemma 1.4.8. Furthermore,

$$|Irr(N/\mathcal{S}_i)| = |\mathcal{S}_i|(r-1)r^{k_i} = |C|\frac{r-1}{\ell_i}r^{k_i},$$

since the kernel of every non-linear character of N contains one and only one element of $\mathcal{M}$. Because G is a Frobenius group, it clearly permutes these characters in orbits of length $|C|$.

Suppose that H is a model subgroup of G. Then HS/S is a model subgroup of G/S, a Frobenius group with Frobenius complement C/S and abelian Frobenius kernel N/S. Therefore Theorem 3.2.1 states that $C \cong C/S$ is cyclic of odd order and

$$|G:N| = |C| = \frac{r^n-1}{r^d-1},$$

for some d dividing n. Hence the index of HS/S in N/S is r^d by Theorem 1.6.4. Since C is cyclic, H is contained in N by Corolla ry 2.3.3. Thus $1_H \uparrow N$ is multiplicity-free and contains exactly one irreducible character from each orbit of $Irr(N)$ viewed as a C-set by Theorem 1.6.4.

Let $T \in \mathcal{S}_i$. Suppose that $\chi \in Irr(N/T)$ and $\tilde{\chi}$ is the corresponding character in N/T. Then

$$\langle 1_H \uparrow N , \chi \rangle = \langle 1_{HT/T} \uparrow N/T , \tilde{\chi} \rangle,$$

by Lemma 2.3.1. In particular, $1_{HT/T} \uparrow N/T$ is multiplicity-free. If $H \cap S \nsubseteq T$, then $S/T \subseteq HT/T$. So

$$ker(1_{HT/T} \uparrow N/T) = \bigcap_{nT \in N/T} (HT/T)^{nT} \supseteq S/T$$

and no non-linear character of $Irr(N/T)$ can be a constituent of $1_H \uparrow N$. If $H \cap S \subseteq T$, then HT/T has index r^{d+1} in N/T. So $1_{HT/T} \uparrow N/T$ has degree r^{d+1}. Since HS/S has index r^d in N/S, the sum of the degrees of the non-linear irreducible constituents of $1_{HT/T} \uparrow N/T$ must equal r^d. Therefore

$$r^{d-\frac{1}{2}(n-k_i)}$$

non-linear characters of $Irr(N/T)$ are constituents of $1_H \uparrow N$. Thus

$$|\{T \in \mathcal{S}_i : H \cap S \subseteq T\}| = \frac{|Irr(N/\mathcal{S}_i)|}{|C|} \Big/ r^{d-\frac{1}{2}(n-k_i)} = \frac{r-1}{\ell} r^{\frac{1}{2}(n+k_i)-d}.$$

Suppose that $H \cap S$ has index r^x in S. Then $H \cap S$ is contained in

$$\frac{r^x - 1}{r - 1}$$

elements of $\mathcal{S}$ and we have

$$\frac{r^x - 1}{r - 1} = \frac{r-1}{\ell_1} r^{\frac{1}{2}(n+k_1)-d} + \cdots + \frac{r-1}{\ell_j} r^{\frac{1}{2}(n+k_j)-d}.$$

Since the left-hand side is co-prime to r we must have

$$\frac{1}{2}(n+k_i) - d = 0$$

for some i. Since $2d \leq n$, this forces $n = 2d$ and $k_i = 0$. So $|C| = r^d + 1$ and $r = 2$, because C has odd order. Rewriting the equation above we obtain

$$2^x - 1 = 2^{\frac{1}{2}k_1} + \cdots + 2^{\frac{1}{2}k_j}.$$

Hence there must be an odd number of orbits of the set of maximal subgroups of S viewed as a C-set with $k_i = 0$. Since every orbit has length $|C| = 2^d + 1$, this implies that N has an odd number of maximal subgroups of S with extra-special quotients. But C acts fixed-point freely on S by Lemma 1.7.4, so $|S| > 2^d$, by Lemma 1.7.1 and Lemma 1.5.1. The result follows by Theorem 3.3.5.

□

3.4 Finite fields and model subgroups

Definition 3.4.1 *For $\alpha \in F = \mathbb{F}_{r^n}$, the absolute trace $Tr_F(\alpha)$ is defined by*

$$Tr_F(\alpha) = \alpha + \alpha^r + \cdots + \alpha^{r^{n-1}}.$$

Theorem 3.4.2 *Let $R = \mathbb{F}_r$ and $F = \mathbb{F}_{r^n}$. Then the trace function Tr_F is a linear transformation from F onto R, where both F and R are viewed as vector spaces over R.*

Proof. Lidl and Niederreiter [3, 2.23 Theorem, page 55] For $\alpha, \beta \in F$ we have

$$\begin{aligned} Tr_F(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^r + \cdots + (\alpha+\beta)^{r^{n-1}} \\ &= \alpha + \beta + \alpha^r + \beta^r + \cdots + \alpha^{r^{n-1}} + \beta^{r^{n-1}} \\ &= Tr_F(\alpha) + Tr_F(\beta). \end{aligned}$$

For $c \in R$ and $\alpha \in F$ we have

$$\begin{aligned} Tr_F(c\alpha) &= (c\alpha) + c^r\alpha^r + \cdots + c^{r^{n-1}}\alpha^{r^{n-1}} \\ &= c\alpha + c\alpha^r + \cdots + c\alpha^{r^{n-1}} \\ &= cTr_F(\alpha). \end{aligned}$$

Furthermore, $Tr_F\alpha$ is an element of R for all $\alpha \in F$, because it is left fixed by every field automorphism of F. We have proved that Tr_F is a linear transformation from F into R, where both F and R are viewed as vector spaces over R. To prove that this mapping is onto, it suffices to show that the existence of an $\alpha \in F$ with $Tr_F(\alpha) \neq 0$. Now $Tr_F(\alpha) = 0$ if and only if α is a root of the polynomial $x^{r^{n-1}} + \cdots + x^r + x$ in F. But since this polynomial can have at most r^{n-1} roots in F and F has r^n elements, we are done. □

Definition 3.4.3 *Let $b \in \mathbb{F}_{r^n}$ and χ_b be the function defined by*

$$\chi_b(c) = e^{2\pi i Tr_F(bc)/r}$$

for all $c \in \mathbb{F}_{r^n}$.

Theorem 3.4.4 *$Irr(F_{r^n}^+) = \{\chi_b \mid b \in \mathbb{F}_{r^n}\}$.*

Proof. Lidl and Niederreiter [3, 5.7 Theorem, page 190] Let $b, c_1, c_2 \in \mathbb{F}_{r^n}$ and χ_b be the function defined in Definition 3.4.3. Then

$$\chi_b(c_1 + c_2) = \chi_b(c_1)\chi_b(c_2),$$

because $Tr_F(b(c_1 + c_2)) = Tr_F(bc_1) + Tr_F(bc_2)$ by Theorem 3.4.2. Thus χ_b is a linear character of $\mathbb{F}_{r^n}^+$ for all $b \in \mathbb{F}_{r^n}$. Now Tr_F maps $\mathbb{F}_{r^n}$ onto $\mathbb{F}_r$ by

Theorem 3.4.2. So the character χ_1 is non- trivial. Therefore, if $a, b \in \mathbb{F}_{r^n}$ with $a \neq b$, then

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1$$

for suitable $c \in \mathbb{F}_{r^n}$, and so χ_a and χ_b are distinct linear characters of $\mathbb{F}^+_{r^n}$. Since $Irr(\mathbb{F}^+_{r^n})$ has cardinality r^n, the proof is complete. □

Theorem 3.4.5 *The map $\chi_b \to b$ is a group isomorphism from $Irr(\mathbb{F}^+_{r^n})$ to $\mathbb{F}^+_{r^n}$.*

Proof. Theorem 3.4.4 ensures that the map $\chi_b \to b$ is a bijection from $Irr(\mathbb{F}^+_{r^n})$ onto $\mathbb{F}^+_{r^n}$. So we need only show that the map $\chi_b \to b$ is a group homomorphism. Let $a, b \in \mathbb{F}_{r^n}$. Then

$$\chi_a\chi_b(c) = \chi_a(c)\chi_b(c) = \chi_1(ac)\chi_1(bc) = \chi_1((a+b)c) = \chi_{a+b}(c),$$

and the result follows. □

Theorem 3.4.6 *Let r be a prime, $n \in \mathbb{N}$ and m be a divisor of $r^n - 1$. Let $C = \langle \epsilon \rangle$, where ϵ is a primitive mth root of unity of $\mathbb{F}_{r^n}$, and $N = \mathbb{F}^+_{r^n}$. Suppose that*

$$G = [N]C,$$

the external semi-direct product of N and C via σ, where σ is the homomorphism from C to $Aut(N)$ defined by

$$x^{\sigma(\epsilon^i)} = x\epsilon^i \quad \textit{(field multiplication)}$$

for all $x \in N$ and $0 \leq i \leq m-1$. Then G is a Frobenius group with Frobenius complement C and Frobenius kernel N. In addition, if $0 \neq a \in \mathbb{F}_{r^n}$ and χ_a

is the corresponding element of $Irr(N)$, then the distinct characters

$$\chi_a = \chi_{a\epsilon^0}, \ldots, \chi_{a\epsilon^{m-1}}$$

are the conjugates of χ_a in S. Thus for $a, b \in \mathbb{F}_{r^n}$, χ_a and χ_b are conjugate in S if and only if $a^m = b^m$.

Proof. Since $\sigma(C)$ is a fixed-point free subgroup of $Aut(N)$, G is a Frobenius group with Frobenius complement C and Frobenius kernel N by Lemma 1.7.1. Suppose that $a \neq 0$ and $\chi_a \in Irr(N)$. Then

$$\begin{aligned} \chi_a^{\epsilon^i}(x) &= \chi_a(x^{\epsilon^{-i}}) \\ &= \chi_a(x\sigma(\epsilon^{-i})) \\ &= \chi_a(x\epsilon^{-i}) \\ &= \chi_{a\epsilon^{-i}}(x) \end{aligned}$$

for all $x \in N$ and $i \in \{0, \ldots, m-1\}$. Since $a \neq 0$, we have $\chi_{a\epsilon^{-i}} \neq \chi_{a\epsilon^{-j}}$ if $i \neq j$. So the conjugates of χ_a in S are the distinct characters

$$\chi_a = \chi_{a\epsilon^0}, \ldots, \chi_{a\epsilon^{m-1}}$$

and

$$(a\epsilon^i)^m = a^m(\epsilon^i)^m = a^m$$

for all $i \in \{0, \ldots, m-1\}$. Since $b^m = a^m$ if and only if b is a root of $x^m - a^m$, which has at most m roots in $\mathbb{F}_{r^n}$, the result follows for $a \neq 0$. If $a = 0$ then χ_a is the trivial character of N, which is invariant in S. Since $b^m = 0$ if and only if $b = 0$, the proof is complete. □

Definition 3.4.7 *Suppose that $\alpha \in F = \mathbb{F}_{r^n}$ and $K = \mathbb{F}_{r^d}$, where d is some divisor of n. Then the norm $N_{F/K}(\alpha)$ of α over K is defined by*

$$N_{F/K}(\alpha) = \alpha^{r^d}\alpha^{r^{2d}}\cdots\alpha^{r^{(n/d)d}} = \alpha^{(r^n-1)/(r^d-1)}.$$

Theorem 3.4.8 *Let $F = \mathbb{F}_{r^n}$ and $K = \mathbb{F}_{r^d}$, where d is some divisor of n. Then the norm function $N_{F/K}$ satisfies the following properties :*

(a) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$ *for all* $\alpha, \beta \in F$;

(b) $N_{F/K}$ *maps* F *onto* K *and* F^* *onto* K^*;

(c) $N_{F/K}(a) = a^{n/d}$ *for all* $a \in K$;

(d) $N_{F/K}(\alpha^{r^d}) = N_{F/K}(\alpha)$ *for all* $\alpha \in F$.

Proof. Lidl and Niederreiter [3, 2.28 Theorem, page 57] (a) Follows immediately from the definition of the norm.

(b) An element of F is contained in K if and only if it is left fixed by all field automorphisms of F of the form

$$\alpha \to \alpha^{r^{di}} \quad i \in \{1, \dots, n/d\}.$$

Hence $N_{F/K}(\alpha) \in K$ for all $\alpha \in F$ and $N_{F/K}$ maps F into K. Furthermore, since $N_{F/K}(\alpha) = 0$ if and only if $\alpha = 0$, $N_{F/K}$ is a group homomorphism from F^* to K^*. Since the elements of the kernel of $N_{F/K}$ are exactly the roots of the polynomial $x^{(r^n-1)/(r^d-1)} - 1$ in F, the order of the kernel is less than or equal to $(r^n - 1)/(r^d - 1)$. So the image of $N_{F/K}$ has order greater than or equal to $r^d - 1$. Therefore, $N_{F/K}$ maps F^* onto K^* and F onto K.

(c) If $a \in K$, then $a^{r^{di}} = a$ for $i \in \{1, \ldots, n/d\}$ and $N_{F/K}(a) = a^{n/d}$ as claimed.

(d) $N_{F/K}(\alpha^{r^d}) = N_{F/K}(\alpha)^{r^d}$ by (a) and $N_{F/K}(\alpha)^{r^d} = N_{F/K}(\alpha)$, because $N_{F/K}(\alpha) \in K$. □

Theorem 3.4.9 *Let r be a prime, $n \in \mathbb{N}$, d be a divisor of n and $m = (r^n - 1)/(r^d - 1)$. Let $F = \mathbb{F}_{r^n}$ and $K = \mathbb{F}_{r^d}$. Let $C = \langle \epsilon \rangle$, where ϵ is a primitive mth root of unity of F, and $N = F^+$. Let*

$$G = [N]C,$$

the external semi-direct product of N and C via σ, where σ is the homomorphism from C to $Aut(N)$ defined by

$$x^{\sigma(\epsilon^i)} = x\epsilon^i \quad \textit{(field multiplication)}$$

for all $x \in F^+_{r^n}$ and $0 \leq i \leq m-1$. Then G has a model subgroup if and only if F has an additive abelian subgroup H_F of order r^d satisfying $N_{F/K}(H_F) = K$.

Proof. Suppose that G has a model subgroup H. Then $H \subseteq G' \subseteq N$ by Corolla ry 2.3.3. Since N is abelian,

$$1_H^N = \sum_{\chi \in Irr(N/H)} \chi$$

and $Irr(N/H)$ is a subgroup of the group $Irr(N)$. But G is a Frobenius group with Frobenius complement C and Frobenius kernel N by Theorem 3.4.6 and H is a model subgroup of G. So no two elements of $Irr(N/H)$ can be conjugate in G and $Irr(N/H)$ must have order r^d by Theorem 1.6.4. Furthermore, Theorem 3.4.4 states that

$$Irr(N) = \{\chi_b \mid b \in \mathbb{F}_{r^n}\},$$

so there exist elements $a_0 = 0, a_1, \ldots, a_{r^d-1}$ of F such that the subgroup

$$Irr(N/H) = \{\chi_{a_0}, \ldots, \chi_{a_{r^d-1}}\}.$$

Let H_F denote $\{a_0 = 0, a_1, \ldots, a_{r^d-1}\}$. Then H_F is a subgroup of F^+ by Theorem 3.4.5 and $a_i^m \neq a_j^m$ for $i \neq j$ by Theorem 3.4.6. But $N_{K/F}(a) = a^m$ for all $a \in F^{r^n}$ and $N_{K/F}$ maps F onto K by Theorem 3.4.8. So $N_{K/F}(H_F) = K$, because K has order r^d.

Now suppose that F has an additive abelian subgroup

$$H_F = \{a_0 = 0, a_1, \ldots, a_{r^d-1}\}$$

satisfying $N_{F/K}(H) = K$, then there exists a subgroup H of N such that

$$Irr(N/H) = \{\chi_{a_0}, \ldots, \chi_{a_{r^d-1}}\}$$

by Theorem 3.4.5. Since K has order r^d and $N_{K/F}(a) = a^m$ for all $a \in F^{r^n}$, no two elements of $Irr(N/H)$ can be conjugate in G by Theorem 3.4.6. But G is a Frobenius group with Frobenius complement C and Frobenius kernel N by Theorem 3.4.6. So H is a model subgroup by Theorem 1.6.4. □

Lemma 3.4.10 *Suppose that a and n are natural numbers and $d < n$ is a divisor of n . Then $(a^n - 1)/(a^d - 1)$ divides $a^n - 1$, but does not divide $a^i - 1$ whenever $0 < i < n$.*

Proof. By Theorem 1.2.5 except in the cases $n = 2$, $a = 2^b - 1$ and $n = 6$, $a = 2$, there is a prime q such that q divides $a^n - 1$ but q does not divide $a^i - 1$ whenever $0 < i < n$. If such a q exists, then

$$q \mid a^n - 1 = (a^d - 1)\left(\frac{a^n - 1}{a^d - 1}\right),$$

but q does not divide $a^d - 1$. Thus

$$q \mid \frac{a^n - 1}{a^d - 1}$$

and the result follows. If $n = 2$ and $a = 2^b - 1$, we need only consider the case when $d = 1$. Since

$$\frac{a^2 - 1}{a - 1} = a + 1 > a - 1,$$

the result holds. Finally, if $n = 6$ and $a = 2$, we need to consider the cases $d = 1, 2, 3$.

$$\frac{2^6 - 1}{2^d - 1} = 63\,,\, 21\,,\, 9\ (for)\ d = 1, 2, 3$$

and it is routine to check that these numbers satisfy the hypothesis. □

Theorem 3.4.11 *Let G be a Frobenius group with an elementary abelian Frobenius kernel of order r^n and a cyclic Frobenius complement of order $(r^n - 1)/(r^d - 1)$, for some d dividing n. Then G has a model subgroup if and only if the finite field $F = \mathbb{F}_{r^n}$ has an additive abelian subgroup H_F of order r^d satisfying $N_{F/K}(H_F) = K$, where $K = \mathbb{F}_{r^d}$.*

Proof. Suppose that $C = \langle c \rangle$ is the cyclic Frobenius complement of G of order $m = (r^n - 1)/(r^d - 1)$ and N is the elementary abelian Frobenius kernel of G of order r^n. Then N can be viewed as an $\mathbb{F}_r[C]$-module via the C-action

$$xc^i = x^{c^i},$$

for all $x \in N$ and $i \in \{1, \ldots, m\}$. Since each element of C acts fixed-point freely on N via conjugation by Lemma 1.7.1, the C-action is faithful and we can apply Theorem 1.1.1 to an irreducible submodule M of N. Thus there exists a primitive mth root of unity ϵ of $\mathbb{F}_{r^n}$, by Lemma 3.4.10, such that M is isomorphic to $\mathbb{F}_{r^n}$ viewed as an $\mathbb{F}_r[C]$-module via the C-action

$$xc^i = x\epsilon^i \quad \text{(field multiplication)}$$

for all $x \in \mathbb{F}_{r^n}$ and $0 \leq i \leq m-1$. Since M is isomorphic to $\mathbb{F}_{r^n}$ viewed as an $\mathbb{F}_r[C]$-module, M must equal N and thus G is isomorphic to

$$S = [\mathbb{F}_{r^n}^+]\langle\epsilon\rangle,$$

the external semi-direct product of $\mathbb{F}_{r^n}^+$ and $\langle\epsilon\rangle$ via σ, where σ is the homomorphism from $\langle\epsilon\rangle$ to $Aut(\mathbb{F}_{r^n}^+)$ defined by

$$x^{\sigma(\epsilon^i)} = x\epsilon^i \quad \text{(field multiplication)}$$

for all $x \in \mathbb{F}_{r^n}^+$ and $0 \leq i \leq m-1$. So G has a model subgroup if and only if S has a model subgroup. The result follows by Theorem 3.4.9. □

3.5 Conclusion

Theorem 3.5.1 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Then G has a model subgroup if and only if the following conditions are satisfied.*

(a) *N is elementary abelian of order r^n.*

(b) *C is cyclic of order $(r^n - 1)/(r^d - 1)$, for some d dividing n.*

(c) *The finite field $F = \mathbb{F}_{r^n}$ has an additive abelian subgroup H_F of order r^d satisfying $N_{F/K}(H_F) = K$, where $K = \mathbb{F}_{r^d}$.*

Proof. Suppose that G has a model subgroup. Then the Frobenius kernel N of G, is elementary abelian of prime power order, by Theorem 3.2.2, Theorem 3.3.6 and Theorem 3.3.7. Furthermore, if N has order r^n, then C is cyclic of order $(r^n - 1)/(r^d - 1)$, for some d dividing n, by Theorem 3.2.1. The result follows by Theorem 3.4.11. □

Theorem 3.5.2 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that N is elementary abelian of order r^n and C is cyclic of order $(r^n - 1)/(r^d - 1)$, for some d dividing n. Then the following statements hold.*

(a) *If $(n/d, r^d - 1) = 1$, then G has a model subgroup.*

(b) *If $(n/d, r - 1) \neq 1$, then G does not have a model subgroup.*

Proof. (a) Let $F = \mathbb{F}_{r^n}$ and $K = \mathbb{F}_{r^d}$. Then the map $a \to N_{F/K}(a)$ is a homomorphism from the cyclic group $K^\times$ of order $r^d - 1$ into itself, by Theorem 3.4.8. Furthermore,

$$a \to N_{F/K}(a) = a^{n/d},$$

for all $a \in K^\times$. So if $(n/d, r^d - 1) = 1$, the map $a \to N_{F/K}(a)$ is an automorphism of $K^\times$. Hence the additive abelian subgroup K of order r^d of F has the property that

$$N_{F/K}(K) = K,$$

since $N_{F/K}(0) = 0$. The result follows by Theorem 3.4.11.

(b) Let $F = \mathbb{F}_{r^n}$ and $K = \mathbb{F}_{r^d}$. Let P be the prime subfield of F. Since the map $a \to N_{F/K}(a)$ is a homomorphism from the cyclic group $F^\times$ into itself by Theorem 3.4.8 and $P^\times$ is a characteristic subgroup of $F^\times$, the map

$$p \to N_{F/K}(p)$$

is a homomorphism from the cyclic group P of order $r-1$ into itself. But $P^\times$ is also a subgroup of $K^\times$. Hence

$$N_{F/K}(p) = p^{n/d}$$

for all $p \in P^\times$ by Theorem 3.4.8. So if $(n/d, r-1) \neq 1$, there exists a non-identity element q of $P^\times$ satisfying $N_{F/K}(q) = 1$. Suppose that H_F is an additive abelian subgroup of F of order r^d and $0 \neq h \in H_F$. Then $h \neq qh \in H_F$ and

$$N_{K/F}(qh) = N_{K/F}(q)N_{K/F}(h) = N_{K/F}(h).$$

So $N_{K/F}(H_F) < K$. The result follows by Theorem 3.4.11. □

Corollary 3.5.3 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that N is elementary abelian of order r^n and C is cyclic of order $(r^n-1)/(r-1)$, then G has a model subgroup if and only if $(n, r-1) = 1$.*

Corollary 3.5.4 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that N is elementary abelian of order $r^{2^a d}$ for any $a, d \in \mathbb{N}$ and C is cyclic of order $(r^{2^a d}-1)/(r^d-1)$, then G has a model subgroup if and only if $r = 2$.*

Lemma 3.5.5 *Let r be a prime, let n be a natural number and let d be a divisor of n. Then $x \mid (n/d, r^d-1)$ if and only if $x \mid ((r^n-1)/(r^d-1), r^d-1)$.*

Proof. Suppose that $x \mid (n/d, r^d - 1)$. Then $ax = r^d - 1$ and $bx = n/d$ for some $a, b \in N$. Thus

$$\begin{aligned} ax\frac{r^n - 1}{r^d - 1} &= \left((r^d - 1) + 1\right)^{n/d} - 1 \\ &= (ax + 1)^{bx} - 1 \\ &= \sum_{k=1}^{bx} \binom{bx}{k} (ax)^k. \end{aligned}$$

So $x \mid (r^n - 1)/(r^d - 1), r^d - 1)$, since $\binom{bx}{1} = bx$.

Now suppose that $x \mid ((r^n - 1)/(r^d - 1), r^d - 1)$. Then $ax = r^d - 1$ and $cx = (r^n - 1)/(r - 1)$ for some $a, c \in N$. Thus

$$\begin{aligned} acx^2 &= \left((r^d - 1) + 1\right)^{n/d} - 1 \\ &= (ax + 1)^{n/d} - 1 \\ &= \sum_{k=1}^{n/d} \binom{n/d}{k} (ax)^k. \end{aligned}$$

So $x \mid (n/d, r^d - 1)$, since $\binom{n/d}{1} = n/d$. The proof is complete. □

Corollary 3.5.6 *Let G be a Frobenius group with Frobenius complement C and Frobenius kernel N. Suppose that N is elementary abelian of order r^n and C is cyclic of order $(r^n - 1)/(r^d - 1)$, for some d dividing n. Then the following statements hold.*

(a) *If $((r^n - 1)/(r^d - 1), r^d - 1) = 1$, then G has a model subgroup.*

(b) *If $((r^n - 1)/(r^d - 1), r - 1) \neq 1$, then G does not have a model subgroup.*

Chapter 4

$\mathcal{X}$-groups

In this chapter we will begin by introducing a new class of finite soluble groups and determine when a group contained in the class admits a model subgroup. We shall then go on to classify those finite soluble groups not contained in the class but whose other epimorphic images are.

4.1 Definition

Let G be a finite soluble group. Suppose that G is abelian or G has subgroups $G_1, \ldots, G_m$ and A satisfying the following statements :

(X.1) $G = G_1 \ldots G_m A$;

(X.2) $[G_i, G_j] = 1$ for $i \neq j$;

(X.3) $[G_i, A] = 1$ for $1 \leq i \leq m$;

(X.4) G_i is not nilpotent for $1 \leq i \leq m$;

(X.5) G'_i is a minimal normal subgroup of G_i for $1 \leq i \leq m$;

(X.6) A is abelian.

Then we call G a $\mathcal{X}$-group.

We begin our analysis by establishing some elementary facts about $\mathcal{X}$-groups.

Lemma 4.1.1 *Let G be a finite soluble group. Suppose that G has subgroups* $G_1, \ldots, G_m$ *and A satisfying the statements* (X.1) - (X.6) above. Then

(a) G is a central product of the subgroups of $G_1, \ldots, G_m$ and A;

(b) $Z(G) = Z(G_1) \ldots Z(G_m)A$;

(c) $G'_i \cap Z(G_i) = 1$ for $1 \leq i \leq m$;

(d) $G' = G'_1 \times \cdots \times G'_m$ is abelian;

(e) $G' \cap Z(G) = 1$;

(f) $G' \cap \Phi(G) = 1$;

Proof. (a) and (b) follow immediately from (X.1) , (X.2) , (X.3) and (X.6)

(c) G'_i is a minimal normal subgroup of G_i for all i, by (X.5). So $G'_i \cap Z(G_i)$ is either equal to G'_i or 1. Suppose that $G'_i \cap Z(G_i) = G'_i$. Then $Z(G_i)$ contains G'_i contradicting (X.4), which states that G_i is not nilpotent. Hence G'_i and $Z(G_i)$ intersect trivially.

(d) follows from (a) , (X.6) and (c).

(e) For $1 \leq i \leq m$, let

$$\hat{G}'_i = G'_1 \times \cdots \times G'_{i-1} \times G_{i+1} \times \cdots \times G'_m.$$

Then $G'/\hat{G}'_i$ is a minimal normal subgroup of $G/\hat{G}'_i$ for all i and

$$\bigcap_{i=1}^{m} \hat{G}'_i = 1.$$

Suppose that $Z(G) \cap G' \neq 1$. Then there exists a j such that $Z(G) \cap G'$ is not contained in $\hat{G}'_j$. So

$$\left(\frac{G}{\hat{G}'_j}\right)' = \frac{G'}{\hat{G}'_j} \subseteq \frac{Z(G)\hat{G}'_j}{\hat{G}'_j} \subseteq Z(G/\hat{G}'_j)$$

and $G/\hat{G}'_j$ is nilpotent. Furthermore,

$$G_j \cong \frac{G_j}{G_j \cap \hat{G}'_j} \cong \frac{G_j\hat{G}'_j}{\hat{G}'_j}$$

is nilpotent contradicting (X.4). The proof is complete.

(f) Can be proved in the same fashion as (e), remembering that a finite group G is nilpotent if and only if $G' \subseteq \Phi(G)$. □

Lemma 4.1.2 *Let G be a finite soluble group. Suppose that G is not nilpotent and G' is minimal. Then G' is complemented in G. Furthermore, if C is a complement of G' in G then $Z(G) = C_C(G')$ and $G/Z(G)$ is a Frobenius group with Frobenius complement $C/Z(G)$ and elementary abelian Frobenius kernel $G'Z(G)/Z(G)$.*

Proof. By the minimality of G', we have $\Phi(G) \cap G' = 1$ or G'. If $\Phi(G) \cap G' = G'$, then $G' \subseteq \Phi(G)$ contradicting our assumption that G is not nilpotent. So the elementary abelian normal subgroup G' is complemented in G, by C say, and

$$G = G'C,$$

where $G' \cap C = 1$. Since C is abelian, $M = C_C(G')$ is a subgroup of $Z(G)$ and is consequently normal. If $C_C(G') = C$, then $G' \subseteq Z(G)$ contradicting our assumption that G is not nilpotent. So $M \neq C$. Clearly

$$G/M = (G'M/M)(C/M)$$

and $G'M/M \cap C/M = 1$.

Now suppose $1 \neq g'M \in C_{G'M/M}(cM)$ for some $cM \in C/M$. Then

$$[c, g'] \in G' \cap M = 1$$

and $g' \in C_{G'}(c) \triangleleft G$. By the minimality of G', we have $C_{G'}(c) = G'$ and $c \in C_G(G') \cap C = M$. Hence $C_{G'M/M}(cM) = 1$ for all $1 \neq cM \in C/M$. Suppose that

$$c_1 \in C/M \cap (C/M)^g$$

for some $g \in G/M - C/M$. Then $g = ch$ with $c \in C/M$ and $1 \neq h \in G'M/M$. So $(C/M)^g = (C/M)^h$ and

$$c_1 = c_2^h \in (C/M) \cap (C/M)^h$$

with $c_2 \in C/M$. Since $G'M/M \triangleleft G/M$,

$$c_1 c_2^{-1} = [h, c_2^{-1}] \in C/M \cap G'M/M = 1$$

and $c_1 = c_2$. So

$$h \in C_{G'M/M}(c_1)$$

and c_1 must be the identity. Thus G/M is a Frobenius group at C/M with elementary abelian Frobenius kernel $G'M/M$. Hence $Z(G/M) = 1$ and consequently $M = Z(G)$. The proof is complete. □

Lemma 4.1.3 *Let G be a non-abelian $\mathcal{X}$-group. Let $\mathcal{M}$ denote the set of all minimal normal subgroups of G contained in G'. Then*

$$G' = \bigtimes_{M \in \mathcal{M}} M$$

and G' is complemented in G. Let D be a complement of G' in G. For $M \in \mathcal{M}$, let

$$D_M = D/C_D(M)$$

and let $[M]D_M$ denote the external semi-direct product of M and D_M via σ_M, where σ_M is the homomorphism from D_M to $Aut(M)$ defined by

$$m^{\sigma_M(dC_D(M))} = m^d$$

for all $m \in M$ and $d \in D$. Then

$$G/Z(G) \cong \bigtimes_{M \in \mathcal{M}} [M]D_M,$$

and $G' \cap Z(G) = 1$.

Proof. Since G is a non-abelian $\mathcal{X}$-group, there exist subgroups $G_1, \ldots, G_m$ and A satisfying the statements (X.1) - (X.6) above and

$$G' = G'_1 \times \cdots \times G'_m,$$

by Lemma 4.1.1(d). In addition, the characteristic subgroup G'_i is complemented in G_i, by C_i say, and

$$Z(G_i) = C_{C_i}(G'_i) < C_i$$

for $1 \leq i \leq m$, by Lemma 4.1.2. So the abelian subgroup G' is complemented in G by $B = C_1 \dots C_m A$ and

$$C_B(G'_i) = C_1 \dots C_{i-1} C_{C_i}(G'_i) C_{i+1} \dots C_m A$$

for $1 \leq i \leq m$. Furthermore,

$$\bigcap_{i=1}^{m} C_B(G'_i) = C_{C_1}(G'_1) \dots C_{C_m}(G'_m) A = Z(G_1) \dots Z(G_M) A = Z(G)$$

by Lemma 4.1.1(b) and $G' \cap Z(G) = 1$ by Lemma 4.1.1(e).

Let $\pi = \{p_1, \dots, p_t\}$ be the set of primes dividing the order of G' and let

$$\mathcal{S}_{p_s} = \{i \in \{1, \dots, m\} : |G'_i| = p_s^a \text{ for some } a > 0\}$$

for $1 \leq s \leq t$. Then

$$\{1, \dots, m\} = \dot{\bigcup_{1 \leq s \leq t}} \mathcal{S}_{p_s}$$

and $G' = G'_{p_1} \times \dots \times G'_{p_t}$, where

$$G'_{p_s} = \bigtimes_{j \in \mathcal{S}_{p_s}} G'_j$$

is the p_s-Sylow subgroup of G'. So G'_{p_s} is elementary abelian and can thus be viewed as an $\mathbb{F}_{p_s}[G]$-module. Regarding G'_{p_s} in this way, we see that

$$G'_{p_s} = \bigoplus_{j \in \mathcal{S}_{p_s}} G'_j,$$

a direct sum of irreducible $\mathbb{F}_{p_s}[G]$- submodules. Hence G'_{p_s} is completely reducible by Isaacs [1, Theorem 1.10, pages 5]. Furthermore, since $C_G(G'_j) \neq C_G(G'_k)$ for $1 \leq j < k \leq m$,

$$G'_j(G'_{p_s}) = G'_j$$

for all $j \in \mathcal{S}_{p_s}$, where $G'_j(G'_{p_s})$ denotes the G'_j-homogeneous part of G'_{p_s}. It now follows from Isaacs [1, Lemma 1.13 page 6] that every minimal normal subgroup of G contained in G' is of the form G'_i for some $1 \leq i \leq m$.

For $1 \leq i \leq m$, let $B_i = B/C_B(G'_i)$ and L_i be the external semi-direct product of G'_i and B_i via τ_i, where τ_i is the homomorphism from B_i to $Aut(G'_i)$ defined by

$$g_i^{\tau_i(bC_B(G'_i))} = g_i^b$$

for all $g_i \in G'_i$ and $b \in B$.

Let $L = L_1 \times \cdots \times L_m$ and let μ_B be the map defined from B to

$$B_1 \times \cdots \times B_m \subseteq L$$

by $\mu_B(b) = (bC_B(G'_1), \ldots, bC_B(G'_m))$ for all $b \in B$. Clearly μ_B is a homomorphism and

$$ker\mu_B = \bigcap_{i=1}^{m} C_B(G'_i) = Z(G).$$

Furthermore, $\mu_B(C_i) = B_i$ for $1 \leq i \leq m$ and consequently

$$\mu_B(B) = \mu_B(C_1) \ldots \mu_B(C_m)\mu_B(A) = B_1 \times \cdots \times B_m.$$

Let μ be the map defined from G to L by

$$\mu(g'b) = g'\mu_B(b)$$

for all $g' \in G'$ and $b \in B$. Then μ is an epimorphism from G to L and $ker\mu(G) = Z(G)$.

Now suppose that D is a complement of G' in G. For $1 \leq i \leq m$, let $D_i = D/C_D(G'_i)$ and $[G'_i]D_i$ denote the external semi-direct product of G'_i and D_i via σ_i, where σ_i is the homomorphism from D_i to $Aut(G'_i)$ defined by

$$g_i^{\sigma_i(dC_D(G'_i))} = g_i^d$$

for all $g_i \in G'_i$ and $d \in D$.

Let N be a normal subgroup of G contained in G'. Then

$$G' \subseteq C_G(N) \subseteq G'D = G'B$$

and

$$G'\left(C_G(N) \cap D\right) = C_G(N) \cap G'D = C_G(N) \cap G'B = G'\left(C_G(N) \cap B\right).$$

In particular, $|C_G(N) \cap D| = |C_G(N) \cap B|$. So $|D_i| = |B_i|$ for $1 \leq i \leq m$ and

$$|G/Z(G)| = |L| = |[G'_1]D_1 \times \cdots \times [G'_m]D_m|.$$

Let λ_D be the map defined from D to

$$D_1 \times \cdots \times D_m \subseteq [G'_1]D_1 \times \cdots \times [G'_m]D_m$$

by $\lambda_D(d) = (dC_D(G'_1), \ldots, dC_D(G'_m))$ for all $d \in D$ and let λ be the map defined from G to

$$[G'_1]D_1 \times \cdots \times [G'_m]D_m$$

by $\lambda(g'd) = g'\lambda_D(d)$ for all $g' \in G'$ and $d \in D$. Then λ is a homomorphism and

$$ker\lambda = \bigcap_{i=1}^{m} C_D(G'_i) = C_D(G') \subseteq Z(G).$$

So $ker\lambda = Z(G)$ and

$$G/Z(G) \cong [G_1']D_1 \times \cdots \times [G_m']D_m,$$

because $|G/ker\lambda| \geq |G/Z(G)| = |[G_1']D_1 \times \cdots \times [G_m']D_m| \geq |G/ker\lambda|$. The proof is complete. □

Theorem 4.1.4 *Let G be a non-abelian $\mathcal{X}$-group. Then $G' \cap Z(G) = 1$ and G admits a model subgroup if and only if $G/Z(G)$ is isomorphic to a direct product of subgroups*

$$G_1, \ldots, G_m$$

satisfying the following statements.

(a) *G_i is a Frobenius group at C_i with Frobenius kernel G_i'.*

(b) *G_i' is elementary abelian of order r^{n_i}.*

(c) *C_i is cyclic of order $(r^{n_i} - 1)/(r^{d_i} - 1)$, for some d_i dividing n_i.*

(d) *The finite field $F = \mathbb{F}_{r^{n_i}}$ has an additive abelian subgroup H_F of order r^{d_i} satisfying $N_{F/K}(H_F) = K$, where $K = \mathbb{F}_{r^{d_i}}$.*

Proof. The result follows by Lemma 4.1.3 , Theorem 2.4.2 , Theorem 2.5.2 , and Theorem 3.5.1 □

4.2 Class closure properties

Lemma 4.2.1 *Let G be a $\mathcal{X}$-group and let K be a normal subgroup of G. Then G/K is a $\mathcal{X}$-group.*

Proof. If G is abelian, then G/K is abelian and the result follows immediately. So we may assume that G has subgroups $G_1, \dots, G_m$ and A satisfying the following statements.

$$[G_iK/K, G_jK/K] = [G_1, G_2]K/K = K/K$$

for $i \neq j$,

$$[G_iK/K, AK/K] = [G_i, A]K/K = K/K$$

for all i and

$$G/K = (G_1K/K) \dots (G_mK/K)(AK/K).$$

So we need only show that the factor groups

$$\frac{G_iK}{K} \cong \frac{G_i}{G_i \cap K}$$

are either abelian or not nilpotent with a minimal derived group in order to complete the proof.

Since G_i' is a minimal normal subgroup of G_i, either $G_i' \subseteq K$ or $G_i' \cap K = 1$. If $G_i' \subseteq K$, then G_iK/K is abelian. So we may assume that

$$G_i' \cap K = 1.$$

Suppose that $z_i \in Z_i$, where

$$\frac{Z_i}{G_i \cap K} = Z(G_i/G_i \cap K),$$

then $[z_i, g_i] \in G_i' \cap K = 1$ for all $g_i \in G_i$. Thus

$$Z(G_i/G_i \cap K) = \frac{Z(G_i)}{G_i \cap K}$$

and $G_i/G_i \cap K$ cannot be nilpotent, because G_i is not nilpotent. Finally,

$$G_i'(G_i \cap K) = G_i' \times (G_i \cap K),$$

and thus $(G_i/G_i \cap K)'$ is a minimal normal subgroup of $G_i/G_i \cap K$, if and only if G_i' is a minimal normal subgroup of G_i. The result follows. □

Lemma 4.2.2 *Let G be a finite soluble group and let K be a normal subgroup of G. Suppose that $G' \cap K = 1$. Then G is a $\mathcal{X}$-group if and only if G/K is a $\mathcal{X}$-group.*

Proof. If G is a $\mathcal{X}$-group then G/K is a $\mathcal{X}$-group by Lemma 4.2.1.

Suppose that G/K is a $\mathcal{X}$-group. If G/K is abelian, then G is abelian because $G' \subseteq K \cap G' = 1$. So we may assume that G/K has subgroups $G_1/K, \ldots, G_m/K$ and A/K satisfying the statements (X.1) - (X.6) above. Thus

$$[G_i, G_j] \subseteq G' \cap K = 1$$

for $i \neq j$,

$$[G_i, A] \subseteq G' \cap K = 1$$

for all i, and

$$G = G_1 \ldots G_m A.$$

Furthermore, A is abelian and the G_i cannot be nilpotent, because the G_i/K are not nilpotent. So we need only show that G_i' is a minimal normal subgroup of G_i for all i in order to complete the proof. But

$$G_i'K = G_i' \times K.$$

So G_i' is a minimal normal subgroup of G_i, if and only if $(G_i/K)'$ is a minimal normal subgroup of G_i/K. The result follows. □

4.3 Minimal non-$\mathcal{X}$-groups

Let G be a finite soluble group. Suppose that G satisfies the following statements :

(a) G is not a $\mathcal{X}$-group;

(b) G/N is a $\mathcal{X}$-group for all $1 \neq N \triangleleft G$.

Then we call G a minimal non-$\mathcal{X}$-group.

Lemma 4.3.1 *Let G be a minimal non-$\mathcal{X}$-group and let K be a minimal normal subgroup of G. Suppose that G/K is abelian. Then*

(A) *G is a p-group, G' is cyclic of order p and is the unique minimal normal subgroup of G.*

Proof. Since G is a minimal non-$\mathcal{X}$-group, G is non-abelian, $G' = K$ is the unique minimal normal subgroup of G by Lemma 4.2.2 and G is nilpotent. The result follows. □

Lemma 4.3.2 *Let G be a minimal non-$\mathcal{X}$-group and let K be a minimal normal subgroup of G. Suppose that $K \subseteq Z(G)$ and G/K is non-abelian. Then*

(B) *$G = UA$, where U and A are subgroups satisfying the following*

(a) *U is a central product of subgroups $G_1, \ldots, G_m$ with amalgamated centres;*

(b) *$G_i = G_i'C_i$, where $(|G_i'|, |C_i|) = 1$, for $1 \leq i \leq m$;*

(c) *G_i' is an extraspecial p-group for all i;*

(d) *$Z(U) = Z(G_i) = Z(G_i')$ for all i;*

(e) *$G_i/Z(U)$ is a Frobenius group at $C_iZ(U)/Z(U) \cong C_i$ with minimal Frobenius kernel $G_i'/Z(U)$ for all i;*

(f) *A is a p-group and $Z(U) \subseteq A \subseteq C_G(U)$;*

(g) *Either A is cyclic or $A' = Z(U)$ is the unique minimal normal subgroup of A.*

Proof. Since K is a central minimal normal subgroup of G, it must be cyclic of order p. Furthermore, K must be the unique minimal normal subgroup of G by Lemma 4.1.1(e), because the minimal normal subgroup K is contained in $G' \cap Z(G)$ by Lemma 4.2.2.

Since G/K is non-abelian, G has subgroups $H_1, \ldots, H_m$ and B containing K satisfying

$$G = H_1 \ldots H_m B,$$

where B/K is abelian, $[H_i, H_j] \subseteq K$ for $i \neq j$ and $[H_i, B] \subseteq K$ for $1 \leq i \leq m$. Furthermore, H_i/K is not nilpotent, $K \subseteq H_i'$, because K is the unique minimal normal subgroup of G, and H_i'/K is a minimal normal subgroup of H_i/K for all i.

Let $Z/K = Z(G/K)$. Then the normal subgroup $K \subseteq G'Z \subseteq G$ is nilpotent, because $K \subseteq Z(G)$ and $G'Z/K$ is abelian by Lemma 4.1.1(d). But

$O_{p'}(G'Z) = 1$, since K is the unique minimal normal subgroup of G, and the nilpotence of $G'Z$ ensures that $G'Z$ is a p-group.

Let $Z_i/K = Z(H_i/K)$ for $1 \leq i \leq m$. Then $H_i'Z_i$ is a p-group and

$$(|H_i : H_i'Z_i|, |H_i'Z_i|) = 1$$

by Lemma 1.5.1 and Theorem 1.5.4, because H_i/Z_i is a Frobenius group with minimal Frobenius kernel $H_i'Z_i/Z_i$ by Lemma 4.1.2. So $H_i'Z_i$ is complemented in H_i, by C_i say. Furthermore,

$$H_i'C_i/K = H_i'C_i/H_i'C_i \cap Z_i \cong H_i'C_iZ_i/Z_i = H_i/Z_i$$

by Lemma 4.1.1(c) and $H_i'C_i/K$ is a Frobenius group at C_iK/K with minimal Frobenius kernel H_i'/K by Lemma 4.1.2.

Let $G_i = H_i'C_i = G_i'C_i$ for $1 \leq i \leq m$ and let $A = Z_1 \ldots Z_mB$. Then

$$G = G_1 \ldots G_mA.$$

and $A/K = Z(G/K)$ is a p-group. Furthermore, the commutators

$$[G_i, G_j] \subseteq K$$

for $i \neq j$ and $[G_i, A] \subseteq K$ for $1 \leq i \leq m$.

Let $c_j \in C_j$. Then $k^{c_j} = k$ for all $k \in K$ and $g_i^{c_j}K = g_iK$ for all $g_i \in G_i$ and $i \neq j$. Thus $g_i^{c_j} = g_i$ for all $g_i \in G_i$ and $i \neq j$, because $(|C_j|, |K|) = 1$. So $C_jK \subseteq C_G(G_i)$ for $i \neq j$ and since G_i'/K is the unique minimal normal subgroup of G_i/K this ensures that $G_j \subseteq C_G(G_i)$ for $i \neq j$. We can show similarly that $G_j \subseteq C_G(A)$ for all j. Thus G is a central product of the subgroups $G_1, \ldots, G_m$ and A. Furthermore, K is the unique minimal normal subgroup of A and consequently $A' = K$ or A is cyclic of prime power order.

Suppose that G_i' is abelian. If G_i' is elementary abelian, then it can be regarded as an $\mathbb{F}_p[G/C_G(G_i')]$-module. But $G/C_G(G_i')$ is isomorphic to C_i, which has order co-prime to p, so we can apply Maschke's theorem. Thus

$$G_i' = K \times L,$$

where $L \cong G_i'/K$ is an $\mathbb{F}_p[G/C_G(G_i')]$-module, contradicting the fact that K is the unique minimal normal subgroup of G. If G_i' is not elementary abelian. Then $\Phi(G_i') = K$. But $G/C_G(G_i') \cong C_i$ is a p'-group of automorphisms of G_i', which acts fixed-point freely and irreducibly on G_i'/K. So G' is homocyclic and G_i'/K and K are $G/C_G(G_i')$-isomorphic contradicting our assumption that K is central. Thus G_i' is non-abelian, $G_i'' = Z(G_i') = \Phi(G_i') = K$ and G_i' is extra- special.

Setting $U = G_1 \cdots G_m$ completes the proof. □

Lemma 4.3.3 *Let G be a minimal non-$\mathcal{X}$-group and let K be a minimal normal subgroup of G. Suppose that $K \subseteq \Phi(G)$, but $K \not\subseteq Z(G)$. Then G satisfies one of the following statements.*

(C) *$G = G'C$ and the following conditions hold :*

(i) $(|G'|, |C|) = 1$;

(ii) *$\Phi(G')$ is the unique minimal normal subgroup of G;*

(iii) *$G/\Phi(G')$ is a Frobenius group at $C\Phi(G')/\Phi(G')$ with minimal Frobenius kernel $G'/\Phi(G')$;*

(iv) *G' is either homocyclic or special.*

(D) *$G = (G'A)C$ and the following conditions hold :*

(i) $(|G'A|, |C|) = 1$;

(ii) *$K = [G', A]$ is the unique minimal normal subgroup of G;*

(iii) $A/K = Z(G/K)$;

(iv) *G/A is a Frobenius group at CA/A with minimal Frobenius kernel $G'A/A$;*

(v) *$G'A$ is an r-group.*

(vi) *A is elementary abelian;*

(vii) *G' is elementary abelian, homocyclic or special;*

(viii) *$K = \Phi(G'A) = (G'A)'$ and $K \subseteq Z(G'A)$.*

(E) *$G = G_1G_2$ and the following conditions hold:*

(i) $G_i = G_i'C_i$;

(ii) $(|G_i'|, |C_i|) = 1$;

(iii) *$K = [G_1', G_2']$ is the unique minimal normal subgroup of G;*

(iv) $G/K \cong G_1/K \times G_2/K$;

(v) *G_i/K is a Frobenius group at C_iK/K with minimal Frobenius kernel G_i'/K;*

(vi) *G_i' is elementary abelian;*

(vii) *$G_1'G_2'$ is special.*

Proof. Since the minimal normal subgroup K is contained in $G' \cap \Phi(G)$ by Lemma 4.2.2, K must be the unique minimal normal subgroup of G by Lemma 4.1.1(f),

Suppose that G/K is abelian. Then $K \subseteq Z(G)$ by Lemma 4.3.1. So we may assume without loss of generality that G has subgroups $H_1, \ldots, H_m$ and B containing K satisfying

$$G = H_1 \ldots H_m B,$$

where B/K is abelian, $[H_i, H_j] \subseteq K$ for $i \neq j$ and $[H_i, B] \subseteq K$ for $1 \leq i \leq m$. Furthermore, H_i/K is not nilpotent, $K \subseteq H_i'$, because K is the unique minimal normal subgroup of G, and H_i'/K is a minimal normal subgroup of H_i/K for all i.

Let $Z/K = Z(G/K)$. Then the normal subgroup $K \subseteq G'Z \subseteq G$ is nilpotent, because $K \subseteq \Phi(G)$ and $G'Z/K$ is abelian by Lemma 4.1.1(d). But $O_{p'}(G'Z) = 1$, since K is the unique minimal normal subgroup of G, and the nilpotence of $G'Z$ ensures that $G'Z$ is a p-group.

Let $Z_i/K = Z(H_i/K)$ for $1 \leq i \leq m$. Then $H_i'Z_i$ is a p-group and

$$(|H_i : H_i'Z_i|, |H_i'Z_i|) = 1$$

by Lemma 1.5.1 and Theorem 1.5.4, because H_i/Z_i is a Frobenius group with minimal Frobenius kernel $H_i'Z_i/Z_i$ by Lemma 4.1.2. So $H_i'Z_i$ is complemented in H_i, by C_i say. Furthermore,

$$H_i'C_i/K = H_i'C_i/H_i'C_i \cap Z_i \cong H_i'C_iZ_i/Z_i = H_i/Z_i$$

by Lemma 4.1.1(c) and $H_i'C_i/K$ is a Frobenius group at C_iK/K with minimal Frobenius kernel H_i'/K.

Let $G_i = H'_iC_i = G'_iC_i$ for $1 \leq i \leq m$ and let $A = Z_1 \ldots Z_mB$. Then

$$G = G_1 \ldots G_mA.$$

and $A/K = Z(G/K)$ is a p-group. Furthermore, the commutators

$$[G_i, G_j] \subseteq K$$

for $i \neq j$ and $[G_i, A] \subseteq K$ for $1 \leq i \leq m$.

Suppose that $K \subseteq \Phi(A)$. Then $C_i \subseteq C_G(A)$ for all i, since C_i centralises A/K and $|C_i|$ is co-prime to p. So $C_iK \subseteq C_G(A)$, since K is central in $G'Z$. But G'_i/K is the unique minimal normal subgroup of G_i/K, so $G_i \subseteq C_G(A)$ for all i, contradicting our assumption that K is not central. Thus we may assume without loss of generality that A is elementary abelian.

Suppose that $K \subseteq \Phi(G'_j)$ for some j. Then $C_i \subseteq C_G(G'_j)$ for all $i \neq j$, since C_i centralises G'_j/K and C_i is co-prime to p. So $C_iK \subseteq C_G(G'_j)$ for all $i \neq j$, since K is central in $G'Z$. But G'_i/K is the unique minimal normal subgroup of G_i/K for all i, so $G_i \subseteq C_G(G'_j)$ for all $i \neq j$ and

$$[G'_i, G'_j] = 1$$

for all $i \neq j$.

If $K \subseteq \Phi(G'_k)$ for some $k \neq j$, then $C_j \subseteq C_G(G'_k)$, since C_j centralises G'_k/K and $|C_j|$ is co-prime to p. But $K \subseteq G'_j \cap G'_k$ and K is central in $G'Z$. So $K \subseteq Z(G)$, contradicting our assumption and we may assume that the G'_i are elementary abelian for all $i \neq j$.

If $[G'_i, G'_\ell] = K$ for some $i, \ell \neq j$, then $C_j \subseteq C_G(G'_iG'_\ell)$ since C_j centralises $G'_iG'_\ell/K$ and $|C_j|$ is co-prime to p. But $K \subseteq G'_iG'_\ell \cap G'_j$ and is thus central, contradicting our assumption. So we may assume that

$$[G'_i, G'_\ell] = 1$$

for all $i, \ell \neq j$. We can show in an identical fashion that

$$[G'_i, A] = 1$$

for all $i \neq j$.

So G'_i is elementary abelian and can be regarded as an $\mathbb{F}_p[G/C_G(G'_i)]$-module. But $G/C_G(G'_i)$ has order co-prime to p, because $G'Z \subseteq C_G(G'_i)$, enabling us to apply Maschke's theorem. Hence

$$G'_i = K \times L,$$

where $L \cong G'_i/K$ is an $\mathbb{F}_p[G/C_G(G'_i)]$-module, contradicting the fact that K is the unique minimal normal subgroup of G. So $G = (G'_jA)C_j$.

If G'_j is abelian, then G'_j is homocyclic, because C_j is a p' group of automorphisms of G'_j acting irreducibly on $G'_j/\Phi(G'_j)$. If G'_j is non-abelian, then $G''_j = \Phi(G'_j) = Z(G'_j)$ and G'_j is special.

If $[G'_j, A] = 1$ and $A > K$, then $G/C_G(A)$ has order co-prime to p. So we can apply Maschke's theorem to the elementary abelian group A regarded as an $\mathbb{F}_p[G/C_G(A)]$-module. Hence

$$A = K \times L,$$

where $L \cong A/K$ is an $\mathbb{F}_p[G/C_G(A)]$- module, contradicting the fact that K is the unique minimal normal subgroup of G. So

$$G = G'_jC_j,$$

and satisfies the conditions outlined in case (a).

If $[G'_j, A] = K$, then $(G'_jA)' = \Phi(G'_jA) = K$. Furthermore, $K \subseteq Z(G'_jA)$ and

$$G = (G'_jA)C_j$$

satisfies the conditions outlined in case (b).

Now suppose that G'_i is elementary abelian for all i. If $[G'_j, G'_k] = K$ for some $1 \leq j < k \leq m$, then

$$(G'_jG'_k)' = \Phi(G'_jG'_k) = K$$

and $Z(G'_jG'_k) \subseteq K$. If $Z(G'_jG'_k) > K$, then by Lemma 4.1.3 either $Z(G'_jG'_k) = G'_j$ or G'_k, contradicting our assumption that $[G'_j, G'_k] = K$. So $Z(G'_jG'_k)$ equals K and $G'_jG'_k$ is special.

Using similar arguments to those given above we may assume that for $i \neq j$ or k, the commutator $[G'_i, G'_jG'_k] = 1$ and

$$[G'_i, A] = [G'_i, G'_\ell] = 1$$

for all $\ell \neq j$ or k. Thus $G/C_G(G'_i)$ has order co-prime to p and we can derive a contradiction to the uniqueness of K by applying Maschke's theorem to the elementary abelian group G'_i regarded as an $\mathbb{F}_p[G/C_G(G'_i)]$-module. Again using arguments similar to those outlined above we can show that $[G'_j, A] = [G'_k, A] = 1$, if $A > K$. Thus $G/C_G(A)$ has order co-prime to p and we can derive a contradiction to the uniqueness of K by applying Maschke's theorem to the elementary abelian group A regarded as an $\mathbb{F}_p[G/C_G(A)]$-module. So

$$G = G_jG_k$$

and satisfies the conditions outlined in case (c).

If $[G'_j, A] = K$ for some $1 \leq j \leq m$, then $\Phi(G'_jA) = K$. So using similar arguments to those given above we may assume that for $i \neq j$, the commutator $[G'_i, G'_jA] = 1$ and $[G'_i, G'_\ell] = 1$ for all $\ell \neq j$. Thus $G/C_G(G'_i)$ has order co-prime to p and we can derive a contradiction to the uniqueness of K by applying Maschke's theorem to the elementary abelian group G'_i regarded as an $\mathbb{F}_p[G/C_G(G'_i)]$-module. So

$$G = (G'_jA)C_j$$

satisfies the conditions outlined in case (b). The proof is complete. □

Lemma 4.3.4 *Let G be a minimal non-$\mathcal{X}$-group and let K be a minimal normal subgroup of G. Suppose that $\Phi(G) = 1$. Then G satisfies one of the following statements.*

(F) *$G = G''X$ and the following conditions hold:*

(i) *$G'' \cap X = 1$;*

(ii) *G'' is the unique minimal normal subgroup of G;*

(iii) *X is a non-abelian $\mathcal{X}$-group;*

(iv) *$X \subseteq Aut(G'')$.*

(G) *There exists a group L and a monomorphism μ from G into L satisfying the following conditions:*

(i) *$L = L_0 \times \cdots \times L_m$;*

(ii) *L_i is a Frobenius group with minimal Frobenius kernel L'_i;*

(iii) $\mu(G') = L'_0 \times \cdots \times L'_m$;

(iv) $L = \mu(G)L_i$ *for* $0 \leq i \leq m$.

Proof. By Lemma 4.3.1 and our assumption that K is a minimal normal subgroup of G not contained in $\Phi(G)$ we may assume without loss of generality that K is complemented in G by a non-abelian $\mathcal{X}$-group, X say. So X has subgroups $G_1, \ldots, G_m$ and A satisfying the statements (X.1) - (X.6) above. Furthermore, Lemma 4.1.2 states that the derived subgroup G'_i of G_i is complemented in G_i by C_i say.

Since X is a $\mathcal{X}$-group, the minimal normal subgroup K is contained in G' by Lemma 4.2.2 and $(G/K)' \cong X'$ is abelian by Lemma 4.1.1(d). So we may assume without loss of generality that G'' is either equal to 1 or K.

Suppose that $G'' = K$. Then K is the unique minimal normal subgroup of G, because every epimorphic image of G is a $\mathcal{X}$-group and consequently has an abelian derived subgroup. So $C_X(G'') = 1$ and G satisfies the conditions outlined in case (a).

Suppose that $G'' = 1$. Then

$$G' = K \times G'_1 \times \cdots \times G'_m$$

and there exists a subgroup

$$B \cong C_1 \ldots C_m A$$

complementing G' in G, since $\Phi(G) = 1$.

Let $B_0 = B/C_B(K)$. Let L_0 be the external semi-direct product of K and B_0 via σ_0, where σ_0 is the homomorphism from B_0 to $Aut(K)$ defined by

$$k^{\sigma(bC_B(K))} = k^b$$

for all $k \in K$ and $b \in B$. Then L_0 is a Frobenius group with minimal Frobenius kernel $L_0' = K$, by Lemma 4.1.2.

For $1 \leq i \leq m$, let $B_i = B/C_B(G_i')$ and L_i be the external semi-direct product of G_i' and B_i via σ_i, where σ_i is the homomorphism from B_i to $Aut(G_i')$ defined by

$$g_i^{\sigma(bC_B(G_i'))} = g_i^b$$

for all $g_i \in G_i'$ and $b \in B$. Then L_i is a Frobenius group with minimal Frobenius kernel L_i', by Lemma 4.1.2.

Let $L = L_0 \times L_1 \times \cdots \times L_m$ and let μ_B be the map defined from B to $B_0 \times B_1 \times \cdots \times B_m \subseteq L$ by

$$\mu(b) = (bC_B(K), bC_B(G_1'), \ldots, bC_B(G_m'))$$

for all $b \in B$. Clearly μ_B is a homomorphism and $ker\mu_B$ is a normal subgroup of G.

If $ker\mu_B \neq 1$, then $G/ker\mu_B$ is a $\mathcal{X}$-group and $ker\mu_B \cap G' = 1$ contradicting our assumption that G is not a $\mathcal{X}$-group by Lemma 4.2.2. So we may assume without loss of generality that μ_B is a monomorphism.

Let μ be the map defined from G to L by $\mu(gb) = g\mu_B(b)$ for all $g \in G'$ and $b \in B$. Then μ is a monomorphism from G to L and

$$\mu(G') = L_0' \times \cdots \times L_m'.$$

Let π_i be the projective map from L to

$$L_0 \times \cdots \times L_{i-1} \times L_{i+1} \times \cdots L_m$$

for $0 \leq i \leq m$. Then $\pi_i(\mu(G))$ is a $\mathcal{X}$-group, by the minimality of G, and

$$(\pi_i(\mu(G)))' = L_0' \times \cdots \times L_{i-1}' \times L_{i+1}' \times \cdots \times L_m'.$$

Furthermore, $(\pi_i(\mu(G)))'$ is complemented in $\pi_i(\mu(G))$ by $\pi_i(\mu(B))$ and

$$\frac{|\pi_i(\mu(B))|}{|C_{\pi_i(\mu(B))}(\pi_i(L_j'))|} = |B_j|$$

for $j \neq i$. The result follows by Lemma 4.1.3. □

Chapter 5

Case Studies

In this chapter we shall consider under what circumstances a minimal non-$\mathcal{X}$-group of derived length 3 satisfying the co-prime condition

$$(|G : G'|, |G' : G''|) = 1$$

can possess a model subgroup.

5.1 Case B

We begin by considering minimal non-$\mathcal{X}$-groups satisfying the conditions outlined in Case B.

Lemma 5.1.1 *Let $G = UA$, where U and A are subgroups satisfying the following conditions.*

(a) *U is a central product of subgroups $G_1, \ldots, G_m$ with amalgamated centres;*

(b) *$G_i = G_i'C_i$, where $(|G_i'|, |C_i|) = 1$, for $1 \leq i \leq m$;*

(c) *G_i' is an extraspecial r-group for all i;*

(d) *$Z(U) = Z(G_i) = Z(G_i')$ for all i;*

(e) *$G_i/Z(U)$ is a Frobenius group at $C_iZ(U)/Z(U) \cong C_i$ with minimal Frobenius kernel $G_i'/Z(U)$ of order r^{n_i} for all i;*

(f) *A is a p-group and $Z(U) \subseteq A \subseteq C_G(U)$;*

(g) *Either A is cyclic or $A' = Z(U)$ is the unique minimal normal subgroup of A.*

Then G does not admit a model subgroup.

Proof. Suppose that H is a model subgroup of G. Then $H \cap Z(U) = 1$ by Lemma 2.6.1 and $HZ(U)/Z(U)$ is a model subgroup of

$$G/Z(U) = G_1/Z(U) \times \cdots \times G_m/Z(U) \times A/Z(U),$$

by Theorem 2.3.2. So

$$HZ(U)/Z(U) = HZ(U)/Z(U) \cap G_1/Z(U) \times \cdots \times HZ(U)/Z(U) \cap G_m/Z(U),$$

by Theorem 2.4.2 and Corolla ry 2.1.2. Furthermore,

$$HZ(U)/Z(U) \cap G_i/Z(U)$$

is a model subgroup of $G_i/Z(U)$. Therefore Theorem 3.2.1 states that

$$C_i \cong C_iZ(U)/Z(U)$$

is cyclic of odd order and

$$|G_i : G_i'| = |C_i| = \frac{r^{n_i} - 1}{r^{d_i} - 1},$$

for some d_i dividing n_i and

$$|HZ(U)/Z(U) \cap G_i'/Z(U)| = r^{n_i - d_i}$$

by Theorem 1.6.4 and Corolla ry 2.3.3. So

$$|HZ(U) \cap G_i'| = r^{n_i - d_i + 1}.$$

Furthermore, $HZ(U) \cap G_i'$ is elementary abelian, since $HZ(U)/Z(U)$ is elementary abelian and$H \cap Z(U) = 1$. Thus $n_i = 2d_i$, by Theorem 1.4.1, and $r = 2$, by Corolla ry 3.5.4. Hence G_i' is a central product of d_i dihedral groups of order 8 with amalgamated centres, by Theorem 1.4.2, and

$$|C_i| = 2^{d_i} + 1.$$

So, by Theorem 1.2.5 and noting that

$$2^{n_i} - 1 = (2^{d_i} - 1)(2^{d_i} + 1),$$

either $n = 6$ or there exists a prime q dividing $|C_i|$ satisfying the following conditions:

(a) q divides $2^{n_i} - 1$;

(b) q does not divide $2^j - 1$ whenever $0 < j < n_i$.

If $n \neq 6$, then regarding C_i as a subgroup of $Aut(G_i')$, we have

$$|C_i| = |C_i Inn(G_i')/Inn(G_i')|,$$

which divides

$$2^{(2d_i(2d_i-2)/4)+1}(2^{d_i} - 1)\Pi_{j=1}^{d_i-1}(2^{2j} - 1),$$

by Theorem 1.4.4. But this contradicts our assumption that there exists a prime q dividing the order of C_i satisfying the statements above.

If $n = 6$, then C_i is cyclic of order 9 and G' is a central product of 3 dihedral groups of order 8. So C_i is isomorphic to a subgroup of

$$S_8 \cong Aut(G_i')/Inn(G_i'),$$

by Theorem 1.4.4. But this cannot not happen, because S_8 contains no element of order 9. The proof is complete. □

5.2 Case C

We now turn to minimal non-$\mathcal{X}$-groups of derived length 3 satisfying the conditions outlined in Case C. We begin by proving three preliminary lemmas.

Lemma 5.2.1 *Let r be a prime, let $a > 1$ be an integer prime to r and let b be the order of r modulo a. Then*

$$r^c \left| \frac{r^b - 1}{a} + 1 \right.$$

if and only if

$$r^c \left| \frac{r^{nb} - 1}{a} + 1 \right.$$

for all $n \in \mathbb{N}$.

Proof. For all $n \in \mathbb{N}$ we have

$$\frac{r^{nb}-1}{a} = \left(\frac{r^{nb}-1}{r^b-1}\right)\left(\frac{r^b-1}{a}\right).$$

Furthermore,

$$\left(\frac{r^{nb}-1}{r^b-1}\right) \equiv 1 \; mod \, r^c$$

for all $0 < c \leq b$ and consequently

$$\frac{r^{nb}-1}{a} \equiv -1 \; mod \, r^c$$

if and only if

$$\frac{r^b-1}{a} \equiv -1 \; mod \, r^c$$

for all $0 < c \leq b$. In order to complete the proof we simply note that r^b does not divide

$$\frac{r^b-1}{a} + 1,$$

because $a > 1$. □

Lemma 5.2.2 *Let r be a prime and let $b > 0$ be an even integer. Suppose that $a|r^b - 1$ and*

$$r^{\frac{1}{2}b} \left| \frac{r^b-1}{a} + 1. \right.$$

Then either $a = r^{\frac{1}{2}b} + 1$ or $a = 1$.

Proof. There exists a y such that

$$\begin{aligned} r^{\frac{1}{2}b}y - 1 &= \frac{r^b-1}{a} \\ &= \frac{\left(r^{\frac{1}{2}b}-1\right)\left(r^{\frac{1}{2}b}+1\right)}{a} \\ &= cd, \end{aligned}$$

Proof. For all $n \in \mathbb{N}$ we have

$$\frac{r^{nb}-1}{a} = \left(\frac{r^{nb}-1}{r^b-1}\right)\left(\frac{r^b-1}{a}\right).$$

Furthermore,

$$\left(\frac{r^{nb}-1}{r^b-1}\right) \equiv 1 \; mod \; r^c$$

for all $0 < c \leq b$ and consequently

$$\frac{r^{nb}-1}{a} \equiv -1 \; mod \; r^c$$

if and only if

$$\frac{r^b-1}{a} \equiv -1 \; mod \; r^c$$

for all $0 < c \leq b$. In order to complete the proof we simply note that r^b does not divide

$$\frac{r^b-1}{a} + 1,$$

because $a > 1$. □

Lemma 5.2.2 *Let r be a prime and let $b > 0$ be an even integer. Suppose that $a|r^b - 1$ and*

$$r^{\frac{1}{2}b} \left| \frac{r^b-1}{a} + 1. \right.$$

Then either $a = r^{\frac{1}{2}b} + 1$ or $a = 1$.

Proof. There exists a y such that

$$\begin{aligned} r^{\frac{1}{2}b}y - 1 &= \frac{r^b-1}{a} \\ &= \frac{\left(r^{\frac{1}{2}b}-1\right)\left(r^{\frac{1}{2}b}+1\right)}{a} \\ &= cd, \end{aligned}$$

where $c | r^{\frac{1}{2}b} - 1$ and $d | r^{\frac{1}{2}b} + 1$.

If $y = 1$, then $a = r^{\frac{1}{2}b} + 1$. So we may assume without loss of generality that $y \neq 1$. Re-arranging the equation above we obtain

$$r^{\frac{1}{2}b}(y-1) + \left(r^{\frac{1}{2}b} - 1\right) = cd$$

and

$$\begin{aligned} r^{\frac{1}{2}b}(y-1) &= cd - \left(r^{\frac{1}{2}b} - 1\right) \\ &= cd - ce \\ &= c(d-e), \end{aligned}$$

where $ce = r^{\frac{1}{2}b} - 1$. So $c | y - 1$, since $y \neq 1$ and $(c, r) = 1$. Furthermore,

$$\begin{aligned} r^{\frac{1}{2}b}(y-1) &= cd - \left(r^{\frac{1}{2}b} - 1\right) \\ &\leq c\left(r^{\frac{1}{2}b} + 1\right) - \left(r^{\frac{1}{2}b} - 1\right) \\ &= r^{\frac{1}{2}b}(c-1) + (c+1). \end{aligned}$$

And consequently, the following inequality holds.

$$(y-c)\, r^{\frac{1}{2}b} \leq (c+1) \leq r^{\frac{1}{2}b}.$$

So $y - c$ must equal 1, since $c | y - 1$, and $c = r^{\frac{1}{2}b} - 1$. Thus $y = r^{\frac{1}{2}b}$ and the order of $a = 1$. □

Lemma 5.2.3 *Let G be a non-abelian r-group. Suppose that $\Phi(G)$ has order r, $Z(G)$ has order r^{k+1} and $C \neq 1$ is a r'-group of automorphisms of G,* *which centralizes $\Phi(G)$ and acts fixed-point-freely on $G/\Phi(G)$. Then the set of non-linear irreducible characters of G regarded as a C-set has*

$$(r-1)\left(\frac{(r^k-1)}{|C|}+1\right)$$

orbits.

Proof. Clearly, $Z(G)$ is a C-invariant abelian subgroup of G and as such can be regarded as a direct product of C-invariant homocyclic subgroups. Suppose that $Z(G)$ is not elementary abelian. Then $k > 0$ and

$$Z(G) = H \times E,$$

where H is a C-invariant cyclic group of order r^2 and E is a C-invariant elementary abelian subgroup of order r^{k-1}, since $\Phi(Z(G)) \subseteq \Phi(G)$. Thus $H/\Phi(H) = H/\Phi(G)$ and $\Phi(H) = \Phi(G)$ are C-isomorphic, contradicting our assumption that C centralizes $\Phi(G)$ and acts fixed-point- freely on $G/\Phi(G)$. So $Z(G)$ must be elementary abelian and consequently can be regarded as a $GF(r)$[C]-module. Hence,

$$Z(G) = \Phi(G) \times Z,$$

where Z is C-invariant, by Maschke's Theorem. Now $G/\Phi(G)$ can also be regarded as a $GF(r)$[C]-module and re-applying Maschke's Theorem we obtain

$$G/\Phi(G) = Q/\Phi(G) \times Z(G)/\Phi(G),$$

where $Q/\Phi(G)$ is C-invariant and Q is extra-special. So

$$G = Q \times Z,$$

and

$$Irr(G) = \{\theta\lambda \mid \theta \in Irr(Q)\,,\, \lambda \in Irr(Z)\}.$$

Furthermore,

$$\chi^c = \theta^c \lambda^c$$

for all $c \in C$. Now since Z is abelian and $Z(G)/\Phi(G)$ and Z are C- isomorphic, the fact that C acts fixed-point-freely on $G/\Phi(G)$ implies that $Irr(Z)$ regarded as a C-set has

$$\frac{r^k - 1}{|C|} + 1$$

orbits. Suppose that $\chi = \theta\lambda$ is a non-linear irreducible character of G. Then θ must be one of the $(r-1)$ non-linear characters of Q, since Z is abelian. So θ vanishes outside $\Phi(Q) = \Phi(G)$ by Theorem 1.4.5 and consequently C centralizes θ. The result follows. □

Theorem 5.2.4 *Let G be a finite group satisfying the following statements.*

(i) $G = G'C$;

(ii) G' *is a special* r*-group;*

(iii) $(|G'|, |C|) = 1$;

(iv) $\Phi(G')$ *is the unique minimal normal subgroup of* G *of order* r^m;

(v) $M = C_G(\Phi(G')) \cap C \neq 1$;

(vi) $G/\Phi(G')$ *is a Frobenius group at* $C\Phi(G')/\Phi(G')$ *with minimal Frobenius kernel* $G'/\Phi(G')$ *of order* r^n;

Then either G does not admit a model subgroup or $n = 6$, $r = 2$, $m < n$ and M acts reducibly on $G'/\Phi(G')$.

Proof. Let $\mathcal{S}$ be the set of maximal subgroups of $\Phi(G')$. Then

$$Irr(G') - Irr(G'/\Phi(G')) = \dot{\bigcup_{T \in \mathcal{S}}} \{\chi \in Irr(G'/T) \mid \chi(1) \neq 1\},$$

by Lemma 1.4.8. Furthermore, if $T \in \mathcal{S}$, then G'/T is a non-abelian r-group and $\Phi(G'/T)$ has order r. Now let

$$\{T_1, \dots, T_j\}$$

be a complete set of orbit representatives of $\mathcal{S}$ viewed as a C-set and let

$$\mathcal{S}_1, \dots, \mathcal{S}_j$$

be the C-orbit containing T_i. Then by Lemma 1.4.7 there exists a $k_i \geq 0$ such that for all $U \in \mathcal{S}_i$, the factor group G'/U has r^n linear characters and

$$(r-1)r^{k_i}$$

irreducible characters of degree

$$r^{\frac{1}{2}(n-k_i)}.$$

Let $Irr(G'/\mathcal{S}_i)$ be the set of non-linear irreducible characters of G', which contain an element of $\mathcal{S}_i$ in their kernel. Then

$$Irr(G') - Irr(G'/\Phi(G')) = Irr(G'/\mathcal{S}_I) \dot{\cup} \cdots \dot{\cup} Irr(G'/\mathcal{S}_j)$$

by Lemma 1.4.8. Furthermore,

$$|Irr(G'/\mathcal{S}_i)| = |\mathcal{S}_i|(r-1)r^{k_i},$$

since the kernel of every non-linear character of G' contains one and only one element of $\mathcal{S}$.

Suppose that H is a model subgroup of G. Then $H\Phi(G')/\Phi(G')$ is a model subgroup of $G/\Phi(G')$, a Frobenius group with Frobenius complement $C\Phi(G')/\Phi(G')$ and abelian Frobenius kernel $G'/\Phi(G')$. Therefore Theorem 3.2.1 states that $C \cong C\Phi(G')/\Phi(G')$ is cyclic of odd order and

$$|G : G'| = |C| = \frac{r^n - 1}{r^d - 1},$$

for some d dividing n and the index of $H\Phi(G')/\Phi(G')$ in $G'/\Phi(G')$ is r^d by Theorem 1.6.4.

By Theorem 1.1.1, C/M acts fixed-point freely on $\Phi(G')$. So if

$$C_i = \{c \in C \mid T_i^c = T_i\},$$

then C_i/M acts fixed-point freely on $\Phi(G')$ and consequently acts fixed-point-freely on $\Phi(G)/T_i$ by Lemma 1.7.4. So

$$|C_i/M| | r - 1,$$

by Lemma 1.7.1 and Lemma 1.5.1 But $(|C|, r - 1) = 1$ by Corolla ry 3.5.6 and C_i must equal M. Thus

$$|\mathcal{S}_i| = |C/M|$$

and $Irr(G'/\mathcal{S}_i)$ has

$$(r-1)\left(\frac{r^{k_i} - 1}{|M|} + 1\right)$$

orbits viewed as a C-set by Lemma 5.2.3.

Now H is contained in G', by Corolla ry 2.3.3, So $1_H \uparrow G'$ is multiplicity-free and has exactly one irreducible constituent from each orbit of $Irr(G')$ viewed as a C-set.

Let $T \in \mathcal{S}_i$. Suppose that $\chi \in Irr(G'/T)$ and $\hat{\chi}$ is the corresponding character in G'/T. Then

$$\langle 1_H \uparrow G', \chi \rangle = \langle 1_{HT/T} \uparrow G'/T, \hat{\chi} \rangle,$$

by Lemma 2.3.1. In particular, $1_{HT/T} \uparrow G'/T$ is multiplicity-free.

Let $\overline{G'} = G'/T$,

$$\overline{Z} = Z(G')/T = \Phi(G')/T,$$

$\overline{Z_i} = Z_i/T = Z(G'/T)$ and $\overline{H} = HT/T$.

If $H \cap \Phi(G') \not\subseteq T$, then $\overline{Z} \subseteq \overline{H}$. So

$$ker(1_{\overline{H}} \uparrow \overline{G'}) = \bigcap_{\overline{g} \in \overline{G'}} (\overline{H})^{\overline{g}} \supseteq \overline{Z}$$

and no non-linear character of $Irr(G'/T)$ can be a constituent of $1_H \uparrow G'$.

Suppose that $H \cap \Phi(G') \subseteq T$ and $\overline{H} \cap \overline{Z_i}$ has order r^{ℓ_i}, then we claim that $\overline{H}$ intersects trivially with $\overline{Z}$ and

$$d = \frac{1}{2}n + \frac{1}{2}k_i - \ell i.$$

If $\overline{H} \cap \overline{Z} \neq 1$, then $\overline{Z} \subseteq \overline{H}$, because $\overline{Z}$ is cyclic of order r and $T \subseteq Z(G') \subseteq HT$. Hence by the Dedekind identity

$$Z(G') = HT \cap Z(G') = T(H \cap Z(G') = T,$$

a contradiction. So $\overline{H}$ must intersect trivially with $\overline{Z}$.

In order to establish the second half of our claim we need to regard $\overline{H}\,\overline{Z}/\overline{Z}$ as a subspace of $\overline{G'}/\overline{Z}$, a vector space of dimension n over $GF(r)$. Choose a basis

$$\{z_1, \ldots, z_{\ell_i}, q_1, \ldots, q_{n-d-\ell_i}\}$$

for $\overline{H}\,\overline{Z}/\overline{Z}$, where

$$\{z_1, \ldots, z_{\ell_i}\}$$

form a basis for $\overline{H}\,\overline{Z}/\overline{Z} \cap \overline{Z_i}/\overline{Z}$.

Let $\overline{Q_i}/\overline{Z}$ be a complementary subspace of $\overline{Z_i}/\overline{Z}$ in $\overline{G'}/\overline{Z}$, where $\overline{Q_i} = Q_i/T$ and $Z(G') \subseteq Q_i$ is extra-special, with a basis of the following form

$$\{q_1, \ldots, q_{n-d-\ell_i}, \ldots, q_{n-k_i}\}.$$

Then

$$\overline{H}\,\overline{Z}/\overline{Z} = (\overline{H}\,\overline{Z}/\overline{Z} \cap \overline{Q_i}/\overline{Z})(\overline{H}\,\overline{Z}/\overline{Z} \cap \overline{Z_i}/\overline{Z})$$

which implies that

$$\overline{H} \subseteq \overline{H}\,\overline{Z} = (\overline{H}\,\overline{Z} \cap \overline{Q_i})(\overline{H}\,\overline{Z} \cap \overline{Z_i}).$$

In consequence if $h \in \overline{H}$ then $h = qz$ for some $q \in \overline{Q_i}$, $z \in \overline{Z_i}$, where $q = h_q z_q$ and $z = h_z z_z$, $h_q, h_z \in \overline{H}$ and $z_q, z_z \in \overline{Z}$. Therefore $h = h_q z_q h_z z_z = q' h_z$, where $q' \in \overline{Q_i}$ and $h_z \in \overline{H} \cap \overline{Z_i}$.

Let $\overline{\overline{H}} = \overline{H}/(\overline{H} \cap \overline{Z_i})$, $\overline{\overline{Z}} = \overline{Z}(\overline{H} \cap \overline{Z_i})$ and $\overline{\overline{Q_i}} = \overline{Q_i}(\overline{H} \cap \overline{Z_i})/(\overline{H} \cap \overline{Z_i})$. Then from above

$$\overline{\overline{H}} \subseteq \overline{\overline{Q_i}}$$

and

$$\overline{\overline{Q_i}} \cong \overline{Q_i}/\overline{Q_i} \cap \overline{H} \cap \overline{Z_i}.$$

But $\overline{Q_i} \cap \overline{Z_i} = \overline{Z}$ and $\overline{H} \cap \overline{Z} = 1$. So

$$\overline{\overline{Q_i}} \cong \overline{Q_i}.$$

Furthermore, $\overline{\overline{H}} \cap \overline{\overline{Z}} = 1$ and

$$1_{\overline{\overline{H}}} \uparrow \overline{\overline{Q_i}}$$

is multiplicity-free. So by Lemma 1.4.6, $\overline{\overline{H}}\,\overline{\overline{Z}}$ is a maximal abelian normal subgroup of $\overline{\overline{Q_i}}$ and $\overline{\overline{H}}$ has order $r^{\frac{1}{2}(n-k_i)}$. Hence

$$|\overline{H}| = r^{\frac{1}{2}(n-k_i)+\ell_i}$$

and

$$r^{d+1} = |\overline{G'} : \overline{H}\,| = r^{(n+1)-(\frac{1}{2}(n-k_i)+\ell_i)} = r^{\frac{1}{2}n+\frac{1}{2}k_i-\ell_i+1},$$

because $\overline{H} \cap \overline{Z} = 1$. So

$$d = \frac{1}{2}n + \frac{1}{2}k_i - \ell i$$

as claimed.

Now if $H \cap \Phi(G') \subseteq T$, then $1_{\overline{H}} \uparrow \overline{G'}$ has degree r^{d+1} and the sum of the degrees of the non- linear irreducible constituents of $1_{\overline{H}} \uparrow \overline{G'}$ must equal $(r-1)r^d$, since $\overline{H} \cap \overline{Z} = 1$. Thus

$$(r-1)r^{k_i-\ell_i} = (r-1)r^{d-\frac{1}{2}(n-k_i)}$$

non-linear characters of $Irr(G'/T)$ are constituents of $1_H \uparrow G'$ and

$$|\{T \in \mathcal{S}_i : H \cap \Phi(G') \subseteq T\}| = \left(\frac{r^{k_i} - 1}{|M|} + 1\right) \Big/ r^{k_i - \ell_i}.$$

Suppose that $H \cap \Phi(G')$ has index r^x in $\Phi(G')$. Then $H \cap \Phi(G')$ is contained in

$$\frac{r^x - 1}{r - 1}$$

elements of $\mathcal{S}$ and we have

$$\frac{r^x - 1}{r - 1} = \sum_{i=1}^{\frac{r^m - 1}{r - 1} / \frac{|C|}{|M|}} \left(\frac{r^{k_i} - 1}{|M|} + 1\right) \Big/ r^{k_i - \ell_i}.$$

Suppose that $n = m$ and $k_i = 0$ for some i. Then $n = 2d$ and

$$\ell_i = \frac{1}{2} k_i$$

for all i. So $r = 2$ by Corolla ry 3.5.4 and

$$2^{\frac{1}{2}k_i} \,\Big|\, \frac{2^{k_i} - 1}{|M|} + 1$$

for all i. So by Lemma 5.2.2

$$|M| = 2^{\frac{1}{2}k_i} + 1$$

for all i satisfying $k_i > 0$ and all the non-zero k_i must be equal. Furthermore,

$$\left(\frac{2^{k_i} - 1}{|M|} + 1\right) \Big/ 2^{\frac{1}{2}k_i} = 1$$

for all i. So the equation

$$2^x - 1 = \sum_{i=1}^{2^n - 1 / \frac{|C|}{|M|}} \left(\frac{2^{k_i} - 1}{|M|} + 1\right) \Big/ 2^{k_i - \ell_i}.$$

reduces to

$$2^x - 1 = 2^n - 1 / \frac{|C|}{|M|}.$$

and we obtain

$$|M| = \frac{2^x - 1}{2^d - 1}.$$

In the case where k_i is greater than zero for some i. This implies that $x = n = k_i$, since $n = 2d$. But $n > k_i$ for all i. So if one of the k_i equals zero then all the k_i must equal zero contradicting Theorem 3.3.5.

So if $n = m$, then we may assume that all the $k_i > 0$. Let $o = o(r) \; mod \, |M|$. Then $o | k_i$ and there exists an o_i such that $k_i = o_i o$ for all i. Furthermore, if o is odd then

$$o_i - o_j \equiv 0 \; mod \, 2,$$

because $n - k_i$ is even for all i.

Let a be the largest integer satisfying

$$r^a \left| \frac{r^o - 1}{|M|} + 1. \right.$$

Then a is less than o and a is the largest integer satisfying

$$r^a \left| \frac{r^{k_i} - 1}{|M|} + 1 \right.$$

for all i, by Lemma 5.2.1. In particular, $a \geq k_i - \ell_i$ for all i and there exists a j such that

$$k_j - \ell_j = a,$$

because

$$\frac{r^x - 1}{r - 1}$$

is co-prime to r. Furthermore, if $o_i = (o_j \pm 2y)$, then

$$\ell_i = \frac{1}{2}k_i + \frac{1}{2}n - d = \frac{1}{2}o_j o \pm yo + \frac{1}{2}n - d = \ell_j \pm yo$$

and

$$k_i - \ell_i = o_i o - \ell_j \mp yo = o_j o \pm 2yo - \ell_j \mp yo = k_j - \ell_j \pm yo = a \pm yo.$$

But $0 \leq k_i - \ell_i \leq a < o$ for all i, so we may assume that all the k_i equal k_j, if o is odd.

If o is even, then $k_j - \ell_j \leq \frac{1}{2}o$ by Lemma 5.2.2 and consequently, if $m = n$ and all the $k_i > 0$, then we may assume that all the k_i are equal to k_j for some j. So

$$\frac{r^x - 1}{r - 1} = \left(\frac{r^n - 1}{r - 1} \Big/ \frac{|C|}{|M|}\right)\left(\frac{r^{k_j} - 1}{|M|} + 1\right) \Big/ r^{k_j - \ell_j}.$$

and re-arranging the equation we obtain

$$r^{k_j - \ell_j}\frac{r^x - 1}{r^d - 1} = \left(r^{k_j} - 1\right) + |M|,$$

and $d|x$. Furthermore, $d < x$, because $|M|$ is greater than 1. Expanding out the left hand side of this equation, we have

$$r^{x-d+k_j-\ell_j} + r^{x-2d+k_j-\ell_j} + \cdots + r^{d+k_j-\ell_j} + r^{k_j-\ell_j} = r^{k_j} - 1 + |M|.$$

But $|M|$ is greater than 1 and divides $r^{k_j} - 1$. So

$$r^{k_j} < r^{k_j} - 1 + |M| < r^{k_j+1}.$$

Furthermore,

$$r^{x-d+k_j-\ell_j} < r^{x-d+k_j-\ell_j} + r^{x-2d+k_j-\ell_j} + \cdots + r^{d+k_j-\ell_j} + r^{k_j-\ell_j} < r^{x-d+k_j-\ell_j+1}.$$

So $x - d + k_j - \ell_i = k_j$, forcing $x = d + \ell_j$. Thus

$$d | \ell_j,$$

since $d | x$. Hence

$$d | k_j,$$

because $d | n + k_j - 2\ell_j$ and $d | n$. So

$$d | k_j - \ell_j$$

and

$$\frac{1}{2}n - \frac{1}{2}k_j = d - k_j + \ell_j \leq 0,$$

contradicting the fact that $n > k_j$.

So we may assume without loss of generality that $m < n$ and consequently, by Theorem 1.2.5, either $n = 6$ and $r = 2$ or there exists a prime q dividing $|M|$ satisfying the following statements.

(a) q divides $r^n - 1$.

(b) q does not divide $r^i - 1$ whenever $0 < i < n$.

Assume that $n \neq 6$ or $r \neq 2$. Then $|M|$ acts irreducibly on $G'/\Phi(G')$ and consequently $k_i = 0$ for all i, which forces $n = 2d$. So r must equal 2 by

Corolla ry 3.5.4 and G'/T is an extra- special 2-group of order 2^{2d+1} for all $T \in \mathcal{S}$. Furthermore, there exists a $T \in \mathcal{S}$ such that

$$HT/T \cap \Phi(G')/T = 1.$$

So G'/T has an elementary abelian subgroup $HT/T \times \Phi(G')/T$ of order 2^{d+1}. Thus G'/T is a central product of d dihedral groups of order 8 with amalgamated centres by Theorem 1.4.2 and M can be viewed as a subgroup of $Aut(G'/T)$. In particular,

$$|M| = |MInn(G'/T)/Inn(G'/T)|$$

divides

$$|Aut(G'/T)/Inn(G'/T)|,$$

which in turn divides

$$2^{(2d(2d-2)/4)+1}(2^d - 1)\Pi_{i=1}^{d-1}(2^{2i} - 1),$$

by Theorem 1.4.4. But this contradicts our assumption that there exists a prime q dividing the order of M satisfying the statements above.

If $n = 6$, $r = 2$ and M acts irreducibly on $G'/\Phi(G')$. Then as above k_i must equal 0 for all i. So $d = 3$,

$$|M| = |C| = 9,$$

by Theorem 1.1.1, and $m = 1$. Thus G' is a central product of 3 dihedral groups of order 8 and M is isomorphic to a subgroup of

$$Aut(G')/Inn(G'),$$

which in turn is isomorphic to a subgroup of S_8. But this cannot not happen, because S_8 contains no element of order 9. The proof is complete. □

5.3 Example C

The following example of a finite group satisfying the conditions above can best be described using a construction of Higman in his paper on Suzuki 2- groups [8]. We shall digress for a moment in order to place the example within context and also because we will need to visit Higman's paper again in another context.

Suppose that $F = GF(2^n)$ and θ is an automorphism of F. We denote by $A(n, \theta)$ the set of all matrices of the form

$$u(a,b) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a\theta & 1 \end{pmatrix}$$

with $a, b \in F$. Then

$$u(a,b)u(a',b') = u(a+a', b+b'+a'(a\theta)),$$

and

$$u(a,b)^{-1} = u(a, b+a(a\theta)).$$

So $A(n,\theta)$ is a group of order 2^{2n} with unit element $u(0,0)$. The mapping $u(a,b) \to a$ is a homomorphism of $A(n,\theta)$ onto the additive group of F with kernel

$$\mathcal{R} = \{u(0,b)\,|b \in F\}.$$

Thus there is an isomorphism $\bar{\rho}$ of $A(n,\theta)/\mathcal{R}$ onto F such that

$$(u(a,b)\mathcal{R})\bar{\rho} = a.$$

Also there is an isomorphism $\bar{\sigma}$ of $\mathcal{R}$ onto F given by

$$u(0,b)\bar{\sigma} = b,$$

and

$$(u(a,b)^2)\bar{\sigma} = a(a\theta).$$

Note that $\mathcal{R} - \{1\}$ is the set of involutions in $A(n,\theta)$, and that $A(n,\theta)$ is abelian if and only if $\theta = 1$. Note also that if $\lambda \in F^\times$, there is an automorphism ξ_λ of $A(n,\theta)$ given by

$$u(a,b)\xi_\lambda = u(\lambda a, \lambda(\lambda\theta)b).$$

Theorem 5.3.1 *Let $F = GF(2^n)$, and let θ be an automorphism of F.*

(a) *The mapping $a \to a(a\theta)$ of F into F is injective if and only if θ is of odd order.*

(b) *If θ is of odd order, there exists $\lambda \in F$ such that the set of involutions of $A(n,\theta)$ is transitively permuted by $<\xi_\lambda>$.*

(c) *If θ is of even order, the set of involutions of $A(n,\theta)$ is intransitively permuted by the group of automorphisms of $A(n,\theta)$.*

Proof. Huppert and Blackburn [7, Theorem 6.9, page 296].

a) Put $a\chi = a(a\theta)$ $(a \in F^\times)$. Then χ is an endomorphism of $F^\times$. If $ker\chi \neq 1$, there exists $a \neq 1$ such that $a\theta = a^{-1}$, so the order of θ is even. If the order of θ is even, the subfield of elements fixed by θ^2 is different from the subfield F_1 of elements fixed by θ. Thus there exists $a \in F$ such that

$a\theta \neq a$, $a\theta^2 = a$. Then $a(a\theta) \in F_1^{\times}$, so, since $|F_1^{\times}|$ is odd, there exists $b \in F_1$ such that $b^2 = a(a\theta)$. Let $c = ab^{-1}$; $c \neq 1$ since $a \notin F_1$. Thus $c\theta = (a\theta)(b\theta)^{-1} = (a\theta)b^{-1} = ba^{-1}$, by definition of b. Hence $c\theta = c^{-1}$ and $\ker\chi \neq 1$.

b) Suppose that θ is of odd order. Let ω be a generator of $F^{\times}$. By a), there exists $\lambda \in F$ such that $\lambda(\lambda\theta) = \omega$. Then $u(0,b)\xi_\lambda = u(\lambda 0, \omega b)$, so ξ_λ has the stated property.

c) Suppose that θ is of even order. By a), χ is not injective and thus not surjective. Hence there exists $a \in F$ such that a is not of the form $b(b\theta)$ with $b \in F$; thus $a\bar{\sigma}^{-1}$ is an involution in $A(n,\theta)$ but is not a square. Since $A(n,\theta)$ is of exponent 4, some involutions are squares. The assertion follows at once. □

Definition 5.3.2 *A Suzuki 2-group is a group G which has the following properties.*

(a) *G is a non-abelian 2-group.*

(b) *G has more than one involution.*

(c) *There exists a soluble group of automorphisms of G which permutes the set of involutions in G transitively.*

Theorem 5.3.3 *Let G be a Suzuki 2-group.*

(a) $G' = \Phi(G) = Z(G) = \{x \,|\, x \in G, x^2 = 1\}$.

(b) *Either (i) $G \cong A(n,\theta)$ for some non-identity automorphism θ of $GF(2^n)$ of odd order, or (ii) $|G| = |Z(G)|^3$.*

Proof. Huppert and Blackburn [7, Theorem 7.9, page 313]. □

Let $F = GF(2^6)$, let θ be the automorphism of F of order 6 defined by

$$a^\theta = a^2$$

for all $a \in F$, and $F^\times = < \lambda >$. Let $\mu = \lambda^7$ and let

$$G = [A(6,\theta)]C$$

be the semi-direct product of $A(6,\theta)$, which is not a Suzuki 2-group by Theorem 5.3.3, and $C = < \xi_\mu >$, a cyclic group of order 9. Let

$$N = < u(0,\lambda^{24}), u(0,\lambda^3), u(0,\lambda^{43}), u(0,\lambda^{12}) > .$$

Then $(G/N)' = A(6,\theta)/N$, the Frattini subgroup $\Phi((G/N)') = \mathcal{R}/N$, and G/N satisfies the statements in Theorem 5.2.4 with $r = 2$, $n = 6$ and $m = 2$. Furthermore, if

$$H =< u(\lambda^{21},\lambda^{40}), u(\lambda^{12},\lambda^{20}), u(\lambda^{48},\lambda^{10}) >,$$

then HN/N is a model subgroup of G/N.

5.4 Case E

Theorem 5.4.1 *Let $G = G_1G_2$ be a finite group satisfying the following statements.*

(a) $G_i = G_i'C_i$;

(b) $(|G_i'|, |C_i|) = 1$;

(c) *G_i' is elementary abelian;*

(d) *$G_1'G_2'$ is a special r-group;*

(e) *$K = [G_1', G_2']$ is the unique minimal normal subgroup of G of order r^m;*

(f) *$G/K = G_1/K \times G_2/K$;*

(g) *G_i/K is a Frobenius group at C_iK/K with minimal Frobenius kernel G_i'/K of order r^{n_i}.*

Then either G does not admit a model subgroup or $r = 2$,

$$|C_i| = 2^{\frac{1}{2}n_i} + 1,$$

for $i = 1, 2$.

Proof. The proof follows along identical lines to that of Theorem 5.2.4 and consequently we shall only outline the key steps.

First note by Theorem 1.1.1, that we may assume without loss of generality that $M = C_G(K) \cap (C_1 \times C_2) = < (c_1^{s_1}, c_2^{s_2}) >$, where

$$s_i = \frac{|C_i|}{(|C_1|, |C_2|)},$$

for $i = 1, 2$ and $C_1 = < c_1 >$ and $C_2 = < c_2 >$ Furthermore, $m = lcm(n_1, n_2)$.

Suppose that H is a model subgroup of G. Then HK/K is a model subgroup of $G/K = G_1/K \times G_2/K$, by Theorem 2.3.2. So

$$HK/K = (HK/K \cap G_1/K) \times (HK/K \cap G_2/K),$$

and $HK/K \cap G_i/K$ is a model subgroup of G_i/K, by Theorem 2.4.2, a Frobenius group with Frobenius complement C_iK/K and abelian Frobenius kernel G_i'/K. Therefore Theorem 3.2.1 states that $C_i \cong C_iK/K$ is cyclic of odd order and

$$|G_i : G_i'| = |C_i| = \frac{r^{n_i}-1}{r^{d_i}-1},$$

for some d_i dividing n_i and the index of $HK/K \cap G_i/K$ in G_i'/K is r^{d_i} by Theorem 1.6.4.

Let $\mathcal{S}$ be the set of maximal subgroups of K. Let

$$\{T_1, \ldots, T_j\}$$

be a complete set of orbit representatives of $\mathcal{S}$ viewed as a $C_1 \times C_2$ set. Let

$$\mathcal{S}_1, \ldots, \mathcal{S}_j$$

be the $C_1 \times C_2$-orbit containing T_i and let

$$r^{k_i+1} = |Z(G_1'G_2'/T_i)|.$$

Then we obtain

$$S_i = \frac{|C_1 \times C_2|}{|M|}$$

and

$$d_1 + d_2 = \frac{1}{2}n_1 + \frac{1}{2}n_2 + \frac{1}{2}k_i - \ell i,$$

where

$$r^{\ell_i} = |HT/T \cap Z(G_1'G_2'/T)|,$$

for all $T \in \mathcal{S}_i$ satisfying $H \cap K \subseteq T$. Furthermore,

$$|\{T \in \mathcal{S}_i : H \cap K \subseteq T\}| = \left(\frac{r^{k_i}-1}{|M|} + 1\right) \Big/ r^{k_i-\ell_i}$$

and if $H \cap K$ has index r^x in K, then

$$\frac{r^x - 1}{r - 1} = \sum_{i=1}^{\frac{r^m-1}{r-1} / \frac{|C_1 \times C_2|}{|M|}} \left(\frac{r^{k_i} - 1}{|M|} + 1 \right) \Big/ r^{k_i - \ell_i}.$$

Suppose that $|M| = 1$. Then $m = n_1 n_2$ and we obtain

$$\frac{r^x - 1}{r - 1} = \sum_{i=1}^{\frac{r^{n_1 n_2}-1}{r-1} / |C_1 \times C_2|} r^{\ell_i}.$$

So $\ell_i = 0$ for some i, because $(r^x - 1)/(r - 1)$ is prime to r. But if $\ell_i = 0$, then $k_i = 0$, because

$$d_1 + d_2 \leq \frac{1}{2} n_1 + \frac{1}{2} n_2,$$

and we may assume without loss of generality that $n_i = 2d_i$ for $i = 1, 2$..

Suppose that $|M| \neq 1$ and $k_i = 0$ for some i. Then $n_i = 2d_i$ for $i = 1, 2$.

Suppose that all the $k_i > 0$ and equal. Then we obtain

$$\frac{r^x - 1}{r - 1} = \left(\frac{r^m - 1}{r - 1} \Big/ \frac{|C_1 \times C_2|}{|M|} \right) \left(\left(\frac{r^{k_i} - 1}{|M|} + 1 \right) \Big/ r^{k_i - \ell_i} \right)$$

and it can be shown that $n_i = 2d_i$ for $i = 1, 2$. The result now follows.

□

5.5 Example E

Definition 5.5.1 *Let G be a finite r-group and let $\mathcal{S}$ be the set of maximal subgroups of $Z(G)$. Then we say that G is* semi-extra-special *if G/T is extra-special for all $T \in \mathcal{S}$.*

Lemma 5.5.2 *Let G be a semi-extra-special r-group. Then G is special and if the order of $G/\Phi(G)$ is r^n, then n is even.*

Proof. Beisiegel [6, Lemma 1]. □

In the case where $p = 2$ the next result can be regarded as a Corollary of Theorem 3.3.5 as has already been stated in the introduction.

Theorem 5.5.3 *If G is a semi-extra-special r-group and $G/\Phi(G)$ has order r^{2n}, then $|\Phi(G)| \leq r^n$.*

Proof. Beisiegel [6, Satz 1]. Let $\{z_i \mid 1 \leq i \leq m\}$ be a basis of the group $G' = \Phi(G)$ regarded as a $GF(r)$ vector space. Then

$$[gG', hG'] = \sum_{i=1}^{m} f_i(gG', h'G')z_i,$$

where the f_i are symplectic scalar products of G/G' regarded as a $GF(r)$ vector space. Let A_i denote the matrix of f_i with respect to a fixed basis of G/G'. Since G is semi-extra-special, the scalar product.

$$\sum_{i=1}^{m} \lambda_i f_i$$

is not regular only if all the $\lambda_i = 0$. Thus the equation

$$0 = Det\left(\sum_{i=1}^{m} \lambda_i A_i\right)$$

has only the trivial solution. But the right side of this equation is the square of a homogeneous polynomial of degree n in the variables λ_i, $1 \leq i \leq m$ and consequently has non-trivial solutions, if the number of variables is greater than the degree of the polynomial by Chevalley's Theorem. The proof is complete. □

Definition 5.5.4 *If G is a semi-extra-special r-group, $G/\Phi(G)$ has order r^{2n} and $\Phi(G)$ has order r^n, then we say that G is* ultra-special.

Lemma 5.5.5 *Let r be a prime, let L be a field with r^n elements, let K be the prime subfield of L and define the following multiplication on the cartesian product $P = L^{(3)}$*

$$(a, b, c)(a', b', c') = (a + a', b + b', c + c' + f(a, b')),$$

where f is a K-bilinear map from $L \times L$ into L. Then

(a) *P is an r-group of class at most 2 with respect to this multiplication;*

(b) *P is ultra-special if and only if*

$$\{f(a, \ell) \mid \ell \in L\} = \{f(\ell, a) \mid \ell \in L\}$$

for all $0 \neq a \in L$.

Proof. Beisiegel [6, Lemma 3]. □

Let $F = GF(2^{2n})$, let $F^\times = < \lambda >$, and let $\mu = \lambda^{2^n - 1}$. Suppose that P is the set of matrices of the form

$$u(a, b, c) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ c & b & 1 \end{pmatrix}$$

with $a, b, c \in F$. Then

$$u(a, b, c)u(a', b', c') = u(a + a', b + b', c + c' + a'b),$$

and setting $f(a, b') = ab'$ in Lemma 5.5.5 we see that P is an ultra- special 2 group. Let α be the map from P to P defined by

$$u(a, b, c)\alpha = u(\mu a, b, \mu c)$$

and let β be the map from P to P defined by

$$u(a, b, c)\beta = u(a, \mu^{-1}b, \mu^{-1}c)$$

for all $a, b, c \in F$. Then $\alpha, \beta \in Aut(P)$ and

$$\alpha\beta = \beta\alpha.$$

Furthermore, if $C_1 =< \alpha >$ and $C_2 =< \beta >$, then

$$C =< \alpha, \beta >= C_1 \times C_2,$$

since $C_1 \cap C_2 = 1$. Let

$$G = [P](C_1 \times C_2)$$

be the semi-direct product of P and $C_1 \times C_2$. Let

$$P_1 = \{u(a, 0, c) \mid a, c \in F\},$$

and let

$$G_1 = [P_1]C_1 \subseteq G.$$

Let

$$P_2 = \{u(0, b, c) \mid b, c \in F\},$$

and let

$$G_2 = [P_2]C_2 \subseteq G.$$

Then $G_i' = P_i$ for $i = 1, 2$ and

$$K = \{u(0,0,c) \mid c \in F\} = [G_1', G_2']$$

is the unique minimal normal subgroup of G. Furthermore, $G = G_1G_2$ satisfies the statements in Theorem 5.4.1 with $r = 2$,

$$|C_i| = 2^n + 1,$$

and $m = n_1 = n_2 = 2n$. Now suppose that $J = GF(2^n)$ and

$$H = \{u(d,e,f) \mid d,e,f \in J\}.$$

Then H is a model subgroup of G.

5.6 Case F

We now look at minimal non-$\mathcal{X}$-groups satisfying

$$(|G : G'|, |G' : G''|) = 1$$

and the conditions outlined in Case F. Before moving onto the main result we will prove a well-known result of Burnside and then look at a restricted case which introduces the techniques in this section as well as highlighting a very near miss.

Theorem 5.6.1 *Let X be a G-set and let t be the number of orbits of G on X. Suppose that*

$$F(g) = \{x \in X \mid xg = x\}$$

for all $g \in G$. Then

$$t|G| = \sum_{g \in G} |F(g)|.$$

Proof. Let $E = \{(x, g) \in X \times G \mid xg = g\}$. Then

$$|E(x, .)| = |G_x| \text{ and } |E(., g)| = |F(g)|.$$

Applying the counting principle

$$\begin{aligned} \sum_{g \in G} |F(g)| &= \sum_{x \in X} |G_x| \\ &= \sum_{i=1}^{t} \sum_{x \in x_i G} |G_x| \end{aligned}$$

where $x_1, \ldots, x_t$ are representatives of the the t orbits. But if $x \in x_i G$, then $G_{x_i} = g^{-1} G_x g$ where $xg = x_i$, so that $|G_{x_i}| = |G_x|$. Thus

$$\begin{aligned} \sum_{g \in G} |F(g)| &= \sum_{i=1}^{t} |x_i G||G_x| \\ &= t|G| \end{aligned}$$

and the proof is complete. □

Theorem 5.6.2 *Let G be a finite soluble group satisfying the following conditions.*

(a) $G = G''X$;

(b) $G'' \cap X = 1$;

(c) *G'' is the unique minimal normal subgroup of G;*

(d) *$X = NC$ is a Frobenius group with cyclic Frobenius complement $C = < c >$ of order p and minimal Frobenius kernel N of order $p + 1$, where $p = 2^m - 1$ is a prime.*

Then G does not possess a model subgroup.

Proof. Let V denote G'' regarded as a faithful irreducible $\mathbb{F}_q[X]$-module and let W be a $\mathbb{F}_q[N]$-submodule of V. Then

$$V = \sum_{x \in X} Wx$$

and $C_N(W) < N$, because $C_X(V) = 1$. Furthermore, the abelian group $N/C_N(W)$ is cyclic of order 2, q is odd, the submodule $W \cong \mathbb{F}_q$, and $wn = (q-1)w$ for all $n \in N - C_N(W)$ and $w \in W$ by Theorem 1.1.1. So $C_N(W) = M$, where M is a maximal subgroup of N and $C_N(Wx) = M^x$ for all $x \in X$. But $Wn = W$ for all $n \in N$ and $Wc^i \ncong Wc^j$ for $i \neq j \in \{0, \ldots, p-1\}$, since C acts regularly on the set of maximal subgroups of N. So, by Clifford's Theorem [1, Theorem 6.5, page 80],

$$V = \bigoplus_{i=0}^{p-1} Wc^i.$$

In other words V is the induced $\mathbb{F}_q[X]$-module W^X of dimension p. Furthermore, if $x \in X - N$ and $w \in W - \{0\}$, then the set

$$\{w, wx, \ldots, wx^{p-1}\}$$

is a basis for V over $\mathbb{F}_q$. So if $x \in X - N$ and $w \in W - \{0\}$, then

$$C_V(x) = < w + wx + wx^2 + \cdots + wx^{p-1} >$$

and

$$|C_{G''}(x)| = |C_V(x)| = q.$$

If $1 \neq n \in N$, then $(wc^i)n = wc^i$ if $n \in M^{c^i}$ and $(wc^i)n = (q-1)wc^i$ if $n \notin M^{c^i}$ for all $i \in \{0, \ldots, p-1\}$ and $w \in W$. So, if $1 \neq n \in N$, then

$$C_V(n) = < xc^i \mid n \in M^{c^i} >$$

and

$$|C_{G''}(n)| = |C_V(n)| = q^{2^{m-1}-1} = q^{(p-1)/2}.$$

Let t denote the number of orbits of $Irr(G'')$ viewed as an X-set. Then, remembering that G'' is abelian, we obtain

$$t = \frac{q^p + pq^{(p-1)/2} + (p-1)(p+1)q}{(p+1)p},$$

by Theorem 5.6.1 and Theorem 1.6.2.

Now since X is a Frobenius group with cyclic Frobenius complement of order p and minimal Frobenius kernel of order $p+1$, where $p = 2^m - 1$ is a prime, a proper subgroup of X is either cyclic of order p or is elementary abelian of order 2^ℓ, where $\ell \leq m$.

Let $1_{G''} \neq \lambda \in Irr(G'')$. Then $I_X(\lambda)$ is a proper subgroup of X, and is as a consquence either cyclic of order p or elementary abelian of order 2^ℓ, where $\ell \leq m$. If $I_X(\lambda)$ is cyclic of prime order p, then λ extends to $I_X(\lambda)$ by Isaacs [1, Corollary 6.20, page 86] and if $I_X(\lambda)$ is elementary abelian of order 2^ℓ, then the linear character λ, whose order is q, extends to $I_X(\lambda)$ by Isaacs [1, Theorem 6.26, page 89]. So

$$\lambda \uparrow^G = \chi_1 + \cdots + \chi_k,$$

where $k = |I_X(\lambda)|$ and χ_i is irreducible of degree $|X : I_X(\lambda)|$ for all i, by Isaacs [1, Theorem 6.11 and Theorem 6.17, page 82 and 85]. Let

$$1_{G''} = \lambda_1, \lambda_2, \ldots, \lambda_t$$

be a set of orbit representatives of $Irr(G'')$ viewed as an X-set and let

$$\mathcal{S}_i = \{\chi \in Irr(G) \mid < \chi_{G''}, \lambda_i > \neq 0\},$$

for $i \in \{1, \ldots, t\}$. Then

$$Irr(G) = \mathcal{S}_1 \dot{\cup} \cdots \dot{\cup} \mathcal{S}_t$$

by Isaacs [1, Theorem 6.2, page 79]. Now

$$\sum_{\chi \in \mathcal{S}_i} \chi(1) = |X| = p(p+1)$$

for $i \in \{2, \ldots, t\}$ and

$$\sum_{\chi \in \mathcal{S}_1} \chi(1) = 2p$$

by Theorem 1.6.4, because $\mathcal{S}_1 = Irr(G/G'')$ by Isaacs [1, Theorem 6.17, page 85]. Thus

$$\sum_{\chi \in Irr(G)} \chi(1) = 2p + p(p+1)(t-1)$$

and substituting in the value above for t, we obtain

$$\begin{aligned}\sum_{\chi\in Irr(G)} \chi(1) &= 2p + p(p+1)\left[\frac{q^p + pq^{(p-1)/2} + (p-1)(p+1)q}{(p+1)p} - 1\right] \\ &= 2p + q^p + pq^{(p-1)/2} + (p-1)(p+1)q - (p+1)p.\end{aligned}$$

Now suppose that H is a model subgroup of G. Then HG''/G'' is a model subgroup of G/G'' by Theorem 2.3.2 and

$$\left|\frac{H}{H\cap G''}\right| = \left|\frac{HG''}{G''}\right| = 2^{m-1},$$

since

$$\sum_{\chi\in Irr(G/G'')} \chi(1) = 2p$$

by Theorem 1.6.4. So there exists an $\ell > 0$ such that

$$|H| = 2^{m-1}q^{p-\ell},$$

where the order of $H\cap G''$ is $q^{p-\ell}$, and

$$\begin{aligned}2pq^{\ell} &= \sum_{\chi\in Irr(G)} \chi(1) \\ &= 2p + q^p + pq^{(p-1)/2} + (p-1)(p+1)q - (p+1)p.\end{aligned}$$

Re-arranging the equation we obtain

$$2pq^{\ell} = q^p + pq^{(p-1)/2} + (p-1)(p+1)q - (p-1)p.$$

So either $p = q$ or q divides $(p-1)$.

If q divides $(p-1)$, then there exists an $a \geq 1$ such that q^a divides $(p-1)$, but q^{a+1} does not. Now

$$q^{(p-1)/2} > 2^{(p-1)/2} = 2^u \geq 2u = (p-1),$$

where $p = 2u + 1$. So $(p-1)/2 > a$ and consequently a must equal ℓ. So

$$2pq^{\ell} = 2pq^{a} < 2p(p-1) < 2p^2.$$

But

$$2pq^{\ell} > (p-1)(p+1)q - (p-1)p = p^2(q-1) - q + p > 2p^2$$

and we may assume without loss of generality that $p = q$.

If $p = q$, then

$$\begin{aligned} 2p^{\ell+1} &= p^p + p^{(p+1)/2} + (p-1)(p+1)p - (p-1)p \\ &= p^p + p^{(p+1)/2} + p^3 - p - p^2 + p \\ &= p^p + p^{(p+1)/2} + p^3 - p^2. \end{aligned}$$

Clearly, ℓ must be greater than or equal to $p - 1$. Furthermore, if $p > 3$, then the largest power of p dividing the right-hand side is 2 and consequently the equality cannot hold. So we may assume without loss of generality that $p = q = 3$.

If $p = q = 3$, then

$$2 \times 3^{\ell+1} = 27 + 9 + 27 - 9 = 54$$

and ℓ must equal 2. So $X \cong A_4$, the unique minimal normal subgroup G'' has order 27, and the model subgroup H has order 6. Furthermore, G has three linear characters $\lambda_1, \lambda_2, \lambda_3$, one irreducible character μ of degree 3, six irreducible characters $\theta_1, \ldots, \theta_6$ of degree 4, two irreducible characters ϕ_1, ϕ_2 of degree six and one irreducible character χ of degree 12. In addition if J is any subgroup of $G''N$ of order 6, then

$$1_J \uparrow^G = \lambda_1 + \lambda_2 + \lambda_3 + \mu + 2\phi_1 + 2\phi_2 + 2\chi$$

or

$$1_J \uparrow^G = \lambda_1 + \lambda_2 + \lambda_3 + \mu + 1\phi_1 + 3\phi_2 + 2\chi$$

or

$$1_J \uparrow^G = \lambda_1 + \lambda_2 + \lambda_3 + \mu + \theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5 + \theta_6 + 2\phi_2 + \chi.$$

The result now follows, because H must be contained in $G''N$ by Corolla ry 2.3.3. □

Lemma 5.6.3 *Let $G = NC$, where G is a Frobenius group with elementary abelian Frobenius kernel N of order r^n and cyclic Frobenius complement C of order z. Let S be a maximal subgroup of N and let*

$$k(x) = |\{c \in C : x \in S^c\}|$$

for all $x \in N$. Suppose that $z = \frac{r^n-1}{r^d-1}$ for some d dividing n and $(z, r-1) = 1$. Then either $n = 2d$ or

$$\frac{(r-1)z}{r^2} \leq k(x) \leq \frac{(r+1)z}{r^2}$$

for all $1 \neq x \in N$.

Proof. Suppose that $C = \langle c \rangle$. Then N can be viewed as an $\mathbb{F}_r[C]$-module via the C-action

$$xc^i = x^{c^i},$$

for all $x \in N$ and $0 \leq i \leq z-1$. Since each element of C acts fixed-point freely on N via conjugation by Lemma 1.7.1, the C-action is faithful and we can apply Theorem 1.1.1 to an irreducible submodule M of N. Thus there exists a primitive zth root of unity ϵ of $F = \mathbb{F}_{r^n}$, by Lemma 3.4.10, such that M is isomorphic to F viewed as an $\mathbb{F}_r[C]$-module via the C-action

$$xc^i = x\epsilon^i \text{ (field multiplication)}$$

for all $x \in F$ and $0 \leq i \leq z - 1$. Since M is isomorphic to F viewed as an $\mathbb{F}_r[C]$-module, M must equal N and we can assume without loss of generality that

$$G = [N]\langle\epsilon\rangle,$$

the external semi-direct product of $N = F^+$ and $\langle\epsilon\rangle$ via σ, where σ is the homomorphism from $\langle\epsilon\rangle$ to $Aut(N)$ defined by

$$x^{\sigma(\epsilon^i)} = x\epsilon^i \text{ (field multiplication)}$$

for all $x \in N$ and $0 \leq i \leq z - 1$.

Let $R = \mathbb{F}_r$ be the prime subfield of F and let $R^\times = < \mu >$. Suppose that

$$\bar{G} = [N]\,(< \epsilon > \times < \mu >),$$

the external semi-direct product of N and $< \epsilon > \times < \mu >$ via τ, where τ is the homomorphism from $< \epsilon > \times < \mu >$ to $Aut(N)$ defined by

$$x^{\tau(\epsilon^i \mu^j)} = x\epsilon^i\mu^j \text{ (field multiplication)}$$

for all $x \in N$ and $0 \leq i \leq z - 1$, $0 \leq j \leq r - 1$. Then

$$k(x) = |\{i \in \{0, \ldots, z-1\} : x \in S^{\epsilon^i}\}|$$

for all $x \in N$. For $y \in N$, let χ_y denote the linear character of N defined by

$$\chi_y(x) = e^{2\pi i Tr_F(yx)/r}$$

for all $x \in N$. Then by Theorem 3.4.4 there exists a $0 \neq y \in N$ such that the kernel of the linear character χ_y is S. Furthermore,

$$Tr_F(y\mu^j x) = \mu^j Tr_F(yx),$$

for all $x \in N$ and all $0 \leq j \leq r-1$, by Theorem 3.4.2. So

$$\chi_y, \chi_{y\mu}, \dots, \chi_{y\mu^{r-1}}$$

are the non-trivial characters of $Irr(N)$ whose kernels contain S. Hence

$$\sum_{j=0}^{r-1} \chi_{y\mu^j}(x) = r-1,$$

if $x \in S$, and

$$\sum_{j=0}^{r-1} \chi_{y\mu^j}(x) = -1,$$

if $x \notin S$. Now applying Theorem 3.4.6 we see that $\chi_y^{\tilde{G}}$ is an irreducible character of $\tilde{G}$,

$$\chi_y^{\tilde{G}}(x) = \sum_{i=0}^{z-1}\sum_{j=0}^{r-1} \chi_{y\epsilon^{-i}\mu^j}(x)$$

for all $x \in N$ and $\chi_y^{\tilde{G}}$ vanishes outside N. Thus

$$\begin{aligned} \chi_y^{\tilde{G}}(x) &= \sum_{i=0}^{z-1}\sum_{j=0}^{r-1} \chi_{y\mu^j}(x^{\epsilon^{-i}}) \\ &= (r-1)k(x) - (z-k(x)) \\ &= rk(x) - z, \end{aligned}$$

and

$$(r-1)zr^n = |\tilde{G}| = \sum_{\tilde{g}\in\tilde{G}} \chi_y^{\tilde{G}}(\tilde{g})^2 = (r-1)^2z^2 + \sum_{0\neq x\in N} \chi_y^{\tilde{G}}(x)^2.$$

Suppose that there exists a $0 \neq x \in N$ such that

$$|\chi_y^{\tilde{G}}(x)| > \frac{z}{r}.$$

Then

$$(r-1)zr^n > (r-1)^2z^2 + z(r-1)\left(\frac{z}{r}\right)^2,$$

from above and because every non-zero element of N is contained in a conjugacy class of length $z(r-1)$. So

$$r^n > (r-1)z + \left(\frac{z}{r}\right)^2.$$

But $r^n = z(r^d - 1) + 1$, so

$$\begin{aligned} z(r^d-1)+1 &> (r-1)z + \left(\frac{z}{r}\right)^2 \\ z(r^d-1) &\geq (r-1)z + \left(\frac{z}{r}\right)^2, \end{aligned}$$

and after re-arranging the equation we obtain

$$r^{d+2} - r^3 \geq z = r^{(\ell-1)d} + r^{(\ell-2)d} + \cdots + r^d + 1,$$

where $\ell = n/d$. It is straightforward to show that this equality holds only if $\ell = 2$. Thus if there exists a $0 \neq x \in N$ such that

$$|\chi_y^{\tilde{G}}(x)| > \frac{z}{r},$$

then n must equal $2d$. So if $n \neq 2d$, then

$$|rk(x) - z| \leq \frac{z}{r}$$

for all $0 \neq x \in N$. Re-stating this as the two inequalities

$$\begin{aligned} rk(x) - z &\leq \frac{z}{r} \text{ and} \\ z - rk(x) &\leq \frac{z}{r} \end{aligned}$$

and solving for $k(x)$ we obtain the desired inequality

$$\frac{(r-1)z}{r^2} \leq k(x) \leq \frac{(r+1)z}{r^2}.$$

The proof is complete. □

Lemma 5.6.4 *Let r be a prime. Let $G = G_1 \times \cdots \times G_m$, where each G_i is a Frobenius group with elementary abelian Frobenius kernel N_i of order r^{n_i} and cyclic Frobenius complement C_i of order z_i. Let S be a maximal subgroup of*

$$N = N_1 \times \cdots \times N_m$$

and let

$$k(x) = |\{c \in C : x \in S^c\}|.$$

for all $x \in N$, where $C = C_1 \times \cdots \times C_m$. Suppose that $z_i = \frac{r^{n_i}-1}{r^{d_i}-1}$ for some d_i dividing n_i and $(z_i, r-1) = 1$ for $1 \leq i \leq m$. Suppose further that $S \cap N_i < N_i$ for all $1 \leq i \leq m$. Then either $n_i = 2d_i$ for some i or

$$\frac{(r-1)z}{r^2} \leq k(x) \leq \frac{(r+1)z}{r^2}$$

for all $1 \neq x \in N$, where $z = \Pi_{i=1}^m z_i$.

Proof. We shall prove the result by induction on m. We have already shown in Lemma 5.6.3 that the result holds in the case when $m = 1$. So in order to complete the proof we need only show that the result holds for m if we assume that it holds for $m - 1$.

Let $\hat{G}_i = G_1 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_m$ and, let $\hat{N}_i$ and $\hat{C}_i$ denote the corresponding subgroups of N and C. Let

$$k_i(\hat{x}_i) = |\{\hat{c}_i \in \hat{C}_i : \hat{x}_i \in (S \cap \hat{N}_i)^{\hat{c}_i}\}|$$

for all $\hat{n}_i \in \hat{N}_i$. Then since

$$(S \cap \hat{N}_i)^{c_i} = S \cap \hat{N}_i$$

for all $c_i \in C_i$, we see that

$$k(\hat{x}_i) = z_i k_i(\hat{x}_i)$$

for all $\hat{x}_i \in \hat{N}_i$ and by our induction hypothesis either $n_j = 2d_j$ for some $j \neq i$ or

$$\frac{(r-1)z}{r^2 z_i} \leq k_i(\hat{x}_i) \leq \frac{(r+1)z}{r^2 z_i}$$

for all $1 \neq \hat{x}_i \in \hat{N}_i$ and

$$\frac{(r-1)z}{r^2} \leq k(\hat{x}_i) \leq \frac{(r+1)z}{r^2}$$

for all $1 \neq \hat{n}_i \in \hat{N}_i$. So if we can show that either $n_i = 2d_i$ for some i or

$$\frac{(r-1)z}{r^2} \leq k((x_1, \ldots, x_m)) \leq \frac{(r+1)z}{r^2},$$

for all $(x_1, \ldots, x_m) \in N$ satisfying $x_i \neq 1$ for all i the proof will be complete.

As in Lemma 5.6.3 we can assume without loss of generality that there exists a primitive z_ith root of unity ϵ_i of $F_i = \mathbb{F}_{r^{n_i}}$ such that

$$G_i = [F_i^+]\langle\epsilon_i\rangle,$$

the external semi-direct product of F_i^+ and $\langle\epsilon_i\rangle$ via σ_i, where σ_i is the homomorphism from $\langle\epsilon_i\rangle$ to $Aut(F_i^+)$ defined by

$$x_i^{\sigma_i(\epsilon_i^{j_i})} = x_i\epsilon_i^{j_i} \quad \text{(field multiplication)}$$

for all $x_i \in F_i^+$ and $0 \leq j_i \leq z_i - 1$. Let $R = \mathbb{F}_r$ and let $R^\times = < \mu >$. Suppose that

$$\bar{G} = [N]\bar{C}$$

the external semi-direct product of $N = F_1^+ \times \cdots \times F_m^+$ and

$$\bar{C} = < \epsilon_1 > \times \cdots \times \ < \epsilon_m > \times \ < \mu >$$

via $\bar{\sigma}$, where $\bar{\sigma}$ is the homomorphism from $\bar{C}$ to $Aut(N)$ defined by

$$(x_1, \ldots, x_m)^{\bar{\sigma}((\epsilon_1^{j_1}, \ldots, \epsilon_m^{j_m}, \mu^k))} = (x_1\epsilon_1^{j_1}\mu^k, \ldots, x_m\epsilon_m^{j_m}\mu^k)$$

for all $(x_1, \ldots, x_m) \in N$ and $0 \leq j_i \leq z_i - 1$ and $0 \leq k \leq r - 1$. Then

$$k(x) = |\{(j_1, \ldots, j_m) \in J : x \in S^{(\epsilon^{j_1}, \ldots, \epsilon^{j_m}, 1)}\}|$$

for all $x \in N$, where

$$J = \{(j_1, \ldots, j_m) : 0 \leq j_i \leq z_i - 1, 1 \leq i \leq m\}.$$

Let $\chi_{(x_1, \ldots, x_m)} = \chi_{x_1} \cdots \chi_{x_m}$, where χ_{x_i} denotes the linear character of F_i^+ defined by

$$\chi_{x_i}(x) = e^{2\pi i Tr_F(x_i x)/r}$$

for all $x \in F_i^+$. Then as in Lemma 5.6.3 there exists a $y = (y_1, \ldots, y_m) \in F^+$ with $y_i \neq 0$ for all i such that

$$\chi_{(y_1,\ldots,y_m)}, \chi_{(y_1\mu,\ldots,y_m\mu)}, \ldots, \chi_{(y_1\mu^{r-1},\ldots,y_m\mu^{r-1})}$$

are the non-trivial characters of N whose kernels contain S. Hence

$$\sum_{k=0}^{r-1} \chi_{(y_1\mu^k,\ldots,y_m\mu^k)}((x_1, \ldots, x_m)) = r - 1,$$

if $(x_1, \ldots, x_m) \in S$, and

$$\sum_{k=0}^{r-1} \chi_{(y_1\mu^k,\ldots,y_m\mu^k)}((x_1, \ldots, x_m)) = -1,$$

if $(x_1, \ldots, x_m) \notin S$. Furthermore, by Theorem 3.4.6, $\chi^{\bar{G}}_{(y_1,\ldots,y_m)}$ is an irreducible character of $\bar{G}$,

$$\chi^{\bar{G}}_{(y_1,\ldots,y_m)}((x_1, \ldots, x_m)) = \sum_{j_1=0}^{z_1-1} \cdots \sum_{j_m=0}^{z_m-1} \sum_{k=0}^{r-1} \chi_{(y_1\epsilon^{-j_1}\mu^k,\ldots,y_m\epsilon^{-j_m}\mu^k)}((x_1, \ldots, x_m))$$

for all $(x_1, \ldots, x_m) \in N$ and $\chi^{\bar{G}}_{(y_1,\ldots,y_m)}$ vanishes outside N. Thus

$$\begin{aligned} \chi^{\bar{G}}_{(y_1,\ldots,y_m)}((x_1, \ldots, x_m)) &= \sum_{j_1=0}^{z_1-1} \cdots \sum_{j_m=0}^{z_m-1} \sum_{k=0}^{r-1} \chi_{(y_1\mu^k,\ldots,y_m\mu^k)}((x_1^{\epsilon^{-j_1}}, \ldots, x_m^{\epsilon^{-j_m}})) \\ &= (r-1)k((x_1, \ldots, x_m)) - (z - k((x_1, \ldots, x_m))) \\ &= rk((x_1, \ldots, x_m)) - z, \end{aligned}$$

and

$$\begin{aligned} (r-1)z\Pi_{i=1}^{m} r^{n_i} &= \sum_{\bar{g} \in \bar{G}} \chi_y^{\bar{G}}(\bar{g})^2 \\ &= \sum_{x \in N} \chi_y^{\bar{G}}(x)^2. \end{aligned}$$

Suppose that there exists a $x = (x_1, \ldots, x_m) \in N$ such that $x_i \neq 0$ for all i and

$$|\chi_y^{\hat{G}}(x)| > \frac{z}{r}.$$

Then

$$(r-1)z\Pi_{i=1}^m r^{n_i} > z(r-1)\left(\frac{z}{r}\right)^2,$$

from above and because x is contained in a conjugacy class of length $z(r-1)$. So

$$\Pi_{i=1}^m r^{n_i} > \left(\frac{z}{r}\right)^2.$$

But $r^{n_i} = z_i(r^{d_i} - 1) + 1$, so

$$\begin{aligned} \Pi_{i=1}^m z_i(r^{d_i} - 1) + 1 &> \left(\frac{z}{r}\right)^2 \\ \Pi_{i=1}^m r^{d_i} - 1 &\geq \frac{\Pi_{i=1}^m z_i}{r^2}, \end{aligned}$$

But $m > 1$ and $z_i \geq r^{2d_i} + r^{d_i} + 1 > r^{d_i+1} - r$ unless $n_i = 2d_i$.

So if $x = (x_1, \ldots, x_m) \in N$ such that $x_i \neq 0$ for all i and

$$|\chi_y^{\hat{G}}(n)| > \frac{z}{r},$$

then $n_i = 2d_i$ for some i. Therefore if $n_i \neq 2d_i$, then

$$|rk(x) - z| \leq \frac{z}{r}$$

and solving for $k(x)$ we obtain the desired inequality

$$\frac{(r-1)z}{r^2} \leq k(x) \leq \frac{(r+1)z}{r^2}.$$

□

Theorem 5.6.5 *Let $G = KX$ be a finite soluble group satisfying the following conditions.*

(a) $K \cap X = 1$;

(b) $K = G''$ *is the unique minimal normal subgroup of* G;

(c) X *is a non-abelian* $\mathcal{X}$*-group;*

(d) $X \subsetneq Aut(G'')$.

(e) $(|X'|, |X : X'|) = 1$.

Then either G does not possess a model subgroup or G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius kernel of order $2^n + 1$.

Proof. Since X is a $\mathcal{X}$-group, $X = X_1 \cdots X_m A$, where A is abelian, $[X_i, X_j] = 1$ for $i \neq j$ and $[X_i, A] = 1$ for all i. Furthermore, $N_i = X_i'$ is complemented in X_i for all i, and if C_i is a complement of N_i in X_i, then $Z_i = Z(X_i) = C_{C_i}(N_i)$ and X_i/Z_i is a Frobenius group with cyclic Frobenius complement C_i/Z_i and elementary abelian Frobenius kernel N_iZ_i/Z_i of order $r_i^{n_i}$.

Suppose that H is a model subgroup of G. Then C_i/Z_i has order

$$z_i = \frac{r_i^{n_i} - 1}{r_i^{d_i} - 1},$$

for some d_i dividing n_i and $(z_i, r_i - 1) = 1$, by Theorem 2.5.2, Theorem 2.5.3 and Corolla ry 3.5.6. Let $x_i = r^{n_i}$ and $y_i = r^{d_i}$.

Furthemore, if we let $x = \Pi_{i=1}^m x_i$, let $y = \Pi_{i=1}^m y_i$, and let $z = \Pi_{i=1}^m z_i$, then

$$\sum_{\chi \in Irr(G)} \chi(1) = |G : H| = \frac{|G|}{|HK/K||H \cap K|} = cyzq^h,$$

where $q^h = |K|/|H \cap K|$ and $c = |Z(X)|$, by Theorem 2.3.2, Theorem 2.4.2, Lemma 2.6.1.

Let $\pi = \{p_1, \ldots, p_t\}$ be the set of primes dividing the order of

$$N = X' = N_1 \times \cdots \times N_m,$$

and let

$$\mathcal{S}_{p_s} = \{i \in \{1, \ldots, m\} : |N_i| = p_s^a\}$$

for $1 \leq s \leq t$. Then

$$\{1, \ldots, m\} = \dot{\bigcup_{1 \leq s \leq t}} \mathcal{S}_{p_s}.$$

and $X = X_{p_1} \ldots X_{p_t} A$, where

$$X_{p_s} = \mathop{\mathsf{Y}}_{j \in \mathcal{S}_{p_s}} X_j.$$

Let N_{p_s} and C_{p_s} denote the corresponding subgroups of X_{p_s}. Now since $(|X|, |X : X'|) = 1$, the subgroup N_{p_s} is the p_s-Sylow subgroup of $NZ(X)$ and

$$NZ(X) = N_{p_1} \times \cdots \times N_{p_s} \times Z(X).$$

Let V denote $Irr(K)$ regarded as a faithful irreducible $\mathbb{F}_q[X]$-module and let W be a $\mathbb{F}_q[NZ(X)]$- submodule of V. Then

$$V = \sum_{x \in X} Wx$$

and $C_{N_i}(W) < N_i$ for all i and $C_{Z(X)}(W) = 1$, because $C_X(V) = 1$. Furthermore, the abelian group $NZ(X)/C_{NZ(X)}(W)$ is cyclic of order $p_1 \times \cdots \times p_t \times c$ and the submodule W has dimension q^b, where

$$b = o(q) \bmod p_1 \times \cdots \times p_t \times c$$

by Theorem 1.1.1. So $M = C_{NZ(X)}(W) = M_{p_1} \times \cdots \times M_{p_t}$, where M_{p_s} is a maximal subgroup of N_{p_s} satisfying $M_{p_s} \cap N_j < N_j$ for all $j \in \mathcal{S}_{p_s}$.

Let $\overline{X} = X/NZ$ and $\overline{C}_i = C_i NZ(X)/NZ(X)$. Then Suppose that $M^{\overline{c}} = M^c = C_{NZ(X)}(Wc)$ is equal to M for some

$$1 \neq \overline{c} \in \overline{X} = \overline{C}_1 \times \cdots \times \overline{C}_m.$$

Then there exists an i such that $\overline{c} = \overline{c}_i \hat{\overline{c}}_i$, where $1 \neq \overline{c}_i \in \overline{C}_i$ and

$$\hat{\overline{c}}_i \in \overline{C}_1 \times \cdots \times \overline{C}_{i-1} \times \overline{C}_{i+1} \times \cdots \times \overline{C}_m.$$

Thus

$$(M \cap N_i)^{\overline{c}_i} = (M \cap N_i)^{\overline{c}_i \hat{\overline{c}}_i} = (M \cap N_i)^{\overline{c}} = M^c \cap N_i = M \cap N_i.$$

So $\overline{c}_i$ acts fixed-point freely on $N_i/(M \cap N_i)$ by Lemma 1.7.4, since it acts fixed-point-freely on N_i and $o(\overline{c}_i)$ must divide $r - 1$ by Lemma 1.7.1 and Lemma 1.5.1. But $(z_i, r-1) = 1$, so $M^c = M$ if and only if $c \in NZ(X)$. Hence $Wc \cong Wc'$ if and only if $c' = cnz$ for $n \in N$ and $z \in Z(X)$. and by Clifford's Theorem [1, Theorem 6.5, page 80],

$$V = \bigoplus_{\ell \in L} W\ell,$$

where L is a transversal for $NZ(X)$ in X. In other words V is the induced $\mathbb{F}_q[X]$-module W^X of dimension zb.

Suppose that $x \in X - NZ(X)$ and $o(xNZ(X)) = u$. Let $W_1, \ldots, W_f$ be a set of orbit representatives of the $<x>$-set

$$\{W\ell : \ell \in L\}$$

and let the set $\{w_{i1}, \ldots, w_{ib}\}$ be a basis of W_i for $1 \leq i \leq f$. Then the set

$$\{w_{11}, w_{11}x, \ldots, w_{11}x^{u-1}, \ldots, w_{fb}, w_{fb}x, \ldots, w_{fb}x^{u-1}\}$$

is a basis for V over $\mathbb{F}_q$ and thus

$$|C_V(x)| \leq q^{\frac{zb}{u}}.$$

In particular, $|C_K(x)| \leq q^{\frac{zb}{3}}$, since z_i has odd order for all i.

Let $n \in NZ(X)$, let $\ell \in L$, and let U be an irreducible $\mathbb{F}_q[< n >]$-submodule of $W\ell$. Suppose that $u = \frac{|<n>|}{C_{<n>}(U)}$ and that $b_n = o(q) \bmod u$. Then, by Theorem 1.1.1, U is either the trivial $\mathbb{F}_q[< n >]$-module or there exists a uth root of unity ϵ of $F = \mathbb{F}_{q^{b_n}}$, by Lemma 3.4.10, such that U is isomorphic to F viewed as an $\mathbb{F}_q[< n >]$-module via the $< n >$-action

$$xn^i = x\epsilon^i \quad \text{(field multiplication)}$$

for all $x \in F$ and $0 \leq i \leq o(n) - 1$. Furthermore, by Clifford's Theorem [1, Theorem 6.5, page 80],

$$Wc = \underbrace{U \oplus \cdots \oplus U}_{\frac{b}{b_n}},$$

since N is abelian. Thus n either centralizes $W\ell$ or n acts fixed-point freely on $W\ell$. So

$$|C_K(n)| = |C_V(n)| = q^{k(n)b},$$

where $k(n) = |\{\ell \in L : n \in M^\ell\}|$. If $n \not\in N$, then clearly $k(n) = 0$, since $M \subseteq N$. If $n \in N$ and $\overline{X} = X/Z(X)$, then

$$k(n) = k(\overline{n}) = |\{l \in L : \overline{n} \in \overline{M}^{\overline{l}}\}|.$$

But

$$\overline{X} = \overline{X}_{p_1} \times \cdots \times \overline{X}_{p_t},$$

where $\overline{X}_{p_1} = \overline{N}_{p_s}\overline{C}_{p_s}$ and $\overline{N}_{p_s} \cap \overline{C}_{p_s} = 1$. So there exists a unique element $\overline{n}_{p_s} \in N_{p_s}$ for $1 \leq s \leq t$ such that

$$\overline{n} = \overline{n}_{p_1} \dots \overline{n}_{p_t}.$$

and if we choose any one element $\overline{c}_{p_s}$ from each subgroup $\overline{C}_{p_s}$ for $1 \leq s \leq t$ then there exists a unique $\overline{\ell} \in L$ such that $\overline{\ell} = \overline{c}_{p_1} \dots \overline{c}_{p_t} n_\ell$. So $\overline{n} \in \overline{M}^{\ell}$ if and only if $\overline{n}_{p_s} \in \overline{M}_{p_s}^{\overline{c}_{p_s}}$ for $1 \leq s \leq t$. Thus

$$k(n) = k(\overline{n}) = \Pi_{s=1}^{t} k_{p_s}(\overline{n}_{p_s}),$$

where $k_{p_s}(\overline{n}_{p_s}) = |\{\overline{c}_{p_s} \in \overline{C}_{p_s} : \overline{n}_{p_s} \in \overline{M}_{p_s}^{\overline{c}_{p_s}}\}|$. Finally, since $\overline{X}_{p_s}$ is a direct product of Frobenius groups satisfying the conditions in Lemma 5.6.4 we see that

$$|C_K(n)| \leq q^{\frac{3zb}{4}}$$

for $1 \neq n \in N$.

Let $\lambda_1 = 1_K, \dots, \lambda_t$ be a set of orbit representatives of $Irr(K)$ regarded as an X-set. Then

$$Irr(G) = Irr(G|\lambda_1)\dot{\cup}\cdots\dot{\cup}Irr(G|\lambda_t),$$

where $Irr(G|\lambda_i) = \{\chi \in Irr(G) : < \chi_K, \lambda_i > \neq 0\}$. Furthermore,

$$\lambda_i^G = \sum_{\chi \in Irr(G|\lambda_i)} a_\chi \chi,$$

where $a_\chi \neq 0$ for all $\chi \in Irr(G|\lambda_i)$. So

$$|X|(t-1) = \sum_{i=2}^{t} \lambda_i^G(1) \geq \sum_{\chi \in Irr(G) - Irr(G|1_K)} \chi(1)$$

and $|X|(t-1) + yzc \geq yzcq^h$, since

$$yzc = \sum_{\chi \in Irr(G|1_K)} \chi(1).$$

Re-arranging the inequality we obtain

$$|X|t - yzcq^h - (x-y)zc \geq 0.$$

Now suppose that $\chi_1, \ldots, \chi_t$ are elements of $Irr(G|\lambda_1), \ldots, Irr(G|\lambda_t)$ respectively. Then, by Clifford's Theorem [1, Theorem 6.5, page 80], $\chi_i(1)$ is greater than or equal to the length of the orbit of $Irr(K)$ containing λ_i for all i. So

$$p^{zb} \leq \sum_{i=1}^{t} \chi_i(1) \leq \sum_{\chi \in Irr(G)} \chi(1) = yzcq^h < yzq^{h+b},$$

since $|Irr(K)| = |K| = q^{zb}$ and $c|q^b - 1$, and consequently $q^{(z-1)b-h} \leq yz - 1$.

Suppose that $h \leq \frac{7zb}{8} + 1$. Then

$$2^{\frac{z-8}{8}-1} \leq 2^{\frac{(z-8)b}{8}-1} \leq q^{\frac{(z-8)b}{8}-1} \leq q^{(z-1)b-h} \leq yz < z^2$$

and applying the substitution $z = 8(w+1) + 8$ we obtain

$$2^w \leq 64w^2 + 144w + 256.$$

So w must be less than 14 and z must be less than 128, if $h \leq \frac{7z}{8} + 1$.

Let $P(q) = \sum_{x \in X} C_K(x) - yzcq^h - (x-y)zc$, a polynomial of degree zb in q. Then

$$P(1) = xzc - yzc - xzc + yzc = 0.$$

and consequently there exists a polynomial $Q(q)$ of degree $zb - 1$ such that

$$P(q) = (p-1)Q(q).$$

Suppose that $P(q) = a_{zb}q^{zb} + \cdots + a_1 q + a_0$ and

$$Q(q) = b_{zb-1}q^{zb-1} + \cdots + b_1 q + b_0.$$

Then $a_n = b_{n-1} - b_n$ for $1 \leq n \leq zb - 1$ and $b_0 = -a_0$. So

$$b_n = -\sum_{i=0}^{n} a_i = \sum_{i=n+1}^{zb} a_i,$$

for $0 \leq n \leq zb - 1$, since $\sum_{i=0}^{zb} a_i = 0$.

Now $C_X(K) = 1$ and consequently $b_{zb-1} = a_{zb} = 1$. Furthermore, if we assume that $z \geq 121$ then $h > \frac{7zb}{8} + 1$ and

$$\begin{aligned} a_{zb-1} &= a_{zb-2} = \cdots = a_{h+1} = 0, \\ a_h &= -yzc \text{ and} \\ a_{h-1} &= a_{h-2} = \cdots = a_{h-2-(zb-h)} = 0, \end{aligned}$$

since $h - 2 - (zb - h) > \frac{3zb}{4}$ and

$$C_K(x) \leq q^{\frac{3zb}{4}}$$

for all $x \in X$. So if $R(x) = b_{h-3-(zb-h)}q^{h-3-(zb-h)} + \cdots + b_1 q + b_0$, then

$$Q(q) = q^{zb-1} + \cdots + q^h - (yzc-1)q^{h-1} - \cdots - (yzc-1)q^{h-2-(zb-h)} + R(x).$$

Now if ℓ is the smallest prime dividing z, then

$$\sum_{i=h-3-(zb-h)}^{\frac{zb}{\ell}} a_i \leq xc - 1 < yzc - 1,$$

since

$$C_K(x) \leq q^{\frac{zb}{t}}$$

for all $x \in X - NZ(X)$. So using this observation and the fact that $b_{i-1} \geq b_i$ for all $i < h - 1$ we obtain

$$R(x) \leq b_0 q^{\frac{zb}{t}} \leq (x - y)zcq^{\frac{zb}{t}},$$

since $b_0 = -a_0 = (x - y)zc - |\{x \in X : |C_K(x)| = 1\}|$, and consequently

$$R(x) \leq yz^2cq^{\frac{zb}{3}}.$$

Furthermore,

$$(yzc - 1)q^{h-2-(zb-h)} > (yzc - 1)q^{\frac{7zb}{8}+1-2-\frac{zb}{8}+1} = (yzc - 1)q^{\frac{3zb}{4}} > yzcq^{\frac{2zb}{3}}.$$

Suppose that $(yzc - 1)q^{h-2-(zb-h)} \leq R(x)$. Then

$$q^{\frac{2zb}{3}} < zq^{\frac{zb}{3}},$$

and applying the substitution $z = 3w$ we obtain

$$2^w < 3w.$$

Thus $w < 4$ and $z < 12$ contradicting our assumption that $z \geq 128$. Combining this inequality with the inequalities

$$q^{zb-i} \leq (yzc - 1)q^{h-i}$$

for $1 \leq i \leq 1 + (zb - h)$ we see that $Q(q) < 0$ if q is a prime and thus $P(q) < 0$ if q is a prime. But

$$P(q) = \sum_{x \in X} C_K(x) - yzcq^h - (x - y)zc = |X|t - yzcq^h - (x - y)zc \geq 0,$$

by Theorem 5.6.1, and we obtain the desired contradiction.

If $z < 128$ and $m = 1$, then

r_1	n_1	d_1	z_1
2	3	1	7
3	3	1	13
2	4	1	15
2	6	2	21
2	5	1	31
5	3	1	31
7	3	1	57
2	6	1	63
2	9	3	73
2	8	2	85
3	6	2	91
9	3	1	91
3	5	1	121
2	7	1	127

So if $z < 128$, then $m < 3$ and if $m = 2$ then

r_1	n_1	d_1	z_1	r_2	n_2	d_2	z_2	z
2	3	1	7	2	3	1	7	49
2	3	1	7	3	3	1	13	91
2	3	1	7	2	4	1	15	105

In all these cases it can be shown using similar methods to those outlined in this proof and those in Theorem 5.6.2 that G does not possess a model subgroup. □

Chapter 6

Main Theorem

In this chapter we shall prove the main results of this thesis. In doing so we shall establish under what circumstances a minimal non-$\mathcal{X}$-group of derived length 3 satisfying the conditions in Case D possesses a model subgroup. We will go on to formulate two conjectures and give examples of metabelian minimal non- $\mathcal{X}$-groups satisfying the conditions outlined in Cases D and G in order to shed light on some of the problems still to be overcome.

6.1 Metabelian Groups

Theorem 6.1.1 *Suppose that G is a metabelian finite soluble group satisfying*

$$(|G'|, |G : G'|) = 1$$

and that G possesses a model subgroup. Then there exists a group $L = L_1 \times \cdots \times L_m$ where L_i is a Frobenius group with minimal Frobenius kernel

N_i and abelian Frobenius complement C_i, and a homomorphism

$$\mu_G : G \to L.$$

such that $ker\mu \cap G' = 1$. In particular, G is a $\mathcal{X}$-group if μ_G is an epimorphism.

Proof. Since $(|G'|, |G : G'|) = 1$, the derived group G' is complemented in G by an abelian group, B say. Let

$$\Pi = \{p_1, \ldots, p_t\}$$

be the set of primes dividing the order of G' and let G'_{p_s} be the p_s-Sylow subgroup of G'. Then

$$G' = G'_{p_1} \times \cdots \times G'_{p_t}.$$

Suppose that $C_B(G'_{p_s}) = B$ for some j. Then

$$G = G'_{p_s} \times \hat{G}'_{p_s},$$

where

$$\hat{G}'_{p_s} = \left(G'_{p_1} \times \cdots \times G'_{p_{s-1}} \times \cdots \times G'_{p_{s+1}} \times \cdots \times G'_{p_t}\right) B,$$

and consequently

$$G' = \hat{G}'_{p_s},$$

contradicting the fact that $G'_{p_s} \subseteq G'$. So $B/C_B(G'_{p_s})$ is a non-trivial p'_s-group of automorphisms of G'_{p_s} for $1 \leq s \leq t$ and thus

$$G'_{p_s} = X_{s1} \times \cdots \times X_{sm_s},$$

where X_{sj} is homocyclic and $X_{sj}/\Phi(X_{sj})$ is an irreducible $B/C_B(G'_{p_s})$-group for $1 \leq j \leq m_s$. Furthermore, using a similar argument to one above we can show that $C_B(X_{sj}) \neq B$ for $1 \leq s \leq t$ and $1 \leq j \leq m_s$. Let

$$\hat{X}_{sj} = X_{s1} \times \cdots \times X_{s(j-1)} \times X_{s(j+1)} \times \cdots \times X_{sm_s}$$

and let

$$K_{sj} = \left(G'_{p_1} \times \cdots \times G'_{p_{s-1}} \times \hat{X}_{sj} \times G'_{p_{s+1}} \times \cdots \times G'_{p_t}\right) C_B(X_{sj}).$$

Clearly, K_{sj} is a normal subgroup of G and

$$G/K_{sj} \cong [X_{sj}]B_{sj},$$

a Frobenius group with homocyclic Frobenius kernel X_{sj} and Frobenius complement $B_{sj} = B/C_B(X_{sj})$. But if H is a model subgroup of G then by Theorem 2.3.2 HK/K is a model subgroup of G/K, so by Theorem 3.3.6 we see that X_{sj} must be minimal for $1 \leq s \leq t$ and $1 \leq j \leq m_s$. Let

$$L = L_{11} \times \cdots \times L_{tm_t},$$

where $L_{sj} = [X_{sj}]B_{sj}$, and let μ_B be the map defined from B to $B_{11} \times \cdots \times B_{tm_t} \subseteq L$ by

$$\mu_B(b) = (bC_B(X_{11}), \ldots, bC_B(M_{tm_t}))$$

for all $b \in B$. Then μ_B is clearly a homomorphism. Furthermore, if μ_G is the map defined from G to L by $\mu_G(g'b) = g'\mu_B(b)$ for all $g' \in G'$ and $b \in B$, then μ_G is a homomorphism and

$$\mu_G(G') = X_{11} \times \cdots \times X_{tm_t}.$$

The result now follows by Lemma 4.2.2. □

6.2 Soluble Groups

We are ready to prove our main result.

Theorem 6.2.1 *Let G be a non-abelian finite soluble group and let $\overline{G} = G/G''$. Suppose that G possesses a model subgroup,*

$$(|\overline{G}'|, |\overline{G} : \overline{G}'|) = 1,$$

and that the homomorphism $\mu_{\overline{G}}$ defined in the proof of Theorem 6.1.1 is onto. Then one of the following three conditions is satisfied :

(a) *G is metabelian.*

(b) *G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius complement of order $2^n + 1$.*

(c) *G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^6 and cyclic Frobenius complement of order $(2^6 - 1)/(2^2 - 1)$.*

Proof. Let G be a minimal counter-example to our claim. Then $K = G''$ is a minimal normal subgroup of G and G/K is a $\mathcal{X}$-group by Theorem 6.1.1. Suppose that N is a minimal normal subgroup of G satisfying $K \cap N = 1$. Then $(G/N)'' = KN/N$ and G/KN is a $\mathcal{X}$-group by Lemma 4.2.1 contradicting the minimality of G. So we may assume without loss of generality that K is the unique minimal normal subgroup of G and re-applying Lemma 4.2.1 we see that G is a minimal non-$\mathcal{X}$-group of derived length 3. The result now follows by Lemma 4.3.2, Lemma 4.3.3, Lemma 4.3.4, Lemma 5.1.1 , Theorem 5.2.4 , Theorem 5.4.1 and Theorem 5.6.2. □

The primary function of the two conditions set out in Theorem 6.2.1 is to limit the number of potential counter-examples that have to be considered. For instance, in the Case studies considered we only use the co-prime condition in Theorem 5.6.2 and this does not appear to have a crucial impact upon its proof. In order to illustrate this point further we return to Case D.

6.3 Case D

In this section we determine a necessary condition for a minimal non-$\mathcal{X}$-group of derived length 3 satisfying the conditions outlined in Case D to possess a model subgroup. The key observation can be viewed as a generalization of a result which plays an important role in the Higman's classification of Suzuki 2-groups [8, Lemma 4 and Theorem 3].

Theorem 6.3.1 *Let $G = RC$, where R is a special r-group and C is cyclic of order*

$$\frac{r^n - 1}{r^d - 1}$$

for some $d|n$. Suppose that R/R' and R' regarded as $GF(r)[C]$-modules are faithful and irreducible. Then R/R' and R cannot be $GF(r)[C]$-isomorphic unless $r = 2$ and $n = 2d$.

Proof. Let M denote the faithful irreducible $GF(r)[C]$-module R/R'. Then there exists a primitive $(r^n - 1)/(r^d - 1)$-st root of unity λ such that

$$K = GF(r)[\lambda] = GF(r^n)$$

by Theorem 1.1.1 and the $K[C]$-module $M \otimes K$ has a basis

$$u_0, \ldots, u_{n-1}$$

such that

$$u_i c = \lambda^{r^i} u_i$$

for $i \in \{0, \ldots, n-1\}$. Let N denote the faithful irreducible $GF(r)[C]$- module R'. Then the $K[C]$-module $N \otimes K$ is spanned by the set of elements

$$\{[u_i, u_j] \mid 0 \leq i < j \leq n-1\}$$

and

$$[u_i, u_j]c = \lambda^{r^i + r^j}[u_i, u_j].$$

Suppose that M and N are $GF(r)[C]$-isomorphic. Then

$$\lambda = \lambda^{r^i + r^j}$$

for some pair $\{i, j\}$ satisfying $0 \leq i < j \leq n-1$, by an argument outlined by Higman [8, Lemma 4 and Theorem 3]. In other words

$$r^i + r^j - 1 \equiv 0 \, mod \, \frac{r^n - 1}{r^d - 1}.$$

But $i < j \leq n-1$ and consequently there exists a $y < r^d - 1$ such that

$$r^i + r^j - 1 = y \times (r^{n-d} + \cdots + r^d + 1)$$

for some pair $\{i, j\}$ such that $0 \leq i < j \leq n-1$.

If $i \leq j < d$, then $r^i + r^j - 1 < r^d$, a contradiction.

If $d \leq i < j$, then

$$r^i + r^j - 1 = y \times r^d \times (r^{n-2d} + \cdots + r^d + 1) + y$$

and

$$r^i + r^j - (y+1) = y \times r^d \times (r^{n-2d} + \cdots r^d + 1).$$

So $(y+1)$ must be congruent to 0 mod r^d contradicting our assertion that $y < r^d - 1$.

If $i < d$ and $d < j$, then

$$r^i - 1 - y = y \times r^d \times (r^{n-2d} + \cdots + r^d + 1) - r^d(r^{j-d})$$

and

$$r^i - 1 - y \equiv 0 \, mod \, r^d,$$

which implies that $r^i - 1$ must equal y. So

$$\begin{aligned} r^i + r^j - 1 &= (r^i - 1)(r^{n-d} + \cdots + r^d + 1) \\ &= r^{i+n-d} + \cdots + r^{i+d} + r^i - r^{n-d} - \cdots - r^d - 1 \end{aligned}$$

and

$$\begin{aligned} r^j &= r^{i+n-d} + \cdots + r^{d+i} - r^{n-d} - \cdots - r^d \\ &= r^d(r^{i+n-2d} + \cdots + r^i - r^{n-2d} - \cdots - r^d - 1), \end{aligned}$$

a contradiction.

If $i < j = d$, then $n = 2d$, $r = 2$ and $i = 1$. The proof is complete. □

The following example illustrates that if $n = 2d$ and $r = 2$, then groups do exist satisfying the conditions above.

Let $F = GF(2^6)$, let θ be the automorphism of F of order 3 defined by

$$a^\theta = a^4$$

for all $a \in F$, and $F^\times =< \lambda >$. Let $\mu = \lambda^7$ and let

$$G = [A(6,\theta)]C$$

be the semi-direct product of $A(6,\theta)$ and $C =< \xi_\mu >$, a cyclic group of order

$$\frac{2^6 - 1}{2^3 - 1},$$

where $A(6,\theta)$ and ξ_μ are as defined in Section 5.3. Then $A(6,\theta)$ is a Suzuki 2-group by Theorem 5.3.3,

$$A(6,\theta)' = \mathcal{R}$$

where $\mathcal{R}$ is as defined in Section 5.3, and $A(6,\theta)/\mathcal{R}$ and $\mathcal{R}$ regarded as $GF(2)[C]$-modules are faithful and irreducible. Furthermore, $A(6,\theta)/\mathcal{R}$ and $\mathcal{R}$ are isomorphic regarded as $GF(2)[C]$-modules. It can be shown that this group does not possess a model subgroup.

Theorem 6.3.2 *Let $G = (G'A)C$ be a finite group satisfying the following conditions :*

(i) $(|G'A|, |C|) = 1$;

(ii) $K = [G', A]$ *is the unique minimal normal subgroup of* G;

(iii) $A/K = Z(G/K)$;

(iv) *G/A is a Frobenius group at CA/A with minimal Frobenius kernel $G'A/A$;*

(v) *$G'A$ is an r-group;*

(vi) *A is an elementary abelian r-group;*

(vii) *G' is a special r-group;*

(viii) *$K = \Phi(G'A) = (G'A)'$ and $K \subseteq Z(G'A)$.*

Then either G does not possess a model subgroup or G/A is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius kernel of order $2^n + 1$.

Proof. Suppose that G has a model subgroup H. Then HA/A is a model subgroup of G/A by Theorem 2.3.2 and consequently by Theorem 3.2.1

$$|C| = \frac{r^n - 1}{r^d - 1}$$

for some d dividing n.

Let $a \in A - K$. Then the map ϕ_a from G'/K to K defined by

$$\phi_a(g'K) = [g', a]$$

for all $g'K$ is well-defined and is a homomorphism, since $K \subseteq Z(G'A)$. Furthermore, if $B = < a > K \triangleleft G$, then

$$A \subseteq C_G(B) \triangleleft G,$$

and consequently $C_G(B)$ either equals A or contains $G'A$, since $G'A/A$ is the unique minimal normal subgroup of G/A.

Suppose that $C_G(B)$ is indeed contained in $G'A$. Then $G/C_G(B)$ has order co-prime to p. So we can apply Maschke's theorem to the elementary abelian group B regarded as an $\mathbb{F}_p[G/C_G(B)]$-module. Hence

$$B = K \times L,$$

where $L \cong B/K$ is an $\mathbb{F}_p[G/C_G(B)]$-module, contradicting the fact that K is the unique minimal normal subgroup of G.

So we may assume without loss of generality that $C_G(B) = A$ and consequently the homomorphism ϕ_a is a monomorphism. Furthermore, since K is an irreducible C-module and G'/K is a faithful irreducible C-module, the order of K must be less than or equal to that of G'/K, by Theorem 1.1.1. So ϕ_a is an isomorphism. Finally, we observe that

$$\phi_a((g'K)^c) = [g'^c, a] = [g', a]^c = \phi_a(g'K)^c,$$

since $a \in Z(G/K)$ and $K \subseteq Z(G'A)$. So G'/K and K are $\mathbb{F}_p[C]$-isomorphic. The result now follows by Theorem 6.3.2. □

6.4 Nilpotent-by-Abelian Groups

Theorem 6.4.1 *Let G be a nilpotent-by-abelian group and let $\overline{G} = G/G''$ be a $\mathcal{X}$-group. Then G possesses a model subgroup only if one of the following three conditions is satisfied :*

(a) *G is metabelian.*

(b) *G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius complement of order $2^n + 1$.*

(c) *G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^6 and cyclic Frobenius complement of order $(2^6-1)/(2^2-1)$.*

Proof. Let G be a minimal counter-example to our claim. Then $K = G''$ is a minimal normal subgroup of G and G/K is a $\mathcal{X}$-group. Suppose that N is a minimal normal subgroup of G satisfying $K \cap N = 1$. Then $(G/N)'' = KN/N$ and G/KN is a $\mathcal{X}$-group by Lemma 4.2.1 contradicting the minimality of G. So we may assume without loss of generality that K is the unique minimal normal subgroup of G and re-applying Lemma 4.2.1 we see that G is a minimal non-$\mathcal{X}$-group of derived length 3. The result now follows by Lemma 4.3.2, Lemma 4.3.3, Lemma 4.3.4, Lemma 5.1.1 , Theorem 5.2.4 , Theorem 5.4.1 and Theorem 6.3.2. □

6.5 Conjecture

Given all that we have seen to date and noting that the group in Example C is not a Frobenius group with elementary abelian Frobenius kernel of order 2^6 and cyclic Frobenius complement of order $(2^6-1)/(2^2-1)$ we make the following conjecture

Conjecture If a finite soluble group G possesses a model subgroup, then G satisfies one of the following two statements :

(a) G is metabelian.

(b) G possesses a normal subgroup N such that G/N is a Frobenius group with elementary abelian Frobenius kernel of order 2^{2n} and cyclic Frobenius complement of order $2^n + 1$.

And finally in order to illustrate some of difficulties that lie ahead in trying to prove the conjecture we give the following two examples of metabelian minimal non- $\mathcal{X}$-groups satisfying the conditions outlined in Cases D and G possessing a model subgroup.

6.6 Example Case D (Metabelian)

Let $F = \mathbb{F}_{r^n}$ and let $F^\times =< \lambda >$ and let M be any maximal subgroup of F^+. Let

$$C = \left\langle \begin{pmatrix} \lambda^{r-1} & 0 \\ 0 & \lambda^{r-1} \end{pmatrix} \right\rangle \subseteq GL(2, F)$$

and let

$$Z = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in M \right\} \subseteq GL(2, F).$$

Let $S = CZ = C \times Z$ and let V be the natural $\mathbb{F}_{r^{2n}}[S]$- module. Then

$$G = [V]S,$$

the external semi-direct product of V and S possesses a model subgroup.

6.7 Example Case G (Metabelian)

Let $F_i = \mathbb{F}_{2^4}$ for $i = 1, 2$. Let $F_i^\times =< \lambda_i >$ for $i = 1, 2$. Let

$$S_i = [F_i^+]\langle\lambda_i\rangle,$$

the external semi-direct product of F_i^+ and $\langle\lambda_i\rangle$ via σ_i, where σ_i is the homomorphism from $\langle\lambda_i\rangle$ to $Aut(F_i^+)$ defined by

$$x_i^{\sigma_i(\lambda_i^j)} = x_i\lambda_i^j \quad \text{(field multiplication)}$$

for all $x_i \in F_i^+$ and $0 \leq j \leq 14$. Let

$$D = S_1 \times S_2.$$

Let

$$C = \langle(\lambda_1^5, 1), (\lambda_1^3, \lambda_2^3), (1, \lambda_2^5)\rangle \subseteq D,$$

and let

$$N = F_1^+ \times F_2^+ \subseteq D.$$

Then

$$G = NC$$

possesses a model subgroup.

Bibliography

[1] Isaacs, I. Martin. *Character theory of finite groups.* Dover Publications, New York, 1994.

[2] Huppert, B. *Endliche Gruppen I* Springer Verlag, Berlin Heidelberg New York, 1967.

[3] Lidl, R. and Niederreiter, H. *Finite Fields* Encyclopaedia of Mathematics and Its Applications. Cambridge University Press, London New York New Rochelle Melbourne Sydney, 1984.

[4] Kleidman, P. and Liebeck, M. *The Subgroup Structure of the Finite Classical Groups* Cambridge University Press, London Mathematical Society Lecture Note Series. 129, 1990

[5] Doerk K. and Hawkes T.O. *Finite Soluble Groups* Walter de Gruyter, Berlin New York, 1992.

[6] Beisiegel, B. *Semi-Extraspezielle p-Gruppen* Math. Z. 156 (1977), no. 3, 247-254

[7] Huppert, B. and Blackburn, N. *Finite Groups II* Springer Verlag, Berlin Heidelburg New York, 1982.

[8] Higman, G. *Suzuki 2-groups* Illinois J. Math. 7, 79-96 (1963)

[9] Gollan, H.W. *On the existence of models in some sporadic simple groups* Arch. Math., 60, 305-309, 1993.

[10] Kljacko, A.A. *Models for the complex representations of the groups* $GL(n,q)$ Math. USSR-Sb, 48, 365-379, 1984.

[11] Inglis, N.F.J. and Richardson, R.W. and Saxl, J. An explicit model for the complex representations of S_n Arch. Math, 54, 258-259, 1990.

[12] Baddeley, R.W. *Models and Involution Models for wreath products and certain Weyl Groups* J.London Math.Soc. (2) 44, 55-74 1991.